ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ

ІНТЕРНЕТ-КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ»

Тези доповідей

19 грудня 2019
м. Київ

ЗМІСТ

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИЩЕНОСТІ ХМАРНИХ ТЕХНОЛОГІЙ

Бойко Олексій Петрович
студент магістратури
ННІ захисту інформації
Державного
університету
телекомунікацій

Хмарні технології , з якими ми знайомі вже доволі довгий час , сьогодні оточують нас майже повсюди – люди використовують їх за для збереження та передачі особистих даних , швидкого доступу до них. Очевидно , що саме через це вони стали потенційною ціллю для кіберзлочинців . І саме через велику доступність та швидкий темп розвитку так важливо приділяти їм необхідну увагу в сфері забезпечення захисту інформації.

Хмарні обчислення продовжують трансформувати спосіб організації, зберігання та обміну даними, програмами та навантаженнями. Вони також представили цілу низку нових загроз та проблем безпеки. У хмарній інфраструктурі є одна велика чітка проблема безпеки: завдяки знаходженню в хмарі вона піддається загальнодоступному Інтернету. Застосування, дані та інші об’єкти, що зберігаються у хмарі, вразливі інакше, ніж якби вони були за центральним брандмауером. Це створює більше можливостей для зловмисників шукати слабкі місця та вразливості [1].

Хмарна інфраструктура, як локальна, так і публічна інфраструктура або в якійсь гібридній формі, використовує контейнери, мікросервіси та безсерверні функції. Це означає, що традиційних підходів до моніторингу безпеки додатків вже недостатньо [1].

Основними загрозами на сьогодні для хмарних технологій на сьогодні є:

Хмарні неправильні конфігурації - компанії ще не повністю усвідомлюють складності, пов’язані із забезпеченням хмарних даних, тому ще більше порушень, спричинених помилками, компромісами та дизайном;

Уразливості Spectre та Meltdown - Деякі зловмисники намагаються використовувати вразливості Spectre та Meltdown і зосереджують свої атаки на процесори, якими користуються хмарні провайдери;

Небезпечні API - у багатьох хмарних системах API (інтерфейси програмування прикладних програм) є єдиними гранями поза довіреною організаційною межею із загальнодоступною IP-адресою. Таким чином, незахищені API можуть надати зловмиснику значний доступ до хмарних додатків і поставити під загрозу всю систему;

Втрата даних - Одним із ризиків, який ніколи не слід ігнорувати, є втрата даних компанії через деякі нешкідливі причини, наприклад стихійне лихо чи людські помилки. Єдиний спосіб пом'якшити такі ризики - це створити безліч резервних копій цінної інформації та зберігати їх на фізичних сайтах, розташованих в різних частинах земної кулі [3].

Серед нападів, які зазнали респонденти в опитуванні хмарної безпеки в 2019 році, найчастішим методом нападу було викрадення облікових записів або облікових даних. Погані конфігурації, що ведуть до публічного впливу, були другими, а привілейовані зловживання користувачами - третіми. Інші методи, що повторюються, включають

невпевнений компроміс із інтерфейсом, тіньові IT (несанкціоновані зловмисне програмне забезпечення службовців), атаки "відмова в обслуговуванні" та ексфільтрацію даних із певного хмарного додатка [2].

Відповіді щодо впроваджених в даний час технологій вказують на те, що все ще існує велика перевага внутрішнім заходам. Що стосується хмарного зберігання та застосувань, це стосується лише того, що лише близько 20-30% респондентів застосували або захід безпеки, або якусь гібридну систему. Крім того, лише 44% респондентів брали основні заходи щодо використання API, наданих їхньою компанією хмарних послуг [2] , що наводить на деякі висновки стосовно рівня безпеки більшості з компаній.

Виходячи з наданих даних , можна підсумувати що на сьогодні з постійним розвитком хмарних технологій зростає й необхідність підтримування рівня безпеки в хмарах.

1. https://www.datacenterknowledge.com/cloud/clouds-cybersecurity-challenges-and-opportunities
2. https://www.cpomagazine.com/cyber-security/2019-sans-institute-cloud-security-survey-reveals-top-threats-which-surprisingly-are-not-ddos-attacks/#targetText=Of%20the%20attacks%20that%20respondents,privileged%20user%20abuse%20was%20third.
3. https://www.readitquik.com/articles/security-2/cybersecurity-challenges-that-need-to-be-on-your-radar-right-now/

ПРИНЦИПИ РОБОТИ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

Коростель Владислав Сергійович
аспірант
Бойко Олексій Петрович
студент магістратури ННІ
захисту інформації
Державного університету
телекомунікацій

Сучасний час вимагає сучасних підходів. Коли алгоритми кодування можна модифікувати , інтелектуальне обладнання – замінити на кращі аналоги , то людський фактор незмінний вже не одну тисячу років. Саме тому , проблема соціального інжинірингу займає не останнє місце серед кіберзлочинних актів проти людей , компаній та інтелектуальної власності в цілому.

Соціальна інженерія - це метод управління діями людини без використання технічних засобів. Метод заснований на використанні слабкостей людського фактору і вважається дуже руйнівним. Найчастіше соціальну інженерію розглядають як незаконний метод отримання інформації [1].

При проведенні атак соціоінженери застосовують такі методи нападу та дослідження:

- Претекстинг ;
- фішинг - електронна пошта (e-mail);
- вішинг - телефонний зв’язок;
- аналіз сміття;
- особистісні підходи;
- реверсивна соціальна інженерія.

Методи несанкціонованого доступу до інформації можна умовно поділити на дві категорії: з використанням методів соціальної інженерії та без них. На відміну від другого

випадку, коли зловмисник повинен володіти знаннями у галузі ІТ, у першому для отримання конфіденційних даних він спирається на знання з соціології та психології.

Претекстинг - це атака, відпрацьована за заздалегідь складеним сценарієм (претексту). В результаті ціль повинна видати певну інформацію або вчинити певну дію. Найчастіше ця техніка включає в себе більше, ніж просто брехню та обман і вимагає попередніх досліджень (наприклад, персоналізації: дата народження, сума останнього рахунку тощо) [1].

Фішинг - техніка соціотехнічної атаки, спрямована на неправомірне отримання конфіденційної інформації шляхом розсилу підроблених листів на електронну пошту - від банку або платіжної системи. Цей лист зазвичай містить посилання на фальшиву веб-сторінку, яка імітує офіційну, з корпоративним логотипом і наповненням, і містить форму, що вимагає ввести конфіденційну інформацію - від домашньої адреси до пін-коду банківської картки [1].

Вішинг - один з методів шахрайства з використанням соціальної інженерії, який полягає в тому, що зловмисники, використовуючи телефонну комунікацію і граючи певну роль (співробітника банку, покупця і т.д.) під різними приводами:

1) виманюють у власника карткові реквізити;
2) стимулюють власника до зняття лімітів по карті, відключення перевірки CVV2 / CVC2-коду і т.д .;
3) стимулюють власника до здійснення перекладу на карту шахрая, а також здійсненню перекладу на карту шахрая через банкомат [2].

Незаконний *аналіз сміття* - надзвичайно плідна з погляду зловмисників діяльність. Зокрема ділові паперові відходи стають безцінною поживою для тих хакерів, які використовують методи соціального інжинірингу (а саме – претекстинг або реверсивну соціальну інженерію), видаючи себе за співробітників тієї чи іншої компанії. На величезну небезпеку наражається й компанія в який не діють суворі правила утилізації використаних цифрових носіїв — жорстких дисків, компакт-дисків, які можуть стати джерелом усіх видів інформації про діяльність такої компанії.

Особистісні підходи - спосіб соціотехнічного впливу на об'єкт (персону) для отримання доступу чи конфіденційної інформації через способи психологічного впливу (психологічного штурму).

Існують чотири різновиди такого підходу:

- залякування (може йтися про уособлення повноважень, що має спонукати жертву нападу до виконання запиту);
- переконання (найбільш звичні форми переконання передбачають застосування лестощів);
- використання довірливих стосунків (потребує підготовчого періоду, протягом якого мають скластися відповідні стосунки);
- допомога (хакер пропонує допомогу потенційній жертві, аби змусити її оприлюднити особисту інформацію).

Зворотна соціальна інженерія описує ситуацію, в якій адресат — представник персоналу звертається до хакера по допомогу в усуненні своїх проблем і пропонує хакерові ту інформацію, яку він має намір продати.

Цьому, як правило, передує дрібна диверсія, у ході якої хакер (можливо інженер компанії) ініціює збій у роботі комп'ютера, підімкненого до мережі. Розрахунок на те, щоб користувач уявляв собі масштаб аварії не таким уже й значним, але при цьому усунути збій власними силами він не зміг. Далі вже справа соціальної техніки: як правило, десь поблизу (наприклад, у списку контактів соціальних мереж , контактах мобільних месенджерів Viber або Telegram) постає «добрий знайомий» когось зі співробітників, який має потрібні знання, або виникає оголошення щодо розташованого неподалік «центру комп'ютерної швидкої допомоги», або з'являється повідомлення про вигідну акцію з підвищення користувальницької грамотності. Головне, що все виконується швидко й дешево (а то й

безплатно), без неодмінного оповіщення колег і топ-менеджерів про ганебну IT-безграмотність конкретного працівника.

1. https://studopedia.su/8_51980_ponyattya-pro-sotsialniy-inzhiniring-politika-bezpeki.html
2. https://www.ema.com.ua/citizens/wiki/vishing/

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ КІБЕРІНЦИЕНТІВ У КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Бахмацький Олексій Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації

Сьогодні існує велика кількість різноманітних загроз і шкідливих програм, що спрямовані на порушення безпеки корпоративної інформаційної системи. Причому частина з них може щодня атакувати або відбуватися в мережі компанії. Тому кібераналітіки щодня зіштовхуються з великою кількість кіберінцидентів. Вирішенням цих проблем може стати штучний інтелект.

Корпоративні інформаційні системи щодня зіштовхуються більше як із 200000 подіями, що пов’язані з безпекою [1]. Причому на кожного аналітика безпеки може припадати до 40 інцидентів [1], для розслідування яких досить часто потрібно витрачати багато часу, за який злочинці можуть досягти своїх цілей. Для вирішення цих завдань в нагоді може стати використання штучного інтелекту.

Протягом останніх років штучний інтелект та машинне навчання почав набувати популярності використання в різних сферах і кібербезпека не стала виключенням цьому. Виробники програмних систем захисту, кібераналітики, а також кіберзлочинці використовують штучний інтелект для виконання своїх цілей.

Отже, штучний інтелект можна характеризувати як систему симуляції людського розуму, що має уміння до раціонального мислення і може приймати рішення, що мають найбільший успіх для досягнення мети [2]. У кібербезпеці використання штучного інтелекту дозволяє автоматизувати процес виявлення кіберінцидентів, зменшити кількість помилок при виявленні, а також пришвидшити процес їхнього виявленн я[3].

Для виявлення кіберінцидентів штучний інтелект може аналізувати базу даних зі всіма відомими шкідливими програмними забезпеченнями (ШПЗ) та проводити аналіз коду, поведінки та сигнатур підозрілих програм у системі. Таким чином штучний інтелект може виявляти як відоме ШПЗ, так і невідоме до цього ШПЗ, що використовує або схожі методи або виконує дії, що раніше були позначені, як шкідливі [4]. Окрім цього штучний інтелект може проводити аналіз даних, які генеруються в системі, для виявлення закономірностей і аномалій у поведінці користувачів, мережевого трафіку, операційної системи. Після чого штучний інтелект формує шаблон нормальної роботи мережі та виявляє підозрілу активність [4].

Важливим елементом при впровадженні штучного інтелекту в систему захисту корпоративної інформаційної мережі є те, щоб він був правильно налаштований, натренований та відкоригований спеціалістами з кібербезпеки. В інакшому випадку штучний інтелект не буде виявляти вразливості, пропускатиме ШПЗ або, навіть, легітимну діяльність відмічуватиме, як шкідливу.

Прикладом використання штучного інтелекту в системі захисту корпоративної інформаційної системи може стати використання IBM Watson з інтеграцією його в SIEM-систему IBM QRadar. IBM Watson провидить аналіз даних, що зібрав IBM QRadar щодо певного інциденту безпеки, та виконує пошук щодо відомих вразливостей у базі даних IBM X-Force. Потім він проводить кореляцію даних в IBM QRadar для пошуку всіх пов'язаних подій з інцидентом безпеки та формує картину, на якій відображає комп'ютери, що прийняли участь у інциденті, веб-ресурси, які використовувалися в інциденті, файли, що були заражені або створені під час інциденту, облікові записи користувачів, що взяли участь у інциденті, інші інциденти, що пов'язані з ним тощо [5].

Також IBM Watson може проводити аналіз кіберінциденту на відповідність до етапів атаки за матрицею MITRE ATT&CK [6]. За рахунок цих даних кібераналітику легше відслідкувати процес протікання кіберінциденту та оцінити, на якій стадій.

Основними недоліками використання штучного інтелекту в корпоративних інформаційних системах можуть стати такі: висока затратність ресурсів для його створення і обслуговування, для його навчання потрібно використати великий обсяг баз даних (код ШПЗ, код нешкідливих програм, аномалії), які важко отримати. Також штучний інтелект може проявити свою неефективність у зв'язку з тим, що кіберзлочинці можуть створювати ШПЗ, що не виявляється штучним інтелектом [7]. Тому рекомендується компаніям співпрацювати з фірмами, щоб забезпечують кібербезпеку, для вирішення частини цих питань.

Отже, використання штучного інтелекту може у ближньому майбутньому лише зростати у сфері кібербезпеки. Кількість шкідливих програм, що будуть використовувати штучний інтелект та машинне навчання теж збільшиться. Тому правильно налаштований штучний інтелект може не тільки зменшити кількість роботи, що покладається на аналітика кібербезпеки, а також допомогти у виявленні кіберінцидентів, які були до цього непоміченими.

Література

1. Falco C. Watson and Cybersecurity: Bringing AI to the Battle [Електронний ресурс] / Christian Falco // Security Intelligence. — 2017. — Режим доступу до ресурсу: https://securityintelligence.com/watson-and-cybersecurity-bringing-ai-to-the-battle/.
2. Frankenfield J. Artificial Intelligence (AI) [Електронний ресурс] / J. Frankenfield, G. Scott // Investopedia. — 2020. — Режим доступу до ресурсу: https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp.
3. 3 Reasons for Using Artificial Intelligence in Cyber Security [Електронний ресурс] // eleks — Режим доступу до ресурсу: https://eleks.com/blog/using-artificial-intelligence-in-cyber-security/.
4. Palmer D. AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know [Електронний ресурс] / Danny Palmer // ZDNet. — 2020. — Режим доступу до ресурсу: https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/.
5. Dheap V. IBM QRadar Advisor with Watson: Revolutionizing the Way Security Analysts Work [Електронний ресурс] / Vijay Dheap // Security Intelligence. — 2017. — Режим доступу до ресурсу: https://securityintelligence.com/ibm-qradar-advisor-with-watson-revolutionizing-the-way-security-analysts-work/.
6. Osborne C. IBM QRadar Advisor with Watson boosted with MITRE framework [Електронний ресурс] / Charlie Osborne // ZDNet. — 2018. — Режим доступу до ресурсу: https://www.zdnet.com/article/ibm-qradar-advisor-with-watson-boosted-with-mitre-framework/.
7. Laurence A. The Impact of Artificial Intelligence on Cyber Security [Електронний ресурс] / Aimee Laurence // CPO Magazine. — 2019. — Режим доступу до ресурсу: https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/.

МЕТОДИ ЗАХИСТУ ВІД СПАМУ

Валетка Д.В.,
Студент групи БСЗМ-61
Державний Університет Телекомунікацій
М. Київ

Одна з найбільших проблем при роботі з електронною поштою – це небажані повідомлення комерційного характеру, а просто кажучи – спам. Крім незручностей, пов'язаних з позбавленням від спаму, спам – це ще й прямі збитки для підприємства: витрачається Інтернет-трафік і місце на носіях, на розбір такої пошти витрачається робочий час користувачів. Один з головних засобів боротьби зі спамом – це підвищення рівня грамотності користувачів. Зокрема, користувачі повинні знати, що:

- ніколи не можна давати свій робочий адрес електронної пошти в ненадійні руки (залишати у формах реєстрації на ненадійних Web-сайтах, гостьових книгах і форумах і т.п.). Навчіть користувача для участі у лотереях використовувати спеціальну адресу електронної пошти де-небудь на безкоштовній поштовій системи типу mail.ru, hotmail.com тощо;
- краще не розміщувати явну адресу електронної пошти на Web-сторінки корпоративного Web-сайту. Для запитів можна використовувати, наприклад, прості Web-додатки з формами;
- навчіть користувачів не використовувати робочу адресу електронної пошти в каталогах ICQ, AOL Instant Messenger і т.п.;
- ніколи не можна відповідати на повідомлення спамерів (навіть якщо дуже хочеться посваритися). Дуже часто «на іншому кінці» знаходиться поштовий робот, який фіксує адреси, з яких надійшли відповіді. Цінність таких адрес сильно зростає і, відповідно, потік спаму стає набагато більше;
- якщо користувач все-таки допустив помилку, можливо, є сенс звернутися до адміністратора, щоб він змінив для цього користувача адреси його електронної пошти.

Проте такі заходи рятують не завжди, і часто доводити боротися зі спамом технічними засобами.

Існує програмне забезпечення (ПЗ) для автоматичного визначення спаму (т.з. фільтри). Воно може бути призначено для кінцевих користувачів або для використання на серверах. Це ПЗ використовує два основні підходи.

Перший полягає в тому, що аналізується зміст листа і робиться висновок, спам це чи ні. Якщо лист класифікований як спам, він може бути помічений, переміщений в іншу папку або навіть видалений. Таке ПЗ може працювати як на сервері, так і на комп'ютері клієнта. При такому підході ви не бачите відфільтрованого спаму, але продовжуєте повністю нести витрати, пов'язані з прийомом пошти, оскільки антиспамне ПЗ у будь-якому випадку одержує кожен спамерський лист (витрачаючи ваші гроші), а тільки потім вирішує показувати його чи ні.

Другий підхід полягає в тому, щоб розпізнавати відправника як спамера не заглядаючи в текст листа. Для визначення застосовуються різні методи. Це ПЗ може працювати тільки на сервері, який безпосередньо приймає листи. При такому підході можна зменшити витрати — гроші витрачаються тільки на спілкування із спамерськими поштовими програмами (тобто на відмови приймати листи) і звернення до інших серверів (якщо такі потрібні) при перевірці. Виграш, проте, не такий великий, як можна було б чекати. Якщо одержувач відмовляється прийняти лист, спамерська програма намагається обійти захист і відправити його іншим способом. Кожну таку спробу доводитися відображати окремо, що збільшує навантаження на сервер.

Місце установки антіспамного ПЗ (комп'ютер кінцевого користувача або поштовий сервер, наприклад, провайдера) визначає того хто нестиме витрати, пов'язані з фільтрацією спаму.

Якщо спам фільрує кінцевий користувач, то він і нестиме витрати (а можливо і провайдер, якщо пошта «безкоштовна»), оскільки буде вимушений одержувати всі повідомлення, включаючи спам.

Якщо спам фільтрує сервер, то користувач не несе витрат, тому що одержує тільки корисну кореспонденцію, а всі витрати лягають на власника сервера.

В даний час використовується декілька методів фільтрації електронної пошти.

Чорні списки

У чорні списки заносяться IP-адреси комп'ютерів, про які відомо, що з них ведеться розсилка спаму. Також широко використовуються списки комп'ютерів, які можна використовувати для розсилки — «відкриті релєї» і «відкриті прокси», а також — списки «діалапів» — клієнтських адрес, на яких не може бути поштових серверів. Можна використовувати локальний список або список, підтримуваний кимось ще. Завдяки простоті реалізації, широкого поширення набули чорні списки, запит до яких здійснюється через службу DNS. Вони одержали назву DNSBL (DNS Black List). В даний час цей метод не дуже ефективний. Спамери знаходять нові комп'ютери для своїх цілей швидше, ніж їх встигають заносити в чорні списки. Крім того, декілька комп'ютерів, що відправляють спам, можуть скомпрометувати весь поштовий домен і тисячі законопокірних користувачів на невизначений час будуть позбавлені можливості відправляти пошту серверам, що використовують такий чорний список.

Сірі списки

Метод сірих списків заснований на тому, що «поведінка» програмного забезпечення, призначеного для розсилки спаму відрізняється від поведінки звичайних поштових серверів, а саме, спамерські програми не намагаються повторно відправити лист при виникненні тимчасової помилки, як того вимагає протокол SMTP.

Спочатку всі невідомі сервери заносяться в «сірий» список і листи від них не приймаються. Серверу відправника повертається код тимчасової помилки, тому, звичайні листи (не спам) не втрачаються, а тільки затримується їх доставка (вони залишаються в черзі на сервері відправника і доставляються при наступній спробі). Якщо сервер поводиться так, як очікувалося, він автоматично переноситься в білий список і наступні листи приймаються без затримки.

Цей метод в даний час дозволяє відсіяти до 90% спаму, практично без ризику втратити важливі листи. Проте його теж не можна назвати бездоганним.

- Можуть помилково відсіватися листи з серверів, що не виконують рекомендації протоколу SMTP, наприклад, розсилки з сайтів, що розсилають новини.
- Затримка при доставці листа може досягати півгодини (а то і більше), що може бути неприйнятно у разі термінової кореспонденції. Цей недолік компенсується тим, що затримка вноситься тільки при посилці першого листа з раніше невідомої адреси.
- Великі поштові служби використовують декілька серверів, з різними IP-адресами, більш того, можлива ситуація, коли декілька серверів по-черзі намагаються відправити один і той же лист. Це може привести до дуже великих затримок при доставці листів.
- Спамерські програми можуть удосконалюватися. Підтримка повторної посилки повідомлення реалізується досить легко і повністю нівелює даний вид захисту.

Контроль масовості

Технологія припускає виявлення в потоці пошти масових повідомлень, які абсолютно ідентичні або розрізняються незначно. Для побудови працездатного «масового» аналізатору потрібні величезні потоки пошти, тому цю технологію пропонують великі виробники, що володіють значними обсягами пошти, що вони можуть піддати аналізу.

Перевірка Інтернет-заголовків повідомлення

Спамери пишуть спеціальні програми для генерації спамерских повідомлень й їхнього миттєвого поширення. При цьому вони свідомо допускають помилки в оформленні заголовків, у результаті спам далеко не завжди відповідає вимогам поштового стандарту

RFC, що описує формат заголовків. По цих помилках можна обчислити спамерське повідомлення.

Контентна фільтрація

Також одна зі старих, перевірених технологій. Спамерські повідомлення перевіряються на наявність специфічних для спама слів, фрагментів тексту, картинок й інших характерних спамерських рис. Контентна фільтрація починалася з аналізу того повідомлення й тих же його частин, які містили текст (plain text, HTML), але зараз спам-фільтри перевіряють всі частини, включаючи графічне вкладення.

У результаті аналізу може бути побудовані текстова сигнатура або зроблений підрахунок «спамерської ваги» повідомлення.

Грейлістінг

Тимчасова відмова в прийоми повідомлення. Відмова йде з кодом помилки, що розуміють всі поштові системи. Через деякий час Вони повторно надсилають повідомлення. А програми, що розсилають спам, у такому випадку повторно лист не відправляють.

Статистичні методи фільтрації спаму

Ці методи використовують статистичний аналіз змісту листа для ухвалення рішення, чи є воно спамом. Найбільшого успіху вдалося досягти за допомогою алгоритмів, заснованих на теоремі Байеса. Для роботи цих методів потрібне «навчання» фільтрів, тобто потрібно використовувати розсортовані вручну листи для виявлення статистичних особливостей нормальних листів і спаму. Після навчання на достатньо великій вибірці, вдається відсікти до 95—97% спаму.

Байєсовські мережі довіри.

Байєсовські мережі довіри - Bayesian Belief Network - використовуються в тих областях, які характеризуються успадкованою невизначеністю. Ця невизначеність може виникати внаслідок: неповного розуміння предметної області; неповних знань; коли завдання характеризується випадковістю.

Таким чином, байєсовські мережі довіри (БМД) застосовують для моделювання ситуацій, що містять невизначеність в деякому розумінні. Для байєсовських мереж довіри іноді використовується ще одна назва: причинно-наслідкова мережа, в який випадкові події сполучені причинно-наслідковими зв'язками.

З'єднання методом причин і наслідків дозволяють простіше оцінювати вірогідність подій. У реальному світі оцінювання найчастіше робиться в напрямі від “спостерігача” до “спостереження”, або від “ефекту” до “наслідку”, яке в загальному випадку складніше оцінити, чим напрям “наслідок -> ефект”, тобто в напрямі від наслідку.

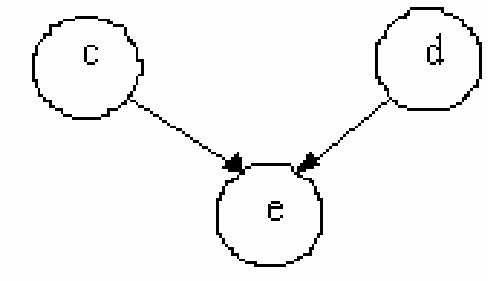

Рис.1. Приклад простої байєсовської мережі довіри.

Розглянемо приклад мережі (рис.1), в якій вірогідність перебування вершини «e» в різних станах (e_k) залежить від станів

$$p(e_k) = \sum_i \sum_j p(e_k \mid c_i, d_j) \times p(c_i, d_j)$$

(c_i, d_j) вершин «c» і «d» і визначається виразом:

де $p(e_k \mid c_i, d_j)$ - вірогідність перебування тільки залежно від станів c_i, d_j. Оскільки події, представлені вершинами «c» і «d» незалежні, то

$p(e_k \mid c_i, d_j) = p(c_i)$ Ч $p(d_j)$.

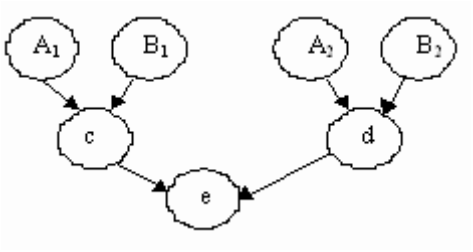

Рис.2. Дворівнева БМД.

Розглянемо приклад складнішої мережі (рис.2). Даний рисунок ілюструє умовну незалежність подій. Для оцінки вершин «c» і «d» використовуються ті ж вирази, що і для обчислення $p(e_k)$, тоді:

$$p(c_j) = \sum_m \sum_n p(c_j \mid A_{1m}, B_{1n}) \times p(A_{1m}) \times p(B_{1n})$$

$$p(d_j) = \sum_m \sum_n p(d_j \mid A_{2m}, B_{2n}) \times p(A_{2m}) \times p(B_{2n})$$

З цих виразів видно, що вершина «e» умовно не залежить від вершин A1, A2, B1, B2, оскільки немає тих стрілок, що безпосередньо сполучають ці вершини.

Розглянувши ці приклади спробуємо тепер точніше визначити основні поняття, що використовуються в БМД. Байєсовські мережі довіри - це направлений ациклічний граф, що володіє наступними властивостями:

- кожна вершина є подією, що описується випадковою величиною, яка може мати декілька станів;
- всі вершини, що пов'язані з “батьківськими”, визначаються таблицею умовної вірогідності (ТУВ) або функцією умовної вірогідності (ФУВ);
- для вершин без “батьків” вірогідності її станів є безумовними (маргінальними).

Іншими словами, в байєсовських мережах довіри вершини є випадковими змінними, а дуги - імовірнісні залежності, які визначаються через таблиці умовної вірогідності. Таблиця умовної вірогідності кожної вершини містить вірогідність станів цієї вершини за умови станів її “батьків”.

Застосування Байєсовського класифікатора для завдання визначення спаму

Формальне визначення Байєсовського класифікатора

Завдання класифікації документів полягає в тому, щоб знайти наближене відображення K´=DxC→{T,F} відображення K, такого що K(d,c)=T тоді і тільки тоді, коли документ d відповідає категорії K(d,c)=F у зворотньому випадку.

Одержана апроксимація K' називається класифікатором. У випадку якщо категорії статистично незалежні одна від одної (тобто K´(dj,c´) не залежить від K´(dj,c´´) для будь-яких c´c´´), то можна без втрати спільності припустити, що безліч категорій складається тільки з двох непересічних категорій, до однієї з яких обов'язково належить кожний з документів. Це пов'язано з тим, що випадок з великою кількістю категорій {c1,...cn} можна представити як n завдань вигляду.

$$D \times \{c_j, \bar{c}_j\}, j = \overline{1,n}$$

Таким чином, завдання класифікації зводиться до пошуку наближеного відображення K´=DxC→{T,F}.

Крім того, вводиться множина характеристик T, які можуть бути зіставлені з документами. Тоді документ d представляється вектором коефіцієнтів (w1,...,w|T|), 0≤wi≤1. Коефіцієнти w_i, грубо кажучи, визначають 'внесок' характеристики t_i в семантику документа d.

У будь-якому методі автоматичної класифікації спочатку визначаються характеристики документів і спосіб обчислення вагів.

Наївний Байєсовський класифікатор

Байесовський класифікатор заснований на використанні знаменитої теореми Байєса, і перші згадки про нього можна зустріти ще в 1960-му році. За вже більш ніж 40-річну історію НБК використовувався для вирішення найрізноманітніших завдань: від класифікації текстів в агентствах новин до первинної діагностики захворювань в медичних установах.

При постановці завдання для НБК як характеристики звичайно вибирається наявність або відсутність будь яких слів в документі, тобто за множину характеристик T береться множина всіх слів в оброблюваних документах. Таким чином, вага характеристики $w_i=1$ в тому випадку, якщо слово t_i було знайдено, і $w_i=0$ у зворотному випадку. У випадку з фільтрами, які використовуються для класифікації спаму, враховується ще і область, в якій зустрілося слово: заголовки, тема листа (subject), тіло листа. Тобто слово 'спам', що зустрілося в темі листа, є іншим терміном, чим слово 'спам' в тілі листа.

Крім того, робиться дуже важливе припущення: передбачається, що всі характеристики документів, одержані таким чином (слова), статистично незалежні; саме із-за цього припущення в назві класифікатора присутнє слово «наївний». Це сильно спрощує застосування теореми Байєса для побудови класифікатора.

НБК, звичайно використовуваний в спам-фільтрах (запропонований Полом Гремом) має вигляд $p_1 \cdot p_2 \ldots p_{|d|}/(p_1 \cdot p_2 \ldots p_{|d|}+(1-p_1)\cdot(1-p_2 \ldots (1-p_{|d|}))>W$, де $p_i=P(w_i=1|c)$, W - заданий користувачем поріг. При цьому використовується вірогідність тільки тих характеристик, які зустрілися в документі. Такий НБК відрізняється від класичної формули тим, що в ньому не використовується вірогідність самих категорій (або, точніше, ці категорії прийняті за рівноймовірні). Таке рішення обґрунтовується тим, що ухвалення рішення про конкретний лист не повинно бути пов'язано з кількістю спаму в поштовій скриньці, а повинно обчислюватися виключно по вмісту самого листа.

Для обчислення вірогідності p_i використовується т.з. процес навчання, під час якого аналізуються наперед класифіковані документи. Тоді вірогідність можна розрахувати, наприклад, таким чином: $p_i=b_i/(g_i+b_j)$, де b_i - кількість 'поганих' документів, що містять характеристику t_i; g_i - кількість 'гарних' документів, що містять характеристику t_i.

У реальних фільтрах, заснованих на НБК, можуть використовуватися інші способи обчислення оцінок вірогідності, що враховують спеціальні випадки рідкісних характеристик (документів, що зустрічаються у малій кількості). Наприклад, Гар Робінсон рекомендує замінити оцінку p_i на f_i: $f_i=(s\cdot x+n_i\cdot p_i)/(s+n_i)$, де s и x - експериментально підібрані параметри (рекомендується 1 і 0.5), а n - кількість документів з характеристикою t_i.

Метод Фішера

Починаючи з публікації статті Гара Робінсона, в деяких фільтрах (наприклад, SpamAssassin) замість НБК став використовуватися метод поєднання вірогідностей, запропонований Р. Фішером в 1950 році.

Стосовно класифікації документів, Робінсон сформулював цей метод таким чином: припустимо, що документ має n характеристик, для кожної з яких вже розрахована вірогідність p_i. Тоді, згідно Фішеру, якщо ці вірогідності не розподілені рівномірно, то значення $-2\cdot\ln\prod_{i=1}^{n} p_i$ підкорятиметься закону розподілу $\chi^2(2n)$.

Таким чином, стає можливим знайти вірогідність того, що для деяких інших значень p_i відповідне число $-2\cdot\ln\prod_{i=1}^{n} p_i$ буде більше, ніж розраховане для даного документа. Якщо ця вірогідність достатньо мала, то документ слід віднести до даної категорії.

Для визначення спаму Робінсон запропонував розрахувати так само не тільки вірогідність 'спамності' документа (H), але і вірогідність того, що лист не є спамом (S), і використовувати показник I, що розраховується по формулі $I=(1+H-S)/2$. Якщо показник I

достатньо близький до 0, то лист вважається 'не спамом'; якщо I достатньо близький до 1, лист вважається 'спамом'. Інакше лист вважається спірним. Таким чином, в роботі вводиться класифікація не по двох категоріях, а по трьох.

Фільтрація спаму на стороні провайдера

Стрімко зростаюча кількість спаму примушує великі інтернет-сервіси упроваджувати нові технології фільтрації пошти. Посилюється боротьба із спамом на Hotmail, Yahoo! і MSN, які упроваджують нові технології фільтрації. Вже запущений безкоштовний фільтр спаму Spamtest.ru, на найбільшому російському поштовому сервісі Mail.ru запроваджений "Антіспам Касперського", Yandex оголосив про запуск власного сервісу "Спамооборона", поштовий сервіс порталу KM.RU упровадив захист від спаму "Карантин", компанії E-Style ISP", "Петерлінк" встановили "Антіспам Касперського", "Корбіна Телеком" оголосила про впровадження власного фільтру спаму, побудованого на безкоштовному програмному забезпеченні SpamAssassin.

Провайдери можуть фільтрувати спам для клієнтів, які тримають у них свої поштові скриньки. Звичайно це домашні користувачі, що використовують доступ по телефонній лінії, або користувачі виділених ліній. Серед них також є деяка кількість корпоративних користувачів. Це характерно тільки для компаній, у яких не створена власна поштова система, і вони тримають пошту виключно у провайдера. В деяких випадках це достатньо зручно і не вимагає великих витрат. Проте для компаній, у яких створена своя поштова система, такий спосіб фільтрації не прийнятний з наступних причин:

- Конфіденційність електронної пошти. Ефективна фільтрація пошти вимагає як мінімум контролю текстової складової листа, а це означає, що провайдер буде обізнаний про зміст електронного листування компанії.
- Неможливість побудови гнучкої політики використання електронної пошти. Компанії, як правило, мають складну структуру, в якій різні групи користувачів можуть одержувати певні категорії листів. При цьому один і той же лист може відноситися одночасно до декількох категорій (лист може бути спамом для однієї категорії користувачів і діловим листом для іншої, наприклад, рекламний лист про виставку профільної продукції для відділу маркетингу буде діловим, а для відділу інформаційних технологій — спамом).
- Методи і технології фільтрації на стороні провайдера не застосовні для корпоративного користувача.

Якщо з першими двома причинами все гранично ясно, то остання причина вимагає деякого пояснення. Для фільтрації спаму провайдери використовують наступні методи фільтрації спаму:

- З використанням RBL-сервісів (за поштовими адресами).
- Розподілені методи виявлення спаму.

Кожний із способів має свої переваги і недоліки.

АНАЛІЗ ВИКОРИСТАННЯ ПРОТОКОЛІВ VPN, ДЛЯ ПОБУДОВИ ЗАХИЩЕННОЇ МЕРЕЖІ

Карпенко Олександр Геннадійович , аспірант 125 кібербезпека
Державний університет телекомунікацій,
м. Київ

Віртуальна приватна мережа (VPN – Virtual Private Network) – загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет.

Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією.

Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією.

Метою дипломної роботи є аналіз сучасних протоколів VPN, які можна використати при побудові захищеної мережі.

На сьогоднішній день кожній організації потрібні безпечні, надійні і недорогі способи з'єднання між собою декількох мереж, які дозволять підключати філії і співробітників до мережі головного офісу корпорації. Крім того, з урахуванням збільшення кількості співробітників, що працюють віддалено підприємствам все частіше потрібні безпечні, надійні та економічні рішення для підключення персоналу, що працюють в секторі SOHO (Small Office/Home Office – малий офіс/домашній офіс), а також в інших віддалених місцях розташування, до ресурсів корпоративних вузлів.

Організації використовують мережі VPN для наскрізного конфіденційного мережевого зв'язку через мережі сторонніх компаній, наприклад, через Інтернет. Тунель усуває бар'єр, пов'язаний з відстанню, і дозволяє віддаленим користувачам отримувати доступ до мережевих ресурсів на центральному вузлі. VPN є приватною мережею, яка створюється за допомогою тунелювання в публічній мережі (як правило, в Інтернеті). VPN – це середовище передачі даних із суворим контролем доступу, що дозволяє встановлювати рівноправні підключення в межах певної цільової спільноти.

В даний час під віртуальними приватними мережами зазвичай розуміють захищену реалізацію мережі VPN з шифруванням (наприклад IPsec VPN – Internet Protocol Security Virtual Private Network).

Мережі VPN з IPsec забезпечують гнучкий і масштабований зв'язок. З'єднання між філіями можуть забезпечувати безпечний, високошвидкісний і надійний віддалений зв'язок. За допомогою VPN з IPsec інформація з приватної мережі передається в захищеному режимі по публічній мережі.

Для реалізації мереж VPN потрібно шлюз VPN. Шлюзом VPN може виступати маршрутизатор, міжмережевий екран або пристрій адаптивного захисту Cisco ASA (Adaptive Security Appliance). ASA – це автономний міжмережевий екран, який об'єднує в межах одного образу програмного забезпечення функції брандмауера, концентратора VPN, а також системи запобігання вторгнень.

В мережі VPN застосовуються віртуальні підключення, які проходять від приватної мережі організації через Інтернет до віддаленого вузла або комп'ютера співробітника. Інформація, що надходить з приватної мережі, передається в захищеному режимі по публічній мережі, що дозволяє створити віртуальну мережу.

Віртуальні приватні мережі на даний час є актуальними із-за наступних переваг:

Скорочення витрат – мережі VPN дозволяють організаціям використовувати надане сторонніми компаніями недороге транспортне середовище Інтернету для підключення віддалених офісів і користувачів до основного вузла, тобто відмовитися від застосування дорогих виділених каналів WAN (Wide Area Network) і банків модемів. Крім того, завдяки появі недорогих технологій, що забезпечують високу пропускну здатність (наприклад DSL – Digital Subscriber Line), організації можуть використовувати мережі VPN для скорочення своїх витрат на організацію зв'язку при одночасному підвищенні рівня пропускної здатності віддалених підключень.

Масштабованість – завдяки мережам VPN організації можуть використовувати інфраструктуру Інтернету в межах інтернет-провайдерів і пристроїв, що дозволяє спростити процедуру додавання нових користувачів. Тому організації можуть серйозно нарощувати пропускну здатність без внесення суттєвих змін до інфраструктури.

Сумісність з широкосмуговою технологією – завдяки мережам VPN мобільні і віддалені співробітники можуть ефективно використовувати високошвидкісний широкосмуговий зв'язок, наприклад DSL і кабельні канали, для доступу до мереж своїх

організацій. Широкосмуговий зв'язок забезпечує високу гнучкість і ефективність. Високошвидкісні широкосмугові підключення також дозволяють створювати економічні рішення для підключення віддалених офісів.

Безпека – мережі VPN можуть підтримувати різні механізми захисту, що забезпечують найвищий рівень безпеки, завдяки застосуванню складних протоколів шифрування і аутентифікації, що дозволяють захищати дані від несанкціонованого доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 .www.netacad.com [Електронний ресурс]: курс «Маршрутизація і комутація CCNA: Підключення мереж», 4 сем. – Режим доступу: https://static-course-assets.s3.amazonaws.com/CN503/ru/index.html

2. Біячуєв Т.А. під ред. Л.Г. Осовецкого Безпека корпоративних мереж. - СПб: СПб ГУ ІТМО, 2006 - 161 с.

3. Браун С. Віртуальні приватні мережі, 2015 - 503с.

4. Зепченков С.В., Милославська Н.Г., Толстої А.І. Основи проектування віртуальних приватних мереж: Навч. Посібник для ВНЗ, 2009 - 249 с.

5. Звіт про глобальні ризики кібербезпеки https://www.marsh.com/ru/ru/insights/research-briefings/marsh-microsoft-cyber-survey-report-2019.html

КЛАСИФІКАЦІЯ ЗАГРОЗ БЕЗПЕКИ ВЕБ-ДОДАТКІВ НА БАЗІ OWASP TOP 10 – 2017

Галузін І.С.

Анотація. Проведено дослідження класифікації загроз безпеки веб-додатків на базі OWASP top 10 – 2017. Виявлено позитивні наслідки використання даної технології для глобального інформаційного середовища.

Кіберзлочинність зараз розвинена як ніколи - адже майже кожна компанія має свій сайт в інтернеті, а зловмисник у мережі може легко залишатися абсолютно анонімним.

Класифікацією векторів атак і вразливостей займається спільнота OWASP (Open Web Application Security Project). Відкритий проект по забезпеченню безпеки веб-додатків (OWASP) - це відкрите співтовариство, що дозволяє організаціям розробляти, здобувати і підтримувати безпечні програми та інтерфейси прикладного програмування (API).

OWASP створив список з 10-и найбільш небезпечних векторів атак на Web-додатки, цей список отримав назву OWASP TOP-10 і в ньому зосереджені найнебезпечніші уразливості, які можуть коштувати деяким людям великих грошей, або підриву ділової репутації, аж до втрати бізнесу.

Перелік вразливостей постійно оновлюється і на 2017 виглядає наступним чином:

• A1:2017 - Ін'єкції, воно ж "Впровадження коду"

Мова про всі типи ін'єкцій: SQL, NoSQL, LDAP - що завгодно. Впровадження коду стає можливим, коли неперевірені дані відправляються інтерпретатору як частина команди або запиту. Такий "зловмисний" запит благополучно виконується і завдає свої збитки. У 90% випадків отриманого доступу до закритої бази даних через веб було реалізовано через атаки типу ін'єкції.

• A2:2017 - Некоректна аутентифікація

Функції додатків, які відповідають за аутентифікацію і управління сесіями, найчастіше застосовуються неправильно, наслідком чого стає компрометація паролів, ключів, сеансових токенов, і навіть можливість повністю перехопити сеанс користувача. Наприклад, коли людина користується публічним WI-FI і раптово виявляє, що від його імені здійснюються якісь дії на публічних веб-ресурсах - це рівень A2.

• A3:2017 - Розкриття чутливої інформації

Багато веб-додатків та API можуть некоректно зберігати і обробляти важливу інформацію персональних даних. Зловмисники можуть вкрасти або змінити таку інформацію, що може стати основою для серйозних фінансових або репутаційних втрат. Чутлива інформація повинна зберігатися належним чином, а також повинна бути захищена при передачі по каналах зв'язку.

• A4:2017 - Впровадження зовнішніх XML-сутностей (XXE)

Багато старих або неправильно сконфігурованних XML-процесорів можуть використовувати зовнішні дані з посилань в XML-файлах. Такі зовнішні дані можуть містити шкідливий код, який дозволить виконати на цільовій машині практичний будь-який сторонній код.

• A5:2017 - Порушений контроль доступу

Матриця доступу може бути некоректно застосована до конкретної системи, таким чином, що нелегітимні користувачі легко отримують доступ до закритих областях сайтів або отримують можливість змінювати права на ресурси на свій розсуд.

• A6:2017 Security Misconfiguration - Помилки в конфігурації

Йдеться мова про більш глобальні речі, як відсутність своєчасного оновлення серверного та прикладного ПО, наявність важливих відомостей в повідомленнях про помилки або навіть в HTTP-заголовках. Додаток може бути практично ідеальним, але якщо веб-сервер, на якому воно запущено, має проблеми з базовою конфігурацією, то система може бути легко скомпрометованою.

• A7:2017 - Міжсайтовий скриптинг (XSS)

XSS виникає тоді, коли програма включає в себе недовірені дані без належної перевірки. Наприклад, програмний код рекламного банера може містити скрипт для перехоплення призначених для користувача даних, дефейса сайту або навіть прозоре перенаправлення на інші сайти.

• A8:2017 - Небезпечна десеріалізація

Небезпечна десеріалізація, як правило, веде до віддаленого виконання коду. Суть в тому, що недовірені дані можуть зруйнувати логіку вашої програми, як тільки будуть десеріалізовані. Досить екзотична на перший погляд вразливість, однак займає своє почесне місце в списку.

• A9:2017 - Використання компонентів з відомими вразливостями

Бібліотеки, фреймворки, операційні системи та інші компоненти інформаційних систем потрібно своєчасно оновлювати. В іншому випадку відома уразливість в одній бібліотеці зможе поставити під удар великий servis, який використовує навіть одну функцію з вразливої бібліотеки.

• A10:2017 - Недостатній моніторинг

Система, без інструментів моніторингу. Мова навіть не про підключеної SIEM-системи, а просто про банальне логування основних подій сервера. На жаль, не рідкість, коли злом системи помічають через півроку після власне злому, причому дізнаються про це не з логів, а від зовнішніх спостерігачів.

Висновки. Отже, класифікація загроз безпеки веб-додатків є необхідністю, яка показує актуальні проблеми безпеки і розподіляє ступінь їх загроз. Знаючи цю інформацію, веб-програмісти зможуть правильно оцінити ризики і створити більш досконалу модель безпеки для своїх додатків, що в цілому зробить всю глобальну інформаційну середу більш захищеною.

Література:
1. [Електронний ресурс]. — Режим доступу: https://www.owasp.org/images/9/96/OWASP_Top_10-2017-ru.pdf
2. [Електронний ресурс]. — Режим доступу: https://habr.com/ru/company/gaz-is/blog/415283/

Дослідження шляхів та розроблення рекомендацій щодо захисту кінцевих точок корпоративної інформаційної системи на прикладі Sophos Intercept X

Кабанов Ярослав Вадимович
Державний університет телекомунікацій,
м. Київ

У сучасному світі корпоративна інформаційна система використовується все частіше. Необхідність цієї системи занадто масштабна , оскільки вона підтримує автоматизацію функцій управління в корпорації , або на підприємствах. Важливим фактом може слугувати постачання інформації для прийняття рішень ,яке в свою чергу піддається управлінню. У даній системі ефективно реалізована управлінська ідеологія , за рахунок цього спостерігається об'єднання бізнес- з прогресом стратегій інформаційних технологій. Заходи, спрямовані на протидію несанкціонованого доступу до конфіденційних даних, визнані створити оптимальні умови для вирішення проблеми забезпечення інформаційної безпеки, що здійснюються за допомогою централізованого управління процесом обробки охороняється інформації.

Управління безпекою корпоративної системи передбачає злагоджену координацію дій всіх структурних підрозділів щодо реалізації політики інформаційної безпеки, зосередження корпоративних ресурсів на вирішенні завдань в залежності від ситуації, що склалася, контроль за своєчасністю та повнотою виконання вимог затвердженої політики [1].

На сьогодення було сформовано новий тип продуктів - платформа захисту кінцевих станцій, або Endpoint Protection Platform (EPP). Endpoint Protection Platform - це система комплексного захисту кінцевої точки, що включає в себе як класичну функціональність антивірусного захисту, так і розширені технології безпеки- персональні міжмережеві екрани, системи запобігання вторгнень, системи контролю портів і пристроїв, що підключаються, системи шифрування дисків та ін.. З певного моменту більшість EPP-рішень перестали задовольняти сучасним вимогам до безпеки кінцевих станцій. В першу чергу це було пов'язано з ростом спрямованих атак, які в основному використовують уразливості нульового дня і відрізняються масовістю завдяки використанню ботнетів і внутрішньої архітектури горизонтального поширення.

Також необхідно відзначити окремий клас загроз - кріптолокеров (або шифрувальників), які в принципі, з точки зору системного програмного забезпечення, не роблять нічого протиправного. Відмінною рисою всіх цих атак є те, що вони не використовують відомі підходи і проломи, а експлуатують ще невідомі уразливості і способи свого поширення. Безумовно, EPP-рішення були змушені еволюціонувати, щоб відповідати сучасним викликам в сфері захисту кінцевих станцій.З метою захисту інформації обмеженого доступу, що циркулює всередині автоматизованої інформаційної системи, застосовуються сертифіковані по встановленим вимогам программно-апаратні засоби захисту інформації [2].

В наш час дуже важливо правильно вибирати засіб захисту кінцевих точок задля забезпечення безпеки корпоративної інформаційної мережі.

Розглянемо один з найкращих продуктів на ринку, а саме *Sophos X* [3].

Sophos пропонує великий інтегрований набір безпечних рішень, що охоплюють кінцеву точку, мобільний, мережу, електронну пошту, публічну хмару, Інтернет та кероване виявлення та реагування. Пропозиція компанії в простір EPP компанії Intercept X витіснила

Sophos за межі його кореневих SMB та підвищила рівень обізнаності в торгових організаціях підприємств

У листопаді 2018 року Sophos вийшов на ринок EDR з Intercept X Advanced. Intercept X використовує машинне навчання завдяки придбанням Invincea та SurfRight та органічно розвинених функцій. У січні 2019 року компанія придбала DarkBytes, стартап, що спеціалізується на криміналістиці кінцевих точок, для забезпечення розширених можливостей EDR. DarkBytes тепер є основоположним елементом керованих служб виявлення та реагування Sophos.

В першу чергу розглянемо сильні сторони , такі як:

Клієнти Intercept X сповіщають про сильну впевненість не лише у захисті від більшості програм, що вимагається, але й у можливості відкотити зміни, внесені процесом вимога програмного забезпечення, що уникає захисту;

Хмарна консоль адміністрування Sophos Central керує іншими аспектами платформи безпеки постачальника з однієї консолі, включаючи шифрування диска, захист сервера, брандмауер та шлюзи електронної пошти.

Intercept X забезпечує простий робочий процес для управління справами та розслідування підозрілих чи зловмисних подій.

Також, слід розглянути й недоліки:

Аналіз причин Intercept X не доступний для клієнтів, які використовують локальну версію захисту від кінцевої точки Sophos. Дійсно, Sophos навмисно орієнтований на Sophos Central як основну пропозицію, і замовники Sophos повинні очікувати, що він отримає більшість зусиль з розвитку.

Клієнти повинні вивчити функції Intercept X EDR у версії Sophos Linux та визначити, чи відповідають їх потребам з точки зору паритету функцій.

Робочий процес Intercept X EDR забезпечує основну співпрацю; однак клієнти повинні дослідити, чи забезпечує їх поточна пропозиція розширену співпрацю між групами реагування на інциденти.

Повний журнальний криміналістичний знімок Intercept X EDR зберігається на кінцевій точці, що робить його чутливим до фальсифікацій та складним запитам. Розширені правила полювання та власні виявлення потребують криміналістичної консолі. Можливість роботи криміналістичної консолі від придбання DarkBytes ще не інтегрована в центральну консоль управління Sophos або її локальну консоль і повинна розгортатися окремо за допомогою окремого агента. (Зараз інтегрований агент перебуває в ранньому доступі, і, як очікується, він буде повністю доступний у вересні.)

Деякі клієнти повідомляють, що встановлення агента та оновлення програмного забезпечення в місцях з низькою пропускною здатністю можуть бути проблематичними.

Отже виходячи з цього, робимо виксновок що аналіз алгоритмів глибокого навчання у Intercept X легко доступний та візуально привабливий для користувачів і надає клієнтам наочний спосіб підтвердити їхнє використання данним продуктом

Можливості запобігання експлуатації зосереджуються на інструментах, прийомах та процедурах, які є загальними для багатьох сучасних атак.

Література:

1. Огляд ринку систем захисту кінцевих точок [Електронний ресурс] – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Market_Analysis/endpoint-protection-platform#part2
2. «Засоби та методи захисту інформації» [Електронний ресурс] – Режим доступу до ресурсу: https://buklib.net/books/28625/
3. SOPHOS Intercept X [Електронний ресурс] – Режим доступу до ресурсу: https://roi4cio.com/catalog/product/sophos-intercept-x

КІБЕРБЕЗПЕКА РОЗУМНИХ МЕРЕЖ

Коваленко С.В.

Анотація. У даній роботі розглядаються заходи безпеки розумних мереж від хакерських атак.
Ключові слова: розумна мережа, електричні мережі, кібербезпека, зломи, віруси, хакерська атака.

У нашому світі все більше впроваджуються різні гаджети і сучасні технології для спрощення повсякденного життя. Щодня ми використовуємо безліч приладів, які дозволяють заощадити вільний час, підвищити ефективність праці, автоматизувати робочі процеси. Такі пристрої охоплюють всі сфери життєдіяльності людини, зберігають в собі важливу інформацію, мають можливість управління виробництвом.

Втрата доступу до інформаційних систем, контролю над ними може привести до несприятливих наслідків. Кожен з нас стикався з комп'ютерними вірусами, зі зломами соціальних мереж, особистих кабінетів і піддавався ризику витоку даних. Кібератаки відбуваються і на більш великі системи, перерва в роботі яких може призвести до тяжких наслідків. Уявіть собі масштаб катастрофи, якщо хакери отримають контроль над національною енергетичною мережею. Кібератака в такій ситуації може загрожувати роботі систем безпеки і викликати перебої в подачі електроенергії населенню, в результаті репутація компанії серйозно постраждає.

На сьогоднішній день стрімко розвиваються інтелектуальні енергосистеми SmartGrid, що представляють собою сукупність споживачів, які підключені до генеруючих джерел і електроустановок, програмно-апаратні засоби, а також інформаційно-аналітичні та керуючі системи, що забезпечують надійність і якість передачі електричної енергії від джерела до приймача своєчасно і в необхідній кількості. Однак інформаційній безпеці цих систем не приділяється достатньої уваги. [2]

Дистанційна система управління, тобто через інтернет, має свої слабкі сторони і може піддаватися загрозам злому і вірусним зараженням систем.

Управління здійснюється центральним сервером – це більш потужний, вузькоспеціалізований комп'ютер, що відрізняється від звичайного ПК програмним забезпеченням.

При з'єднанні з інтернетом «розумна мережа» стає вразливою, але незважаючи на це система підключена до нього постійно, адже це є необхідним для дистанційного контролю або управління. Зловмисники мають можливість отримати доступ до інформації, використовуючи також уразливості смартфона, через який відстежується система.

Злому навіть піддаються системи, які не підключені до мережі Інтернет. Часто інформація від датчиків контролю до центрального сервера передається через Wi-Fi або Bluetooth, так як бездротове з'єднання більш зручне. Однак, це є слабким місцем, так як для злому паролів не потрібно спеціальних пристроїв.

Таким чином, для запобігання стороннього проникнення доцільно використовувати систему «SmartGrid» розподіленого типу, в якому відсутній керуючий центр. Злом системи може призвести до її виходу з ладу, збоїв в роботі приладів, до витоку конфіденційної інформації, до знищення програм управління та інших негативних наслідків. [1]

Звичайно, що атака електромереж – нелегке завдання, для якого необхідні знання обладнання, програмних забезпечень та методів управління, контролю системою.

Основні причини, що ослабляють захист «розумних мереж», – такі ж, як і в звичайних комп'ютерних мережах. Наприклад, застосування звичайного комп'ютера в якості контролера і систем з функцією дистанційного керування, яка підключається через Інтернет, використання програм Windows, які значною мірою схильні до хакерських атак, відкритий доступ до управління у великої кількості персоналу.

Для того, щоб отримати впевненість у безпеці мережі і захистити її, існують такі способи: впроваджувати сучасні контролери, що відрізняються від простих ПК; для систем «розумна мережа» слід використовувати операційні системи і програми вузькопрофільної

спеціалізації, так як вони менш вразливі до хакерських атак; інформація про систему повинна бути секретною і закритою, а доступ необхідно обмежити стороннім особам. [3]

Необхідно пам'ятати і про звичайні правила безпеки комп'ютерних мереж: використовувати системи з відключенням дистанційного керування через інтернет; для обміну даними між пристроями встановлювати секретний цифровий ключ. Так вся інформація між сервером і контролером через мережу інтернет буде передаватися зашифрованою. До того ж, рекомендується записати майстер-ключ кожній групі контролерів для того, щоб вхід в систему без нього був неможливий.

Також необхідно використовувати захист Firewall, тобто «стіну» між комп'ютером та Інтернетом, яка пропускає тільки потрібні вам файли та програми.

Можна застосовувати двухфакторную аутентифікацію: після введення логіна і пароля по SMS приходить багатозначний код, який видається один раз і на короткий час. Такий метод забезпечує надійний захист від перехоплення доступу. Для підвищення рівня безпеки слід використовувати програму SMS-оповіщення, що попереджає співробітників про спроби злому. [4]

Висновки: Створити віруси для проникнення в систему досить важко. Але такі віруси вже існують, і їх будуть розвивати, а значить необхідно зміцнювати захист. Якщо ж кібератака була здійснена, встановити особу злочинця проблематично. Слід розширити нормативну базу по експлуатації розумних мереж, розробити міжнародні акти по їх безпеки. Всі злочини повинні переслідуватися за законом.

Список використаної літератури:

1. SmartGrid або розумні мережі електропостачання [Електронний ресурс]. URL:http://www.eneca.by/ru_smartgrid0/ (Дата звернення 27.03.2020).
2. Ігнатіч А.В, Ледин С.С. Розвиток промислових стандартів внутрішньо- і межсистемного обміну даними інтелектуальних енергетичних систем // Автоматизація та IT в енергетиці. - 2010. - № 10. - С. 39-43.
3. Костров Д. «Розумні мережі електропостачання» (smartgrid) і проблеми з кібербезпекою // Інформаційна безпека [Електронний ресурс]. URL: http: //www.itsec.ru/articles2/in-ch-sec/umnyeseti-elektrosnabzheniya-smart-grid-i-problemy-s-kiberbezopasnostyu (Дата звернення 27.03.2020).
4. Семенов В. Технологія Smartgrid і майбутнє світової електроенергетики // Електрик. Міжнародний електротехнічний журнал. 2013. № 12.- С. 16-20.

СОЦІАЛЬНІ МЕРЕЖІ ТА КІБЕРБЕЗПЕКА

Колісник Д.Р

Анотація. Сайти соціальних мереж забезпечують простір, де користувачі відчувають себе в безпеці, взаємодіючи з друзями і сім'єю. Розглянуто розвиток соціальних мереж в кіберпросторі. Виявлено негативні наслідки аналізу інформації в соціальних мережах.

Розвиток соціальних мереж створює нові проблеми в області кібербезпеки. Хакери вже давно покладаються на "соціальні інжиніринг", переконуючи людей розкривати інформацію про те, що вони не повинні завойовувати довіру мішеней, і скомпрометувати їх мережі. У міру того, як ми стаємо все більш соціальними через ці соціальні мережі, компанії повинні знаходити нові способи захисту особистої інформації. Соціальні мережі відіграють величезну роль в забезпеченні кібербезпеки і вносять внесок у кібер-загрози.

У міру того як корпоративна безпека поліпшується, противники все більше покладаються на "соціальну інженерію", щоб завоювати довіру

мішеней, переконувати людей розкривати інформацію, яку вони не повинні розкривати, і згодом компрометувати мета мережі. Майже сорок відсотків записів, скомпрометованих в результаті злому кібернетичних даних, були скомпрометовані як в результаті інцидентів із застосуванням соціальної тактики. Більш того, галузеві дані свідчать про те, що ловля списи лежить в основі більшість спрямованих атак. Тому люди повинні вживати відповідних заходів, особливо при роботі з соціальними мережами в щоб запобігти втраті їх інформації.

Здатність людей ділитися інформацією з мільйонною аудиторією лежить в основі конкретного виклика, який соціальні мережі кидають бізнесу. Хоча соціальні мережі можуть використовуватися для кіберзлочинів, ці компанії не можуть дозволити собі припинити використання соціальних мереж, оскільки вони відіграють важливу роль в рекламі компанії.

Висновки. Здатність виявляти, розслідувати, аналізувати і реагувати на кіберзагрози і атаки є невід'ємним компонентом кібербезпеки. Отже, компанії повинні розуміти і усвідомлювати важливість аналізу інформації, особливо, в соціальних розмовах і надавати відповідні рішення щодо забезпечення безпеки, щоб триматися подалі від ризиків. Необхідно працювати з соціальними мережами, використовуючи певні політики і правильні технології.

Література:

1. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
2. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
3. IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “July/ Aug 2018.

ДОСЛІДЖЕННЯ МЕТОДИКИ ПРОТИДІЇ СОЦІАЛЬНОГО ІНЖЕНІРИНГУ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Косенко В.В

Сьогодні, коли володіння інформацією стало активно використовуватися в комерційних цілях, важливу роль в інформаційній безпеці відіграє людський фактор. Технології безпеки, такі як міжмережеві екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак і т.д. малоефективні в протистоянні зловмисники, які використовують методи соціальної інженерії. У зв'язку з цим актуальною стає проблема роботи з персоналом, навчання співробітників застосуванню політики безпеки і технікам протистояння соціоінженерам, що є запорукою безпеки для баз корпоративної інформації.

Соціальна інженерія (від англ. Social Engineering) - це використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації. Цей метод зазвичай застосовується без комп'ютера, з використанням звичайного телефону, поштового листування і т.д. В ході атаки зловмисник встановлює контакт з носієм інформації (вводить в оману, входить в довіру) і таким чином намагається отримати відомості, які або складно отримати іншим шляхом або ці шляхи є більш ризикованими.

Найчастіше соціальну інженерію розглядають як незаконний метод отримання інформації, проте це не зовсім так. Якщо розглядати сучасну професійну соціальну інженерію, то область її застосування цілком законна - наприклад, вона допомагає досягти спочатку недосяжний результат, або «програмувати» для здійснення позитивних і корисних дій конкретної людини або групи людей. Звичайно, сьогодні соціальну інженерію часто використовують в інтернеті для отримання закритої інформації або інформації, яка є великою цінністю. Але сучасні соц-інженери використовують свої навички для підвищення результатів у бізнесі і житті

За результатами робіт встановлено, що 26% співробітників здійснюють перехід по посиланню на фішингових веб-ресурс, причому практично половина з них в подальшому вводять свої облікові дані в підроблену форму аутентифікації. Кожен шостий співробітник піддає корпоративну інфраструктуру ризику вірусного зараження шляхом запуску прикладеного до листа файлу. Крім того, 12% співробітників готові вступити в діалог з порушником і розкрити інформацію, яка в подальшому може бути використана при проведенні атак

Всього при оцінці обізнаності співробітників в 2018 році було відправлено понад 1300 листів, половина з яких містила посилання на фішингових ресурс, а друга - файл зі спеціальним скриптом, який відправляв нашим фахівцям інформацію про час відкриття файлу, а також адресу електронної пошти співробітника. Справжній зловмисник в вміст файлу може додати набір експлойтів, спрямованих на експлуатацію різних вразливостей. Подібна атака може привести до отримання зловмисником контролю над робочою станцією відповідного користувача, поширенню шкідливого коду, відмови в обслуговуванні і інших негативних наслідків.

Основним способом захисту від методів соціальної інженерії є навчання співробітників. Всі працівники компанії мають бути попереджені про небезпеку розкриття персональної інформації та конфіденційної інформації компанії, а також про способи запобігання витоку даних. Крім того, у кожного співробітника компанії, в залежності від підрозділу і посади, повинні бути інструкції про те, як і на які теми можна спілкуватися зі співрозмовником, яку інформацію можна надавати для служби технічної підтримки, як і що повинен повідомити співробітник компанії для отримання тієї або іншої інформації від іншого співробітника.

Крім цього, можна виділити наступні правила:

• Облікові дані користувача є власністю компанії.

Всім співробітникам в день прийому на роботу має бути роз'яснено те, що ті логіни і паролі, які їм видали, не можна використовувати в інших цілях (на web-сайтах, для особистої пошти тощо), передавати третім особам або іншим співробітникам компанії, які не мають на це право.

• Необхідно проводити вступні та регулярні навчання співробітників компанії, спрямовані на підвищення знань з інформаційної безпеки.

• Обов'язковим є наявність регламентів з безпеки, а також інструкцій, до яких користувач повинен завжди мати доступ. В інструкціях повинні бути описані дії співробітників при виникненні тієї чи іншої ситуації.

• На комп'ютерах співробітників завжди має бути актуальне антивірусне програмне забезпечення.

На комп'ютерах співробітників також необхідно встановити брандмауер.

• У корпоративної мережі компанії необхідно використовувати системи виявлення та запобігання атак.

• Всі співробітники повинні бути проінструктовані, як вести себе з відвідувачами.

• Необхідно максимально обмежити права користувача в системі.

Отже, корпоративні інформаційні системи як і раніше уразливі до атак з боку зовнішніх і внутрішніх зловмисників. Якщо при проведенні зовнішнього тестування на проникнення все частіше зустрічаються компанії, які стурбовані питанням захищеності свого мережевого периметра, то при тестуванні захищеності корпоративної системи від імені внутрішнього зловмисника ситуація значно гірша. У 2018 році від особи зовнішнього зловмисника, котрий використовує, в числі іншого, методи соціальної інженерії і атаки на бездротові мережі, подолати мережевий периметр вдалося в 68% робіт. При цьому від імені внутрішнього порушника повний контроль над ресурсами був отриманий у всіх без винятку проектах - незважаючи на використовувані в компаніях технічні засоби і організаційні заходи для захисту інформації.

НЕЧІТКА МОДЕЛЬ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ERP-СИСТЕМ

Кожухівський А.Д.,д.т.н., професор
Курило Олена Василівна, магістрант 125 Кібербезпека
Державний університет телекомунікацій
м. Київ

В ERP-системі, як центральній інформаційній системі підприємства, зосереджено велику кількість конфіденційної інформації та даних обмеженого доступу. Розкриття такої інформації, або порушення доступності та цілісності в результаті різного роду інцидентів може принести підприємству значних збитків, що можуть біти виражені як в матеріальній, так і в нематеріальній формі. Тому проблеми забезпечення інформаційної безпеки ті контролю ризиків є актуальними для ERP-систем.

Enterprise Resource Planning System (ERP-система) – це корпоративна інтегрована інформаційна система, що реалізує концепцію узгодженого рішення завдань планування, обліку, контролю й управління виробничими і фінансовими ресурсами підприємства, створюючи єдине інформаційне середовище для автоматизації рішення цих завдань [1].

Ключовим аспектом будь-якої стратегії безпеки є здатність досягти рівня безпеки, який належним чином демонструє прихильність організації до регламентів інформаційної безпеки та безпеки даних, зібраних від своїх партнерів. Порушення інформаційної безпеки, включаючи невідповідність

нормативним стандартам, може призвести до фінансових та репутаційних наслідків як для великих, так и для малих підприємств [2].

У загальному випадку розрахунок ризиків інформаційної безпеки ERP-систем повинен проводитися по відношенню до кожного критичного бізнес-процесу та інформаційного ресурсу лише за тими загрозами та уразливостями, які є для них актуальними. Для кожної пари загроза-властивість повинна проводиться оцінка ймовірності її виникнення, оцінка цінності та оцінка впливу реалізації цієї пари на цілісність, конфіденційність, доступність та спостережуваність інформаційного ресурсу ERP-системи [3].

Для оцінки ризику відповідно факторів його виникнення пропонується використовувати співвідношення :

$$R_{ij} = A_j^v \cdot F_{ij}^e \cdot P_i^t \cdot P_{ij}^v,$$

де: R_{ij} – ризик *j*-го ресурсу при реалізації *i*-ї загрози, A_j^v – вартість (цінність) *j*-го ресурсу; F_{ij}^e – вплив наслідку при реалізації і-ї загрози для j-го ресурсу, або схильність j-го ресурсу до і-ї загрози, P_i^t – ймовірність виникнення і-ої загрози, P_{ij}^v – вразливість j-го ресурсу для і-ої загрози.

На практиці оцінка ризиків інформаційної безпеки є досить складним та повним невизначеностей процесом,ёпо оскільки оцінки факторів їх виникнення мають властивості багатозначності та невизначеності, не є лінійними, динамічно змінюються, носять суб'єктивний характер, оскільки залежать від досвіду фахівців та експертів з інформаційної безпеки.

Відповідно до таких умов для визначення рівня ризику бачиться доцільним використання апарату теорії нечітких множин, що дає змогу описувати оцінки нечіткими змінними, а знання експертів нечіткими висловлюваннями, оперувати ними і робити нечіткі висновки. Застосування лінгвістичного підходу забезпечить опис значення рівня ризику, цінності ресурсу, впливу наслідку на ресурс, ймовірності виникнення загрози, вразливості захисту ресурсу в умовах нечіткої інформації про них.

Для оцінки ризиків пропонується нечітка продукційна модель структури MISO (Multi Inputs – Single Output, багато входів – один вихід) з чотирма вхідними параметрами (X_1, X_2, X_3, X_4) та одним виходом Y, що використовує систему нечіткого висновку FIS (Fuzzy Inference System)(рис.1).

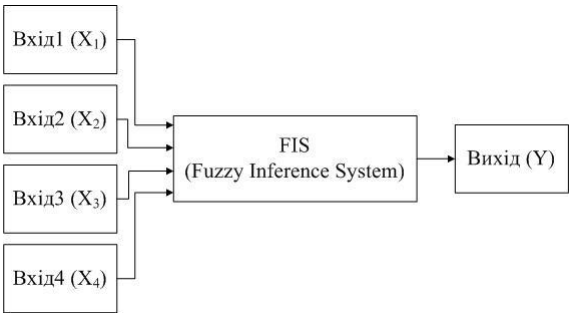

Рис. 1. Нечітка модель оцінки ризику

Кожен фактор рівня ризику інформаційної безпеки та рівень ризику опишемо лінгвістичними змінними $X \in \overline{X}$, де $\overline{X}$множина лінгвістичних змінних моделі має вигляд: $\overline{X}$ = {« Цінність ресурсу», «Вплив наслідку», «Ймовірність загрози», «Вразливість ресурсу», «Ризик»}, а оцінку ризику інформаційної безпеки як функцію від вхідних лінгвістичних змінних:

$$Y = f_Y(X_1, X_2, X_3, X_4).$$

Лінгвістичні змінні опишемо терм-множинами якісних термів (Т):

– цінність ресурсу: $T(X_1)$={Низька (LW); Середня (MW); Висока (HW)};

– вплив наслідку: $T(X_2)$ = {Не суттєвий (VLC); Низький (LC); Середній (MC); Суттєвий (HC), Дуже великий (VHC)};

– ймовірність загрози: $T(X_3)$ = {Дуже низька (VLT); Низька (LT); Середня (MT); Висока (HT); Дуже висока (VHT)};

– вразливість ресурсу: $T(X_4)$ = {Низька (LV); Середня (MV); Висока (HV); Критична (CV)};

– ризик: T(Y) = {Дуже низький (VLR); Низький (LR); Середній (MR); Високий (HR); Дуже високий (VHR)}.

Базу нечітких задамо правилами ПР виду «якщо-то», наприклад:

ПР1: **якщо** X_1 **є** LW **та** X_2 **є** VLC **та** X_3 **є** VLT **та** X_4 **є** LV, **то** Y **є** VLR

ПР2: **якщо** X_1 **є** HW **та** X_2 **є** LC **та** X_3 **є** VLT **та** X_4 **є** CV, **то** Y **є** MR і т.д.

Моделювання оцінки ризику проведено за допомогою пакету інструменту Fuzzy Logic Toolbox [4] пакету MATLAB: побудовано структуру нечіткої продукційної моделі (рис.2), задано функції приналежності вхідних параметрів розподілом Гауса (наприклад, рис.3 – X_4 ,вразливість ресурсу), сформовано базу продукційних правил (рис.4). В результаті моделювання отримано FIS модель, що надає можливість отримувати оцінки ризику та візуально спостерігати результатами роботи системи нечіткого висновку за допомогою діаграми (рис.5).

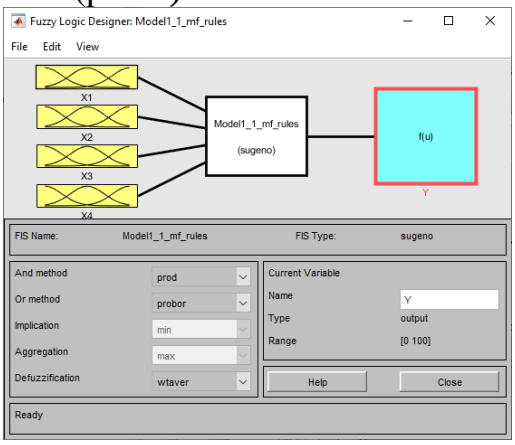

Рис.2. Структура нечіткої моделі

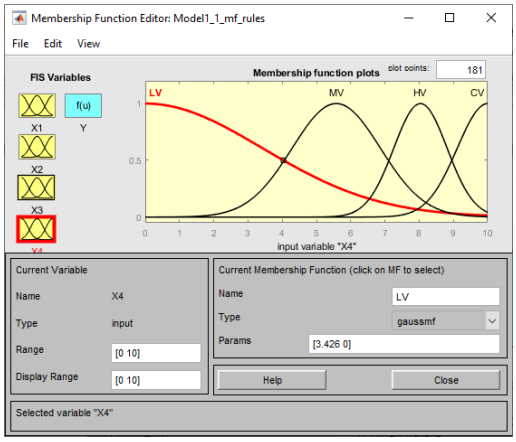

Рис.3. Функції приналежності

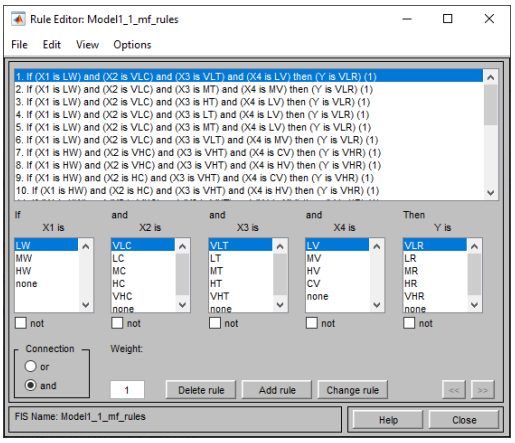

Рис.4. База продукційних правил

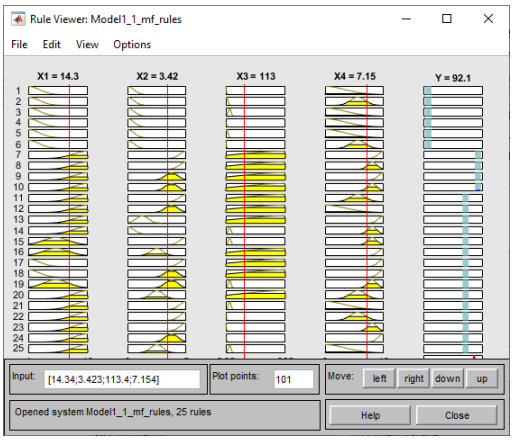

Рис.5. Діаграма нечіткого висновку

Таким чином, було запропоновано нечітку продукційну модель та виконано моделювання процесу отримання оцінки ризику інформаційної безпеки на основі оцінок факторів його виникнення та наслідків його можливої реалізації для інформаційного ресурсу підприємства.

Розроблена нечітка модель має певні недоліки, такі як: можливість виявлення вихідного набор нечітких правил неповним або суперечливим, суб'єктивність у виборі виду і параметрів функцій приналежності або відсутність можливості автоматичного набуття знань. Для усунення цих недоліків у подальшому пропонується використати нечітку адаптивну продукційну модель, що дозволить виконувати корекцію параметрів функцій приналежності за результатами її навчання.

Література:

1. *ERP-система (планування ресурсів підприємства) [Електронний ресурс] / Навчальні матеріали онлайн (pidruchniki website). – Режим доступу: https:// pidruchniki.com/1171062647760/informatika/erp-sistema_planuvannya_ resursiv_ pidpriyemstva.*
2. *Security issues in ERP. Security, Audit and Control Features SAP ERP 4th Edition, Audit Program. – Isaca. – 2015. – 574p.*
3. *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст]: НД ТЗІ 2.5-004-99. – 1999. – Чин. 1999.07.01. – К. : ДСТСЗІ СБ України, 1999. – 57 с.*
4. *Fuzzy Logic Toolbox [Електронний ресурс] // Центр Инженерных Технологий и Моделирования Экспонента. – Режим доступу: https://exponenta.ru/fuzzy-logic-toolbox.*

Козачок В.А., Лакатош Г.Ф.

ПОЛІТИКА БЕЗПЕКА В СУЧАСНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Доповідь присвячена актуальній темі «Політика безпека в сучасних інформаційно-телекомунікаційних системах». Політика інформаційної безпеки (ПІБ) є планом високого рівня, в якому описуються цілі і завдання заходів в сфері безпеки. Розглянуто яким чином потрібно розробляти правила безпеки, адже перш ніж починати розробку керівних документів, необхідно визначити глобальні цілі політики. Чи полягає мета в захисті компанії і її взаємодії з клієнтами? Або ж необхідно забезпечити захист потоку даних в системі? У будь-якому випадку, на першому етапі необхідно визначитися в тому, що потрібно захищати і чому саме це повинно бути захищене.

Ключові слова: політика безпеки, інформаційні ресурси, правила безпеки, автоматизована система, захист інформації, правила безпеки.

Вступ

При створенні інформаційної інфраструктури корпоративної автоматизованої системи (АС) на базі сучасних комп'ютерних мереж неминуче виникає питання про захищеність цієї інфраструктури від загроз безпеки інформації. Наскільки адекватні реалізовані в АС механізми безпеки існуючих ризиків? Чи можна довіряти цій АС обробку (зберігання, передачу) конфіденційної інформації? Чи є в поточній конфігурації АС помилки, що дозволяють потенційним зловмисникам обійти механізми контролю доступу? Чи містить встановлене в АС програмне забезпечення (ПО) уразливості, які можуть бути використані для злому захисту? Як оцінити рівень захищеності АС і як визначити чи є він достатнім в даному середовищі функціонування? Які контрзаходи дозволять реально підвищити рівень захищеності АС? На які критерії оцінки захищеності слід орієнтуватися, і які показники захищеності використовувати?

Такими питаннями рано чи пізно задаються всі фахівці IT-відділів, відділів захисту інформації та інших підрозділів, що відповідають за експлуатацію і супровід АС. Аналіз захищеності АС від загроз безпеки інформації робота складна. Вміння оцінювати і управляти ризиками, знання типових загроз і вразливостей, критеріїв і підходів до аналізу захищеності, володіння методами аналізу і спеціалізованим інструментарієм, професійне знання різних програмно-апаратних платформ, що використовуються в сучасних комп’ютерних мережах - ось далеко не повний перелік професійних якостей, якими повинні володіти фахівці, які проводять роботи з аналізу захищеності АС.

Аналіз захищеності є основним елементом таких взаємно перетинаючих видів робіт як атестація, аудит і обстеження безпеки, експлуатація АС.

Успіх бізнесу забезпечується ретельним плануванням, особливо в питаннях безпеки. Не думайте, що купивши міжмережеві екрани, можна вважати, що ваші мережі достатньо захищені. Перш необхідно визначити, що саме потрібно захистити.

1 Про політику інформаційної безпеки

Політика інформаційної безпеки (ПІБ) є планом високого рівня, в якому описуються цілі і завдання заходів в сфері безпеки. Політика не являє собою ні норматив, ні інструкції, ні засоби управління. Політика описує безпеку в узагальнених термінах без специфічних деталей. Вона забезпечує планування всієї програми безпеки так само, як специфікація визначає номенклатуру продукції, що випускається.

На сьогодні відомо достатньо велику кількість визначень ПІБ. Приведемо далеко не повний їх перелік. Наприклад:

1) політика інформаційної безпеки – це сукупність правил, що визначають і обмежують види діяльності об’єктів і учасників, системи ІБ;

2) політика інформаційної безпеки – це сукупність документованих управлінських рішень і розроблених превентивних заходів, направлених на захист інформаційних ресурсів (ІР);

3) політика інформаційної безпеки – це комплекс превентивних заходів щодо захисту конфіденційних даних та інформаційних процесів на підприємстві (організації).

Приведені вище дефініції однієї і тієї самої категорії наведені у передмові невипадково. Річ у тім, що мало хто, навіть з вузького кола фахівців, розуміє дійсну сутність ПІБ, а ще менша кількість людей спроможна до розробки та впровадження такої політики у конкретну організацію. Тому, як показує аналіз сучасного стану питання і власний практичний досвід, справи у визначеній галузі йдуть не кращим чином, у тому числі і в сенсі відсутності висококваліфікованих кадрів, для підготовки яких і створена книга, яку Ви тримаєте в руках.

Таким чином, розробка політики інформаційної безпеки – це процес суто практичного характеру, що безпосередньо ґрунтується на знаннях набутих студентами за усіма розділами інформаційної безпеки та який в першу чергу спрямовується на створення каркасу ІБ, тобто конкретних правил і рекомендацій, що регламентують функціонування всіх рівнів системи забезпечення інформаційної безпеки.

Коли люди заявляють, що технологічний процес не є частиною політики, завжди виникають питання. Технологічний процес являє собою детальний опис
всіх дій. А політика являє собою виклад цілей, які повинні бути досягнуті впровадженням цього технологічного процесу. Для опису політики використовуються загальні терміни, так що політика не оперує способами реалізації. Наприклад, якщо політика визначає єдине рішення виробника для єдиного контракту, то в компанії виникнуть труднощі, коли з'являється необхідність модернізації для створення нової продукції. Незважаючи на те, що при розробці політики може знадобитися технологічна документація, сама технологічна документація не повинна бути частиною політики.

2 Чому важливо працювати за правилами інформаційної безпеки?

Незважаючи на те, що політика не відповідає на питання, яким чином повинні досягатися технологічні цілі, все ж, визначивши належним чином, що необхідно зберегти, ми тим самим забезпечуємо належне управління процесом. У правилах безпеки описано, що має бути захищене і які обмеження накладаються на управління. Незважаючи на те, що в них не обговорюється ні
номенклатура виробленого продукту, ні виробничі цикли, все ж правила безпеки допоможуть краще орієнтуватися і при виборі продукту, і при виборі

шляхів розвитку компанії. Реалізація вимог політики забезпечить більш високу захищеність усієї системи.

Коли в розробці політики інформаційної безпеки бере участь керівництво, це говорить про те, що керівництво вітає ідею створення політики безпеки, наділяючи довірою всю програму безпеки. Підтримка керівництва завжди важлива. Без підтримки керівництва службовці не стануть сприймати політику серйозно. Тому, якщо не мати підтримку вищого керівництва, програма впровадження політики безпеки буде приречена на невдачу ще до закінчення її розробки.

3 Розробка правил безпеки

Перш ніж починати розробку керівних документів, необхідно визначити глобальні цілі політики. Чи полягає мета в захисті компанії і її взаємодії з клієнтами? Або ж необхідно забезпечити захист потоку даних в системі? У будь-якому випадку, на першому етапі необхідно визначитися в тому, що потрібно захищати і чому саме це повинно бути захищене.

Правила можуть бути написані для захисту апаратних засобів, програмного забезпечення, засобів доступу до інформації, людей, внутрішніх комунікацій, мережі, телекомунікацій, правозастосування тощо. Перед тим, як починати процес розробки правил, потрібно визначити, які системи і технологічні процеси є важливими для виконання завдань компанії. Це допоможе визначити, скільки і яких правил повинно бути розроблено для успішної діяльності компанії.

Правила інформаційної безпеки не повинні бути єдиним документом. Щоб спростити користування ними, правила можуть бути включені в кілька документів. Саме з тією ж метою ця книга розбита на окремі, об'єднані змістом, глави. Тому не прагніть описати політику компанії одним документом, просто розробіть необхідні вам керівні документи і назвіть їх главами опису політики інформаційної безпеки. Тоді їх буде легше розуміти, легше впроваджувати і простіше організувати вивчення цих документів, оскільки кожному аспекту політики безпеки буде присвячений свій власний розділ. Невеликі розділи також легше коригувати і оновлювати.

Скільки різних правил безпеки необхідно розробити? Для кожної системи, що забезпечує ваш бізнес, і кожної підзадачі, на які може бути розбита глобальна мета вашого бізнесу, необхідно розробити окремий документ. Абсолютно нормально розробляти антивірусний захист окремо від правил використання Internet. Загальноприйнята помилка полягає в спробах втиснути опис політики безпеки в один документ, який описує тільки загальні принципи.

В результаті з'являється великий документ, з яким дуже важко працювати, який, можливо, ніколи не буде прочитаний і не отримає ніякої підтримки.

На рис. 1 представлений приблизний перелік розробляючих правил інформаційної безпеки.

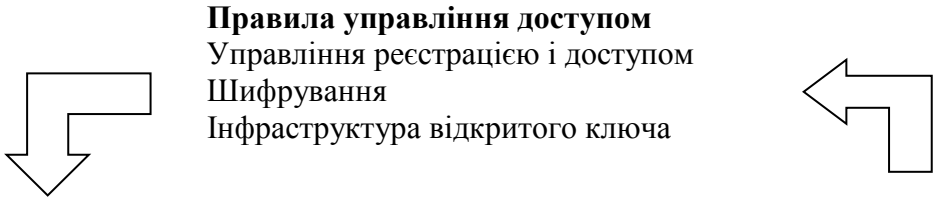

Рис. 1 Приблизний список систем, що підтримують бізнес, для яких розробляються правила безпеки

Розробка адекватної і актуальної політики інформаційної безпеки дозволить підвищити рівень довіри до компанії з боку акціонерів, потенційних інвесторів, ділових партнерів, професійних учасників ринку цінних паперів, уповноважених державних органів і інших зацікавлених сторін.

Висновки

Підводячи підсумок всьому вищесказаному, слід відзнаити, що в даний час питання побудови системи безпеки і аналізу захищеності корпоративних АС є вже досить добре опрацьованими. Є багатий арсенал засобів і методів для проведення подібних робіт. Використання формальних та неформальних методів дозволяє на практиці досить точно оцінювати захищеність АС, із застосуванням як якісних, так і кількісних шкал. Відпрацьовані методики проведення обстеження (аудиту) безпеки АС відповідно до перевіреними критеріями, затверджений ними в якості міжнародних стандартів, роблять можливим отримання вичерпної інформації про властивості АС, що мають відношення до безпеки. На практиці аналіз захищеності АС проводиться за допомогою потужного програмного інструментарію, в достатньому обсязі представленого на ринку засобів захисту інформації. Однак, якщо говорити про управління безпекою, то перш за все слід мати на увазі людський фактор, тобто інтелект керівника у формуванні правил інформаційної безпеки.

Розробка адекватної і актуальної ПІБ дозволить підвищити рівень довіри до компанії з боку акціонерів, потенційних інвесторів, ділових партнерів, професійних учасників ринку цінних паперів, уповноважених державних органів і інших зацікавлених сторін. Також впровадження ПІБ дозволить:

- підвищити загальний рівень захисту інформаційних ресурсів і IT – інфраструктури організації;

- скоординувати, формалізувати і зафіксувати вимоги і процедури забезпечення ІБ;
- мінімізувати ризики бізнесу шляхом захисту інтересів компанії в інфосфері;
- зафіксувати відповідальність між адміністраторами, користувачами і керівниками структурних підрозділів в частині, що стосується ІБ;
- забезпечити безпечне, довірене і адекватне управління підприємством;
- планувати і підтримувати безперервність бізнесу;
- підвищити якість діяльності щодо забезпечення ІБ;
- знизити витрати і підвищити ефективність інвестицій в ІБ;
- забезпечувати ІБ з урахуванням вимог національних і міжнародних стандартів.

Перелік посилань

1 Курило А.П. Основы управления информационной безопасностью. Учебное пособие для вузов. / А.П.Курило, Н.Г.Милославская, М.Ю.Сенаторов, А.И.Толстой / – М.: Горячая линия-Телеком, 2012. – 244 с.

2 Галашенко В. А. Информационная безопасность: практический подход. – М : Наука, 1998. – 301 с.

3 Петренко С.А. Политики информационной безопасности /С.А.Петренко, В.А.Курбатов / – М.: Компания АйТи, 2006. – 400 с.

4 Єжова Л.Ф., Хорошко В.О. та ін.. Управління інформаційною безпекою. В 2-х томах. – Вид. 2-е, доповн. і перероб. – К.: НАУ, 2012. – 316 с.

5 Політика інформаційної безпеки : [підруч. для студентів] / [О. Л. Голубенко, В. О. Хорошко., О. С. Петров та ін.]. – Луганськ : Східноукраїнський національний університет ім. В. Даля, 2009. – 300 с.

6 Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие.2-е изд. – М.: Издательско-торговая корпорация «Дашков и К°». 2005. – 336 с.

Лібега Лілія Андріївна, БСД-43
Державний університет телекомунікацій,
м. Київ

Програмний комплекс IBM i2 Analyst's Notebook надає можливість досліджувати групові структури і потоки інформації на схемі мережі, фокусуючись на взаємозв'язках, що існують між об'єктами. Цей тип аналізу називається *аналізом соціальних мереж (АСМ)*.

Стандартними показниками централізації АСМ є проміжковість (кількість шляхів, що проходять через кожен об'єкт), близькість (близькість об'єкта до інших в мережі) і ступінь (кількість прямих зв'язків). Ці показники дозволяють швидко визначити потенційних ключових осіб в мережі та складають представлення про різні соціальні взаємини між об’єктами мережі.

Проміжковість вимірює кількість шляхів які проходять через об’єкт. Цей показник може ідентифікувати об'єкти, які здатні контролювати потік інформації між різними частинами мережі. Такі об'єкти називають об'єктами-воротарями. Через об'єкт-воротар проходить багато шляхів, що дозволяє

йому направляти інформацію більшості інших об'єктів в мережі. В іншому варіанті шляхів, які проходять, може бути мало, але роль об'єкта може бути високою, якщо об'єкт знаходиться між різними мережевими кластерами. Проміжковість центральності вимірює як пряму, так і непряму близькість: пряма близькість - коли два об'єкти з'єднані зв'язком; непряма близькість - коли інформація може передаватися від одного об'єкта до іншого тільки по шляху, що проходить через один або кілька проміжних об'єктів.

Близкість об'єкта показує його розташування відносно інших об'єктів в соціальній мережі. У об'єкта з високим ступенем близькості шлях до інших об'єктів найбільш короткий. Цей показник дозволяє їм передавати і отримувати повідомлення швидше за всіх інших об'єктів в організації. Інформація проходить більшу відстань при передачі об'єкта на краю мережі, з'єднаному з невеликим числом інших об'єктів, або від нього. У таких об'єктів показник центральності близькості нижче.

Степінь центральності вимірює, наскільки об'єкт пов'язаний з іншими об'єктами, підраховуючи число прямих зв'язків кожного об'єкта з іншими об'єктами в мережі. Це допоможе зрозуміти наскільки активний об'єкт і хто з учасників мережі активний в максимальній степені.

Для визначення тісно пов'язаних груп в мережі має місце показник *ядерності*. К-ядро - це максимальна група об'єктів, всі з яких з'єднані щонайменше з k іншими об'єктами в групі. Цей показник допомагає визначити невеликі пов'язані ключові області в мережі. Щоб бути включеним в К-ядро, об'єкт повинен бути пов'язаний щонайменше з k іншими об'єктами в групі. Для визначення пов'язаних об'єктів неважливо, зі скількома іншими об'єктами вони з'єднані поза групою. Значення k іноді називають ядерністю групи.

АСМ може бути також посилена за рахунок використання зважених показників для визначення міцності різних взаємозв'язків (зв'язків), кожен з яких впливає на цільову мережу. Це допомагає отримати більш реальне уявлення про динаміку та структуру даної цільової мережі. [2].

Таким чином, завдяки АСМ можна визначити:

продуктивність мережі в цілому і її здатність досягти своїх ключових цілей;

неочевидні характеристики мережі, наприклад, існування меншої підмережі, що працює всередині мережі;

взаємозв'язки між значущими об'єктами, положення яких дозволяє найбільш сильно впливати на іншу мережу;

наскільки безпосередньо і швидко передається інформація між об'єктами в різних частинах мережі.

Література:

1. 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
2. Using IBM i2 Analyst's Notebook. IBM Knowledge Center [Електронний ресурс] – Режим доступу: https://www.ibm.com/products/enterprise-intelligence-analysis/details

ПРОТИДІЯ ВНУТРІШНІЙ ЗАГРОЗІ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВА НА ОСНОВІ IBM QRADAR SIEM З USER BEHAVIOR ANALYTICS FOR QRADAR

Ліщук Інна Володимирівна, БСД-42
Державний університет телекомунікацій,
м. Київ

З кожним роком, для підвищення ефективності сучасного бізнесу, все більше і більше використовуються інформаційні технології. Кожна компанія прагне оптимізувати та автоматизувати свої процеси, але при цьому виникає проблема забезпечення кібербезпеки корпоративних інформаційних систем, оскільки людський фактор є найбільшою небезпекою для них, адже саме людина, відповідно до сучасного підходу в безпеці, є основним джерелом порушень, загроз і ризиків.

З метою розуміння шляхів протидії внутрішній загрозі в корпоративних інформаційних системах підприємства на основі IBM QRadar SIEM з User Behavior Analytics for QRadar, пропонуються проаналізовані наступні питання: призначення, умови функціонування корпоративних інформаційних систем, аналіз внутрішніх загроз, проблеми їх виявлення, визначення ролі і місця процесу протидії внутрішній загрозі у забезпеченні кібербезпеки, аналіз методів виявлення порушника, способи застосування програмного комплексу User Behavior Analytics for QRadar, а також рекомендації щодо застосування методів та засобів протидії внутрішній загрозі в корпоративній інформаційній системі.

На сьогоднішній день корпоративні інформаційні системи є невід'ємною складовою конкурентного функціонування сучасного підприємства. Корпоративна інформаційна система - це інформаційна система, яка підтримує автоматизацію функцій управління і надає інформацію для поглиблення знань та прийняття управлінських рішень. В ній реалізована сучасна управлінська ідеологія, яка поєднує бізнес-стратегію підприємства і прогресивні інформаційні технології [1]. Забезпечення IT-безпеки підприємства вимагає комплексного підходу, який збалансовує захист як від зовнішніх, так і від внутрішніх загроз, але зазвичай приділяється достатньо уваги лише зовнішнім загрозам.

За результатами дослідження інституту «Ponemon», частота та вартість інсайдерських загроз різко зросли протягом останніх двох років. Загальна вартість інсайдерських загроз зросла, збільшившись на 31 відсоток – з 8,76 млн доларів у 2018 році до 11,45 млн доларів у 2020 році. Крім того, кількість інцидентів збільшилася на 47 відсотків – з 3200 в 2018 році до 4716 в 2020 році [2]. Ці дані показують, що інсайдерські загрози все ще залишаються тривалими і часто недооціненими загрозами кібербезпеки в організаціях, порівняно із зовнішніми загрозами.

Не залежно від того, чи інсайдерські загрози спричинені випадково або зловмисно, атаки не можуть бути пом'якшені лише технологією. Організаціям потрібна програма управління внутрішньою загрозою, яка поєднує людей, процеси та технології для виявлення та запобігання інцидентам в організації. Відомі чотири класи таких систем. Серед них: *системи моніторингу та аудиту*, *системи автентифікації*, *засоби шифрування* та *системи виявлення і попередження витоку інформації*.

Тому в останні роки на глобальному ринку систем забезпечення безпеки з'явилися рішення, призначені для аналізу поведінки користувача, тобто системи виявлення і попередження – User (and Entity) Behavior Analytics (UBA/UEBA). User (and Entity) Behavioral Analytics – клас систем, що дозволяють на основі масивів даних про користувачів. За допомогою алгоритмів машинного навчання і статистичного аналізу будувати моделі поведінки користувачів і визначати відхилення від цих моделей, як в режимі реального часу, так і ретроспективно.

Машинне навчання – це здатність вчитися з великої кількості даних, використовуючи алгоритми, побудовані людиною, для виконання завдань. Результат – автоматизоване, точне виявлення загрози та аномалії. Складаючи разом показники загрози, виявлені за допомогою різних алгоритмів, машинне навчання допомагає програмному забезпеченню чи рішенню виявляти

загрози з високою ймовірністю. Компанії повинні встановлювати критерії аномальної поведінки, яка зосереджує свою інсайдерську програму на навмисних та ненавмисних інсайдерських загрозах. Правила виявлення аномалій перевіряють результати збереженого потоку або виробляють пошук подій, щоб виявити, коли в мережі виникають незвичайні шаблони трафіку. Вони складається з: правил аномалій, правил порогів та правил поведінки.

Додаток User Behavior Analytics for QRadar допомагає визначити профілі ризику користувачів у мережі та вжити заходи, коли додаток повідомляє про поведінку, що може за собою спричинити інцидент безпеки. UBA інтегрується безпосередньо в рішення QRadar Security Analytics, який надає існуючий користувальницький інтерфейс та базу даних QRadar. UBA додає дві основні функції до SIEM: *профілювання ризику* та *уніфікацію особистості користувачів*. QRadar UBA виявляє внутрішні загрози, сформовані поведінкою людей з високою точністю, які зазвичай неможливо виявити за допомогою кореляції, керованої правилами.

Перш ніж впровадити будь-які системи виявлення внутрішніх загроз, задля ефективного виявлення інсайдерських атак, потрібно оцінити поточні системи та потреби, адже ключовим фактором обліку та усунення інсайдерських загроз є правильний підхід і правильні рішення для виявлення проблем безпеки та захисту від інсайдерських загроз. Цифрова криміналістика та аналітика є найефективнішими способами виявлення внутрішніх загроз. Аналіз поведінки користувачів та аналітика безпеки допомагають виявляти потенційні інсайдерські загрози, аналізуючи та попереджуючи, коли користувач поводиться підозріло або коли його дії поза типовою поведінкою [29].

Література:

1. Глушко С. В. Управлінські інформаційні системи / С. В. Глушко, А. В. Шайкан. – Львів: Магнолія Плюс, 2006. – 320 с.

2. Cost of insider threats. Global report – Rolling Meadows: Ponemon Institute, 2020. – 31 p.

3. Petters J. What is an Insider Threat? Definition and Examples [Електронний ресурс] / Jeff Petters. – 2020. – Режим доступу до ресурсу: https://www.varonis.com/blog/insider-threats/.

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Луценко І.М.

Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації

Анотація. *Сучасний етап розвитку української держави, як і багатьох держав світу, характеризується максимальною інформатизацією всіх сфер її життєдіяльності. В той же час перенесення багатьох процесів, зокрема й тих, що стосуються критичної інфраструктури, у кіберпростір, несе в собі разом з позитивними, також й негативні наслідки: уразливість цих процесів перед численними кіберзагрозами [1].*

Одні з основних проблем кібербезпеки України:

1.Неефективна нормативна база та система управління

Аналіз першопричин призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче. Одна з головних – неефективна нормативна база та система управління.

2. Низька готовність реагувати на кібератаки

Більшість компаній все ще не готові організаційно до нових хвиль кібератак та не мають підготовлених в достатній мірі фахівців у своєму штаті.

Відсутнє й централізоване управління силами реагування на кіберінциденти на загальнодержавному рівні.

3.Низький рівень залучення професійної спільноти, відсутність трансформаційного підходу

Національна система кібербезпеки обмежується переважно участю в ній силових органів (Нацполіція, СБУ, Держспецзв'язок тощо). Приватний бізнес та кіберспільнота до вирішення важливих питань майже не залучаються.

Відсутній трансформаційний підхід до управління національною кібербезпекою, що передбачає наявність організації, яка керує впровадженням програми з кібербезпеки, та регулярного контролю за процесом впровадження.

4. Кіберрозвідка потребує покращення

Ще одна суттєва проблема – все ще недостатньо ефективно працює система кіберрозвідки (Threat Intelligence). Є приклади, коли приватні організації та волонтерські угрупування попереджають державу про атаки, які плануються. Але ж в умовах існуючих загроз цього видається недостатньо.

5. Низька якість аудиту кібербезеки

Окрема проблемна ділянка – аудити кібербезпеки. В системі координат НД ТЗІ, дозвіл на проведення аудиту мають лише акредитовані державою організації. Міжнародні сертифікати з інформаційної безпеки та IT-аудиту наразі не визнаються, що негативно впливає на якість аудиту.

Питання регулювання та контролю можна делегувати галузевим регуляторам або саморегулюючим організаціям. Одним із прикладів останніх є NERC CIP в США, що розробила галузеві стандарти з кібербезпеки для енергетичного сектора.

6. Створення bug bounty програм

Один з головних акцентів має бути зроблений на розвитку bug bounty програм як дієвого механізму виявлення вразливих місць в інформаційних системах.

Суть bug bounty у тому, що будь-хто може знайти вразливість у системі компанії та повідомити про це власників системи, отримавши при цьому певну винагороду.

7. Співпраця з дослідниками та створення галузевих центрів реагування на кібератаки

Створення галузевих центрів реагування на кіберінциденти (SOC) та центрів обміну інформацією про кібератаки (ISAC) допоможе з вирішенням цієї проблеми.

8. Створення національної експертної ради з кібербезпеки

Важливим кроком має стати створення експертної ради з питань кібербезпеки за участю представників бізнесу, професійних спільнот та державних органів.

Така рада має готувати пропозиції щодо нормативно-правових актів у цій сфері, давати рекомендації по функціонуванню національної системи кібербезпеки та вирішувати інші завдання та проблеми, які потребують належної експертизи [2].

Прикладом такої організації є Національна Рада Кібербезпеки в Нідерладнах.

Література

1. Кібербезпека: українські реалії [Электронный ресурс] / А. Шкуро, І. Федик. — Электрон. журн. — Київ: 2017. — Режим доступа к журн.: http://timeua.info/post/oborona-i-bezopasnost/k-berbezpeka-ukra-ns-k--real--07454.html

2. Україні потрібна нова кіберстратегія [Электронный ресурс] / О. Янковський, К. Корсун, О. Барановський, и др. — Электрон. журн. — Київ: 2019. — Режим доступа к журн.: https://www.pravda.com.ua/rus/columns/2019/09/14/7226291/

ТЕОРЕТИЧНА МОДЕЛЬ ЗАХИЩЕНОЇ СИСТЕМИ В КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

Маковський А.П., група БСДМ-51
Державний університет телекомунікацій

Інтернет речей-концепція пристроїв об'єданих в одну мережу.Технології Інтернету речей почали стрімко розвиватися з 2011 року, коли з'явився глобальний інтерес до цієї концепції. З її впровадженням почали задумуватися над тим, як захистити пристрої IoT(Internet of Things).Для реалізації на практиці захищеної системи, необхідно враховувати безліч факторів,наприклад, протоколи передачі даних,які технології використовуються додатково,де розміщено пристрої,тощо.Абсолютного захисту не може бути, проте мінімізувати можливі збитки та наслідки буде головною задачою при розробці такої моделі захисту.У даному разі розробка захисту буде найбільш доцільною для системи «Розумний будинок».

Найважливішим джерелом для аналізу вразливостей буде інформація з відкритого проекту OWASP,а саме список вразливостей IoT, можна обрати список 2018-го року.Це дозволить пришвидшити розробку,не витрачаючи час на аналіз великої кількості джерел.

В результаті можна сформулювати таку модель захищеної системи:

- Адміністраторський доступ до пристроїв можливо отримати тільки через багатофакторну аутентифікацію,наприклад зв'язка біометричних даних та ключа доступу(USB-ключ,тощо)
- Зв'язок має бути через кабелі,які будуть сховані від людського ока.У випадку бездротового з'єднання,використовується «тунелювання» через приватні мережі

- Команди та інше мають надходити тільки у шифрованому вигляді,повинно використовуватися асимметричне шифрування
- Реалізований зв'язок тільки для довірених пристроїв та при певних умовах,наприклад певна відстань до пристрою.
- Для додаткового рівня захисту можливе використання підмережі,для розпаралелювання пристроїв та їх незалежності одне від одного.
- В пристроях має бути вбудований захист,що дозволить у випадку будь-якої аномальної події поза стандартним протоколом роботи,відмежовуватися у разі спроби втручання в роботу пристрою та отримання контролю над ним.

ДЖЕРЕЛА

1. Rob van Kranenburg .The Internet of Things A critique of ambient technology and the all-seeing network of RFID.
2. OWASP Internet of Things Project [Электроний ресурс] - Режим доступа до статті: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО НОРМАТИВНО-ПРАВОВОГО ВРЕГУЛЮВАННЯ КІБЕРЗАХИСТУ В УКРАЇНІ

Маринченко Антон Геннадійович ***125 кібербезпека***
Державний університет телекомунікацій
м. Київ

Однією з основних тенденцій сучасного інформаційного суспільства є стрімкий розвиток глобальної комп'ютерної мережі Інтернет та створення у ній низки нових сервісів, зокрема таких, як електронний уряд, соціальні мережі, електронна комерція, Інтернет-банкінг**.**

З технологічного погляду інформаційний простір характеризується удосконаленням інформаційних систем, віртуалізацією обчислювальних мереж, інтегруванням телекомунікацій та медіасфери. Широке використання інформаційних технологій у кіберпросторі пришвидшує розвиток різних галузей виробництва, науки, банківського сектору, дає можливість кожному створювати інформацію і знання, мати до них доступ, користуватися та обмінюватися ними тощо. Водночас новітні кіберзагрози підривають можливість максимально використовувати переваги, надані інформаційно-комунікаційними технологіями. Особливого значення для суспільства сьогодні набуває надійне функціонування інформаційних ресурсів критичної інфраструктури Історично розвиток кібербезпеки як однієї з основних складових інформаційної, а отже й національної безпеки, починається з появи перших зловмисних дій щодо персональних обчислювальних машин. Так у 1988 році Робертом Морісом у дослідницьких цілях був створений перший комп'ютерний черв'як - вірус, який сам розповсюджується по мережі й став першою успішною масштабною DoS атакою на попередника Інтернету

- мережі ARPANET. Лавиноподібне розповсюдження даного вірусу призвело до численних прямих та опосередкованих втрат, і це в далекому 1988 році. В нашому сьогоденні через мережу інтернет працює не тільки окремі офіси, підприємства, галузі. Держава не може існувати в сьогоденні без мережі, тому нормативно-правове регулювання кібербезпеки життєво необхідне. Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

Суб'єктами забезпечення кібербезпеки в Україні виступають:

Президент України через очолювану ним Раду національної безпеки і оборони України, як координатор діяльності у сфері кібербезпеки як складової національної безпеки ;

Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України;

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на 31 об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України).

Суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки:

міністерства та інші центральні органи виконавчої влади;

місцеві державні адміністрації;

органи місцевого самоврядування;

правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності.

Але ж необхідно впроваджувати організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем в різних умовах, та усунення їх наслідків, а також постійний обмін досвідом, тренінги, реальні навчання у взаємодії між суб'єктами які забезпечують кібербезпеку. Серед великої кількості інцидентів потрібно розрізняти ті, які ставлять під загрозу національну безпеку країни. На першому етапі взаємодії між суб'єктами я пропоную, із

загальної маси інцидентів виокремити кіберінциденти, що ставлять під загрозу національну безпеку держави та потребують швидкої та злагодженої взаємодії суб'єктів національної системи кібербезпеки та спільно протидіяти інцедентам та загрозам.

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ З ТЕСТУВАННЯ ЗІ, ЩОДО ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ WEB-СЕРВІСІВ, WEB 2.0 І МЕРЕЖЕВИХ ПРОГРАМ

Баргилевич Олександр Анатолійович, БСД-44
Державний університет
телекомунікацій,
м. Київ

Кожен день ми користуємося Web-сайтами для різних потреб, таких як: спілкування с друзями, рідними; навчання; оплата комунальних послуг або придбання необхідних речей. Через Web-сервіси та мережеві програми проходять різні конфіденційні данні, особливо за час пандемії в інтернеті зросла циркуляція такої інформації. Тому через велике навантаження деякі Web-сервіси не справляються з коректним захистом даних, це призводить, до того, що хакери отримують несанкціонований доступ до чутливої інформації, розміщеної на сервері або в базі даних. Вони зламують сайти і замінюють їх зміст, а також можуть вивести сервіс з ладу. Майже усі програми мають свої вразливості через розвинення програмної середи та не дотримання сучасних методів захисту Web-технологій.

На сьогоднішній день розробникам досить тяжко підтримувати стійкість Web-сайтів до загроз . Отже постає питання як захистити Web-технології. Для цього спочатку потрібно виявити загрози за допомогою тестування системи на наявність уразливостей.

Для успішного тестування веб-додатків необхідно застосовувати систематизований підхід або методологію. На сьогоднішній день існує безліч методологій, серед них є наступні:

- OWASP – перелік найбільш небезпечних ризиків інформаційної безпеки для веб-додатків на думку експертного співтовариства;
- CWE – класифікація уразливостей і недоліків програмного забезпечення;
- CAPEC – класифікація шаблонів комп'ютерних атак;
- WASC – класифікація загроз безпеки веб-додатків;

З цього переліку найбільш відомі OWASP та WASC, але у першій рекомендації публікувалися в 2017 році, а друга останній раз обновлювала в 2013. Отже будемо розглядати OWASP, вона має рейтинг з 10 обновлюваних звітів про безпеку для захисту веб-додатків, зосереджених на найбільш критичних ризиках. Також OWASP подає велику кількість інформації про загрози, їх різновидність, методи їх запобігання та оцінка ризику. Для оцінки вона використовує дві групи :

- що впливають на можливості атакуючого з виявлення і експлуатації уразливостей;
- що впливають на критичність наслідків експлуатації уразливостей;

Потрібно також звернути увагу на такі стандарти :

X.805 – це рекомендації для вирішення проблем з безпекою в мережі. Рекомендації описують підходи по управлінню, контролю безпеки та безпечному використанню мережі.

ISO/IEC 27001 – стандарт з управління та регулювання інформаційної безпеки (ІБ). Цей стандарт направлений на збереження цілісності, конфіденційності, доступності за рахунок процесів управління ризиками. Він включає вимоги для оцінки та обробки ризиків ІБ.

На даний час виділяють два базові методи тестування, на яких базуються інші:

- BlackBox – техніка тестування, основана на роботі виключно з зовнішніми інтерфейсами тестової системи;
- WhiteBox – метод тестування програмного забезпечення, який передбачає, що всі дані відомі для тестувальників;

Є декілька видів тестування, такі як:

- DAST – динамічний (тобто вимагає виконання) аналіз, це додатки без доступу до вихідного коду і серверної частини, з метою виявлення потенційних уразливих місць безпеки веб-програми. Виконується за принципом BlackBox;
- SAST – статичний (тобто не вимагає виконання) аналіз, це додатки з доступом до вихідного коду веб-додатка і веб-сервера, по суті це аналіз вихідного коду для розробника на наявність недоліків. Виконується за принципом WhiteBox;
- IAST – інтерактивний аналіз безпеки веб-додатка, з повним доступом до вихідного коду та веб-сервера – фактично є WhiteBox тестуванням.

Перелік найбільш небезпечних вразливостей:

- Впровадження коду;
- Некоректна аутентифікація і управління сесією;
- Витік чутливих даних (конфіденційних даних);
- Впровадження зовнішніх XML- сутностей (це, як правило, DoS-атаки)
- Порушення контролю доступу;
- Небезпечна конфігурація;
- Міжсайтовий скриптинг;
- Небезпечна десеріалізацію;
- Використання компонентів з відомими уразливими;
- Відсутність журналирования і моніторингу.

Отже, слід зауважити, що розробники повинні постійно оновлювати свої знання у галузі безпеки. До кожного сервісу, мережевого пакету та мережевих програм потрібно вибудовувати індивідуальний алгоритм тестування. Такі методології, як OWASP або WASC, допомагають розробникам аналізувати та запобігати зловмисникам отримати

конфіденційні дані. Методики з тестування допомагають тестувальникам більш легко та структуровано перевіряти систему на наявність загроз.

Література:

1. Habr. Современные методы исследования безопасности веб-приложений [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/owasp/blog/335820/
2. Quality-Lab. Тестирование безопасности: изнутри и снаружи [Електронний ресурс] – Режим доступу: https://quality-lab.ru/blog/security_testing_inside_and_out/
3.Habr. OWASP TOP-10: практический взгляд на безопасность веб-приложений [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/simplepay/blog/258499/

ТЕХНОЛОГІЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА БАЗІ ІНТЕГРАЦІЇ IBM QRADAR SIEM ТА IBM RESILIENT SOAR

Красноштан Іван Вікторович, БСД-44
Державний університет телекомунікацій, м. Київ

Бажання підприємств швидко впроваджувати нові технології надає величезні можливості, але також приносить непередбачені ризики та непередбачувані наслідки, які можуть мати негативний вплив. Важливо мати розуміння того, що в будь-який момент будь-яка структура може стати мішенню кібернападу. Якісний план реагування на інциденти в кібербезпеці може перетворити потенційну кризу кібербезпеки організації на черговий усунений кіберінцидент. Для швидкого та якісного створення таких планів використовуються системи моніторингу та аналізу в зв'язці з системами автоматизації реагування на інциденти. Вони відіграють ключову роль, оскільки темп, з яким організація здатна розпізнати, проаналізувати та реагувати на інцидент, напряму впливає на заподіяну шкоду та витрати на відновлення.

Сьогодні порушники удосконалюються у своїх методах ведення кібератак використовуючи все більш досконалі та складні методи. В той час, як корпоративні інформаційні системи постійно ростуть і розширюються, вміщуючи в себе все більше цінних даних та представляючи з себе критичний актив для захисту, забезпечувати їх стабільність та захищеність стає все складніше. Причиною тому можуть бути як і великі масштаби інформаційних систем та їх децентралізованість, так і, банально, недостатньо великий штаб спеціалістів, які могли б услідкувати за всіма точками захисту та діяти згідно необхідних рекомендацій, що різняться для кожного типу інциденту.

Для забезпечення захисту компанії, спеціалістам потрібно моніторити величезну кількість дій в системі та сигнали тригерів кожного дня. Для одночасного полегшення та покращення процесів моніторингу та превентивного підходу компанія IBM розробила рішення IBM QRadar Security Intelligence Platform [1], яка надає єдину архітектуру для інтегрування інформації про захищеність та управління подіями (SIEM) і журналами, визначення аномальних ситуацій, аналізу інцидентів, управління

налаштуваннями, а також усунення вразливостей. Зазвичай, коли організації планують обрати в якості основного сервісу захисту їх інформаційних систем IBM QRadar, вони звертають увагу на те, що дане програмне забезпечення пропонує модульний підхід до SIEM на основі додатків [2], який може масштабуватись для задоволення потреб більшості організацій щодо моніторингу та аналізу потоку подій та мережі. Додаткові інтегровані модулі для управління ризиками та вразливостями, криміналістичний аналіз та реакції на інциденти також доступні в якості опцій. Але перед тим як використовувати даний сервіс необхідно в першу чергу визначитись з його розміщенням та необхідним набором додатків для конкретної компанії.

Як вже було згадано, командам, що відповідають за безпеку, доводиться реагувати на все більшу кількість складніших та деструктивніших кібератак на їхні організації. Це послугувало причиною розгляду методів та засобів, які зможуть автоматизувати процеси SOC та IR для скорочення часу як на стримування інцидентів, так і на повне усунення нападу, що стосується кібербезпеки. Якщо IBM QRadar відповідає більше за функції SOC в своїй стандартній комплектації, то IBM Resilient Platform [3] цілком сконцентрований навколо IR.

Інтегруючи платформу IBM Resilient Security Orchestration, Automation and Response (SOAR) з IBM QRadar Security Intelligence, команди безпеки можуть створити провідне рішення управління загрозами на ринку, яке охоплює виявлення, розслідування та виправлення загроз у широкому колі кіберінцидентів. Інтеграція технологій між двома рішеннями дозволяє аналітикам безпеки швидко та ефективно передавати підозри про порушення від QRadar до Resilient, запускати додаткові автоматизовані процеси та проводити повний процес розслідування. По мірі того, як інцидент розвивається, вся інформація синхронізується між QRadar та Resilient, забезпечуючи повну цілісність даних, а будь-яку нову інформацію, яку виявив Resilient, команда реагування може направити назад у QRadar для покращення процесу подальшого моніторингу [4, с. 2].

Таким чином, за допомогою покрокових дій, можна, фактично з нуля, створити методику захисту інформації всередині організації, завдяки чітким рекомендаціям та вибору спеціалізованого програмного забезпечення для компенсації слабких місць установи в кіберпросторі.

Зрештою, відносячись відповідально до питань кібербезпеки та реалізації всіх аспектів технологій захисту на базі SIEM та SOAR систем, можна забезпечити комплексний та ефективний захист активів, а також належний рівень безпеки корпоративної інформаційної системи.

Література:

1. IBM QRadar SIEM Security Information Event Management Enterprise Product Overview [Електронний ресурс] – Режим доступу до ресурсу: https://www.midlandinfosys.com/power-systems-iseries-software/ibm-qradar/qradar-siem.html.

2. Types of QRadar content extensions [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/support/knowledgecenter/SS42VS_7.4.0/com.ibm.appfw.doc/c_appframework_extComponents.html.

3. Incident Response Platform Automation and Orchestration [Електронний ресурс] – Режим доступу до ресурсу: https://www.northdoor.co.uk/partners/ibm/security/ibm-resilient-incident-response.
4. IBM Security Solution Brief: IBM Resilient SOAR Platform and IBM QRadar® Security Intelligence [Електронний ресурс] / Claudio Neiva, Craig Lawson, Toby Bussa, Gorka Sadowski // Biz tech insights – 2019. – Режим доступу до ресурсу: https://advance.biz-tech-insights.com/whitepaper/IBM-Resilient-SOAR-Platform.pdf.

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ НА БАЗІ РІШЕНЬ ESET

Сокол Антон Васильович, БСД-44
Державний університет телекомунікацій,
м. Київ

В сучасному світі нові технології надзвичайно тісно пов'язані з побутовим життям людей. Сьогодні вже нікого не здивуєш покупками через Інтернет, миттєвим пошуком необхідної інформації, чи бронюванням авіаквитків онлайн. Така колаборація здійснюється і в різних сферах бізнесу. Разом зі зміною економічних відносин ми спостерігаємо зміну використання інформаційних технологій у напрямку зростання.

Дане питання постає особливо гостро на тлі пандемії, коли компанії все частіше задумуються про переведення бізнесу в онлайн. Зростання впливу інформаційних систем на бізнес зумовлює необхідність підвищення рівня безпеки інформаційних ресурсів. З огляду на це набувають необхідності дослідження теоретичних завдань та методичних рекомендацій з впровадження інформаційних технологій. Не менш важливими є дослідження з використання засобів та заходів для забезпечення безпеки інформаційних ресурсів підприємства.

Важливо розрізняти підходи до забезпечення кібербезпеки інформаційних ресурсів корпорацій та малого і середнього бізнесу. При розробці рекомендацій для малого та середнього бізнесу потрібно враховувати доцільність використання тих чи інших засобів з погляду на фінансову спроможність компанії та вартість інформаційних ресурсів.

Інформаційні системи для підприємств поділяються на наступні види:

ERP (англ. Enterprise Resource Planning) - система планування (управління) ресурсами підприємства.

CRM (англ. Customer relationship management) - модель взаємодії, що визначає, що центром всієї філософії бізнесу є клієнт, а основними напрямками діяльності є заходи з підтримки ефективного маркетингу, продажів і обслуговування клієнтів.

ECM (англ. Enterprise Content Management) - це стратегічна інфраструктура і технічна архітектура для підтримки єдиного життєвого циклу неструктурованою інформації (контенту) різних типів і форматів.

CPM (англ. Corporate Performance Management) - концепція управління ефективністю бізнесу, що охоплює весь спектр завдань в області стратегічного і фінансового управління компанією.

HRM (англ. Human Resource Management) - галузь знань і практичної діяльності, спрямована на своєчасне забезпечення організації персоналом і оптимальне його використання.

EAM (англ. Enterprise Asset Management) - це інформаційна система, призначена в основному для автоматизації процесів пов'язаних з технічним обслуговуванням устаткування, його ремонтом, а також післяпродажним обслуговуванням цього обладнання.

Основну загрозу функціонуванню інформаційних систем становлять таргетовані (цільові) атаки.

Особливість цілеспрямованих атак (APT) полягає в тому, що зловмисників цікавить конкретна компанія або державна організація. Це відрізняє дану загрозу від масових хакерських атак - коли одночасно атакується велике число цілей і найменш захищені користувачі стають жертвою. Цілеспрямовані атаки зазвичай добре сплановані і включають кілька етапів - від розвідки і впровадження до знищення слідів присутності. Як правило, в результаті цілеспрямованої атаки зловмисники закріплюються в інфраструктурі жертви і залишаються непоміченими протягом місяців або навіть років - протягом усього цього часу вони мають доступ до всієї корпоративної інформації.

Під інформаційною безпекою слід розуміти захищеність від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації або її власникам. Завдання забезпечення інформаційної безпеки повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Існує багато методів забезпечення інформаційної безпеки:

засоби антивірусного захисту;

засоби шифрування інформації, що зберігається на комп'ютерах і переданої мережами;

інструменти перевірки цілісності вмісту дисків;

віртуальні приватні мережі;

міжмережеві екрани;

засоби аутентифікації користувачів;

системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожен з перерахованих методів може бути використаний як самостійно, так і в інтеграції з іншими. Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють

виявляти новостворювані вірусні програми. Виявлені об'єкти можуть піддаватися лікуванню, та можуть бути видалені. Захист від вірусів може бути встановлений на робочі станції, файлові і поштові сервери, міжмережеві екрани, що працюють під практично будь-який з поширених операційних систем (Windows, Unix-і Linux системи, Novell).

Для забезпечення криптографічного захисту компанія Eset пропонує використання продукту ESET Endpoint Encryption (EEE).

Важливо зазначити, що в ESET Endpoint Encryption використовується модуль шифрування DESlock.

ESET Endpoint Encryption Server здійснює всі операції з клієнтськими робочими станціями за допомогою консолі DESLock + Enterprise Server. Також користувач має змогу здійснювати операції шифрування безпосередньо на клієнтській робочій станції.

Для забезпечення аутентифікації користувачів в інформаційних системах малих та середніх підприємств компанія Eset пропонує використовувати Eset Secure Authentication.

Принцип дії.

ESET Secure Authentication (ESA) додає автентифікацію Two Factor Authentication (2FA) до налаштувань доменів Microsoft Active Directory або локальної мережі. Після цього для входу в систему разом зі звичайним іменем користувача та паролем потрібно буде вводити згенерований одноразовий пароль (OTP). Також може створюватися push-сповіщення, яке має бути підтверджене на мобільному телефоні під керуванням ОС Android, iOS або Windows, коли користувач успішно пройшов автентифікацію за допомогою облікових даних загального доступу.

Для забезпечення безпеки робочих станцій та серверів компанія Eset пропонує використання свого продукту Eset Endpoint Protection, до складу якого входять Eset Endpoint Security (для робочих станцій) та Eset File Security for Windows Server (для Windows Server) та аналогічні версії програми для інших операційних систем.

ESET Security Management Center (раніше відома як ERA) - це додаток для централізованого управління продуктами ESET на клієнтських робочих станціях, серверах і мобільних пристроях в мережевому середовищі. Завдяки вбудованій в ESET Security Management Center системі управління завданнями можна встановлювати рішення ESET по забезпеченню безпеки на віддалені комп'ютери і швидко реагувати на нові проблеми і загрози.

Саме по собі рішення ESET Security Management Center не забезпечує захист від шкідливого коду. Для захисту середовища потрібно, щоб на робочих станціях було встановлено рішення ESET по забезпеченню безпеки, наприклад ESET Endpoint Security.

Таким чином, правильна реалізація технології захисту інформаційних систем підприємства на базі рішень ESET повинна забезпечити ефективний захист інформаційних ресурсів підприємства та кібербезпеку інформаційної системи підприємства

Література:

1. FossDoc. Класифікація інформаційних систем [Електронний ресурс] – Режим доступу: https://fossdoc.com/klassifikacija-informacionnyh-sistem

2. Tadviser. Advanced Persistent Threat (APT).Таргетированные или целевые кибератаки. "Развитая устойчивая угроза" 2019/11/25 [Електронний ресурс] – Режим доступу: http://www.tadviser.ru/index.php/Статья:APT_-_Таргетированные_или_целевые_атаки

ТЕХНОЛОГІЯ ПРОВЕДЕННЯ АУДИТУ ТА МОНІТОРИНГУ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Гайдур І.І., д.т.н, професор
Костюк Юлія Владимировна , магістр 125 кібербезпека
Державний університет
телекомунікацій,
м. Київ

Аудит інформаційної безпеки є одним з найбільш актуальних напрямків стратегічного і оперативного менеджменту в області безпеки інформаційних систем і викликає постійний інтерес фахівців. Його основне завдання – виявлення та усунення вразливостей, а також оцінка загального рівня стану інформаційної безпеки. Аналіз міжнародних стандартів та методів аудиту інформаційної безпеки, методик оцінки ризиків дасть можливість визначити критерії вибору заходів і засобів аудиту в залежності до рівня вимог, що пред'являються до режиму інформаційної безпеки об'єктів інформаційної діяльності.

Сучасний ринок безпеки насичений засобами забезпечення інформаційної безпеки. Тут аудит дає можливість аналізувати поточну безпеку функціонування корпоративної інформаційної системи, оцінювати і прогнозувати ризики, управляти їх впливом на бізнес-процеси компанії, коректно і обґрунтовано підійти до питання підтримки безпеки її інформаційних активів - стратегічних планів розвитку, маркетингових програм, фінансових і бухгалтерських відомостей, вмісту корпоративних баз даних. В результаті грамотно проведений аудит безпеки корпоративної інформаційної системи дозволяє домогтися максимальної віддачі від коштів, інвестованих у створення і обслуговування систем безпеки. [1] [2] Дослідження показують, що організації, які впровадили сучасну систему аудиту інформаційної безпеки, мають кращі показники в порівнянні з організаціями, що працюють на основі старих принципів управління. У багатьох розвинених країнах менеджери у своїй роботі звертаються до послуг спеціальної служби безпеки. [3] [4]

Аудит стану інформаційної безпеки об'єктів інформаційної діяльності є перевіркою діяльності, інструментом ідентифікації проблем, ризиків і невідповідностей, а також моніторингом прогресу в усуненні раніше ідентифікованих невідповідностей. [5]

Аудит інформаційної безпеки об'єктів інформаційної діяльності – систематизований, незалежний і документований процес отримання об'єктивної оцінки стану інформаційної безпеки та відповідності її встановленим вимогам національних та рекомендаціям міжнародних стандартів інформаційної безпеки [7].

Суть, призначення, цілі, результати та процеси проведення аудиту ІБ визначаються типом організації, видом і приналежністю оброблюваної конфіденційної інформації та роллю організації в загальних процесах забезпечення безпеки держави в інформаційній сфері.

Метою аудиту є надання незалежної і об'єктивної комплексної оцінки поточного стану інформаційної безпеки об'єкту інформаційної діяльності, що дозволяє

систематизувати загрози інформаційної безпеки і запропонувати рекомендації щодо їх усунення.

Аналіз міжнародних стандартів та методів аудиту інформаційної безпеки, методик оцінки ризиків дасть можливість визначити критерії вибору заходів і засобів аудиту в залежності до рівня вимог, що пред'являються до режиму інформаційної безпеки об'єктів інформаційної діяльності.

Дослідження сучасних методів аудиту інформаційної безпеки показав, що наявні методи не в повній мірі задовольняють вимогам оцінки стану інформаційної безпеки. Це зумовлено тим, що в розглянутих методиках питання оцінки стану розглядають лише з точки зору обчислення окремих показників, а не як технологія, що охоплює чітко регламентовану послідовність виконання операцій, дій, етапів різного ступеня складності над даними, що характеризують інформаційну безпеку. [8]

Проаналізувавши методи проведення аудита, зроблено висновки, що за параметри оцінки захищеності можна використовувати як кількісні, так і якісні критерії. Під час оцінювання якісних критеріїв проводиться або аудит відповідності об'єкта інформаційної діяльності стандартам в сфері інформаційної безпеки (такими стандартами можуть бути національні чи міжнародні стандарти), або тестування системи захисту об'єкта інформаційної діяльності, яке орієнтовано на виявлення вразливостей. [10] Під час оцінювання кількісних критеріїв використовують методи аналізу ризиків (зокрема, використовуючи інструментальні засоби) і методи оцінки ефективності створених систем захисту інформації.

Можна вважати, що головні труднощі проведення оцінок пов'язані зі складністю формалізації процесів, що протікають в інформаційно-телекомунікаційних системах. У більшості випадків, оцінки ймовірностей реалізації загроз, величин нанесеної в разі їх реалізації шкоди і очікуваних ризиків, виконуються експертними методами, а отже суб'єктивний чинник тут вагомий впливний чинник. [11] Для зведення суб'єктивного чинника до мінімуму, пропонується виконувати оцінку захищеності на єдиній методологічній основі з використанням надійних схем і методик. Під схемою оцінки зазвичай розуміють сукупність нормативно-правових актів, нормативних документів (національного і міжнародного рівня прийняття) та розпорядчих (внутрішніх) документів, що забезпечують отримання стандартизованого значення оцінки захищеності експертами за уніфікованими критеріями (ці критерії будуть зрозумілі та відтворювані незалежно від органу сертифікації). Під час проведення таких оцінок використовують інструментальні засоби, спеціально створені для цих цілей. [12]

Література:

1. Про інформацію [Текст] : Закон України № 2657-XII від 02.10.1992 / Верховна Рада України // Відомості Верховної Ради України. –1992. - N48. - ст.650.

2. Про захист інформації в інформаційно-телекомунікаційних системах [Текст] : Закон України № 80/94-ВР від 05.07.1994 / Верховна Рада України // Відомості Верховної Ради України. – 1994. - N 31. - ст.286.

3. Про основні засади забезпечення кібербезпеки України [Текст] : Закон України № 2163-VIII від 5 жовтня 2017 р. / Верховна Рада України // Відомості Верховної Ради України. –2017.- № 45. - ст.403.

4. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення [Текст] : НД ТЗІ 1.1-005-07. – Чин. 2007.12.12 – К.: Адміністрації Держспецзв'язку, 2007. – 5 с.

5. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Текст] : НД ТЗІ 2.5-004-99. – Чин. 1999.28.04. – К.: ДСТСЗІ СБ України, 1999. – 52 с.

6. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів : ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT). Діючий 01.10.2017 –К.: ДП «УкрНДНЦ», 2017.-41с.

7. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT) Діючий 01.01.2017 –К.: ДП «УкрНДНЦ», 2016 – 28 с.

8. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) Діючий 01.01.2017 –К.: ДП «УкрНДНЦ», 2016 – 98 с.

9. Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT) Діючий 01.01.2019 –К.: ДП «УкрНДНЦ», 2018 – 41с.

10. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В.Кавун, В.В.Носов, О. В.Манжай — Харків: Вид. ХНЕУ, 2008. — 352 с.

11. Амелин Р. В. Информационная безопасность / Р. В. Амелин - Саратов: УЦ «Новые технологии в образовании», 2008- 121 с.

12. Комплексні системи захисту інформації. Навчальний посібник / Ю.Є. Яремчук, П.В. Павловський, В,С. Катаєв, В.В. Сінюгін – Вінниця : ВНТУ, 2017. – 120 с.

ТЕХНОЛОГІЯ ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ПОЛІТИКАМИ ТА ЗАСОБАМИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ MCAFEE EPOLICY ORCHESTRATOR

Матола Роман Юрійович ***125 кібербезпека***
Державний університет телекомунікацій,
м. Київ

Ринок найму і роботи зараз переживає кардинальні зміни. Інтернет повністю змінює принцип роботодавець – виконавець. Сьогодні часто виходить, що замовнику, який готовий платити за результати роботи без різниці, де територіально знаходиться виконавець. Питання про IT безпеку встає на перше місце. Безпека використання Інтернету та інформаційних і комунікаційних технологій одна з найактуальніших і найважливіших тем сучасності.

З розвитком всесвітньої мережі практично кожен щодня користується ресурсами Інтернету. Відомо, що глобальна мережа, перш за все, є невичерпним джерелом інформації і полем для віртуального спілкування. Однак далеко не всі знають, якої шкоди може бути завдано персональному комп'ютеру користувача. Безпека в Інтернеті є прийняття необхідних заходів, що забезпечують захист від комп'ютерних вірусів різної складності, а також від злому ПК зловмисниками з метою заволодіння особистим або корпоративною інформацією. У цих обставинах систему захисту інформації можна вважати базовою підсистемою забезпечення інформаційної безпеки суспільства, без якої неможливе здійснення жодного виду інформаційної діяльності. Таким чином, не вирішивши проблеми захисту інформації на рівні, адекватному економічно розвинутим країнам, Україна не зможе увійти до мирової спільноти на правах рівноправного партнера.

Для вдосконалення технології централізованого управління політиками та засобами захисту кінцевих точок корпоративної інформаційної системи пропоную розглянути та проаналізувати наступні питання:

– дослідити сутність проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи;

– дослідити сутність завдань захисту кінцевих точок корпоративної інформаційної системи;

– проаналізувати існуючі технології захисту кінцевих точок корпоративної інформаційної системи;

– проаналізувати методи та засоби централізованого управління політиками та засобами захисту кінцевих точок корпоративної інформаційної системи на базі McAfee ePolicy Orchestrator;

– проаналізувати основні функції та принципи роботи реалізації захисту кінцевих точок корпоративної інформаційної системи.

Основним об'єктом бажань зловмисників, природно, є інформація, оброблювана в

корпоративній мережі за допомогою спеціального інструменту – програмного забезпечення. Базисом будь – якої корпоративної мережі є загальносистемне програмне забезпечення, яке може містити різні операційні системи, програмні оболонки, програми загального призначення, текстові процесори, редактори і інтегровані пакети програм, системи управління базами даних.

При створенні або модернізації корпоративної мережі необхідно поклопотатися про створення або модернізацію підсистеми інформаційної безпеки своєї корпоративної інформаційної системи. Поняття підсистеми інформаційної безпеки включає весь комплекс засобів і заходів по захисту інформації в корпоративній інформаційній системі.

Побудова будь – якої корпоративної системи починається з установки робочих станцій, отже, підсистема інформаційної безпеки корпоративної системи починається із захисту саме цих об'єктів. Для цього можна використовувати відомі штатні засоби захисту операційних систем, антивірусні пакети, додаткові пристрої автентифікації користувача і засобу захисту робочих станцій від НСД, засоби шифрування прикладного рівня і т.д.

У корпоративній мережі повинні бути реалізовані необхідні мережеві служби безпеки та повинні використовуватися відповідні засоби безпеки.

Засоби захисту інформації повинні мати модульну структуру, кожен модуль повинен підтримувати область пам'яті для власного виконання. Для кожного модуля системи захисту інформації, кожного компонента системи захисту інформації, розділеного в автоматизовану систему, повинна забезпечуватися ізоляція ресурсів, що потребують захисту так, щоб вони підкорялися контролю доступу і вимогам ревізії.

При поділі систем захисту інформації повинна забезпечуватися здатність повідомлення адміністративному персоналу про відмови, помилки, спробах несанкціонованого доступу, виявлених в розділених компонентах систем захисту інформації. Протоколи, здійснені в межах систем захисту інформації, повинні бути розроблені так, що повинно забезпечуватися правильне функціонування у випадку відмов (збоїв) комунікаційної мережі або її індивідуальних компонентів.

Ефективна система кібербезпеки вимагає постійного відстеження та аналізу слабких місць корпоративних мереж. Зловмисники можуть використовувати подібні проломи для проведення атак, тому моніторинг наявності вразливостей в інформаційних системах і їх своєчасне усунення стає важливим завданням для захисту даних компанії.

Захист кінцевих точок – це широке поняття, яке може позначати низку заходів безпеки, однак зазвичай стосується сфери захисту мережі. Засоби захисту кінцевих точок мають на меті захист мережі компанії під час її використання віддаленими, безпровідними або мобільними пристроями, як ноутбуками, планшетами та мобільними телефонами.

Захист кінцевих точок (Endpoint Security) – клієнт – серверна методологія інформаційної безпеки, призначена для захисту корпоративної мережі за допомогою фокусування на кінцевих точках, і аналізу (моніторингу) відповідних станів, таких як мережева активність, наявність певного переліку програмного забезпечення, відповідності правильного призначення прав доступу і аутентифікації.

Традиційні сигнатурні антивіруси не можуть впоратися із загрозою шкідливого програмного забезпечення. Все це призвело до того, що як кінцеві користувачі, так і корпорації усвідомили потребу в додатковому рівні захисту, який зможе виявити і зупинити шкідливі і небажані програми.

Політика захисту мережі має описувати технологію та процедури, що використовуються для моніторингу стану захисту системи. Власне, моніторинг дозволяє виявляти загрози мережі. Контроль активності в мережі може виявити спроби компрометації системи та допомагти зробити аналіз загроз. Моніторинг забезпечує відповідність налагоджень засобів мережного захисту вимогам політики безпеки. Він може містити аналіз повідомлень системних журналів маршрутизаторів периметру, брандмауерів і системи керування доступом.

Таким чином, проблема захисту кінцевих точок (Endpoint Security) в корпоративній мережі з розмитим периметром є сьогодні найбільш нагальною для сучасного підприємства.

ТЕХНОЛОГІЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ IBM QRADAR VULNERABILITY MANAGER

Саливон Олександр Борисович 125 кібербезпека
Державний університет
телекомунікацій,
м. Київ

На фоні всесвітньої пандемії все більш актуальнішим стає віддалений доступ до інформаційних ресурсів та забезпечення безпеки інформації на різних етапах її обробки. Процес тотальної інформатизації переважної більшості суспільних та бізнесових процесів є актуальними щодо забезпечення безпеки великих інформаційних систем. Системи управління вразливістю є базисом для побудови інформаційної безпеки великих інформаційних систем. Головними питаннями, які постають при роботі з системою управління вразливістю для кожного спеціаліста з інформаційної безпеки, це оцінка можливості конкретної системи, варіант використання та конкретні налаштування для виконання покладених на них обов'язків для захисту активів інформаційної системи, виправлення вразливостей, усунення або зменшення ризиків пов'язаних вразливостями.

З метою розуміння підходу до управління вразливостями в корпоративній інформаційній системі пропонуються проаналізовані наступні питання: -поняття корпоративних інформаційних систем та їх роль у сучасному світі; -поняття вразливостей, як і де вони виникають; -сучасні системи управління врзливостями як інструмент запобігання та зменшення ризику від вразливостей; - можливості налаштування та використання системи управління IBM QRadar Vulnerability Manager; – комплексне рішення IBM QRadar; - оцінка ризиків та прийнятті рішення про їх усунення; - результат роботи та найкращі практики використання.

Сьогодні збільшується вразливість сучасного інформаційного суспільства до недостовірної інформації, несвоєчасного надходження інформації, промислового шпигунства, комп'ютерної злочинності тощо. Корпоративна інформаційна система - це велика сукупність активів, програмно та апаратно об'єднаних за допомогою мережі, які допомагають в генеруванні, використанні, обробці та зберіганні інформації. Чим більша інформаційна мережа, тим більше різноманітних апаратних та програмних ресурсів використовується для надання бізнес-сервісів користувачам. Кожен з програмних та апаратних активів, а в подальшому кожен сервіс, може бути вразливий і може потребувати санації. Вразливість інформаційної системи - це нездатність системи протистояти реалізації певній загрозі або сукупності загроз [1]. Тобто, це певні недоліки в комп'ютерній системі, завдяки яким можна навмисно порушити її цілісність і викликати неправильну роботу. Пошук вразливостей іноді називають зондуванням, де мають на увазі пошук відкритих мережевих портів і наявності вразливостей, пов'язаних з додатками, що використовують відповідні порти.

Існують інструментальні засоби, які можуть допомогти у виявленні вразливостей в системі. Ці інструменти можуть забезпечити аудитору хороший огляд можливих вразливостей, що існують в системі, але не можуть замінити участь людини в їх оцінці.

Для забезпечення захищеності і цілісності системи необхідно постійно стежити за нею: встановлювати оновлення, використовувати інструменти, які допомагають протидіяти можливим атакам. Уразливості виявлялися у всіх основних операційних системах, включаючи Microsoft Windows, Mac OS, різні варіанти UNIX (у тому числі GNU / Linux). Так як нові вразливості знаходять безперервно, єдиний шлях зменшити ймовірність їх використання проти системи — постійна пильність.[2]

Підтримувати постійну пильність допомагає використання спеціального програмного забезпечення, що має назву системи управління вразливостями. Системи управління вразливостями це той інструмент який дозволяє оцінити наявні активи інформаційної системи, підключитись до кожного з них та виявити які операційні системи на них використовуються, яке програмне забезпечення було встановлено та використовується, які вразливості притаманні цим версіям програмного та апаратного забезпечення, хто і як може експлуатувати ці вразливості. Це дозволяє проводити аналіз кіберінцидентів пов'язаних з використанням вразливостей.

Оцінка стану кіберзахисту об'єктів критичної інформаційної інфраструктури з урахуванням індикаторів кіберзагроз будь якого масштабу є об'єднанням та пошуком кореляції між: - даними

аудиту стану захищеності об’єктів критичної інфраструктури; - даних щодо оцінки ризиків та моделей кіберзагроз; - даними про індикатори, що передують відомим кіберзагрозам.

Вищезазначена оцінка потребує використання датасету (набору даних), моделі та програмних засобів, що здійснюють обробку датасету за зазначеною моделлю, що в свою чергу дозволить визначити стан кіберзахисту об’єктів критичної інфраструктури на поточний момент часу, та\або його відхилення за певними індикаторами.

Ключовим моментом є вибір типів даних та джерел інформації, на основі яких буде здійснюватися оцінка. Слід вказати, що всі можливі вхідні дані, з яких буде сформовано датасет розподіляються на структуровані та не структуровані.[8]

Якість оцінки буде залежати від наступних факторів: - визначення основного переліку індексів щодо оцінки кіберзагроз типових для даного об’єкту критичної інфраструктури; - здійснення збагачення (уточнення) даних моделі шляхом введення регіональних індексів; - застосування технології великих даних для роботи з структурованими та не структурованими даними; - вибору технології машинного навчання, що буде здійснювати обробку даних моделі, її тренування та перенавчання; - здійснення кореляції та виявлення залежностей між індексами (створення шаблону індикаторів); - визначення дельти часу (вікна спостереження), період за який буде здійснено спостереження.

В ході оцінки може знадобитись проведення очистки даних та таргетування датасету, для цього можливо слід задіяти експертну систему чи визначити певну роль експерта з даних, що зможе визначити взаємопов’язані ключові індикатори.[9]

Окремими питання стоїть доставка даних про стан ІТ інфраструктури об’єкту критичної інфраструктури в режимі реального часу, можливістю порівняння цих даних з даними моделі для пошуку відхилень та виявлення початку зміни параметрів індикаторів, що призведуть до появи певного індексу, що в свою чергу дозволить виявляти кіберзагрозу на ранній стадії. [10]

Також слід відокремити питання прогнозування результатів виникнення кіберзагроз з врахування вищезазначеної оцінки та впливу цих результатів на стан кіберзахисту об’єкту критичної інфраструктури. Модель прогнозування повинна використовувати дані оцінки, проте базуватись на інших математичних інструментах. На основі отриманого результату здійснюються подальша побудова сценаріїв розвитку кібератак, що дозволить їх використовувати в інших експертних системах.[11]

На оцінку кіберзахисту впливає стан пов’язаних з об’єктом критичної інфраструктури взаємодіючих систем. На сьогоднішній день відбувається загальне об’єднання ІТ інфраструктури (діджиталізація), тому оцінка стану одного об’єкту критичної інфраструктури впливає на інший, пов'язаний з ним.

Щодо технічних аспектів - технологія машинного навчання та роботи з великими даними слід дотримуватись Cross-industry standard process for data mining.[12] В хорді навчання моделі буде визначено шаблон індикаторів кіберзагроз, відповідно за якими необхідно здійснювати заходи моніторингу, або шукати додаткові джерела для отримання показників за ними. Підготовку, обробку та візуалізацію даних можливо виконувати у стеці технологій подібних до платформ хмарного обчислення, що передбачає високу відмовостійкість та масштабованість. В подальшому можливо використати будь-які засоби з відкритим програмним кодом, які інтегруються з даними технологіями.

Впровадження оцінки стану кіберзахисту об’єктів критичної інформаційної інфраструктури в режимі реального часу, з використання індикаторів кіберзагроз на рівні прийняття рішень дозволить забезпечити інформацією загальнодержавний центр кіберстікості CRC (Cyber Resilience Center) у разі його створення.[13]

Література:

1. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999.

2. ISO/IEC, «Information technology — Security techniques-Information security risk management» ISO/IEC FIDIS 27005:2008

ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ІНДИКАТОРІВ КІБЕРЗАГРОЗ

Ткаченко Іван Вікторович , аспірант 125 кібербезпека
Державний університет телекомунікацій,
м. Київ

В умовах сьогодення України актуальним є питанням формування системи управління інформаційної безпекою критичної інформаційної інфраструктури основним розділом якого є оцінка стану кіберзахисту об'єктів критичної інфраструктури з урахуванням індикаторів кіберзагроз.

З метою розуміння підходу до оцінки стану кіберзахисту та вірної класифікації кіберзагроз пропоную проаналізовані наступні питання: - сучасні підходи, міжнародні та регіональні індекси щодо оцінки кіберризиків; - порядок та етапи організації оцінки стану кіберзахисту, з урахуванням індикаторів кіберзагроз; - технологія великих даних як основний інструмент здійснення заходів з оцінки стану кіберзахисту об'єктів критичної інфраструктури.

Існують визначені міжнародні, загальнодержавні та регіональні індекси щодо оцінки, аналізу, класифікації кіберзагроз та оцінки ризиків, що вони несуть, а також індекси оцінки готовності ІТ інфраструктурний держав (організацій) до боротьби з кібератаками.[1] [2] Кожен індекс має певне кількісне та якісне значення, яке розраховується шляхом об'єднання значень декількох математичних розрахункових показників.[3] [4]

Також існують типові моделі кіберзагроз та методи класифікації кібератак з використанням різноманітних типів експертних систем. В ході класифікацій та аналізу атаки використовуються державні, комерційні та не комерційні центри обміну інформацією про кіберінциденти, та індикатори кіберзагроз, що їм передують, з занесенням структурованої інформації про кіберінцидент до єдиного реєстру.[6] Це дозволяє проводити аналіз кіберінцидентів та виявляти певні закономірності(індикатори кіберзагроз), які складаються з показників щодо ступеня небезпеки того чи іншого виду кібератаки(у разі класифікації), векторної направленості кіберзагрози, сукупність методів, що були застосовані при кібератаці, критичності збитку при вжитті захисних заходів в той чі інший момент часу.[7]

Оцінка стану кіберзахисту об'єктів критичної інформаційної інфраструктури з урахуванням індикаторів кіберзагроз будь якого масштабу є об'єднанням та пошуком кореляції між: - даними аудиту стану захищеності об'єктів критичної інфраструктури; - даних щодо оцінки ризиків та моделей кіберзагроз; - даними про індикатори, що передують відомим кіберзагрозам.

Вищезазначена оцінка потребує використання датасету(набору даних), моделі та програмних засобів, що здійснять обробку датасету за зазначеною моделлю, що дозволить визначити стан кіберзахисту об'єктів критичної інфраструктури на поточний момент часу, та\або його відхилення за певними індикаторами.

Ключовим моментом є вибір типів даних та джерел інформації, на основі яких буде здійснюватися оцінка. Слід вказати, що всі можливі вхідні дані, з яких буде сформовано датасет розподіляються на структуровані та не структуровані.[8]

Якість оцінки буде залежати від наступних факторі: - визначення основного переліку індексів щодо оцінки кіберзагроз типових для даного об'єкту критичної інфраструктури; - здійснення збагачення(уточнення) даних моделі шляхом введення регіональних індексів; - застосування технології великих даних для роботи з структурованими та не структурованими даними; - вибору технології машинного навчання, що буде здійснювати обробку даних моделі, її тренування та перенавчання; - здійснення кореляції та виявлення залежностей між індексами(створення шаблону індикаторів); - визначення дельти часу (вікна спостереження), період за який буде здійснено спостереження.

В ході оцінки може знадобитись проведення очистки даних та таргетування датасету, для цього можливо слід задіяти експертну систему чи визначити певну роль експерта з даних, що зможе визначити взаємопов'язані ключові індикатори.[9]

Окремими питання стоїть доставка даних про стан ІТ інфраструктури об'єкту критичної інфраструктури в режимі реального часу та порівняння цих даних з даними моделі для пошуку відхилень, та виявлення початку зміни параметрів індикаторів, що призведуть до появи певного індексу, що в свою чергу дозволить виявляти кіберзагрозу на ранній стадії. [10]

Також слід відокремити питання прогнозування результатів виникнення кіберзагроз з врахування вищезазначеної оцінки, та впливу цих результатів на стан кіберзахисту об’єкту критичної інфраструктури. Модель прогнозування повинна використовувати дані оцінки, проте базуватись на інших математичних інструментах. На основі отриманого результату здійснюються подальшої побудови сценаріїв розвитку кібератак, що дозволить їх використовувати в інших експертних системах.[11]

На оцінку впливає стан пов’язаних з об’єктом критичної інфраструктури взаємодіючих систем. На сьогоднішній день відбувається загальне об’єднання IT інфраструктури (діджиталізація), тому оцінка стану одного об’єкту критичної інфраструктури впливає на інший, пов'язаний з ним.

Щодо технічних аспектів технологія машинного навчання та роботи з великими даними слід дотримуватись Cross-industry standard process for data mining.[12]

В хорді навчання моделі буде визначено шаблон індикаторів кіберзагроз, відповідно за якими необхідно здійснювати заходи моніторингу, або шукати додаткові джерела для отримання показників за ними. Підготовку, обробку та візуалізацію даних можливо виконувати у стеці технологій подібних до платформ хмарного обчислення, що передбачає високу відмовостійкість та масштабованість. В подальшому можливо використати будь-які засоби з відкритим програмним кодом, які інтегруються з даними технологіями.

Впровадження оцінки стану кіберзахисту об’єктів критичної інформаційної інфраструктури в режимі реального часу, з використання індикаторів кіберзагроз на рівні прийняття рішень дозволить забезпечити інформацією загальнодержавний центр кіберстікості CRC (Cyber Resilience Center) у разі його створення.[13]

Література:

1. *Глобальний індекс кібербезпеки.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
2. *Звіт про глобальні ризики кібербезпеки* https://www.marsh.com/ru/ru/insights/research-briefings/marsh-microsoft-cyber-survey-report-2019.html
3. *Загальна система оцінювання вразливості SIG.https://www.first.org/cvss/*
4. *NIST_Cybersecurity_Framework* https://www.nist.gov/cyberframework
5. *Метод мережево-центричного моніторингу кіберінцидентів в сучасних інформаційно-телекомунікаційних системах Олександр Корченко, Віктор Гнатюк, Євгенія Іванченко, Сергій Гнатюк, Нургуль Сейлова ЗАХИСТ ІНФОРМАЦІЇ, ТОМ 18, №3, ЛИПЕНЬ-ВЕРЕСЕНЬ 2016 УДК 621.391:004.056.53 (045)*
6. *Зміна гри на кібер-ризик* https://www2.deloitte.com/cy/en/pages/risk/solutions/cyber-security-services.html
7. *Великі дані.* https://en.wikipedia.org/wiki/Big_data
8. *Jason W. Osborne. Best Practices in Data Cleaning: A Complete Guide to Everything You Need to Do Before and After Collecting Your Data . - Sage, 2012. - 275 p.*
9. *Полювання на кіберзагри.* https://en.wikipedia.org/wiki/Cyber_threat_hunting
10. *Система виявлення впливів.* https://en.wikipedia.org/wiki/Intrusion_detection_system
11. *Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры Гаськова Д.А.1, Массель А.Г. DOI: 10.21681/2311-3456-2019-2-42-49*
12. *Міжгалузевий стандартний процес обміну даними.* https://ru.wikipedia.org/wiki/CRISP-DM
13. *Огляд кіберстійкості.* https://en.wikipedia.org/wiki/Cyber_Resilience_Review

ТЕХНОЛОГІЯ ЗАБЕСПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ РОЗПОДІЛЕНОГО МОНІТОРИНГУ СТАНУ КОРПОРОТИВНОЇ МЕРЕЖІ ZABBIX

Пімченко Віталій Сергійович, БСЗМ-71
Державний університет телекомунікацій,
м. Київ

Розглянуто зміст технології управління захистом системи розподіленого моніторингу корпоративної мережі Zabbix. Визначено мету і основні завдання щодо управління захистом системи розподіленого моніторингу Zabbix. Розроблено рекомендації щодо управління захистом системи розподіленого моніторингу Zabbix.

Як відомо, однією з найважливіших частин інформаційної інфраструктури сучасних підприємств, приватних компаній та багатьох державних організацій є корпоративні мережі передачі даних, які давно перейшли в розряд критичних для забезпечення бізнес-процесів.

Корпоративні мережі мають високу складність в силу територіальної розподіленої інфраструктури, поєднання можливостей передачі даних з використанням VoIP-телефонії, відео конференц-зв'язку, та наявності вбудованих систем підтримки інформаційної безпеки, а також резервних і дублюючих елементів, що відповідають за забезпечення надійності та доступності корпоративної мережі. Вихід з ладу такої системи фактично означає зупинку діяльності всієї організації. В таких умовах гостро стоїть проблема підтримки параметрів роботи розподіленої мережі на заданому рівні що є складною задачею. Вирішити ці завдання допоможуть системи централізованого моніторингу та управління мережею передачі даних.

Існує безліч готових систем, як вільно розповсюджених, так і комерційних, але перш ніж впроваджувати будь-яку з них у виробничий процес, необхідно провести ретельний аналіз і врахувати всі ризики, пов'язані із застосуванням таких систем на окремо взятій інфраструктурі.

Найчастіше подібні системи мають вразливість в програмному забезпеченні і здійснюють передачу даних у відкритому вигляді, а зловмисник має можливість перехопити та фальсифікувати дані моніторингу, що серйозно обмежує сферу застосування деяких систем, особливо у великих компаніях. Для того, щоб впровадити систему в діючу інфраструктуру, необхідно врахувати декілька параметрів. Система повинна включати в себе інструменти захисту від несанкціонованого доступу збоку зловмисників (хакерів), модулі, які дозволяють здійснювати управління мережевим обладнанням, робочими станціями і серверами, як в ручному режимі, так і автономному. Перш за все, система розподіленого моніторингу повинна відповідати декільком вимогам:

- висока безпека;
- висока швидкість впровадження;
- мінімальна кількість матеріальних витрат на впровадження;
- підтримка сучасних мережевих протоколів і технологій;
- взаємодія з наявними програмними продуктами.

Критерії вибору системи розподіленого моніторингу вимогливі і ним відповідає одна з таких систем - Zabbix. Значна увага при створенні вказаної системи приділяється забезпеченню безпеки цілісності і конфіденційності даних.

Zabbix - це програмне забезпечення з відкритим вихідним кодом для моніторингу мереж і додатків. Він пропонує в реальному часі перевірку даних, зібраних з серверів, віртуальних машин, мережевих пристроїв та веб-додатків та використовує гнучкий механізм сповіщень. Ці показники можуть допомогти вам визначити поточний стан вашої IT-інфраструктури і виявити проблеми з апаратними або програмними компонентами.

Zabbix складається з:

- сервера моніторингу, який виконує періодичне отримання даних, обробку, аналіз і запуск скриптів оповіщення;
- проксі-сервера;
- бази даних (MySQL, PostgreSQL, SQLite або Oracle);
- веб-інтерфейсу на PHP;
- агент - демона, який запускається на об'єктах, що відслідковує і надає дані до сервера. Агент опційний, моніторинг можна проводити не тільки за допомогою нього, але і по SNMP, запуском зовнішніх скриптів, що видають дані, і кілька видів вбудованих перевірок, таких як ping, запит по http, ssh, ftp і іншим протоколам, а також визначення часу відповіді цих сервісів.

Розподілена система моніторингу Zabbix різноманітна і вміщує багато потужних і гнучких інструментів, тим самим викликає особливий інтерес зі сторони зловмисників, які можуть спробувати скористатися наявними можливостями системи в своїх цілях. Завдяки можливостям Zabbix, маючи доступ до системи моніторингу, безпеки і конфігурації, хакери можуть здійснити атаки на хости, моніторинг яких здійснюється за допомогою Zabbix. При певних налаштуваннях зловмисник може перехопити (zbx_sessionid) і далі створити собі нового користувача з правами адміністратора і закріпитись в системі Zabbix. Використовуючи особливості роботи Zabbix-агента, зловмисник (при певних налаштуваннях агента) може проникнути на всі ПК, які моніторяться Zabbix-сервером. В основному загрози безпеки виникають з помилок конфігурації, а система моніторингу є таким компонентом, неправильним з точки зору безпеки, конфігурація якого може критично вплинути на безпеку всіх компонентів мережі.

Перш за все, для безпечної роботи системи потрібно потурбуватися захистом переданих даних:

- не використовуйте стандартні порти для роботи Zabbix-сервера;
- видаляйте із сервера утиліти, які дозволять зловмисникові швидко покинути тунель;
- розділіть привілеї облікових записів користувачів в Zabbix;
- налаштуйте аудит подій в Zabbix-сервері, щоб фіксувати і відслідковувати події безпеки;
- ізолюйте Zabbix-сервер від тих компонентів, які зловмисник може використовувати в якості точки входу в корпоративну мережу;
- налаштуйте відправку оповіщення про критичні події.

Безпека Zabbix агента теж вимагає пильної уваги:

- не використовуйте стандартні порти для роботи Zabbix-агента;
- на Windows ОС, Zabbix агент запускається як служба, краще зробити для неї окремого користувача, інакше служба буде запущена з параметрами системного облікового запису;
- вимкніть запуск віддалених команд за допомогою Zabbix;
- налаштуйте шифрування даних в конфігурції агента.

Основне завдання адміністратора в Zabbix - це правильна настройка безпечного доступу, підвищення безпеки системи з використанням додаткових інструментів і наявних методів захисту. Zabbix пропонує розширені опції безпечної автентифікації, та гнучку схему доступів користувачів за допомогою веб-інтерфейсу.

Основні методи автентифікації, які використовує Zabbix це:

- Open LDAP;
- Active Directory.

В Zabbix можна задати глобальний метод автентифікації. Використовуючи веб-інтерфейс, Zabbix підтримує кілька способів автентифікації:

- автентифікація через внутрішню базу даних;
- HTTP автентифікація;

- LDAP автентифікація.

Підтримка шифрування і взаємної автентифікації в Zabbix дає можливість користувачам поступово і вибірково покращувати безпеку компонентів системи моніторингу.

В керуванні і налаштуванні зашифрованими сполуками Zabbix використовує:

- шифрування на основі сертифікатів RSA;
- шифрування на основі PSK.

Для підтримки шифрування Zabbix, система повинна бути скомпільована і пов'язана з однією з чотирьох криптографічних бібліотек:

- OpenSSL;
- LibreSSL;
- GnuTLS;
- Mbed TLS.

Все це дає можливість використовувати Zabbix в тих системах, де шифрування між вузлами є обов'язковою умовою.

Для забезпечення надійного захисту системи моніторингу в корпоративній мережі розподіленої інфраструктури, потрібно використовувати більш гнучкі інструменти, які будуть ефективно відстежувати події інформаційної безпеки.

Zabbix Threat Control - це плагін з відкритим вихідним кодом, написаний на Python, який дозволяє перетворити систему моніторингу Zabbix в сканер безпеки за участю системи Vulners.

Vulners - це дуже велика і безперервно обновлювана база даних ІБ-контента, що дозволяє шукати вразливості, експлоїти, патчі, результати bug bounty так само, як звичайний пошуковик шукає сайти. Vulners агрегатор даних про уразливість з більш ніж 115 джерел.

Zabbix Threat Control надає Zabbix розширену інформацію про вразливість, що існують у всій вашій інфраструктурі, і пропонує застосовні плани виправлення.

Основний принцип роботи плагіна:

- використовуючи Zabbix API, плагін отримує списки встановлених пакетів, імен і версій ОС з усіх серверів в інфраструктурі (якщо з ними пов'язаний шаблон «Vulners OS-Report»);
- показує рівень загрози кожної вразливості за стандартом CVSS;
- пропонує легко застосовні способи усунення знайдених вразливостей;
- передає дані в Vulners;
- дозволяє корелювати дані з різних джерел;
- отримує інформацію про уразливість для кожного сервера;
- обробляє отриману інформацію, агрегує її і відправляє назад в Zabbix через zabbix-sender;
- відображає в веб-інтерфейсі Zabbix інформацію про уразливість, знайдених у вашій інфраструктурі в Zabbix.

Час, за яке буде опрацьовано всі дані про вразливість залежить від кількості серверів в інфраструктурі і кількості встановлених на них пакетів. Орієнтовно на обробку 1 тисячі серверів витрачається близько 30 хвилин.

Zabbix Threat Control не зможе замінити професійні системи, оскільки не має таких багатих можливостей. Однак він багатофункціональний, швидкий, безкоштовний і добре вписується в існуючу інфраструктуру.

Отже, в Zabbix Threat Control є багато функціональних компонентів для захисту інфраструктури, які добре зарекомендували себе та підходять для цілей ІБ. Також за допомогою Zabbix можна так само і дуже ефективно відстежувати події ІБ на мережевих пристроях Cisco і Juniper, використовуючи протокол SNMP. З точки зору ІБ можна виділити наступні події, які необхідно відстежувати - зміни конфігурацій обладнання,

виконання команд на комутаторі / маршрутизаторі, успішну авторизацію, невдалі спроби входу і багато іншого.

При виборі системи моніторингу IT-інфраструктури потрібно врахувати ряд факторів: в першу чергу оцінити відповідність функціоналу системи моніторингу вашим технічним й бізнес-вимогам та розглянути особливості розгортання та супроводу, щоб підібрати інструмент, що відповідає вашій інфраструктурі і рівню компетенції IT-фахівців.

Література

1. АНАЛИЗ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/analiz-primeneniya-tehnologiy-monitoringa-kompyuternyh-setey.

2. МОНИТОРИНГ И УПРАВЛЕНИЕ СЕТЬЮ ПЕРЕДАЧИ ДАННЫХ [Електронний ресурс] – Режим доступу: http://elib.sfu-kras.ru/handle/2311/6919.

3. БЕЗОПАСНОСТЬ И АУТЕНТИФИКАЦИЯ [Електронний ресурс] – Режим доступу: https://www.zabbix.com/ru/features#security_authentication.

4. Система мониторинга как точка проникновения на компьютеры предприятия [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/dsec/blog/350108/.

5. Мониторинг событий информационной безопасности с помощью ZABBIX [Електронний ресурс] – Режим доступу: https://habr.com/ru/post/215509/.

6. Угрозы под контролем. Превращаем Zabbix в сканер безопасности [Електронний ресурс] – Режим доступу: https://xakep.ru/2018/07/24/zabbix-scanner/.

7. Zabbix как сканер безопасности [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/vulners/blog/416137/.

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ КОМП'ЮТЕРІВ ВІД НОВІТНІХ ЗАГРОЗ НА БАЗІ ESET ENDPOINT SECURITY ТА ESET SECURITY MANAGEMENT

Лук'янець Валентин Геннадійович, БСДМ-71
Державний університет телекомунікацій,
м. Київ

Розглянуто зміст технології захисту корпоративних комп'ютерів. Визначено мету і основні завдання щодо забезпечення кібербезпеки інформаційних систем підприємства. Розроблено рекомендації щодо застосування технології захисту корпоративних комп'ютерів на підприємстві.

Під час ведення сучасного бізнесу широко застосовуються інформаційні технології, які підвищують його ефективність. При цьому виникає проблема забезпечення кібербезпеки корпоративних інформаційних систем, бо вони мають уразливості. Корпоративні комп'ютери (робочі станції) є невід'ємною складовою частиною корпоративних інформаційних систем.

Один з векторів для проведення кібератак і розповсюдження шкідливого програмного забезпечення є користувачі та їх робочі станції. Захист корпоративних комп'ютерів є обов'язковим елементом забезпечення кіберзахисту. Сьогодні класичні підходи до захисту корпоративних комп'ютерів вже не забезпечують належний рівень захищеності користувачів та підприємств від сучасних кіберзагроз.

Впровадження системи контролю та безпеки корпоративних комп'ютерів (робочих станцій) дозволяє здійснювати моніторинг та своєчасно усувати загрози, що пов'язані з несанкціонованою користувацькою активністю, такі як копіювання корпоративних даних на носії, що знімаються, передача таких даних через програми-месенджери, веб-серфінг сумнівних Інтернет-ресурсів, випадкове або навмисне скачування чи встановлення вірусного чи шпигунського програмного забезпечення тощо.

Для забезпечення ефективного захисту кінцевих точок і користувацьких даних використовуються нові підходи й рішення, що забезпечують комплексний захист, який включає в себе крім антивірусу, систему попередження втручання на кінцевій точці (HIPS), локальний брандмауер та технології захисту засновані на репутаційних алгоритмах і світової мережі збору даних про загрози.

За результатами дослідження Gartner [1] ринку рішень уніфікованого управління кінцевими точками компанія ESET визначена як компанія-challenger.

Для протидії сучасним загрозам компанія ESET пропонує цілу екосистему власних розробок і партнерських рішень. Це продукти для захисту кінцевих точок, єдина консоль управління, хмарний сервіс LiveGrid. При застосуванні LiveGrid потенційно небезпечний об'єкт вивчається за допомогою таких інструментів як пошук по репутаційним базам, пісочниця, модуль машинного навчання, і нарешті, при необхідності – експертна оцінка фахівцем. Для захисту критичних даних має використовуватися шифрування, а привілейованих облікових записів – двофакторна автентифікація [2].

ESET Endpoint Security 7 – це комплексне рішення для забезпечення безпеки, що є результатом довгих зусиль, спрямованих на досягнення оптимального поєднання максимальному ступені захисту з мінімальним впливом на продуктивність комп'ютера. Сучасні технології, засновані на застосуванні штучного інтелекту, здатні превентивно протидіяти заражень вірусами, шпигунськими, троянськими, рекламними програмами, хробаками, руткітами і іншими атаками з Інтернету без впливу на продуктивність комп'ютера і перерв у роботі [3].

ESET Security Management Center дозволяє централізовано керувати програмами ESET, встановленими в мережевому середовищі на робочих станціях, серверах і мобільних пристроях. За допомогою веб-консолі ESET Security Management Center (веб-консолі ESMC) можна розгортати рішення ESET, управляти завданнями, застосовувати політики безпеки, відстежувати стан системи і оперативно реагувати на проблеми і виявлення, що виникають на віддалених комп'ютерах [4].

Таким чином, сучасні підходи базуються на комплексному захисті кінцевої точки корпоративної інформаційної системи у вигляді клієнта зі всіма необхідними компонентами, що є зручним для кінцевого користувача. Централізоване управління захистом корпоративних комп'ютерів спрощує роботу адміністраторів безпеки із засобами захисту, так як використовується менше додатків безпеки та, відповідно, витрачається менше зусиль щодо забезпечення їх функціонування.

Література

1. Gartner. Magic Quadrant for Unified Endpoint Management Tools. 6 August 2019. Chris Silva, Manjunath Bhat, Rich Doheny, Rob Smith [Електронний ресурс] – Режим доступу: https://www.gartner.com/doc/reprints?id=1-1ODRVFHP&ct=190812&st=sb.

2. Евгений Куликов. На страже безопасности [Електронний ресурс] – Режим доступу: https://ko.com.ua/na_strazhe_bezopasnosti_129182.

3. Интернет-справка ESET. ESET Endpoint Security for Windows. [Електронний ресурс] – Режим доступу: https://help.eset.com/ees/7/ru-RU/documentation_for_users_connected.html?index.html.

4. Интернет-справка ESET. ESET Security Management Center [Електронний ресурс] – Режим доступу: https://help.eset.com/esmc_admin/71/ru-RU/.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ АНАЛІТИЧНИМИ ДАНИМИ ЩОДО НОВІТНІХ ЗАГРОЗ ЗАСОБІВ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Самандрула В'ячеслав Віталійович, БСДМ-71
Державний університет телекомунікацій,
м. Київ

Сьогодні цифрові технології лежать в основі майже кожної галузі, вони дозволили революціонізувати світ, але вони також підвищують уразливість до кібератак. Протягом усього минулого року в гонці кіберозброєнь між атакуючими і захисниками все більшої популярності набирала тема забезпечення аналітичними даними щодо кіберінцидентів. Інформація про кіберзагрози широко висвітлюється в медіа, обговорюється в соціальних мережах, на спеціалізованих форумах, конференціях з питань кібербезпеки і була визначена, як рішення для боротьби зі зростанням числа і складності інцидентів безпеки.

З метою розуміння підходу до забезпечення аналітичними даними щодо новітніх загроз засобів безпеки корпоративних інформаційних систем пропонуються проаналізовані наступні питання: потреба в забезпеченні аналітичними даними щодо новітніх загроз засобів кібербезпеки корпоративних інформаційних систем; мета та завдання забезпечення аналітичними даними щодо новітніх загроз засобів кібербезпеки корпоративних інформаційних систем; існуючі технологій забезпечення аналітичними даними щодо новітніх загроз засобів кібербезпеки корпоративних інформаційних систем.

Інформація про кіберзагрози широко висвітлюється в пресі і докладно вивчається аналітиками з Gartner, Forrester Research, IDC, Інституту SANS і Національного інституту стандартів і технологій (NIST) та інших. [1, с. 2] Це предмет підвищеного інтересу для бізнесу і державних установ всіх розмірів. При цьому на ринку критично не вистачає не тільки ресурсів, що дозволяють обробити всі інциденти, але і загальної системи, завдяки якій стало б можливим реагувати на них на ранніх стадіях кібератак – в ідеалі до експлуатації, а також накопичувати розподілені знання про загрози, обмінюватися отриманими даними, розслідувати причини загроз і миттєво реагувати на них.

Зростання інтересу до забезпечення аналітичними даними щодо кіберінцидентів багато в чому обумовлено руйнівною історією складних цілеспрямованих кібератак, включаючи всюди поширені постійні загрози (APTs). Навіть найбільші, нібито найбільш захищені, підприємства стали жертвами, іноді на десятки мільйонів доларів. Десять років тому фахівці з IT-безпеки найбільше турбувалися про масові атаки. Сьогодні вони розглядаються як вторинні загрози, які просто створюють «шум» в мережі. У більшості випадків постачальники засобів безпеки і підприємства успішно захищаються від них, аналізуючи перші виявлені екземпляри і швидко поширюючи сигнатури і індикатори компрометації (IOCs). Постраждали кілька початкових жертв, але всі інші можуть виявити і заблокувати атаки. Сьогодні найбільш серйозні порушення і збої даних виникають в результаті добре спланованих комплексних атак, спрямованих на конкретні компанії або галузі. [1, с. 2]

Останній огляд кіберзагроз показує, що дуже важко запобігти атакам і порушенням безпеки через здатність зловмисників націлюватися на уразливості в людях, процесах, а також технологіях. [2, с. 3] Кіберзлочинці поліпшили свою тактику, техніку і процедури до такої міри, що їх дії стало важко виявити, складно досліджувати та запобігти. Їх тактика, техніка і процедури стають менш передбачуваними, більш наполегливими, винахідливими, краще фінансуються, набагато більш організованими і мотивованими грошима. Багато організацій схильні до впливу організованої злочинності, яка використовує шахраїв і вимагає оплати, щоб розблокувати важливі дані і системи. Наприклад, атака вимагачів WannaCry, що почалася в п'ятницю, 12 травня 2017 року, протягом дня охопила понад 150 країн і заразила понад 230 000 комп'ютерів. [3, с. 7]

Атаки і компрометації можуть здійснюватися за хвилини, а процес: атака – компрометація – витік даних – виявлення інциденту – реагування та усунення займає дні, тижні і навіть місяці. І найчастіше це відбувається вже після того, як зловмисник скомпрометував дані. При цьому відповідно до щорічного звіту з інформаційної безпеки Cisco фахівці з безпеки протягом свого робочого дня здатні обробити лише 56% вхідних повідомлень про загрози, а серед цих повідомлень про загрози обґрунтованим визнається тільки кожне друге (тобто 28%). Таким чином, 44% інцидентів залишаються без уваги [4, с. 4]

Забезпечення аналітичними даними щодо кіберінцидентів – система, що дозволяє дізнаватися про загрози, атаки до того, як вони зможуть нашкодити. У випадках, якщо інцидент все ж стався, забезпечення аналітичними даними щодо кіберінцидентів дозволить відреагувати, провести аналіз і його розслідування, при цьому розширюючи базу знань контекстом, механізмами, індикаторами компрометації і аналітикою про існуючі або можливі загрози. [4, с. 10-11]

Аналітичні дані про новітні загрози – це знання про зловмисників, їх мотиви, наміри і методи, які збираються, аналізуються і поширюються таким чином, щоб допомогти співробітникам служб безпеки і бізнесу на всіх рівнях захистити критично важливі активи підприємства. [1, с. 6] Забезпечення аналітичними даними щодо кіберінцидентів організовано навколо конкретних супротивників – кіберзлочинців, агентів кібершпіонажу і хактівістів. Підприємство, яке знає своїх супротивників, може оптимізувати свій захист для протидії супротивникам і атакам, які вони використовують. Програми забезпечення аналітичними даними щодо кіберінцидентів, орієнтовані на ризики, засновані на оцінці інформаційних активів, які необхідно захистити підприємству. Ці активи включають в себе дані, документи і інтелектуальну власність (наприклад, бази даних клієнтів і технічні креслення), а також обчислювальні ресурси (такі як веб-сайти, додатки, вихідний код і мережі).

Використання інтелектуального підходу вже давно визнано найкращою практикою в галузі безпеки. Без цього організації будуть незмінно захищатися від занадто малих, тому що вони не розуміють загроз, з якими вони стикаються, або намагаються захиститися від всіх потенційних загроз – нестійкий підхід, який також може послабити здатність організації діяти ефективно. Наприклад, компанія, яка бажає побудувати об'єкт в потенційно ворожому середовищі, спочатку буде шукати інформацію про загрози, що виходять від зловмисників поблизу, перш ніж намагатися вжити відповідних заходів безпеки. Цей же принцип можна застосувати до кібербезпеки: потрібно зрозуміти свою загрозу, перш ніж можливо захиститися від неї. Ґрунтуючись на даних, аналіз загроз надає контекст, наприклад, хто вас атакує, які їхні мотиви і можливості, і які індикатори компрометації (IOCs) в ваших системах потрібно шукати. Це допомагає вам приймати обґрунтовані рішення про вашу безпеку.

Очевидно, що превентивне отримання інформації про кіберзагрози – дуже корисно, проте саме по собі воно не забезпечить безпеку інфраструктурі. Необхідно вибудувати процес, який допоможе грамотно розпоряджатися як інформацією про способи можливої атаки, так і наявним часом для підготовки до неї. І ключовою умовою для формування такого процесу є повнота забезпечення аналітичними даними щодо новітніх загроз.

Аналітичні дані про загрози допомагають надаючи аналітикам центру операцій безпеки (SOC) і командам реагування на інциденти (IR) діагностичні дані про інструменти атаки і базовий контекст про зловмисників. Ряд постачальників технологій і компаній, що надають послуги безпеки, пропонують потоки даних про загрози. До них відносяться набори індикаторів, які були перевірені і визначені за пріоритетами, а також детальний технічний аналіз зразків шкідливих програм, ботнетів, методів атаки DDoS і інших шкідливих інструментів. Іноді вони додають статистичні дані та інформацію про тенденції, наприклад, списки «топ 10», процентне співвідношення типів шкідливих програм і місць розташування спам-атак і бот-мереж. [1, с. 5-6]

Грубо кажучи, постачальники технологій безпеки діляться на три категорії: компанії, які фокусуються на індикаторах загроз, компанії, які комбінують індикатори загроз з потоками даних про загрози, і компанії, які надають комплексні послуги з забезпечення аналітичними даними щодо кіберінцидентів. Невелика кількість фірм пропонує всі три типи аналізу загроз: перевірені індикатори загроз, канали даних про загрози і аналітичні відомості про стратегічні загрози.

Типовим рішеням в забезпеченні аналітичними даними щодо новітніх кіберзагроз є використання платформ забазпечееня аналітичними даними щодо кіберінцидентів.

Платформи забезпечення аналітичними даними щодо кібернцидентів призначені, в першу чергу, для збору індикаторів компрометації з різних джерел. Вибір платформи безпосередньо повинен залежати від масштабу системи забезпечення аналітичними даними щодо кібернцидентів, планованої до реалізації. Для забезпечення аналітичними даними щодо кібернцидентів можна розглянути такі платформи, наприклад, як: CIF (Collective Intelligence Framework), Maltego, MISP Threat Sharing, IBM X-Force Exchange і ін..

Аналітична інформація про кіберзагрози повинна надходити в діючі системи інформаційної безпеки безперервно і в автоматичному режимі. Причому «автоматичний режим» не обов'язково має на увазі розробку і інтеграцію такої системи з нуля, а «безперервність» не обов'язково означає, що інформація повинна надходити щомиті. Для цих цілей може бути цілком достатньо якої-небудь

не особливо складної технології (наприклад, API-інтерфейсу), що забезпечує обмін даними з пристроєм.

Важливим доповненням до глобальної аналітичної інформації про кіберзагрози служить аналітична інформація локального характеру, що надає додаткові рівні контексту і інформованості. Така інформація базується на аналізі локальних мережевих даних організації і виявленні особливостей, характерних для конкретної інфраструктури. Завдяки цьому досягається ще більша ступінь інтелектуалізації захисних пристроїв, а захисні заходи можуть бути адаптовані до специфіки існуючого обчислювального середовища.

Література:

1. Jon Friedman, Mark Bouchard. Definitive Guide to Cyber Threat Intelligence Using Knowledge about Adversaries to Win the War against Targeted Attacks. Published by: CyberEdge Group, LLC. – 2015 – p. 71.
2. Ernst & Young Global Limited. Cyber Threat Intelligence – How To Get Ahead Of Cybercrime. Insights on Goverance, Risk and Compliance. – 2014. – p. 16.
3. Kaur Sahi Asst S. A Study of WannaCry Ransomware Attack. Int J Eng Res Comput Sci Eng. – 2017. – p. 9.
4. The Threat Intelligence Handbook, Second Edition Moving Toward a Security Intelligence Program Edited by Zane Pokorny Foreword by Christopher Ahlberg, Ph.D. Published by: CyberEdge Group, LLC. – 2019 – p. 121.

ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ МОБІЛЬНИХ ПРИСТРОЇВ НА БАЗІ ESET ENDPOINT SECURITY ТА ESET SECURITY MANAGEMENT CENTER

Гахов Сергій Олександрович, к.військ.н.
Сергієнко Максим Анатолійович, БСДМ-71
Державний університет
телекомунікацій,
М. КИЇВ

Розглянуто зміст технології захисту корпоративних мобільних пристроїв. Визначено мету і основні завдання щодо забезпечення кібербезпеки інформаційних систем підприємства. Розроблено рекомендації щодо застосування технології захисту корпоративних мобільних пристроїв на підприємстві.

Шляхом підвищення ефективності бізнес-процесів сучасного підприємства є впровадження та застосування інформаційних технологій. Підвищення технологічності бізнес-процесів підприємства обумовлює бурхливий ріст числа клієнтських додатків зі зручним інтерфейсом, розрахованим на застосування не тільки ноутбуків, але і мобільних пристроїв, в першу чергу планшетних комп'ютерів і смартфонів.

Застосування мобільних пристроїв в мережах та інформаційних системах підприємства, а також впровадження системи управління мобільними пристроями призводе до більш швидкого реагування користувача на поставлене завдання, веде до можливості спрощення робочих процесів і їх оптимізації, приводячи до значного збільшення продуктивності і ефективності праці, підвищуючи конкурентні переваги даного підприємства.

Експлуатація мобільних пристроїв реалізується за різними концепціями, що, в свою чергу, зумовлює необхідність організації безпечного доступу до внутрішніх ресурсів підприємства з будь-яких віддалених місць та вимагає контролю над мобільними пристроями з боку адміністраторів безпеки підприємства.

Так, за даними дослідження компанії Verizon (Mobile Security Index 2020 Report): 39 відс. організацій зізналися, що постраждали від компрометації безпеки мобільних пристроїв; 66 відс. постраждалих від компрометації сказали, що вплив був значним; 36 відс. сказали, що він мав тривалі наслідки; 37 відс. постраждалих, сказали, що відновлення було важким і дорогим.

Існування загроз безпеці застосування корпоративних мобільних пристроїв зумовлює розроблення та застосування відповідних технологій кібербезпеки, а також проектування і впровадження MDM-систем для реалізації повного циклу управління мобільними пристроями (Mobile Device Management, MDM).

За визначенням компанії Citrix "система управління мобільними пристроями" (MDM) – це будь-який інструмент або програмне рішення, призначені для сприяння адміністраторам в управлінні мобільними пристроями в організації, наприклад смартфонами і планшетами, і забезпеченні їх безпеки. Управління мобільними пристроями є важливим компонентом управління мобільністю підприємства і управління кінцевими пристроями, зокрема тому, що все більше компаній впроваджують політику використання власних пристроїв, що дозволяє співробітникам здійснювати доступ до корпоративних даних, файлів і додатків зі своїх особистих пристроїв [1].

Під час застосування корпоративного мобільного пристрою здійснюється контроль за доступом до додатків, за реалізацією парольної політики і процедурами застосування шифрування. Також при управлінні мобільними пристроями обов'язковим є регулярне проведення аудиту конфігурації і установка необхідних оновлень. У разі необхідності є можливість обнулення параметрів безпеки, видалення критично важливих даних і блокування пристрою при його втраті або звільненні власника.

Рішення захисту корпоративних мобільних пристроїв можна розділити на дві категорії: забезпечення безпеки і управління [2]. Реалізуються різні функції безпеки: від захисту від шкідливих програм, фішингу, обмеження доступу до забезпечення захищеного з'єднання тощо. Управління включає в себе віддалену очистку пристроїв, обмеження установки додатків, попереднє налаштування пристроїв для користувачів і інші елементи, пов'язані з управлінням IT.

Програмне забезпечення ESET Endpoint Security для Android (EESA) призначене для роботи з ESET Security Management Center 7 (ESMC) – консоллю управління, за допомогою якої можна дистанційно керувати всіма рішеннями для забезпечення безпеки ESET.

Програмне забезпечення ESET Endpoint Security для Android призначене для захисту корпоративних мобільних пристроїв від новітніх загроз, а також для захисту даних навіть у разі втрати або крадіжки пристрою. Також воно допомагає адміністраторам безпеки забезпечувати відповідність пристроїв корпоративним політикам безпеки.

Програмне забезпечення ESET Endpoint Security може застосовуватися компаніями малого та середнього розміру без необхідності у відділеному керуванні за допомогою ESET Security Management Center. Адміністратор або користувач кінцевого пристрою може просто надати конфігурацію ESET Endpoint Security для використання іншими колегами. Цей процес повністю усуває необхідність в активації продукту і налаштуванні кожного модуля програми, які в іншому випадку слід виконувати відразу ж після установки програми ESET Endpoint Security.

ESET Security Management Center 7 це програмне забезпечення для централізованого управління продуктами ESET на клієнтських робочих станціях, серверах і мобільних пристроях в мережевому середовищі. Завдяки вбудованій в ESET Security Management Center системі управління завданнями можна встановлювати вирішення ESET по забезпеченню безпеки на віддалені комп'ютери і швидко реагувати на виникаючі проблеми і загрози.

Саме по собі рішення ESET Security Management Center не забезпечує захист від шкідливого коду. Для захисту середовища потрібно, щоб на робочих станціях було встановлено рішення ESET по забезпеченню безпеки, наприклад ESET Endpoint Security.

Таким чином, сучасні підходи базуються на комплексному захисті мобільних пристроїв, що входять до складу корпоративної інформаційної системи, у вигляді клієнта зі всіма необхідними компонентами, що є зручним для кінцевого користувача. Централізоване управління захистом корпоративних мобільних пристроїв спрощує роботу

адміністраторів безпеки із засобами захисту, так як використовується менше додатків безпеки та, відповідно, витрачається менше зусиль щодо забезпечення їх функціонування.

Література

1. Что такое управление мобильными устройствами (MDM)? [Електронний ресурс] – Режим доступу: https://www.citrix.com/ru-ru/glossary/what-is-mobile-device-management-mdm.html.
2. ESET. Mobile protection. Solution overview [Електронний ресурс] – Режим доступу: https://eset.ua/download_files/new_products_pdf/ESET_Mobile_Protection_Product_Overview.pdf.