ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ

ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

Тези доповідей

27 жовтня 2021

м. Київ

№	ПІБ студента/Назва тези	№ ст
1	*Анохін Дмитро Геннадійович* **ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ**	10 - 11
2	*Висоцький Ігор Ігорович* **ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМИ НА БАЗІ РІШЕННЯ CYBERARK PRIVILEGED ACCOUNT SECURITY**	12 - 14
3	*Гуляєва Оксана Ігорівна* **ПРОТИДІЯ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ДИСТАНЦІЙНОЇ РОБОТИ СПІВРОБІТНИКІВ**	15 - 16
4	*Воскобойник Олексій Володимирович* **АНАЛІТИЧНЕ РІШЕННЯ В ОБЛАСТІ ІБ, ЯКЕ ЗАБЕЗПЕЧУЄ ВСЕБІЧНИЙ МОНІТОРИНГ ЗАГРОЗ В РОЗПОДІЛЕНІЙ МЕРЕЖІ**	17 - 18
5	Дешко Михайло Дмитрович **FORTICASB ЯК ІНСТРУМЕНТ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ**	19 -20
6	*Дорохін Орест Олександрович* **ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ РУХОМОГО ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЙ 4G**	21 - 23
7	*Кабанов Ярослав Вадимович* **ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES**	24 - 27
8	*Колотухін Денис Вадимович* **ТЕХНОЛОГІЯ РОЗПОДІЛЕНОГО ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА**	28 - 30

9	*Кучер Владислав Ігорович* **ТЕХНОЛОГІЯ ЗАХИСТУ ІНТЕРНЕТ-ДОДАТКІВ ЗА ДОПОМОГОЮ AWS WEB APPLICATION FIREWALL**	31 - 34
10	*Кушнір Дмитро Іванович* **ЗАГРОЗИ ПОВ'ЯЗАНІ З ВІДДАЛЕНОЮ РОБОТОЮ. ЯК ЗРОБИТИ ВІДДАЛЕНУ РОБОТУ ЕФЕКТИВНОЮ ТА БЕЗПЕЧНОЮ**	35 - 39
11	*Наконечний Максим Юрійович* **ТЕХНОЛОГІЯ РОЗШИРЕНОГО ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД ЗАГРОЗ НА БАЗІ FortiEDR**	40 - 42
12	*Павловський Олексій Юрійович* **ТЕХНОЛОГІЯ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ НА БАЗІ FortiGate IPS**	43 - 46
13	*Поремський Максим Олександрович* **ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В DEVOPS СЕРЕДОВИЩІ**	47 - 48
14	*Семенова Інна Дмитрівна* **ХАРАКТЕРНІ УРАЗЛИВОСТІ СИСТЕМ ПОБУДОВАНИХ НА ОСНОВІ KNX ТЕХНОЛОГІЙ**	49 - 50
15	*Стрічко Сергій Сергійович* **РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ХМАРНИХ СЕРВІСІВ. МЕТОДИ ЗАХИСТУ**	51 - 53
16	*Смирнов Денис Сергійович* **УЧАСТЬ АРТ ГРУП ДЛЯ ЗБИРАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ**	54 - 55
17	*Хотінь Кароліна Юріївна* **МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ФАЙЛОВИХ СЕРВЕРІВ ОРГАНІЗАЦІЇ**	56 - 59

18	*Ярчук Андрій Андрійович* **МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ СПЕЦІАЛІЗОВАНИХ ПРОЦЕСОРІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ**	60
19	*Багрилевич Олександр Анатолійович* **ДОСЛІДЖЕННЯ СПОСОБІВ І ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМАХ**	61 - 62
20	*Бутковський Семен Валерійович* **ТЕХНОЛОГІЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ ОРГАНІЗАЦІЇ**	63 - 64
21	*Гаврилей Олександр Петрович* **ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ШКІДЛИВИХ ЗАПИТІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ПРОТОКОЛУ DNS**	65 - 66
22	*Гізун Ігор Ігорович* **ТЕХНОЛОГІЯ УПРАВЛІННЯ ІНЦИДЕНТАМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ WAZUH**	67 - 68
23	*Данильченко Юлія Сергіївна* **ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ**	69 - 70
24	*Добреля Віталій Олексійович* **ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАННИМИ В КОРПОРАТИВНІЙ МЕРЕЖІ**	71 - 72
25	*Драгунцов Роман Ігорович* **ЩОДО ОСОБЛИВОСТЕЙ МОНІТОРИНГУ БЕЗПЕКИ СИСТЕМ ACTIVE DIRECTORY**	73 - 74
26	*Дяченко Максим Миколайович* **ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ НА БАЗІ FortiMail**	75 - 76

27	*Зеленко Євгеній Юрійович* **УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ**	77 - 79
28	*Калиндрузь Богдан Миколайович* **ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ DECEPTION ТЕХНОЛОГІЇ**	80 - 81
29	*Клімов Антон Олегович* **ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ЗАХИЩЕННИХ ТУНЕЛЕЙ VPN ДЛЯ ОРГАНІЗАЦІЇ СТРИМІНГОВИХ ТЕХНОЛОГІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ**	82 - 83
30	*Коваль Владислав Романович* **ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ**	84 - 86
31	*Красноштан Іван Вікторович* **ТЕХНОЛОГІЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ ПЛАТФОРМИ ESET PROTECT**	87 - 88
32	*Лібега Лілія Андріївна* **ТИПОВИЙ СЦЕНАРІЙ РЕАГУВАННЯ НА ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	89 -90
33	*Нечипуренко Ксенія Олександрівна* **ПРИВІЛЕЙОВАНИЙ ДОСТУП. ЧОМУ ЦЕ ВАЖЛИВО І ЯК ЙОГО КОНТРОЛЮВАТИ**	91 - 92
34	*Нощенко Станіслав Андрійович* **ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ OPEN VPN**	93 - 94
35	*Рєзнік Роман Вікторович* **ПОРІВНЯННЯ ШЛЯХІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ**	95 - 96

36	*Смолєв Євген Сергійович* **ТЕХНОЛОГІЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ВЕБ-ДОДАТКУ СУЧАСНОГО ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ BURP SUITE**	97 - 98
37	*Сокол Антон Васильович* **ВИКОРИСТАННЯ BLOCKCHAIN ДЛЯ IOT**	99 - 100
38	*Шпуй Валентин Іванович* **ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ**	101-103
39	*Стародубець Владислав Олександрович* **МЕТОДИ ТА ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВНУТРІШНІХ ЗАГРОЗ НА ПІДПРИЄМСТВІ**	104-105
40	*Рожко Владислав Геннадійович* **ПОЯВА ТА ЕВОЛЮЦІЯ APT-АТАК**	106-107
41	*Тищенко Віталій Сергійович* **СЕРТИФІКАЦІЙНІ ПРОГРАМИ EC-COUNCIL ТА COMPTIA ДЛЯ ФАХІВЦІВ З IT ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	108-109
45	*Зіновський Ростислав Олександрович* **РОЛЬ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**	110-111
45	*Шекера Ольга Олександрівна* **МЕТРИКИ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**	112-114
46	*Грабчук Артем Ярославович* **ЗАХОДИ ВПРОВАДЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ**	115-119
47	*Данильченко Ю. М.., УБДМ-61* **ПОНЯТТЯ ХМАРНИХ ОБЧИСЛЕНЬ: ОСНОВНІ МОДЕЛІ ТА ХАРАКТЕРИСТИКИ**	120-123

48	*Поляков Дмитро Андрійович* **ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КІБЕРСПОРТИВНИХ ЗАХОДАХ**	124-126
49	*Журавель Вячеслав Олександрович* **ШИФРУВАННЯ ЛОКАЛЬНОГО ДИСКУ, ЯК МЕТОД ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ**	127-129
50	*Кукшин Дарія Вікторівна* **ВИКОРИСТАННЯ МЕТОДУ SWOT- АНАЛІЗУ В ОЦІНЦІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	130-132
51	*Каленський Юрій Миколайович* **АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. АТАКИ НА UEFI**	133-135
52	*Герніченко Гліб Дмитрович* **СЕРІАЛІЗАЦІЯ ТА ДЕСЕРІАЛІЗАЦІЯ. УРАЗЛИВІСТЬ ДЕСЕРІАЛІЗАЦІЇ**	136-138
53	*Єрмак Максим Володимирович* **ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**	139-141
54	*Макеєв Микола Броніславович* **ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА МЕТОДИ ПРОТИДІЇ ПРОГРАМАМ ВИМАГАЧАМ**	142-143
55	*Григоренко Дмитро Юрійович* **АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ**	144-145
56	*Івахненко Маріанна Володимирівна* **АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**	146-147
57	*Ахтьоров Владислав Юрійович* **АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК МЕТОД ПРОТИДІЇ КІБЕРАТАКАМ**	148-151

58	*Грищенко Ярослав Олександрович* **КІБЕРБЕЗПЕКА: ЗАГРОЗИ, ВИКЛИКИ, РІШЕННЯ**	152-154
59	*Костроміна Марія Олександрівна* **ЗАХИСТ ВІД ВИТОКУ ІНФОРМАЦІЇ. РІШЕННЯ DLP**	155-157
60	*Борщ Дмитро Васильович* **АНАЛІЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ**	158-160
61	*Ганченко Марія Іванівна* **ПІДТВЕРДЖЕННЯ ОСОБИСТОСТІ У КОРПОРАТИВНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ**	161-163
62	*Ярчук Андрій Андрійович* **МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ СПЕЦІАЛІЗОВАНИХ ПРОЦЕСІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ**	164
63	*Кравчук В.В* **КІБЕРАТАКИ 2021. СТАТИСТИКА ВИКОРИСТАННЯ КИБЕРЗОГРОЗ**	165-167
64	*Лабяк Дар'я Сергіївна* **АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ БАНКУ**	168-170
65	*Дьячук Олександр Станіславович* **ДОСЛІДЖЕННЯ КІБЕРСКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ**	171-172
66	*Якименко Юрій Михайлович* **ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДИЧНИХ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА ВІД СУЧАСНИХ ВИДІВ ЗАГРОЗ, КІБЕРАТАК І РИЗИКІВ**	173-176

67	*Недодай Михайло Геннадійович* **СПОСОБИ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ У ФОРМАТІ“DEEPFAKE”**	177-179
68	О. О. Коваленко **ОСОБЛИВОСТІ КЕРУВАННЯ ПЕРСОНАЛОМ НА ПІДПРИЄМСТВІ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	180-181
69	*А. В. Жовтюк* **ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ПРОТИ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ З ВИНИ ПЕРСОНАЛУ**	182-184
70	*Кузьменко Дарина Олександрівна,* *Гриньків Роман Васильович,* *Сочинський Орест Романович* **ЩОДО ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙ БЕЗПЕКИ В ПРОЦЕСАХ ЖИТТЄДІЯЛЬНОСТІ**	185-187
71	*Букет Дар’я Анатоліївна* **УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА ДОПОМОГОЮ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ**	188-189

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Анохін Дмитро Геннадійович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

В роботі досліджується питання захисту персональних даних, які підлягають закону України «Про захист персональних даних» та загального регламенту захисту даних (GPDR). Все це зумовлює керівників компаній які оброблюють, зберігають та передають такі дані відповідати таким вимогам як збір, уніфікацію і використання персональних даних в країнах ЄС та України.

Ключові слова: інформаційна система, персональні дані, GDPR.

Загальний регламент про захист даних (General Data Protection Regulation, GDPR) - це нова узагальнена постанова Європейського Союзу, яке замінює собою Директиву ЄС про захист Персональних даних 95/46 / EC (EU Data Protection Directive 95/46 / EC). Даний регламент уніфікує регулювання захисту персональних даних в країнах ЄС і посилює вимоги до захисту персональних даних (будь-якої інформації, що відноситься до ідентифікованого або ідентифікованому фізичній особі (суб'єкт даних), по якій прямо або побічно можна його визначити. до такої інформації належить число ім'я, дані про місце розташування, онлайн ідентифікатор або один або кілька факторів характерних для фізичної, фізіологічної, генетичної, розумової, економічної, культурної або соціальної ідентичності цієї фізичної особи).

Новий регламент націлений на підвищення рівня захисту та надання громадянам контролю над своїми даними. Невиконання правил компаніями веде до накладення великих штрафів.

Підхід до захисту персональних даних в GDPR відображені в семи пунктах:

1. Принцип законності, справедливості і прозорості.
2. Мінімізація даних.
3. Обмеження мети.
4. Точність.
5. Обмеження зберігання.
6. Цілісність і конфіденційність.
7. Підзвітність.

Тому для компаній, які оброблюють, зберігають та передають персональні дані необхідно впроваджувати відповідні методи та заходи щодо захисту персональних даних в IT системах.

Дія GDPR охоплює не тільки правову сферу діяльності організації і питання дотримання вимог, але також зачіпає підрозділи, що відповідають за інформаційні технології, безпеку, управління даними та інформацією.

Для вирішення правові питань і дотримання вимог необхідно в організації запроваджувати такі посади як:

Керівник з питань конфіденційності;

Директор по управлінню ризиками;

Директор з контролю дотримання вимог;

Головний юрисконсульт.

Нові вимоги GDPR приведуть до зміни підходів до розробки та управління технологіями. Для цього необхідно впроваджувати посади відповідальних за інформаційні технології та безпеку, а саме:

Директор з інформаційної безпеки;

Директор по інформаційним технологіям.

Перед фізичними особами та командами, які відповідають за управління інформацією, буде поставлено завдання забезпечення більш чіткого контролю за процесами зберігання, обробку та передачі даних, а також відстеження цих процесів щодо персональних даних. Тож для цього необхідно вводити посади по управлінню даними та інформацією, а саме:

Директор по управлінню даними;

Директор по операційній діяльності.

Для захисту персональних даних регламент GDPR рекомендує використовувати псевдонімізацію та шифрування як два механізми, які можна використовувати для захисту персональних даних. Ці механізми необхідно дослідити та надати рекомендації щодо їх застосування.

Перелік посилань:

1. Закону України «Про захист персональних даних» [Електронний ресурс] – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/ed_2010_06_01/T102297.html .

2. NIST SP-800-38G [Електронний ресурс] – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38G.pdf .

3. Топ 10 питань захисту персональних даних [Електронний ресурс] – Режим доступу: https://ecpl.com.ua/news/top-10-pytan-u-sferi-zakhystu-personal-nykh-danykh/ .

4.Особливості GPDR [Електронний ресурс] – Режим доступу: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/gdpr.pdf .

ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ НА БАЗІ РІШЕННЯ CYBERARK PRIVILEGED ACCOUNT SECURITY

Висоцький Ігор Ігорович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

В роботі розглядається необхідність впровадження управління привілейованим доступом до інформаційної системи організації, який є першим кроком для забезпечення кібербезпеки організації. Виток даних, отримання доступу до роботи інформаційної системи може скомпрометувати організацію, нанести великих фінансових збитків, втрату репутації. Тому дослідження технології привілейованого доступу є актуальною.

Ключові слова: привілейований доступ, інформаційна системи, життєвий цикл.

Для виконання бізнес-процесів будь-яка компанія використовує інформаційну систему, яку адмініструють адміністратори з привілейованим доступом, крім цього для запуску відповідних процесів в системі виконуються відповідні привілейовані процеси. Саме такі дані повинні бути захищені в інформаційній системи, адже отримання адміністративних привілеїв становлять загрозу щодо кібербезпеки компанії. Не меншу небезпеку можуть нести і надлишкові права власних співробітників організації, здатних скористатися відсутністю контролю і заподіяти компанії збиток - з корисливих мотивів або з особистих мотивів. Тому є необхідність в впровадженні рішень щодо захисту привілейованого доступу та впровадження PAM-систем [1].

Для визначення кому необхідно надавати привілейований доступ, необхідно визначити склад і функції фахівців інформаційної системи організації [2]. До них необхідно віднести:

Адміністратор - це фахівець (або група фахівців), який розуміє потреби кінцевих користувачів, працює з ними в тісному контакті і відповідає за визначення, завантаження, захист і ефективність роботи необхідних ресурсів системи. Він повинен координувати процес збору інформації, проектування і підтримки, враховувати поточні та перспективні потреби користувачів [1].

Системні програмісти займаються розробкою і супроводом базового програмного забезпечення ЕОМ (ОС, СУБД, трансляторів, сервісних програм загального призначення).

Прикладні програмісти розробляють програми для реалізації запитів до БД інформаційної системи організації.

Аналітик будує математичну модель предметної області, виходячи з інформаційних потреб кінцевих користувачів; ставить завдання для прикладних програмістів.

Саме для PAM Gartner визначив основні допущення стратегічного планування кібербезпеки компаній [3].

До 2024 року 50% організацій будуть впроваджувати модель привілейованого доступу «точно в строк», яка усуває постійні привілеї, і на 80% зменшує порушення привілеїв, ніж у тих, які цього не роблять.

До 2024 року 65% організацій, що використовують функції автоматизації привілейованих завдань, заощадять 40% витрат на персонал для IT-операцій для IaaS і PaaS і отримають на 70% менше порушень, ніж ті, які цього не роблять.

Gartner визначає ринок управління привілейованим доступом (PAM) як інструменти, які пропонують одну або декілька з наступних функцій:

• Виявлення, управління і управління привілейованими обліковими записами (облікові записи з привілеями суперкористувача / адміністратора) в декількох системах і додатках.

• Керування доступом до привілейованих облікових записів, включаючи загальний та аварійний доступ.

• Випадкова зміна, управління і зберігання облікових даних (пароль, ключі і т. д.) Для облікових записів адміністраторів, служб і додатків.

• Забезпечення єдиного входу (SSO) для привілейованого доступу, щоб запобігти розкриттю облікових даних.

• Відстеження, фільтрація і координація привілейованої команди, дії і завдання.

• Управління обліковими даними додатків, служб і пристроїв і відправка їх посередникам, щоб уникнути викриття.

• Моніторинг, запис, аудит і аналіз привілейованого доступу, сеансів і дій.

Привілейовані облікові записи можуть бути людськими або нелюдськими. Деякі привілейовані облікові записи пов'язані з окремими особами, такими як бізнес-користувачі або мережеві адміністратори, в той час як інші є обліковими записами додатків, що використовуються для запуску служб, і не пов'язані з унікальною особистістю людини.

Після оцінки впливу на дані, наступним кроком до зрілості буде дотримання життєвого циклу привілейованого доступу. Це допоможе швидко просунутися по шляху захисту і захисту привілейованого доступу[4,5].

Основними кроками життєвого циклу PAM є:
Визначати
Виявити
Керувати і захищати
Моніторинг
Виявлення ненормального використання
Реагування на інциденти
Аналіз та аудит

Таким чином життєвий цикл PAM є неперевний процес, для роботи якого необхідно впроваджувати відповідні рішення для управління привілейованим доступом до інформаційної системи організації.

Для цього будемо досліджувати система управління привілейованими обліковими записами CyberArk Privileged Account Security Solution - рішення корпоративного класу, орієнтоване на великі центри обробки даних (локальні і хмарні), а також на OT / SCADA-середовища. Рішення є комплексним і включає

в себе ряд модулів: Enterprise Password Vault, Privileged Session Manager, SSH Key Manager, Application Identity Manager, CyberArk Viewfinity, On-Demand Privileges Manager (рис.1).

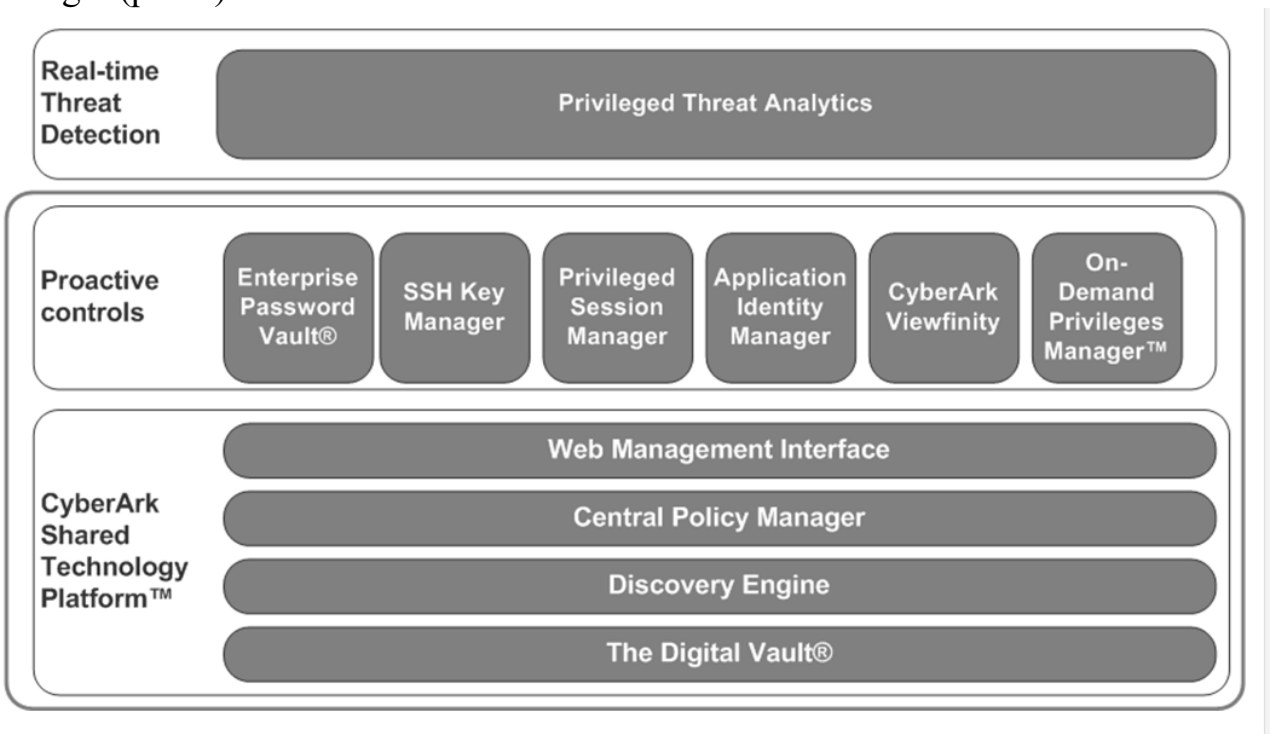


Рис.1. Склад модулів CyberArk Privileged Account Security

Таким чином, робота всіх модулів разом забезпечує закінчене комплексне рішення для управління привілейованими користувачами.

Перелік посилань

1. Герард Блокдик Полное руководство по управлению привилегированным доступом. – 2020. - 450с.
2. NIST Cybersecurity Framework.
3. Cyberark. Програма привілейованого доступу. [Електронний ресурс]. – Режим доступу: https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/IMP-Program/IMP-Program-discoveryANDplanning.htm?tocpath=Get%20Started%7CImplementation%20Program%7C_____1.
4. Blueprint-for-PAM. [Електронний ресурс]. – Режим доступу: http://www.robyhill.com/yahoo_site_admin/assets/docs/Blueprint-for-PAM-Success-WP-1.8341041.pdf.
5. Архітектура PAM. [Електронний ресурс]. – Режим доступу: https://blog.51sec.org/2019/07/cyberark-notes.html.

ПРОТИДІЯ СОЦІАЛЬНОМУ ІНЖИНІРИНГУ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ДИСТАНЦІЙНОЇ РОБОТИ СПІВРОБІТНИКІВ

Гуляєва Оксана Ігорівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

В тезі йдеться про проблеми соціальної інженерії під час дистанційної роботи співробітників. Проаналізовані звіти компаній VMware та Positive Technologies щодо проблем кібератак методом соцінженерії. Надані рішення для власників підприємств, які не в змозі, з різних причин (в т.ч. фінансових), створити власний відділ інформаційної безпеки для зменшення ризиків атак методом соціальної інженерії.

Кіберзлочинці все частіше використовують методи соціальної інженерії для проникнення в інфраструктуру організації при цільової атаці. Людський фактор як і раніше залишається слабкою ланкою в будь-якій системі захисту корпоративних даних, тому сьогодні, в умовах дистанційної роботи співробітників, обумовленої спалахом пандемії Covid-19, як ніколи зростає потреба в навчанні співробітників основам інформаційної безпеки.

З точки зору безпеки даних – дистанційна робота стала серйозною проблемою. Аналізуючи звіт Global Security Insights компанії VMware про проблеми кібератак і уразливості систем безпеки компаній з усього світу, можна окреслити такі статистичні дані [1]:

- 76% опитаних респондентів вказали, що кількість атак збільшилась в 2 рази (більше 2 цілеспрямованих проникнень на рік);
- 78% респондентів вказали що з переходом співробітників на дистанційний формат роботи атаки стали частішими;
- більше 60% співробітників працюють з дому, де умови роботи не відповідають стандартам інформаційної безпеки.

За даними звіту компанії Positive Technologies «Актуальні кіберзагрози: II квартал 2021 року» частка соціальної інженерії зросла з 36% в I кварталі 2021 року до 53% в II кварталі [2].

Основною причиною всіх проблем є те, що організації часто просто не хочуть вживати належних заходів з інформаційної безпеки і інвестувати в неї.

Натомість соціальні інженери використовують в своїй діяльності психологічні маніпуляції, які не потребують великих витрат і специфічних знань, а ще їх складно виявити.

В умовах віддаленої роботи «периметр» захисту компанії розширився до домашніх мереж та особистих пристроїв співробітників. Окрім того, складні економічні умови та відповідні кадрові рішення могли призвести до демотивації персоналу. Ризик зловмисних дій з боку інсайдерів значно зріс [3].

Часто трапляється, що компанії не мають власного відділу інформаційної безпеки з різних причин (в т.ч. фінансових). В цьому випадку найбільш правильним рішенням для розуміння стану справ з кібербезпеки можуть стати консультаційні послуги, які приміром, надаються компаніями: Deloitte,

TechExpert, ProNET та багатьма іншими. Вони допомагають організаціям запобігати кібератакам та захищати цінні активи.

На мою думку, однією з актуальних послуг подібних компаній в умовах дистанційної роботи співробітників є емуляція фішингової атаки. З її допомогою можна оцінити обізнаність персоналу щодо правил кібергігієни шляхом проведення розсилки або дзвінків співробітникам компанії та аналізу їхніх дій.

Отже, перехід на віддалений режим роботи підвищує ризики для інформаційної безпеки. Єдиний вихід для організацій – це інвестування в інформаційну безпеку власного підприємства.

Список використаних джерел:

1. *Інтернет-джерело: https://www.businesswire.com/news/home/20210603005357/en/*
2. *Інтернет-джерело: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threats-2021-Q2-rus.pdf*
3. *Інтернет-джерело: https://www2.deloitte.com/ua/uk/pages/risk/solutions/cybersecurity-on-remote.html*
4. *Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. — К.: ДУТ, 2015.— 288 с.*

АНАЛІТИЧНЕ РІШЕННЯ В ОБЛАСТІ ІБ, ЯКЕ ЗАБЕЗПЕЧУЄ ВСЕБІЧНИЙ МОНІТОРИНГ ЗАГРОЗ В РОЗПОДІЛЕНІЙ МЕРЕЖІ

Воскобойник Олексій Володимирович
студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

Як ви розслідуєте загрози зараження вірусами і шкідливим ПО, які вже трапилися, у вашій інфраструктурі? Як ви розслідуєте питання, пов'язані з мережевою продуктивністю робочих станцій, за умови що знаєте, наприклад, тільки ім'я користувача в мережі? Як ви зараз визначаєте або розслідуєте інсайдерські загрози? Як тільки у вас виникають подібні питання, стає зрозуміло, що традиційні засоби забезпечення ІБ в корпоративній мережі не можуть на них якісно відповісти. Фактично Вам потрібен інструмент, що доповнює традиційні засоби захисту. І такий інструмент є - у всім відомій компанії Cisco є прекрасний продукт під назвою Cisco StealthWatch.

Ключові слова: Cisco StealthWatch, корпоративна мережа, аномальна поведінка

Cisco StealthWatch - це засіб забезпечення ІБ в мережі, яке засноване на зборі телеметричних даних з різних пристроїв, тобто не тільки з МСЕ, які стоять на периметрі, а також з інфраструктурних пристроїв, таких як маршрутизатори, комутатори, сервери з віртуальними машинами і навіть з призначених для користувача пристроїв (не важливо підключені вони зсередини корпоративної мережі або перебувають за її межами).

Оскільки в якості основного протоколу збору даних по телеметрії в рішенні Cisco StealthWatch є широковідомий і популярний NetFlow/IPFIX, це дозволяє обійтися без окремої виділеної фізичної мережі для моніторингу, тобто можна використовувати вже наявне мережеве обладнання. А якщо на якійсь ділянці корпоративної мережі немає пристроїв з підтримкою NetFlow, то в Cisco StealthWatch є рішення і для цього випадку.

Причому Cisco StealthWatch не просто збирає ці дані (тобто є колектором цих даних), він вміє їх дедупліцірувати, збагачувати дані телеметрії даними з інших джерел і т.д., все це формує із розрізнених джерел інформації найбільш повний контекст ІБ про потоках трафіку в корпоративній мережі, доступний в real time режимі. Розширену інформацію про контекст безпеки для Cisco StealthWatch надає інше рішення - Cisco ISE, а також хмарні служби Cisco, що містять бази даних IP / URL-репутацій).

З допомогою Cisco StealthWatch вся корпоративна мережа передачі даних трансформується в єдиний сенсор, детектующий атаки, аномальну поведінку і т.д. Це рішення виходить за межі корпоративної мережі, дозволяючи навіть моніторити хмарні середовища і мобільних користувачів. Рішення знає все про кожен хост і користувача в мережі, записує всі його дії в мережі (в тому числі бачить мережевий трафік на рівні сигнатур додатків), відстежує відхилення від «нормальної» поведінки (причому в рішенні є можливість створення профілю «правильногї» поведінки (baseline) у вигляді механізму автонавчання), забезпечує зберігання цих даних, дозволяє робити вибірки з цих даних (включаючи аналіз підозрілої активності, так як в Cisco StealthWatch вже зашито

більше 100 різних алгоритмів виявлення аномалій і поведінки), попереджає адміністраторів про будь-які зміни. Рішення можна використовувати в якості інструменту для проведення постійного аудиту працездатності традиційних засобів забезпечення ІБ, а також його корисно використовувати для розслідування шляхів поширення шкідливого коду і векторів атаки (та сама можливість «пірнути» в історичні дані).

Якими засобами для аналітики користується дане ПО?

По-перше, поведінкове моделювання та поведінкові сигнатури, іншими словами, постійне відстежування кожного пристрою в мережі і можливість визначати базові показники нормальної і аномального поведінки. Для кожного хоста будь то користувач, сервер або роутер будується свій baseline (ідеальна модель поведінки), відхилившись від якого ми бачимо все аномалії щодо даного хоста.

Як приклад: користувач раптом почав завантажувати великі обсяги даних, хоча він цього ніколи не робив - StealthWatch практично миттєво це визначає.

По-друге, глобальна аналітика загроз. Під цим розуміється інтеграція з відомої Cisco Talos - величезною базою даних сигнатур відомих атак, оновлюваної по всьому світу в режимі реального часу.

По-третє, старе добре машинне навчання, у випадку з Cisco засноване на технології Cognitive Intelligence.

Технологія також лежить в основі рішення ETA - Encrypted Traffic Analytics, яка дозволяє визначити погане чи зашифроване з'єднання без його розшифровки (атака, небажаний трафік і C & C комунікації).

Перелік посилань:

1. Функції моніторингу мережі та аналітика безпеки в масштабах підприємства. URL: https://www.cisco.com/c/ru_ua/products/security/stealthwatch/index.html
2. Cisco StealthWatch або класичні засоби захисту корпоративної мережі (FW, IPS, ACL, NAC, AV, SIEM)? URL: https://habr.com/ru/company/tssolution/blog/414195/

StealthWatch: базові поняття та мінімальні вимоги. URL: https://habr.com/ru/company/tssolution/blog/509812/

FORTICASB ЯК ІНСТРУМЕНТ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ

Дешко Михайло Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

У сучасному світі спостерігається тенденція до переносу сховищ даних та обчислювальних потужностей до хмарних сервісів, це дозволяє знизити операційні витрати компаній та приватних осіб. З цього витікає стрімка необхідність забезпечення стану захищеності хмарних сервісів. Рішення FortiCASB підтримує продукти всіх найбільших постачальників служб SaaS і за допомогою комплексних інструментів ведення звітності надає відомості про користувачів, їх поведінці і стані даних, що зберігаються в хмарі.

FortiCASB призначений для забезпечення видимості, відповідності, безпеки даних та захисту від загроз для хмарних сервісів, які використовуються організацією та взаємодіє з більшістю типів додатків. Додатки SaaS і IaaS дуже гнучкі і економічні, що робить їх дуже привабливими для організацій, проте в процесі відстеження та адміністрування таких програм можуть виникнути труднощі.

SaaS (Software-as-a-Service). Ця хмарна модель - найпоширеніша. Програми та сервіси розробляє і обслуговує провайдер, розміщує їх в хмарі і пропонує кінцевому користувачеві через браузер або додаток на його ПК, технічною підтримкою програм займається провайдер. SaaS-сервіси можуть надавати місце для зберігання файлів (Dropbox), офісний пакет документів для роботи (Google Doc, Microsoft Office 365). Основний клієнт SaaS-сервісів - звичайний користувач.

PaaS (Platform-as-a-Service). В цьому випадку хмарний провайдер надає доступ до операційних систем, засобів розробки і тестування, системам управління базами даних. Провайдер контролює не тільки сервери, системи зберігання даних і обчислювальні потужності, але також пропонує користувачеві на вибір певні платформи і засоби управління ними. Приклади PaaS: Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry. Користувачі PaaS-сервісів - це розробники ПЗ.

IaaS (Infrastructure-as-a-Service). При цій моделі споживач отримує інформаційно-технологічні ресурси - віртуальні сервери з певною обчислювальною потужністю та обсягами пам'яті. Провайдер контролює тільки фізичну та віртуальну інфраструктуру. Приклади IaaS: IBM Softlayer, Hetzner Cloud, Microsoft Azure, Amazon EC2, GigaCloud. Клієнти IaaS - це системні адміністратори компаній.[2]

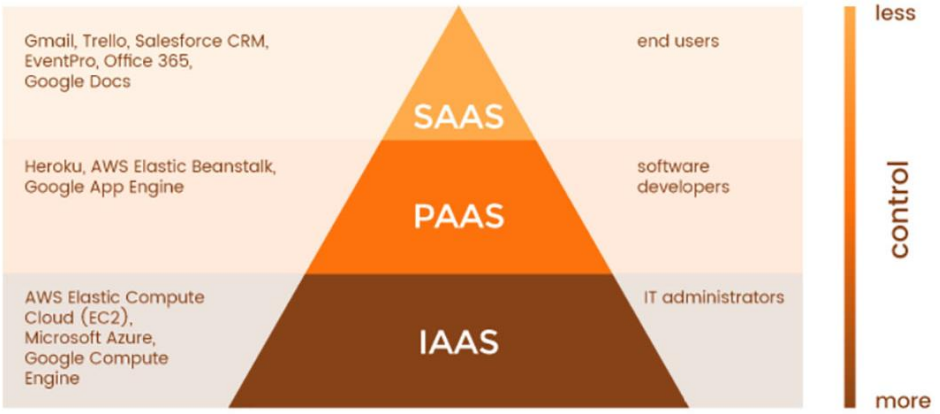


Рис. 1 – Піраміда хмарних сервісів[2]

Рішення FortiCASB підтримує продукти всіх найбільших постачальників служб SaaS і за допомогою комплексних інструментів ведення звітності надає відомості про користувачів, їх поведінку та стан даних, що зберігаються в хмарі. Крім того, це рішення включає нові елементи управління, за допомогою яких в сферу охоплення політик безпеки можна включити не тільки ресурси всередині мережевого периметра (IaaS), але і додатки SaaS.

Особливості та переваги

- Опора на API - Прямий доступ до даних, що зберігаються в хмарі, для забезпечення мережевої та дистанційної захисту.
- Відповідність вимогам і політиці захисту від втрати даних (DLP), - Засоби захисту від втрати даних з можливістю налаштування і попередньо визначені параметри системи звітів про відповідність вимогам.
- Статистика і політика для користувачів - Дані про використання, права і конфігурації забезпечують видимість і контроль для хмарних додатків.
- Інтеграція адаптивної системи мережевої безпеки Security Fabric - Інтегрована «пісочниця» і антивірус сканують зберігаються дані і захищають їх від новітніх загроз.
- Тіньові IT-ресурси - Консолідована звітність для компонентів FortiGate і FortiAnalyzer для визначення використання служб SaaS в мережі.
- Розширена аналітика - Комплексні і прості у використанні візуальні інструменти забезпечують швидку ідентифікацію ризиків і випадків порушення правил.[3,4]

Література

1. https://gigacloud.ua/ru/blog/navchannja/hmarna-piramida-iaas-paas-i-saas
2. https://1cloud.ru/services/private-cloud/iaas-paas-saas
3. https://softprom.com/ru/vendor/fortinet/product/forticasb
4. https://www.fortinet.com/ru/products/cloud-access-security-broker

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ РУХОМОГО ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЙ 4G

Дорохін Орест Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Описані системи рухомого зв'язку на основі технологій 4G було досліджено з метою розробки рекомендації щодо забезпечення безпеки від вразливостей різного виду платформи EPS (Evolved Packet System). Розглянуто шляхи вирішення даного питання через використання захисту абонентів, захисту переданих повідомлень, шифрування повідомлень та аутентифікацію і абонента, і мережі.

Смартфон для людини сьогодення – невід'ємна частина життя, з для виходу в Інтернет з різних місць світу керуючись різною метою. Це може бути: спілкування, пошук маршруту, інформації, замовлення доставки чи таксі, що прибудуть керуючись модулем GPS та мобільним Інтернет працюючими на такому ж смартфоні аналогічно тому, що використовувався для їх виклику й зроблять це завдяки розвитку мереж мобільного зв'язку, саме таких як LTE, що є еволюційним варіантом мережі UMTS (Universal Mobile Telecommunications System) - технології стільникового зв'язку з впровадження 3G в Європі.

Системи рухомого зв'язку на основі технологій 4G працюють на платформі EPS. Розглянемо ці системи з метою розробити рекомендації щодо забезпечення безпеки від вразливостей різного виду платформи EPS (Evolved Packet System)

LTE складається з двох найважливіших компонентів: мережі радіодоступу E-UTRAN та базової мережі SAE (System Architecture Evolution) - архітектура ядра мережі, розробленого консорціумом 3GPP для стандарту бездротового зв'язку LTE. SAE є еволюційним продовженням ядра мережі GPRS. Evolved Universal Terrestrial Radio Access Network є мережею радіодоступу в стандарті LTE й зображена нижче за логікою роботи.

Користь технології, що не забезпечує захисту таких властивостей інформації як конфіденційності, цілісності, й доступності нівелюється.

Саме тому безпека в мережах LTE забезпечується в декількох видах:

- Захист абонентів.
- Захист переданих повідомлень.
- Шифрування повідомлень.
- Аутентифікація і абонента, і мережі.

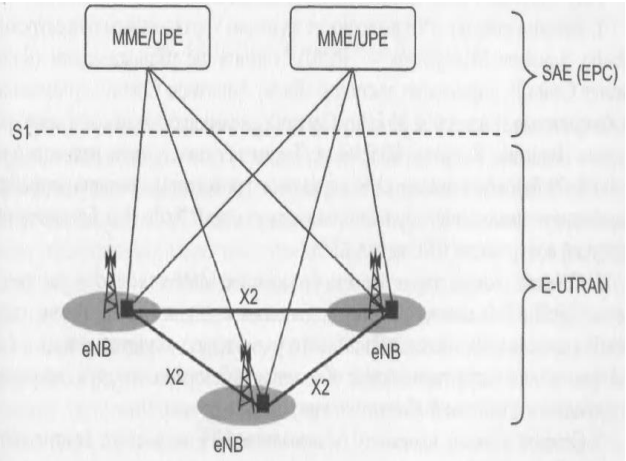


Рис. 1 Архітектура LTE

Після того, як мобільна станція (UE / ME) була ідентифікована, система управління мобільними станціями (MME) в обслуговуючій мережі запитує аутентифікаційні дані з домашньої мережі. Далі MME ініціалізує протокол аутентифікації і угоди по ключам з мобільною станцією. Після успішного завершення виконання даного протоколу, MME і мобільна станція розділяють загальний секретний ключ KASME, де абревіатура ASME - Access Security Management Entity (доступ до сутності управління безпекою). У EPS роль сутності управління безпекою бере на себе MME.

Тепер MME і UE здатні отримати інші ключі з KASME. Два ключа використовуються для захисту конфіденційності та цілісності сигнального трафіку між MME і UE. На рисунку це позначено як 'NAS захист'.

Ще один ключ направляється на базову станцію (eNB). Ще три ключа послідовно випускаються на базовій станції і на мобільної станції. Два з них використовуються для захисту конфіденційності та цілісності сигнального трафіку між eNB і UE - 'AS захист' на рисунку. Третій ключ використовується для захисту конфіденційності даних користувача між eNB і UE - 'UP шифрування'.

Найкраші практики в організації безпеки передбачають такі шляхи:

- Використання AKA (Authentication and Key Agreement) - протоколу аутентифікації і угоди по ключам.
- Ієрархія ключів в EPS
- Безпека платформи для базових станцій

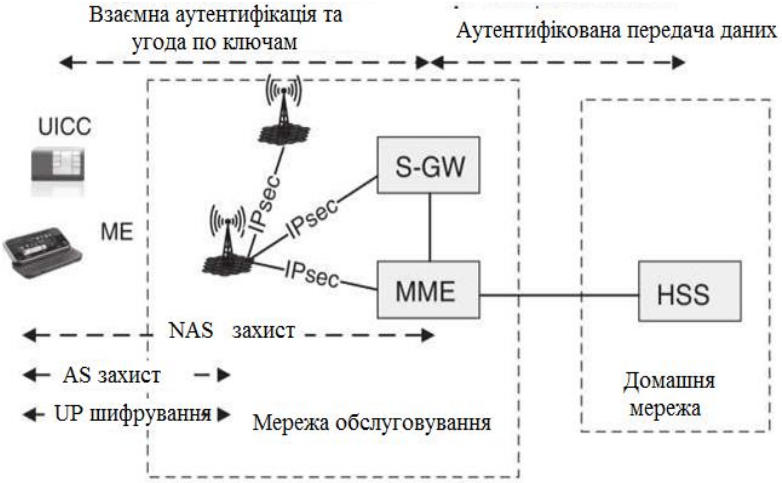


Рис. 2 Архітектура EPS

Основним шляхом та рекомендацією по забезпеченню безпеки мереж LTE було визначено:

1. Використання та удосконалення протоколів аутентифікації АКА, KASME;
2. Розробка та впровадження нових протоколів для забезпечення безпеки базових станцій.

Література:

1. *Архитектура системы безопасности в сетях LTE [Електронний ресурс]. URL: https://ru.wikipedia.org/wiki/Архитектура_системы_безопасности_в_сетях_ LTE*

Технологии GSM и 3G | Сети сотовой связи. [Електронний ресурс]. URL: http://pro3gsm.com/arhitektura-seti-lte/

ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО СЕРВІСІВ ТА РЕСУРСІВ AMAZON WEB SERVICES

Кабанов Ярослав Вадимович, БСДМ-61
Державний університет
телекомунікацій,
м. Київ

Визначено мету і основні завдання щодо управління доступом користувачів до сервісів та ресурсів Amazon Web Services. Розглянуто основні елементи інфраструктури AWS IAM. Досліджено порядок реалізації управління доступом користувачів в AWS IAM.

Компанія Gartner Research визначає ринок хмарних інфраструктур і платформних послуг як стандартизовані, високоавтоматизовані пропозиції, в яких ресурси інфраструктури (наприклад, обчислення, мережа і сховище) доповнюються послугами інтегрованої платформи [1]. Ресурси можуть бути однокористувальницькими або багатокористувальницькими та розміщуватися у постачальника послуг або локально в центрі обробки даних клієнта.

Компанія Gartner Research помістила Amazon Web Services (AWS) в число лідерів в звіті Magic Quadrant for Cloud Infrastructure & Platform Services (CIPS) за 2021 рік. AWS є найпоширенішею в світі хмарною платформою з широкими можливостями, що надає більше 200 повнофункціональних сервісів для центрів обробки даних по всій планеті. Мільйони клієнтів, в тому числі стартапи, які стали лідерами за швидкістю зростання, найбільші корпорації і передові урядові установи, використовують AWS для зниження витрат, підвищення гнучкості і прискореного впровадження інновацій.

AWS Identity and Access Management (IAM) – це веб-сервіс, який допомагає безпечно контролювати доступ до ресурсів AWS. IAM застосовується, щоб контролювати, хто автентифікований (увійшов в систему) і авторизований (має дозвіл) на використання ресурсів. AWS IAM надає інфраструктуру, необхідну для управління автентифікацією й авторизацією профілю користувача. Інфраструктура AWS IAM (рис. 1) включає в себе наступні елементи: терми, принципал, запити, автентифікація, авторизація, дії та операції, ресурси [2].

До ресурсів IAM відносяться об'єкти користувача, групи, ролі, політики та ідентифікатори, які зберігаються. Як і в інших сервісах AWS, ресурси можна додавати, редагувати та видаляти з IAM.

До ідентифікаторів IAM відносяться об'єкти ресурсів IAM, які використовуються для ідентифікації та групування. До ідентифікатора IAM можна додати політику, якій належать користувачі, групи та ролі.

До сутностей IAM відносяться об'єкти ресурсу IAM, які AWS використовує для автентифікації. До них належать користувачі та ролі IAM.

До принципалів відносяться особа або програма, яка використовує кореневого користувача облікового запису AWS, користувача IAM або роль IAM для входу та надсилання запитів до AWS. Принципали включають об’єднаних користувачів та прийняті на себе ролі. Принципал може надсилати запит щодо дії чи операції над ресурсом AWS. Принципал автентифікується як кореневий

користувач облікового запису AWS або сутність IAM для надсилання запитів до AWS.

Коли відповідальна особа намагається використовувати Консоль керування AWS, API AWS або CLI AWS, вона надсилає запит до AWS. Запит містить таку інформацію [2]:

дії або операції, які хоче виконати принципал. Це може бути дія в Консолі управління AWS або операція в інтерфейсі командного рядка AWS або API AWS;

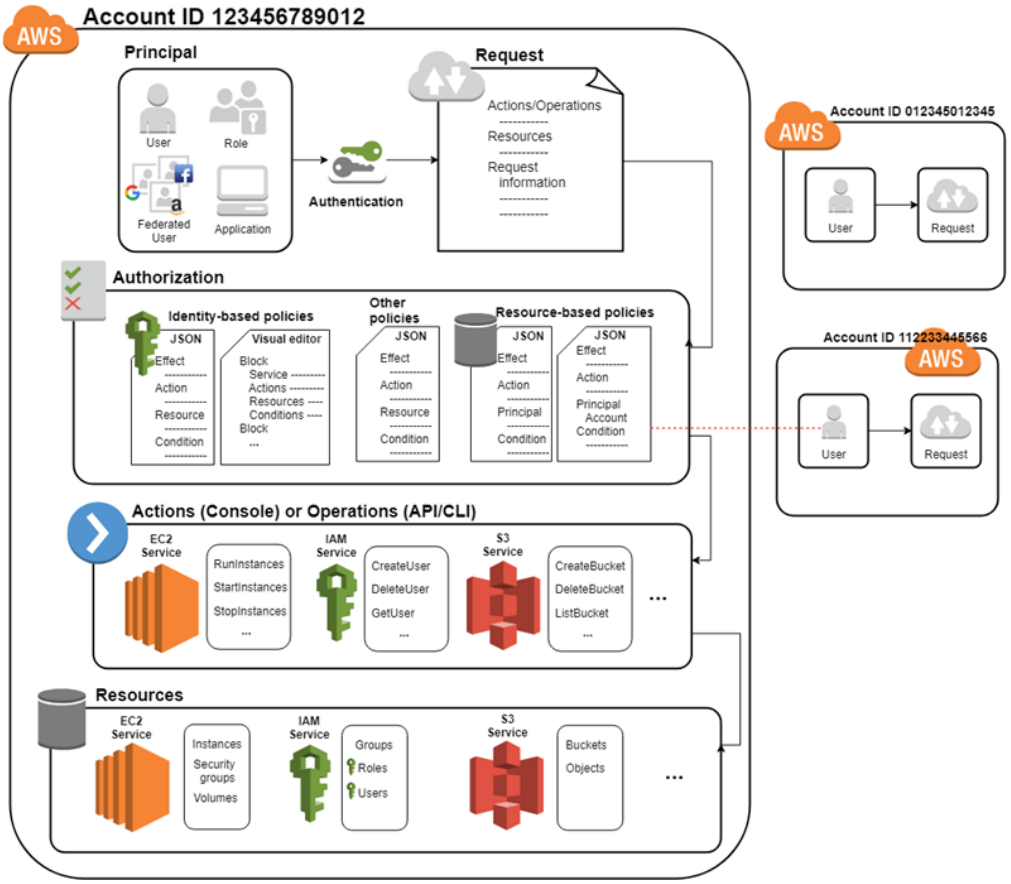


Рис. 1. Основні елементи інфраструктури AWS IAM [2]

ресурси – об'єкт ресурсу AWS, над якими виконуються дії або операції;

принципал – особа або додаток, які використовували сутність (користувача або роль) для відправки запиту. Інформація про принципала включає політики, пов'язані з сутністю, яку принципал використовував для входу в систему;

дані середовища – інформація про IP-адресу, користувача агента, стан включення SSL або час доби;

дані ресурсу – дані, що відносяться до запитуваного ресурсу. Це може включати таку інформацію, як ім'я таблиці DynamoDB або тег в Amazon EC2.

AWS збирає інформацію про запит в контекст запиту, який використовується для оцінки та авторизації запиту.

Принципал повинен пройти автентифікацію (увійти в AWS) з використанням своїх облікових даних для відправки запиту в AWS. Деякі сервіси, такі як Amazon S3 і AWS STS, допускають кілька запитів від анонімних користувачів. Однак вони є винятком із правил.

Щоб пройти автентифікацію з консолі в якості користувача root, необхідно увійти в систему, вказавши свою адресу електронної пошти і пароль. Як користувач IAM, необхідно вказати свій ідентифікатор облікового запису або псевдонім, а потім своє ім'я користувача та пароль. Для автентифікації за допомогою API або інтерфейсу командного рядка AWS необхідно надати ключ доступу і секретний ключ. Коистувачеві також може знадобитися надати додаткову інформацію про безпеку. Наприклад, AWS рекомендує використовувати багатофакторну автентифікацію (MFA) для підвищення безпеки користувальницького профілю [2].

Користувачі повинні бути авторизовані (дозволені) для виконання їх запиту. Під час авторизації AWS використовує значення з контексту запиту для перевірки політик, які застосовуються до запиту. Потім він використовує політики, щоб визначити, дозволити чи відхилити запит. Більшість політик зберігаються в AWS як документи JSON і вказують дозволи для основних сутностей. Існує кілька типів політик, які можуть впливати на те, чи є запит авторизованим. Щоб надати своїм користувачам дозволи на доступ до ресурсів AWS у їхньому власному обліковому записі, їм потрібні лише політики на основі ідентифікації. Політика на основі ресурсів популярна для надання доступу до кількох облікових записів.

AWS перевіряє кожну політику, яка застосовується до контексту запиту користувача. Якщо одна політика дозволів містить відхилену дію, AWS відхиляє весь запит і припиняє оцінку. Це називається явним запереченням. Оскільки запити за замовчуванням відхиляються, AWS санкціонує запит користувача, лише якщо кожна частина його запиту дозволена відповідною політикою дозволів. Логіка оцінки запиту в межах одного облікового запису відповідає таким загальним правилам [2]:

за замовчуванням усі запити відхиляються. (Загалом, запити, зроблені за допомогою кореневих даних облікового запису користувача AWS щодо ресурсів в обліковому записі, завжди дозволяються);

явний дозвіл у будь-якій політиці дозволів (на основі ідентифікаційних даних або ресурсів) замінює це значення за замовчуванням;

існування SCP організації, межі дозволів IAM або політики сеансу замінює дозволи. Якщо існує один або кілька із цих типів політик, усі вони повинні дозволити запит. В іншому випадку це неявно заперечується;

явне заперечення в будь-якій політиці замінює будь-які дозволи.

Після автентифікації та авторизації запиту користувача AWS схвалює дії або операції у цьому запиті. Операції визначаються службою і включають такі дії, які користувач може зробити з ресурсом, такі як перегляд, створення, редагування та видалення цього ресурсу. Щоб дозволити принципалу виконувати операцію, необхідно включити необхідні дії до політики, яка застосовується до принципала або ресурсу, на який впливає.

Після того, як AWS схвалить операції у запиті користувача, їх можна буде виконувати на відповідних ресурсах у обліковому записі користувача. Ресурс – це об’єкт, який існує в межах служби. Прикладами є екземпляр Amazon EC2, користувач IAM та кошик Amazon S3. Служба визначає набір дій, які можна

виконувати над кожним ресурсом. Якщо користувач створює запит на виконання не пов’язаної дії над ресурсом, цей запит відхиляється. Наприклад, якщо користувач подаєте запит на видалення ролі IAM, але надає ресурс групи IAM, запит не вдається виконати.

Таким чином, використовуючи сервіс AWS IAM, можна керувати дозволами і доступом користувачів до сервісів та ресурсів AWS. Також з його допомогою можна управляти дозволами для своїх користувачів і додатків, використовувати федерації посвідчень для управління доступом до акаунту AWS і аналізувати доступ до ресурсів і сервісів.

Література

1. Gartner. Magic Quadrant for Cloud Infrastructure and Platform Services. Published 27 July 2021 https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb.
2. AWS Identity and Access Management. User Guide. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmw-nsx-distributed-ids-ips-tech-white-paper-dec.pdf.

ТЕХНОЛОГІЯ РОЗПОДІЛЕНОГО ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНУ СИСТЕМУ ПІДПРИЄМСТВА

Колотухін Денис Вадимович, БСДМ-61
Державний університет телекомунікацій,
м. Київ

Визначено мету і основні завдання щодо виявлення та попередження вторгнень в інформаційну систему підприємства. Розглянута архітектура системи та технологія розподіленого виявлення та попередження вторгнень в інформаційну систему підприємства. Розроблено рекомендації щодо застосування методів та засобів розподіленого виявлення та попередження вторгнень в інформаційну систему підприємства.

Під виявленням вторгнень розуміється процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі, їх аналізу на наявність ознак можливих інцидентів, які представляють собою порушення або неминучі загрози порушення політик безпеки, політик допустимого використання або стандартних методів забезпечення безпеки. Під запобіганням вторгненням розуміється процес виявлення вторгнень та спроба зупинити виявлені можливі інциденти [1].

Системи виявлення й запобігання вторгнень (IDPS) в першу чергу орієнтовані на виявлення можливих інцидентів, реєстрацію інформації про них, спроби їх зупинити і повідомити про них адміністраторів безпеки. Крім того, організації використовують IDPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання людей від порушення політик безпеки. IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації. IDPS зазвичай записують інформацію, що відноситься до спостережуваних подій, повідомляють адміністраторів безпеки про важливі спостережуваних події і створюють звіти. Багато IDPS також можуть реагувати на виявлену загрозу, намагаючись запобігти її успішної реалізації [1].

Системи виявлення вторгнень (IDS) з'явилися в кінці 1990-х для виявлення схем потоків трафіку, що свідчать про проведені атаки. У 2000-х рішення IDS трансформувалися в системи запобігання вторгненням (IPS), оскільки придбали додаткові можливості забезпечення безпеки. З роками система IDS/IPS стала стандартним компонентом стека мережі і безпеки [2]. Незважаючи на це, через вартість і експлуатаційну складність область застосування IDS/IPS обмежувалася окремими сегментами мережі, наприклад знаходяться на периметрі організацій з загальнодоступними мережами [2].

З розвитком розподілених додатків і мікросервісів спостерігається значне зростання об’єму мережевого трафіку інформаційних систем підприємств. У той же час межі інформаційних систем підприємств стали розмитими через зростаючі можливостей підключення різних додатків до публічної хмари і пристроїв кінцевих користувачів. В результаті організації стали набагато частіше використовувати IDS/IPS як рівня захисту в інформаційних системах підприємства. Тому, набув актуальності новий підхід до архітектури IDS/IPS,

який забезпечує необхідне охоплення системи безпеки без підвищення вартості та експлуатаційної складності.

Реалізацію функцій IDS/IPS забезпечують модулі регулярних виразів, що визначають схеми потоків трафіку. Ці модулі запрограмовані на пошук відомих загроз на основі схем потоків трафіку за допомогою мови конфігурації. Адміністратори мережі і систем безпеки використовують схеми, виражені за допомогою мови конфігурації IDS/IPS, в якості сигнатур. В даний час в більшості систем IDS/IPS крім виявлення загроз на основі сигнатур використовуються такі методи забезпечення безпеки, як перевірка відповідності протоколів і портів, а також виявлення аномального трафіку.

Системи IDS/IPS можна впроваджувати у вигляді автономних спеціалізованих пристроїв або в складі міжмережевого екрану [2].

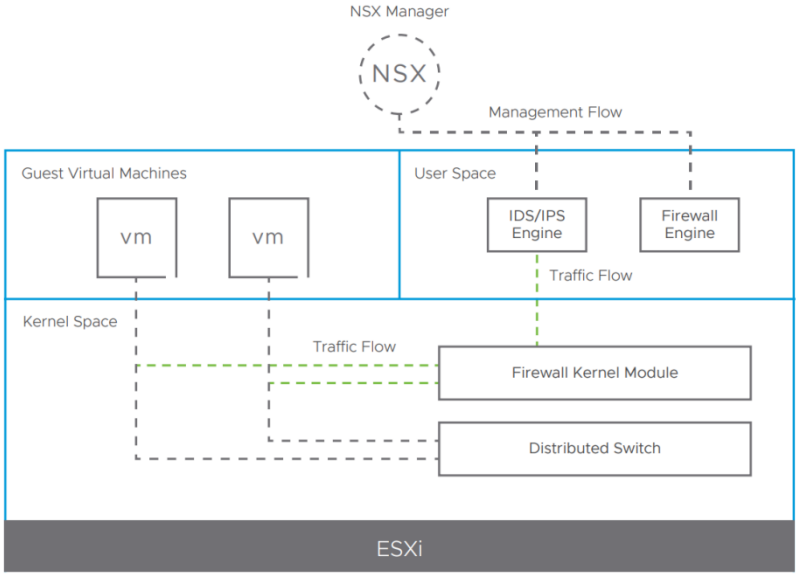


Рис. 1. Архітектура міжмережевого екрану з IDS/IPS рішення VMware NSX [2]

Механізми NSX Distributed IDS/IPS виникли в Suricata, відомому і широко застосованому проекту з відкритим вихідним кодом. Рішення VMware NSX поєднує функції міжмережевого екрану з IDS/IPS (рис. 1), що призводить до перевірки трафіку за один прохід. Весь трафік спочатку проходить через міжмережевий екран, а потім проводиться перевірка IDS/IPS в залежності від конфігурації. Таке спільне розміщення функцій міжмережевого екрану з IDS/IPS також спрощує визначення та застосування політик мережевої безпеки [2].

Як показано на рис. 1, розподілені механізми IDS/IPS рішення VMware NSX розміщуються в просторі користувача і підключені до модуля міжмережевого екрану, який знаходиться в ядрі гіпервізора. Трафік, який виникає при взаємодії додатків, на гіпервізорі перевіряється міжмережевим екраном. Згодом міжмережевий екран перенаправляє трафік на модуль IDS/IPS в середовищі користувача.

Модуль IDS/IPS використовує сигнатури, декодери протоколів і виявлення аномалій для пошуку атак в потоці трафіку. Якщо атак немає, трафік повертається на міжмережевий екран для подальшого транспортування до місця призначення. З іншого боку, якщо атака виявлена, попередження генерується і реєструється. Процес перевірки IDS/IPS на хості призначення, який отримує

трафік, аналогічний. Однак адміністратори можуть відмовитися від перевірки IDS/IPS в пункті призначення, якщо вони вважають, що перевірка IDS/IPS на одному кінці потоку трафіку є адекватною.

Таким чином, новий архітектурний підхід до розподіленої IDS/IPS дозволяє знайти компроміс між вартістю, експлуатаційною складністю і ступенем захисту. Для належного захисту від кіберзагроз, що проникають через периметр, а також від зловмисників зсередини, підприємствам слід реалізувати стратегію розподіленої IDS/IPS. Розподілена IDS/IPS проактивно забезпечує видимість і захист від внутрішніх загроз, а також мінімізують збиток від кібератак, що виходять за межі традиційного периметра корпоративної мережі.

Література

1. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-94. 2007. https://doi.org/10.6028/NIST.SP.800-94.
2. VMware NSX Distributed IDS/IPS. A new paradigm for east-west security. White Paper – December 2019. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmw-nsx-distributed-ids-ips-tech-white-paper-dec.pdf.

ТЕХНОЛОГІЯ ЗАХИСТУ ІНТЕРНЕТ-ДОДАТКІВ ЗА ДОПОМОГОЮ AWS WEB APPLICATION FIREWALL

Кучер Владислав Ігорович, БСДМ-61
Державний університет телекомунікацій,
м. Київ

Визначено призначення та основні складові технології AWS WAF. Визначено множину загроз, якій можна протистояти за допомогою AWS WAF. Розглянуто архітектуру системи AWS WAF та технологію протидії основним загрозам веб-додаткам інформаційної системи підприємства.

Amazon Web Services Web Application Firewall (AWS WAF) – це міжмережевий екран для інтернет-додатків, який дозволяє захистити їх (або різні API) від поширених мережевих експлойтів і ботів, здатних вплинути на доступність, створити загрозу безпеці або задіяти надмірну кількість ресурсів API або додатків. AWS WAF надає повний контроль над трафіком додатків користувача: за допомогою правил безпеки, які контролюватимуть трафік від ботів і блокують такі виконувані по поширеним шаблонами атаки, як SQL-ін'єкції або міжсайтовий скриптінг [1]. Існує можливість налаштовувати та застосовувати правила фільтрації для певних шаблонів трафіку. Можна в застосовувати керовані правила для AWS WAF в попередньо налаштованому наборі правил з боку AWS для вирішення таких проблем, як 10 основних ризиків безпеки OWASP і автоматизовані боти, які споживають зайві ресурси, відхиляють метрики або призводять до простоїв. Ці правила регулярно оновлюються в міру виникнення нових проблем. AWS WAF пропонує повнофункціональний API, що дозволяє автоматизувати процеси створення, розгортання та обслуговування правил безпеки [1].

Виконати розгортання AWS WAF можна в сервісі Amazon CloudFront у вигляді компонента рішення CDN, на Application Load Balancer, розташованому перед веб-серверами або серверами джерела, які працюють на EC2, на Amazon API Gateway для використовуваних API REST або на AWS AppSync для API GraphQL (рис. 1) [1].

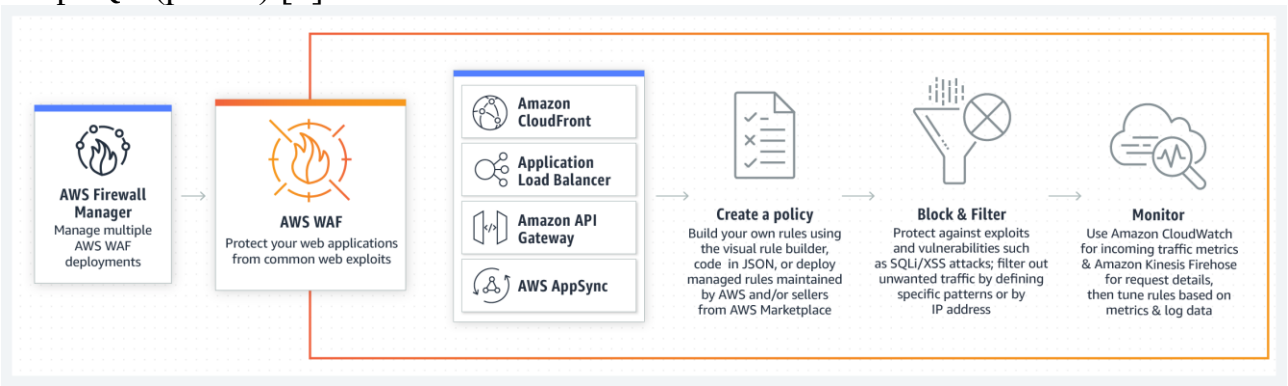


Рис. 1. Основні складові технології AWS WAF [1]

Веб-додатки є вразливими для різних атак. Ці атаки включають в себе спеціально створені запити, призначені для використання вразливості або отримання контролю над сервером; об'ємні атаки, спрямовані на закриття веб-

сайту; погані боти і веб-скрапери, запрограмовані для очищення і крадіжки веб-контенту.

AWS WAF використовує AWS CloudFormation для налаштування правил, які допомагають блокувати такі поширені атаки:

SQL-ін'єкція: зловмисники вставляють шкідливий код SQL в веб-запити, щоб витягти дані з бази даних. AWS WAF призначений для блокування веб-запитів, що містять потенційно шкідливий код SQL;

міжсайтовий скриптінг: також відомий як XSS, зловмисники використовують уразливості на веб-сайті в якості засобу для впровадження шкідливих скриптів клієнт-сайт в веб-браузер легітимного користувача. AWS WAF призначене для перевірки часто досліджуваних елементів вхідних запитів з метою виявлення і блокування XSS-атак;

HTTP-флуд: веб-сервери та інші внутрішні ресурси схильні до ризику розподілених атак типу «відмова в обслуговуванні» (DDoS), таких як HTTP-флуд. AWS WAF автоматично запускає правило, коли веб-запити від клієнта перевищують встановлений поріг. В якості альтернативи можна посилити цей поріг, обробивши журнали AWS WAF за допомогою функції AWS Lambda або запиту Amazon Athena;

сканери та зонди: шкідливі джерела сканують веб-додатки, підключені до Інтернету, та перевіряють їх на наявність вразливостей. Вони відправляють серію запитів, які генерують коди помилок HTTP 4xx, і це використовується для ідентифікації та блокування шкідливих вихідних IP-адрес. AWS WAF створює функцію AWS Lambda або запит Amazon Athena, який автоматично аналізує журнали доступу до Amazon CloudFront або Application Load Balancer, підраховує кількість невірних запитів з унікальних вихідних IP-адрес в хвилину і оновлює AWS WAF, щоб блокувати подальше сканування з визначених IP-адрес;

відоме походження зловмисників (списки репутації IP-адрес): ряд організацій підтримують списки репутації IP-адрес, якими користуються відомі зловмисники, такі як спамери, розповсюджувачі шкідливих програм і бот-мережі. AWS WAF використовує інформацію з цих списків репутації, щоб блокувати запити з шкідливих IP-адрес;

боти і веб-скрапери: оператори загальнодоступних веб-додатків повинні бути впевнені, що клієнти, які звертаються до їх контенту, ідентифікують себе точно і будуть використовувати служби за призначенням. Однак деякі автоматизовані клієнти, такі як веб-скрапери контенту або погані боти, вводять себе в оману, щоб обійти обмеження. AWS WAF допомагає виявляти і блокувати погані ботів і веб-скрапери.

Розгортання AWS WAF з параметрами за замовчуванням створює середовище в хмарі AWS, яке показано на рис. 2 [2].

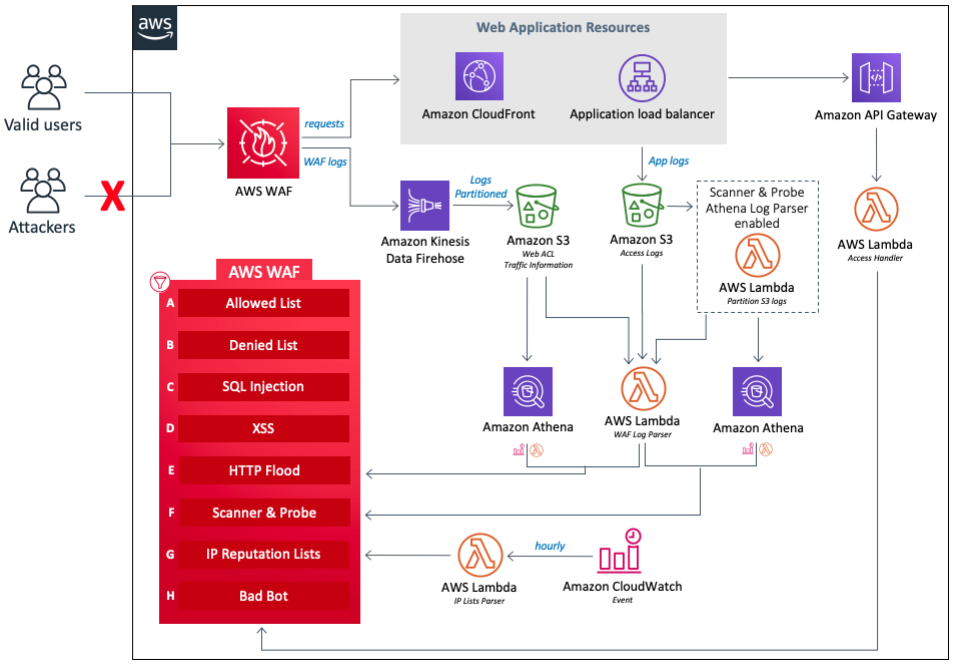


Рис. 2. Основні компоненти архітектури AWS WAF [2]

В основі побудови AWS WAF лежить веб-ACL, який діє як центральний пункт перевірки та прийняття рішень для всіх вхідних запитів до веб-додатку. Під час початкового налаштування стеку AWS CloudFormation користувач визначає, які захисні компоненти активувати. Кожен компонент працює незалежно і додає різні правила до веб-ACL.

Компоненти AWS WAF можна згрупувати в такі зони захисту (рис. 2) [2]:

списки IP-адрес (A і B): цей компонент створює два специфічних правила AWS WAF, які дозволяють вручну вставляти IP-адреси, які дозволяються або забороняються;

SQL-ін'єкція (C) і XSS (D): цей компонент AWS WAF налаштовує два власних правила AWS WAF, призначені для захисту від загальних шаблонів введення SQL або міжсайтового сценарію (XSS) в URI, рядку запиту або тілі запиту;

HTTP-флуд (E): цей компонент AWS WAF захищає від атак, які складаються з великої кількості запитів з певної IP-адреси, таких як DDoS-атака на веб-рівні або спроба атаки «груба сила». За допомогою цього правила встановлюється поріг, який визначає максимальну кількість вхідних запитів, дозволених з однієї IP-адреси протягом п’яти хвилин. Після того, як цей поріг буде перевищено, додаткові запити з IP-адреси тимчасово блокуються. Це реалізується на основі створеного правила в AWS WAF, обробляючи журнали AWS WAF за допомогою функції AWS Lambda або запиту Amazon Athena;

сканери та зонди (F): цей компонент аналізує журнали доступу до програм, які шукають підозрілу поведінку, наприклад, ненормальну кількість помилок, спричинених джерелом. Потім він блокує ці підозрілі IP-адреси джерел на визначений клієнтом період часу. Це правило реалізується за допомогою функції AWS Lambda або запиту Amazon Athena;

списки репутації IP (G): цей компонент реалізує функцію аналізу списків

IP-адрес AWS Lambda, яка щогодини перевіряє списки репутації IP сторонніх виробників на наявність нових діапазонів для блокування. Ці списки включають списки Spamhaus Don't Route Or Peer (DROP) та Extended DROP (EDROP), список IP-адрес Proofpoint Emerging Threats та список вузлів виходу Tor;

погані боти (H): цей компонент автоматично встановлює honeypot, який є механізмом безпеки, призначеним для заманювання та відхилення спроби атаки. Honeypot цього рішення є кінцевою точкою пастки для виявлення вхідних запитів від веб-скраперів та поганих ботів. Якщо джерело звертається до honeypot, функція AWS Lambda обробника доступу перехопить та перевірить запит на вилучення його IP-адреси, а потім додасть його до списку блокування AWS WAF.

Таким чином, застосування технології AWS WAF дозволить ефективно протидіяти основним загрозам веб-додаткам інформаційної системи підприємства.

Література

1. AWS WAF - Web Application Firewall. Protect your web applications from common web exploits. https://aws.amazon.com/waf/?nc1=h_ls.
2. AWS WAF Security Automations. https://docs.aws.amazon.com/solutions/latest/aws-waf-security-automations/architecture.html.

ЗАГРОЗИ ПОВ'ЯЗАНІ З ВІДДАЛЕНОЮ РОБОТОЮ. ЯК ЗРОБИТИ ВІДДАЛЕНУ РОБОТУ ЕФЕКТИВНОЮ ТА БЕЗПЕЧНОЮ

Кушнір Дмитро Ігорович
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

У сучасних реаліях віддалена робота давно є необхідністю. IT-фахівці повинні бути готові забезпечити безпечний і зручний віддалений доступ до корпоративних систем. Будь-яке віддалене підключення є загрозою кібербезпеки. Важливо пам'ятати про моніторинг віддалених співробітників - відстеження їх продуктивності і контролю активності на предмет безпеки. У тезі описані основні загрози кібербезпеки для компаній в рамках віддаленої роботи та надано рекомендації щодо їх ліквідації.

Фахівці з кібербезпеки сприймають віддалених співробітників як потенційну загрозу, і виявляються праві. Однак віддалена робота вже давно перестала бути чимось тимчасовим і, судячи з усього, ще надовго залишиться актуальним явищем. Для багатьох фахівців можливість працювати поза офісом - важлива перевага при виборі роботодавця. Крім того, віддалений доступ необхідний підрядникам, під час відряджень та надзвичайних ситуацій, таких як пандемія, транспортні колапси і екстремальні погодні явища. У таких випадках IT-фахівці повинні бути готові забезпечити безпечний і зручний віддалений доступ до корпоративних систем, а також ефективний віддалений моніторинг співробітників. Також важливо стежити за продуктивністю останніх - в кінці кінців, деякі співробітники можуть відволікатися на домашні справи.

Згідно з опитуванням OpenVPN, 73% IT-керівників вважають віддалених співробітників більш небезпечними в порівнянні з тими, хто працює в офісі. В основному тому, що віддалені співробітники отримують доступ до конфіденційних даних за межами традиційного периметра кібербезпеки. Відсутність знань і захисних заходів робить таких співробітників уразливішими для атак хакерів і витоку даних. Ось найпоширеніші загрози, які виходять від віддалених співробітників:

1. *Використання загальнодоступних мереж Wi-Fi.*
2. *Використання особистих пристроїв для роботи.*
3. *Відсутність належних знань в кібербезпеці.*
4. *Уразливість до атак соціальної інженерії.*
5. *Відсутність коштів авторизації і контролю доступу.*
6. *Використання застарілого ПЗ.*
7. *Шкідливі дії з даними.*
8. *Відпочинок замість роботи.*

Проблеми можна усунути за допомогою передових практик в області кібербезпеки і моніторингу віддалених співробітників.

Основні перевірені часом методи захисту віддалених підключень і співробітників, які допоможуть відстежити і захистити дії віддалених співробітників. Деякі носять чисто організаційний характер, а деякі вимагають наявність спеціального ПЗ для моніторингу віддалених співробітників.

1. *Створіть інструкцію по віддаленому доступу.*

Ця інструкція повинна включати:

- список ПЗ і засобів контролю доступу;
- керівництво по віддаленому підключенню до мережі;
- заходи щодо захисту облікових даних;
- умови надання віддаленого доступу співробітникам.

Переконайтеся, що в цій інструкції ви відповіли на всі можливі питання ваших співробітників і забезпечте доступ до неї в будь-який час.

2. *Інформуйте співробітників про атаки соціальної інженерії*. Такі атаки зазвичай виявляються успішними через неуважність, поспішність співробітника або завдяки новим прийомам хакерів. Кращий спосіб уберегтися від них – оповістити співробітників про всі останні «досягнення» соціальної інженерії та вихідної від них загрозу.

3. *Встановіть безпечні віддалені підключення за допомогою VPN*. Ця технологія створює захищене пряме з'єднання між комп'ютером співробітника і корпоративною мережею з використанням алгоритму шифрування і аутентифікації. Таким чином, VPN є ефективним інструментом для захисту підключень по ненадійних мереж, таким як загальнодоступний Wi-Fi.

4. *Введіть примусову многофакторную аутентифікацію.* Перевірка декількох факторів дозволить вам точно ідентифікувати того, хто намагається підключитися до вашої мережі.

5. *Обмежте доступ до загальних облікових записів або використовуйте вторинну аутентифікацію*. Загальні профілі, наприклад, для віддалених адміністраторів, спрощують життя співробітників, але вкрай ускладнюють пошук винних в порушенні безпеки. Деякі IT-фахівці вважають за краще блокувати такі акаунти. Якщо ви не можете цього зробити, використовуйте вторинну аутентифікацію, щоб ідентифікувати користувача, який переховується за безликим профілем.

6. *Відстежуйте і записуйте активність користувачів*. Безперервний моніторинг віддалених комп'ютерів забезпечує повну видимість дій співробітників з конфіденційними даними і їх загальної продуктивності.

7. *Контролюйте продуктивність співробітників*. Простого лічильника робочого часу часто недостатньо для оцінки ефективності співробітника. Використовуючи дані активності користувачів, ви можете оцінити ефективність співробітників в робочий час. Аналіз запису екрану, відкритих файлів, папок, додатків і сайтів допомагає виявити тих, хто при роботі віддає перевагу новинам і соціальним мережам. Також рекомендується відстежувати продуктивність, проводячи періодичні зустрічі з віддаленими співробітниками і просячи їх складати щоденні або щотижневі звіти про стан їх завдань.

8. *Налаштуйте повідомлення про підозрілі події*. Своєчасне оповіщення про можливе порушення безпеки з посиланням на подію допоможе службі безпеки зупинити підозрілу активність. Завжди краще запобігти загрозу, ніж боротися з її наслідками.

9. *Керуйте обліковими даними і конфіденційною інформацією*. Облікові дані віддалених співробітників особливо легко вкрасти. Ви можете захистити їх, запровадивши рішення для управління паролями. Менеджер паролів дозволяє безпечно створювати, зберігати, передавати і чергувати логіни і паролі без участі

користувачів. Крім захисту облікових даних, ви також можете керувати секретною інформацією служб каталогів Windows Active Directory, ключами SSH / Telnet для середовищ Unix та інших.

Дистанційні працівники допомагають компаніям заощадити на оренді офісу, при цьому вони так само віддані своїй справі, як і офісні співробітники і підтримують зв'язок зі своїми керівниками. Іноді вони навіть більш продуктивні, ніж їх колеги в офісі. З іншого боку, загрози кібербезпеки при наявності віддаленого доступу вимагають серйозних захисних заходів. Навіть якщо ваша компанія зазвичай наймає на роботу в офіс, бувають ситуації, коли необхідно надати віддалений доступ і контролювати своїх віддалених співробітників. До такого краще підготуватися заздалегідь.

У цій тезі я розглянув основні ризики кібербезпеки, пов'язані з наданням вашим співробітникам можливості працювати з дому. Деякі із загроз можливо усунути за допомогою таких організаційних заходів як розробка інструкцій і навчання співробітників. Але для забезпечення максимальної безпеки і прозорості найкраще використовувати спеціалізоване програмне забезпечення для контролю та моніторингу співробітників.

У зв’язку з пандемією більшість компаній переходять у режим віддаленої роботи та зосереджують свою увагу на програмних методах протидії інсайдерським загрозам. Не меншу роль відіграє фізичний захист носіїв інформації та даних. В тезі описані основні наслідки для компаній в рамках фізичного впливу на дані та обумовлено основні фізичні проблеми в організації.

Фізичний доступ до захищених сегментів організації, обладнання або матеріалів, що містять конфіденційні дані може скоротити шлях для скоєння злочину зловмисним інсайдером. Таким чином, фізичний контроль безпеки організації часто настільки ж важливий, як і його технічні засоби контролю безпеки. У деяких випадках, інциденти зловмисної інсайдерської діяльності, в тому числі злочинів IT саботажу, крадіжок інтелектуальної власності, а також шахрайства, близько 8% пов'язані з питаннями фізичної безпеки, що викликає занепокоєння. Розглянемо та проаналізуємо деякі з цих випадків:

- Уже більше року, двірник вкрав рахунок клієнта і особисту інформацію з паперових документів в великому банку США. Двірник і два спільники використовували цю інформацію, щоб вкрасти особистості більше 250 людей. Вони відкривали кредитні картки, а потім представити онлайн обмін повідомленнями про зміну адреси запитів, так що жертви не отримуватимуть виписки з банківських рахунків або інших повідомлень про шахрайську діяльність. Інсайдери виводили гроші з рахунків клієнтів так що втрата організації перевищила 200 тисяч доларів.
- Програміст переконав робочий персонал щоб вони відкрили офіс іншого співробітника. Він замінив табличку на дверях і попросив, щоб двірник впустив його в «свій» офіс. Програміст, який вже отримав роботу в конкурента, був в змозі завантажити чутливий вихідний код на носій.
- Охоронець лікарні отримав доступ і вкрав особисту інформацію про пацієнтів організації. Охоронець і три спільники відкрили фальшиві номера телефонів і рахунки кредитних карт. В рамках схеми, вони змінили рахунки

адреси жертв, так що рахунки ніколи не досягнуть власників рахунків. Після того, як їх спіймали, інсайдера зобов'язали виплатити 18 тисяч доларів за злочин.

- Директор зв'язку показав прострочене посвідчення охоронцю, щоб дістати несанкціонований доступ до резервного сховища даних об'єкта. Опинившись всередині, директор відключив камери безпеки і вкрав резервні данні, які містили записи про 80 тисяч співробітників.
- Охоронець безпеки використав ключ, щоб отримати фізичний доступ до опалення, вентиляції, кондиціонування повітря, комп'ютерів лікарні та інших робочих станцій. Охоронець використовував програмне забезпечення для підбору паролю для отримання доступу і встановлення шкідливих програм на комп'ютери. Подія могла вплинути на температурно-чутливих пацієнтів, ліки та матеріали.
- Інсайдер вкрав торгові секретні креслення організації, які були визначені для знищення, та продав їх конкуруючій організації. Організація жертви оцінює свої втрати в 100 мільйонів доларів. Конкуруюча організація, яка отримала вкрадені документи була змушена оголосити про банкрутство після судового процесу.

Можемо виокремити основні фізичні проблеми безпеки:

- Інфільтрація/ексфільтрація фізичної властивості: такі заходи, як винесення змінних носіїв за об'єкт.
- Неправильне припинення фізичного доступу працівника або доступу по карті.
- Несанкціонований доступ до об'єкту: співробітники, що пропускають неуповноважених осіб, що йдуть через відкриті двері за картою працівника, також відомий метод як «piggybacking».
- Як правило, слабка фізична безпека: загальні питання, такі як недостатнє покриття «сліпих зон» або недостатнє розділення обов'язків для фізичного контролю доступу
- Співробітник використав несанкціоновану робочу станцію: співробітники, які здатні фізично увійти в інший офіс/робоче місце і отримати доступ до їх робочої станції.
- Злом і проникнення/фізичне знищення: співробітники вриваючись в на підконтрольні об'єкти та крадуть фізичне обладнання.
- Кадрові питання: технічний персонал, який викрадає конфіденційну інформацію або направлений на порушення фізичної безпеки.
- Неправильне видалення або знищення інформації в організації.

Сильний фізичний контроль безпеки, так як фізична підготовки в спорті або постійні перевірки здоров'я, можуть запобігти деяким проблемам. Фізичний контроль безпеки включають в себе запобігання несанкціонованого фізичного доступу до захищених сегментів організації, а також запобігання прямої фізичної крадіжки. Інсайдерські загрози фізичної безпеки можуть виходити від нинішніх або колишніх співробітників, підрядників і надійних ділових партнерів, в тому числі технічних працівників і охоронців. Особи з широким доступом необхідно до ретельніше перевіряти. Наприклад, технічних персонал і охоронці повинні пройти ту ж перевірку, як і інші інсайдери.

Співробітники, що мають високий рівень доступу повинені також мати звичайну підготовку з питань безпеки, тому що їх позиція робить їх головною мішенню для атак соціальної інженерії.

Перелік посилань:

Insider Threat and Physical Security of Organization. Posted on May 10, 2011 [Електронний ресурс] - https://insights.sei.cmu.edu/blog/insider-threat-and-physical-security-of-organizations/

ТЕХНОЛОГІЯ РОЗШИРЕНОГО ЗАХИСТУ КОРПОРАТИВНИХ КІНЦЕВИХ ТОЧОК ВІД ЗАГРОЗ НА БАЗІ FortiEDR

Наконечний Максим Юрійович, БСДМ-61
Державний університет телекомунікацій,
м. Київ

Визначено призначення та основні складові технології FortiEDR. Визначено характерні особливості FortiEDR. Розглянуто технологію виявлення та реагування на кінцеві точки із застосуванням FortiEDR.

На малий бізнес все частіше націлюються кіберзлочинці. Торік 66% малого бізнесу зазнали кібератаки. Все частіше компанії звертаються до програмного забезпечення для захисту кінцевих точок для захисту мереж інформаційних технологій [1].

Одним з найпопулярніших та найефективніших підходів є реалізація технології виявлення та реагування на кінцеві точки (EDR) [1]. Основні функції рішень класу EDR показано на рис. 1.

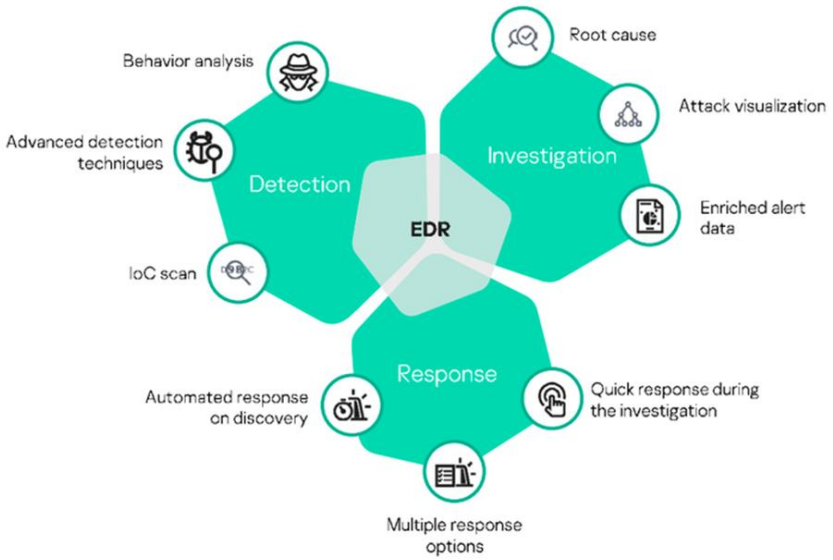


Рис. 1. Основні функції рішень класу EDR [1]

Необхідність застосування систем класу EDR продиктована постійно зростаючої складністю кібератак, спрямованих на корпоративний сектор. З одного боку, продукти, призначені для контролю мережевого трафіку, не покривають весь потенційний фронт нападу, залишаючи поза сферою своєї уваги процеси, що відбуваються всередині кінцевих точок. З іншого боку, класичні антивіруси і рішення рівня Endpoint Protection Platform (EPP) не завжди мають можливість детектувати багатоетапні, цільові атаки [2].

Рішення FortiEDR дозволяє в режимі реального часу відстежувати роботу кінцевих точок, автоматично блокує шкідливу активність, а також надає адміністраторам SOC детальну інформацію, необхідну для розслідування складних кіберінцідентов. Можливості рішення FortiEDR дозволяють використовувати її для боротьби з нетиповими, цільовими атаками, мінімізувати

шкоду від програм-шифрувальників, швидко усувати наслідки шкідливих дій на корпоративних кінцевих точках [2].

Платформа FortiEDR являє собою розподілену архітектуру (рис. 2), яка збирає потік встановлення з'єднань між пристроями організації, які обмінюються даними, безпосередньо з внутрішніх компонентів операційної системи кожного пристрою. FortiEDR аналізує потік подій, що передували встановленню з'єднання, і визначає, чи був запит на встановлення з'єднання зловмисним. Система може забезпечити дотримання політики організації, заблокувавши запит на встановлення з'єднання, щоб запобігти крадіжці [3].

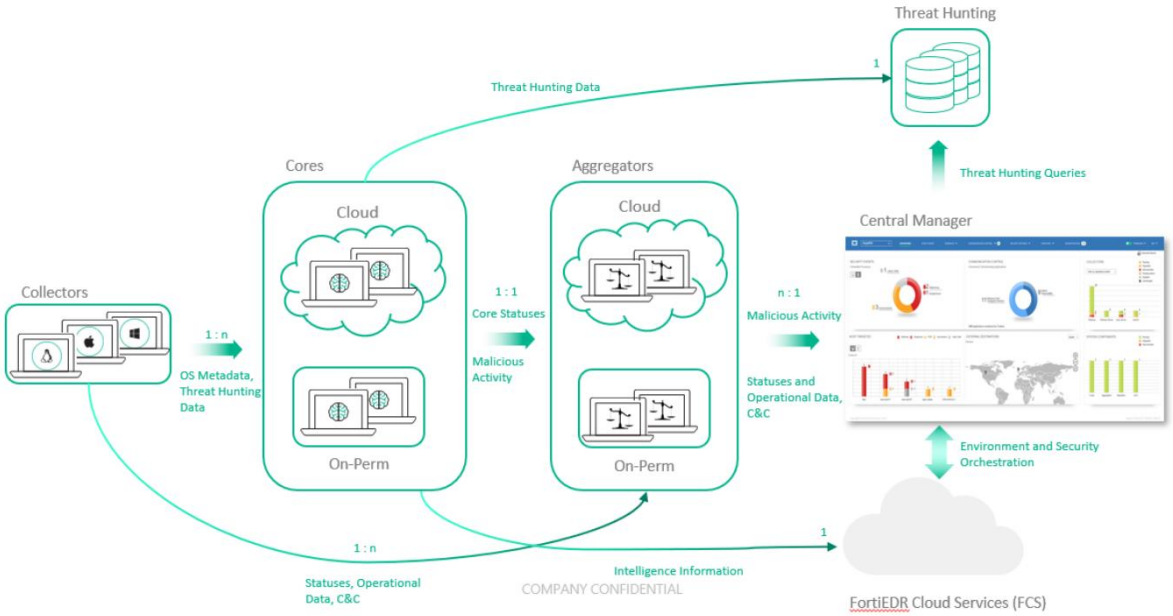


Рис. 2. Архітектура FortiEDR [3]

Отже, сучасні методи захисту кінцевих точок потребують адаптації до існуючого ландшафту складних загроз і мають включати функціональність щодо виявлення комплексних атак, спрямованих на кінцеві точки, та бути здатними своєчасно реагувати на інциденти. Рішення FortiEDR є повнофункціональною системою захисту кінцевих точок в режимі реального часу. Воно має розвинені засоби моніторингу та реагування, що надає змогу в випереджувальному режимі знижувати кількість напрямків атак, запобігати ураженню шкідливими програмами, виявляти і знешкоджувати потенційні загрози.

FortiEDR контролює процеси, що запускаються на робочих станціях і серверах, виявляючи підозрілу активність і при необхідності блокуючи її. Робота FortiEDR значно звужує потенційний фронт атаки за рахунок відстеження мережевих з'єднань і автоматичного переривання шкідливих процесів. Розвинені можливості реагування дозволяють в ручному або автоматичному режимі блокувати несанкціоновані дії та ізолювати заражений пристрій.

Література

1. Robert Izquierdo. A Beginner's Guide to EDR Security. https://www.fool.com/the-blueprint/edr/.
2. Денис Сарычев. Обзор FortiEDR, системы защиты конечных точек от сложных атак. https://www.anti-malware.ru/reviews/FortiEDR.

3. FortiEDR Installation and Administration Guide. Version 4.2. *https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5e261ba9-cc73-11ea-8b7d-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.2.pdf*.

ТЕХНОЛОГІЯ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ НА БАЗІ FortiGate IPS

Павловський Олексій Юрійович, БСДМ-61
Державний університет телекомунікацій,
м. Київ

Встановлено місце технології запобігання вторгнень в системі забезпечення мережевої безпеки. Визначено характерні особливості технології FortiGate IPS. Досліджено особливості архітектури рішення FortiGate 200E.

Розвиток корпоративних мережевих інфраструктур призвів до розширення поверхні атаки для відомих, невідомих та загроз нульового дня. Оскільки першопричини більшості порушень пов'язані з використанням відомих вразливостей, багато організацій, щоб не відставати, звернулися до систем запобігання вторгнень (IPS). Правильна IPS пропонує найбільш ефективний спосіб блокувати загрози, які використовують відомі вразливості.

Технологія запобігання вторгнень все ширше застосовується в системах мережевої безпеки. Вона доступна як в форматі одного з компонентів мережевого доступу, так і у вигляді окремого автономного засобу [1].

Компанія Fortinet, одним з найвідоміших продуктів якої є міжмережевий екран наступного покоління (NGFW), більше десяти років займається розробкою технології IPS. Відмінною рисою Fortinet є висока продуктивність міжмережевих екранів FortiGate. Рішення FortiGate IPS розроблено на основі кращої на ринку технології IPS і повністю виправдовує свою вартість і очікування клієнтів [2].

Загрози «нульового дня», просунуті цілеспрямовані атаки, програми-вимагачі, поліморфне шкідливе ПЗ і розподілені атаки типу «відмова в обслуговуванні» вимагають складних механізмів виявлення, які відсутні в традиційних автономних системах IPS і в більшості міжмережевих екранів.

Рішення FortiGate IPS включає в себе кілька комплексних модулів перевірки, джерел даних про загрози і варіантів захисту від просунутих загроз для захисту від невідомих загроз. FortiGate IPS – це потужне рішення на декількох платформах FortiGate (апаратні, віртуальні, хмарні засоби) з функцією поглибленого аналізу та управління робочими процесами через компонент FortiAnalyzer, яке представляє собою економічно ефективне рішення для забезпечення безпеки мережі, що відповідає вимогам реагування на інциденти в центрі управління системою безпеки (SOC) організації [2].

Система запобігання проникненню (IPS) є найважливішим компонентом основних можливостей безпеки кожної мережі. Він захищає від відомих загроз та атак нульового дня, включаючи шкідливе програмне забезпечення та основні вразливості.

Треба підкреслити, що рішення FortiGate IPS побудоване на унікальній архітектурі спеціалізованих процесорів безпеки і мережевих процесорів, які дозволяють йому забезпечувати безпрецедентну продуктивність в поєднанні з можливостями FortiGuard Labs. Рішення NGFW FortiGate надають кращі в

своєму класі можливості IPS для мережевої інфраструктури, заснованої на безпеці, забезпечуючи тонкий баланс та високу ефективність безпеки без порушення бізнес-процесів [3].

Як в автономних системах IPS, так і в конвергентних міжмережевих екранах нового покоління інноваційна система FortiGate IPS забезпечує надійний захист світового класу. Завдяки виділеним блокам обробки даних для забезпечення безпеки і сучасної ефективної архітектурі продуктивність навіть в найбільших центрах обробки даних залишається стабільною. Автоматизовані процеси безпеки і експлуатації дають фахівцям з безпеки більше часу, щоб зосередитися на інших потребах, які потребують ручного втручання. Як частина Fortinet Security Fabric, FortiGate IPS використовує глобальну і локальну аналітику безпеки з іншими рішеннями Fortinet і довіреними сторонніми продуктами, забезпечуючи оцінку ризиків з використанням самої останньої інформації, а також поліпшення загального стану безпеки [3].

Перевагами FortiGuard IPS є [3]:

більш 13000 сигнатур вразливостей і експлойтів;

захист від вразливостей нульового дня;

більш швидкий час захисту з щоденним оновленням сигнатур IPS.

Автоматичні оновлення IPS FortiGuard забезпечують актуальний захист від мережевих вторгнень, виявляючи і блокуючи загрози до того, як вони досягнуть мережевих пристроїв. FortiGate IPS є новітнім засобом захисту від прихованих загроз мережевого рівня, має велику бібліотеку IPS з тисячами сигнатур, гнучкі політики, що забезпечують повний контроль над методами виявлення атак відповідно зі складними додатками безпеки, стійкість до методів ухилення (що доведено NSS Labs) і службу пошуку сигнатур IPS [3].

Більшість моделей FortiGate мають спеціалізоване апаратне прискорення (так зване блоки обробки даних), яке може вивантажувати інтенсивну обробку ресурсів з основних ресурсів обробки (Security Processing Units, SPUs)). Більшість компонентів FortiGate включають спеціалізовані процесори контенту (CP), які прискорюють широкий спектр важливих процесів безпеки, таких як сканування вірусів, виявлення атак, шифрування та дешифрування. Тільки вибрані моделі початкового рівня FortiGate не включають процесор CP [2].

Багато моделей FortiGate також містять процесори безпеки (SP), які прискорюють обробку для певних функцій безпеки, таких як IPS та мережеві процесори (NP), які розвантажують обробку великого обсягу мережевого трафіку.

Розглянемо апаратне забезпечення блоку обробки даних (Security Processing Unit, SPU), яке Fortinet вбудовує в пристрої FortiGate для прискорення трафіку через блоки FortiGate. Існують три типи SPU:

процесори контенту (Content processors, CPs), які прискорюють широкий спектр функцій безпеки

процесори безпеки (Security processors, SPs), які прискорюють певні функції безпеки

мережеві процесори (Network processors, NP і NPlites), які розвантажують мережевий трафік до спеціалізованого обладнання, оптимізованого для

забезпечення високого рівня пропускної здатності мережі.

Розглянемо архітектуру на прикладі рішень FortiGate 200E and 201E (рис. 1).

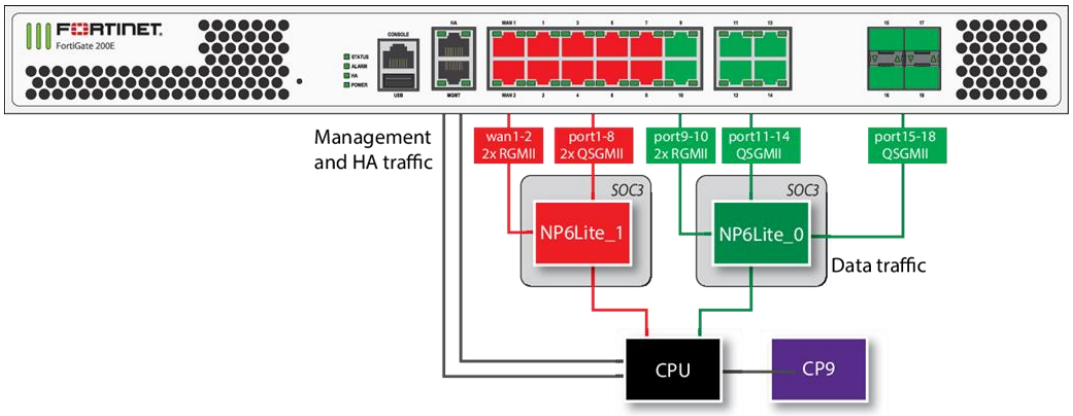


Рис. 1. Архітектура рішення FortiGate 200E [2]

Процесор контенту CP9 надає такі послуги [2]:

а) інспекція на основі потоку (IPS та контроль додатків) прискорення, що відповідає шаблону, з перепускною здатністю понад 10 Гбіт/с:

попереднє сканування IPS/розвантаження перед матчем;

розвантаження сигнатурної кореляції IPS;

розвантаження повного узгодження (лише CP9);

глибока перевірка пакетів на основі DFA;

б) високопродуктивний механізм масових даних VPN:

процесор протоколів IPsec та SSL/TLS;

DES/3DES/AES128/192/256 відповідно до FIPS46-3/FIPS81/FIPS197;

MD5/SHA-1/SHA256/384/512-96/128/192/256 з RFC1321 та FIPS180;

генерація MS/KM (хеш) (лише CP9);

HMAC відповідно до RFC2104/2403/2404 та FIPS198;

мод ESN;

підтримка GCM для NSA «Suite B» (RFC6379/RFC6460), включаючи GCM-128/256; GMAC-128/256;

в) процесор обміну ключами, який підтримує високопродуктивні обчислення IKE та RSA:

механізм посилення відкритого ключа з підтримкою апаратної CRT;

первинна перевірка для генерації ключа RSA;

прискорювач рукостискання з автоматичною генерацією ключових матеріалів;

справжній генератор випадкових чисел (TRNG) з джерелом ентропії PLL (лише CP9 та CP9XLite);

кільце джерела ентропії OSC;

підтримка криптографії еліптичної кривої ECC (P-256) для NSA «Suite B» (лише CP9);

механізм допоміжного відкритого ключа (PKCE) для безпосередньої підтримки роботи до 4096 біт (4k для DH та 8k для RSA з CRT);

г) підтримка fingerprint DLP:

налаштовувані фрагменти контенту з двома порогами-двома дільниками (Two-Thresholds-Two-Divisors, TTTD).

Отже, рішення NGFW FortiGate надають кращі в своєму класі можливості IPS для мережевої інфраструктури, заснованої на безпеці, забезпечуючи тонкий баланс та високу ефективність безпеки без порушення бізнес-процесів. Відмінною ознакою рішення FortiGate IPS є унікальна архітектура на спеціалізованих процесорах безпеки і мережевих процесорах, які дозволяють йому забезпечувати безпрецедентну продуктивність в поєднанні з можливостями FortiGuard Labs.

Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки корпоративних мереж.

Література

1. Cyber Threat Predictions for 2021. An Annual Perspective by FortiGuard Labs. White Paper. *https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-cyber-threat-predictions-for-2021.pdf*.

2. Hardware Acceleration Guide FortiOS 7.0.0. *https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/54ac6091-922e-11eb-b70b-00505692583a/fortios-hardware-acceleration-700.pdf*.

3. Protect Against Known and Unknown Threats with FortiGate IPS and FortiGuard IPS Service. Solution Brief. *https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protect-against-known-and-unknown-threats-with-fortigate-ips.pdf*.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В DEVOPS СЕРЕДОВИЩІ

Поремський Максим Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Методи покращення безпеки у сучасних компаніях, що займаються розробкою програмного забезпечення не поспішають за еволюцією самого процесу розробки, а тому важливо адаптувати підхід забезпечення безпеки до нинішніх реалій розробки. Розглянуто проблематику розробки сучасного програмного забезпечення з урахуванням DevOps підходу та забезпечення безпеки цього програмного забезпечення.

Сьогодні розробка програмного забезпечення є досить швидким та гнучким процесом. Існує багато методологій, підходів та практик, що допомогають випускати продукт швидко та задовольняти потреби бізнесу, але швидкість розробки може завадити дотриманню всіх вимог по безпеці програмного забезпечення, що створюється.

Завдяки впровадженню практик DevOps у процес розробки програмного забезпечення, можна назвати такі переваги:

- скорочення часу виправлення вразливостей;
- скорочення часу випуску нових релізів;
- підвищення якості програмного забезпечення;
- підвищення продуктивності.

Практики DevOps підходу також почали використовуватися в безпеці. Цей підхід до безпеки почали називати DevSecOps. При використані DevSecOps, питання безпеки та тестування на вразливості програмного забезпечення автоматизуються та переносяться на більш ранні етапи розробки програмного забезпечення.

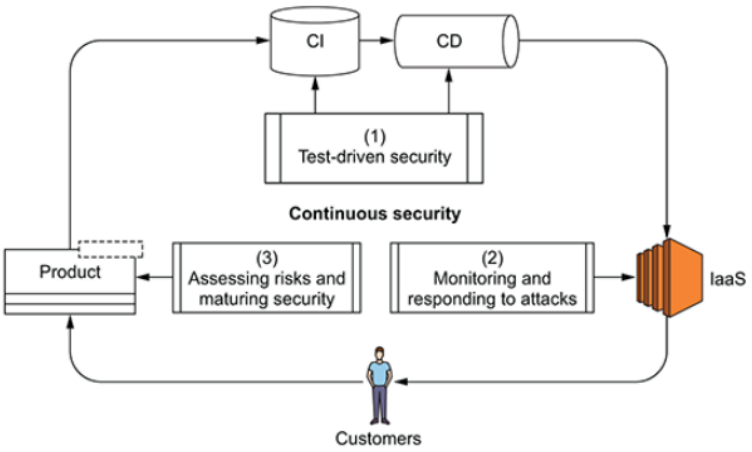


Рисунок 1 – Три фази безперервної безпеки [1, с. 27]

Прикладом DevSecOps практики можна назвати концепцію безперервної безпеки, коли методи забезпечення безпеки вплетені в процес розробки. Ця концепція базується на трьох етапах:

- керована тестами безпека;

- моніторинг і реагування на атаки;
- оцінка ризиків і зріла безпека.

Керована тестами безпека дозволяє автоматизувати перевірку програмного забезпечення на вимогу щодо його безпеки, пришвидшує розробку безпечного продукту та дозволяє виправляти вразливості ще до релізу програмного забезпечення. Керована тестами безпека використовує принципи DevOps щодо автоматизації розробки та тісної співпраці з командами. Це дозволяє людям, що займаються безпекою використовувати засоби безпеки в середовищах, які використовуються розробниками, замість створення власної окремої інфраструктури. Це зменшує ризик та допомагає усувати вразливості ще на ранніх етапах розробки.

Моніторинг і реагування на атаки також може доповнюватися DevSecOps практиками, а наприклад автоматизацією відповіді на інциденти.

Іншим важливим методом забезпечення безпеки є оцінка ризиків на етапі архітектурного дизайну програмного забезпечення. DevSecOps підхід вплинув на цей етап так, що зробив його швидким та ітеративним.

Можна зробити висновок, що разом з еволюцією процесу розробки, змінювався і процес забезпечення безпеки продукту, що розробляється. Методи стали більш швидкими та почали використовувати багато автоматизації.

Список використаних джерел:

1. *Жульєн Вегент // Securing Securing DevOps: Security in the Cloud*

ХАРАКТЕРНІ УРАЗЛИВОСТІ СИСТЕМ ПОБУДОВАНИХ НА ОСНОВІ KNX ТЕХНОЛОГІЙ

Семенова Інна Дмитрівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

Інтернет речей (IP) - один з найперспективніших напрямків розвитку інформаційних технологій на сьогодні. Частиною IP є концепція автоматизації яка дозволяє інтегрувати набір самостійних технологій, таких як керування світлом, кліматом, охоронною системою, тощо, в єдиний диспетчерський пункт керування будівлею. Для цього використовуються технології різного рівня, від польової шини, що реалізую фізичну комутацію до технологій вищого рівня, які базуються на мережевій взаємодії.

З боку захисту інформації, варто приділити увагу недолікам безпосередньо технологій інтеграції та мережевими уразливостями. Не можливо відмежувати їх один від одного, оскільки вони нероздільно взаємопов'язані протоколами взаємодії. Варто розглядати технічні канали витоку інформації, оскільки неможна недооцінювати фізичну складову системи.

1. Шифрування

Однією з найбільш поширених проблем системи розумного будинку є слабке або, навіть, відсутнє шифрування.

Деякі системи взагалі не мають можливості шифрування, наприклад, передача сигналів шиною KNX – усі сигнали передаються в незашифрованому вигляді, як двійкові послідовності, сигнальним кабелем, в даному випадку ми не маємо технічної можливості використати додаткове обладнання для апаратного або програмного шифрування, оскільки це, по-перше, значно підвищить вартість системи, а, по-друге, сповільнить її до неприйнятного рівня.

2. Віддалене підключення

Як правило, використовується VPN-підключення зі стандартнім налаштуванням, або «перенаправлення портів», знову ж таки, зі стандартними відкритими портами. Подібне нехтування може призвести до того, що, хто завгодно зможе підключитися до керування системою.

3. Підміна DHCP сервера

Підміна DHCP сервера, яка дозволяє зловмиснику змусити клієнта використовувати нелегітимний вузол в якості шлюза за замовчуванням, виключити таку можливість для зловмисника дозволяє коректне налаштування мережі: Увімкнути dhcp snooping, визначити довірені порти, вказати адресу довіреного DHCP сервера який доступний через довірений порт.

4. Маскування під легітимною MAC адресою

Зловмисник знаходиться в мережі з параметрами дозволеного пристрою, це дозволяє перехоплювати певну інформацію, або «підставити» пристрій – власник буде вважати, що це його пристрій «збожеволів» та атакує мережу. Найпростіше рішення – гарантована авторизація пристроїв у мережі після кожного перепідключення[3].

Авторизація - це не те ж саме що ідентифікація та автентифікація: ідентифікація - це називання особою себе системі; автентифікація - це встановлення відповідності особи, призначеному ним самим ідентифікатором; а авторизація - надання цій особі можливостей у відповідність до покладених йому правами або перевірка наявності прав при спробі виконати будь-яку дію[4].

Access Control List або ACL - список управління доступом, який визначає, хто або що може отримувати доступ до об'єкта), і які саме операції дозволено або заборонено виконувати суб'єкту. Використання таких списків достатньо простий та ефективний метод захисту від підключення нелегітимних пристроїв та користувачів

5. Витік інформації акустичними каналами

Одним із різновидів датчиків охоронної сигналізації є датчики розбиття віконного скла та вібраційні датчики, котрі в якості чутливого елементу використовують високочутливі мікрофони та п’єзоелементи, відповідно, і реагують на події в діапазоні звукових хвиль. Ці датчики з’єднані з пультом охорони багатопровідним шлейфом, з допомогою якого здійснюється живлення датчиків постійною напругою, а від нього до пульта охорони передаються логічні сигнали про стан, в якому знаходиться датчик та цілісність самого датчика.

Відомо, що пульти охорони, як правило, знаходяться за межами контрольованої зони і можуть бути віддалені від датчиків на відстань до 100 і більше метрів. В силу акустоелектричного перетворення, в таких охоронних датчиках на струмопровідному шлейфі останніх, можуть утворюватися небезпечні напруги в звуковому діапазоні частот, які можуть бути використані зловмисником для нелегального прослуховування приміщень при несанкціонованому підключенні до шлейфу[2]. В ході досліджень було доведено, що до 90% тексу може бути розшифровано за допомогою аналізу характеристик цих напруг.

Література

1. https://ru.vpnmentor.com/

2. Бржевський М.В., Пузняк З.М. Дослідження процесу акустоелектричного перетворення в охоронних датчиках. - Сучасний захист інформації №2(34), 2018 ст.65-71

3. Ярочкин В.И., Информационная безопасность. Учебник для студентов. 2-е изд. - М.: Академический Проект, Гаудеамус, 2004. – 544 ст.

4. https://wiki.diphost.ru/Authentication

РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ХМАРНИХ СЕРВІСІВ. МЕТОДИ ЗАХИСТУ

Стрічко Сергій Сергійович
Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

Сьогодні багато підприємств виявляють активний інтерес до хмарних сервісів через скорочення інвестицій в порівнянні з on-premises-рішеннями і відсутністю платформних витрат. Слідом за інноваційними компаніями такими сервісами зацікавився малий бізнес, фінансова та інші галузі. Користувач SaaS, FaaS, fPaaS, CaaS отримує бажані послуги, не замислюючись про середовище їх функціонування, інфраструктурі і навантаженнях. Апаратна частина існує, має звичну реалізацію, але питання її роботи повністю віддаються провайдеру послуги: в його компетенції питання розподілу навантаження на систему, масштабування і відмовостійкості, організації захисту інфраструктури, її регулярне оновлення, питання фізичного функціонування.

Інформаційні сервіси все більше абстрагуються від платформних потужностей. Користувач хоче звузити коло своєї відповідальності до рівня необхідних йому сервісів, забувши про програмне забезпечення і платформі для їх функціонування. Слідом за IaaS- і PaaS-послугами розвивається ринок SaaS-, FaaS-, fPaaS-, CaaS-послуг і мікросервісов - всі вони є різними рівнями абстракції одержуваного клієнтом сервісу. Чим менше у користувача механізмів роботи із середовищем функціонування бажаного сервісу, тим простіше і надійніше робота для провайдера і самого сервісу.[1]

Така методологія має свої зручності, але несе і певні ризики ІБ, зокрема:

• Активніше використовуються HTTP API, підключаються зовнішні джерела (зовнішні сервіси повідомлень, хмарні сховища і т.д.) і, таким чином, розширюється поверхню атаки.

• І для замовника, і для провайдера стає складніше виявлення і діагностування атак, аналіз ризиків. Модель розділеної відповідальності вносить заплутаність.

Для FaaS додатково характерні наступні проблеми:

• Vendor Lock - сервіси FaaS використовують певний нестандартизоване набір функцій (бібліотеки, сховища та ін.), Який вкрай рідко може бути повторений повністю в альтернативному FaaS-сервісі. Тобто додаток, написане або адаптоване під конкретний FaaS-ресурс, не може бути перенесено на інший ресурс без додаткової адаптації, що вимагає значної переробки вихідного коду продукту.

• Складно реалізувати повноцінне тестування продукту, повноцінне антивірусне сканування.

Для CaaS додатково характерні наступні ризики ІБ:

• Вбудовування шкідливого ПО в ланцюжок постачання. Оскільки цей ланцюжок багатоступенева, існують ризики публічного сховища, залежностей пакетів, успадкування уразливого коду, використання open-source-продуктів.

• Тривалість процедури антивірусного сканування при розгортанні контейнера.

З точки зору SaaS:

• Легкість проникнення і в зв'язку з цим поява тіньових неконтрольованих сервісів - Shadow IT, - яке загрожує витоками конфіденційної інформації.

• Обмеженість функціоналу, неможливість його самостійного розширення, додавання функцій ІБ.

Засоби і методи захисту

У схемі SaaS / FaaS захист інфраструктури сервісу покладено на провайдера. Якщо ви використовуєте сервіс від великого провайдера, то у нього гарантовано реалізовані базові механізми захисту, моніторингу та реагування, відмовостійкості, резервного копіювання та відновлення систем. Але захист контенту сервісу залишається прерогативою користувача, будь то поштове листування, файли на файловому ресурсі або вихідний код програми.

Багато SaaS- і FaaS-провайдерів пропонують вбудовані механізми захисту - наприклад, Advanced Threat Protection у Microsoft Office 365. Вони реалізують мінімально необхідний набір функцій захисту, але, як правило, неглибокої і недостатньо гнучкі. Інший приклад - Google App Engine пропонує вбудовані механізми міжмережевого екранування (включаючи DDoS-фільтр) і Google Cloud Security Scanner - сканер додатків.

Можливе використання перенаправлення трафіку через свій фільтруючий вузол. Зокрема, захист поштового потоку через додатковий фільтруючий хоп. Для веб-додатків - застосування WAF-рішень в якості reverse-proxy. На своєму вузлі ви можете організувати будь-які необхідні політики фільтрації, аналогічно традиційним методам. Але такий варіант складно організувати з точки зору маршрутизації і може привести до появи «вузького горла» (BottleNeck) в особі контент-шлюзу.

Спеціалізовані рішення щодо забезпечення ІБ

Якими продуктами, представленими на ринку, можна мінімізувати свої ризики при використанні хмарних сервісів рівня SaaS / FaaS / fPaaS / CaaS:

• У випадку з SaaS - це Cloud Access Security Brocker (CASB).

• Варіант fPaaS або CaaS можна захистити за допомогою рішення Cloud Workload Protection Platform (CWPP).

• У випадку з бессерверной додатками або FaaS користувач може використовувати статичний аналіз коду і API Gateway.

У разі CASB інтеграція з хмарними продуктами проводиться через Representational State Transfer (REST) APIs і не вимагає перенаправлення e-mail-трафіку або використання веб-проксі. Або додається вузол і інтегрується в ролі прямого або реверс-проксі. Оптимальний варіант - використання гібридної інсталяції. CASB дозволяє здійснювати сканування вхідного і вихідного поштового потоку від шкідливого ПО, застосовувати політики безпеки.

Рішення виконує наступні основні функції:

• Моніторинг та аудит. Відстеження Shadow IT - використання сторонніх сервісів. Під Shadow IT розуміються IT-пристрої, програмне забезпечення та сервіси, які присутні в організації, але не обслуговуються IT-відділом. Вони не стоять на балансі IT-відділу, їх стан і робота не контролюються, більш того, IT-департамент може взагалі нічого про них не знати. До них відносяться Amazon AWS, GPC, amoCRM і інші сервіси.

• Захист від фішингових атак і фішингових URL. Іноді додатковий аналіз і виявлення атак типу Business Email Compromise (BEC) з використанням штучного інтелекту (AI) і машинного навчання.

• Пошук і блокування відомого шкідливого ПО, включаючи приховані експлойти. Іноді пошук невідомого шкідливого ПО механізмами машинного навчання, аналіз файлів в «пісочниці», внутрішні техніки виявлення обфускацій.

• Реалізація функцій Data Loss Prevention (DLP), в тому числі для ресурсів файлового обміну.[2]

Література

1. https://www.xelent.ru/blog/bezopasnost-v-publichnom-oblake/
https://www.it-world.ru/cionews/security/149716.html

УЧАСТЬ АРТ ГРУП ДЛЯ ЗБИРАННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Смирнов Денис Сергійович

Студент групи БСДМ-61, ННІЗІ ДУТ, Київ, Україна

На сьогоднішній день існує безліч різноманітних шкідливих програмних забезпечень. Деякі з них поширюються через шкідливі посилання, але є ті, що мають профіль злому українського сектору. В даній роботі розглянуто один з прикладів шкідливого програмного забезпечення Pterodo, створений групою Gameredon. Техніки та модулі цього зловмисного програмного забезпечення постійно оновлюються, а командні центри періодично змінюються.

Група Gameredon [1] діє приблизно з 2013 року та відповідальна за ряд атак, які направлені на українські установи. За 2021 рік активність цієї групи зросла, і постійні хвилі шкідливих листів потрапляють у поштові скриньки цілей. Вкладені файли до цих листів – це документи зі шкідливими макросами, які після виконання намагаються завантажити безліч різних варіантів шкідливого програмного забезпечення.

Gameredon використовує різні мови програмування від c# до VBScript, C/C++. Інструменти, що використовуються компанією Gameredon дуже прості і призначені для збору конфіденційної інформації зі зламаних систем та подальшого поширення.

На відміну від інших груп APT, Gameredon не намагається приховати себе. Незважаючи на те, що їх інструменти мають можливість завантажувати та виконувати довільні файли, які могли б бути набагато прихованими. Основна увага цієї групи – поширюватись якомога швидше в мережу своєї жертви, намагаючись вилучити конфіденційні дані.

Група Gameredon використовує пакет, що містить власний проект Microsoft Outlook Visual Basic for Application (VBA). Цей пакет шкідливого коди починається з VBScript, який спочатку вбиває процес Outlook, якщо він запущений, а потім знімає безпеку навколо виконання макросу VBA у Outlook, змінюючи значення реєстру. Він також зберігає на диску шкідливий файл OTM (проект Outlook VBA), який містить макрос, вкладений файл шкідливої електронної пошти та, у деяких випадках, список одержувачів, яким слід надсилати електронні листи.

Далі він перезапускає Outlook за допомогою спеціальної опції, які завантажує проект Gamaredon VBA. Шкідливий код виконується після отримання події Application.Startup . Вони використовували цей модуль трьома різними способами для надсилання шкідливої електронної пошти на адресу:

1) Усі в адресній книзі жертви.
2) Усі в одній організації.
3) Попередньо визначений список цілей.

Цікаво, що деякі спеціальні інструменти, що були описані в публікації Palo Alto Networks [2] за 2017 рік все ще оновлюються та використовуються

сьогодні. Деякі демонструють значну схожість, але є переписані на іншу мову програмування.

Важливо, що модуль компілятора, який використовується Gameredon, використовує такі ж методи обфускації, як вставка небажаного коду та обфускація рядків. Він містить у своєму тілі вихідних код завантажувача, закодований base64.

Група Gamaredon використовує багато різних доменів, безкоштовних та платних, для своїх серверів C&C. Безкоштовні домени-це переважно DDNS з No-IP: hopto.org , ddns.net , myftp.biz , тоді як платні домени реєструються через реєстратора REG.RU і включють .fun, .site, .space, .r , .website. і .xyz TLD. Вони постійно змінюють домени, що використовуються їх інструментами, але переважно на невеликій кількості ASN.

Незважаючи на простоту більшості своїх інструментів, група Gamaredon також здатна впровадити деякі новинки, наприклад, їх модуль Outlook VBA. Однак, оскільки це далеко не приховано, в довгостроковій перспективі це не може відповідати здатній організації. Різноманітність інструментів, якими володіє Gamaredon, може бути дуже ефективним при відбитку пальців на машині та розумінні наявних конфіденційних даних, а потім розповсюдженню по мережі.

Джерела :

1) Gamaredon group grows its game [Електронний ресурс] – Режим доступу до ресурсу: https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/.
The Gamaredon Group Toolset Evolution [Електронний ресурс] – Режим доступу до ресурсу: https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/.

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ФАЙЛОВИХ СЕРВЕРІВ ОРГАНІЗАЦІЇ

Хотінь Кароліна Юріївна

Студентка групи БСДМ – 61 ННІЗІ, Київ, Україна

В роботі розглянуто проблему захисту файлових серверів організації. Для захисту файлових серверів запропоновоно рішення SecureSphere File Security, для якого визначено їх архітектуру та основні функціональні можливості.

Ключові слова: файловий сервер, моніторинг, користувач, складові архітектури, функції

Організації, які працюють з інформаційними технологіями, для зручного використання своїх даних впроваджують до своє інфраструктури файлові сервери. Тож питання, як захистити дані, які знаходяться на файловому сервері з`являється у керівників підрозділів безпеки [1, стор.7].

Використання файлового серверу, дозволяє користувачам організації отримувати необхідні права для доступу до певних файлів у мережевій системі сховища даних, можуть їх відкривати та редагувати, а також видаляти файли та папки точно так, як якщо б вони працювали на власному комп’ютері.

На файловому сервері для кожного авторизованого користувача надається певне місце для зберігання робочих файлів. Інші користувачі можуть також відкривати, читати та редагувати їх відповідно до їх прав доступу. Ці права встановлюють адміністратор файлового сервера. Він визначає, хто які файли та у яких папках може відкривати та переглядати, а також (якщо було надано дозвіл) редагувати, видаляти або додавати нові файли [2].

В загальному випадку архітектура інформаційної системи та місце файлового серверу показано на рис.1.

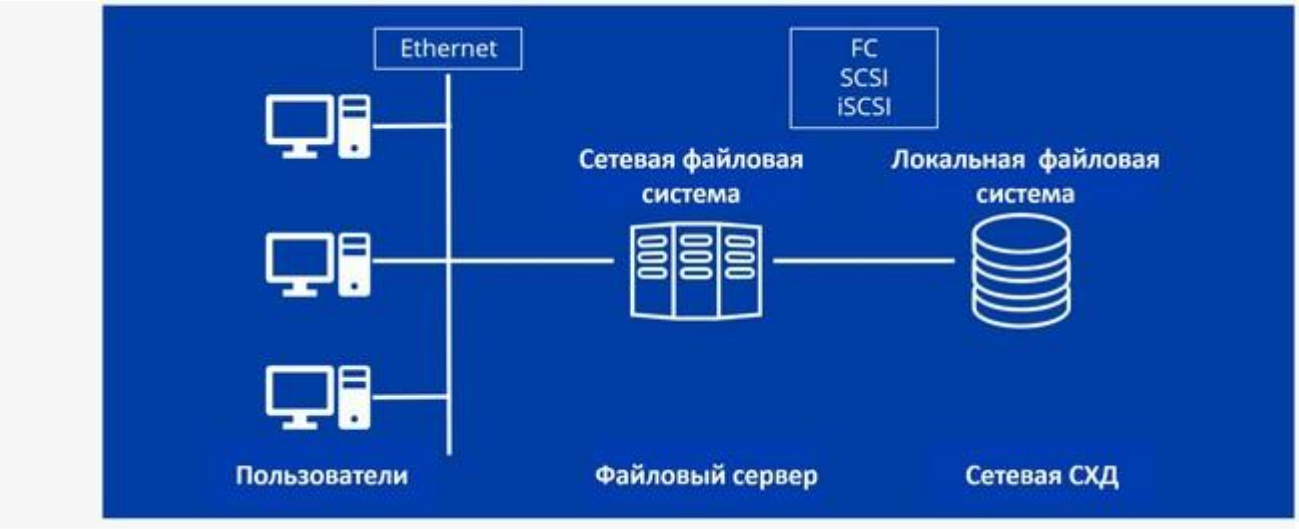


Рис.1. Місце файлового серверу в інформаційній системі компанії [https://itelon.ru/blog/faylovyy-server/]

Для захисту даних, які зберігаються на файловому сервері необхідно забезпечити безпеку файлового серверу. Для вирішення поставленої задачі пропонується використати рішення SecureSphere File Security, яке забезпечує безпеку файлових серверів CIFS та NFS (RHEL та Solaris), захищає та контролює важливі дані, зберігає файли у неструктурованих файлах, такі документи як текстові редактори, електронні таблиці та багато іншого.

Рішення SecureSphere File Security захищає конфіденційні файли на файлових серверах, пристроях зберігання та репозиторіях вмісту. SecureSphere забезпечує повну прозорість управління даними, їх використанням та правами доступа, а також дозволяє керівникам, аудиторам, спеціалістам з питань безпеки та IT-менеджерам підвищити безпеку даних та забезпечити нормативні вимоги [3].

SecureSphere виконує наступні функції:

•Аудит доступу до конфіденційних файлів з боку привілейованих користувачів та користувачів додатків.

•Попереджує або блокує запити на доступ до файлів, які порушують корпоративні політики.

•Оцінює реагування на інциденти та цифрову криміналістику за рахунок централізованого управління та розширеної аналітики.

Основні функціанолтні складові даного рішення показано на рис.2.

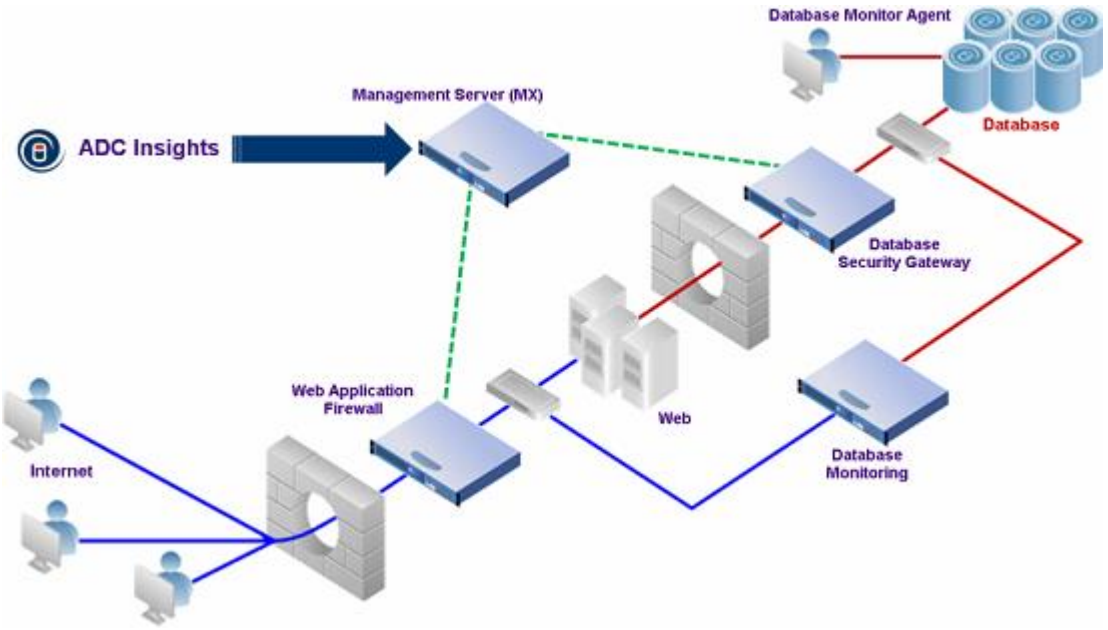


Рис.2. Складові архітектури SecureSphere

Моніторинг та шлюз безпеки. Шлюз моніторингу та безпеки виконує моніторинг додатків та даних, який забезпечує повну видимість того, що ці дані фактично використовуються на підприємствах, незалежно від того, отримують вони прямий або непрямий доступ через додатки. Це також забезпечує повний обсяг моніторингу активності баз даних, файлових серверів та додатків та блокує поточний трафік.

Сервер управління (MX). Надає інструмент централізованого управління для 15 шлюзів SecureSphere, що дозволяє виконувати великомасштабні розгортання в розподілених середовищах.

SecureSphere пропонує ряд основних функцій, які зачіпають всі аспекти діяльності файлових служб.

Доступні функції SecureSphere включають наступне:

Центрі захисту додатків

Політики -політики безпеки захищають від більшості відомих атак і загроз. Надається велика кількість політик за замовчуванням. Адміністратори можуть змінювати існуючі політики та створювати нові.

Моніторинг -Моніторинг SecureSphere інформує про всі події, що відбуваються в Active Directory, і дозволяє зрозуміти ризик, пов'язаний з підозрілою активністю.

Аудит - SecureSphere надає комплексні можливості аудиту, які дозволяють налаштовувати політики аудиту, які визначають, які дані підлягають аудиту, а потім відображати перевірені дані у вигляді зручних для читання графіків, які розбивають перевірені дані на легкі для читання звіти на основі безлічі чинників, таких які відслідковують сервери, різні типи користувачів, аспекти, пов'язані із запитами, і багато іншого. SecureSphere додатково може інтегруватися із зовнішніми системами управління інформацією і подіями безпеки (SIEM), щоб включити ці системи в робочий процес управління даними.

Складання звітів - SecureSphere включає надійний механізм звітності, який дозволяє адміністраторам створювати заздалегідь визначені або визначені користувачем звіти на основі накопичених даних, які можуть бути створені або автоматично, або на льоту, або за розкладом для регулярного виконання, а потім розподілятися по мірі необхідності.

Універсальне відстеження користувачів - функція універсального відстеження користувачів (UUT) SecureSphere підвищує безпеку і аудит, аналізуючи трафік, щоб точно пов'язувати користувачів зовнішнього інтерфейсу додатку до запитів до бази даних.

Таким чином обрана рішення дозволить забезпечити безпеку файлових серверів інформаційної системи компанії та дозволить визначати та вирішувати завдання щодо підвищення безпеки роботи компанії.

Перелік посилань:

1. Guide to General Server Security [електронний ресурс] режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf .

2. Функції файлового сересеру https://itelon.ru/blog/faylovyy-server/ [електронний ресурс] режим доступу: https://itelon.ru/blog/faylovyy-server/

3. v12.6 Guide File Security [електронний ресурс] режим доступу: https://docs.imperva.com/bundle/v12.6-file-security-user-guide/page/375.htm .

МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ СПЕЦІАЛІЗОВАНИХ ПРОЦЕСОРІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Ящук Андрій Андрійович

Студент групи БСДМ – 61 ННІЗІ, Київ, Україна

Метою доповіді є постановка та рішення задачі оптимального резервування структури високопродуктивних процесорів, що будуються на базі непозиційної системи числення у залишкових класах (СЗК).

Однією з основних вимог, що пред'являється до сучасних комп'ютерних систем (КС), які працюють у реальному часі, є забезпечення заданого рівня надійності їх функціонування. Це пов'язано, перш за все, з тим, що вихід з ладу або навіть короткочасний збій у роботі таких КС може призвести до аварій або завдати серйозної економічної шкоди.

Існує два основні підходи для підвищення надійності КС підвищення надійності окремих логічних елементів (використання нової елементної бази) та введення різних типів надлишковості (застосування різних видів резервування).

Оскільки надійність елементів КС визначається рівнем розвитку технології, то очевидно, що введення надлишковості при використанні будь-якої елементної бази є найбільш ефективним шляхом підвищення надійності КС. У той же час, застосування кодів у СЗК дає можливість підвищити надійність КС за рахунок використання властивостей СЗК (малорозрядність, рівноправність та незалежність залишків). Це дозволяє більш ефективно застосовувати структурне резервування у порівнянні з кодами, що представлені позиційною системою числення (ПСЧ).

При використанні резервування, формулювання задачі оптимального резервування можливе в двох варіантах пряма задача, коли потрібно забезпечити ймовірність безвідмовної роботи КС не менше заданої, при мінімальних витратах; обернена задача, коли потрібно забезпечити максимально можливу ймовірність безвідмовної роботи КС при заданих витратах.

Список використаних джерел:

1. Computing System Reliability. Kluwer Academic Publishers; 2004; Available from: http://dx.doi.org/10.1007/b100619

2. Hongbin LI, Qing Zhao, Zhenyu Yang. Reliability modeling of fault tolerant control systems. Int. J. Appl. Math. Comput. Sci. 2007. Vol. 17, No. 4. P. 491–504. http://eudml.org/doc/207854.

ДОСЛІДЖЕННЯ СПОСОБІВ І ПРОТОКОЛІВ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМАХ

Баргилевич Олександр Анатолійович, БСДМ-62
Державний університет телекомунікацій,
м. Київ

При спробі потрапити в закритий клуб вас ідентифікують (запитають ваше ім'я і прізвище), автентифікують (попросять показати паспорт і звірять фотографію) і авторизують (перевірять, що прізвище знаходиться в списку гостей), перш ніж пустять усередину. На сьогоднішній день розробникам досить тяжко підтримувати стійкість інформаційно-телекомунікаційні системи до загроз . Отже постає питання як захистити такі технології. Для цього спочатку потрібно виявити загрози за допомогою тестування системи на наявність вразливостей. Тож далі мі розглянемо способи автентифікації користувачів для подальшої безпеки.

Автентифікація по паролю

Цей метод ґрунтується на тому, що користувач повинен надати «username» та «password» для успішної ідентифікації і автентифікації в системі. Пара «username» та «password» задається користувачем при його реєстрації в системі, при цьому в якості «username» може виступати адреса електронної пошти користувача.

HTTP автентифікація

Цей протокол, описаний в стандартах HTTP 1.0 / 1.1, існує дуже давно і до цих пір активно застосовується в корпоративному середовищі. Стосовно до веб-сайтам працює наступним чином:

- Сервер, при зверненні неавторизованого клієнта до захищеного ресурсу, відсилає HTTP статус "401 Unauthorized" і додає заголовок "WWW-Authenticate" із зазначенням схеми і параметрів автентифікації.
- Браузер при отриманні такої відповіді, автоматично показує діалог введення «username» та «password». Користувач вводить деталі свого облікового запису.
- Сервер автентифікує користувача за даними з цього заголовка. Рішення про надання доступу (авторизація) проводиться окремо на підставі ролі користувача, ACL або інших даних облікового запису.

Існує кілька схем автентифікації, що відрізняються за рівнем безпеки:

- Basic - найбільш проста схема, при якій «username» та «password» користувача передаються в заголовку Authorization в незашифрованому вигляді (base64-encoded). Однак при використанні HTTPS є відносно безпечною.
- Digest - схема, при якій сервер посилає унікальне значення, а браузер передає хеш пароля користувача.
- NTLM (відома як Windows authentication) - схема, при якій пароль не передається в чистому вигляді. Ця схема не є стандартом HTTP, але підтримується більшістю браузерів і веб-серверів. Вразлива до pass-the-hash-атакам.

Форм автентифікація

Для цього протоколу немає певного стандарту, тому всі його реалізації специфічні для конкретних систем.

Працює це за наступним принципом: в веб-додаток включається HTML-форма, в яку користувач повинен ввести свої «username» та «password» і відправити їх на сервер. У разі успіху веб-додаток створює токен (ключ), який зазвичай поміщається в cookies.

Автентифікація за сертифікатами

Сертифікат являє собою набір атрибутів, що ідентифікують власника, підписаний акредитованим центром сертифікації ключів (CA). CA виступає в ролі посередника, який гарантує справжність сертифікатів. Також сертифікат криптографічно пов'язаний з закритим ключем, який зберігається у власника сертифіката і дозволяє однозначно підтвердити факт володіння сертифікатом.

У веб-додатках традиційно використовують сертифікати стандарту X.509. Автентифікація за допомогою X.509-сертифіката відбувається в момент з'єднання з сервером і є частиною протоколу SSL / TLS.

Автентифікація за одноразовими паролями

Автентифікація за одноразовими паролями зазвичай застосовується додатково до автентифікації по паролів для реалізації «two-factor authentication» (2FA). Наявність двох факторів дозволяє в значній мірі збільшити рівень безпеки, що м. Б. затребуване для певних видів веб-додатків. Інший популярний сценарій використання одноразових паролів - додаткова автентифікація користувача під час виконання важливих дій: переказ грошей, зміна налаштувань і так далі.

Отже вище ми розглянули основні способи та методи автентифікації користувачів в повноцінних корпоративних системах.

Література:

1. HTTP Authentication [Електронний ресурс] – Режим доступу: https://www.httpwatch.com/httpgallery/authentication/

2. Автентифікація за допомогою форм [Електронний ресурс] – Режим доступу: https://professorweb.ru/my/ASP_NET/security/level2/2_1.php

3. Огляд способів і протоколів аутентифікації в веб-додатках [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/dataart/blog/262817/

ТЕХНОЛОГІЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ ОРГАНІЗАЦІЇ

Бутковський Семен Валерійович

БСДМ-62

Державний університет телекомуникацій

Навчально-науковий інститут захисту інформації

м.Київ

Захист конфіденційних даних, є важливою частиною кібербезпеки на підприємстві. Втративши ці дані організація може понести великі збитки, не тільки фінансові, а й репутаційні.

Згідно закону України про захист персональних даних: «Персональні дані - це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»;[1] (наприклад: інформація про найманого працівника є базою персональних даних, оскільки особиста справа, трудові книжки, копії паспорта, документів про освіту зберігаються та обробляються роботодавцем).

Та згідно цього ж закону: «Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкової втрата або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.»[1]

Аби забезпечити захист персональних даних, потрібен комплекс заходів технічного, організаційного та організаційно-технічного характеру, спрямованих на захист даних.

Одним із засобів захисту, є Data Loss Prevention (DLP) системи.

DLP - технології запобігання витоків конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої для такого запобігання витоків. DLP-системи будуються на аналізі потоків даних, які перетинають периметр захищаємої інформаційної системи.

Цінні корпоративні дані, які ваша організація намагається захистити за допомогою міжмережевих екранів і паролів, буквально витікають крізь пальці інсайдерів. Це відбувається як випадково, так і в результаті умисних дій - неправомірного копіювання інформації з робочих комп'ютерів на флеш-накопичувачі, смартфони, планшети та інші носії даних. Крім того, дані можуть безконтрольно передаватися інсайдерами через електронну пошту, служби миттєвого обміну повідомленнями, веб-форми, форуми та соціальні мережі. Бездротові інтерфейси - Wi-Fi і Bluetooth- нарівні з каналами локальної синхронізації даних з мобільними пристроями відкривають додаткові шляхи для витоків інформації з комп'ютерів користувачів організації.[2]

Крім інсайдерських загроз, інший небезпечний сценарій витоків реалізується при зараженні комп'ютерів шкідливими програмами, які можуть записувати введений з клавіатури текст або окремі види збережених в оперативній пам'яті комп'ютера даних і згодом передавати їх в Інтернет.[2]

DLP-системи здійснюють аналіз потоків даних, які перетинають периметр захищаємої інформаційної системи. При виявленні в цьому потоці конфіденційної інформації спрацьовує активна компонента системи і передача повідомлення (пакета, потоку, сесії) блокується. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак: грифа документа, спеціально введених міток, значень хеш-функції з певної множини і т.д.[3]

Сучасні DLP-системи володіють величезною кількістю параметрів і характеристик, які обов'язково необхідно враховувати при виборі рішення для організації захисту конфіденційної інформації від витоків. Мабуть, найважливішим з них є використовувана мережева архітектура. Згідно з цим параметром продукти розглянутого класу поділяються на дві великі групи[3]:

1. Шлюзові
2. Хостові.

У першій групі використовується єдиний сервер, на який направляється весь вихідний мережевий трафік корпоративної інформаційної системи. Цей шлюз займається його обробкою з метою виявлення можливих витоків конфіденційних даних.[3]

Другий варіант заснований на використанні спеціальних програм - агентів, які встановлюються на кінцевих вузлах мережі - робочих станціях, серверах додатків та ін.[3]

Список використаних джерел:

1. *Інтернет-джерело:* https://zakon.rada.gov.ua/laws/show/2297-17#Text
2. *Інтернет-джерело:* https://www.devicelock.com/ru/dlp/data-loss-prevention/data-leakage-prevention.html
3. *Інтернет-джерело:* http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ШКІДЛИВИХ ЗАПИТІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ПРОТОКОЛУ DNS

Гаврилей Олександр
Петрович, БСДМ-62
Державний Університет
Телекомунікацій
Навчально-науковий
інститут захисту інформації
м.Київ

На сьогоднішній день комп'ютерні мережі використовуються майже у всіх сферах людського побудут, тому вони мають неабияку увагу у кіберзлочинців які можуть завдати як фінансового так і репутаційних збитків. Сучасні засоби виявлення шкідливих запитів можуть знаходити більшість видів атак спрямованих на компютерну мережу, але потребують часу для правильного налаштування та постійної підтримки тому вплив і вартість нападів залишаються надзвичайно високими і продовжують зростати з року в рік. Це впливає не тільки на фінанси компаній, але і на імідж бренду та конфіденційність користувацьких даних.

З початком пандемії кількість програм-вимагачів зросла і стала самостійною галуззю, що викликає серйозне занепокоєння у багатьох організацій. Використання фільтрації і блокування DNS має вирішальне значення, оскільки може допомогти зупинити атаки програм-вимагачів відразу після зараження, коли шкідливе ПО намагається зв'язатися з системою управління та контролю (C&C). При запуску хмарного середовища складно покладатися на службу DNS хмарних провайдерів, і для цього потрібні постійні оновлення та моніторинг безпеки сервісів. 52% розглядають DNS як критично важливий компонент своєї загальної стратегії, 46% постраждали від простою хмарного середовища в результаті DNS-атаки і 23% постраждали від DNS-атаки з неправильною конфігурацією хмарного середовища. Основною причиною такої схильності DNS-систем загрозам є те, що вони працюють по протоколу UDP, більш уразливому, ніж TCP. Згідно Cloud Security Alliance в своєму звіті State of Cloud Security 2020 року, неправильна конфігурація хмари залишається основною причиною витоку даних в хмарі. «Неправильна конфігурація і в хмарних середовищах можуть завдати серйозної шкоди. Наприклад, забуті IP-адреси віртуальних машин в хмарі можуть залишити двері відчиненими для DNS-атак, які, як правило, націлені на організації з великими і складними інфраструктурами. Використання спеціального рішення DDI (DNS-DHCP-IPAM) допоможе усунути ризик неправильного налаштування, особливо якщо включена автоматизація», - йдеться в звіті [3]. Хоча безпеку DNS є критичним компонентом загальної стратегії безпеки, і майже у всіх (99%) організацій є рішення, 42% не використовують виділене рішення безпеки DNS, щоб допомогти їм заповнити потенційні прогалини в уразливостях компютерних мереж, залишені традиційними продукти мережевої безпеки. «Дослідження безпеки DNS в 2021 році підтверджує, що майже у всіх компаній були порушені додатки і сервіси через DNS-атак. У міру того, як кордони підприємства стираються, організації приділяють більше уваги захисту віддалених співробітників, а також своєї локальної та хмарної інфраструктури. Для досягнення цілей нульового довіри за рахунок сегментації мережі і контролю

доступу до додатків ключова роль DNS в забезпеченні видимості поведінки клієнтів і детальної фільтрації стає все більш важливою для запобігання поширенню атак якомога раніше в потоці трафіку » сказав Жан-Ів Бізіо, технічний директор EfficientIP [1].

На сьогоднішній день існує багато підходів виявлення шкідливого мережного трафіку [2]. В запропоновано систему виявлення шкідливих доменів на основі пасивного DNS-аналізу, що здійснює класифікацію доменних імен за 4 групами ознак, які можуть бути вилучені з DNS-трафіка: часові ознаки; ознаки, що базуються на DNS-відповідях; ознаки, що базуються на значеннях TTL; ознаки, що базуються на доменному імені. В запропоновано підхід, який дозволяє виявляти доменні імена бот-мереж, які використовують метод «швидкозмінних» мереж. Висновок щодо шкідливості доменного імені здійснюється за рядом ознак, отриманих на основі аналізу даних, вилучених з A-, NS-, SOA- та BGP-запитів щодо доменного імені: значення часу життя A-записів (TTL-періоду), IP-адрес в A- та NS-записах, а також значення таймера “retry”.

Список використаних джерел:

1. EfficientIP release 2021 Global DNS threat report [Електронний ресурс] – Режим доступу до ресурсу: https://cybermagazine.com/network-security/efficientip-release-2021-global-dns-threat-report
2. Detecting DNS Tunneling [Електронний ресурс] – Режим доступу до ресурсу: https://sansorg.egnyte.com/dl/r4ouqZy5dp
3. IDC 2021 Global DNS Threat Report [Електронний ресурс] – Режим доступу до ресурсу: https://www.efficientip.com/resources/idc-dns-threat-report-2021/

ТЕХНОЛОГІЯ УПРАВЛІННЯ ІНЦИДЕНТАМИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ WAZUH

Гізун Ігор Ігорович, БСДМ-62
Державний університет телекомунікацій
Навчально-науковий інститут Захисту Інформації
м. Київ

На сьогоднішній день технології виявлення загроз та реагування на інциденти в інформаційній системі підприємства залишаються складними. Головною проблемою виступає збільшення обсягу та різносторонності кібератак. Тобто, збільшується не лише їх ефективність, а й складність виявлення. Саме ці критерії передбачають потребу у пошуку шляхів виявлення інцидентів та забезпечення захисту інформаційної системи підприємства.

Протягом двох років складність управління інцидентами лише збільшувалась, зловмисники стали більш витонченими та небезпечними і своєчасне виявлення стало справжньою проблемою. Шкідливе ПЗ, додатки-вимагачі, інциденти, пов’язані з компрометацією робочої пошти та ін. Рішення з кібербезпеки в інформаційних системах підприємства повинні забезпечувати виявлення поведінкових аномалій у режимі реального часу, забезпечувати швидке реагування на інциденти та інтелектуальну візуалізацію мережі та всіх її взаємопов’язаних вузлів.

SIEM-система Wazuh [1] використовується для збору, агрегації, індексування та аналізу даних безпеки, допомагаючи організаціям виявляти вторгнення, загрози та поведінкові аномалії. Оскільки кіберзагрози стають все більш складними, моніторинг у реальному часі та аналіз безпеки необхідні для швидкого виявлення та усунення загроз. Wazuh надає необхідні можливості моніторингу та реагування та забезпечує розвідку безпеки і виконує аналіз даних. Збір даних в SIEM-системі Wazuh здійснюється встановленими на них агентами. У разі відсутності колектора відповідного джерела, події можуть бути відправлені в форматі стандарту Syslog.

Wazuh сканує відстежувані системи, шукаючи шкідливе програмне забезпечення, руткіти та підозрілі аномалії. Він може виявляти приховані файли, масковані процеси або незареєстровані слухачі мережі, а також невідповідності у відповідях системних викликів.

Wazuh читає журнали операційної системи та програм і аналізує та зберігає відповідно до спрацьованих правил на ту чи іншу подію. Правила Wazuh допомагають користувачеві помічати помилки програми або системи, неправильні налаштування, спроби та/або успішні зловмисні дії, порушення політики та інші проблеми безпеки та експлуатації.

Wazuh відстежує файлову систему, визначаючи зміни у вмісті, дозволах, власності та атрибутах файлів, які потребують уваги. Він також ідентифікує користувачів та програми, які використовуються для створення або зміни файлів. Можливості моніторингу цілісності файлів можна використовувати в поєднанні

з аналізом загроз для виявлення загроз або скомпрометованих хостів. Крім того, цього вимагають декілька стандартів відповідності нормам, таких як PCI DSS.

Wazuh зберігає дані інвентаризації програмного забезпечення та порівнює з базами даних CVE (Common Vulnerabilities and Exposure), щоб ідентифікувати добре відоме вразливе програмне забезпечення. Автоматизована оцінка вразливості допомагає користувачеві визначити слабкі місця своїх критичних активів і вжити заходів, перш ніж зловмисники можуть їх використовувати.

Wazuh дозволяє домогтися практично повної автоматизації процесу виявлення загроз, та його не правильне налаштування не призведе до лише витрачених коштів.

Список використанних джерел:

1. Wazuh documentation [Електронний ресурс] – Режим доступу: https://documentation.wazuh.com/current/index.html

ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ

Данильченко Юлія Сергіївна

Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації

м. Київ

У даній роботі розглянуто проблему захисту кінцевих точок організації. Було встановлено необхідність наявності технології визначення рівня безпеки кінцевих точок, аби запобігти доступу неавторизованих користувачів до конфіденційних даних організації. Особливо важливим є використання таких рішень в компаніях, які дозволяють співробітникам приносити з собою власні пристрої, наприклад ноутбуки або смартфони, що може поставити під загрозу безпеку інформації компанії або мережі. На основі дослідження було запропоновано оптимальне та актуальне рішення, щодо захисту кінцевих точок організації.

Кінцевим пристроєм називається апаратний пристрій, підключений до локальної або глобальної мережі організації, який ініціалізує процес передачі даних по мережі з такими ж кінцевими пристроями. Іноді інформацію з кінцевого пристрою запитує користувач, а іноді такі пристрої самі обмінюються даними без втручання користувача.

У широкому сенсі термін може відноситися до будь-якого пристрою, який підключено до мережі: настільних комп'ютерів, ноутбуків, смартфонів, планшетів, принтерів або іншого спеціалізованого обладнання, наприклад POS-терміналів або роздрібним кіоскам, які діють як кінцева точка користувача в розподіленій мережі [1].

Одна з найбільших проблем кінцевих пристроїв - це комплексна безпека мережі або корпоративної системи. В організації необхідна наявність технології, яка зможе оперативно визначати, чи можуть кінцеві пристрої бути вразливими точками в безпеці мережі, тобто чи можуть неавторизовані користувачі отримати доступ до кінцевого пристрою і використовувати його для отримання важливих або конфіденційних даних організації.

Безпека кінцевих точок має вирішальне значення для підприємств будь-якого розміру. Кіберзлочинці постійно винаходять нові способи використання співробітників, проникнення в мережі і крадіжки приватної інформації. Незалежно від розміру організації, повинні використовуватися надійні служби безпеки кінцевих точок [2].

Для захисту інформації, яка зберігається на кінцевих точках організації доцільно використовувати рішення Endpoint Protection або захист кінцевих точок, які є комплексною протидією атакам на комп'ютери, планшети, мобільні та інші пристрої, які використовуються в організації.

Одним з передових рішень для захисту кінцевих точок є Panda Adaptive Defense 360, яке представляє з себе інноваційне хмарне рішення інформаційної безпеки комп'ютерів, ноутбуків і серверів. Воно автоматизує процеси запобігання і виявлення атак на кінцеві пристрої, стримування і реагування на будь-які сучасні і перспективні складні загрози, загрози нульового дня, шифрувальники, фішинг, експлойти в пам'яті, безфайлові атаки і атаки, які не використовують шкідливі програми, всередині і за межами корпоративної мережі.

Panda Adaptive Defense 360 поєднує в собі традиційні технології захисту кінцевих пристроїв (EPP) з інноваційними технологіями адаптивної захисту, виявлення і реагування (EDR), що дозволяє справлятися з передовими кіберзагрозами.

Дане рішення буде цінним для організації через наявність розширеного захисту кінцевих точок, яке засновано на чотирьох принципах:

1. Запобігання, виявлення та реагування на атаки, що використовують шкідливі програми або ні.
2. Видимість в реальному часі і ретроспективі всієї докладної інформації про всі процеси на кінцевих пристроях.
3. Класифікація 100% процесів на кінцевих пристроях.
4. Threat Hunting і Експертний аналіз атак на кінцеві пристрої [3].

Інтеграція та використання даного рішення для захисту кінцевих точок організації, забезпечить детальний огляд всіх процесів на кожному кінцевому пристрої організації, повний контроль всіх запущених процесів і скорочення схильності до атак.

Список використаних джерел

1. Endpoint Device [Електроний ресурс] – Режим доступу до ресурсу: https://www.barracuda.com/glossary/endpoint-device
2. Understanding Endpoints and Endpoint Security [Електроний ресурс] – Режим доступу до ресурсу: https://www.webroot.com/us/en/resources/glossary/what-is-endpoint-security
3. Panda Adaptive Defense 360 – WatchGuard Technologies, 2021 – 1p.

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАННИМИ В КОРПОРАТИВНІЙ МЕРЕЖІ

Добреля Віталій Олексійович, БСДМ-62
Державний університет
телекомунікацій,
м. Київ

Тенденція до віддаленої роботи пропонує підприємствам ряд переваг, таких як гнучкість співробітників, скорочення витрат на офісні приміщення і багато іншого. Однак тут є свої проблеми. А саме, організаціям необхідно визначити, як вони можуть найкращим чином захистити свої мережі і конфіденційні дані, коли значний відсоток їх співробітників виконує роботу з особистих пристроїв і в загальнодоступних мережах.

Без належного захисту співробітники, підключені до корпоративної мережі з дому, можуть піддавати корпоративну інформацію ризику. Це пов'язано з тим, що доступ в Інтернет через повністю загальнодоступну мережу, тобто через звичайного постачальника інтернет-послуг (ISP), відкриває доступ до пристроїв і онлайн-активності для зловмисників. Це не означає, що кожен раз, коли співробітник виконує роботу з віддаленого місця, він піддає ризику особисту інформацію. Проте, без будь-яких запобіжних заходів ймовірність того що інформація буде перехоплена зростає.

Відповідь - корпоративна мережа VPN. Ця технологія може фактично з'єднувати цілі філії з центральним офісом, дозволяючи командам в географічно розділених організаціях працювати разом і обмінюватись важливою інформацією.

Традиційний апаратний VPN був вперше представлений більш 30 років тому. Трафік у віртуальній мережі відправляється безпечно шляхом встановлення зашифрованого з'єднання через Інтернет, відомого як тунель. VPN-трафік з такого пристрою, як комп'ютер, планшет або смартфон, шифрується при проходженні через цей тунель. Після цього віддалені співробітники можуть використовувати віртуальну мережу для доступу до корпоративної мережі.

Незважаючи на розвиток VPN протягом багатьох років, застарілий віддалений доступ створює додаткові ризики для безпеки підприємств. Критичні обмеження VPN включають відсутність сегментації мережі, видимість мережі, локальну безпеку користувачів, а також відсутність надійної безпеки мережі. VPN також не підходять для зростаючого використання хмарних ресурсів, оскільки вони вимагають комп'ютерного обладнання, постійного управління і не можуть легко адаптуватися до змін мережі або сервера. Це ускладнює масштабування для нових користувачів і мережевого розташування. Для порівняння, корпоративна модель VPN усуває традиційні обмеження VPN, забезпечуючи при цьому більш гнучку хмарну платформу, підвищену безпеку, конфіденційність, деталізацію управління доступом користувачів і аналітику.

Незважаючи на те, що існує кілька типів VPN, організації прагнуть реалізувати або безпеку по інтернет-протоколу (IPsec VPN), або многопротокольную комутацію по мітках (MPLS VPN) для підключення своїх віддалених співробітників до даних, додатків та інших корпоративних ресурсів своєї організації.

Терміни «IPsec» і «MPLS» представляють спосіб передачі даних для кожного типу VPN. Основні відмінності між IPsec і MPLS пов'язані з типом мереж. IPsec з'єднує сайти за допомогою загальнодоступного Інтернет-транспорту, який складається з взаємозв'язаних мереж, керованих різними

операторами. MPLS з'єднує сайти, використовуючи мережу MPLS одного оператора. Оператор зв'язку має адміністративний контроль над мережею, в тому числі можливість застосовувати політики якості обслуговування до потокам трафіку. MPLS VPN відокремлюють трафік одного клієнта від трафіку інших, щоб зберегти його конфіденційність в інфраструктурі.

Корпоративні VPN забезпечують безпеку мережі і відповідність нормативним вимогам для організацій, які перейшли на загальнодоступну хмарну середу або гібридну хмарну середу з використанням SSL або IPsec, набору захищених мережевих протоколів, який аутентифікує і шифрує дані на рівні IP-пакетів. Встановлення віртуальних тунельних з'єднань з IPsec між мережевими ресурсами та зовнішнім пристроєм та користувачем вимагає двох основних компонентів: програмного забезпечення VPN-клієнта та захищеного шлюзу доступу до мережі.Для створення корпоративного тунелю VPN протокол IPsec узгоджує асоціації безпеки (SA) з протоколом управління Internet Key Exchange (IKE) для створення автентифікованого та безпечного каналу зв'язку між користувачем, пристроєм та мережевими ресурсами. IPsec VPN обмінюється ключами для наскрізного шифрування в два етапи. По-перше, користувачі зі своїми пристроями встановлюють безпечний канал, який узгоджує відповідність безпеки (SA) IPsec. По-друге, користувачі і пристрої узгоджують IPsec SA для аутентифікації трафіку, який буде проходити через тунель.

IP-трафік, який проходить між двома компонентами, проходить між приватним шлюзом і клієнтом, тим самим створюючи тунель IPsec для встановлення безпечного тунелю зв'язку VPN. Приватний тунель і дані, що передаються по будь-якій мережі, загальнодоступній або приватній, зашифровані, що забезпечує конфіденційність і безпеку всіх даних.

Література:

1. Cisco. Virtual Private Network [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

2. N-able. Common Uses of a VPN Corporate Network [Електронний ресурс] – Режим доступу: https://www.n-able.com/blog/how-vpn-works

3. Perimeter 81. Corporate VPN [Електронний ресурс] – Режим доступу: https://www.perimeter81.com/resources/corporate-vpn-solution

ЩОДО ОСОБЛИВОСТЕЙ МОНІТОРИНГУ БЕЗПЕКИ СИСТЕМ ACTIVE DIRECTORY

Драгунцов Роман Ігорович
студент кафедри навчально наукового інституту Захисту інформації
e-mail: draguntsow@yahoo.com

Анотація

Сучасна інформаційна інфраструктура у середовищах корпоративних ІС здебільшого покладається на використання певного масштабного фреймворку, системи, що може задовольнити вимоги централізованого керування більшістю функцій адміністрування, надати можливості надійної аутентифікації та авторизації користувачів, здійснити контроль доступу. Одним з найбільш поширених рішень такого классу є Microsoft Active Directory. Дана технологія дозволяє ефективно вирішити всі вищеназвані питання а також ефективно відобразити організаційну струкутуру підприємства у її інформаційну систему. Однак централізація будь-яких адміністративних можливостей створює істотні ризики безпеки, які підтверджуються численними фактами використання вразливостей MS AD для підвищення привілеїв та просування по інфраструктурі при складних кібератаках. Для запобігання виникнення таких вразливостей та попереджання здійснення ризиків необхідно здійснювати постійний специфічний моніторинг середовища. Особливості даного моніторингу будуть висвітлені в даній доповіді.

Вступ

Microsoft Active Directory є в першу чергу ієрархічною системою – службою каталогів. Даний статус передбачає можливість ефективного відображення організаційно-адміністративної структури на інформаційної системи зі створенням відповідних зв’язків та контролів розмежувань доступу. Дана структура навіть в умовах відносно невеликих організацій (до декількох десятків співробітників) може мати істотну складність та розгалудженість - враховуючи також включення істотної кількості службових та технічних облікових записів, необхідних для підтримки функціонування інформаційних сервісів, загальна структура стає ще більш заплутаною та непрозорою навіть при наявності повного доступу до адміністрування системи. В умовах більших підприємств складність структури системи не дозволяє адміністративному персоналу ефективно контролювати всю інфраструктуру та підтримувати в актуальному стані прийняті архітектурні рішення. [1]

Накопичувана складність структури AD зумовлює появу дефектів у зв’язках між об’єктами – складних для виявлення та найчастіше непрозорих для аналізу. Такі дефекти можуть проявлятись у непередбачених привілеях в певних суб’єктів, транзитивних контролях та неефективності прийнятих контролів доступу; в деяких випадках, в наслідок адміністративних помилок в базі AD можуть залишатись конфіденційні дані та тестові об’єкти. Усі ці особливості можуть бути використані потенційним зловмисником для здійснення підвищення привілеїв від менш привілейованих до найбільш привілейованих облікових записів не здійснюючи жодних дій, що не є запланованими з точки зору експлуатаційних характеристик MS AD. Такі особливості створюють істотні складнощі у виявленні таких атак та вчасному попередженню появи відповідних вразливостей. Саме тому, перманентний моніторинг архітектури середовища AD представляється необхідною умовою для виконання цих процесів.

Зважаючи на особливості ієрархічної структури MS AD найбільш сприятливою моделллю для представлення системи може слугувати

направлений граф, де кожна вершина представляє собою об’єкт чи суб’єкт в AD (користувач, комп’ютер, GPO, тощо), а ребра – зв’язки між ними. Таку можливість, зокрема, дозволяє здійснювати рішення Bloodhound, доступне на правах вільної ліцензії. Використання подбіних інструментів на постійній основі для напів-автоматизованого виявлення помилок в архітектурі – принаймні, деяких основних класів таких помилок – може розглядатися как потенційно ефективна компенсаційна міра проти окреслених вище проблем.

Висновок

Вбачається цілком перспетивним вектором подальших досліджень пошук технології ефективного виявлення складних архітектурних дефектів середовищ AD на основі наявних у вільному доступі рішень та технологій.

Список використаних джерел:

1. Active Directory Domain Services Overview [Електронний ресурс] / Microsoft – 2021. – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
2. Top 16 Active Directory Vulnerabilities [Електронний ресурс] / InfosecMatter – 2020. – Режим доступу до ресурсу: https://www.infosecmatter.com/top-16-active-directory-vulnerabilities/

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ НА БАЗІ FortiMail

Дяченко Максим Миколайович, БСДМ-62
Державний університет телекомунікацій,
м. Київ

Встановлено місце технології захисту корпоративної електронної пошти в системі забезпечення мережевої безпеки. Визначено характерні особливості технології FortiMail. Розроблено рекомендації щодо забезпечення безпеки корпоративної електронної пошти.

Сьогодні корпоративна електронна пошта для більшості компаній є основним засобом комунікації. Листування необхідне як для спілкування всередині самих підприємств та організацій, так і для обміну даними з партнерами, клієнтами, постачальниками, державними органами тощо.

Постійно спостерігається зростаюча тенденція до атак, які направлені на компрометацію ділової електронної пошти, коли зловмисник або захоплює, або ретельно імітує (підробляє) законний обліковий запис електронної пошти, щоб більш ефективно застосовувати соціальну інженерію в шахрайських діях та фінансових операціях. За оцінками фахівців, у 2020 році компрометація ділової електронної пошти була поширена у всіх галузях і розмірах бізнесу.

FortiMail забезпечує комплексний захист електронної пошти від загроз при кращій в галузі вартості і ефективності. Це рішення пропонує гнучкі варіанти розгортання і режими роботи для хмарних, локальних або гібридних середовищ електронної пошти, включаючи керовані рішення [1].

Засіб FortiMail 200F, який розглядається у даній роботі, призначений для підприємств малого бізнесу, відділень філій і організації. Він виконує наступні основні функції захисту корпоративної електронної пошти [2]:

захист від загроз. Потужний засіб захисту від спаму і шкідливих програм включає в себе такі передові технології як протидія поширенню вірусів, знешкодження та реконструкція контенту, аналіз за допомогою технології «пісочниця», захист від імперсонації та інші технології для запобігання небажаної масової розсилки, атаки з метою вимагання викупу, компрометації корпоративної електронної пошти і націлених атак;

захист даних. Передбачені надійні функції запобігання втрати даних, шифрування електронної пошти на основі ідентифікації та архівування, які сприяють запобіганню ненавмисної втрати конфіденційної інформації та дотримання корпоративних і галузевих правил;

інтеграція з Fortinet Security Fabric. Інтеграція з продуктами Fortinet, а також з компонентами сторонніх організацій забезпечує випереджувальний підхід замовника до безпеки за допомогою спільного використання індикаторів компрометації (IoC) з сумісним середовищем Fortinet Security Fabric. Він також забезпечує розширений і додатковий захист електронної пошти для середовищ Microsoft 365 за рахунок інтеграції на рівні API.

Рішення FortiMail об'єднує передові можливості для протидії загрозам, що передаються по електронній пошті, з якими стикаються організації сьогодні (рис. 1). Воно захищає від таких загроз: відомі загрози, передбачувані загрози, невідомі загрози, від спроб імперсонації та компрометації корпоративної електронної пошти [2].

Передовий захист електронної пошти має бути заснований на адаптивній системі, яка протидіє зростаючій складності загроз і розмаїття напрямків розвитку компаній. У складі адаптивної системи можна спільно використовувати індикатори компрометації та інші телеметричні дані для підвищення безпеки всієї інфраструктури безпеки. Також, інтенсивні і повторювані робочі процеси, в тому числі процеси реагування на інциденти, мають бути автоматизовані для зниження навантаження на фахівців з безпеки.

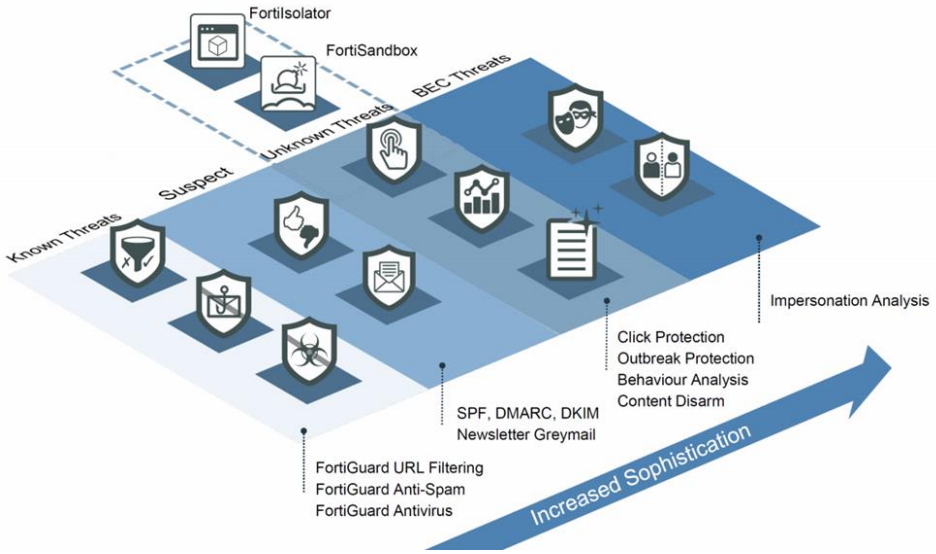


Рис. 1. Технології, які реалізовані в рішенні FortiMail [2]

При розгортанні та застосуванні рішення FortiMail необхідно обирати один із можливих варіантів: прозорий режим, режим шлюзу або режим сервера, який відповідає певним вимогам до безпеки електронної пошти, мінімізуючи зміни інфраструктури та переривання обслуговування. Безпеку поштового сервера слід враховувати на етапі планування на початку життєвого циклу розробки системи, щоб максимізувати безпеку і мінімізувати витрати.

Отже, безпека електронної пошти повинна бути головним пріоритетом для будь-якої компанії. Тому, першою лінією захисту повинен бути шлюз електронної пошти – платформа, яка захищає електронні листи від хакерів, спаму та вірусів. Необхідно захищати корпоративну електронну пошту, так як основний об’єм документів пересилається через неї. При цьому треба закупляти, розгортати та застосовувати сучасні методи та засоби захисту корпоративної електронної пошти.

Література

1. Email Security: FortiMail. Advanced, multi-layer protection against the full spectrum of email-borne threats. https://www.fortinet.com/products/email-security.

2. FortiMail. Data Sheet. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf.

УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Зеленко Євгеній Юрійович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

В доповіді представлено вибір рішення для компаній, які мають свою інформаційну систему та впроваджують привілейований доступ користувачів. Основним завданням такої системи забезпечити контроль та управління облікових записів співробітників IT-підрозділів, системних адміністраторів, співробітників аутсорсингових організацій, які займаються адмініструванням інфраструктурних компаній, управління аутентифікацією та авторизацією зазначених співробітників, аудиту, які здійснюють відповідні дії, контролю доступу та запису їх сесій.

Ключові слова: інформаційна система, привілейований доступ, облікові записи, сесія, моніторинг.

Система привілейованого доступу користувачів PAM призначені для виконання бізнес-завданнь, які направлені на підвищення ефективності роботи співробітників з привілегованими обліковими записами, виявлення нелояльного персоналу та запобіганню використанню конфіденційних даних [1].

Основні можливості PAM включають:

Виявлення привілейованих облікових записів в декількох системах, інфраструктурі і додатках;

Керування: ідентифікація привілейованих облікових записів;

Делегування доступу до привілейованих акаунтів;

Встановлення сеансу, управління, моніторинг і запис для інтерактивного привілейованого доступу;

Дослідники Gartner визначають управління привілейованим доступом як «основну технологію безпеки для захисту облікових записів, облікових даних і операцій, які пропонують підвищений («привілейований») рівень доступу [2]. Привілейований доступ, на відміну від звичайного доступу може вирішувати функції безпеки або обслуговування, змінювати конфігурацію системи або додатки або обходити встановлені заходи безпеки через доступ суперкористувача.

Основними функціями привілейованого доступу є виявлення привілейованих облікових записів в декількох системах, інфраструктурі і додатках, управління обліковими даними для привілейованих облікових записів, делегування доступу до привілейованих облікових записів і управління сеансами.

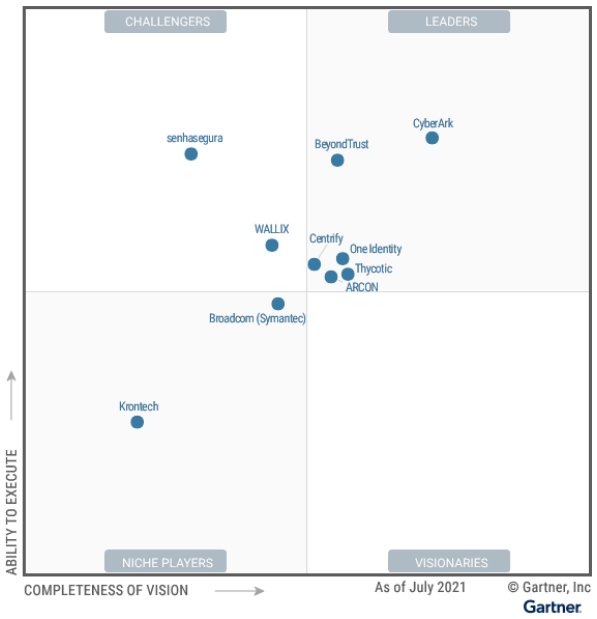


Рис.1 - Магічний квадрант управління привілейованим доступом

Як видно з рисунку One Identity, є лідером в цьому магічному квадраті. PASM-рішення One Identity Safeguard та складається з трьох модулів: Safeguard for Privileged Passwords, Safeguard for Privileged Sessions і Safeguard for Privileged Analytics. Рішення доступне в вигляді апаратного або програмного забезпечення або як SaaS [3].

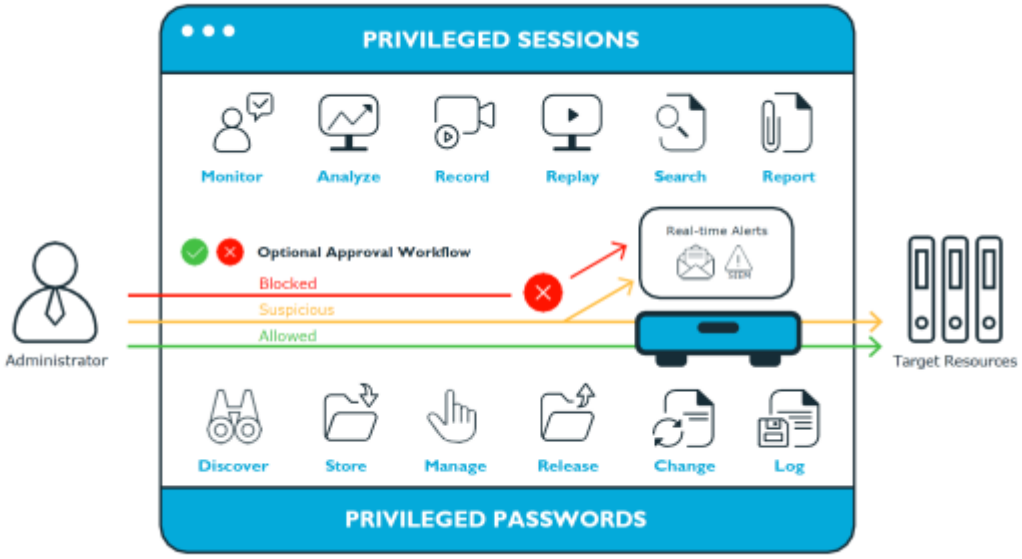


Рис.2 – Склад One Identity Safeguard PAM

До складу One Identity Safeguard наступні модули:

One Identity Safeguard for Privileged Passwords автоматизує, контролює і захищає процес надання привілейованих облікових даних з доступом на основі ролей управління та автоматизує робочі процеси.

One Identity for Privileged Sessions- це привілейоване рішення для управління сеансами, яке забезпечує провідний контроль доступу, а також моніторинг та запис сеансів для запобігання неправильного використання

привілейованих облікових записів, полегшення дотримання вимог та прискорення проведення розслідувань.

One Identity Safeguard for Privileged Analytics об'єднує дані з Safeguard для привілейованих сеансів для аналізу поведінки привілейованих користувачів. Safeguard for Privileged Analytics використовує алгоритми машинного навчання для перевірки поведінкових характеристик і формує профілі поведінки користувачів для кожного окремого привілейованого користувача. Safeguard for Privileged Analytics порівнює фактичну активність користувачів із профілями користувачів у режимі реального часу, а профілі постійно коригуються за допомогою машинного навчання. Використання привілейованої аналітики дозволяє виявляти аномалії та ранжирувати їх на основі ризику, щоб визначити пріоритети та вжити відповідних заходів щодо запобігання порушенню даних.

Однією з переваг One Identity Safeguard є те, що для привілейованих сеансів можна забезпечити повне розпізнавання тексту для захоплених графічних сеансів, дозволяючи аудиторам шукати артефакти, які відображаються на екранах під час активності, які інакше було б важко знайти.

Аналітика та аудит сеансів One Identity Safeguard для Privileged Analytics виділяється серед інших рішень тим, що використовує машинне навчання для аналізу не тільки спроб привілейованого доступу, але і всієї активності сеансу, включаючи команди. Пасивний поведінковий біометричний аналіз може виявляти несанкціоноване використання за допомогою динаміки натискання клавіш.

Тож на мій погляд дана технологія є викликом сьогодення для захисту та управління привілейованих користувачів інформаційної системи організацій, які повинні відповідати вимогам щодо захисту даних.

Перелік посилань:

1 Morey J. Haber, Darran Roll Identity Attack Vectors: Implementing an Effective Identity and Access. - 2020. 200p. Management Solution [Електронний ресурс] – Режим доступу: https://www.gartner.com/doc/reprints?id=1-26UE4193&ct=210719&st=sb]/

2. Звіт Gartner; Магічний квадрант управління привілейованим доступом [Електронний ресурс] – Режим доступу: https://www.gartner.com/doc/reprints?id=1-26UE4193&ct=210719&st=sb]/

3. One Identity Safeguard for Privileged Sessions 6.7.2. Quick Start Guide. – 2020. – 45p.

ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ DECEPTION ТЕХНОЛОГІЇ

Калиндрузь Богдан Миколайович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

Хакерські атаки часто базуються на соціальної інженерії. Зловмисники підробляють листи, групи в соціальних мережах, сторінки інтернет-магазинів і навіть цілі сайти. Їх мета - змусити жертву запустити на комп'ютері шкідливий файл або відправити свої аутентифікаційні дані. Попросту кажучи, вони обманюють людину. Технологія Deception бере на озброєнні цей же принцип - вона обманює самих хакерів. І робить це досить успішно. Аналітики Gartner помістили Deception в свій радар новітніх технологій безпеки, за їхньою оцінкою вона проста в розгортанні і при цьому ефективна для виявлення і усунення загроз в організаціях будь-яких розмірів.

Технологія Deception, або «технологія обману» (від англ. Deception technologies) - сукупність технік імітації IT-інфраструктури та дезінформації зловмисників, які використовуються з метою виявлення і уповільнення просування атак зловмисників і дозволяють в результаті зупиняти атаки до нанесення значного збитку.

Розвиток технологій обману атакуючих бере початок з 1990-х років - саме тоді з'явилися перші honeypot, призначені для залучення уваги зловмисника і його виявлення. Найчастіше honeypot є виділений сервер або сервіс на реальній системі, який реалізує різні протоколів та служб, наприклад HTTP, FTP і Telnet. Їх недоліком є складність адміністрування і технічного супроводу, до того ж помилкова конфігурація honeypot може привести до використання його зловмисником при проведенні атаки. Сучасні технології обману зловмисника еволюціонували і представлені в рішеннях нового класу - Distributed Deception Platform (DDP), або Deception Platform, або платформах для створення розподіленої інфраструктури помилкових цілей, для яких характерні автоматизація і легкість розгортання, централізоване управління, а також широкий арсенал пасток і приманок . За допомогою централізованої системи управління по мережі підприємства розміщуються пастки - емулюючі пристрої або пристрої під управлінням реальних операційних систем (Windows або Linux) з різними наборами сервісів. Так як у звичайних користувачів немає причин звертатися до цих пристроїв, будь-яка спроба взаємодії з ними буде вважатися зловмисною. Мета розміщення пасток полягає в тому, щоб привернути увагу зловмисника, відвернути його від реальних ресурсів підприємства і зайняти на деякий час, і при цьому зібрати інформацію про місцезнаходження атакуючого, його інструментах і методах атак - тобто все необхідне, щоб виявити і зупинити пропущену атаку .

Складність пасток варіюється від імітації простих мережевих сервісів, таких як SMB, RDP, SSH, HTTP (S), MySQL та інших, до імітації таких пристроїв, як комутатори, банкомати, POS-термінали, пристрої інтернету речей (IoT), медичне обладнання. А кількість пасток, розміщених в мережі підприємства, може досягати декількох тисяч. Таким чином, зловмисник неминуче зіткнеться з пастками при розвідці мережі або слідуючи за приманками. Принади (від англ. Lures), або «хлібні крихти» (від англ. Breadcrumbs) - це підроблені дані, які розміщуються на реальних пристроях

мережі, наприклад: облікові дані для підключення по RDP в диспетчері облікових даних Windows, по SSH - в історії команд , до веб-додатку - в файлах cookie і так далі. Іншим прикладом можуть служити неправдиві масиви даних, наприклад конфіденційні документи, бази даних, які зацікавлять зловмисників. Технології обману атакуючих найбільш ефективні на ранніх стадіях атаки, коли зловмисники збирають дані про інфраструктуру, аналізують їх і використовують для горизонтального просування по мережі. У той же час застосування технологій обману потенційно можливо на всіх етап атаки по моделі Cyber Kill Chain. Підроблений шар інфраструктури, що створюється з використанням пасток і приманок, дозволяє використовувати тактику зловмисників проти них. Найважливіша риса пасток і приманок - це, мабуть, їх реалістичність, адже якщо зловмисник зможе зрозуміти, що це обман, пастка не спрацює. І щоб домогтися нерозрізненості від реальних ресурсів, виробники рішень даного класу вдаються до передових методів: машинному навчанню, використанню штучного інтелекту і іншим. При цьому пастки і приманки зазвичай генеруються на основі аналізу мережі та є орієнтованими на специфіку організації, з урахуванням можливих векторів атак. В результаті інфраструктура організації починає складатися з двох шарів: реального і підробленого. Причому підроблений шар виглядає набагато більш привабливим і привабливим для зловмисника. Розгорнуті пастки і приманки «приймають удар на себе», захоплюють зловмисника в мережі фіктивної інфраструктури, тим самим виграючи час для прийняття контрзаходів, що призводить до збереження реальних активів. На додаток з'являється можливість спостерігати за діями зловмисника, аналізувати його інструменти та попереджати подібні атаки в майбутньому.

У той же час платформи для створення розподіленої інфраструктури помилкових цілей швидкі в розгортанні, що не навантажують роботою IT-підрозділу і не створюють шум для ІБ-підрозділу безліччю помилкових спрацьовувань.

Перелік посилань:

1. Machine Learning Algorithms for Network Intrusion Detection [Електронний ресурс]: Режим доступу https://link.springer.com/chapter/10.1007/978-3-319- 98842-9_6
2. An Intrusion Detection Model [Електронний ресурс]. – 1986. – Режим доступу до ресурсу: https://www.academia.edu/8674514/An_IntrusionDetection_Model.
3. A System for Detecting Network Intruders in Real-Time [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/paxson/paxson.pdf.

ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ВІРТУАЛЬНИХ ЗАХИЩЕННИХ ТУНЕЛЕЙ VPN ДЛЯ ОРГАНІЗАЦІЇ СТРИМІНГОВИХ ТЕХНОЛОГІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ

Клімов Антон Олегович, БСДМ – 62
Державний університет телекомунікацій
Навчально – науковий інститут Захисту інформації
м. Київ

Все частіше документообіг і передача корпоративної інформації відбувається в електронному вигляді в той чи інший спосіб. Для цього вже існує безліч протоколів і методів передачі даних. Корпоративна інформація, передана через відкриту мережу інтернет, легко може бути перехоплена за допомогою спеціальних програм-сніфферов – зловмисниками і використовуватись в корисливих цілях. Крім цього може бути перехоплені логіни і паролі від пошти або інших сервісів. Конфіденційність інформації, що передається виходить на перший план при створені корпоративної мережі. Захист інформації, що передається по каналам зв'язку, використовуючи паролювання документів або їх шифрування, не надає потрібного рівня безпеки, так як будь-який пароль може бути зламаний і це лише питання часу (все залежить від його складності), а за допомогою криптоаналіза, можна виявити і шифрування ключів.

У всьому, що стосується приватності, захисту та доступності в інтернеті, VPN просто немає рівних. Чим вище рівень розвитку інформаційних технологій та інтернету, тим вище попит на VPN, які вже стали невід'ємною частиною нашого життя і нашої безпеки. Однак важливо розуміти, що немає нічого ідеального, і VPN не виняток. Хоча ця технологія розвивалась довгі роки, деякі її аспекти ще далекі від досконалості. Недоліки для кожного користувача будуть свої, але зазвичай вони пов'язані з місцем розташування, інтернет-каналам і іншими факторами. Якщо ви читаєте важливі листи, переглядаєте соціальні мережі або транслюєте або завантажуєте відео та інший контент. VPN захистить вас від більшості загроз при використанні загальнодоступних і приватних мереж Wi-Fi.

Державні органи, інтернет провайдери та хакери, як правило, отримують інформацію шляхом її перехоплення, проте якщо вона зашифрована, вони не зможуть її прочитати, тому що не мають ключа шифрування.

У деяких VPN використовують алгоритми шифрування військового призначення, які надійно бережуть вашу інформацію, і ваші нерви. Залежно від того, в якій країні ви живете, деякі інтернет-контент може мати географічні обмеження, через які у вас не вийде його подивитись. Однак з VPN обійти географічні блокування дуже легко VPN-сервер просто підмінить ваш IP-адрес на свій, і блокування не спрацюють.

Саме по собі використання VPN не означає, що інтернет-загрози вам більше не страшні. Хоча VPN – це потужний інструмент, не варто вдаватися до помилкового почуття безпеки і забувати про обережність. Регулярно міняйте паролі, підвищуйте їх складність і будьте обережні, відкриваючи дивні повідомлення в пошті або відвідуючи небезпечні сайти.

Потокове передавання - це безперервна передача аудіо- чи відеофайлів із сервера на клієнта. Якщо говорити простіше, потокове передавання - це те, що відбувається, коли споживачі дивляться телевізор або слухають підкасти на підключених до Інтернету пристроях. Під час потокового передавання мультимедійний файл, що відтворюється на клієнтському пристрої, зберігається віддалено та передається через Інтернет кілька секунд за раз.

Потокове передавання відбувається в режимі реального часу, і це ефективніше, ніж завантаження медіафайлів. Якщо відеофайл завантажено, копія всього файлу зберігається на жорсткому диску пристрою, і відео не може відтворюватися, поки весь файл не закінчиться. Якщо воно передається потоково, браузер відтворює відео, фактично не копіюючи та не зберігаючи його. Відео завантажується потроху, замість того, щоб завантажуватись весь файл відразу, і інформація, яку завантажує браузер, не зберігається локально.

Список використаних джерел:

1. Соколов, А.В. Захист інформації в розподілених корпоративних мережах і системах / А.В. Соколов, В.Ф. Шаньгін – М.: ДМК Пресс, 2012. – 656с.
2. PrivateVPN [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wizcase.com/reviews/privatevpn

ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Коваль Владислав Романович, БСДМ – 62
Державний університет телекомунікацій
Навчально – науковий інститут Захисту інформації
м. Київ

Спочатку дамо визначення основному об’єкту дослідження роботи, а саме IoT або ж інтернету речей. У самому широкому сенсі термін IoT охоплює все, що пов'язане з Інтернетом, але він все частіше використовується для визначення об'єктів, які «говорять» один з одним. Просто, Інтернет речей складається з пристроїв - від простих датчиків до смартфонів і носіїв - з'єднаних разом. Об'єднуючи ці підключені пристрої з автоматизованими системами, можна "збирати інформацію, аналізувати її і створювати дії", щоб допомогти людині з певним завданням або дізнатися з процесу. Іншими словами, Інтернет Речей - це концепція підключення будь-якого пристрою (до тих пір, поки він має вимикач вкл / викл) до Інтернету та інших підключених пристроїв. IoT - це гігантська мережа пов'язаних речей і людей, які збирають і обмінюються даними про те, як вони використовуються, і про навколишнє середовище.

Серед головних переваг інтернету речей:

1. Безпека, комфорт, ефективність

Серед IoT рішень багато таких, що забезпечують набагато більший рівень комфорту (контрольовані кавоварки, пральні машинки і т.п.), безпеки (wi-fi камери, дистанційні сигналізації та різного роду детектори), а також засоби для збільшення ефективності праці.

2. Краще прийняття рішень

Якщо ми можемо аналізувати більше тенденцій з емпіричних даних, то ми можемо приймати розумніші рішення. IoT надає доступність даних у кожному аспекті вашого бізнесу.

3. Генерація доходів

По-перше, перераховані вище переваги вплинуть на нижній прибуток підприємств, що будуть використовувати IoT, зменшуючи витрати. IoT також допоможе підвищити ефективність. Але, лише питання часу, перш ніж аналіз даних IoT допоможе вам реалізувати нові бізнес-функції. Також це призведе до нових можливостей отримання доходу. IoT може бути спеціальним «фактором X». Його унікальність надає багатьом організаціям стратегічну перевагу над конкурентами. Ця перевага буде корисною для компаній і в наступному десятилітті

Але при всих перевагах інтернету речей йому присутні деякі проблеми, а саме:

1. Атаки на хмарні середовища

Враховуючи, що велика кількість даних, які будуть запускатися в IoT, зберігатиметься в хмарі, ймовірно, що провайдери хмари стануть однією з головних цілей у цій війні.

2. Проблеми з ботнетом

Мільйони нових підключених споживчих пристроїв створюють широку атакуючу поверхню для хакерів, які продовжуватимуть досліджувати зв'язки між малопотужними, дещо немічними пристроями та критичною інфраструктурою. Найбільшою проблемою безпеки, яку він бачить, є створення атак DDoS з розподіленим руйнуванням, які використовують рої погано захищених споживчих пристроїв для атаки громадської інфраструктури через масу скоординованого зловживання каналами зв'язку.

Бот-мережі IoT можуть направляти величезні рої підключених датчиків, таких як термостати або контролери дощувальних пристроїв, щоб викликати шкідливі та непередбачувані спади в інфраструктурному використанні, що призводить до таких подій, як стрибки напруги, руйнівні атаки або зменшення доступності критичної інфраструктури на рівні міста чи штату.

3. Відсутність довіри

Компанія Gemalto, розташована в Амстердамі, в Нідерландах, є фірмою з кібербезпеки, яка дослідила вплив безпеки на розвиток IoT. Якщо встановлено, що 90 відсотків споживачів не мають впевненості в безпеці пристроїв IoT. Це призводить до того, що більше двох третин споживачів і майже 80% організацій підтримують уряди, які беруть участь у забезпеченні безпеки IoT. Фактично його нещодавній звіт про стан безпеки IoT, опублікований наприкінці жовтня, показав наступні дані.

a) 96 відсотків підприємств і 90 відсотків споживачів вважають, що повинні існувати правила безпеки ІН

b) 54% споживачів володіють у середньому чотирма пристроями IoT, але лише 14% вважають, що вони знають про безпеку пристроїв IoT

c) 65 відсотків споживачів стурбовані тим, що хакер контролює їх

пристрій IoT, а 60 відсотків стурбовані тим, що дані витікають

Зрозуміло, що і споживачі, і підприємства мають серйозні побоювання щодо безпеки IoT і мало впевненості в тому, що постачальники послуг IoT і виробники пристроїв зможуть захистити пристрої IoT і, що більш важливо, цілісність даних, створених, збережених і переданих цими пристроями

4. Розуміння IoT

У 2019 році справжня проблема полягає в тому, як підвищити здатність

людей чіткіше зрозуміти зміни та їхні наслідки, а також зробити конкретні дії, щоб скористатися потенційним потенціалом.

Інтернет речей переходить у підлітковий вік, оскільки підключені пристрої стають розумнішими та більш захоплюючими, а також очікуванням перетворення даних IoT на розуміння та збільшення фінансової вартості. Крім того, алгоритми та шаблони візуалізації даних розвивалися таким чином, щоб нові випадки використання могли скористатися перевагами попередніх. Експоненціальне прийняття IoT призведе до зниження витрат на датчик і придбання, що дозволить все більше і більше життєздатних бізнес-кейсів, які раніше були занадто дорогими.

Висновки: Це підкреслює важливість автентифікації IoT - якщо ви не впевнені, з яким об'єктом ви обмінюєтеся повідомленнями, то не можете захистити потенційно конфіденційні дані, а також транзакції, що проводяться.

Література:

1. https://developer.ibm.com/articles/iot-top-10-iot-security-challenges/
2. https://internetofthingswiki.com/biggest-security-issues-iot-devices-face/1344/

ТЕХНОЛОГІЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ ПЛАТФОРМИ ESET PROTECT

Красноштан Іван Вікторович, БСДМ-62
Державний університет телекомунікацій,
Навчально-науковий інститут Захисту інформації
м. Київ

На сьогоднішній день, до Інтернету під'єднано більше пристроїв, ніж будь-коли раніше. Саме це слугує зловмисникам полем для реалізації їх ідей, оскільки вони добре використовують такі пристрої, як принтери та камери, які ніколи не розроблялись для запобігання складним вторгненням. Змога підприємства швидко реагувати на інцидент може зменшити втрати, відновити процеси та послуги, та зменшити рівень небезпеки реалізованих вразливостей. Реагування на інциденти забезпечує першу лінію захисту від інцидентів безпеки, а в довгостроковій перспективі допомагає встановити низку кращих практик для запобігання порушень, ще до їх виникнення. Все ці фактори змушують компанії та приватних осіб переосмислити поняття про безпеку своїх мереж.

Корпоративні інформаційні системи щороку стають все складнішими в своїй структурі та важливішими, в якості корпоративної інфраструктури. Вміщуючи все більше даних та стаючи цінним активом організацій, інформаційні системи стають ласим шматком для зловмисників, які також вдосконалюються в способах проникнення в захищені системи. Через природу все більшого масштабування та цінності, захист таких систем стає все складнішим, як в наслідок підвищеної цікавості до викрадення даних з боку порушників, так і з точки зору відсутності достатнього штабу спеціалістів та сучасного програмного забезпечення в активі компаній. Зіткнувшись із реальною загрозою інформаційної безпеки, мало організацій знають, які кроки слід вжити першими, щоб впоратися з інцидентом і мінімізувати його вплив на бізнес. Наявність добре продуманого плану реагування в сфері кібербезпеки (IRP) стала надважливим способом повної підготовки до вирішення подібних ситуацій.

Процес захисту підприємства в кіберпросторі вимагає проведення великої кількості дій та надзвичайної пильності від спеціалістів. Розумним рішенням буде використання програмних комплексів для полегшення та одночасного покращення як процесу, так і результатів діяльності команди реагування на інциденти. Одним з передових рішень сьогодення є розробка від компанії Eset, платформа «Eset Protect», яка представляє з себе комплексну систему захисту кінцевих точок в формі хмарного рішення в межах корпоративної системи [1]. Зазвичай, компанії схильні обирати якомога меншу кількість постачальників продуктів для захисту їх інформаційного простору, економлячи таким чином кошти, співпрацюючи з одним-двома вендорами, замість трьох і більше. В цьому є досить розумна логіка, але необхідно розуміти, що при економії не можна втрачати у якості програмного забезпечення. З цієї причини можна вважати рішення від Eset доволі збалансованим, так як один постачальник надає доступ до широкого спектру інструментів у своєму продукті, які відповідають циклу технології реагування на кіберінциденти. В свою чергу, технологія реагування

складається з таких складових частин: етапу підготовки до можливих загроз, виявлення та аналізу інцидентів, обмеження рівня шкоди, ліквідації та відновлення після інциденту, а також етапу розслідування та оптимізації програмного комплексу на базі отриманого досвіду.

Платформа Eset Protect використовує власні розробки для протидії порушенням цілісності системи, в якій вона впроваджена. До таких рішень відносяться: ESET Endpoint Security, що спеціалізується на безперервному моніторингу точок на рахунок останніх відомих загроз, а також блокуванню та захисту системи від атак та втручань; ESET Dynamic Threat Defense, що аналізує атаки та відтворює їх в ізольованому хмарному середовищі для оцінки поведінки; ESET Full Disk Encryption, яка дозволяє розгортання та шифрування даних одним натисканням кнопки на підключених в системі кінцевих точках Windows та Mac. Платформа пропонує розгорнуті звітності про інциденти безпеки та загальну продуктивність встановлених рішень у мережі організаціях [2].

Інтегруючи в свою корпоративну систему платформу Eset Protect, організації впроваджують провідне рішення з управління загрозами на ринку, яке охоплює виявлення, розслідування та виправлення загроз у широкому колі кіберінцидентів, база яких постійно оновлюється.

Таким чином, за допомогою одного рішення можна, досить швидко, розгорнути комплексну систему реагування на інциденти, що охоплює всі кроки захисту корпоративної мережі від несанкціонованого втручання та вести контроль за станом системи в зручний спосіб: в головному відділенні компанії, або використовуючи аутсорсинг-послуги, оскільки рішення використовується як хмарне.

Зрештою, ставлячись відповідально до питань кібербезпеки та реалізації технології реагування на інциденти на базі комплексних рішень, можна забезпечити ефективний захист активів організації, а також належний рівень безпеки корпоративної інформаційної системи у зручний та вигідний спосіб.

Список використаних джерел:

1. ESET PROTECT Enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://www.eset.com/int/business/enterprise-protection-bundle/#protect-data.

2. ESET PROTECT Advanced Reviews & Product Details [Електронний ресурс] – Режим доступу до ресурсу: https://www.g2.com/products/eset-protect-advanced/reviews.

ТИПОВИЙ СЦЕНАРІЙ РЕАГУВАННЯ НА ІНЦИДЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Лібега Лілія Андріївна, БСДМ-62
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
М. Київ

Security Operations Center (SOC) дослівно оперативний центр безпеки, в практичній діяльності отримав назву центр моніторингу та реагування на інциденти інформаційної безпеки. Основною метою його діяльності є виявлення і реагування на інциденти інформаційної безпеки. Розглянемо, типовий сценарій реагування на інцидент інформаційної безпеки.

Процес реагування на інциденти проходить в кілька етапів. Перший і початковий етап передбачає створення та підготовку команди реагування на інциденти, а також отримання необхідних інструментів та ресурсів. Під час підготовки організація також намагається обмежити кількість інцидентів, що відбуватимуться, вибравши та впровадивши набір функцій контролю та попередження на основі результатів оцінки ризиків. Проте завжди є залишковий ризик, який неминуче залишатиметься після впровадження контролю. Таким чином, своєчасне виявлення та сповіщення про будь-які порушення безпеки є невід'ємною складовою процесу реагування. Адже, відповідно до серйозності інциденту, організація може пом'якшити його наслідки, усунувши порушення і зрештою відновлюючи систему. Під час цієї фази активність часто повертається до етапу виявлення та аналізу - наприклад, щоб дізнатися, чи були заражені додаткові хости шкідливими програмами під час викорінення інциденту зловмисного програмного забезпечення.

При прийнятті від користувачів та систем сповіщень чи повідомлень про події ІБ, необхідна їх реєстрація. Надалі потрібно визначити чи є подія інцидентом інформаційної безпеки. У разі наявності ознак належності події до інцидентів ІБ проводиться попередній аналіз, збір та уточнення інформації про подію, визначається класифікація інцидентів за рівнем критичності до якого відноситься подія. Останнім кроком реагування є фіксація результатів реагування на інциденти ІБ, їх закриття в системі реагування та інформування ініціаторів повідомлень про закриття інцидентів.

Після того, як інцидент буде повністю оброблений, організація видає звіт, який детально описує причину виникнення, вартість збитків, які завдав інцидент та кроки, які організація повинна вжити для запобігання майбутніх інцидентів.

Отже, основними завданнями етапу розслідування інциденту інформаційної безпеки є:

- точно діагностувати інцидент;

- локалізація та мінімізація наслідків та втрат;
- виявлення основних причин виникнення інциденту
- збір доказів інциденту;
- відновлення скомпрометованих інформаційних систем;
- вдосконалення систем безпеки;
- впровадження заходів захисту для унеможливлення таких інцидентів у майбутньому.

Список використаних джерел:

1. Реагування на інциденти: що вам повинен SOC [Електронний ресурс] – Режим доступу : https://www.anti-malware.ru/analytics/Technology_Analysis/Correct-SOC-Incident-Response
2. Analyst's Notebook data. IBM Knowledge Center [Електронний ресурс] – Режим доступу : https://www.ibm.com/support/knowledgecenter/SSXVXZ_2.3.1/com.ibm.i2.landing.doc/eia_welcome.html

ПРИВІЛЕЙОВАНИЙ ДОСТУП. ЧОМУ ЦЕ ВАЖЛИВО І ЯК ЙОГО КОНТРОЛЮВАТИ

Нечипуренко Ксенія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

Досить очевидно, що привілейовані облікові записи (Privileged Access) та дані забезпечують безперешкодний доступ до критично важливої локальної та хмарної інфраструктури, і додатків. За даними опитування Cyber-Privileged Account Security & Compliance Survey, близько 30% компаній, з кількістю співробітників понад 1000 чоловік не змогли дати відповідь на питання: «Скільки PA використовується у Вашій компанії?». Другою за популярністю була відповідь − від 1 до 250.

PA існує в багатьох формах в корпоративному середовищі (наприклад, локальні адміністративні облікові записи, адміністративні облікові записи домену, облікові записи служб, облікові дані додатків, ключі SSH, сервісні облікові записи з різним рівнем дозволів, облікові записи адміністраторів в соціальних мережах). PA, облікові дані і секрети знаходяться в пристроях, додатках і операційних системах. Вони дозволяють організаціям захищати інфраструктуру і додатки, ефективно вести бізнес і підтримувати конфіденційність критичних даних.

Відповідно, ризики, які можуть виникнути в зв'язку з цим це:

- Спільне використання облікових записів;
- Надмірні привілеї;
- Неконтрольований доступ;
- Не регулярна зміна паролів;
- Неактивні аккаунти.

В чужих руках PA можуть бути використані, щоб нанести катастрофічну шкоду бізнесу. Ось чому вони повинні бути захищені, управлятися і контролюватися.

Привілейовані облікові записи, облікові дані і секрети є скрізь. І зловмисники переслідують їх.

На практиці для контролю використання привілейованих доступу використовуються рішення класу Privileged accounts management (PAM).

Організаційно та функціонально, з їх допомогою, завдання розбивається на кілька складових, а саме:

- Пошук і аудит стану PA;

- Управління життєвим циклом привілейованих облікових даних (створення\ заміна\ деактивація, безпечне зберігання, контроль доступу до облікового запису, регулярна звітність);
- Контроль сесій з використанням РА (ізоляція сесій, їх моніторинг, журналювання команд, відеофіксація дій);
- Аналітика використання РА і поведінковий аналіз для оперативного виявлення підозрілої активності зловмисників.

Підсумовуючи, можна констатувати, що управління та контроль використання РА повинні займати одне з найважливіших місць в процесі забезпечення інформаційної безпеки компанії. Втрата контролю над РА дає зловмисникам (як зовнішнім, так і внутрішнім) ключі до критично важливих ресурсів IT-інфраструктури. Також безперервність захисту РА допомагає знизити ризик витоку даних і відповідати нормативним вимогам.

Список використаних джерел:

1. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту.Управління ризиками інформаційної безпеки.
Привілейований доступ [Електронний ресурс] // KO. – 2019. – Режим доступу до ресурсу: https://ko.com.ua/privilejovanij_dostup_chomu_ce_vazhlivo_i_yak_jogo_kontrolyuvati_129976.

ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ OPEN VPN

Нощенко Станіслав Андрійович
Державний університет телекомунікацій,
Навчально-науковий інститут Захисту інформації
м. Київ

В наш час зростає попит на підключення до внутрішніх мереж з віддалених місць. Працівники часто потребують підключення до внутрішніх приватних мереж через Інтернет (що з самого початку небезпечно) з дому, готелів, аеропортів або з інших зовнішніх мереж. Безпека стає головним фактором, коли співробітники чи ділові партнери мають постійний доступ до внутрішніх мереж із незахищених зовнішніх місць.

Технологія віртуальних приватних мереж - VPN (Virtual Private Network) забезпечує спосіб захисту інформації, що передається через Інтернет, дозволяючи користувачам створити віртуальний приватний «тунель» для безпечного входу у внутрішню мережу, надає доступ до ресурсів, даних та комунікацій через незахищену мережу, таку як Інтернет.

OpenVPN - вільно поширювана програма для створення віртуальних приватних мереж. ПЗ OpenVPN передає дані мережею за допомогою протоколів UDP або TCP із застосуванням драйвера TUN / TAP. Протокол UDP і драйвер TUN дозволяє підключатися до сервера OpenVPN клієнтам, розташованим за NAT (від англ. Network Address Translation - перетворення мережних адрес) – це механізм зміни мережної адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший.

Для OpenVPN можна вибрати довільний порт, що дозволяє долати обмеження брандмауера, через який здійснюється доступ з локальної мережі в Інтернет (якщо такі обмеження встановлені). Безпека і шифрування в OpenVPN забезпечується бібліотекою OpenSSL і протоколом транспортного рівня Transport Layer Security (TLS). Замість OpenSSL в нових версіях OpenVPN можна використовувати бібліотеку PolarSSL. Протокол TLS – це засіб оптимізації протоколу захищеної передачі даних рівня захищених сокетів Secure Socket Layers (SSL). В OpenSSL може використовуватися симетрична та асиметрична криптографія.

Основними перевагами OpenVPN можна підкреслити:

- підтримка різноманітних операційних систем (Linux, FreeBSD, Windows, Solaris, Mac OS X, NetBSD);
- Робота за довільними TCP / UDP портами, а також через HTTP проксі-сервер. Доцільно використовувати, якщо існують обмеження по

протоколу і портам, але також це вносить невелику кількість надлишкової інформації за рахунок заголовків TCP або UDP.

- Підтримка різних режимів захисту каналу зв'язку, а також алгоритму шифрування. У режимі точка-точка шифрування може відключатися.

Що стосується налаштування безпосередньо самого з'єднання, то із з'єднанням точка-точка ніяких проблем не виникає, а щодо з'єднання сервер-клієнт, то викликає кілька проблем. Основна і мабуть найважливіша проблема, це питання безпеки і шифрування даних. Оскільки в цьому режимі необхідно замість ключів для аутентифікації і шифрування використовувати сертифікати.

Зазвичай центрами сертифікації є компанії, що підписують сертифікати і відповідають за правильність представленої в сертифікаті інформації. При роботі з сертифікатами використовуються алгоритми асиметричного шифрування, на яких і грунтується метод електронного цифрового підпису - ЕЦП; він дозволяє встановити відсутність спотворення інформації в електронному документі з моменту формування ЕЦП і перевірити приналежність підпису власникові сертифіката ключа ЕЦП.

Для створення власного центру сертифікації, можна скористатися пакетом OpenSSL. OpenSSL - це криптографічна бібліотека, яка реалізує два протоколи: Secure Sockets Layer і Transport Layer Security. Дана бібліотека має інструменти, призначені для генерації приватних ключів RSA і Certificate Signing Requests (CSR-запитів), управління сертифікатами та виконання кодування/декодування.

Література:

1. Доповідь «Побудова віртуальних приватних мереж на основі обладнання фірми Cisco», Конференція «Проблеми Телекомунікацій», 2020. – 3 с. – Волік Д.В., Григоренко О. В;
2. Feilner, Markus OpenVPN: Building and Integrating Virtual Private Networks/ Markus Feilner – Packt Publishing, 2006;
3. Graf, Norbert Beginning OpenVPN 2.0.9/ Norbert Graf – Packt Publishing, 2009;
4. OpenSSL – опис криптографічного пакету з відкритим кодом: [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/OpenSSL.

ПОРІВНЯННЯ ШЛЯХІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Рєзнік Роман Вікторович, БСДМ-62
Державний університет
телекомунікацій,
м. Київ

На сьогоднішній день компанії дуже рідко замислюються про безпеку своєї інформації в мережі і зовсім не приділяють цьому питанню уваги, часто починаючи вживати заходів лише після витоку або втрати важливої інформації.

Щоб забезпечити або ж усунути існуючу проблему, пов'язану із захистом інформації, застереження від атак зловмисників корпоративного сайту, його бази даних або всередині мережі додатків, компаніям варто розглядати рішення для діагностики вразливостей і моніторингу комп'ютерів в мережі, спеціальні сканери - програмні або апаратні засоби, скануючі систему на предмет виявлення можливих проблем в безпеці, що дозволяють виявляти, оцінювати і усувати вразливості в мережі..

Сканери уразливості діляться на дві основні групи:

1. Сканери корпоративних мереж, призначення яких полягає в аналізі мережі на наявність відкритих портів, а також вразливостей в операційних системах і додатках.

2. Сканери уразливості веб-додатків. На даний момент їхня популярність зростає в силу того, що більшість комерційних організацій і банків використовують у своїй діяльності інтернет ресурси, захист яких стає важливим фактором. У цій роботі буде розглянуто більше інформації саме по цій групі.

Пропоновані продукти мають всі можливості і засоби для ефективного виявлення і управління виправленнями вразливостей, які створені після аналізу та фільтрації результатів [1].

Функціонувати такі засоби можуть на мережевому рівні (network-based), рівні операційної системи (host-based) і рівні додатку (application-based). Найбільшого поширення набули засоби аналізу захищеності мережевих сервісів і протоколів.

Крім виявлення вразливостей, за допомогою засобів аналізу захищеності можна швидко визначити всі вузли корпоративної мережі, доступні в момент проведення тестування, виявити всі використовувані в ній сервіси та протоколи, їх налаштування і можливості для несанкціонованого впливу (як зсередини корпоративної мережі, так і зовні). Також ці засоби виробляють рекомендації і покрокові заходи, що дозволяють усунути виявлені недоліки [1].

Оскільки найбільшого поширення набули засоби, що функціонують на рівні мережі то основна увага приділяється саме їм.

Існує два основних механізми, за допомогою яких сканер перевіряє наявність уразливості - сканування (scan) і зондування (probe).

Сканування - механізм пасивного аналізу, за допомогою якого сканер намагається визначити наявність уразливості без фактичного підтвердження

її наявності - за непрямими ознаками. Цей метод є найбільш швидким і простим для реалізації.

Зондування - механізм активного аналізу, який дозволяє переконатися, присутня чи ні на уже згадуваному вузлі вразливість. Зондування виконується шляхом імітації атаки, що використовує вразливість яка перевіряється. Цей метод більш повільний, ніж "сканування", але майже завжди набагато більш точний [2].

Практично будь-який сканер проводить аналіз захищеності в кілька етапів:

1. Збір інформації про мережу.
2. Виявлення потенційних вразливостей.
3. Підтвердження обраних вразливостей. Генерація звітів.
4. Автоматичне усунення вразливостей. Цей етап дуже рідко реалізується в мережевих сканерах, але широко застосовується в системних сканерах.

Отже, для превентивного захисту від помилок програмування, недоліків, допущених при проектуванні системи, ненадійних паролів, вірусів та інших шкідливих програм, скриптових і SQL-ін'єкцій є безліч варіантів продуктів на ринку, які мають різні засоби досягнення бажаного результату.

Список використаних джерел:

1.Інтернет-джерело: http://bug.kpi.ua/web/index.php?r=site%2Farticle&id=37

2. Інтернет-джерело: https://maccase.ru/uk/android/upravlenie-uyazvimostyam i-intellektualnoe-skanirovanie.html.

ТЕХНОЛОГІЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ВЕБ-ДОДАТКУ СУЧАСНОГО ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ BURP SUITE

Смолєв Євген Сергійович, БСДМ-52
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Сучасний бізнес використовує останні технологічні досягнення, щоб перенести більшість своїх операцій в Інтернет. Віддалена робота є більш поширеною, ніж будь-коли раніше, і компанії, розділені великими відстанями, можуть миттєво ділитися конфіденційними даними. Але ці переваги також пов'язані з ризиками. Веб-додатки вразливі до різноманітних кіберзагроз, і багато організацій не мають стратегій або технологій, необхідних для протидії їм.

Веб-додаток – це комп’ютерна програма, яка використовує веб-браузери та веб-технології для виконання завдань через Інтернет.

Веб-додатки використовують комбінацію сценаріїв на стороні сервера (PHP та ASP) для обробки та зберігання інформації, а також сценарії на стороні клієнта (JavaScript та HTML) для подання інформації користувачам. Це дозволяє користувачам взаємодіяти з компанією, використовуючи онлайн-форми, системи управління контентом тощо. Крім того, додатки дозволяють працівникам створювати документи, обмінюватися інформацією, співпрацювати над проектами та працювати над загальними документами незалежно від місця розташування та пристрою [1].

OWASP Топ-10 — є визнаною світовою методологією оцінки вразливостей веб-додатків у всьому світі і відображає сучасні тренди безпеки веб-додатків, є першим кроком організації до створення культури більш безпечного коду програмного забезпечення.

На даний момент найактуальнішим документом є «OWASP Top 10 2021». Top 10 2021 був заснований, в основному, на матеріалах, наданих компаніями, які спеціалізуються на безпеці додатків, і на дослідженні більш ніж 500 незалежних галузевих опитувань. Ці дані охоплюють уразливі місця, отримані від сотень різних організацій і більше 100 000 реальних додатків та API. В основі списку Top 10 лежать дані про поширеність, простоту експлуатації, а також про складність виявлення вразливостей і про можливості заподіяння шкоди.

Топ-10 актуальних вразливостей від OWASP у 2021 році включає: Injection, Injection flaws, SQL, NoSQL, OS, LDAP, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting XSS, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging & Monitoring [2].

Управління вразливістю – це процес виявлення, оцінки, знешкодження та звітності про вразливості безпеки в системах та програмному забезпеченні, яке в них працює. Це реалізується разом з іншими тактиками безпеки та є життєво важливим для організацій, щоб визначити пріоритети можливих загроз та мінімізувати їх поверхню атаки.

Вразливі місця безпеки у свою чергу, посилаються на технологічні недоліки, які дозволяють зловмисникам компрометувати продукт та інформацію, яку він

містить. Саме тому процес управління потрібно виконувати безперервно, щоб не відставати від нових систем, що додаються до мереж, змін, що вносяться до систем, та виявляти з часом нові вразливості [3].

Програмне забезпечення для управління вразливостями може допомогти автоматизувати цей процес. Воно може використовувати сканери вразливостей, а іноді і агентів кінцевих точок, щоб інвентаризувати різноманітні системи в мережі та знаходити в них уразливості. Після виявлення вразливих місць, ризик, який вони становлять, необхідно оцінювати в різних контекстах, щоб можна було приймати рішення про те, як найкраще з ними поводитися. Наприклад, перевірка вразливості може бути ефективним способом визначення контексту та реальної тяжкості вразливості. Одним з таких рішень, що може забезпечити управління вразливостями сучасного підприємства є Burp Suite від компанії PortSwigger.

Burp Suite – це інтегрована платформа, призначена для проведення аудиту веб-додатків, як в ручному, так і в автоматичних режимах. Містить інтуїтивно зрозумілий інтерфейс із спеціально спроектованими розділами, що дозволяють поліпшити і прискорити процес тестування. Сам інструмент вдає із себе проксі сервер, що перехоплює і обробляє всі запити від браузера.

Різні інструменти бездоганно працюють разом, щоб підтримувати весь процес тестування, починаючи від початкового аналізу середовища, до пошуку та використання вразливостей безпеки.

PortSwigger – світовий лідер у створенні програмних засобів для тестування безпеки веб-додатків. Програмне забезпечення Burp Suite добре зарекомендувало себе як фактичний стандартний набір інструментів, що використовується професіоналами веб-безпеки. Burp Suite використовують понад 47 000 осіб у 12 500 організаціях у більш ніж 140 країнах.

Burp Suite Professional – це вдосконалений набір інструментів для пошуку та використання вразливих місць у веб-додатках. Пакет Burp Suite можна використовувати для тестування та звітування про велику кількість вразливостей, включаючи SQLi, XSS та весь перелік OWASP Top 10 [4].

Список використаних джерел:

1. *Інтернет-джерело:* https://blog.stackpath.com/web-application.
2. *Інтернет-джерело:* https://owasp.org/Top10.
3. *Інтернет-джерело:*https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning.
4. *Інтернет-джерело:* https://portswigger.net/burp.

ВИКОРИСТАННЯ BLOCKCHAIN ДЛЯ IOT

Сокол Антон Васильович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Сьогодні дуже стрімко розвивається сфера Інтернету Речей, підключення якої досягнуть мільярдів уже незабаром. Основна проблема полягає в тому, що зростання IoT прямо пропорційно збільшує незахищеність даних. Підключення Інтернету Речей створюють серйозні проблеми: потреба забезпечення мільярдів взаємодій між різними машинами та потреба захисту приватної інформації, яка передається через пристрої. Як результат, усе це потребує неймовірних коштів на обслуговування та розвиток. Децентралізоване управління на основі блокчейн дозволяє забезпечити більш масштабовану безпеку IoT та забезпечує прозору перевірку і захист від втручання.

Blockchain дозволяє використовувати безпечні однорангові мережеві вузли, які працюють одночасно і можуть бути представлені через одиничні вбудовані сенсори IoT з можливістю перевірки кожного блоку в мережі блокчейн.

В сфері Інтернету Речей blockchain може застосовуватися для збереження інформації сенсорів, забезпечення безпеки шляхом ідентифікації окремого IoT пристрою та його захисту від злому, спрощення налаштування мережі та здійснення оплати за послуги.

По-перше, blockchain – це та технологія, яка забезпечує безпеку. У контексті Інтернету Речей, де безпека є дуже головним аспектом – ця технологія дуже перспективна.

По-друге, масштабованість – блокчейн-мережі можуть впоратися з дуже великими об’ємами даних. За допомогою цієї технології можливо значно швидше отримувати та передавати інформацію, що дуже важливо у сучасному світі.

По-третє, необхідно розподілити права та обов’язки користувачів та виробників. Наприклад, якщо пристрій, встановлений пацієнту, завдає шкоди пацієнту, то хто в цьому випадку має понести покарання.

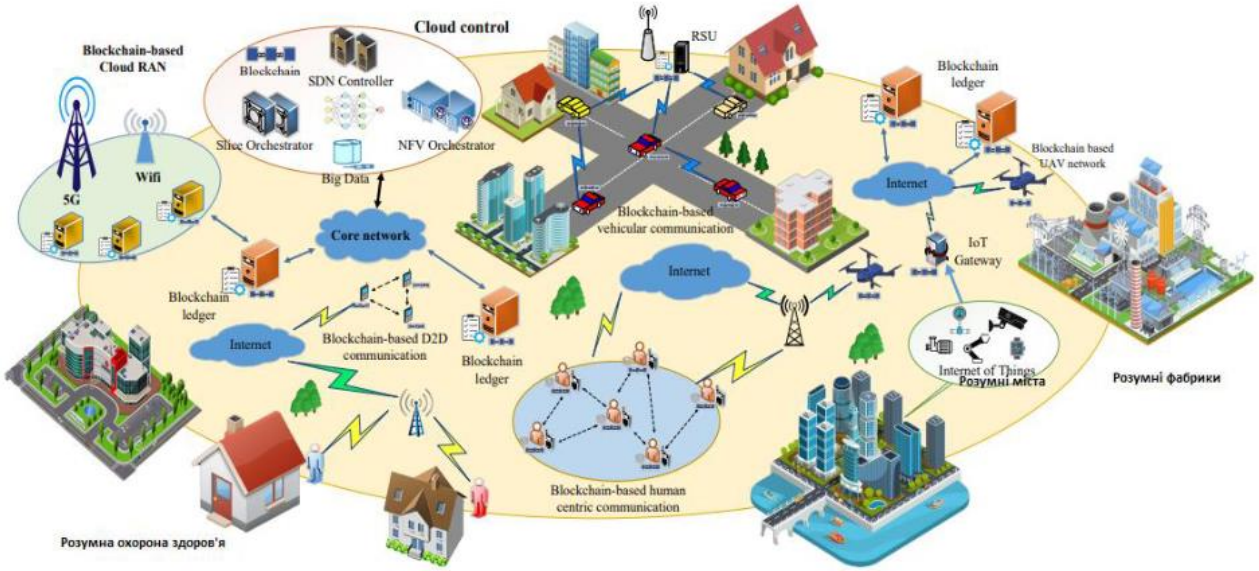


Рис.1 Співіснування IoT та blockchain

Технологія blockchain може забезпечити просту інфраструктуру для двох пристроїв, щоб безпосередньо передавати дані між собою, чи передавати кошти за допомогою захищеного та надійного контрактного сеансу зв'язку. Для обміну використовуються уже відомі смарт-контракти, які моделюють угоду між двома сторонами.

Переваги використання тандему IoT-blockchain:

1) Відстежування активів в режимі реального часу під час переміщення по багаточисельному ланцюгу

2) Проста перевірка дотримання договорів

3) Незмінюваність записів, що дозволяє уникнути зайвих суперечок

4) Надійність збереження даних, які обробляються і записуються за певними галузевими стандартами з дотриманням законодавств.

Список використаних джерел

1. The History of Blockchain Technology [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://101blockchains.com/history-of-blockchain- timeline/
2. J. Golosova, A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology", Riga, 2018
3. SCTelecom. IRBIS Network Decentralized telecommunications network [Електронний ресурс]. – 2019. - Режим доступу до ресурсу: https://safecalls.io/ieo/docs/SCTelecomWPv1.2.pdf

ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ

Шпуй Валентин Іванович
студент групи БСДМ-62, ННІЗІ ДУТ, Київ, Україна

Обсяг кінцевих пристроїв, включаючи мобільні, в мережах підприємств за останні десятиліття зріс в рази. За звітом Symantec, щодня в глобальній мережі з'являється понад мільйон вірусних зразків. Наприклад, число вірусів-вимагачів за минулий рік потроївся, а число викупів збільшилася на 266% і в середньому по світу склало 1000 доларів з жертви.
Схоже, завдання кібербезпеки кінцевих пристроїв сьогодні стало одним із головних і навряд чи може бути реалізованим вручну і/або за допомогою одного тільки антивіруса.
І дійсно, аналітики Gartner відзначають стійкий тренд багаторівневого захисту кінцевих пристроїв, включаючи створення білих і чорних списків програм, вузлів і додатків і інших інструментів контролю в рамках повного циклу захисту.

Від чого залежить зріла стратегія захисту кінцевих пристроїв, якщо кожен девайс, підключений до вашої корпоративної мережі, по суті являє собою "двері" до цінних персональних і ділових даним?

Перш за все від розуміння, що ІБ-адміністрування - явище комплексне, а кінцеві пристрої - елемент IT (і значить, ІБ-) інфраструктури і вичленувати, де закінчується їх захист і починається захист, наприклад, мережі, фактично неможливо і безглуздо.

Тобто політики адміністрування і сам протокол безпеки повинні охоплювати захист всіх елементів IT-інфраструктури. А сучасна мережа підприємства з'єднує безліч кінцевих пристроїв, включаючи ПК, ноутбуки, смартфони, планшети, POS-термінали ... і кожен такий пристрій повинен відповідати вимогам доступу до мережі. А це означає, що їх кіберзахист повинен бути як мінімум автоматизований. Більш того, дотримання політик безпеки кінцевих точок з урахуванням зростаючого числа загроз сьогодні вимагає використовувати як мінімум:

1. файрволи для різних типів пристроїв;
2. антивіруси для електронної пошти;
3. моніторинг, фільтрацію і захист веб-трафіку;
4. управління безпекою і захисні рішення для мобільних пристроїв;
5. контроль роботи додатків;
6. шифрування даних;
7. засоби виявлення вторгнень [1].

При цьому ринок пропонує три основні рішення захисту кінцевих пристроїв і їх комбінації:

1. Традиційні антивіруси, засновані на сигнатурах. Дають стабільний результат - але лише в межах бази сигнатур. В силу неймовірно великої кількості шкідливих

зразків вони не може бути актуальним на 100% в кожен момент часу, плюс користувач здатний відключити антивірус на своїй машині.
2. Endpoint Detection and Response (EDR) або виявлення і реагування на інциденти. Такі рішення, розпізнають індикатори компрометації на кінцевому пристрої і блокують і / або лікують його. Зазвичай ці системи працюють тільки за фактом злому (вторгнення) на пристрій або в корпоративну мережу.
3. Advanced Endpoint Protection (AEP) або просунуту захист кінцевих пристроїв, яка включає превентивні методи захисту від експлойтів і шкідливого ПО, контроль пристроїв і портів, персональні файрволи та так далі. Тобто AEP-рішення бореться з погрозами: загроза розпізнається і знищується ще до злому, як, наприклад, в Palo Alto Networks Traps, Check Point SandBlast Agent (це рішення при виявленні підозрілих активностей робить резервні копії) або Forticlient [1].

Endpoint Detection and Response (EDR) - просунута система безпеки, що представляє собою інтегроване рішення для забезпечення безпеки кінцевих точок (комп'ютерних апаратних пристроїв) від потенційних загроз. Технологія поєднує в собі безперервний моніторинг і збір даних про кінцевих точок в режимі реального часу.

Інформація, зібрана в процесі моніторингу, записується для аналізу і дослідження. EDR постійно контролює кінцеві точки, забезпечуючи швидке реагування і негайну відповідь.

Система для збору даних про кінцевих точках підвищує рівень захисту користувачів, що працюють за межами захисту периметра компанії, а також захищає від безфайлових та інших видів атак і навіть заражених USB-накопичувачів. Щоб усунути недоліки в безпеці корпоративної мережі, організації розгортають рішення для виявлення і реагування кінцевих точок (EDR) в якості доповнення до існуючих засобів захисту [2].

Рішення EDR пропонують важливі переваги:

- Безперервний моніторинг широкого діапазону кінцевих пристроїв в корпоративних мережах і за їх межами дозволяє організаціям відстежувати не тільки зловмисні атаки з зовнішніх джерел (наприклад, постійні погрози APT , які можуть привести до витоку даних), але також для відстеження аномальної активності всередині організації (наприклад, видобутку криптовалюти або крадіжки даних співробітниками).
- Використання штучного інтелекту для моніторингу систем на предмет зловмисної активності з метою запобігання атак до і в міру їх виконання.
- Запис величезних обсягів активності в мережі , на відміну від інших інструментів, таких як SIEM і платформи захисту кінцевих точок, які не здійснюють запис або зберігають мала кількість інформації.

- Інтеграція з розширеними функціями, такими як пісочниця (Sandbox), для пошуку сплячих загроз.
- Включення попереджувального пошуку індикаторів атаки, щоб побачити загрози, які ще не були виявлені.
- Розширені можливості аналізу, що дозволяють командам безпеки швидше оцінювати і блокувати наступні атаки. До них відносяться пошук індикаторів компрометації; попереджуючий пошук індикаторів атаки і визначення першопричини зараження; кібер-інцидент і включення захисту від нього.
- Виправлення наслідків здійснених атак з можливістю відкату кінцевих точок до раніше відомого справного стану.
- Створення деталізованих політик для обробки USB-пристроїв з метою блокування невідомих і потенційно шкідливих USB-ключів.
- Включення захисту для віддалених співробітників , які не можуть покладатися на захист периметра [2].

Перелік посилань:

1. Захист кінцевих пристроїв [Електронний ресурс] – режим доступу: https://www.securitylab.ru/analytics/494402.php
2. What isEndpoint detection and response (EDR) [Електронний ресурс] – режим доступу: https://www.malwarebytes.com/what-is-edr

МЕТОДИ ТА ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВНУТРІШНІХ ЗАГРОЗ НА ПІДПРИЄМСТВІ

Стародубець Владислав Олександрович

студент групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

Актуальність і своєчасність звернення до даного питання обумовлена тим, що, на сьогодні найбільшу загрозу інформаційній безпеці представляють внутрішні зловмисники. З кожним роком ця загроза все зростає. Часи, коли керівники підприємств боялися атак хакерів і вірусів тепер в минулому. Звичайно, даний клас загроз донині несе в собі велику небезпеку, але більш за все компанії стурбовані саме через втрату, витоку корпоративної інформації й персональних даних. Про це говорять результати практично будь-яких досліджень в області інформаційної безпеки.

«Нехороші» співробітники своїми нелегітимними діями всередині підприємства можуть завдати йому шкоди не тільки у вигляді витоків даних, але й у вигляді прямої крадіжки грошових і матеріальних ресурсів з використанням IT-систем. Бувають випадки, коли персонал організовує реальні хакерські атаки всередині компанії. Наприклад, дуже складно протистояти загрозам, при реалізації яких співробітники компанії вступають в змову з третіми особами. Так, якщо зловмисникові вкрай непросто впровадити шкідливий код в продакшн-систему (для цього потрібно обійти масу бар'єрів і тільки після цього провести впровадження коду, який буде, наприклад, перенаправляти зловмисникові інформацію про замовлення в інтернет-магазині), то при можливості «домовитися» з розробником програми завдання істотно спрощується. [1]

За деякими оцінками, внутрішній співробітник сьогодні виявляється замішаний в 80% ІБ-інцидентів. Зловмисники спочатку захоплюють ідентифікаційні дані внутрішнього співробітника і вже потім діють від його імені.

Дослідження інституту SANS показали, що 74% опитаних ІБ-фахівців стурбовані внутрішніми загрозами; 32% визнають, що у них немає можливостей протистояти інсайдерам, 28% відзначили, що в їхніх організаціях захист від інсайдерів взагалі не вважається пріоритетною; 62% вважають, що в планах реагування на інциденти немає відмінності між зовнішніми атакуючими та внутрішніми.

Водночас в нещодавно опублікованих компанією Solar Security результатах досліджень приблизно 64% вивчених її фахівцями ІБ-інцидентів, були класифіковані як такі, що мали внутрішні причини. [2]

Внутрішні атаки залишаються найнебезпечнішими через розміри заподіюваних ними прямих збитків. Це підтверджують щорічні звіти, що публікуються ISACA, PwC, Verizon і іншими аналітичними компаніями. Відбувається це тому, що потенційний внутрішній порушник знає, як влаштовані інформаційні системи, і часто у своєму розпорядженні має прямий доступ до конфіденційної інформації. Крім того, внутрішньому порушнику заздалегідь

відомо, яку інформацію можна використовувати для вилучення особистої вигоди.

Для протидії внутрішнім загрозам застосовують спеціалізовані засоби захисту та комплексні рішення, спрямованими на протидію таргетованим атакам: пісочниці, системи управління ІБ і подіями ІБ, веб-шлюзи, шлюзи електронної пошти, засоби моніторингу дій адміністраторів та інших привілейованих користувачів, контроль виконуваних транзакцій і поведінкових моделей, контроль вразливостей інфраструктурних компонентів і бізнес-додатків й ін.

Комплексний підхід до захисту в першу чергу виражається в кореляції подій безпеки та інтеграції різних механізмів захисту між собою. Сучасна система захисту повинна будуватися не на розрізнених засобах захисту, здатних працювати тільки у своїй вузькій сфері, а на комплексних продуктах, які вміють зіставляти між собою різні події та дозволяють виробляти комплексну реакцію в залежності від загальної ситуації.

Не можна також забувати, що забезпечення ІБ - безперервний процес. Поки існує сама інформація, що вимагає захисту, система менеджменту ІБ (СМІБ) повинна ґрунтуватися на відомій моделі PDCA (Plan-Do-Act-Control, плануй - роби - перевіряй - впливай).[3]

Висновок

Резюмуючи наведену вище інформацію, можна зробити висновок, що попри велику кількість наявних алгоритмів виявлення конфіденційної інформації, всі вони не ефективні. Актуалізація проблеми внутрішніх загроз викликана незахищеністю від них організацій і відсутністю ефективного рішення по боротьбі з ними. Практично на всіх підприємствах використовуються програмні та / або апаратні засоби захисту, які призначені для боротьби із зовнішніми загрозами (антивіруси, брандмауери, IDS й т.д.) і досить ефективно з ними борються. Що стосується засобів захисту від внутрішніх загроз, то тільки дуже незначна частина компаній їх використовує, хоча необхідність в цих засобах об'єктивно існує.

Перелік посилань:

1. Валерий Васильев «Внутренние и внешние ИБ-угрозы: есть ли смысл в их разделении?» – Електронний ресурс – Режим доступу: https://www.itweek.ru/security/article/detail.php?ID=178063

2. Solar Security – «Какие организации чаще других подвержены внутренним нарушениям корпоративной безопасности» – Електронний ресурс – Режим доступу: https://rt-solar.ru/analytics/reports/

Единый Стандарт – «PDCA простыми словами» – Електронний ресурс – Режим доступу: https://1cert.ru/stati/pdca-prostymi-slovami

ПОЯВА ТА ЕВОЛЮЦІЯ APT-АТАК

Рожко Владислав Геннадійович

студент групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

Анотація

Розглянуто сутність поняття атак типу APT, їх поява, критерії виявлення таких атак та техніки, що активно використовуються для реалізації APT-атак.

Сьогодні велику частину загроз ІБ підприємств та організацій становлять APT-атаки. APT-атаки – це різновид складних кібератак з метою отримання несанкціонованого доступу до інформаційних систем та встановлення прихованого доступу з метою використання або контролю в майбутньому. Вперше термін APT (Advanced Persistent Threat) приблизно з 2004 року в своїх дослідженнях стала використовувати американська команда реагування на комп'ютерні інциденти Lockheed Martin (LM-CIRT). Так почали називати складні атаки, які здійснюються переважно на IT-інфраструктуру військових та державних об'єктів. Як правило, в їх проведенні підозрювали спецслужби інших країн та команди хакерів, що працюють на уряд.

Завдяки журналістам поняття APT розширилось до багаторівневих атак, ціллю яких може бути мережа будь-якої організації або група пристроїв із загальними ознаками. Навіть сьогодні термін APT залишається неоднозначним. Його перекладають як «розвинена стійка загроза» або «складна постійна загроза», маючи на увазі або багатоетапний сценарій атаки, або використовувані в ній інструменти, або взагалі потужні хакерські групи [1].

Компанія Sophos також відмічає, що досі не існує єдиних критеріїв, які дозволяють віднести ту чи іншу атаку саме до APT. Успішні цілеспрямовані атаки зазвичай виконуються з використанням старих наборів експлойтів, тому 0day вразливості – необов'язковий атрибут APT.

Інший критерій APT, який часто виділяють – розсилка фішингових листів для компрометації облікового запису рядового працівника компанії. Далі вона використовується як точка входу до локальної мережі та плацдарм для переходу на наступний рівень – до комп'ютерів керівників та серверів організації. Проте методи соціальної інженерії і так є дуже популярними, тому було б некоректно виділяти їх як маркер «складної постійної загрози». На що ж тоді варто орієнтуватися?

Аналізуючи звіти різних спеціалістів з інформаційної безпеки, можна сформувати наступні критерії APT (дані критерії можуть бути уточнені та доповнені) [2]:

- це завжди цілеспрямована атака. Жертвою зазвичай виступає не конкретна людина або організація, а який-небудь більш загальний сегмент (наприклад, фінансові установи) або однорідна група людей;
- це довготривала атака. Вона може тривати не один місяць і продовжуватися до переможного кінця або втрати доцільності;
- це добре фінансована атака. Навіть банальний DDoS – витратна процедура, якщо триває довгий час;
- це багатостадійна атака. У APT послідовно використовується декілька векторів і різних технік. Самі по собі вони можуть бути примітивними. Цікавим є саме їх поєднання. Наприклад, секретарю надсилають фішингові листи для того, щоб скомпрометувати її корпоративний обліковий запис і через неї (як від довіреної особи) відправити заражений документ на ноутбук керівника;
- APT не зупиняють окремі інструменти безпеки (антивірус, брандмауер, спам-фільтри, прості SIEM-системи) і вона довгий час може залишатися непоміченою або протікати під маскою окремих типових інцидентів. Важливим є те, що аномальна поведінка мережі або окремих пристроїв зберігається, хоча при рутинних перевірках нічого підозрілого не виявляється;
- В ході APT часто (але не обов'язково) використовують просунуті техніки, які ефективно маскують їх компоненти від типових систем захисту. Наприклад, reverse shell для обходу міжмережевого екрану.

За даними Sophos, в APT використовуються наступні техніки (перераховані в порядку зменшення частоти застосування): фішинг та соціальна інженерія; DDoS та ботнети; вразливості нульового дня та просунуте шкідливе ПЗ, яке їх використовує; традиційне шкідливе ПЗ; скомпрометовані пристрої; атаки інсайдерів; атаки на рівні додатків [3].

Таким чином, APT-атаки на даний час є серйозною загрозою для будь-якої організації у будь-якій сфері діяльності. Незважаючи на те, що існує велика кількість рішень від крупних вендорів, вони не забезпечать повний захист від таких атак. Розумна обережність та уважність дозволить значно знизити ризик реалізації APT-атак.

Список використаних джерел

1. Advanced Persistent Threat (APT) [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

2. Anatomy of Advanced Persistent Threats [Електронний ресурс] – Режим доступу: https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html

3. What Is an Advanced Persistent Threat (APT)? [Електронний ресурс] – Режим доступу: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

СЕРТИФІКАЦІЙНІ ПРОГРАМИ EC-COUNCIL ТА COMPTIA ДЛЯ ФАХІВЦІВ З ІТ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тищенко Віталій Сергійович
студент групи УБДМ-61, ННІЗІ ДУТ,Київ, Україна
Мужанова Тетяна Михайлівна
к. держ.упр., доц., доцент кафедри УІКБ, ННІЗІ, ДУТ, Київ, Україна

Розглянуто перелік вендоронезалежних сертифікаційних програм для фахівців з ІТ та інформаційної безпеки від знаних експертних організацій галузі: Міжнародної ради консультантів з питань електронної комерції (EC-Council) та Асоціації галузі інформаційних технологій (CompTIA). Зазначені некомерційні організації пропонують низку професійних сертифікацій за вузькоспеціалізованими напрямами ІТ та інформаційної безпеки різних рівнів складності.

Внаслідок швидких темпів розвитку сучасних технологій та виникнення нових викликів для інформаційно-телекомунікаційних систем та інформаційних ресурсів підприємств перед фахівцями з питань інформаційної безпеки постає питання удосконалення власних професійних знань і навичок. Одним із перевірених і найбільш престижних способів підвищення кваліфікації у сфері інформаційної безпеки є незалежні від виробників сертифікаційні програми, зокрема таких авторитетних експертних організацій як EC-Council та CompTIA.

Міжнародна рада консультантів з питань електронної комерції (International Council of Electronic Commerce Consultants - EC-Council) - це американська неурядова організація, яка була створена у 2001 році після сумнозвісних атак 11 вересня для того, щоб надавати послуги із сертифікації та навчання в галузі електронного бізнесу та кібербезпеки. Фундатори Ради бачать метою організації пом'якшення й усунення кіберчуми, яка загрожує світові сьогодні. За час свого існування EC-Council сертифікувала понад 200 тис. фахівців із 87 країн [1].

Організація є власником і розробником всесвітньо відомої програми сертифікованого етичного хакера (Certified Ethical Hacker - CEH) і ще 19-ти курсів за 6-ма категоріями:

1. Просунутий рівень, зокрема сертифікований тестувальник на проникнення – CPENT, сертифікований аналітик операційного центру безпеки – CSA;
2. Базовий рівень, в т.ч. сертифікований спеціаліст з безпеки – ECSS, сертифікований спеціаліст з криптографії – ECES;
3. Основи, серед яких CEH, CEH (Master), сертифікований фахівець із безпеки мереж - CND;
4. Спеціаліст: сертифікований спеціаліст з обробки інцидентів – ECIH, сертифікований спеціаліст із розслідувань інцидентів комп'ютерної безпеки - CHFI;
5. Управління - сертифікований директор з інформаційної безпеки – CCISO;
6. Обізнаність з безпеки - сертифікований безпечний користувач ПК – CSCU.

Іншою відомою організацією, яка надає сертифікаційні послуги фахівцям у сфері IT та інформаційної безпеки є американська Асоціація галузі інформаційних технологій (Computing Technology Industry Association – CompTIA). Компанія CompTIA, що базується в Даунерс-Гроуві, штат Іллінойс, видає професійні сертифікати, які не прив'язані до постачальників, у більш ніж 120 країнах. Щорічно організація випускає понад 50 галузевих досліджень для відстеження тенденцій та змін у галузі IT [2].

На сьогодні CompTIA реалізує професійні сертифікаційні курси за такими 4-ма напрямами в галузі IT та кібербезпеки:

1. Основи IT: Основи IT - IT Fundamentals (ITF+); IT для початківців - CompTIA A+, Мережі - CompTIA Network+; IT-безпека - CompTIA Security+;
2. Інфраструктура: Хмарні технології - CompTIA Cloud+; ОС Linux - CompTIA Linux+; Серверні платформи - CompTIA Server+;
3. Кібербезпека: Аналітик кібербезпеки - CySA+; Фахівець з тестування вразливостей - CompTIA PenTest+; Просунутий професіонал з кібербезпеки - CompTIA CASP+;
4. Додаткові професійні сертифікати: IT-проекти - CompTIA Project+; Технічний тренер з IT - CompTIA CTT+; Основи хмарних технологій для нетехнічних фахівців - CompTIA Cloud Essentials+.

Отже, одними з найбільш відомих некомерційних експертних організацій у сфері сертифікації фахівців з IT та інформаційної безпеки у світі є EC-Council та CompTIA, кожна з яких пропонує широкий перелік сертифікаційних програм за різними вузькоспеціалізованими напрямами IT та інформаційної безпеки на рівні від початківця до професіонала.

Перелік посилань:

1. EC-Council. About us. URL: https://www.eccouncil.org/about/.
2. CompTIA About us URL: https://www.comptia.org/about-us/.

РОЛЬ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Зіновський Ростислав Олександрович
студент групи УБДМ-61 ННІЗІ ДУТ, Київ, Україна

Розглянуто перелік загроз інформаційно-телекомунікаційним системам підприємства. Визначено завдання, які виконуються на організаційному рівні забезпечення інформаційної безпеки, серед яких планування, організація та контроль заходів безпеки; розробка і впровадження нормативних вимог з інформаційної безпеки; розмежування й обмеження доступу; сертифікація і ліцензування у сфері інформаційної безпеки; навчання і формування обізнаності персоналу; оцінювання ефективності й удосконалення системи захисту інформації.

В Україні за останні часи збільшилася кількість кібератак як у корпоративному, так і державному секторі. За даними Ради національної безпеки і оборони України у 2020 році в Україні зафіксували близько 1 мільйона випадків кібератак, серед них - мережеві атаки, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення [1].

У результаті хакерських атак на інформаційно-телекомунікаційні системи підприємства можуть бути реалізовані так типи загроз інформаційній безпеці:

- Крадіжка інформації. Втручання в роботу комп'ютерних систем з метою отримання конфіденційної інформації.
- Втрата та маніпулювання даними через злом комп'ютера з метою знищення або зміни записів даних.
- Крадіжка ідентичності. Це форма крадіжки інформації, метою якої є заволодіння персональними даними.

Для запобігання і протидії загрозам інформаційній безпеці підприємства здійснюється комплекс різнопланових заходів: інженерно-технічних, фізичних, нормативно-правових та організаційних.

На організаційному рівні забезпечення інформаційної безпеки вирішуються такі завдання:

- планування, організація та контроль заходів забезпечення інформаційної безпеки;
- розробка і впровадження нормативних вимог з інформаційної безпеки (корпоративних політик, стандартів, процедур тощо);
- розмежування й обмеження доступу до інформаційних ресурсів, засобів їх обробки та передачі;
- сертифікація і ліцензування у сфері інформаційної безпеки;
- навчання і формування обізнаності персоналу й користувачів з питань інформаційної безпеки;
- оцінювання ефективності й удосконалення системи захисту інформації тощо [2].

Також завдяки впровадженню організаційних заходів підприємство здатне забезпечувати збирання й аналіз повних і об’єктивних відомостей про появу, сутність і розвиток проблем інформаційної безпеки; акумулювати досвід

попередніх досліджень, розробок і практичного вирішення завдань захисту; формувати науково обґрунтовані напрямки розвитку практики забезпечення інформаційної безпеки.

Отже, організаційні заходи відіграють важливу роль у забезпеченні інформаційної безпеки підприємства, створюючи і підтримуючи умови для ефективного запобігання і протидії загрозам інформаційній безпеці, роблячи значний внесок у забезпеченні безперервності бізнесу і конкурентоздатності підприємства на ринку.

Список використаних джерел:

1. В Україні в 2020 році зафіксували 1 мільйон кібератак – РНБО. URL: https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvaly-1-milyon-kiberatak-rnbo/

2. Організаційні методи захисту інформації. URL: https://tzi.ua/ua/organzacjn_metodi_zahistu_nformac.html

МЕТРИКИ ДЛЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Шекера Ольга Олександрівна

студентка групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

Основна цінність діяльності багатьох компаній сучасності – інформація. Саме тому тема захисту інформації стає актуальнішою з року в рік. Підвищення інформаційної безпеки починається з визначення показників, які визначають рівень зрілості та одразу вказують на можливості для покращення. Визначення оптимальних та вичерпних метрик для забезпечення належного рівня інформаційної безпеки допоможе підприємству оперативно відслідковувати за запобігати можливим втратам від наслідків інцидентів інформаційної безпеки

Ключові слова: оцінка інформаційної безпеки, показники для оцінки інформаційної безпеки, методи оцінки інформаційної безпеки

Під час віддаленої роботи, спричиненої пандемією, все більше компаній переходять на обмін інформацією через зовнішні мережі, використовують хмарні технології та при цьому не мають змоги контролювати своїх співробітників на місцях. В такому середовищі необхідно вибудувати систему, в якій конфіденційна інформація буде надійно захищена і передаватиметься лише між авторизованими користувачами.

Як саме компанії оцінити рівень захищеності інформації? Яку інформацію збирати та на що звертати увагу? Саме для цього розробляються метрики, які допомагають відслідковувати та коригувати стан інформаційної безпеки підприємства.

Метрики зазвичай мають кілька загальноприйнятих характеристик. Наприклад, хороший показник чіткий і однозначний. Це забезпечує оптимальну вартість збору даних (тобто вартість збору даних вимірювань не перевищує значення даних для підприємства). Хороший показник також підтримує прийняття рішень і виключає суб’єктивне тлумачення [1, ст.9].

Нижче наведено перелік певних метрик, які допомагають слідкувати за рівнем інформаційної безпеки на підприємстві [2]:

1. Середній час виявлення та середній час реагування

Середній час ідентифікації (MTTI - Mean Time To Identify) та середній час вирішення (MTTC - Mean Time To Contain) вказує на фази виявлення та реагування на інциденти інформаційної безпеки. Ці два показники є пріоритетними та найбільш показовими в оцінці ефективності системи управління загрозами інформаційної безпеки, так як покращення значень цих показників напряму впливає на зменшення потенційних втрат від інцидентів інформаційної безпеки

2. Кількість систем з відомими вразливими місцями

Знання кількості вразливих активів у системному середовищі є ключовим показником кібербезпеки для визначення ризику бізнесу. Управління оновленнями та виправленнями - складний процес, але дуже важливий, щоб уникнути лазівок, які можна використати у для проникнення у внутрішні системи компанії. Сканування вразливості, що включає всі активи, вказуватиме,

що потрібно зробити, щоб покращити безпеку вашої компанії. Програма управління вразливістю - це не опціональне покращення, а необхідність.

3. Кількість неправильно налаштованих сертифікатів SSL

Сертифікат SSL - це невеликий файл, який засвідчує право власності на криптографічний ключ до веб -сайту або компанії, з якою відбувається обмін даними, що гарантує достовірність транзакції. Моніторинг вимог безпеки для кожного сертифіката, а також гарантування того, що вони належним чином налаштовані на серверах, запобігає їх потраплянню в чужі руки та тому, що цифрова ідентичність вашої компанії не використовується для крадіжки інформації користувача.

4. Обсяг даних, переданих за допомогою корпоративної мережі

Якщо ваші співробітники мають необмежений доступ до Інтернету через корпоративну мережу, моніторинг обсягу трафіку дозволяє виявити зловживання ресурсами компанії. Завантажуючи програмне забезпечення, відео, фільми та програми, користувач може залишити двері відкритими для вторгнення ботнетів та шкідливого програмного забезпечення у систему компанії, навіть більше, якщо завантаження здійснюються з веб -сайтів, відомих як небезпечні.

5. Кількість користувачів із рівнем доступу "суперкористувача".

Найкращі практики управління інформаційною безпекою включають повний контроль рівня доступу користувачів до ресурсів компанії, коли працівник має доступ лише до даних, систем та активів, необхідних для його роботи. Визначення рівнів доступу всіх користувачів мережі дозволяє вам коригувати їх у разі потреби, блокуючи будь якого суперкористувача або адміністратора, що не має авторизації для цього статусу.

6. Кількість днів для деактивації облікових даних колишніх працівників

Відстежуючи цей показник, можливо визначити, чи співпрацюють кадрові та IT -команди. За ідеального сценарію доступ користувачів, які припинили свою діяльність в компанії, слід негайно скасувати. Підтримка їх активності - це величезний ризик, оскільки це може спричинити витік конфіденційної інформації та призвести до злому пристроїв.

7. Періодичність перевірки доступу третіх сторін

Часто IT -менеджери надають доступ третім сторонам у своїх мережах для здійснення проекту чи іншої діяльності. Важливо відстежувати, чи скасовано доступ після закінчення надання послуг. Якщо цього не зробити, це загрожує системі компанії, якщо третя сторона вирішує повернутися і отримати доступ до даних або здійснити іншу шкідливу діяльність - наприклад, передачу конфіденційної інформації конкурентам. Можливо, ще гірше, якщо мережа третьої сторони зламана, ви можете піддати свою мережу тій самій загрозі.

8. Частота доступу третіх сторін до критичних систем підприємства

Створення картографування критичних систем для компанії та знання користувачів, які мають до них доступ, є обов’язковими у контексті безпеки. Моніторинг спроб отримати доступ до серверів або програм, на які не повинні

націлюватися неавторизовані користувачі, може свідчити про порушення та наміри поставити під загрозу інформаційне середовище компанії.

9. Відсоток ділових партнерів з ефективною політикою в галузі кібербезпеки

Необхідно регулярно оцінювати показники кібербезпеки ділових партнерів, які надають послуги компанії. Надання доступу до внутрішнього середовища аутсорсинговій компанії може становити величезний ризик, якщо в першу чергу у цієї компанії немає ефективної політики безпеки. Не зайве сказати, що якщо компанія інвестує в безпеку, але до її систем підключені треті сторони, які цього не роблять, безпека компанії залишається під загрозою та всі інвестиції не мають сенсу.

Ефективне управління різними показниками ефективності інформаційної безпеки є основною відмінністю попереджувального підходу до управління загрозами інформаційної безпеки від наслідкового. Хоча менеджери вже деякий час слідкують за показниками ефективності діяльності компаній, в інформаційній безпеці це нова практика відстеження показників кібербезпеки, що продовжує розвиватися.

Перелік посилань:

1. SANDIA REPORT// Cyber Threat Metrics// March 2012. URL: https://irp.fas.org/eprint/metrics.pdf
2. 10 Cybersecurity Metrics You Should Be Monitoring, Cipher company blog [Електронний ресурс] – Режим доступу: https://cipher.com/blog/10-cybersecurity-metrics-you-should-be-monitoring/

ЗАХОДИ ВПРОВАДЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ

Грабчук Артем Ярославович,

студентка групи УБДМ-61, ННІЗІ ДУТ, Київ, Україна

Розглянуті проблеми необхідності впровадження політики безпеки в компанії та які саме способи для її реалізації існують. Проаналізувавши статті, стало зрозуміло, що існує, як мінімум, три заходи, вжиття який може надати потрібний рівень захисту інформації, а саме: нормативно-правовий,адміністративний та використання спеціального обладнання та програмного забезпечення. Також було розглянуто питання реалізації політики безпеки в компанії. Було надано список необхідних функцій, які повинні бути реалізовані при створенні політики безпеки, та виконання яких буде свідчити про серйозне ставлення до безпеки.

На сьогоднішній день захист інформації - достатньо розвинена галузь науки і техніки, що пропонує широкий спектр різноманітних засобів захисту даних. Проте жодний окремо взятий засіб не забезпечує потрібного рівня захисту інформаційних систем. Захист на потрібному рівні можливий лише за умови комплексного вжиття взаємодоповнюючих заходів, а саме [1, с. 45]:

- нормативно-правових;
- адміністративних;
- спеціального обладнання та програмного забезпечення.

Для протидії загрозам, які існують у сучасному світі, одним з методів є застосування механізмів безпеки, які реалізують прийняту політику безпеки. Політика безпеки відповідно до мети та умов функціонування системи може визначати права доступу до ресурсів та регулювати процедуру аудиту ктивності користувачів у системі, виконувати захист мережевих комунікацій,формулювати шляхи відновлення системи після випадкових збоїв та інше

Для реалізації прийнятої політики безпеки існують правові, організаційні, адміністративні та інженерні заходи щодо захисту інформації.

Правове забезпечення інформаційної безпеки - це сукупність законів, правових документів, нормативних актів, інструкцій, посібників, вимог, які вимагаються системою захисту інформації.

Інженерні заходи - це сукупність технічних інструментів та заходів спеціальних органів, які діють разом для виконання конкретного завдання. До інженерних інструментів відносяться скринінгові кімнати, організація сигналізації, засоби безпеки з персональними комп'ютерами тощо.

Організаційне та адміністративне забезпечення інформаційної безпеки - це регулювання виробничої діяльності та взаємовідносин між виконавцями на нормативно-правовій основі таким чином, що розкриття, витік та несанкціонований доступ до інформації стає неможливим або суттєво складнішим внаслідок здійснення організаційної діяльності [2, с. 36-37].

Ефективна безпека інформаційних систем базується на ряді функцій. Список, наведений нижче, не є повним. Тим не менше, докази того, що всі ці функції виконуються ефективно та скоординовано є свідченням того, що до безпеки інформаційних систем відносяться серйозно і імплементують ефективно [3, с. 10-14].

1) Збір, аналіз та розповсюдження стратегічної інформації про загрози системам.

   Збір інформації про вразливості в системах надає можливість адміністраторам інформаційних систем, на які можуть вплинути ці загрози, вжити виправних заходів.

2) Моніторинг показань системи та попереджень.

   В цьому випадку є декілька основних пунктів, які повинні виконуватися:

   - моніторинг показників загроз;
   - оцінка та характеристика атаки (якщо така є);
   - визначення цілі атаки.

3) Мати можливість ідентифікувати зловмисників.

Звичайно, визначити зловмисників важко. Тим не менше, певні типи інформації - якщо вона буде зібрана - можуть пролити світло на особу зловмисника. Наприклад, деякі зловмисники переважно використовують певні інструменти або техніки (наприклад, той самий словник для перевірки паролів).

4) Тест на слабкі місця в безпеці систем.

Назва цього пункту говорить сама за себе. Для забезпечення безпеки системи від загроз, потрібно постійно перевіряти, які слабкі місця є в системі. Адже щодня дослідники та користувачі знаходять нові дірки в безпеці різних систем.

5) Сплануйте як система повинна реагувати на атаки.

Це є дуже важливою частиною дизайну інформаційної системи.Коли атака неминуча (або в процесі), організація може завбачливо прийняти додаткові заходи безпеки.

6) Координувати оборонну діяльність на всьому підприємстві.

Будь-яка велика розподілена організація має безліч інформаційних систем та підмереж, які повинні бути захищені. Діяльність, спрямована на захист кожної з цих систем та мереж, повинна бути скоординована оскільки розподілені частини мають взаємозв’язки і від цього залежить безпека всієї організації.

7) Забезпечити доступність та функціонування публічної інфраструктури, що використовується в системах.

Небагато мереж будуються повністю з використанням систем, контрольованих організацією, яка їх використовує. Тому організації повинні співпрацювати з власниками інфраструктури, на яку вони покладаються, та відповідними органами влади для їх захисту.

8) Забезпечити доступність та функціонування публічної інфраструктури, що використовується в системах.

Небагато мереж будуються повністю з використанням систем, контрольованих організацією, яка їх використовує. Тому організації повинні співпрацювати з власниками інфраструктури, на яку вони покладаються, та відповідними органами влади для їх захисту.

9) Включіть вимоги безпеки до будь-яких специфікацій системних або мережевих вимог що використовується в процесі придбання.

Переобладнання функцій безпеки в системи, не призначені для безпеки незмінно залишає діри в безпеці, а процедурні виправлення властивих технічних вразливостей не виправлять всіх вразливостей.

10) Запровадити високий рівень оборонних інформаційних технологій (та процесів) за допомогою досліджень.

Хоча зазвичай можна багато чого зробити для поліпшення безпеки інформаційних систем просто за допомогою відомих та доступних технологій, виправлень помилок та процедур, завжди потрібні кращі інструменти для підтримки місії захисту інформаційних систем.

11) Підвищення рівня обізнаності щодо інформаційних систем.

Незалежно від того, наскільки добре захищена система, якщо її користувачі не дотримуватимуться хоча б мінімальних правил безпеки, вони завжди будуть ставити систему під загрозу.

12) Встановлення стандартів безпеки (як технічних, так і процедурних).

Стандарти безпеки повинні чітко сформулювати те, що організація очікує зробити в галузі безпеки.

13) Розробка та використання критеріїв для оцінки стану безпеки.

Інформаційна безпека є не одноразовою проблемою, а постійною. Загрози, технології та організації постійно змінюються, а тому організації повинні мати способи вимірювання та оцінки того, чи мають вони ефективні захисні заходи.

В теперішній час, коли безпека інформації є однією з головних та важливих цілей багатьох компаній, дуже важливо правильно ЇЇ спланувати та реалізувати. Як видно з усього згаданого вище, захист інформації - це процес, який повинен включати в себе достатньо велику кількість важливих рішень та заходів, одним з яких є створення та запровадження політики безпеки.

Література

1. Ромашко С. М. Опорний конспект лекцій з дисципліни "Інформаційні системи в менеджменті"[Електронний ресурс] / С. М. Ромашко. – 2007. – Режим доступу до ресурсу: http://www.dut.edu.ua/uploads/l_1937_18003221.pdf.
2. Boiko A. System Integration and Security of Information Systems [Електронний ресурс] / A. Boiko, V. Shendryk. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/313483965_System_Integration_and_Security_of_Information_Syst ems.
3. Berson T. Information Systems Security [Електронний ресурс] / T. Berson, R. Kemmerer, B. Lampson. – 1999. – Режим доступу до ресурсу: https://www.microsoft.com/en-us/research/wp- content/uploads/2016/11/Acrobat-5

ПОНЯТТЯ ХМАРНИХ ОБЧИСЛЕНЬ: ОСНОВНІ МОДЕЛІ ТА ХАРАКТЕРИСТИКИ

Данильченко Ю. М.., УБДМ-61

Державний університет телекомунікацій

Вступ. Хмарні обчислення стають невід'ємною частиною роботи сучасних компаній. Але, щоб домогтися успішного використання цієї технології, варто чітко розуміти головні характеристики хмари, її види і які послуги використовуються для оптимізації роботи в хмарі.

Основна частина. Хмарні обчислення (cloud computing) – це модель роботи, за допомогою якої компанія отримує доступ до загальних обчислювальних ресурсів на кшталт серверів, сховищ, мережі, додатків та інших хмарних послуг. Всі ресурси можуть використовуватися й керуватися користувачем без додаткової допомоги провайдера хмарних послуг.

Хмарні обчислення мають наступні ключові характеристики:

- **Самообслуговування за запитом**
  Якщо ви вирішите в суботу ввечері, що вам необхідно використовувати обчислювальні можливості хмари, ніби мережевого сховища інформації, ви зможете зробити це самостійно без допомоги співробітників провайдера.
- **Вільний доступ через мережу Інтернет**
  В основному, щоб скористатися можливостями і послугами хмарних обчислень, потрібно мати доступ в мережу. Більш того, скористатися послугами можна з різних пристроїв, будь то ноутбук або ж мобільний телефон.
- **Об'єднання ресурсів**
  Провайдер об'єднує всі хмарні ресурси в один пул і пропонує їх для використання шляхом множинної оренди. Всі віртуальні та фізичні ресурси хмари виділяються в залежності від ваших і інших користувачів потреб. До ресурсів належать сховище, оперативна пам'ять, віртуальні машини, обчислювальна потужність, пропускна здатність.

- **Швидка масштабованість**

  У разі необхідності обсяг ресурсів швидко резервується і масштабується під ваші вимоги. Провайдери часто практикують сценарії, щоб ви могли купити необхідні ресурси в будь-який час і в будь-якому обсязі.

- **Вимірна послуга**

  Щоб ви і хмарний провайдер оперували чесними даними про обсяг використаних послуг, усі ресурси автоматично контролюються, вимірюються й оптимізуються. Серед таких ресурсів: обчислювальна потужність, число активних користувачів, обсяг сховища, пропускна здатність і інше.

Моделі хмарних обчислень:

- **Software as a Service (SaaS) – програмне забезпечення як послуга.**

Подібна хмарна модель має означає використання ПЗ провайдера, яке функціонує в хмарній інфраструктурі. Ви можете використовувати подібне програмне забезпечення через клієнтський або програмний інтерфейс. Важливо розуміти, якщо ви використовуєте SaaS-послугу, ви не зможете керувати такою хмарною інфраструктурою як ОС, мережа, сховище, сервер. Серед яскравих прикладів: Microsoft 365.

- **Platform as a Service (PaaS) – платформа як послуга.**

Вам надається в користування платформа хмарних обчислень, де є всі необхідні хмарні мови, послуги, інструменти, бібліотеки від самого хмарного провайдера. Ви також не можете управляти базовою хмарною інфраструктурою, серверами, мережею, ОС і сховищами. Але натомість ви можете керувати програмами та частково параметрами конфігурації середовища додатків. Серед яскравих прикладів: Microsoft Azure.

- **Infrastructure as a Service (IaaS) – інфраструктура як послуга**

У вас в розпорядження є обчислювальні потужності, сховище, мережа та інші важливі обчислювальні ресурси, за допомогою яких ви можете розгортати та керувати довільно вибраними ПЗ. У них може входити додатки й операційні системи. Ви також не керуєте хмарною інфраструктурою, але можете

налаштовувати ОС, розгорнуті додатки, сховище та частково управляти деякими компонентами на зразок міжмережевих екранів вузла. Серед відомих провайдерів послуги – Google, IBM, Amazon і інші.

Моделі розгортання хмарних обчислень:

Приватна хмара (Private Cloud)

Всі ресурси приватної хмари використовуються лише однією компанією або групою компаній. Подібна модель розгортання хмарних обчислень управляється як самою компанією-клієнтом, так і провайдером хмарних послуг. Зазвичай подібна деталь обговорюється ще на стадії укладання договору. Якщо компанія розуміє, що у неї немає відповідних фахівців, вона користується послугою віддаленого адміністрування. Якщо ви сумніваєтеся в необхідності приватної хмари, дізнайтеся детальніше про її можливості на нашій сторінці.

Хмара спільноти (Community cloud)

Провайдер надає хмарну інфраструктуру в використання для спільноти споживачів, у яких є спільна місія, політика безпеки, і вимоги для коректного виконання роботи. Хмарою можуть володіти й управляти відразу кілька організацій спільноти або провайдер послуги.

Публічна хмара (Public cloud)

Ресурси подібної хмари відкрито й активно використовуються різними користувачами в Інтернеті. Зазвичай така хмарна інфраструктура управляється і належить певній державній, комерційній або академічній організації. Послугами публічної хмари користуються не тільки звичайні користувачі, але і стартапи, і великі компанії з великим кількістю філій.

Гібридна хмара (Hybrid cloud)

Подібна модель складається з двох інших моделей хмарної інфраструктури. Навіть коли вони працюють як один гібрид, вони все ще залишаються незалежними об’єктами, які пов’язані пропріетарною технологією. За допомогою неї компанія передає дані.

Література:

1. https://sites.google.com/site/hmaarniobcislenna/
2. http://integritysys.com.ua/solutions/pricatecloud-solution/
3. https://onbiz.biz/cloud-computing-models/

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В КІБЕРСПОРТИВНИХ ЗАХОДАХ

Поляков Дмитро Андрійович

Студент групи УБДМ-61, ННІЗІ, ДУТ, Київ,Україна

Визначено, що кіберспортом називають змагання з комп'ютерних та відео ігор, в яких беруть участь професійні гравці. Показані найпопулярніші кіберспортивні дисципліни : Dota 2, Counter-Strike: Global Offensive, Fortnite, League of Legends, StarCraft II. Відмічено, що Україна входить у 10 топових країн світу за розвитком кіберспорту і займає 5-е і 6-е місце в світі серед країн з найбільш розвиненою галуззю кіберспорту. Масштабність розвитку кіберспорту України в останні роки звертає увагу на необхідність захисту від кіберзагроз при проведенні спортивних заходів, які суттєво знижують кінцеві результати ігри або зовсім приведуть до її зупинки. Запропоновані напрямки

забезпечення кібербезпеки в кіберспортивних заходах.

Ключові слова: кібербезпека, кіберспорт, спортивні ігри, комп'ютерні ігри, системи захисту.

Кіберспортивні заходи стали надзвичайно популярними. Те, що колись було мрією багатьох геймерів (від англ. gamer — гравець) і стримерів (гравець у прямому ефірі) , тепер стало реальністю в організації проведення спортивних офлайн ігор. Кіберспортом називають змагання з комп'ютерних та відео ігор, в яких беруть участь професійні гравці. До найпопулярніших кіберспортивних дисциплін відносяться: Dota 2, Counter-Strike: Global Offensive, Fortnite, League of Legends, StarCraft II. Найбільш знакові турніри — це The International (грають в Dota 2), Evolution Championship Series (файтинг), Intel Extreme Masters (Starcraft II, Counter-Strike: Global Offensive), Fortnite World Cup Finals, LoL World Championship і PUBG Global Championship. Ці заходи організовуються на найвищому рівні: з відеотрансляцією і мільйонними призовими фондами для переможців. У Києві існують 3 студії, які створюють турніри на найвищому рівні. Україна входить у 10 топових країн світу за розвитком кіберспорту і займає 5-е і 6-е місце в світі серед країн з найбільш розвиненою галуззю кіберспорту. Існують прогнози, що через 10 років кіберспорт стане навіть популярніше ніж футбол [1].

Із 2018 року, початку існування "Федерації кіберспорту України" (UESF), проведено понад 250 турнірів у всіх областях країни, із них 6 - національних і 4 - міжнародних. Взяли участь у змаганнях понад 70 000 українців.

В останні роки кількість глядачів і людей, які почали грати у різні комп'ютерні ігри – зросла приблизно на 20%.[2]. Структура кіберспорту включає велику кількість організаторів, команд, менеджерів, турнірів та чемпіонатів світу з різних дисциплін. Тому можна вважати, що кіберспорт вже став повноцінним спортом і серйозною індустрією. Офіційно кіберспорт визнали видом спорту в Україні 7 вересня 2020 року. Ця індустрія вже давно перетворилась в справжній бізнес, який приносить багато користі й можливостей як локального, так і світового масштабу. Деякі комп'ютерні ігри сьогодні перетворилися на спортивні дисципліни. Кіберспортивні турніри стали явищем планетарного масштабу, а гравці часом відчувають такі ж фізичні і психологічні навантаження, як і в традиційних видах спорту. Міжнародний олімпійський комітет всерйоз обговорює майбутнє кіберспорту в рамках Олімпійських ігор.

При проведенні спортивних заходів можуть виникати кіберзагрози, які суттєво знижують кінцеві результати ігри або зовсім приведуть до її зупинки.

В правилах спортивних змагань з кіберспорту, затверджених 26 січня 2021 р., відзначено: створення умов для безпеки під час проведення ЛАН змагань з кіберспорту здійснюється відповідно до законодавства України [3, п.15].

Комп'ютери та технічні пристрої за параметрами продуктивності повинні відповідати вимогам, рекомендованим Міжнародною Федерацією Кіберспорту, або, в разі їх відсутності, тими, що вказуються виробниками (розповсюджувачами, правовласниками) ігрових дисциплін, що використовуються в якості рекомендованих, а також бути обладнаними усіма необхідними для проведення змагань, пристроями введення / виводу.

Для того, щоб зробити кіберспорт більш безпечним від дій кіберзлочинців, необхідно більше уваги приділяти впровадженню сучасних систем захисту інформації при підготовці гри, в процесі гри і при обробці результатів гри.

Треба здійснювати постійний контроль за працездатністю різноманіття обладнання, прикладних систем, бізнес-додатків, IT-сервісів, що використовуються на змаганнях. Автоматизація цих процесів, запобігання збоїв – повинно стати першочерговим завданням проведення проактивного моніторингу. Від розповсюдження гри до обслуговування клієнта кожен аспект ігрового досвіду також повинен бути захищеним. Необхідно запроваджувати тестування, допомогу експертів із кібербезпеки, індивідуальні рішення та багато інших заходів безпеки.

Перелік посилань:

1.8 технологічних революцій України. Революція восьма: кіберспорт.

URL: https://techiia.com/ua/news/8-tehnologichnih-revolyucij-ukrayini-revolyuciya-vosma-kibersport.

2.18000 Вісімнадцять три нуля.

URL: https://18000.com.ua/strichka-novin/rozvitok-kibersportu-v-ukrayini-ta-shho-vidomo-pro-nogo-v-cherkasax/.

3. Правила спортивних змагань з кіберспорту (електронного спорту).

URL: https://sport.gov.ua/storage/app/sites/16/Sport/Pravyla_zmagan/2020/pravila-kibersport.pdf.

ШИФРУВАННЯ ЛОКАЛЬНОГО ДИСКУ, ЯК МЕТОД ПРОТИДІЇ ВИТОКУ ІНФОРМАЦІЇ

Журавель Вячеслав Олександрович

Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

Шифрування локального диску серверу/персонального комп'ютера може бути дуже важливим в тих випадках, коли існує хоча б і не великий, але ризик того, что важлива інформація разом з диском може потрапити до рук тих, хто не повинен був її отримати.

До прикладів такої ситуації можна віднести:

- Персональний компьютер в офісі, в якому зберігаються сессії аккаунтів, паролі, важлива інформація, тощо. В даному випадку за відсутністю властника даної інформації, недоброзичливий коллега може отримати доступ до інформації властника за допомогою зовнішнього носія з встановленним Live-CD образом системи, що дозволить йому отримати доступ до інформації на накопичувачі навіть не знаючи пароль користувача.

- Мобільний телефон, на більшості з яких зберігається безліч персональних даних, таких як фото, відео, що були зняті на камеру пристрою, активні сессії соціальних мереж та мессенджери, збережені кредитні та дебетові карти, нотатки, додатки для двухфакторних авторизацій (Google Authenticator, SteamGuard, Authy, тощо), особисті повідомлення в СМС, та безліч іншої інформації.

- Виділенний сервер чи VPS/VDS може зберігати проприєтарні коди у випадку компаній-розробників, або докази у випадку опозиційних незалежних засобів массової інформації, тощо. У випадку виділенних серверів, отримати доступ до носіїв інформації зацікавлені персони можуть за допомогою атаки методом "груба сила" на IPMI серверу, якщо зацікавлена особа знає його IP-адресу. У випадку політичного переслідування, місцеві правоохоронні органи можуть зробити запит до хостинг-компанії, у якої зберігається обладнання, з вимогою предоставити побітову копію накопичувача серверу та усі персональні дані, що має хостинг-компанія на певну особу.

  Якщо сервіси знаходяться на VPS/VDS, то більшість компаній представляють додатковий доступ до серверу за допомогою NoVNC та аналогічних технологій, що дозволяють отримати доступ до зображення на сервері через HTML5. В такому випадку, зловмистник може отримати безпосередній доступ до особистого кабінету користувача та звідти

завантажитись в зовнішній .iso образ Live-CD системи, отримавши доступ до даних користувача.

Також важливо пам’ятати що для більшої безпеки, безліч компаній шифрує резервні копії своих файлів при завантаженні їх на сторонні сервіси хмарних сховищ.

Метою даної роботи є дослідження методів та єфективності шифрування дисків у найпоширеніших системах, таких як Windows, Linux, FreeBSD. Дані системи були вибрані завдяки широкому поширенню їх у повсякденному використанню.

Windows – це найпоширеніша система для персональних комп’ютерів та ноутбуків. Згідно статистиці від Statcounter, дана операційна система встановлена на 76.58% від всіх персональних комп’ютерів. Як і інші найпопулярніші операційні системи, Microsoft Windows має вбудоване програмне забезпечення для шифрування локального диску, а саме BitLocker, що доступний починаючи з Windows Vista. Розглядаючи найпоширенішу версію Windows на момент написання даного тезису, а саме Windows 10, важливо відмітити, що шифрування BitLocker недоступне для Windows 10 Home edition. В інших випадках, шифрування можна включити в налаштуваннях безпеки системи, в меню “Шифрування пристроїв”.[1]

У якості алгоритмів шифрування можуть використовуватися AES 128 та AES 256. Станом на 2021 рік, алгоритм AES ще не був успішно атакованим та є достатньо криптостійким рішенням серед доступних та був прийнятий урядом США як американський стандарт шифрування.

У якості отримання доступу можуть використовуватися три методи, що можуть поєднуватися між собою:

TPM;

PIN (не може бути використанний незалежно від інших);

USB-ключ;

Пароль.

Linux – найпоширеніша система для серверних операційних систем. Найбільш популярними рішеннями серед дистрибутивів є Ubuntu та CentOS. Згідно з статистикою W3Techs, системи на базі Unix та їм подібні займаюсь 77.4% від усіх серверних рішень, що використовуються в мережі Інтернет. Дані системи частіше за все використовують шифрування LUKS як шифрування за-замовчуванням.

У якості алгоритмів шифрування, LUKS також використовує AES, але при бажанні можуть бути альтернативно вибрані алгоритми Serpent, Twofish, CAST-128 та CAST-256.[2]

У якості отримання доступу для файлів використовуються ключі шифрування мастер-ключу. В системах LUKS можуть використовуватися до восьми ключів користувачів, які в свою чергу можна спробувати відгатати за допомогою атаки методом “груба сила”, а тому для них слід використовувати важкі комбінації з великими та малими буквами, цифрами, та спеціальними символами, а сам пароль має бути довгим. Для генерації такого паролю можна використовувати “пісок” з файлу /dev/urandom.

FreeBSD – доволі поширена система для побудування фаєрволів чи просто серверів з максимально стабільною операційною системою. Використання FreeBSD зумовлено тим що не дивлячись на повільну розробку системи, ядро та програмне забезпечення проходить детальне тестування на наявність помилок. Фаєрволл в системі FreeBSD (ipfw), згідно з інформацією з відкритих джерел, є більш стабільним та здатний працювати з більшою кількістю правил та запитів до нього, ніж (iptables) в Linux.

У якості шифрування за замовчуванням, FreeBSD використовує файлову систему ZFS з шифруванням програмним забезпеченням GELI, що може використовувати алгоритми AES, 3DES, Blowfish та Camellia. Також, як альтернатива, можна використовувати UFS, але за замовчуванням, рекомендується саме ZFS, що з недавнього часу перейшла на кодову базу OpenZFS.[3]

У якості висновків можна відмітити що існує безліч різноманітних методів шифрування файлових систем для різноманітних систем. Подібні механізми захисту існують і для систем на базах ОС Mac OSX, IOS, Android, тощо. Майже все сучасне програмне забезпечення підтримує сучасний алгоритм шифрування AES, що може гарантувати безпеку данних в найближчі роки. А у випадках відсутності необхідності в шифруванні всієї файлової системи, існує безліч програмного забезпечення для шифрування певних директорій чи окремих файлів.

Перелік посилань:

1. Изучаем и вскрываем BitLocker. Как устроена защита дисков Windows и как ее взломать. URL: https://xakep.ru/2017/02/23/bitlocker-hacking/
2. LUKS – Вікіпедія. URL: https://ru.wikipedia.org/wiki/LUKS
3. Geli (software) – Вікіпедія. URL: https://en.wikipedia.org/wiki/Geli_(software)

ВИКОРИСТАННЯ МЕТОДУ SWOT- АНАЛІЗУ В ОЦІНЦІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кукшин Дарія Вікторівна

Студентка групи БСДМ-51, ННІЗІ ДУТ,Київ,Україна

Бізнес не вічний двигун, запустивши який можна спокійно займатись іншими справами. Якщо ваша мета не просто відкрити компанію, а зробити її успішною, прибутковою та конкурентоспроможною, навчіться приймати об'єктивні та виважені рішення. Для цього необхідно чітко розуміти позиції компанії на ринку, можливі перспективи та наявні проблеми. І навряд чи щось допоможе розібратися в ситуації краще, ніж SWOT-аналіз. Цей метод завдячує своєю появою групі авторів книги Business Policy, Text and Cases, що побачила світ у 1969 році. Вже майже 50 років SWOT-аналіз залишається одним з найефективніших інструментів стратегічного планування.

Найважливіше завдання SWOT-аналізу — допомогти організації побачити та оцінити всі чинники, що впливають на прийняття рішень, а також визначити можливості розвитку.

Абревіатура цього терміну включає перші букви елементів аналізу і розшифровується як:

- Strengths (сильні сторони);
- Weaknesses (слабкі сторони);
- Opportunities (можливості);
- Threats (загрози).

Головною метою проведення SWOT-аналізу є отримання достовірних даних про можливості компанії і загрози просування її на ринку товарів і послуг. Тому, для досягення цієї мети перед SWOT-аналізом ставляться наступні завдання: виявлення маркетингових можливостей, які відповідають ресурсам фірми; визначення маркетингових загроз і розробка заходів щодо знешкодження їхнього впливу; виявлення сильних сторін фірми й зіставлення їх з ринковими можливостями; визначення слабкостей фірми та розроблення стратегічних напрямів їх подолання; виявлення конкурентних переваг фірми та формування її стратегічних пріоритетів[5].

Для здійснення SWOT-аналізу на підприємстві необхідне відповідне інформаційне забезпечення, яке повинно включати: базу даних; методи та моделі, необхідні для SWOT-аналізу; набір організаційних і методичних прийомів, необхідних для підвищення надійності інформаційного забезпечення[4]. Методика SWOT-аналізу ґрунтується на підході, який дає змогу

вивчати зовнішнє і внутрішнє середовище підприємства разом. За допомогою цієї методики можна встановити взаємозв'язки між силою та слабкістю, які властиві підприємству, і зовнішніми загрозами і можливостями. Спершу виявляють сильні і слабкі сторони, а також загрози та можливості, після цього встановлюють взаємозв'язки між ними, що може бути використано для розробки стратегії підприємства.

При проведенні SWOT-аналізу необхідно ретельно визначити сферу кожного SWOT-аналізу, зрозуміти відмінності між його елементами, бути об'єктивним і використовувати різносторонню вхідну інформацію, уникати просторових і двозначних заяв. SWOT-аналіз повинен проводитися за участю всіх найважливіших членів даної організації. Це стосується загальної ідентифікації слабких і сильних сторін, які усередині організації мають бути добре видні. SWOT-аналіз може виконуватися із застосуванням методу «мозкового штурму». Якість аналізу можна підвищити, залучаючи до його проведення осіб, що не відносяться до організації. Такі особи можуть виступити неупередженими арбітрами, які в змозі оцінити пропозиції, а також, ставлячи особливі питання, спровокувати організацію до переосмислення своїх положень і дій. При проведенні SWOT-аналізу, а особливо аналізу шансів і погроз, повинні використовуватися раніше проведені дослідження громадської думки [5].

Для визначення стану безпекового середовища та подальшої розробки стратегічних планів найчастіше використовуються методи стратегічного аналізу. Одним з найпоширеніших та якісних інструментів стратегічного планування є методика SWOT-аналізу. SWOT-аналіз не містить в собі економічних категорій, тому на сьогоднішній він зарекомендував себе як універсальну методологію, що використовується для формування стратегій у різних сферах життєдіяльності.

Тому цей метод використовують для оцінки ризиків і інформаційній сфері різні компанії та підприємства. Навіть для покращення стратегії розробки національної безпеки України. Таким чином керівники можуть вирішити, який ризик можна проігнорувати, щоб вирішити більш важливіші питання інформаційної безпеки. Для такої оцінки збирається повна інформація про діяльність підприємства і експерти проводять оцінку цих даних для побудови матриці SWOT – аналізу.

SWOT-аналіз в порівнянні з іншими методами має як переваги, так і недоліки. Основною його перевагою є простота і можливість витрачати невеликі кошти на його проведення, а також гнучкість і наявність безлічі варіантів. Також, це систематизація знань про внутрішні та зовнішні фактори, що впливають на процес стратегічного планування; можливість визначити конкурентні переваги

підприємства та сформувати стратегічні пріоритети, періодично проводити діагностику ринку та ресурсів підприємства. Недоліками SWOT-аналізу, які потрібно враховувати є: неможливість врахування всіх сил і слабкостей, можливостей і загроз; суб'єктивність вибору та ранжування факторів зовнішнього та внутрішнього середовища; погана адаптація до середовища, що постійно змінюється.

Перелік посилань:

1. SWOT-аналіз: кому, коли й навіщо потрібен. Стаття.- [Електронний ресурс]. – Режим доступу: https://bakertilly.ua/news/id44448
2. Згуровський М.З., Перевезра К.В. Методика побудови сценаріїв розвитку України з використанням SWOT-аналізу / М.З. Згуровський, К.В. Перевезра // Системні дослідження та інформаційні технології. – 2014. – № 2. – С. 7–17.

Застосування методів стратегічного планування через визначення актуальності загроз безпеки інформації промислових підприємств. Монографія / А.А. Христолюбова. – К.: НІСД, 2010. – 288 с

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. АТАКИ НА UEFI

Каленський Юрій Миколайович

Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

Публікація актуалізує проблему поширення складних атак на UEFI. Перехід більшості нових комп'ютерних систем на технології з новими методами захисту та виправленими «концептуальними вразливостями» не є панацеєю від атак нового типу. Ігнорування сучасних трендів в сфері кібербезпеки негативно впливає на шанс комп'ютерної системи залишатись неатакованою, тому їх необхідно освітлювати. Підсумовуючи, спеціалістам будуть запропоновані рекомендації, виконання яких допоможе знизити ризик стати жертвою кіберзлочинців.

Ключові слова: бекдор, кібербезпека, UEFI, BIOS, шпіонаж, rootkit, bootkit, викрадення даних.

UEFI (Unified Extensible Firmware Interface, уніфікований розширюваний мікропрограмний інтерфейс) – це передова технологія, яка використовується в деяких чіпах сучасних комп'ютерних систем (КС). Вона прийшла на зміну традиційній системі BIOS, зазвичай застосовується для прискорення початкового завантаження комп'ютера і операційної системи (ОС) і володіє багатими функціональними можливостями [1].

Протягом тривалого часу UEFI залишалась надійною технологією для запуску обладнання при включенні КС – як з технічної точки зору (підтримка великих розділів диску, графічний інтерфейс, налаштування без встановленої ОС (в тому числі й через мережу) тощо), так і з точки зору безпеки (Secure boot). Проте й UEFI став жертвою зловмисників, які навчились використовувати вразливості та особливості роботи для зараження комп'ютеру шкідливим програмним забезпеченням (ШПЗ).

Проблема атак на UEFI полягає у тому, що необхідне шкідливе навантаження відбувається до запуску ОС та її антивірусних компонентів, унеможливлюючи використання стандартних методів боротьби з ШПЗ. А технологія Secure boot, що покликана захистити комп'ютер від запуску нелегітимних EFI-додатків, вочевидь, була подолана.

На сьогодні відомо про два вектори ураження КС з технологією UEFI: імплантування в флеш-чіп SPI та редагування окремих EFI-додатків системного розділу EFI (EFI system partition, ESP).

Вперше про виявлення практичного використання UEFI в зловмисних цілях розповіли експерти компанії ESET. Дослідники заявили, що руткіт для UEFI використовувала російська група хакерів, відома як APT28 або Fancy Bear. Для впровадження руткіту зловмисники використовували ШПЗ LoJax – «близнюка» легітимного рішення LoJack від компанії Absolute Software, створеного для захисту пристроїв від втрати і крадіжки. Цей інструмент вбудовується в UEFI і дозволяє, наприклад, відслідковувати місцезнаходження пристрою або віддалено стерти дані. Хакери ж використовували «власну версію» рішення LoJack для шпигунства [2].

Другим випадком стало виявлення буткіту, який був частиною фреймворку MosaicRegressor. Експерти «Лабораторії Касперського» так і не змогли назвати точний вектор ураження системи, хоча припустили, що для ураження комп’ютеру необхідний фізичний доступ або компрометація механізму оновлення прошивки [1].

Вказані вище випадки підпадають під категорію імплантування в флеш-чіп SPI – компрометації прошивки шляхом імплантування нелегітимних компонентів, які можуть збирати дані про КС, інсталювати шкідливі модулі та бекдори й отримувати інші команди від інфраструктури управління та контролю (C&C infrastructure, C2). Відмінною рисою є й те, що технологія Secure boot не зможе захистити КС.

Два наступних випадки є представниками категорії, де «точкою входу» є ESP – буткіти, які редагують менеджер завантаження Windows *bootmgfw.efi*, що знаходиться в каталозі ESP за адресою \EFI\Microsoft\Boot\. Додавши нові секції, буткіт може встановити бекдор, а також встановити зв'язок з C2.

Першим представником цієї категорії, і третім загалом, став буткіт FinSpy – шпигунське ПЗ, яке може бути встановлено на ОС Windows, Linux, MacOS, Android та iOS. У випадку з Windows не відомо, яким чином відбувається зараження системи та подальша модифікація завантажувача [3].

Четвертим та «найновішим» став ESPecter – буткіт, який з 2012 року використовувалось для атак на системи з BIOS. Проте, цього року дослідники

виявили його оновлену версію для роботи не тільки з BIOS, а й з UEFI. Як і FinSpy, він модифікує *bootmgfw.efi* з встановленням бекдору та зв'язоку з C2 [4].

На жаль, спеціалісти до сих пір не знають, яким чином відбувається зараження згаданими буткітами, але існує декілька версій:

- Фізичний доступ до КС;
- Вимкнений Secure boot;
- Використання невідомої вразливості UEFI;
- Використання відомої непропатченої вразливості UEFI.

Атаки на UEFI, судячи з кількості згаданих випадків, є явищем досить рідкісним, проте втрати від вдалої атаки цього типу можуть бути катастрофічними. Тому доцільним є наведення рекомендацій, дотримання яких підвищить шанси виявлення цього ШПЗ:

1. Необхідно використовувати останню версію прошивки;
2. Необхідно увімкнути Secure boot;
3. Рекомендується використовувати технологію Intel Boot Guard;
4. Рекомендується постійно оновлювати ОС;
5. Рекомендується використовувати рішення для контролю привілейованих користувачів – Privileged Account Management (PAM).

Перелік посилань:

1. MosaicRegressor: Lurking in the Shadows of UEFI. Posted on October 5, 2020, by Mark Lechtik, Igor Kuznetsov and Yury Parshin [Електронний ресурс] – Режим доступу: https://securelist.com/mosaicregressor/98849/
2. LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group. Posted on September 27, 2018, by ESET Research Team [Електронний ресурс] – Режим доступу: https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/
3. FinSpy: unseen findings. Posted on September 28, 2021, by GReAT [Електронний ресурс] – Режим доступу: https://securelist.com/finspy-unseen-findings/104322/
4. UEFI threats moving to the ESP: Introducing ESPecter bootkit. Posted on October 5, 2021, by Martin Smolár and Anton Cherepanov [Електронний ресурс] – Режим доступу: https://www.welivesecurity.com/2021/10/05/uefi-threats-moving-esp-introducing-especter-bootkit/

СЕРІАЛІЗАЦІЯ ТА ДЕСЕРІАЛІЗАЦІЯ. УРАЗЛИВІСТЬ ДЕСЕРІАЛІЗАЦІЇ.

Герніченко Гліб Дмитрович

Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

У публікації розглянуто вразливості процесу десеріалізації, як спосіб втілення різноманітних атак на додатки та API. Не дивлячись на важкість реалізації даної вразливості, вона може призвести до катастрофічних наслідків. Проте, спеціалісти можуть заздалегідь побудувати систему таким чином, що

ризики зводяться до мінімуму. У підсумку були запропоновані методи запобігання використання вразливості зловмисниками.

Ключові слова: серіалізація, десеріалізація, додаток, код, мови програмування.

Процеси серіалізації та десеріалізації часто використовуються у додатках, що базуються на принципах об’єктного моделювання. Серіалізація – процес переведення об’єктів та структур даних у послідовність байтів, у свою чергу, десеріалізація є зворотнім процесом[1]. Дані процеси використовуються для можливості перетворення об’єктів у формати, що забезпечують зручність зберігання, передавання тощо. Мають дуже широку область використання: RPC та IPC, протоколи передачі даних, веб-сервіси, брокери повідомлень, хешування, бази даних, файлові системи, кукі-файли, токени автентифікації API тощо [2].

Найпопулярнішими способами серіалізації та десеріалізації наразі є переведення об’єктів у формати JSON та XML. Проте велика кількість мов програмування пропонують власні методи, що надають великі можливості для розробників ПЗ, для гнучкого налаштовування серіалізації та десеріалізації. На жаль, ці ж методи можуть бути використані зловмисниками для реалізації багатьох видів атак. [3]

Незахищена десереалізація посідає восьме місце у рейтингу вразливостей OWASP. Це обумовлено складністю реалізації загроз, через необхідність модифікації експлоїтів та відповідної підготовки до атаки. Проте й ідентифікувати наявність загрози без участі відповідного спеціаліста часто буває неможливо, а збитки, які можуть виплисти з атак, що базуються на цій вразливості, можуть бути катастрофічними. [2,3,4]

Нижче наведено приклади реалізації атак, що базуються на використанні даної вразливості:

- React-додаток викликає набір мікрослужб Spring Boot, задля забезпечення незмінності коду. Реалізовано це, через серіалізацію стану користувача та відправкою його за запитом. Таким чином, зловмисник, може використати Java Serial Killer для віддаленого виконання коду на сервері додатка [2];
- На сторінці, що написана мовою PHP, використовується серіалізація об’єктів для зберігання суперкукі, що містять різноманітні дані про користувачів, помітивши це, зловмисник може змінити свою роль та отримати несанкціонований доступ до функціоналу адміністратора [2];

```
a:4:{i:0;i:132;i:1;s:7:"Mallory";i:2;s:4:"user";
i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
```

Рис.1 – Вигляд початкового суперкукі [2]

```
a:4:{i:0;i:1;i:1;s:5:"Alice";i:2;s:5:"admin";
i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
```

Рис.2 – Вигляд зміненого суперкукі [2]

- Використання вразливості десеріалізації Adobe's BlazeDS AMF (CVE-2011-2092). Дана вразливість надає змогу вказати довільні класи та властивості, що будуть вивантажуватись на цільовий сервер додатка. Наведений нижче код, демонструє приклад створення об'єкта з властивістю defaultCloseOperation, що відключить JVM цілком, що призведе до аварійного завершення роботи програми [4].

```
[RemoteClass(alias="javax.swing.JFrame")]
public class JFrame {
    public var title:String = "Gotcha!";
    public var defaultCloseOperation:int = 3;
    public var visible:Boolean = true;
}
```

Рис.3 – Код, що створює небажаний об'єкт [4]

Наведені приклади є лише невеликою та примітивною часткою того, що зловмисник може реалізувати через цю вразливість. Маючи достатню кваліфікацію та ресурси, особа може отримати повний доступ над додатком, викрасти цінні дані, або вивести складну систему з ладу.

Надійними способами боротьби з вразливістю згідно з OWASP [1] є:

- За можливістю приймати значення для десеріалізації лише з довірених джерел, або виставити параметри десеріалізації таким чином, щоб приймались лише примітиви;
- Перевіряти цілісність серіалізованих об'єктів, задля запобігання підміни даних та створення небезпечних об'єктів;
- Сурове обмеження типів даних при десереалізації;
- За можливістю запуск процесу десеріалізації в ізольованому середовищі;
- Звітування випадків виникнення помилок, винятків та довготривалої десеріалізації;
- Обмеження та контроль мережевих підключень до середовищ, що виконують десеріалізацію;
- Відслідковування десеріалізації;
- Правильне використання синтаксису та методологій безпеки мов програмування, при створенні коду процесу десеріалізації [3].

Перелік посилань:

5. Insecure deserialisation. [Електронний ресурс] – Режим доступу: https://portswigger.net/web-security/deserialization

6. A8:2017-Insecure Deserialization. [Електронний ресурс] – Режим доступу: https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization

7. Deserialization Cheat Sheet. [Електронний ресурс] – Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html

8. Deserialization of untrusted data. [Електронний ресурс] – Режим доступу: https://owasp.org/www-community/vulnerabilities/Deserialization_of_untrusted_data

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Єрмак Максим Володимирович

Студент групи БСДМ-51, ННІЗІ ДУТ, Київ, Україна

Дана робота розкриває актуальну проблему, яка нині стосується кожного – як захистити інформацію. Оскільки технології стрімко розвиваються майже щохвилинно, потрібно мати нові системи захисту інформації.

Текст допоможе зрозуміти наскільки цінна може бути інформація для людей, які намагаються зрозуміти загальну стратегію захисту інформації.

Неможна не згадати, що ця робота надає перелік термінів інформаційної, телекомунікаційної та інтегрованої систем.

Нині, в часи, коли електронна техніка та інформаційні технології розвиваються дуже стрімко, можливість створювати сучасні пристрої несанкціонованого отримання інформації збільшується. Найпоширенішим прикладом є вбудований пристрій, який встановлений на об’єкті інформаційної діяльності є технічним засобом негласного отримання інформації, який створює загрозу її витоку. Такі вбудовані пристрої вмонтовуються в засоби, які забезпечують роботу комп'ютерних систем та мереж і становлять більшу загрозу з боку хакерів, ніж загроза комп'ютерних вірусів. І таким чином збирається інформація, використання якої може призвести до банкрутства банків, компаній, приватних осіб та створити дестабілізацію в суспільстві або в країні. Для виявлення небезпечних пристроїв, необхідно мати певний обсяг компетенції.

Варто звернутися до НД ТЗІ, де подано терміни та визначення згідно із ДСТУ 3396.2, ДСТУ 2226, НД ТЗІ 1.1-003.

Так під інформаційно-телекомунікаційною системою в цьому НД ТЗІ розуміється будь-яка система, яка відповідає одному з трьох наведених ниже видів автоматизованих систем [1, с. 4].

Терміни тлумачаться так: [1, с. 4]

Інформаційна система – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

Телекомунікаційна система – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;

Інтегрована система - сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Концепція технічного захисту інформації розкриває основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації в Україні – це діяльність, що спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. Концепція технічного захисту інформації також визначає загрози безпеці інформації, стан її технічного захисту та систему технічного захисту інформації як сукупність суб'єктів, об'єднаних цілями та певними завданнями. У Концепції технічного захисту інформації зазначені принципи формування і проведення державної політики у цій сфері, описані основні функції організаційних структур.

Конкретні завдання у сфері захисту інформації, що розробляються на рівні певної організації, системи публічного управління чи держави в цілому, мають підпорядковуватися заздалегідь визначеній стратегії у цій сфері. Стратегія захисту інформації виступає основою для побудови комплексу заходів щодо

інформаційної безпеки. Суть організації стратегії захисту інформації полягає у пошуку оптимального компромісу між необхідністю використання конкретних засобів захисту і наявними ресурсами для реалізації цього захисту. У стратегії захисту інформації важливо визначити мету, критерії, принципи і процедури, необхідні для побудови надійної системи.

Отже, важливою особливістю загальної стратегії захисту інформації є проектування системи інформаційної безпеки, де визначаються напрями: визначення мети та задач захисту інформації, цільової установки об'єктів та суб'єктів захисту інформації; визначення загроз інформаційної безпеки; визначення рівнів протидії загрозам та побудова політики інформаційної безпеки [2, с. 476].

Список використаної літератури:

1. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТСЗІ СБ України No125 від 8.11.2005. (Серія видань «Тимчасове положення»).

2. Остапов С.Е. Технології захисту інформації: навч. посіб. / С.Е. Остапов, С.П. Євсеєв, О.Г. Король. Харків: ХНЕУ, 2013. 476 с.

ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА МЕТОДИ ПРОТИДІЇ ПРОГРАМАМ ВИМАГАЧАМ

Макеєв Микола Броніславович
Студент групи БСДМ-51,Ж ННІЗІ, ДУТ, Київ, Україна

На сьогоднішній день проблема програм вимагачів стоїть достатньо гостро. Такі програми виступають як одне з ключових етапів в багатьох відомих світових кіберінцидентах, що призвели до значних репутаційних та фінансових втрат. Вирішення проблеми таких кібернетичних атак повинно бути одним з пріоритетів.

Ключові слова: Програма вимагач, Kaseya VSA, DarkSide

Актуальність проблеми вимагачів

Протягом 2021 світ зазнав великої кількості інформаційних атак різного роду та виду. Внаслідок атак страждають як компанії приватного так і державного сектору. В цьому матеріалі мова буде йти про програми-вимагачі. Хоча цей тип атак є дуже старим, з часом він та зловмисники прогресують і використовують нові шляхи та підходи для досягнення своїх цілей.

В цьому матеріалі буде описано приклади атак вірусів вимагачів, та описані методи попередження та протидії таким загрозам. Для початку розглянемо актуальні атаки програм вимагачів 2021 року та наслідки атак.

- Атака на Kaseya VSA[1]

Програму вимагач було доставлено через заражену систему Віртуального керування розробленого Kaseya. Вимагач розповсюджувався по зараженій мережі серед клієнтів, які використовували дане програмне забезпечення. При зараженні цілі програма шифрує дані на серверах та робочих станціях компанії, що паралізує подальшу роботу компанії та приносить колосальні фінансові збитки.

- Атака на Colonial Pipeline Co[1]

Атака угрупування DarkSide на компанію Colonial Pipeline Co, яка займається постачанням Паливно-мастильних матеріалів по всьому східному узбережжі США. Атаку було проведено за допомогою компрометованого паролю від VPN сервісу компанії. Після зараження та виявлення атаки було припинено роботу трубопроводу та принесло колосальні збитки, та призвело до паралізування роботи та введення надзвичайного положення президентом Джо Байденом. Після проникнення в систему, зловмисники заразили мережу програмою шифрувачем.

- Атака на Brenntag[1]

Проводилась тією самою зловмисною організацією, що і Colonial Pipeline Co. Внаслідок атаки було захоплено велику кількість особистих даних клієнтів та працівників компанії, зашифровано велику кількість даних.

Усі вищеописані випадки призвели до великих фінансових та репутаційних втрат. Для реалізації шифрувача в повному обсязі, потрібен повний доступ до мережі жертви аби провести шифрування та викрадення даних. Тому при зараженні системи злочинці проявляють комплексний підхід до зараження систем. Так наприклад угрупування DarkSide кооперувалось з іншими

угрупуваннями для проникнення в систему компаній для проведення зараження шифрувальником.

Загальна класифікація

Програма вимагач (Ransomware)[1] це шкідливий програмний засіб основною метою якого є вимагання коштів з жертви шляхом викрадання, шифрування, або обмеженням доступу інформації. При досягненні своєї мети зловмисники отримують фінансові кошти в обмін на інформацію жертви. Основною проблемою шифрувальників є відсутність будь-яких гарантій зі сторони зловмисників. Основною ознакою цієї атаки є втрата доступу до ресурсів, інформації, та/або втрата контролю над системою вцілому. В обмін на доступ до заблокованих, або зашифрованих ресурсів, інформації або системи зловмисники вимагають грошову або будь-яку іншу винагороду.

Методи протидії

Для мінімізації та/або попередження збитків потрібно:

- Провести роботу по організації регулярного шифрування важливих даних та регулярне резервне копіювання даних;
- Встановлення та налаштування системи захисту (антивірусне забезпечення, IDS/IPS);
- Робота з персоналом та його регулярне навчання.

Слід враховувати, що атака програми вимагача це комплекс дій спрямований на компрометацію системи захисту компанії задля отримання особистої вигоди або досягнення глобальних цілей. Підхід до захисту своєї системи повинен мати в собі аналіз совєї системи захисту та випадків схожих атак задля виявлення слабких місць в корпоративній системі захисту.

Перелік посилань:

1. Ransomware [Електронний ресурс]. – 2021 – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Ransomware

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. КІБЕРБЕЗПЕКА КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ.

Григоренко Дмитро Юрійович

студент групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна

Кібербезпека – це тема, яка в наш час займає досить важливе питання. У даній статті розглядається проблема корпоративних інформаційних систем.

На сьогоднішній день інформація має найбільшу цінність в компаніях, але на жаль багато з керівників не розуміють цього. Також, є велика кількість способів створити захист для інформаційної системи. Потрібно створити «золоту середину», так як мала або велика кількість компонентів захисту негативно вплинуть на підприємство.

Ключові слова: кібербезпека, інформація, системи захисту.

В наш час компаніям доводиться стикатися з різними ризиками інформаційної безпеки. Терористичні атаки, пожежі, повені, землетруси та інші катастрофи можуть зруйнувати інформаційні системи. Тому організаціям дуже важливо докладати зусиль для забезпечення своєї здатності надійно захищати свої інформаційні активи та IT-інфраструктуру. Впровадження контролю безпеки має вирішальне значення для організацій, щоб забезпечити безперервність їх діяльності, а також моніторинг та оцінку їх ефективності.

В наш час існують безліч способів захистити інформацію, кожна компанія вибирає засоби безпеки відповідно до своїх потреб бізнесу та відповідних вимог безпеки. Ця вимога безпеки повинна бути чітко визначена в політиці захисту інформації, а політика безпеки визначатиме набір елементів управління, які забезпечуватимуть необхідний захист [1, с.292].

Існують декілька найбільш популярних проблем кібербезпеки корпоративних інформаційних систем з якими стикаються більшість компаній, а саме [2]:

1. Безпека даних. Частіше всього невеликі компанії піддаються більшому ризику, оскільки багато з них навіть не мають політики безпеки. Але кожна компанія ризикує бути зламаною. Моніторинг мережі - це одне з вирішення цього питання, до якого звертаються багато експертів і малі та середні підприємства, що мають обмеження в грошовій формі, щоб захистити себе від кіберзлочинців.

2. Проблеми резервного копіювання даних. Резервне копіювання даних – це те, що повинне бути в кожній організації. Нажаль в багатьох малих і середніх підприємствах цього не роблять. У поєднанні з проблемою номер один, безпека, хороший план резервного копіювання даних є останньою лінією захисту від успішної атаки. Якщо шкідливе програмне забезпечення заблокує інформаційні системи та запропонує викуп, ви можете проігнорувати викуп і використовувати свої резервні копії для перезавантаження системи. Залежно від частоти резервного копіювання ви можете втратити деякі дані, але це набагато краще,

ніж втратити всі дані або виплату викупу (немає жодної гарантії, що хоча б якісь данні вдасться повернути).

3. Хмара. Компанії витрачають великі суми грошей на розробку та встановлення програмного забезпечення для покращення своєї діяльності. Хмарні обчислення дозволяють вашому бізнесу отримувати доступ до програмного забезпечення в Інтернеті як послуги. Хмарні обчислення також є безпечним способом зберігання та обміну даними. Але нажаль багато підприємств не використовують дану технологію.

4. Проблеми з обладнанням та програмним забезпеченням. Багато підприємств стикаються з проблемами пов'язаними з терміном служби технологій, які вони використовують. Поширеною помилкою, яка часто допускається, є припущення, що термін служби ПК становить чотири-шість років.

5. **Незаконне програмне забезпечення.** За оцінками Business Software Alliance, 22 відсотки всього програмного забезпечення Північної Америки є неліцензійним. Багато організацій не усвідомлюють, що вони використовують незаконне або неліцензійне програмне забезпечення, і це може призвести до жахливих наслідків.

Основне, це те, що більшість компаній не хочуть витрачати велику суму на захист інформаційної системи. Деякі думають, що інформацію не зможуть викрасти так як одного брандмауера вистачить для захисту. Іноді буває, що цінність інформації менше чим потрібно витратити.

Список використаних джерел

1. Андреев ВА. Основи інформаційно! безпеки / В.І. Андреев, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест ; за ред. проф. В.О. Хорошка. - 2-е вид., доп. і перероб. - К. : Вид. ДУІКТ, 2009. - 292 с.
2. Studebaker K. The 5 Most Common IT Problems Your Company Faces [Електронний ресурс] / Kirk Studebaker. – 2017. – Режим доступу до ресурсу: https://www.coordinated.com/blog/5-common-it-problems

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Івахненко Маріанна Володимирівна

студентка групи БСДМ-53, ННІЗІ ДУТ, Київ, Україна

Технічний захист інформації - це діяльність, спрямована на забезпечення некриптографічними методами безпеки інформації (даних), що підлягає захисту відповідно до чинного законодавства, із застосуванням технічних, програмних і програмно-технічних засобів. Такого роду захист спрямований на збереження технологічних даних, ноу-хау, інформації з патентів, власних напрацювань або придбаних методик, ліцензій. Також методами і засобами технічного захисту забезпечується інформаційна безпека відомостей про фінансові операції організації, кредитах, контрагентів, персональних даних співробітників, керівництва, клієнтів і постачальників.

Ключові слова: захист, інформація, безпека, конфіденційність, шифрування.

Для створення ефективної системи захисту конфіденційної інформації необхідно діяти продумано і послідовно. Процес складається з декількох етапів:

- Всебічний аналіз наявних інформаційних ресурсів.
- Вибір концепції інформаційної безпеки, що відповідає специфіці й особливостям використовуваних даних.
- Впровадження засобів захисту.
- Розробка організаційних заходів захисту даних, що відповідають специфіці компанії.

Всі вжиті заходи повинні відповідати чинним законодавчим нормам, інакше виникнуть конфлікти правового характеру. В цьому відношенні співробітникам ІБ-служби необхідно постійно звірятися з нормами, вимогами та законами, щоб не допустити порушень і не втягнути підприємство в судові процеси. Правова основа повинна бути базою, на якій будується вся система захисту інформації на підприємстві.

Важливим етапом є вивчення ризиків і визначення джерел небезпеки. Від цього залежить ефективність системи захисту інформації. Якщо всі можливі загрози правильно визначені, небезпека витоку даних знижується до мінімальних значень. Необхідно виконати наступні дії [1]:

- скласти перелік усіх пристроїв, що містять конфіденційну інформацію. Крім цього, врахувати всі діючі та резервні канали зв'язку, як провідні, так і мережеві;
- визначити найбільш відповідальні ділянки, розмежувати доступ в приміщеннях, встановити систему контролю за переміщенням співробітників і сторонніх осіб;
- використовуючи результати аналізу, розрахувати величину збитку, визначити наслідки несанкціонованого доступу і шахрайського використання інформації;

- скласти перелік документів і інформаційних масивів, що підлягають першочергового захисту. Встановити рівень допуску і скласти списки довірених користувачів;
- створити службу інформаційної безпеки, яка є окремим підрозділом і, крім фахівців з безпеки, включає системних адміністраторів і програмістів.

Основними завданнями ІБ-служби є:

- загальний технічний захист інформації;
- виключення доступу і несанкціонованого використання конфіденційних даних;
- забезпечення цілісності інформаційних масивів, в тому числі при виникненні надзвичайних ситуацій (пожежі, стихійні лиха).

Методи, які використовуються для технічного захисту інформації, повинні відповідати специфіці підприємства. Серед них можна виділити найбільш ефективні заходи [2, с. 273]:

- криптографічний захист інформації (шифрування);
- використання електронного підпису для підтвердження авторства довіреного користувача;
- резервне копіювання баз даних і операційних систем;
- створення системи паролів для ідентифікації і аутентифікації співробітників;
- контроль подій, що відбуваються в інформаційній системі. Фіксація спроб входу і виходу, дій з файлами;
- застосування смарт-карт, електронних ключів в рамках системи допусків і обмеження переміщень працівників;
- встановлення і використання на комп'ютерах міжмережевих екранів (файрволів).

Крім цих заходів необхідно ввести процедуру перевірки і тестування співробітників з високим рівнем допуску. Рекомендується присутність ІБ-співробітника в приміщеннях, де проводиться обробка конфіденційних даних.

Перелік посилань:

1. Технології захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.
2. Митник К.Д. Мистецтво обману: метод. посібник / К.Д. Митник – NYC: Wiley Books. 2008 – 273 с.

АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК МЕТОД ПРОТИДІЇ КІБЕРАТАКАМ

Киричок Роман Васильович

ст. викладач

Ахтьоров Владислав Юрійович

студент БСД-42

Державний університет телекомунікацій

м. Київ, Україна

На сьогодні, через активну інтеграцію інформаційних технологій в роботу приватних організацій та державних установ, стрімкого зростання кількості шкідливого програмного забезпечення та реалізації за його допомогою кібернетичних атак, гостро постає питання забезпечення швидкого виявлення та нейтралізації негативного кібернетичного впливу.

Аналіз шкідливого програмного забезпечення є одним з превентивних методів протидії кібератакам, який використовується фахівцями в галузі інформаційної та кібернетичної безпеки. Дослідження даного питання дозволяє підвищити загальну ефективність систем захисту інформації, зокрема, що стосується оцінки, прогнозування збитків від кібератак та проведення розслідувань кіберінцидентів.

Аналіз шкідливого програмного забезпечення (ШПЗ) – це дослідження або процес визначення функціоналу, походження та потенційні наслідки його функціонування в системі певного шкідливого програмного забезпечення. Аналіз ШПЗ виконує декілька функцій при протидії кібератакам: визначення точних збитків та вектору атаки в інформаційній системі, розробка методів протидії на основі інформації зібраної під час аналізу, визначення вразливостей інформаційної системи до реалізації атак певного типу.

Можна виділити два основні напрямки використання даних отриманих при аналізі шкідливого ПЗ. Першим є формування сигнатурної бази. Сигнатура шкідливого ПЗ – це послідовність байтових даних, які характерні для даного ШПЗ. Під час аналізу файлів шкідливого ПЗ генерується сигнатура, яку можуть використовувати антивірусні ПЗ, детектори та монітори. Це допоможе в майбутньому запобігти реалізації атак на інформаційну систему.

Існують хешові (hash signature) та рядкові (string signature) сигнатури. Хешові – генерується при процесі хешування, тобто при перетворенні даних програмного забезпечення в рядок даних встановленої довжини за допомогою певного алгоритму [1]. Рядкові сигнатури являють собою короткий байтовий рядок з шкідливого програмного забезпечення. На відміну від хешових сигнатур вони можуть використовуватись для виявлення великої кількості ШПЗ. Рядкові сигнатури створюються вручну фахівцем з кібернетичної безпеки, адже потрібно виділити конкретну частину ШПЗ для формування ефективної сигнатури [2].

Другим напрямком є використання даних аналізу для визначення наслідків кібератаки та можливе зменшення збитків. Для цього аналізується структура ПЗ, принципи його роботи. Перш за все проводиться статичний аналіз, тобто проводиться робота з файлами без запуску шкідливого ПЗ. В результаті такого аналізу можна вивести первинну інформацію про об’єкт дослідження, перевірити наявність інформації про нього в відповідних джерелах, якщо робота проводиться над відомим шкідливим ПЗ. Корисним є метод пошуку рядків за допомогою якого можна знайти звернення до певних файлів, переходи по URL, IP-адреси. Щоб отримати більш детальну інформацію необхідно провести зворотну розробку (reverse engineering), яка дозволить отримати детальну інформацію про принципи роботи шкідливого ПЗ.

Наступним етапом буде динамічний аналіз, який надасть інформацію про поведінку ПЗ та дозволить вивести повну картину щодо кібератаки. При динамічному аналізі звертається увага на процеси в системі, використання її ресурсів. Також аналізується мережева активність ШПЗ – DNS-звернення, використані порти тощо.

В результаті проведення статичного та динамічного аналізів можна вивести класифікацію шкідливого ПЗ, що дасть змогу зручно описати його функціонал. Зазвичай класифікація включає в себе наступні типи шкідливого ПЗ: шпигунські програми, вимагачі, кейлогери, троянські програми, мережеві хробаки,

бекдори[3]. В більшості випадків ШПЗ відноситься зразу до кількох згаданих типів. При детальному аналізі структури ШПЗ можна визначити:

- залежності від операційних систем (чи може ШПЗ функціонувати на декількох ОС) або інших факторів;
- мережеву активність ШПЗ;
- наявність корисного навантаження;
- принципи пакування ШПЗ, якщо вони використовуються;
- точний функціонал ШПЗ;
- іншу інформацію.

Після надання класифікації та детального аналізу структури та принципів дії ШПЗ можна підрахувати збитки, які принесла кібератака, визначити заражені частини інформаційної системи та знайти уразливості в системі захисту, які були використані для реалізації кібератаки. До таких вразливостей можна віднести в тому числі людський фактор, якщо шкідливе ПЗ потрапило в інформаційну систему за допомогою методів соціальної інженерії використаних зловмисником.

Інколи на основі отриманих даних можна створити певні механізми відновлення системи від ураження шкідливим ПЗ. Як приклад проаналізувавши оперативну пам’ять пристрою на якому файли були зашифровані програмою-вимагачем можна віднайти ключі шифрування, які були використані цією програмою. Також при аналізу ШПЗ можна знайти інформацію, яка може вивести на зловмисника, яким була проведена кібератака.

Отже аналізуючи шкідливе програмне забезпечення можна створити сигнатури для подальшого попередження реалізацій атак з використанням даного ШПЗ, точно визначити наслідки кібератаки, зменшити збитки які принесла кібератака. На даний момент статичний та динамічний аналізи ШПЗ є невід’ємною частиною розслідувань кіберінцидентів та мають виконуватись фахівцями з інформаційної та кібернетичної безпеки для ефективної протидії кібератакам.

Література:

1. Michael S. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software / S. Michael, H. Andrew. – San Francisco: No Starch Press, 2012. – p.32

2. Szor P. THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE / Piter Szor., 2005. – p.36

3. Automatic Generation of String Signatures for Malware Detection / K.Griffin, S. Schneider, X. Hu, T. Chiueh. // RAID '09: Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection. – 2009. – №1. – p. 102–103.

КІБЕРБЕЗПЕКА: ЗАГРОЗИ, ВИКЛИКИ, РІШЕННЯ

Грищенко Ярослав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ, Україна

Надійна і захищена робота мереж передачі даних, комп'ютерних систем і мобільних пристроїв є найважливішою умовою для функціонування держави і підтримки економічної стабільності суспільства. На безпеку роботи ключових інформаційних систем загального користування впливає багато факторів: кібератака, порушення, викликані загрозою фізичної розправи, вихід з ладу програмного та апаратного забезпечення, людські помилки. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільності роботи інформаційних систем.

Метою дослідження даної проблеми стала актуальність питання в сучасному світі, де захист інформації в кіберпросторі стоїть вкрай гостро. Кібербезпека все частіше розглядається, як стратегічна проблема держави, яка комплексно зачіпає економіку країни, в тому числі взаємодія національних розробників програмного забезпечення і систем управління, виробників обладнання та компонентів для забезпечення безпеки інфраструктури. На практиці ж дане явище призводить до стрімкого зростання залежності від іноземних виробників і зниження рівня інформаційного захисту. Маючі на увазі вимушене використання «закритого» програмного та апаратного забезпечення в усіх сегментах інфраструктури, як для спеціальних державних відомств, так і громадянського сектора.

Уже найближчим часом залежність від іноземних виробників обладнання та розробників програмного забезпечення може досягти критичного рівня. Наприклад, попри створення віртуальної «залізної завіси», влада Китаю фактично визнали повну залежність і незахищеність внаслідок постійного використання програмної платформи для мобільних пристроїв Android (частка платформи на ринку Китаю за підсумками 2020 року – 86,4%), засновану на «відкритому» коді, але вона є підконтрольною спеціальним службам США [1, с.3]. З точки зору економіки це явище надає позитивний вплив на розвиток електронної промисловості і реального сектора, що використовують «відкрите» програмне забезпечення для виробництва мобільних пристроїв, але при цьому створює реальну загрозу для національної безпеки, переводячи її під контроль іноземних спецслужб.

Для того, щоб національна кібербезпека могла відповідати рівню провідних економічних держав, необхідні, в тому числі послідовні дії з боку держави, спрямовані на підвищення ефективності та розвиток системи взаємодії учасників ІКТ-галузі. У свою чергу підприємства розробники і виробники повинні приділяти особливу увагу питанню інформаційної безпеки в розроблюваної продукції, що випускається, пред'являючи підвищені вимоги до надійності і захищеності пропонованих рішень, і тільки в крайніх випадках і при необхідності підвищення ринкової орієнтованості окремих продуктів повинні використовувати рішення іноземних вендорів і розробників програмного забезпечення.

Головна проблема для України полягає в тому, що найбільші споживачі такої продукції не можуть відмовитися від продуктів зарубіжних вендорів на користь вітчизняних рішень. При цьому більшість державних відомств, маючи власні мережі і здійснюючи щорічні витрати на амортизацію (у тому числі на розробку телекомунікаційного обладнання та засобів захисту інформації), набувають імпортні рішення [2, с. 36-37]. Саме завдяки таким тенденціям, на думку експертів, для іноземних виробників в Україні крім цивільного відкривається додатковий ринок – ринок спеціального і державного призначення.

В якості вирішення може бути обрана популярна у світі аутсорсингова модель виробництва, згідно з якою розробка і вивід на ринок затребуваних продуктів можливі лише за умови тісної кооперації з зарубіжними і вітчизняними компаніями. Це дозволяє на етапі проектування сформувати концепцію нового продукту, пред'являючи йому затребувані ринком сучасні вимоги та передати стороннім спеціалізованим виробникам види робіт, які не є профільними для підприємства. Наприклад, такі види робіт, як організація схемотехніки пристрої, виробництво електронних компонентів, промислове серійне виробництво пристроїв, технічна підтримка і дистрибуція можуть бути передані спеціалізованим підприємствам галузі [3, с. 10-14]. Дана модель дозволяє з максимальною економічною ефективністю забезпечити розробку і виведення на ринок рішень згідно зі світовими стандартами виробництва в умовах обмеженого за часом циклу виробництва.

Таким чином, системний підхід до питань кібербезпеки на рівні держави охопить не тільки підвищення обізнаності щодо існування ризиків в кіберпросторі, створення національних структур, що займаються питаннями кібербезпеки, але і встановлення необхідних взаємин між різними групами учасників, в тому числі між галузями економіки, для розвитку аутсорсингової моделі виробництва. Комплексна програма по забезпеченню кібербезпеки, підкріплена системним плануванням, з одного боку, допоможе захистити економіку країни від збоїв, сприяючи планування безперервності бізнесу в різних секторах і захищаючи інформацію, що зберігається в інформаційних системах, і, з іншого боку, допоможе стимулювати виробництво і збут для вітчизняних інфокомунікаційних підприємств, знижуючи тим самим залежність країни від іноземних виробників і розробників і поставляючи на цивільний і спеціальні ринки повністю безпечні та сучасні рішення світового рівня.

Література:

1. CNews – [электронный ресурс]. http://www. cnews.ru/top/2013/03/13/android_zahvatil_kitay_vlasti_byut_trevogu_522278 – «Android захватил Китай. Власти бьют тревогу»
2. Boiko A. System Integration and Security of Information Systems [Електронний ресурс] / A. Boiko, V. Shendryk. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/313483965_System_Integration_and_Security_of_Information_Systems.
3. CNews – [электронный ресурс]. http://www. cnews.ru/top/2013/03/13/android_zahvatil_kitay_vlasti_byut_trevogu_522278 – «Android захватил Китай. Власти бьют тревогу»

ЗАХИСТ ВІД ВИТОКУ ІНФОРМАЦІЇ. РІШЕННЯ DLP

Костроміна Марія Олександрівна

студентка групи УБДМ-51, ННІЗІ ДУТ, Київ, Україна

Анотація

Розглянуто причини та канали витоку інформації з організації. Порівняно та оцінено можливій негативний вплив від загроз, які надходять inside та outside. Установлені необхідні дії, які націлені на збереження критичних даних від витоку сторонніми каналами зв'язку. Розглянуто рішення Data Leak Prevention від вендора Forcepoint, а також його ключові можливості та переваги

Ключові слова: персональні дані; загрози безпеці; конфіденційна інформація; контентний аналіз; політики безпеки.

Більшість корпоративних витоків даних відбувається не внаслідок спланованих технологічних зломів і атак, а набагато більш тривіальними шляхами. Зокрема, через співробітників організації, які навмисно або випадково сприяють витоку чутливих даних. Саме на запобігання такій ситуації орієнтовані DLP-рішення (Data Leak Prevention).

Згідно зі звітом IBM і Ponemon Institute Більше 50% організацій не можуть запобігти інсайдерські загрози. Витоку даних стоять організаціям мільйони доларів збитку і втрати репутації бренду.

DataInsider опитала 47 експертів з безпеки з метою сравнівніть ризики внутрішніх і зовнішніх загроз.

97% опитаних стверджують, що загрози, які виходять із середини, набагато складніше запобігти і виявити за допомогою універсальних заходів безпеки. Оскільки інсайдери мають доступ до конфіденційної інформації на регулярній основі і можуть знати, як ця інформація захищена.

Ще одна з причин того, що внутрішні загрози складніше запобігти, пов'язана з тим, що інсайдери не завжди навмисно загрожують безпеці даних компанії. Фактично, багато витоку даних в результаті внутрішніх загроз є абсолютно ненавмисними і за статистичними даними складають близько 90%. Це може бути втрата пристрою (ноутбук, телефон), використання незареєстрованих накопичувачів (флешка), помилки при відправці поштою і тд.

У 2020 році 43% бізнес-керівників C-Suite, які повідомили про витік даних, назвали в якості другої основної причини людський фактор, а середня вартість таких витоків даних склала 3,86 мільйона доларів. Незалежно від джерела, на виявлення і усунення таких порушень йде в середньому 239 днів.

Як відбуваються витоку даних? Якщо узагальнити, витоку даних відбуваються або через недоліки:

- Технологія (апаратна або програмна частина)
- поведінка користувача

Загрози через недоліки технологій:

• Шкідливі програми: трояни, шпигуни, віруси, черв'яки;

• Man-in-the-middle attack;
• SQL injection;
• Spoofing;
• Sniffing;
• Атаки грубої сили.

Поведінка користувачів:

• Випадковий інсайдер. Прикладом може служити співробітник, який використовує комп'ютер колеги і читає файли без відповідних дозволів авторизації. Доступ є ненавмисним, і ніяка інформація не передається. Однак, оскільки вони були переглянуті не уповноваженою особою, дані вважаються порушеними.

• Загублені або вкрадені пристрої. Незашифрований і розблоковано ноутбук або зовнішній жорсткий диск - все, що містить конфіденційну інформацію - пропадає.

• Шкідливий інсайдер. Ця особа навмисно отримує доступ до даних і / або ділиться ними з метою заподіяння шкоди фізичній чи юридичній особі. Зловмисний інсайдер може мати законний дозвіл на використання даних, але намір полягає в тому, щоб використовувати інформацію в особистих нелегітимних цілях.

• Шкідливі зовнішні злочинці. Це хакери, які використовують різні вектори атак для збору інформації з мережі або від окремої людини.

Что касается корпоративных решений, Gartner and Forrester выделяет четырех ведущих поставщиков DLP: Symantec, Forcepoint, McAfee и Digital Guardian (рис. 1).

Рис. 1 Рейтинг рішень DLP на ринку

Чому Forcegoint DLP? Forcepoint DLP усуває ризики, пов'язані з людьми, за рахунок прозорості і контролю всюди, де працюють співробітники і де зберігаються дані компанії (рис. 2). Дана система здійснює оцінку ризиків користувачів, щоб зосередити увагу на найбільш важливі події і прискорити дотримання глобальних правил обробки даних.

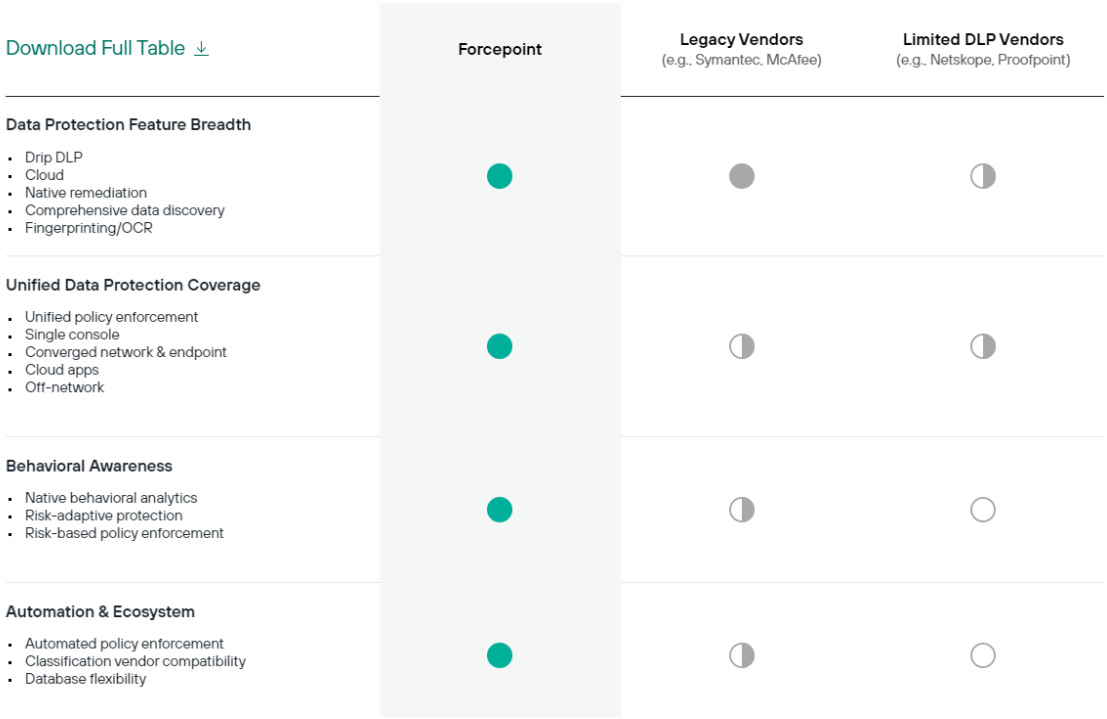


Рис. 2 Порівняльна таблиця рішень DLP

Рекомендації щодо зниження ризиків (згідно з технологією):

- чітка класифікація даних;
- рольова модель доступу до даних;
- на вузли, з яких можливий витік конфіденційних даних, встановити агенти DLP
- ретельна настройка правил в системі DLP (DLP-агент, встановлений на робочої станції, блокувати спроби користувача скопіювати на USB або відправити на друк конфіденційні документи. Факт підключення USB-накопичувача фіксується на агента, за результатами фахівець з інформаційної безпеки може змінити політику DLP- системи, включивши даний накопичувач в «чорні» або «білі» списки.) «чорні» або «білі» списки знімних носіїв, заборона не тільки на нелегітимність відправку за допомогою поштового сервера компанії чутливих даних, але і на друк, копіювання на носії , сторонніх поштових сервісів, соц. Мережі і тд.
- використання DLP в поєднанні з рішеннями по автоматичної класифікації даних (наприклад, Microsoft Information Protection, Titus, Boldon James)

Перелік посилань:

1. DLP Security Solution Forcepoint URL: https://www.forcepoint.com/product/dlp-data-loss-prevention
2. Що таке DLP-системи і навіщо потрібні DLP-рішення захисту від витоків даних? URL: https://www.devicelock.com/ru/dlp/data-loss-prevention/data-leakage-prevention.html
3. Принцип работы DLP-системы. Защита данных с помощью DLP-системы. URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/printsip-raboty-dlp-sistemy/

АНАЛІЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Борщ Дмитро Васильович

студент групи УБ351, ННІЗІ ДУТ, Київ, Україна

Ключові слова: **система захисту інформації, підприємство**

Актуальними проблемами, які стоять перед сучасними підприємствами – це проблеми пов’язані з забезпеченням інформаційної безпеки на підприємстві.

Адже стрімкий розвиток інформатизації виробництв, з постійно зростаючою вартістю інформації, з одного боку, і активність інформаційно-аналітичних структур і різного роду порушників, з іншого мотивують керівників підприємств більше уваги приділяти, саме інформаційній безпеці.

Бо, метою системи захисту інформації є:

- запобігання витоку, розкраданню, втраті, перекручуванню, підробці інформації;
- запобігання загрозам безпеці особистості, підприємства, суспільства, держави;
- запобігання несанкціонованого доступу щодо знищення, модифікації, перекручування, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси й системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, що існують в інформаційних системах;
- збереження конфіденційності документованої інформації відповідно до законодавства [1, с. 46].

Сучасні науковці, які досліджували проблематику інформаційної безпеки підприємств є: І. Арістова, І. Бачило, В. Брижко, В. Гавловський, Р. Калюжний, В. Копилов, В. Ліпкан, А. Марущак, В. Цимбалюк, М. Швець, Ю. Шемшученко та інші вчені. Адже наявність широкої різноманітності поглядів на окреслену проблему дозволяє отримати більш розгорнутий аналіз.

Деякі науковці вважають, що захист інформації є цілеспрямованою діяльністю власників інформації, спрямованою на виключення чи суттєве обмеження можливостей витоку, нав’язування, блокування або знищення інформації, що підлягає захисту [2, с. 126]. Одним із можливих шляхів наукового пошуку в обраному напрямі є дослідження захисту інформації як системи, тобто як цілісного утворення, що цікавить нас у своїй єдності, причому варто пам’ятати, що будь-який об’єкт становить систему лише щодо певної мети [3, с. 7].

З позиції теорії управління на загальному рівні система складається з керуючого й керованого об’єкта та створюється з урахуванням заданих вимог і наявних обмежень [2, с. 128].

Зауважимо, що відповідно до системного підходу, застосованого в науковій літературі, закономірності цілого (системи) безумовно домінують над її компонентами. Однак роль складників не варто зводити до становища суто пасивних частин. Будучи залежними від системи як цілого, компоненти мають певну відносну самостійність [4, с. 13].

Побудова системи захисту інформації здійснюється поетапно:

1 етап – визначення й аналіз загроз;
2 етап – розроблення системи захисту інформації;
3 етап – реалізація плану захисту інформації;
4 етап – контроль функціонування та керування системою захисту інформації [5].

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог захисту інформації для всіх періодів життєвого циклу об’єкта захисту. Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів технічного захисту інформації (далі – ТЗІ). Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ. Для технічних засобів інформації необхідно застосовувати спосіб приховування або спосіб технічної дезінформації.

Для забезпечення ТЗІ створюється комплекс технічного захисту інформації, що є складовою комплексних систем захисту інформації (КСЗІ).

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне та системне ПЗ.
- апаратна частина серверів та робочих станцій.
- комунікаційне обладнання та канали зв'язку.
- периметр інформаційної системи.

Системи захисту інформації на різних рівнях		
Рівні прикладного та системного ПЗ	*Апаратний рівень*	*Мережевий рівень*
• системи розмежування доступу до інформації; • системи ідентифікації та автентифікації; • системи аудиту та моніторингу; • системи антивірусного захисту.	• апаратні ключі. • системи сигналізації. • засоби блокування пристроїв та інтерфейс вводу-виводу інформації.	• міжмережеві екрани; • системи виявлення втручань; • засоби створення віртуальних приватних мереж; • засоби аналізу захищеності

Реалізація заходів щодо захисту інформації передбачає стадії проектування й будівництва об’єкта.

Важливо, щоб заходи з протидії виглядали правдоподібно та відповідали умовам обстановки, виконувались згідно з планами захисту інформації об’єкта. У зв’язку із цим розробляються й реалізовуються практичні заходи щодо маскування захисних заходів [6].

Таким чином, на сьогоднішній день пропонується безліч способів забезпечення безпеки інформації, але не всі вони є ефективними. Відомо, що тільки «комплексна система може гарантувати досягнення максимальної ефективності захисту інформації, оскільки системність забезпечує необхідні складові захисту і встановлює між ними логічний і технологічний зв'язок, а

комплексність, що вимагає повноти цих складових, всеосяжності захисту, забезпечує її надійність»

Перелік посилань:

1. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (14), 2007 р.
2. Шепета О. Адміністративно-правові засади технічного захисту інформації : дис. … канд. юрид. наук : спец. 12.00.07 «Теорія управління; адміністративне право і процес; фінансове право; інформаційне право» / О. Шепета ; Нац. академія Служби безпеки України. – К., 2011. – 215 с.
3. Кузьменко А. «Системный взгляд» на систему права / А. Кузьменко // Известия высших учебных заведений. Серия «Правоведение». – 2003. – № 3. – С. 4–11.
4. Костицька І. Політико-правова природа народного представництва / І. Костицька // Право України. – 2006. – № 10. – С. 9–14.
5. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. – К. : Держстандарт України, 1997. – 15 с.
6. Підприємство, господарство і право/ УДК 65.012.8+342.951:007. - А. Нашинець-Наумова, 2/2016. – 7 с.

ПІДТВЕРДЖЕННЯ ОСОБИСТОСТІ У КОРПОРАТИВНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Ганченко Марія Іванівна
студентка групи БСДМ-41, ННІЗІ ДУТ, Київ, Україна

Зазначення необхідності та доцільності проведення процедур ідентифікації, автентифікації та авторизації у комп'ютених системах підприємства для доступу до корпоративного інформаційного середовища на основі аналізу найрозповсюдженіших інцидентів інформаційної безпеки в Україні за осінній період 2021 року.

Ключові слова: корпоративна безпека, інформаційна безпека, інформаційні ресурси, ідентифікація, автентифікація, авторизація.

Корпоративна безпека – це проблема, що охоплює внутрішні і корпоративні бізнес-секрети компаній, дані співробітників, замовників [1]. Тому важливим етапом у побудові і підтримці корпоративної безпеки є використання сучасних інформаційних технологій, таких як: технології управління інцидентами і подіями інформаційної безпеки (далі - ІБ), технології управління уразливостями, системи безпеки корпоративних мереж, системи антивірусного захисту та продитії шпигунському програмному забезпеченню (далі - ШПЗ), системи управління обліковими записами користувачів і безпечного доступу до інформаційних ресурсів та даних.

Захист конфіденційних і персональних даних є основним завданням ІБ будь-якої компанії. Та, нажаль, корпоративні системи не стійкі до загроз викрадення даних, знищення робочого середовища співробітника або компрометації його облікового запису. Адже доступ до незашифрованих паролів та інформації для входу до систем є загрозою як для окремих облікових записів, так і для всієї корпоративної мережі.

За даними Державної служби спеціального зв'язку та захисту інформації України [2], яка щотижня проводить збір інформації та формує статистику [3] про зафіксовані та заблоковані атаки різних видів на державні інформаційні ресурси, можна визначити найрозповсюдженіші вразливості та підозрілі події, спрямовані на порушення конфіденційності та інших властивостей інформації: спроби отримання прав користувачів, спроби отримання прав адміністраторів, порушення корпоративної політики безпеки, виявлення мережевого ШПЗ, підозріле виконання коду. Зафіксовані та заблоковані інциденти за вересень та жовтень (до 20.10) 2021 року статистично подані на графіках (рис.1).

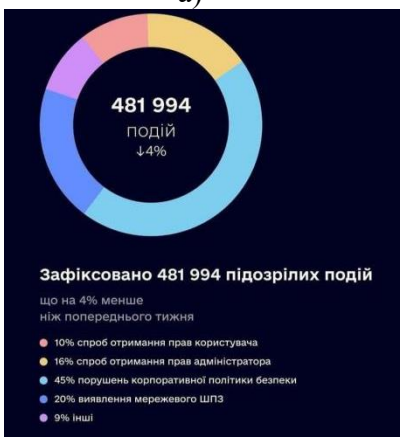
За наведеними графіками можна зробити висновок, що основна маса кіберінцидентів спрямована на отримання прав для доступу до інформаційних ресурсів, корпоративних даних (компрометація облікових записів користувачів) та порушення корпоративної політики безпеки (нестача чи втрата документів, посвідчень, перепусток, ключів, печаток та штампів, критичних відомостей, незаконне їх отримання і використання особами без прав). Такі ризики пов'язані з: низьким рівнем чи відсутністю системи охорони, захисту майна та контрольно-пропускних пунктів; низьким рівнем обізнаності персоналу з положенням про комерційну таємницю; відсутністю регулярної підготовки персоналу та

підвищення рівня кваліфікації кадрів з використанням сучасних інформаційних технологій; доступом до мережевих ресурсів підприємства з використанням особистих технічних засобів та за межами території без дозволів та відома керівних посадових осіб.

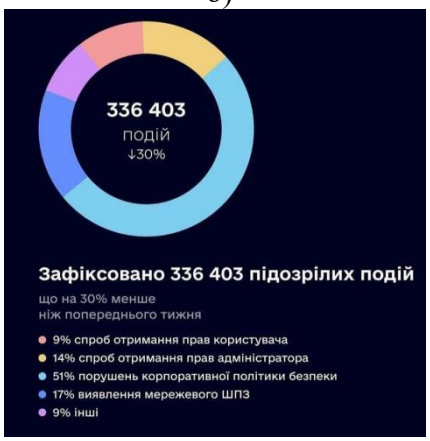
а)

б)

в)



г)



д)

е)

ж)

Рис.1. Статистика зафіксованих та заблокованих інцидентів за вересень та жовтень 2021 року: а) з 1 по 7 вересня; б) з 8 по 14 вересня; в) з 15 по 21 вересня; г) з 22 по 28 вересня; д) з 29 вересня по 5 жовтня; е) з 6 по12 жовтня; ж) з 13 по 19 жовтня

Тож безпека комп’ютерної системи підприємства є головною умовою забезпечення кібербезпеки корпоративних інформаційних ресурсів. А з огляду на те, що основним порушником вважається сам користувач, варто визначити,

що безпека попередньо зазначених процесів базується на трьох основних процедурах підтвердження особистості у інформаційному просторі: ідентифікації, автентифікації та авторизації. Ці заходи (рис.2) мінімізують вплив загроз (несанкціонований доступ, витік інформації) так як здійснюють контроль за отриманням доступу до даних відповідно до розроблених і прийнятих політик керування доступом користувачів та співробітників. Суб'єкти (користувачі, процеси) підтверджують свою ідентифікацію шляхом введення деякої унікальної інформації про себе до системи. Далі аутентифікація надає можливість стороні, що перевіряє суб'єкт, впевнитись у його автентичності. А рішення про надання доступу - авторизація, приймається системою лише після доведення користувачем своєї справжності.

Рис.2. Заходи щодо отримання суб'єктом доступу до інформаційної системи

Ґрунтуючись на вищезазначеному, доцільно стверджувати, що забезпечення безпечного доступу до корпоративних інформаційних сервісів, платформ, додатків та ресурсів є актуальним питанням на сьогоднішній день і вимагає підвищення рівня захищеності методів проведення процедур підтвердження особистості у корпоративному інформаційному середовищі. А ефективність використання таких заходів базується на: цілісності системи захисту; розширенні та контролі доступу; забезпеченні конфіденційності інформації, що зберігається та обробляється; мінімізації реалізації загроз та виникненню слабких місць.

Перелік посилань:

1. Що таке корпоративна безпека? [електронний ресурс] – Режим доступу: https://www.vmware.com/ru/topics/glossary/content/enterprise-security.html
2. Державна служба спеціального зв'язку та захисту інформації України. [електронний ресурс] – Режим доступу: https://cip.gov.ua/ua
3. Державна служба спеціального зв'язку та захисту інформації України. // @dsszzi // [електронний ресурс] – Режим доступу: https://instagram.com/dsszzi?utm_medium=copy_link

МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ СПЕЦІАЛІЗОВАНИХ ПРОЦЕСОРІВ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

Ярчук Андрій Андрійович

Державний університет телекомунікацій

Навчально-науковий інститут

м. Київ

Метою доповіді є постановка та рішення задачі оптимального резервування структури високопродуктивних процесорів, що будуються на базі непозиційної системи числення у залишкових класах (СЗК).

Однією з основних вимог, що пред'являється до сучасних комп'ютерних систем (КС), які працюють у реальному часі, є забезпечення заданого рівня надійності їх функціонування. Це пов'язано, перш за все, з тим, що вихід з ладу або навіть короткочасний збій у роботі таких КС може призвести до аварій або завдати серйозної економічної шкоди.

Існує два основні підходи для підвищення надійності КС підвищення надійності окремих логічних елементів (використання нової елементної бази) та введення різних типів надлишковості (застосування різних видів резервування).

Оскільки надійність елементів КС визначається рівнем розвитку технології, то очевидно, що введення надлишковості при використанні будь-якої елементної бази є найбільш ефективним шляхом підвищення надійності КС. У той же час, застосування кодів у СЗК дає можливість підвищити надійність КС за рахунок використання властивостей СЗК (малорозрядність, рівноправність та незалежність залишків). Це дозволяє більш ефективно застосовувати структурне резервування у порівнянні з кодами, що представлені позиційною системою числення (ПСЧ).

При використанні резервування, формулювання задачі оптимального резервування можливе в двох варіантах пряма задача, коли потрібно забезпечити ймовірність безвідмовної роботи КС не менше заданої, при мінімальних витратах; обернена задача, коли потрібно забезпечити максимально можливу ймовірність безвідмовної роботи КС при заданих витратах.

Список використаних джерел:

1. Computing System Reliability. Kluwer Academic Publishers; 2004; Available from: http://dx.doi.org/10.1007/b100619

2. Hongbin LI, Qing Zhao, Zhenyu Yang. Reliability modeling of fault tolerant control systems. Int. J. Appl. Math. Comput. Sci. 2007. Vol. 17, No. 4. P. 491–504. http://eudml.org/doc/207854.

КИБЕРАТАКИ 2021. СТАТИСТИКА ВИКОРИСТАННЯ КИБЕРЗОГРОЗ 2021

Кравчук В.В., студентка БСДМ-52

Державний Університет Телекомунікацій

м. Київ, Україна

Всесвітній економічний форум назвав кібератаки п'ятим за значимістю ризиком 2020 року. Оскільки 77% керівників служб безпеки прогнозують порушення критичної інфраструктури, для великих і малих підприємств важливо бути готовими до такого розвитку подій.

Кібератаки можуть відбутися в будь-який час, тому потрібно вчасно приймати правильні рішення. Атаки можуть бути активними або пасивними, відбуватися зсередини або зовні організації. Розпізнаючи атаки на ранній стадії, організації можуть заощадити гроші і запобігти подальшому доступу до конфіденційної інформації.

Кібератака - це шкідлива, здійснювана свідомо спроба людини або організації проникнути в інформаційну систему іншої людини або організації. Як правило, порушуючи роботу мережі жертви, хакер прагне отримати вигоду.

Підсумки I кварталу 2021 року:

- Кількість атак збільшилася на 17% в порівнянні з I кварталом 2020 року, а відносно IV кварталу 2020 року приріст склав 1,2%. Цілеспрямованими були 77% атак. Інциденти з приватними особами склали 12% від числа всіх інцидентів.

  -Шкідливе ПЗ, яке найчастіше використовують зловмисники, - це як і раніше шифрувальники. У I кварталі вони запитували нечувані суми викупу, допрацьовували свої інструменти, в тому числі додаючи нові способи приховування від засобів захисту. З'явилося безліч нових шифрувальників, наприклад Cring, Humble і Vovalex,

  -Найбільш популярними уразливими у зловмисників в цьому кварталі стали проломи в програмному забезпеченні Microsoft Exchange Server (ProxyLogon) і застарілою програмою для обміну файлами Accellion FTA. В VPN-рішеннях компанії SonicWall була виявлена уразливість нульового дня, скориставшись якою зловмисники не тільки зламали саму компанію, але і приступили до атак на клієнтів. Передбачається, що SonicWall своєчасно не оповістила клієнтів про виявлену уразливість і необхідності реалізації захисних заходів. Такий інцидент підтверджує, що виробники ПЗ повинні якомога швидше доводити до клієнтів інформацію про існуючі вразливості і про те, як захиститися до випуску патча.

Для захисту від кібератак потрібно дотримуватися загальних рекомендацій щодо забезпечення особистої і корпоративної кібербезпеки. Також, з огляду на специфіку атак в цьому кварталі, треба своєчасно встановлювати оновлення безпеки і приділяти особливу увагу захисту віртуальної інфраструктури. Зміцнити безпеку на периметрі компанії можна за допомогою сучасних засобів захисту. Щоб запобігти зараженню шкідливим ПЗ, можна використовувати

пісочниці, які аналізують поведінку файлів у віртуальному середовищі і виявляють шкідливу активність.

Кількість інцидентів в I кварталі 2021 року в порівнянні з аналогічним періодом 2020 року збільшилось на 17%, а відносно IV кварталу 2020 приріст склав 1,2%. На організації були направлені 88% атак. Найчастіше зловмисники атакували держустанови, промислові компанії і організації в сфері науки і освіти. Основним мотивом в атаках як на організації, так і на приватних осіб залишається отримання даних. Головними цілями зловмисників є персональні і облікові дані, а при атаках на організації до них додається ще й комерційна таємниця(рис.1).

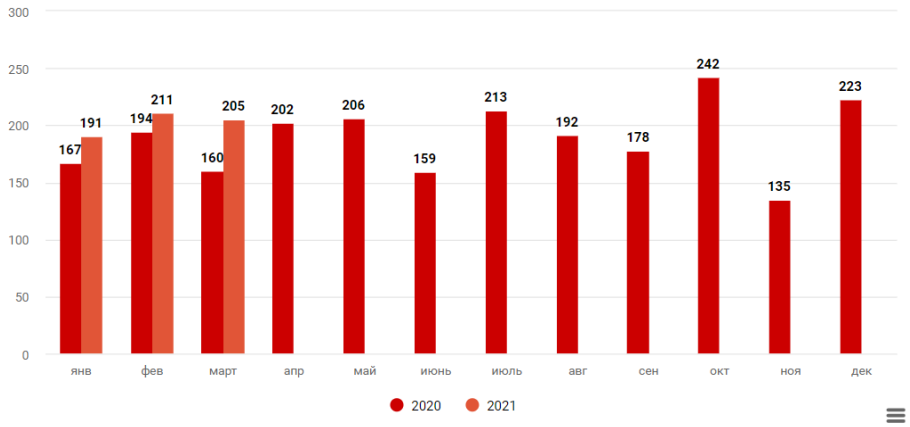


Рис.1 – Кількість випадків у 2020 та 2021 році

Діаграма нижче вказує які саме типи даних буди вкрадені зловмисниками у відсотковому відношенні(рис.2).

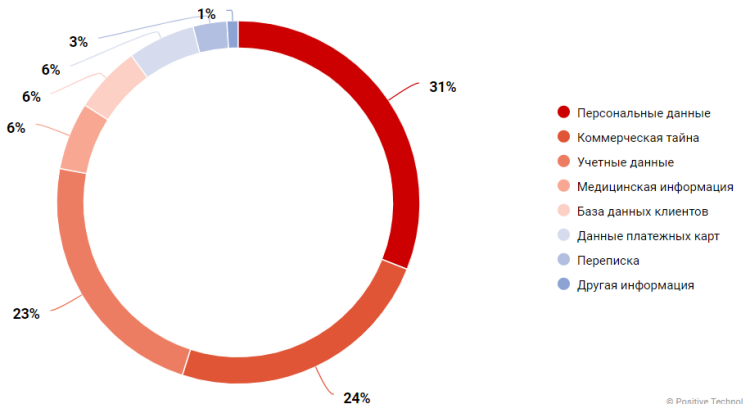


Рис.2 – Типи вкрадених даних(атаки на організації)

Найбільш популярним шкідливим ПЗ традиційно стали програми-вимагачі. Їх частка серед іншого ШПЗ, що застосовується в атаках на організації, збільшилася на сім процентних пунктів порівняно з IV кварталом 2020 року і становить 63%. Переважаючим способом доставки шкідливий залишається електронна пошта, зловмисники використовували її в шести з десяти атак на організації із застосуванням ШПЗ. Приватних осіб, як і раніше найчастіше атакують використовуючи банківські трояни, шпигунські програми і шкідливий, що надають віддалений доступ до пристрою. На наступній діаграмі вказані

найпоширеніші типи шкідливого ПЗ, яке використовується у проведенні атак зловмисниками(рис.3).

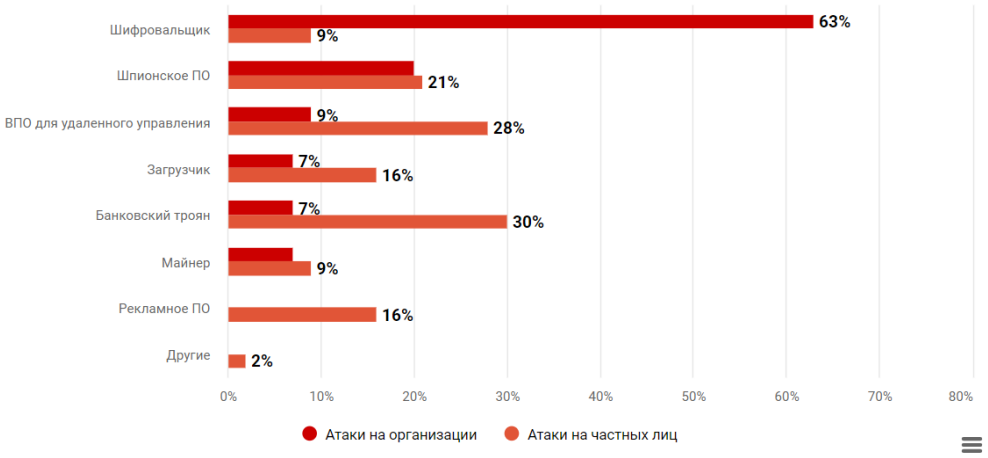


Рис.3 – Типи шкідливого ПЗ

Деякі зловмисники доповнили свої інструменти функціями, стирають сліди шкідливої активності. Подібне оновлення було помічено у Майнер OSAMiner, Black-T і Pro-Ocean. У коді кріптомайнера OSAMiner, орієнтованого на пристрої на платформі macOS, закладені функції, що дозволяють завершити процеси, пов'язані з інструментами моніторингу, наприклад, Activity Monitor і очистити систему від інших шкідників. Майнер Black T, націлений на Unix-системи, очищає історію в bash після реалізації корисного навантаження і затирає всі сліди своєї активності. Додана загальнодоступна функція для приховування процесу називається libprocesshider, в разі її виявлення фахівці з безпеки можуть припустити наявність шкідливої навантаження. Цим інструментом також користуються і зловмисники, які розповсюджують майнер Pro-Ocean, який атакує сервери Apache ActiveMQ, Oracle WebLogic і Redis, а перед установкою перевіряє середу запуску. На цьому етапі він визначає, чи потрібно приховувати шкідливе ПЗ, а якщо, наприклад, шкідливий виявився в середовищі Tencent Cloud або Alibaba Cloud - запускає процес видалення агентів моніторингу.

Використана література:

1. *Актуальные киберугрозы: I квартал 2021 года[Електроний ресурс]/ Режим доступу* - https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q1/
2. *Что такое кибератака?[Електроний ресурс]/ Режим доступу* - https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ЗАХИСТУ ІНФОРМАЦІЇ БАНКУ

Лабяк Дар'я Сергіївна

студентка групи УБД-41, ННІЗІ ДУТ, Київ, Україна

Активний розвиток банківського сектору потребує збільшення клієнтських баз з конфіденційною інформацією, через що питання захисту інформації в системах набуває більшої актуальності. Але для покращення та розуміння в якому стані знаходяться інформаційні системи (ІС) на даний момент, необхідно проводити аудит ІС, що наддасть оцінку всім використаним засобам та заходам при захисті.

Ключові слова: інформаційна система, аудит, оцінка.

Аудит інформаційної безпеки банку – це процес отримання якісної та кількісної оцінки про поточний стан інформаційної безпеки банку. Аудит проводиться з метою впевнитися, що всі співробітники дотримуються політик, законів та інших правил, що впроваджені в банку. Також під час аудиту можна виявити вразливості, які призводять до різноманітних атак. Аудит є важливою частиною існування та підтримування інформаційної безпеки в актуальному стані.[1]
На сьогоднішній день всі існуючі мережеві операційні системи мають багато вразливих місць зі сторони інформаційної безпеки. Тому необхідно проводити заходи боротьби із зломами та проникненням в інформаційні системи банку. Зазвичай за такими послугами звертаються до компаній, які надають послуги аудиту або наймають на роботу людину, яка може самостійно провести дані роботи. Але маємо пам'ятати, що є різні види аудиту, а саме: зовнішній аудит, та внутрішній аудит. Різниця в тому, що зовнішній аудит, разовий захід, який необхідно проводити регулярно. Особливо популярний для фінансових установ та акціонерних товариств.
Внутрішній аудит – це безперервна діяльність, яка виконується відповідно до плану з участю спеціального підрозділу.[2]
Цілями аудиту безпеки банку є:

- аналіз ризиків, що показує можливі загрози на ІС;
- оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки;
- вироблення рекомендацій щодо впровадження нових та підвищення ефективності вже існуючих механізмів безпеки ІС.

Також, аудит безпеки ІТ включає два типи оцінювання: ручне та автоматизоване.

Оцінки вручну відбуваються, коли зовнішній або внутрішній аудитор ІТ - безпеки опитує співробітників, переглядає засоби контролю доступу, аналізує фізичний доступ до обладнання та виконує перевірку вразливості. Такі огляди повинні проводитися щонайменше щорічно; деякі організації роблять це частіше.
До автоматизованої оцінки відносять генерування звіту оцінки інформаційних систем. Наприклад, можемо віднести до автоматизованої оцінки сканування

внутрішньої, так і зовнішньої мережі на наявність вразливостей за допомогою відомих сканерів Nessus, Qualys і т. д.

Не менш важлива частина аудиту це оцінка ризиків. Оцінка ризиків надає високорівневий огляд інформаційної інфраструктури банку, засобів інформаційної безпеки та мереж. Мета – це виявити зони вразливості та як впливає цей ризик на банківські системи. Оцінка ризиків має 6 важливих переваг.

1. **Визначення фінансових витрат.** Даний етап допомагає чітко визначити та обґрунтувати витрати необхідні для захисту ІС.
2. **Формулювання ризику та кількісна оцінка загроз.** Навчання співробітників та всіх зацікавлених сторін, щоб вони могли бачити не тільки вразливості, але й цінність зниження критичних ризиків. Оцінка ризиків безпеки допомагає виправдати інвестиції в безпеку.
3. **Покращення продуктивності ІТ відділу.** Шляхом формалізації структур, які допомагають в постійному моніторингу, ІТ відділ може зосередитися на активному перегляді та зборі документації, а не на захисних відповідях на загрози.
4. **Створення бази для самоперевірки.** Оцінка ризиків надає звіти, що показують необхідні заходи для того щоб всі працівники знали свою зону відповідальності за захист систем та інформації.
5. **Поширення інформації серед відділів.** Через не усвідомлення роботи іншого відділу, можуть виникати конфлікти в забезпеченні інформаційної безпеки. Даний етап допомагає отримати кожному розуміння, розвитку та покращення ІТ безпеки.
6. **Зламування бар'єрів між відділами.** Кожний відділ має співпрацювати один з одним, та виконувати всі правила задля зменшення загальних ризиків.

Щодо типу відповідності, то існує два основних– відповідність нормативним та галузевим вимогам. До нормативних відноситься наступне – Постанова №4 «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг». Дана Постанова вступила в силу з 21 січня 2021. Кожен банк України має щорічно або частіше проходити цей аудит в зазначений час.

До галузевих вимог відноситься Стандарт PCI DSS, що направлений на захист платіжних карток та даних. Даний стандарт визначає вимоги до програми захисту, критерії захисту даних та необхідні заходи безпеки. Стандарт оновлюється кожні декілька років задля актуальності. Цей аудит необхідно проходити кожному банку України, та не тільки.

Отже, розглянувши лише деякі моменти в аудиті банків, можемо сказати, що це велика система, що потребує системного підходу та постійного покращення.

1. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ [Електронний ресурс] – Режим доступу: http://unit.com.ua/ua/audit-informatsionnoj-bezopasnosti/ .
2. Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с.: ил. — (Серия «Для профессионалов»).

ДОСЛІДЖЕННЯ КІБЕРСКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ

Дьячук Олександр Станіславович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Дослідження кіберскладової інформаційної війни Російської Федерації проти України, інформаційний вплив та його складові, види та методи ведення війни сторонами, інформаційний спротив України, а також, проведення наступальної кібернетичної війни Україною.

З початком гібридної війни проти України Російська Федерація значним чином посилила інформаційний вплив на аудиторію України та західних країн. Основними характерними рисами такого впливу на населення України стало розповсюдження ідеї “русского мира” серед російськомовного населення. При цьому інформаційний вплив містить три складові.

Перша складова- пропагандистська. Вона спрямована на ту частину населення, яка частково або повністю не сприймає ідею розвитку України як самостійної держави. До цієї складової входять інформаційні повідомлення, що носить форму неприкритої дезінформації. При такому розкладі російську сторону абсолютно не турбує достовірність інформації, оскільки підтримка впевненості в діях РФ на території України серед такого роду аудиторії досить висока, інша точка зору,практично, не сприймається цією категорією населення. Інформація такого роду, переважно, розповсюджується на окупованій території Автономної Республіки Крим, та на окупованих територіях Донецької та Луганської областей.

Друга складова- інформаційно-просвітницька. Вона розрахована на ширшу аудиторію, і полягає у викриванні дій незаконної української влади проти власного народу. У формуванні і розповсюдженні такої інформації приймають участь частина українських засобів масової інформації, що певним чином, контролюються проросійськими політичними силами на території України. [1 с. 56-57]

Третя складова- інтернет-ресурси – розраховані на українську аудиторію. Особливо активно вони були задіяні на початковому етапі гібридної війни. Так, званий інтернет-тролінг був організований з метою впливу на активних користувачів інтернету в Україні.

Четверта складова- кібератаки. Спрямована передусім на дестабілізацію комп’ютерних систем і доступу до інтернету державних установ, фінансових та ділових центрів і створення безладу та хаосу в житті країни

Спроби агітації та розповсюдження інформації шляхом поширення чуток великого успіху не мали, ні на початковому етапі гібридної війни, ні сьогодні. Всі зазначені складові продовжують активно використовуватися Російською Федерацією в гібридній війні проти України.

Основний пропагандистський меседж Кремля в гібридній війні стосується розмежування братнього українського народу та київської влади, яка перебуває під зовнішнім управлінням. На Україну покладається провина за

невиконання Мінських домовленостей. Окупований Крим позиціонується як історично російський регіон, повернення якого відбулося відповідно до норм міжнародного права. [2 с. 24]

Стійкими тенденціями інформаційного впливу РФ на Україну в гібридній війні залишаються:

1. Підтримка функціонування пропагандистських каналів за кордоном, і формування потоків неправдивих повідомлень про Україну та її владу;

2. Подальший розвиток сучасних способів впливу на аудиторію за допомогою Інтернету, що включає активне використання соціальних мереж з одночасним обмеженням можливості всесвітньої мережі на власну аудиторію. Україна значною мірою узалежнена від Рунету та його інформаційних ресурсів. За оцінками експертів, щонайменше 50% усіх міжнародних зв'язків України зі всесвітньою мережею припадають на РФ. А завдяки популярності ресурсів ВКонтакте, Yandex та Одноклассников серед наших співвітчизників 55– 60% Інтернет-трафіка йде з країни-агресора. За даними Gemius, у травні 2021 р. у ТОП-10 найпопулярніших серед українців сайтів чотири були родом із РФ: vk.com і mail.ru (3-є і 4-е місця – відразу після google.com та youtube.com), yandex.ru та ok.ru (6-те е і 9-те місця) [3].

3. Спроби нанесення шкоди для критичної інфраструктури та органів державної влади, за допомогою шкідливого ПЗ та іншими методами. Наприклад 23 грудня 2015 року сталась перша у світі підтверджена атака, спрямована на виведення з ладу енергосистеми: російським зловмисникам вдалось успішно атакувати комп'ютерні системи управління в диспетчерській «Прикарпаттяобленерго», було вимкнено близько 30 підстанцій [3]. Також 29 серпня 2021 року на засіданні РНБО Президент України Володимир Зеленський заявив, що за останні 2 місяці в Україні було зафіксовано 2.5 тисячі кібератак. [4]

В умовах гібридної війни з РФ подолання Рунет-залежності є нагальним імперативом української інформаційної політики, і вимагає відповідних заходів владних структур, незалежних інтернет-організацій та кожного громадянина зокрема.

Список використаних джерел:

5. *Дубов Дмитро Володимирович // Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України*
6. *В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа// Інформаційна на кіберберзпека: соціотехнічний аспект*
7. *Інтернет-джерело: https://en.wikipedia.org/wiki/Russian-Ukrainian_information_war*
8. *Інтернет-джерело: https://www.mil.gov.ua/*

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДИЧНИХ ЗАХОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА ВІД СУЧАСНИХ ВИДІВ ЗАГРОЗ, КІБЕРАТАК І РИЗИКІВ

Якименко Юрій Михайлович

Доцент кафедри УІКБ, ННІЗІ ДУТ, Київ,Україна

Показана необхідність управління величезними потоками даних і захисту інформації від сучасних видів кібератак завдяки наявності на підприємстві системи управління інформаційною безпекою. Перелічені методи виконання кіберзлочинності: використання шкідливого програмного забезпечення; використанням шкідливих кодів і додатків, спрямованих на уразливості інформаційних систем для здійснення несанкціонованого доступу до баз даних, файлової системи локальної корпоративної мережі і інформації на робочих комп'ютерах співробітників; приведений спектр загроз інформаційній безпеці, викликаних використанням шкідливого програмного забезпечення; приведені нормативні документи, що містять методології управління ризиками; розкритий підхід до класифікування загроз; розкриті стандартні кроки, опис яких повинен бути присутнім в будь-якої методиці аналізу ризиків; показани особливості оцінки ризиків.

Ключові слова: захист інформації, загрози, управління ризиками, програмне забезпечення, підприємство

Для сучасних підприємств характерно стрімкий розвиток їх інформаційного середовища. Постійне накопичення інформації вимагає її належної обробки, зберігання та захисту. На сьогодні захист інформації від безлічі існуючих загроз на підприємстві [1] являє собою комплекс заходів, які спрямовані на те, щоб зберегти її цілісність, уберегти від крадіжки і підміни основних даних з:

- бази даних клієнтів і партнерів;
- електронного документообігу;
- технічних особливостей діяльності підприємства;
- комерційної таємниці.

Для успішного управління величезними потоками перерахованих даних підприємство повинно мати систему управління інформаційною безпекою (ІБ), яка виконує також і забезпечення захисту інформації від сучасних видів кібератак . Кібератаки сьогодні це реальна і серйозна небезпека для інформаційної інфраструктури, інтелектуальної і фізичної власності підприємства.

Найбільш поширеною і різноманітною за методами виконання кіберзлочинності є використання шкідливого програмного забезпечення (ПЗ). Такі загрози

становлять пряму небезпеку конфіденційності і цілісності інформаційних ресурсів підприємства.

В атаках з використанням шкідливих кодів і додатків, спрямованих на уразливості інформаційних систем для здійснення несанкціонованого доступу до баз даних, файлової системи локальної корпоративної мережі і інформації на робочих комп'ютерах співробітників. Спектр загроз ІБ, викликаних використанням шкідливого ПЗ надзвичайно широкий [2], деякі з них:

- впровадження вірусів і інших руйнівних програмних впливів;
- аналіз і модифікація / знищення встановленого ПЗ;
- впровадження програм-шпигунів для аналізу мережевого трафіку і отримання даних про систему та стан мережних з'єднань;
- використання вразливостей ПЗ для злому програмного захисту з метою отримання несанкціонованих прав читання, копіювання, модифікації або знищення інформаційних ресурсів, а також порушення їх доступності;
- розкриття, перехоплення і розкрадання секретних кодів і паролів;
- читання залишкової інформації в пам'яті комп'ютерів і на зовнішніх носіях;
- блокування роботи користувачів системи програмними засобами.

На даний момент в світі розроблено безліч стандартів, рекомендацій та інших нормативних документів, що містять як методології управління ризиками, так і основні підходи до цього важливого процесу. Найпоширеніші світові практики управління ризиками ІБ визначені в NIST 800-30, ISO / IEC 27005, COBIT, ITIL, OCTAVE і ін. Але, тим не менш, відповідно до цих стандартів, основою для проведення аналізу ризиків ІБ і найважливішою стороною визначення вимог до системи захисту є формування моделі потенційного порушника, а також ідентифікація, аналіз і класифікація загроз з подальшою оцінкою ступеня ймовірності їх реалізації.

Для того щоб правильно визначити можливі загрози, в першу чергу, необхідно визначити які об'єкти підлягають захисту. До таких об'єктів можуть відноситись як матеріальні, так і абстрактні ресурси, наприклад, документи та інші носії інформації, приміщення, обладнання системи, а також співробітники і клієнти. Наступним етапом визначення можливих загроз є розгляд і класифікація тільки тих, які можуть вплинути на роботу системи і організації в цілому, а, часом, і привести до негативних наслідків. В залежності від розташування джерела загроз прийнято виділяти внутрішні і зовнішні загрози, тобто загрози розташовані всередині контрольованої зони (псування устаткування, інсайдерські загрози) або за її межами. У більшості стандартів по-своєму також здійснюється і

класифікація можливих джерел загроз. Додатково можна класифікувати загрози за ступенем впливу на системи і за способом доступу до ресурсів, що захищаються. За ступенем впливу розрізняють пасивні та активні загрози.

За способом доступу до ресурсів, що захищаються прийнято розділяти на загрози, які використовують стандартний доступ, наприклад, незаконне отримання облікових даних шляхом підкупу, шантажу законного володаря, або, загрози, які використовують нестандартний (прихований) доступ - використання декларованих можливостей засобів захисту і програмних закладок в ПЗ (в обхід наявних в системі засобів захисту інформації). До того ж часто зустрічається класифікація по використанню порушниками фізичного і технічного доступу.

Таким чином, класифікацію загроз, характерних для тієї чи іншої системи можна уточнювати, грунтуючись при цьому або на методологіях, описаних у вітчизняних і зарубіжних стандартах, або використовуючи практичний досвід, але в будь-якому випадку їх перерахування є важливим етапом визначення вразливостей і створює фундамент для майбутнього проведення аналізу ризиків.

Ідентифікувати і оцінити активи, розробити модель порушника і модель загроз, ідентифікувати уразливості - все це стандартні кроки, опис яких повинне бути присутнім в будь-якій методиці аналізу ризиків [3]. Всі перераховані кроки можуть виконуватися з різним рівнем якості і деталізації. Дуже важливо зрозуміти, що і як можна зробити з величезною кількістю накопиченої інформації, в тому числі і формалізованою за допомогою моделей.

Отримані результати необхідно оцінити, агрегувати, класифікувати і відобразити. Так як збиток визначається на етапі ідентифікації та оцінки активів, необхідно оцінити ймовірність появи подій ризику. Як і у випадку з оцінкою активів, оцінку цієї ймовірності можна отримати на підставі статистики по інцидентах, причини яких збігаються з розглянутими загрозами ІБ, або методом прогнозування - на підставі зважування чинників, відповідних розробленої моделі загроз. При цьому слід зазначити, що в процесі ідентифікації та оцінки вразливостей активів дуже важливий експертний досвід фахівців з ІБ, що виконують оцінку ризиків і використовують статистичні матеріали, звіти по вразливостям і загрозам в області ІБ.

На підставі отриманих результатів можна виходити на розробку найбільш достовірних рекомендацій щодо захисту інформації від кіберзагроз та підвищенню рівня забезпечення ІБ підприємства [4].

Перелік посилань:

1. Угрозы информационной безопасности в АС.

URL: http://asher.ru/security/book/its/05.

2. Анализ угроз информационной безопасности.

URL: http://ypn.ru/106/analysis-of-threats-to-information-security/4/

3. Анализ рисков в управлении информационной безопасностью

URL:http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi-bezopasnostyu

4. Организационные меры защиты информации на предприятии

URL:https://easyncam.ru/organizatsionnye-mery-zaschity-informatsii-na-predpriyatii/.

СПОСОБИ ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ У ФОРМАТІ“DEEPFAKE”

Недодай Михайло Геннадійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Технології створення дезінформації покращуються з кожним роком, створюються нові шляхи розповсюдження, нові методи просування в соціальних мережах. А нещодавно до цього списку додався штучний інтелект з його можливостями простого створення фотореалістичної інформації.

В сучасному світі завдяки Інтернету можна як отримувати будь-яку інформацію за лічені хвилини, так і створювати контент для інших. Тому важливо, щоб інформація була достовірна. Тема цифрової гігієни в багатьох країнах лише набирає обертів, а перевіркою фактів займається лише невелика кількість людей, та деякі профільні агентства. Це все створює гарні умови для ведення інформаційних війн, пропаганди та іншого інформаційного впливу на людей. Все більше новин про виявлення ферм ботів, що розповсюджують неправдиву інформацію [1]. А завдяки можливостям штучного інтелекту можна створювати реалістичні фото, відео та тексти з неправдивою інформацією навіть силами однієї людини.

Deepfake - методика синтезу зображення людини з застосуванням штучного інтелекту [2] . Сьогодні, одна з найпопулярніших программ для створення відео-deepfake- DeepFaceLab [3] знаходится у відкритому доступі і кожен бажаючий навіть без знання програмування може на персональному комп’ютері з потужним графічним прискорювачем створити власне deepfake відео. Приклад роботи алгоритму на Рисунку 1 та Рисунку 2 [4]. Так, можна виділити три основні напрямки deepfake відео контенту:

1. Заміна обличчя, коли у відео обличчя актора автоматично підміняється обличчям іншої людини. Цей тип техніки застосовувався для вставки голів відомих акторів у різноманітні фільми, в яких вони ніколи не з'являлися. А ще – для створення порнографії без згоди згаданих осіб.
2. Синхронізація губ, за якої вихідне відео модифіковане таким чином, що область рота узгоджується з неоригінальним, іншим аудіо записом.
3. "Лялькovод", в якому зображення людини (рухи голови, рухи очима, міміка) анімує виконавець, що сидить перед камерою і виконує дії, які він хоче бачити на відео від "ляльки".

Найскладніший метод - заміна обличчя, для якого потрібно навчати нейронну мережу домальовувати обличчя “донора” на відео з “реципієнтом”. Так можна створювати контент, що буде показувати конкретну людину в

ситуації, в якій вона не була, наприклад створення порнографії, або виступ політика на якому його не було. Через досить гарну реалістичність, а також можливість подальшої обробки відео для усунення “артефактів” нейронної мережі такий контент є досить переконливим для людей. Метод “ляльковод” є простішим в реалізації, але в той час може нести більше інформаційне навантаження на аудиторію. Адже він дозволяє створити реалістичну анімацію обличчя за допомогою лише камери комп’ютера та потужного графічного прискорювача. За допомогою такої анімації можна зачитати текст повідомлення політика, який він ніколи не казав і подати це як інфопривід.

Для розпізнавання deepfake контенту пропонується використовувати штучний інтелект, що буде тренуватись розрізняти згенеровані зображення так само, як і в алгоритмі що створює deepfake. Також можливо додатково шукати першоджерела deepfake контенту - відео на яке наклали обличчя, фотографії що використовуються в методі “Ляльковод”, перевіряти метадані відеозаписів та джерела які поширюють підозрілий контент.

Рисунок 1 Результат заміни обличчя.

Рисунок 2 Процес заміни обличчя.

Список використаних джерел:

9. Інтернет-джерело: https://ssu.gov.ua/novyny/sbu-likviduvala-botofermu-yaka-pratsiuvala-na-zryv-natsionalnoi-prohramy-vaktsynatsii-v-ukraini

10. Інтернет-джерело: https://uk.wikipedia.org/wiki/Deepfake

11. Інтернет-джерело: https://github.com/iperov/DeepFaceLab

12. *Інтернет-джерело:*

УДК 004.056:621

О. О. Коваленко, студент
Державний університет телекомунікацій

ОСОБЛИВОСТІ КЕРУВАННЯ ПЕРСОНАЛОМ НА ПІДПРИЄМСТВІ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКи

Розглянуто Особливості керування персоналом на підприємстві у галузі інформаційної безпеки. Проаналізовано особливості керування персоналом на підприємстві у галузі інформаційної безпеки.

Здійснення зовнішньоекономічної діяльності підприємством, випуск продукції, яка була б конкурентоспроможною на зарубіжних ринках, залежить не тільки від технічного оснащення підприємства, наявності сучасних технологій, чітко поставленої системи контролю якості продукції, маркетингових досліджень ринкового середовища та послідовного впровадження концепції просування товарів на зарубіжні ринки, а й від кваліфікації співробітників підприємства, ефективного управління персоналом.

Управління персоналом набуває дедалі більшого значення як чинник підвищення конкурентоспроможності підприємства, досягнення успіху в реалізації його стратегії розвитку.

Управління персоналом можна визначити як діяльність, що спрямована на досягнення найбільш ефективного використання працівників для досягнення цілей підприємства та особистісних цілей. Перші, традиційно, пов'язуються з забезпеченням ефективності підприємства. Причому ефективність іноді розуміється у вузькому значенні - як отримання максимального прибутку. Однак дедалі частіше ефективність розглядається не тільки в економічному плані - як економічність, якість, продуктивність, нововведення, прибуток, а і в більш широкому контексті й пов'язується з такими поняттями особистісного, психологічного плану, як задоволеність співробітників своєю працею, участю у трудовому колективі підприємства, високий рівень самооцінки колективу, мотивація персоналу до ефективної праці.

Метою роботи є дослідження особливостей управління персоналом підприємства та удосконалення керування персоналом на підприємстві у галузі інформаційної безпеки.

Для досягнення поставленої мети були поставлені та вирішені такі завдання:

- вивчити методолічні основи управління персоналом підприємства у галузі інформаційної безпеки;
- проаналізувати основні методи та технології управління персоналом на підприємстві у галузі інформаційної безпеки;
- вивчити існуючі концепції управління персоналом підприємства;
- розробити рекомендації по удосконаленню управління персоналом на підприємстві у галузі інформаційної безпеки.

Об'єктом дослідження є система управління персоналом на підприємствах, орієнтована на підвищення її економічного успіху і конкурентоспроможності.

Предметом дослідження є особливості керування персоналом на підприємствах в галузі інформаційної безпеки.

В результаті опрацювання наявного наукового матеріалу та проведених досліджень повинно бути виокремлено основні моменти управління персоналом, що мають визначальний вплив на успішне функціонування промислового підприємства, визначено найсуттєвіші принципи планування, організації, регулювання, контролю та оцінки трудових ресурсів.

Література:

1. Базаров Т.Ю. Управление персоналом. К., 2001
2. Баканов М.И. Анализ хозяйственной деятельности в торговле: Учеб.пособие. - Москва.: Экономика, 1997
3. Барановский А.Б., Потапенко Г.М., Щекин Г.В. Система методов профессиональной ориентации. Основы профессиональной ориентации:Учебно-методическое пособие.–К., 1991. -231с.

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ З ВИНИ ПЕРСОНАЛУ

А. В. Жовтюк – Державний університет телекомунікацій

Актуальність обраної теми обумовлена участю у порушеннях інформаційної безпеки інсайдерів, які складають близько 80% зловмисників. У компаніях телекомунікаційної сфери вони створюють передумови та, що призводять до величезних фінансових втрат.

Таким чином, з огляду на значні обсяги втрат та шкоди підприємству внаслідок загрозливих дій персоналу, а також відсутність достатніх заходів для захисту або протидії від дій інсайдерів, необхідним є вивчення та аналіз різних видів загроз інформаційній безпеці підприємства з вини його працівників.

З огляду на зазначене, використання результатів дослідження сприятиме підвищенню рівня інформаційної безпеки на підприємстві, включаючи дотримання персоналом вимог щодо її забезпечення та уникнення створення умов для завдання шкоди.

Заходи захисту інформації можна умовно розділити на дві основні групи:

- правові;
- організаційні-технічні;

Правові заходи захисту інформації

Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані заходи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а так само гарантують їх здійснення. Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкту правовідносин.

Узагальнено до правових принципів захисту інформації відносяться:

- легітимність;
- пріоритет міжнародного права над внутрішньодержавним;

- економічна доцільність.

Організаційні - технічні заходи захисту даних:

Роль організаційно - технічних заходів захисту інформації в системі безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Організаційні - технічні заходи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, а так само включають в себе наступні принципи захисту інформації, які мають впроваджуватись на підприємстві задля забезпечення інформаційної безпеки:

- науковий підхід до організації захисту інформації;
- планування захисту;
- керування системою захисту;
- безперервність процесу захисту інформації;
- системний підхід до організації та проектування систем та методів захисту інформації;
- комплексний підхід до організації захисту інформації;
- відповідність рівня захисту цінності інформації;
- гнучкість захисту;
- багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки;
- обмеження числа осіб, які допускаються до захищеної інформації;
- особиста відповідальність персоналу за збереження довіреної інформації.

Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, підбору персоналу, що працюватимуть з конфіденціною інформацією, допоможуть підібрати ефективні методи протидії загрозам інформаційній безпеці.

Отже, забезпечення інформаційної безпеки підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням

дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Література

1. http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf
2. http://zi.vntu.edu.ua/uploads/NMKD///OZIB/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%97.pdf
3. http://dspace.lvduvs.edu.ua/bitstream/1234567890/669/1/%D0%9A%D0%BE%D0%BF%D0%B8%D1%82%D0%BA%D0%BE%20%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D1%96%D0%B2%20%D0%BD%D0%B0%D0%B2%D1%87%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1.pdf

Щодо проблем забезпечення інформаційної безпеки в процесах життєдіяльності

Кузьменко Дарина Олександрівна,

Гриньків Роман Васильович,

Сочинський Орест Романович

Студенти групи МТП-21, ЛНУ, Львів, Україна

Бардін Оксана Іванівна

Науковий керівник, старший викладач кафедри безпеки життєдіяльності

В умовах сучасних глобальних та регіональних інформаційних протистоянь, поширення інформаційної агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними та стратегічними завданнями сучасності. Постановка питання про інформаційну безпеку в цій сфері має особливе значення для України. Інформаційну безпеку вважають пріоритетною функцією держави, так як вона є інтегрованою складовою національної безпеки. Бурхливість розвитку інформаційних та інформаційно-комунікаційних технологій супроводжується підвищенням рівня традиційних і появою загроз принципово нового характеру для громадян, суспільства та держави, що актуалізує тематику дослідження. Незважаючи на це розвиток механізмів забезпечення інформаційної безпеки потребує подальшої розробки та наукового обґрунтування шляхів їх модернізації, що зумовило вибір теми наукового дослідження.

Суттєвий прогрес і поширення інформаційних технологій привели до утворення глобальної інформаційної сфери, яка змушує світову спільноту, кожну державу швидко адаптуватись у сучасному інформаційному середовищі. Здатність суспільства та його інституцій збирати, обробляти, аналізувати, систематизувати та нагромаджувати інформацію, забезпечувати свободу інформаційного обміну є важливою передумовою соціального та технологічного прогресу, однією з основ успішної внутрішньої та зовнішньої політики держави, чинником національної безпеки. Але бурхливий розвиток інформаційної сфери супроводжується появою принципово нових та зростанням небезпечності вже відомих інформаційних загроз інтересам особистості, суспільства, держави та її інформаційній безпеці. Під час розробки проекту Закону України «Про засади інформаційної безпеки України» було запропоноване наступне визначення: інформаційна безпека –стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій. [3, ст. 30]

Важливою проблемою є відсутність усталеного поняття «інформаційна безпека».[1]

На наш погляд, сучасну увагу до проблем інформаційної безпеки держави викликано такими причинами:

– розвиток інформаційних технологій привів до якісних і кількісних змін у змісті національних інтересів, національної й міжнародної безпеки, у методах її забезпечення;[1]

– інформаційна сфера, що являє собою специфічну сферу діяльності суб'єктів громадського життя, пов'язану зі створенням, збереженням, поширенням, передачею, обробленням і використанням інформації, стала однією з найважливіших складових сучасного суспільства; [4]

– інформаційна інфраструктура й інформаційні ресурси стають ареною міждержавної боротьби за світове лідерство; [4]

– демонополізація послуг зв'язку, створення ринку послуг і засобів зв'язку привели до появи на території України мереж і систем зв'язку, що належать акціонерним товариствам і приватним особам;

– індустрія інформатизації, телекомунікації і зв'язку, інформаційних послуг на сучасному етапі соціально-економічного розвитку є однією зі сфер економіки.

Ще одна, також важлива, проблема – відсутність інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в публічному управлінні.[1]

Ураження свідомості оперує образами майбутнього та суспільними міфами. Йдеться про історичну пам'ять, релігійну сферу та національну ідею.[2] Вона не є новою і з її наслідками ми стикаємось не одне десятиріччя, але досі не можемо нічого протиставити Росії.

Когнітивна війна легко вбудовується в політичні системи, за яких панує невисокий рівень довіри до органів влади.[2]

Одне з головних правил війни – приховування авторства атакуючого. Воно може ховатися за нейтральною подачею негативної інформації. [2] Атакована країна може «відмиватися від бруду», але у неї немає доказів, що її ворог перед нею. Всі докази виключно непрямі.

Україна все частіше стикається з масштабними проявами інформаційної злочинності, що загрожують сталому та безпечному функціонуванню інформаційно-телекомунікаційних систем. В теперішніх умовах перед нашою державою особливо гостро постала проблема впливу політики Російської Федерації на інформаційну інфраструктуру України, на суспільну свідомість, підсвідомість особистості з метою нав'язати «правильну» систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної та державної діяльності, маніпулювати поведінкою громадян України.[2]

Отже, національний інформаційний простір України зазнає суттєвих загроз, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури.[1] До загроз національній безпеці України в інформаційній сфері також варто зарахувати:

- прояви обмеження свободи слова та доступу громадян до інформації; [3, ст. 41]
- викривлення, спотворення, блокування, замовчування упереджене та тенденційне висвітлення інформації; [3, ст. 41]
- несанкціоноване її поширення; відкриту дезінформацію; [3, ст. 41]
- інформаційну експансію з боку інших держав та руйнівне інформаційне вторгнення у національний інформаційний простір;
- виникнення і функціонування у національному інформаційному просторі держави непідконтрольних й інформаційних потоків;
- поширення засобами масової інформації культу насильства, жорстокості; повільність входження України у світовий інформаційний простір; [3, ст. 41]
- розміщення дезінформації в Інтернеті.

На сьогоднішній день існує ризик порушення цілісності та конфіденційності інформації, у тому числі навмисних нападів у вигляді зловмисного програмного забезпечення, злому інформаційно-телекомунікаційних систем або блокування надання послуг. Зловмисниками можуть бути як злочинні групи, що мають на меті фінансову вигоду або терористичні мотиви та групи, які можуть бути підтримані іноземними державами.[3, ст. 53] Щодо органів, які забезпечують інформаційну безпеку, то у ЄС у 2004 році було створено Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). ENISA надає практичні поради та рішення для державного та приватного секторів в країнах ЄС.[4]

Варто наголосити, що зараз ведеться гібридна війна, в тому числі інформаційна, між Україною та Російською Федерацією, яка спрямована на нав'язування певних ідеологічних стереотипах. Вирішення таких проблем забезпечить конфіденційність, цілісність та доступність даних. Ми будемо впевнені у правдивості інформації.

Враховуючи вищенаведене необхідно постійно розробляти програми для підвищення безпеки у сферах, де використовується інформаційні технології. Хакерські втручання в процеси призводять до порушень, аварій, катастроф, що в свою чергу впливає на економічні небажані наслідки.

Перелік посилань:

1) Закон України «Про інформацію»
2) Інформаційна безпека України як складова національної безпеки, Печенюк Андрій Васильович
3) Дисертація «Механізми забезпечення інформаційної безпеки як складова державної безпеки», Турчак Анна Василівна
4) ni.biz.ua/16/16_7/16_76859_ponyattya-elektronnogo-...zhavnoi-sluzhbi.html

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА ДОПОМОГОЮ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ

Букет Дар'я Анатоліївна
студентка групи БСДМ-52, ННІЗІ ДУТ, Київ, Україна

У часи такого стрімкого технологічного розвитку у світі вже майже не лишилось компаній та організацій, які так чи інакше не були б пов'язані з кіберпростором. Такі швидкі тенденції прогресу породжують багато не лише позитивних, а й негативних наслідків, одними з яких є велика кількість різноманітних загроз, наприклад, кібератак. Тому все більше уваги і ресурсів приділяється впровадженню та забезпеченню кібернетичної та інформаційної безпеки.

Ключові слова: інформаційна безпека, методи забезпечення інформаційної безпеки, кібербезпека, система захисту інформації.

Аналізуючи деякі існуючі публікації [1 с. 89-94, 2 с. 29-33], у яких зокрема розглядаються способи та підходи до захисту інформації, все ж постає питання який з методів є найефективнішим.

Загалом будь-яка система захисту та управління кібербезпекою в інформаційних системах повинна базуватись на трьох основних критеріях: доступність інформації (можливість використовувати інформацію згідно встановленим правилам), цілісність інформації (здатність інформації зберігатись в незмінному вигляді, без права на модифікацію неавторизованими користувачами), конфіденційність інформації (стійкість до спроб несанкціонованого доступу до інформації, збереження конфіденційності при її використанні) [3, с. 12-13].

Вибір способів, за допомогою яких буде гарантуватись інформаційна безпека, відбувається в залежності від особливостей та сфери діяльності організації. В основному у середовищі інформаційної безпеки виокремлюють наступні методи захисту: організаційні (управлінські), програмно-технічні, правові та методи мережевої безпеки [3, с. 14].

Проте оптимальним варіантом може бути комплексне застосування кількох базових методів. Тобто створення, реалізація, введення в експлуатацію з подальшим управлінням та вдосконаленням системи захисту інформації.

Отож, проблема інформаційної безпеки є дійсно важливою та потребує постійного пошуку нових рішень захисту, адже світ змінюється, і кіберзлочинці відповідно вдосконалюють способи вчинення атак. Оскільки вірогідність того, що загрози у кіберпросторі можуть повністю припинитись, є мінімальною, то основна задача – вміти приймати запобіжні заходи: правильно створювати, впроваджувати та контролювати систему, яка допомагає керувати інформаційною безпекою. Тож основною метою подальшої роботи буде формування та детальна розробка кожного елемента системи захисту, на основі розглянутої концепції. Також буде проведено аналіз ефективності запропонованого комплексу із заходів для захисту інформації після тестового впровадження.

Перелік посилань:

1. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.

2. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека»/ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 166 с.

3. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.