ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ

Всеукраїнська науково-практична конференція

«ЦИФРОВА ТРАНСФОРМАЦІЯ КІБЕРБЕЗПЕКИ»

Тези доповідей

26 березня 2020
м. Київ

ЗМІСТ

ОГЛЯД ТА ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ В УМОВАХ ПРОМИСЛОВОЇ РЕВОЛЮЦІЇ (INDUSTRY 4.0) В УКРАЇНІ

Якименко Ю. М., к.в.н., доц. - Державний університет телекомунікацій

Сьогодні в світі відбувається четверта промислова революція INDUSTRY 4.0 - її початок покладено в 2011 р. [1,2,3]. (з 2016 р її почали називати епохою четвертої революції, а в Україні підтримали тільки з восени 2018 р.). INDUSTRY 4.0 спрямована насамперед на розвиток: виробництва і мережевих з'єднань шляхом використання Кіберфізичних Систем (CPS), Кіберфізичних виробничих систем (CPPS) і Інтернету речей (IoT). Принцип INDUSTRY 4.0 полягає в тому, що шляхом з'єднання машин, деталей і систем, а також інтелектуальних мереж створюються ланцюжки, елементи яких можуть керувати один одним автономно. Тому ця революція характеризується великою кількістю соціальних медіа та комунікаціями «розумної» технології. Основні компоненти Четвертої промислової революції розглянуті в [1].

Разом із технологічними рішеннями в Індустрії 4.0 важливе місце стало відводитись Кібербезпеці (Cybersecurity) тому, що з'явилися нові типи кіберзагроз, на які треба реагувати, і, насамперед, завдяки організаційним заходам її забезпечення і новим рішенням у розробці та організації систем кібербезпеки.

Кібербезпека в першу чергу повинна передбачати проведення заходів, які пов'язані із захистом місць зберігання, обробки даних і мереж їх передачі, а також - з захистом компютерних систем від різного шкідливого програмного забезпечення та кібератак. Використання цих заходів буде можливо коли в Індустрії 4.0 всі пристрої будуть постійно підключені до промислового IoT, тому актуальність проблеми кібербезпеки буде лише підвищуватися.

Масова цифровізація (діджиталізація), яка є базовим елементом моделі «Індустрія 4.0», також передбачає насичення електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, а їх об'єднання створює кіберфізичні системи, які функціонують в одному просторі [4].

Застарілі або неефективні програмно-апаратні рішення, заощадження виробниками на безпекових компонентах та недостатня кваліфікація спеціалістів з кібербезпеки теж не створюють умови для підвищення ефективності боротьби з кіберзагрозами, а для зловмисників – це тільки збільшує можливості нанесення ними кібератак. Все це є перешкодою на шляху поширення такого важливішого компоненту Індустрії 4.0, як технології IoT.

Для несанкціонованого доступу до IoT- компонентів підприємств зловмисники все частіше використовують: інструменти запуску DDoS-атак - пристрої як точки входу (доступу) до корпоративної мережі; підходи до порушення «периметру системи безпеки» - через велику кількість підключених зовнішніх пристроїв; використання викрадених конфіденційних даних користувачів – через наявність сучасних технологій глибинного збору даних (data mining та інші). Слід враховувати те, що широке використання елементів штучного інтелекту може використовуватися як для запобігання кіберзагрозам, так і для їх створення [5].

Питання кібербезпеки для Індустрії 4.0 все ще залишаються відносно новими для українських реалій. За швидкістю та обсягами впровадження Індустрії 4.0 Україна, маючи для цього великий і подекуди унікальний потенціал, поки демонструє порівняно скромні результати і відстає від всіх своїх основних сусідів у Північній та Східній Європі [5].

Висновки. Для України кібербезпекові аспекти подальшого розвитку в новітньому цифровому середовищі Індустрії 4.0 повинні вирішуватися шляхом модернізації існуючих законодавчих та інших нормативних документів і пов’язаної з ними - політики кібербезпеки.

Настала необхідність в формуванні індустрії кібербезпекових рішень нового покоління, здатних ефективно протистояти сучасним загрозам та ризикам.

Література

1. Четверта промислова революція: зміна напрямів міжнародних інвестиційних потоків: моногр. / А.І. Крисоватий, О.М. Сохацька, І.В. Скавронська і інші //за наук. ред. д.е.н., проф. А.І. Крисоватого та д.е.н., проф. О.М. Сохацької. – Тернопіль: ТНЕУ ФОП Осадца Ю.В., 2018. – 478 с.

2. Опанасюк В. В. Економічні передумови індивідуального виробництва в умовах четвертої науково-технічної революції / В. В. Опанасюк // Економіка. Фінанси. Право. - 2016. - № 11(6). - С. 4-7.

3. Краус Н.М., Краус К.М. Які зміни несе в себе «індустрія 4.0» для економіки та вироáництва? Економічні проблеми розвитку галузей та видів економічної діяльності. / Формування ринкових відносин в Україні № 9 (208)/2018, 2018.- С. 128 - 135.

4. Піжук, О.І. Цифровізація як зміна парадагми розвитку економічних систем / О. І. Піжук // Науковий вісник Ужгородського університету : серія: Економіка. – Ужгород, вип. 2(52). 2018. – С.84-91.

5. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України.- Національний інститут стратегічних досліджень, 2019. -[Електронний ресурс] . – Режим доступу: https://niss.gov.ua/en/node/135.

МОЖЛИВОСТІ SIEM-СИСТЕМ З ТОЧКИ ЗОРУ АНАЛІЗУ БЕЗПЕКИ В ІНТЕРНЕТІ РЕЧЕЙ

Щебланін Ю.М., к.т.н., с.н.с. - Державний університет телекомунікацій

На сьогодні існує значна кількість SIEM-систем, розроблених такими компаніями як IBM (IBM Security QRadar SIEM), Symantec (Symantec Security Information Manager), Hewlett-Packard (HP ArcSight) і багатьма іншими.

Постає питання оцінки можливості використання зазначених рішень в процесі забезпечення інформаційної безпеки інтернету речей.

В більшості випадків SIEM-системи збирають та аналізують таку інформацію як:

- події безпеки: події, одержані від брандмауерів (міжмережевих екранів), віртуальних приватних мереж (VPN), систем виявлення злому, систем протидії злому і т.ін.;
- мережеві події: події, отримані від комутаторів, маршрутизаторів, серверів, хостів;
- відомості про операційні системи: найменування виробника та номер версії мережевих активів і т.д.

Одні рішення використовують велику кількість правил кореляції, що поставляються разом з продуктом, та можливість написання своїх правил, інші на зборі та аналізі подій, що виконуються в режимі реального часу і реалізуються за допомогою зіставлення потоку нормалізованих подій з урахуванням правил.

В результаті виявлення події або групи подій, відповідних правилу кореляції, створюється висновок. Висновок в свою чергу може ініціювати створення нового інциденту, або бути автоматично прив'язаним до вже існуючого. Висновки супроводжуються короткими описами, що дозволяють без детального вивчення логів зрозуміти, що відбувається в системі.

Таким чином, можна зробити висновок про те, що розглянуті SIEM-системи мають досить багатий функціонал, гнучкість і масштабованість, однак вони не в повній мірі можуть бути застосовані для аналізу безпеки в інтернеті речей з наступних причин:

- орієнтованість на роботу з вже готовими подіями: події породжують засоби забезпечення безпеки, записуючи їх в журнали, однак для інтернету речей це в загальному випадку не застосовується;

- переважне використання методу кореляції на основі правил, що, по-перше, є досить суб'єктивним рішенням, а по-друге, вимагає регулярного поповнення списку правил, що для великомасштабних систем інтернету речей не завжди може бути можливим;

- відсутність орієнтованості на особливості інтернету речей, в яких ключовими елементами взаємодії є пристрої, а користувач як керуюча одиниця відсутня;

- наявність у більшості рішень програмних агентів, що не завжди можуть бути встановлені на пристрої системи інтернету речей в зв'язку з їх малою потужністю.

Література

1. Обзор SIEM-систем. [Електронний ресурс]. - Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market.
2. Корреляция SIEM. [Електронний ресурс]. - Режим доступу: https://www.securitylab.ru/analytics/431459.php.
3. SIEM как центр системы информационной безопасности. [Електронний ресурс]. - Режим доступу: http://channel4it.com/publications/SIEM-kak-centr-sistemy-informacionnoy-bezopasnosti-kompanii-14716.html.

КЛАСИФІКАЦІЯ КІБЕРФАХІВЦІВ ЗГІДНО З КОНЦЕПЦІЄЮ РОБОЧОЇ СИЛИ З КІБЕРБЕЗПЕКИ

Мужанова Т.М., к.держ.упр.- Державний університет телекомунікацій

У рамках Національної ініціативи з освіти в галузі кібербезпеки США (NICE), метою якої є активізація і розвиток надійної мережі та екосистеми освіти, навчання та розвитку робочої сили в кібербезпеці за допомогою стандартів та найкращих практик [1], була оприлюднена Концепція робочої сили з кібербезпеки (NICE Framework). Цей документ вважають основним ресурсом-орієнтиром для опису та обміну інформацією про фахову діяльність з кібербезпеки, знання, навички та вміння, необхідні у цій сфері.

Концепція звертає увагу на міждисциплінарний характер професійної діяльності з кібербезпеки і встановлює сім категорій фахівців з кібербезпеки, кожна з яких складається зі спеціальностей та робочих ролей. Ця організаційна структура базується на широкому аналізі посад, в результаті якого згруповано види професійних активностей і категорії посад фахівців, які виконують спільні функції, незалежно від робочого місця чи інших умов щодо фаху чи посади [2]. Розглянемо види робочої сили з кібербезпеки детальніше.

До першої категорії «*Безпечне постачання»* (Securely Provision) відносять спеціалістів, які виконують функції з концептуалізації, проектування, закупівель і розробки захищених систем ІТ і відповідають за аспекти розвитку систем або мереж. Спеціальності: управління ризиками, розробка ПЗ, розробка, тестування й оцінювання систем, інші.

Фахівці з кібербезпеки другої категорії «*Експлуатація та супровід»* (Operate and Maintain) забезпечують підтримку, адміністрування та обслуговування, необхідні для забезпечення результативної та ефективної роботи ІТ та засобів безпеки. Спеціальності: технічна підтримка, адміністрування систем і даних, мережеві сервіси тощо.

Управлінські функції (лідерство, стратегічне й поточне управління, просування та інформаційний супровід ідей кібербезпеки), завдяки яким ефективно здійснюється діяльність з кібербезпеки, виконують фахівці з *нагляду й управління* (Oversee and Govern).

Спеціальності: менеджмент кібербезпеки, юридична допомога, адвокація, менеджмент програм та проектів, стратегічне планування й політика, навчання та інформування з кібербезпеки.

Окрему категорію становлять кіберпрофесіонали з *захисту й охорони* (Protect and Defend), до завдань яких входять ідентифікація, аналіз та пом'якшення кіберзагроз для внутрішніх IT та/або мереж. Спеціальності: підтримка інфраструктури кіберзахисту, реагування на інциденти, оцінювання й менеджмент вразливостей.

Аналітики з кібербезпеки (група «*Аналіз*» (Analyze) здійснюють вузькоспеціалізований огляд та оцінку вхідної інформації з питань кібербезпеки з метою визначення її корисності для розвідки. Спеціальності: аналіз усіх можливих даних, аналіз загроз і вразливостей.

До наступної категорії відносять фахівців зі *збирання й обробки* (Collect and Operate), які забезпечують проведення спеціалізованих операцій щодо відмов та шахрайства, а також збір інформації з кібербезпеки для розвідки. Спеціальності: операції зі збору інформації, планування і проведення кібероперацій.

Останню категорію «*Розслідування* (Investigate (IN) становлять спеціалісти, які розслідують кіберподії або кіберзлочини, пов'язані з системами, мережами та цифровими доказами. Спеціальності: кіберрозслідування, цифрова криміналістика.

Отже, функції із кібербезпеки виконують широке коло фахівців з багатьох професійних сфер, а успішне забезпечення кібербезпеки організації є результатом їх добре спланованої і скоординованої фахової діяльності.

Література

1. NICE Cybersecurity Workforce Framework.
URL: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework
2. NIST Special Publication 800-181 National Initiative for Cybersecurity Education Cybersecurity Workforce Framework. 2017. 135 p.
DOI: https://doi.org/10.6028/NIST.SP.800-181

ВИБІР ПОКАЗНИКІВ ДЛЯ ОЦІНЮВАННЯ ВРАЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ

Рабчун Д. І., к.т.н. - Державний університет телекомунікацій

Сучасні підходи до організації процесу оцінювання вразливостей будуються навколо спеціалізованих сканерів, які в автоматичному режимі здійснюють сканування інформаційної інфраструктури. За результатами сканування створюється перелік знайдених вразливостей та їх опис, відповідно до якого здійснюється аналіз/оцінювання та обробка вразливостей.

Одним із загальноприйнятих світових стандартів оцінювання вразливостей інформаційних систем є Common Vulnerability Scoring System (CVSS).

Цей стандарт пропонує простий інструментарій для розрахунку числового показника за десятибальною шкалою, який дозволяє фахівцям з безпеки оперативно приймати рішення про те, як реагувати на ту чи іншу вразливість. Чим вище значення метрики, тим більше оперативна реакція необхідна.

До стандарту водить три групи метрик: *базові*, *часові* та *контекстні* метрики.

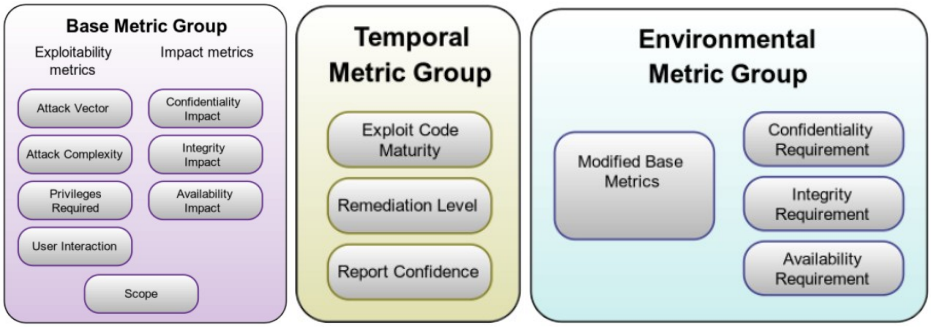

Рис.1. Класифікація метрик згідно з CVSS

Базові метрики описують характеристики вразливостей, які не змінюються з плином часу і не залежать від середовища виконання. Цими метриками описується складність експлуатації вразливості і потенційний збиток для конфіденційності, цілісності та доступності інформації.

Часові метрики вносять в загальну оцінку поправку на повноту наявної інформації про вразливість, зрілість вразливого коду (при його наявності) і доступність виправлень.ё

За допомогою контекстних метрик в результуючу оцінку вносяться поправки з урахуванням характеристик досліджуваної інформаційної системи.

Часові і контекстні метрики не обов'язкові і застосовуються для більш точної оцінки небезпеки, яку представляє дана вразливість для визначеної інфраструктури.

Значення метрики прийнято публікувати у вигляді пари: вектор – конкретні значення окремих показників, і числового значення, розрахованого на основі всіх показників за допомогою формули, визначеної в стандарті. Наприклад, вразливість CVE-2015-2373, відповідно до CVSSv3 має оцінку: (*AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C*) 8.5.

Для визначення якісної оцінки, стандарт CVSSv3 рекомендує використовувати наступну шкалу якісних оцінок: *0* – **None**; *0.1-3.9* – **Low**; *4.0-6.9* – **Medium**; *7.0-8.9* – **High**; *9.0-10.0* – **Critical**.

Таким чином, імплементація наведеного стандарту в процес оцінювання вразливостей, дозволяє отримувати адекватну та обґрунтовану оцінку що, в свою чергу, підвищить захищеність інформаційної системи на підприємствах.

Література

1. Common Vulnerability Scoring System version 3.1: Specification Document [Електронний ресурс] / - Режим доступу: https://www.first.org/cvss/v3.1/specification-document

ДИНАМІЧНА ІТЕРАТИВНА ОЦІНКА РИЗИКІВ, ЯК ЧАСТИНА СИСТЕМИ БЕЗПЕРЕРВНОГО АУДИТУ

Слободяник К.В. - Державний університет телекомунікацій

На сьогоднішній день очевидно істотне відставання в розвитку між технологіями, що використовуються при створенні систем, і методами оцінки ефективності засобів захисту цих систем. Складність інформаційних систем швидко зростає, що неминуче веде до збільшення складності аналізу загроз і оцінки його застосовуваних методів захисту. Недостатня оцінка створюваних систем з точки зору інформаційної безпеки, в свою чергу, веде до виникнення нових загроз або збільшення ймовірності реалізації старих. Існуючі засоби автоматизації

складно адаптуються до розвитку технологій і не дозволяють здійснювати комплексний аналіз взаємозв'язків використовуваних технологій в термінах інформаційної безпеки. У зв'язку з цим все більшої важливості набуває завдання автоматизації процесів і завдань, що вирішуються в ході аналізу та управління ризиками, а також підвищення актуальності одержуваних результатів.

При використанні класичного підходу, час між початком аналізу системи і створенням звіту часто перевищує час появи і реалізації загроз. Крім того, для проведення процедури аналізу ризиків інформаційної безпеки в класичному підході необхідно провести моделювання автоматизованої системи, що само по собі є досить важким завданням.

Отже, можна виділити наступні основні недоліки існуючих підходів до оцінки ризиків інформаційної безпеки:

- складність роботи в умовах явної неповноти інформації про складові ризику і їх неоднозначні властивості;
- необхідність створення моделі інформаційної системи;
- тривалість процесу і швидка втрата актуальності результатів оцінки;
- складність агрегації даних з різних джерел, в тому числі статистик і експертних оцінок;
- необхідність залучення окремих фахівців з аналізу ризиків;
- суб'єктивність і неоднозначність одержуваних оцінок;
- труднощі використання оцінок для завдань управління;
- складність автоматизації процесу.

У зв'язку з цим виникає необхідність отримувати поступово уточнюється оцінки ризиків в ході роботи фахівця. Шляхом автоматизації процесу обліку загроз, пов'язаних з появою нових вразливостей в типовому ПЗ, і формалізації змін в бізнес-ландшафті, можна створити середовище, що дозволяє фахівцеві створювати звіти про стан захищеності тієї чи іншої інформаційної системи, ґрунтуючись на серії послідовних звітів, складених за короткий проміжок часу. Обробка цих даних з використанням різних методів статистичного прогнозування дозволить визначити оптимальний набір контрзаходів з урахуванням «майбутніх ризиків» і тим самим підвищити ефективність впровадження превентивних контрзаходів істотно знизити час реакції системи на появу нових вразливостей [1, 2].

При послідовній реалізації даного підходу оцінка ризиків перетворюється в безперервний процес, що дозволяє здійснювати контроль відповідності поточних значень інформаційних ризиків їх оптимальних значень, і, в кінцевому підсумку, забезпечувати підтримку стану інформаційної безпеки в автоматизованих системах на заданому рівні.

Повертаючись до визначення, безперервний аудит - це середовище, що дозволяє внутрішньому або зовнішньому аудитору виносити судження по значущих питань, грунтуючись на серії створених одночасно або з невеликим проміжком звітів.

Відповідно до цього, визначимо поняття безперервного аналізу ризиків як середовища, що дозволяє фахівцеві оцінювати ризики інформаційної безпеки грунтуючись на створених одночасно або з невеликим проміжком звітів про функціонування АС, засобів захисту інформації та інцидентів інформаційної безпеки, пов'язаних з реалізацією загроз.

Для реалізації безперервної оцінки ризиків необхідно створити систему динамічної ітеративної оцінки ризиків інформаційної безпеки. При цьому входом даної системи в загальному вигляді будуть спостерігатись параметри системи. Відповідно до використовуваним в роботі підходом, для отримання оцінки ризику необхідно на підставі даних спостережень зробити оцінку апостеріорної ймовірності реалізації загроз. Підсумкова оцінка ризику виходить множенням результуючої ймовірності на величину наслідків. Можуть бути використані також інші методи. Методи оцінки наслідків, які застосовуються для отримання результуючої оцінки, в даній роботі не розглядаються.

Аналіз окремих методологій, що використовуються в практиці роботи аудиторів і фахівців з безпеки, а також інструментальних засобів дозволяють проводити кількісну оцінку ризиків мають ряд недоліків, а саме: потрібна побудова моделі автоматизованої

системи; процес аналізу ризиків не є ітеративним, не забезпечена можливість для уточнення оцінок ризиків, отриманих на попередніх етапах; не передбачені кошти для агрегації якісних і кількісних оцінок, що ускладнює використання результатів аналізу для вирішення завдань управління; не передбачено можливості навчання системи.

Для більш ефективного аналізу ризиків інформаційної безпеки телекомунікаційних мереж є застосування методики динамічної ітеративної оцінки ризиків інформаційної безпеки, який позбавлений зазначених вище недоліків.

Література

1. Уткин Л.В. - http://www.levvu.narod.ru/Papers/Bayes.pdf
2. G. Dreyfus, Neural networks:methodology and applications, Birkhauser, 2015

УПРАВЛІННЯ РИЗИКАМИ В СИСТЕМІ МЕНЕДЖМЕНТУ ПІДПРИЄМСТВА

Самосюк В.В. - Державний університет телекомунікацій

Порядок ринкових взаємовідносин об’єктивно обумовлює існування ризику в усіх галузях господарського функціонування. За останні кілька років, роль ризик-менеджменту на глобальному рівні набуває все більшого значення.

Актуальність даної проблеми обґрунтована реальністю існування ризиків у функціонуванні більшості компаній.

Ефективність управління ризиками повинна відповідати кінцевій меті всього менеджменту та контролю ризиків – забезпеченню максимального збереження активів і капіталу на основі мінімізації ризиків, які можуть несподівано різко скоротити ресурси компанії. Так як підприємство веде свою діяльність не лише на внутрішньому, але й на зовнішньому ринку, то часто ефективній роботі підприємства заважають різного роду ризики.

Так, можна виділити три основні організаційні аспекти створення структури управління ризиком на підприємстві:

діяльність ведучого ризик-менеджера;

діяльність відділу управління ризиками;

взаємозв'язок відділу з іншими структурними підрозділами підприємства.

Формуючи механізм управління ризиками, в першу чергу, необхідно визначити рівень централізації управління ними на конкретному підприємстві [1]. Дослідження діяльності машинобудівних підприємств продемонструвало, що функцію управління ризиками покладено саме на директора чи фахівців основних структурних підрозділів. Дані робітники не є фахівцями з ризикології, а тому не здатні ефективно прогнозувати і керувати виникаючими ризиковими ситуаціями. Проте, для забезпечення стабільного розвитку підприємства, директори не повинні чекати настання таких обставин, а залучати до управління ризиками фахівців, на яких можна покласти обов’язки з управління ризиками підприємницької діяльності – ризик-менеджерів.

Таким чином, безпосереднє виконання функцій з управління ризиками, можливе на рівні:

спеціального підрозділу з управління ризиками (відділу управління ризиками чи служби управління ризиками в межах планово-економічного відділу) або спеціаліста по управлінню ризиками (ризик-менеджера) з певними функціональними обов’язками та необхідними матеріальними, фінансовими, трудовими та інформаційними ресурсами;

керівника та (чи) кваліфікованих фахівців головних функціональних підрозділів підприємства [2].

Вивчення передумов виникнення ризиків, оцінка причин та розробка конкретних заходів з ризик-менеджменту є важливими складовими ефективного управління діяльністю підприємства. Управління ризиками можна здійснювати самостійно – управлінським апаратом організації, так і з залученням консультаційних послуг фірм, що спеціалізуються на ризик-менеджменті.

Література

1. Галіч М.Ю. Теоретичні засади ризику та ризик-менеджменту. – Режим доступу: http://n- visnik.oneu.edu.ua/files/archive/nv.

2. Цвігун Т.В. Формування механізму управління ризиками машинобудівних підприємств. – Режим доступу: http://elar.khnu.km.ua/jspui/bitstream.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СИСТЕМ

Костенко В.С. - Державний університет телекомунікацій

Корпоративні інформаційно-аналітичні системи (КІАС) стають сьогодні одним з головних інструментів керування бізнесом, найважливішим засобом виробництва сучасних корпорацій.

Корпоративна інформаційно-аналітична система - це сукупність технічних і програмних засобів підприємства, що реалізують ідеї й методи автоматизації. Головне завдання КІАС - ефективне управління ресурсами підприємства (матеріально - технічними, фінансовими, технологічними й інтелектуальними) для одержання максимального прибутку й задоволення матеріальних і професійних потреб усіх співробітників підприємства.

Забезпечення інформаційної безпеки актуально насамперед для корпорацій зі складною, територіально-розподіленою, багаторівневою структурою. Найчастіше корпоративні інформаційно-аналітичні системи подібних організацій побудовані з використанням устаткування різних поколінь і від різних виробників, та обслуговуються різними підрозділами, що помітно ускладнює процес керування. Крім того, інформаційні структури корпорацій відрізняються різнорідністю, вони складаються з різних баз, наборів розподілених систем і завдань локального характеру. Це робить ресурси корпоративного рівня особливо вразливими.

Компанії поступово усвідомлюють, що традиційного антивірусу та файрволу вже недостатньо, ландшафт загроз і атаки стають усе більш складними [1].

Загалом наразі існує дві тактики атак на корпоративні інформаційно-аналітичні системи [2]:

1) Застосувати вірус, троянський кінь, черв’як, маючи на меті компрометацію якомога більшої кількості систем. В результаті створити ботнет - мережу скомпрометованих комп’ютерів та застосувати її для організації розподілених атак на відмову в обслуговуванні (DDoS) або для іншої злочинної діяльності.

2) Проводити атаку прицільно (таргетована атака) для компрометації комп’ютерів конкретної установи або конкретних користувачів або типів систем (наприклад енергетичних - Stuxnet). Застосувати спеціально сконструйоване шкідливе програмне забезпечення (заради успіху атаки на розробку таких програм можуть виділятись значні кошти). Для таргетованої атаки може здійснюватись впровадження в атаковану організацію шпигунів і інформаторів, а також атаки на треті сторони, що надають сервіси тим, кого атакують.

Для протидії загрозам або хоча б зменшення збитків необхідно свідомо й цілеспрямовано вибирати заходи і засоби забезпечення захисту інформації від навмисного

руйнування, крадіжки, псування, несанкціонованого доступу, несанкціонованого читання й копіювання.

Література

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа / За заг. ред. д-ра. тех. наук, проф. В.Б. Толубка – К.: ДУТ, 2015. – 288 с.

2. Хмелевський Р.М. – Дослідження оцінки загроз інформаційній безпеці об’єктів інформаційної діяльності. – Сучасний захист інформації № 4, 2016.

АУДИТ СУІБ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Алєксєєнко М.В. - Державний університет телекомунікацій

Інформаційна безпека організації – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Сучасна інформаційна система організації являє собою розподілену і неоднорідну систему, яка використовує різні програмно-апаратні компоненти і має точки виходу в мережі загального користування (наприклад, Інтернет). У зв'язку з цим значно ускладнюється завдання правильної і безпечної конфігурації компонентів і забезпечення захищеної взаємодії між ними, і, як наслідок, збільшується кількість вразливих місць в системі.

Наявність вразливостей в системі дає можливість потенційному порушнику провести успішну атаку і завдати шкоди діяльності організації.

Поява «слабких місць» може бути зумовлене різними причинами, як об'єктивного (наприклад, недоробки в базовому програмному забезпеченні), так і суб'єктивного характеру (наприклад, неправильне налаштування обладнання).

Виявлення та усунення вразливостей, а також оцінка загального рівня захищеності є надзвичайно важливою складовою забезпечення безпеки, що дозволяє істотно підвищити рівень захищеності інформаційних та інших ресурсів системи.

Саме для оцінки реального стану інформаційної безпеки підприємства (організації) і проводиться аудит. Він дозволяє оцінити поточну безпеку функціонування інформаційної системи, оцінити і прогнозувати ризики, управляти їх впливом на бізнеспроцеси, коректно і обґрунтовано підійти до питання забезпечення безпеки інформаційних активів, стратегічних планів розвитку, маркетингових програм, фінансових і бухгалтерських відомостей, вмісту корпоративних баз даних.

В кінцевому рахунку, грамотно проведений аудит безпеки інформаційної системи дозволяє забезпечити максимальну віддачу від коштів, інвестованих у створення і обслуговування системи безпеки підприємства.

В основу проведення аудиту покладені вимоги міжнародних стандартів таких як ISO/IEC 27k, COBIT, ITIL, ДСТУ ISO/IEC 19011 та інших, що дозволяє використовувати знання та кращі міжнародні практики в сфері аудиту систем інформаційної безпеки [1, 2].

Розрізняють внутрішні та зовнішні аудити інформаційної безпеки.

Внутрішній аудит ІБ - безперервна діяльність, яка здійснюється відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту та затверджується керівництвом компанії. Аудит проводиться силами та засобами штатних працівників компанії.

Зовнішній аудит ІБ - систематичний, незалежний і документований процес отримання свідчень діяльності організації із ЗІБ і встановлення ступеня виконання в ній критеріїв аудиту ІБ, що проводиться зовнішньою по відношенню до організації, яка перевіряється, незалежною організацією і допускає можливість формування професійного аудиторського судження про стан інформаційної безпеки організації.

Таким чином, в залежності від розмірів підприємства, кількості інформаційних систем, інформації, яка обробляється і ресурсів, які виділяються на проведення аудиту інформаційної безпеки, керівництво підприємства визначається з видом аудиту інформаційної безпеки.

Література

1. ISO/IEC 19011:2002 «Guidelines for quality and/or environmental management systems auditing».
2. ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems».

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

Андрусінко В.Ю. - Державний університет телекомунікацій

Сучасне життя немислиме без ефективного управління. Зважаючи на бурхливу інформатизацію суспільства в останній час більшої уваги потребують системи обробки інформації, від яких багато в чому залежить ефективність роботи будь-якого підприємства чи установи.

Така система повинна:

- забезпечувати отримання загальних та деталізованих звітів за підсумками роботи;
- дозволяти легко визначати тенденції зміни найважливіших показників;
- забезпечувати отримання інформації, без істотних затримок;
- виконувати точний і повний аналіз даних.

Сьогодні, на ринку є великий вибір сучасних СУБД, з різноманітним інструментарієм та функціоналом, призначених для різних ОС (операційних систем).

Проблема забезпечення захисту інформації є однією з найважливіших при побудові надійної інформаційної структури установи. Ця проблема охоплює як фізичний захист даних і системних програм, так і захист від несанкціонованого доступу до даних, що передаються по лініях зв'язку і перебувають на накопичувачах, що є результатом діяльності як сторонніх осіб, так і спеціальних програм-вірусів.

Таким чином, в поняття захисту даних включаються питання збереження цілісності даних і управління доступу до даних (санкціонування) та безпосередньо доступ до даних (доступність).

Технологічний аспект цього питання пов'язаний з різними видами обмежень, які підтримуються структурою СУБД і повинні бути доступні користувачу [1].

До них відносяться:

- обмеження поновлення певних атрибутів з метою збереження необхідних пропорцій між їхніми старими і новими значеннями;
- обмеження, які потребують збереження значень поля показника в певному діапазоні;
- обмеження, пов'язані із заданими функціональними залежностями.

У світі існує безліч СУБД. Незважаючи на те, що вони можуть по-різному працювати з різними об'єктами і надають користувачу різні функції й засоби, більшість СУБД спираються на єдиний комплекс основних понять що дає можливість розглянути одну

систему й узагальнити її поняття, прийоми й методи на весь клас СУБД [2].

Література

1. Основні відомості про бази даних. – Режим доступу: -https://support.office.com/uk-ua/article.
2. Шамшина Н.В. Методичні особливості вивчення зв'язків та типів об'єднання у базах даних Microsoft ACCESS. – Режим доступу: - https://cyberleninka.ru/article/n/metodichni-osoblivosti-vivchennya-zv-yazkiv-ta-tipiv-ob-ednannya-u-bazah-danih-microsoft-access

ЗАХИСТ ВЕБ-СТОРІНКИ НА ПРИКЛАДІ ВЕБ-СЕРВЕРУ IIS

Лукашук М.Ю. - Державний університет телекомунікацій

В час нестримного розвитку технологій, інформатизації та щоденного їх вдосконалення, інформація стає легко- та зручно-доступною. Достатньо ввести у пошукове вікно слово або словосполучення і ви отримаєте велику кількість відповідей. Так само легко можна зайти на WEB-сторінку відомих газет, журналів, телеканалів. Ви одразу бачите безліч інформації. У чому ж полягає одна з основних проблем інформаційної безпеки на сьогоднішній день? У захисті відкритих і закритих інтернет-ресурсів.

Під час створення WEB-сторінки та визначення операторів, вузли яких будуть використовуватися для підключення до мережі Інтернет, необхідно керуватися законами України, іншими нормативно-правовими актами, що встановлюють вимоги з технічного захисту інформації.

WEB-сторінка може бути розміщена на власному сервері або на сервері, що є власністю оператора. Власник сервера зобов'язаний гарантувати власнику інформації рівень захисту у відповідності до нормативного документа системи технічного захисту інформації НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» [1].

Розглянемо реалізацію захисту WEB-серверу на прикладі IIS.

IIS (Internet Information Services) - це набір серверів для декількох служб Інтернету від компанії Майкрософт. IIS поширюється з операційними системами родини Windows.

Основним компонентом IIS є веб-сервер, який дозволяє розміщувати в Інтернеті сайти. IIS підтримує протоколи HTTP, HTTPS, FTP, POP3, SMTP, NNTP. IIS другий за популярністю веб-сервер за кількістю сайтів, після Apache HTTP Server [2].

Компанія Microsoft випускає три типи засобів для забезпечення безпеки WEB-серверу IIS. До них відносяться:

- сервіс-пакети - набір оновлень програмного забезпечення, що об'єднані для зручності. Вони виправляють помилки у коді, удосконалює можливості програмних продуктів і містять оновлення для драйверів. Також надають додаткові функціональні можливості. Сервіс-пакети кумулятивні. Це зручно, так як для встановлення всіх оновлень необхідно встановити лише один сервіс-пакет;
- «гарячі виправлення» - патчі певних продуктів, що забезпечують оновлення за конкретними параметрами. «Гарячі виправлення» слід встановлювати лише тоді, коли трапилась певна серйозна помилка, для виправлення якої вони і розроблені.
- додаткові компоненти безпеки - «гарячі виправлення», що усувають конкретне уразливе місце. При роботі з додатковими компонентами безпеки керуються тими ж правилами, що її при встановленні «гарячих оновлень».

Не дивлячись на те, що слід дуже серйозно відноситись до встановлення оновлень, пов'язаних з безпекою, не слід встановлювати абсолютно усі оновлення, що з'являються.

Перед встановленням нового патчу слід переконатися у тому, що ризик не встановлення цього патчу більший за ризик, пов’язаний з його встановленням.

Таким чином, використання веб-серверу IIS (за умови регулярного встановлення оновлень безпеки) дозволяє забезпечити безпеку веб-ресурсу. Використання технології SSL є рекомендованим для забезпечення шифрування критичної інформації під час її передачі (наприклад, під час аутентифікації та авторизації користувача на сайті).

Література

1. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу [Електронний ресурс]. - Режим доступу: http://dstszi.kmu.gov.ua/
2. Налаштування роботи веб-клієнту на IIS сервері. [Електронний ресурс]. - Режим доступу: https://fossdoc.com/sed-docs/configuring-webclient-on-iis-server.

АНАЛІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СТАНДАРТІ IEEE 802.16E (WIMAX)

Іванов Б.К. - Державний університет телекомунікацій

Оскільки безпека є питанням першочергової ваги для кожної організації, доречно буде сказати, що ефективне функціонування бездротової мережі залежить від того, наскільки сильні її параметри захисту. Основними вимогами до забезпечення безпеки для будь-якого протоколу зв'язку є аутентифікація (відправник/одержувач впевнені в автентичності особистості один одного), конфіденційність інформації (ніхто не може зрозуміти повідомлення, крім передбачуваного одержувача), цілісність даних (повідомлення не може бути змінено) і доступність, під якою розуміють так звану нечутливість до DoS-атак, тобто впливів на систему, які призводять до її відмови у наданні послуг.

Типовими загрозами будь якої бездротової мережі є [1]:

Зловмисник може отримати доступ в мережу через бездротові з'єднання, які не захищені належним чином; зловмисник потенційно може обійти будь-який захист, встановлений в мережі, міжмережеві екрани.

Незашифрована інформація, що передається, може бути перехоплена будь-якою особою, у якої є приймач, налаштований відповідним чином.

DoS-атаки можуть проводитися дуже легко.

Тут перераховано лише деякі загрози, тоді як насправді їх існує набагато більше. Саме через це при розробці стандарту IEEE 802.16e - 2005, 2009 підрівню безпеки приділялася особлива увага .

Задовольняючи вимоги сервіс-провайдерів (NSP , Network Service Provider), підрівень безпеки забезпечує послуги аутентифікації і авторизації . Аутентифікація дозволяє встановити справжність користувача і пристрою, який він використовує. За допомогою процедури авторизації NSP встановлює відповідність між аутентифікованим користувачем і списком доступних йому сервісів. Таким чином , сервіс-провайдери можуть бути впевнені в тому , що доступ до мережі отримають тільки їх клієнти , і що вони будуть використовувати тільки ті сервіси , які оплатили.

З іншого боку, підрівень безпеки стандарту IEEE 802.16e-2005, 2009 задовольняє основні вимоги користувачів - впевненість у конфіденційності й цілісності даних, що передаються в мережі, а також у тому, що клієнт завжди зможе отримати доступ до оплачених ним сервісів [2].

Підрівень безпеки визначений тільки на канальному рівні еталонної моделі OSI. Тому всі поставлені перед ним завдання вирішуються трьома способами:

використання засобів протоколу EAP (Extensible Authentication Protocol) і алгоритму RSA (Rivest, Shamir і Adleman) для аутентифікації і авторизації АС;

здійснення криптографічних перетворень над трафіком, забезпечуючи конфіденційність, цілісність і автентичність даних, а також автентичність і цілісність службових повідомлень MAC-рівня;

використання протоколу управління ключами PKM (Privacy and Key Management protocol) для безпечного розподілу ключової інформації[1].

Література

1. Технологія WiMAX. [Електронний ресурс]. - Режим доступу: https://wiki.cuspu.edu.ua/index.php_WiMAX.
2. Аналіз мереж стандарту WiMAX. [Електронний ресурс]. - Режим доступу: http://inmad.vntu.edu.ua/portal/static/F25CA304-6EB7-454E-BDB9-C09BD03F8D36.pdf

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Щебланін Ю.М. к.т.н., с.н.с., Дьячук О.С. – Державний університет телекомунікацій

Інформаційна безпека відіграє важливу роль у забезпеченні життєво важливих інтересів будь-якої держави і компанії.

Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства, держави та успішної компанії. За умов конкурентного середовища, значного поширення набули такі негативні явища, як підслуховування та викрадення інформації з обмеженим доступом на матеріально-речових носіях, зняття інформації з технічних засобів та інформаційно-телекомунікаційних мереж [1].

Суперечності перехідного періоду свідчать про наявність комплексу невирішених проблем, що стримують економічний розвиток українських підприємств.

Нині перед суб’єктами підприємницької діяльності гостро стоїть питання щодо вирішення спільної проблеми — інформаційної безпеки підприємств незалежно від форм їх власності.

Тільки наявність достатніх сил та засобів охорони інформації може гарантувати успіхи в економічній сфері не лише одного окремо взятого підприємства чи установи, а й в масштабах держави.

На сьогодні інформаційна безпека дедалі більше стосується саме суб’єктів підприємницької діяльності, яким потрібно захищатися від витоку інформації [2].

Інформаційна безпека — це здатність персоналу підприємства забезпечити захист інформаційних ресурсів та потоків від загроз несанкціонованого доступу до них.

За результатами негативного впливу на основні властивості інформації (конфіденційність, цілісність, доступність) вирізняють дестабілізуючі фактори техногенного, антропогенного, природного характеру.

Останнім часом розвиток суспільства характеризується негативною динамікою не тільки зловмисних порушень роботи інформаційних систем чи мереж, а й злочинів, вчинених з використанням новітніх технологій, найсучаснішої техніки.

Одним із шляхів усунення цих недоліків у сфері підприємництва є проектування організаційно-функціональної підсистеми інформаційної безпеки підприємства і її ресурсного забезпечення.

Актуальність досліджуваної проблеми полягає в тому, що з розвитком конкуренції значного поширення набули такі злочини, як викрадання інформації через комп’ютерні

мережі і прослуховування ліній зв’язку. Тому знання потенційних загроз, причин та умов скоєння таких злочинів дозволить працівникам підрозділів служб інформаційної безпеки підприємств у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зловмисних замахів на інформаційні ресурси та потоки господарюючого суб’єкта.

Література

1. Козачок В. А. Особливості побудови комплексних систем захисту інформації в розподілених корпоративних мережах / В. А. Козачок, Ю. Б. Коваленко // Сучасний захист інформації. - 2015. - № 1. - С. 41-47. - Режим доступу: http://nbuv.gov.ua/UJRN/szi_2015_1_8.
2. Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К. : МАУП, 2006. - 134 с.

АНАЛІЗ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ ЯК ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Недодай М.Г. - Державний університет телекомунікацій

Політика інформаційної безпеки — набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку певного стану інформаційної безпеки організації [1].

Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора — організації, що визначає правила роботи підприємств даної галузі.

У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Крім того, певні вимоги пред'являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства — позиції в рейтингу, рівень надійності і т. ін.

Цікаво, що, згідно з дослідженням з безпеки, проведеного компанією Deloitte, підприємства, які мають формалізовані політики інформаційної безпеки, значно рідше піддаються злому. Це свідчить про те, що наявність політики є ознакою зрілості підприємства в питаннях інформаційної безпеки. Те, що підприємство виразно сформулювало свої принципи і підходи до забезпечення інформаційної безпеки означає, що в цьому напрямку була проведена серйозна робота.

Основа управління інформаційною безпекою це повна та вичерпна модель політики інформаційної безпеки. Таким чином, правильно розроблена політика інформаційної безпеки є основою ефективного управління інформаційною безпекою будь-якого підприємства або організації, звісно, при умові дотримання всіх вимог та правил її створення, впровадження та управління [2].

Таким чином, можемо зробити висновок, що основи ефективного управління інформаційною безпекою починаються з правильно визначених політик інформаційної безпеки. Аналіз сучасних практик, щодо розробки відповідних політик дозволяє, використовувати оптимальні варіанти для різних моделей підприємств. Проведення такого аналізу допоможе краще зрозуміти підходи та принципи, якими керуються організації при створенні власних політик інформаційної безпеки.

Література
1. Хохлачова Ю. Політика інформаційної безпеки об’єкта. / Ю.Хохлачова // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2(24) вип., 2012 р. - Режим доступу: https://ela.kpi.ua/bitstream/123456789/8581/1/24_p23.pdf.
2. Політика інформаційної безпеки АТ «Райффайзен Банк Аваль». - Режим доступу: https://www.aval.ua/storage/files/politika-informacijnoyi-bezpeki-rba-newlogo-1550006492_1550655128.pdf.

ВИДИ ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ВІД ЗАГРОЗ ШКІДЛИВОГО ПЗ

Коваль Т. М., Довбешко В. С. - Державний університет телекомунікацій

В еру глобальної мережі Інтернет одним із основних завдань кібербезпеки підприємства є захист можливостей використання й цілісності мереж та даних, які в них циркулюють. Комплекс заходів безпеки мереж включає як апаратні, так і програмні технології і націлений на запобігання та протидію різноманітним загрозам, Мережева безпека поєднує в собі декілька рівнів захисту на периферії та в мережі. Кожен рівень захисту мережі реалізує політику та елементи управління.

Відповідно до рекомендацій компанії Cisco серед основних напрямів забезпечення мережевої безпеки виділяють, зокрема, такі як: управління доступом, ПЗ проти шкідливого коду, захист бізнес-додатків, засоби безпеки хмарних технологій та електронної пошти, міжмережеві екрани, системи запобігання вторгнень, захист мобільних пристроїв, сегментація мережі, використання віртуальних приватних мереж, засоби веб- та бездротової безпеки [1].

Однак, статистика інцидентів кібербезпеки у 2019 році свідчить, що особливо актуальним є запобігання та протидія загрозам застосування шкідливого програмного коду [2].

На думку фахівців Cisco, з цією метою доцільним є використання удосконалених технологій виявлення та захисту від зловмисного ПЗ, які можуть відслідковувати невідомі файли, блокувати відомі шкідливі файли та запобігати виконанню зловмисних програм у кінцевих точках мережі та мережевих приладах.

Засоби мережевої безпеки, такі як міжмережеві екрани й системи запобігання вторгнень нового покоління, знаходять шкідливі файли, які намагаються вийти в мережу з Інтернету або переміститься всередині мережі. Платформи видимості мережі та аналітики безпеки виявляють аномалії внутрішньої мережі, які можуть свідчити про зловмисне програмне забезпечення. Нарешті, сегментація може запобігти руху загроз всередині мережі і обмежити їх розповсюдження.

Використання веб-сканування через безпечний веб- або Інтернет-шлюз допоможе блокувати підключення користувачів до шкідливих доменів, IP- та URL-адрес, незалежно від того, чи користувачі є в мережі підприємства чи поза нею.

Технологія захисту електронної пошти, розгорнута на базі організації або в хмарі, блокує шкідливі електронні листи, що надсилаються суб’єктами загроз у рамках деструктивних кампаній. Це зменшує загальну кількість спаму, видаляє шкідливий спам та сканує всі компоненти електронної пошти (наприклад, такі як відправник, тема, вкладення та вбудовані URL-адреси) для пошуку повідомлень, що містять загрозу. Ці можливості є критичними, оскільки електронна пошта все ще є вектором номер один, який використовуються суб'єктами загроз для запуску атак.

Розширені технології виявлення та захисту від зловмисного ПЗ для кінцевих точок мережі запобігають запуску зловмисного ПЗ на периферії. Це також допомагає виділити, дослідити та усунути інфіковані кінцеві точки для одного відсотка атак, які проходять навіть через найсильніші системи захисту [2].

Отже, для протидії зловмисному ПЗ доцільно використовувати комплекс різноманітних засобів, які виконують функції виявлення шкідливих програм та захисту даних і мереж організації від їх деструктивного впливу.

Література

1. What Is Network Security? URL: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html#~types-of-network-security (дата звернення: 12.03.2020).
2. Defending against today's critical threats A 2019 Threat Report URL: https://www.cisco.com/c/dam/en/us/products/se/2019/2/Collateral/cybersecurity-series-threat.pdf (дата звернення: 12.03.2020).

РОЛЬ АНАЛІТИКИ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

Муржа П. В. - Державний університет телекомунікацій

Дослідження британської компанії Ernst & Young Global Limited під назвою Global Information Security Survey 2018-19, в якому взяли участь понад 1,4 тис. відповідальних за кібербезпеку керівників найбільших міжнародних компаній з доходами від 10 млн. доларів США, показало, що кібербезпека залишається важливим питанням їх порядку денного. Відповідно до опитування одним із найбільш перспективним напрямом інвестування у цій сфері є аналітика безпеки (Security analytics) (38%) [1].

І для цього є цілком об'єктивні підстави. Загалом під аналітикою безпеки розуміють процес використання інструментів збору, агрегації та аналізу даних для моніторингу стану захищеності систем і мереж підприємства та виявлення загроз їх безпеці. Використовуючи інструменти аналітики безпеки, підприємства й організації отримують кращі можливості для збору максимальної кількості корисних даних для поліпшення практики виявлення та надання оповіщень про спроби атак чи інцидентів, які відбуваються в режимі реального часу.

Залежно від типів програмних інструментів, рішення аналітики безпеки можуть включати у свої алгоритми виявлення великі й різноманітні набори даних. Аналітичні дані збирають кількома способами, зокрема з мережевого трафіку, даних про кінцеву точку та поведінку користувача, хмарних ресурсів, бізнес-додатків, контекстних даних, що не належать до IT, даних ідентифікації та управління доступом, зовнішніх джерел розвідки про загрози.

Останні технологічні досягнення в галузі аналітики безпеки включають адаптивні системи навчання, які налаштовують моделі виявлення на основі досвіду та знань, а також враховуючи логіку виявлення аномалії. Ці технології акумулюють та аналізують в режимі реального часу такі види даних як метадані активів, дані геолокації, розвідувальну інформацію про загрози, IP-контекст тощо [2]. Ці форми даних можуть бути використані як для негайного реагування на загрозу, так і для розслідування.

Використання інструментів аналітики безпеки надають підприємствам кілька ключових переваг. Насамперед, вони забезпечують проактивне виявлення та реагування на інциденти кібербезпеки. Для виявлення загроз або інцидентів безпеки в режимі реального часу програмні засоби аналізують дані з різних джерел, зокрема реєстраційні та облікові дані, поєднують їх з даними з інших джерел та визначають кореляційні зв'язки між подіями.

Інструменти безпекової аналітики сприяють дотриманню підприємствами державних і галузевих нормативних вимог, зокрема щодо обробки та захисту інформації обмеженого доступу, дотримання авторського права та прав інтелектуальної власності тощо. Шляхом моніторингу активності даних, збору облікових даних для аудиту та криміналістики, інтеграції широкого спектру даних засоби аналізу безпеки надають підприємству єдину версію щодо усіх подій, пов’язаних з даними, на всіх пристроях. Це дає можливість постійно стежити за даними, обробка яких регулюється законодавством або нормативними документами, і виявляти потенційну невідповідність.

Рішення аналітики безпеки також є дуже цінними для проведення розслідувань інцидентів, оскільки дозволяють виявити джерело й обставини атаки, скомпрометовані ресурси і втрачені дані, а також встановити етапи розвитку інциденту. Наявність можливості реконструювати й аналізувати інцидент допомагає інформувати та покращувати кіберзахист, запобігати виникненню подібних інцидентів у майбутньому.

Література

1. What is Security Analytics? URL: https://digitalguardian.com/blog/what-security-analytics-learn-about-use-cases-and-benefits-security-analytics-tools (дата звернення: 12.03.2020).
2. Cybersecurity in organizations must enable competitive advantage while they continue to protect and optimize security, EY report reveals URL: https://www.ey.com/en_gl/news/2018/10/cybersecurity-in-organizations-must-enable-competitive-advantage-while-they-continue-to-protect-and-optimize-security-ey-report-reveals (дата звернення: 12.03.2020).

СОЦІАЛЬНІ МЕРЕЖІ, ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Стародубець В. О.- Державний університет телекомунікацій

Актуальність і своєчасність звернення до даного питання обумовлена тим, що, по-перше, на сьогодні Інтернет, як форма подання і поширення інформації використовується переважною більшістю населення різного віку і соціального стану; по-друге, інформація, поширювана в Інтернеті, як правило доходить до цільової аудиторії без необхідної «фільтрації» з боку державних органів, що дозволяє її розповсюджувачам практично безконтрольно реалізовувати відомості протиправного характеру; по-третє, вітчизняна правова система ще не виробила завершений правовий механізм, який регулює правовідносини у віртуальному просторі.

Зворотною стороною стрімкого розвитку соціальних мереж є те, що вони неминуче стають об'єктами та засобами інформаційного управління, а також ареною інформаційного протиборства. Соціальні мережі сьогодні - один з ключових і найбільш ефективних інструментів інформаційного впливу, в тому числі засіб для маніпулювання особистістю, соціальними групами та суспільством в цілому. Не дивно, що вони все частіше використовуються в якості майданчику для ведення інформаційних війн.

Що таке Інтернет для сучасного суспільства? Соціальні мережі - повноцінне спілкування і його невід'ємні атрибути: дружба, сварки, віртуальна любов, загрози. Мережа - клуб за інтересами, «круглий стіл» для обговорення питань, починаючи від варіантів підгузників для дитини і закінчуючи політичними дебатами.

Інтернет - потужний маніпулятор людської свідомості. Нічого не варто "загуглити" в мережі інформацію про супротивників або прихильників будь-якої партії, угруповання. Чи не замислювалися ви про те, що всі ваші дані зберігаються в системі, яку можуть розкрити в будь-яку хвилину?

Таким чином, на основі вивчення та аналізу відповідних джерел визначено основні особливості соціальних мереж, досліджено засоби та методи інформаційних операцій в соціальних мережах в різних країнах світу та запропоновано основні засоби захисту для збереження персональних даних в соціальних мережах, як одного з інструментів сучасних інформаційних операцій.

Література

1. Seth Stephens-Davidowitz [«Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are»]: IT Bestseller / Seth Stephens-Davidowitz: Dey Street Books, 2016. – 352 pages
2. Навіщо за нами стежать в соцмережах і хто продає наші дані? Велике інтерв'ю про Big Data [Електронний ресурс] https://www.youtube.com/watch?v=LZIpsq1YyBg

ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ ПЛАТФОРМИ ANDROID

Тищенко В. С. - Державний університет телекомунікацій

Швидкий розвиток комп’ютерної техніки, стрімкий процес мініатюризації, широке поширення персоналізованих мультимедійних технологій – все це втілилося у тому, що на початку 2020-х років у кожного соціалізованого громадянина є в наявності мобільний телефон, причому у переважній більшості (особливо у людей молодого та середнього віку) мова йде конкретно про смартфони.

Зважаючи на дуже високу складність сучасних смартфонів, насправді дуже важко швидко оцінити, яку конфіденційну інформацію несе у собі смартфон того, чи іншого користувача (особливо, беручи до уваги, що набір програмного забезпечення кожного пристрою може відрізнятися, залежно від особливостей та потреб його власника). Однак, існують і деякі універсальні дані, що потребують захисту. Це, наприклад, банківський рахунок, який може управлятися через мобільний телефон спеціальним додатком, із яких найбільш поширеним в Україні є Privat24.

Для дослідження інформаційної безпеки інформаційних систем на базі Android платформи необхідно вирішити такі задачі:

- проаналізувати важливі, з точки зору питань кібербезпеки, особливості ОС Android, виконати аналіз загроз системі;
- проаналізувати існуючі методи та засоби захисту мобільних систем на базі ОС Android;
- обрати загрози, що не перекриваються (або недостатньо перекриваються) існуючими засобами;
- спроектувати систему захисту для інформаційних систем на базі ОС Android, що нейтралізує загрозу (декілька загроз), обраних на попередньому кроці;
- здійснити програмну реалізацію окремих ланок спроектованої системи захисту;
- здійснити тестування розробленого програмного продукту;
- проаналізувати результати роботи системи захисту, зокрема, оцінити її ефективність та зробити висновки по роботі.

Таким чином, у виконано проектування та реалізацію мобільного програмного забезпечення на базі поширеної ОС Android, призначене для служби централізованого інформування працівників про події галузі кібербезпеки. Такий вибір обумовлений тим, що розробник операційної системи компанія Google приділяє дуже багато уваги питанням технічного захисту інформації та покращити її виріб саме в даній частині в рамках

бакалаврської роботи уявляється малоймовірним. В той же час гарні технічні рішення часто не доходять до кінцевого користувача, оскільки порівняно мало уваги приділяється механізму забезпечення встановлення оновлень операційної системи (зокрема оновлень безпеки). У роботі виконано проектування програмних складових додатку, реалізовано 3 класи, докладно описуються методи цих класів. Наведено методику роботи з програмою.

Література

1. Голощапов А. Google Android. Программирование для мобильных устройств (+ CD-ROM). Москва: БХВ-Петербург, 2011. 438 с.
2. Голощапов А. Google Android. Программирование для мобильных устройств. Москва: БХВ-Петербург, 2012. 448 с.

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Жовтюк А. В. – Державний університет телекомунікацій

Актуальність обраної теми обумовлена перманентною участю у порушеннях інформаційної безпеки інсайдерів, які складають близько 80% зловмисників. У компаніях телекомунікаційної сфери вони створюють передумови та, що призводять до величезних фінансових втрат. Таким чином, з огляду на значні обсяги втрат та шкоди підприємству внаслідок загрозливих дій персоналу, а також відсутність достатніх заходів для захисту від дій інсайдерів, необхідним є вивчення та аналіз різновидів загроз інформаційній безпеці підприємства з вини його працівників.

З огляду на зазначене, використання результатів дослідження сприятиме підвищенню рівня інформаційної безпеки на підприємстві, включаючи дотримання персоналом вимог щодо її забезпечення та уникнення створення умов для завдання шкоди.

Заходи захисту інформації можна умовно поділити на дві групи:

- правові;
- організаційні-технічні.

Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані заходи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а так само гарантують їх здійснення. Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкту правовідносин.

До правових принципів захисту інформації відносяться: легітимність; пріоритет міжнародного права над внутрішньодержавним; економічна доцільність.

Роль організаційно – технічних заходів захисту інформації в системі безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів. Організаційні – технічні заходи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, а так само включають в себе наступні принципи захисту інформації, які мають впроваджуватись на підприємстві задля забезпечення інформаційної безпеки:

- науковий підхід до організації захисту інформації;
- планування захисту;
- керування системою захисту;
- безперервність процесу захисту інформації;
- мінімальна достатність організації захисту;
- системний підхід до організації та проектування систем та методів захисту інформації;

- комплексний підхід до організації захисту інформації;
- відповідність рівня захисту цінності інформації;
- гнучкість захисту;
- багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки;
- багаторубіжність захисту інформації;
- обмеження числа осіб, які допускаються до захищеної інформації;
- особиста відповідальність персоналу за збереження довіреної інформації.

Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, підбору персоналу, що працюватимуть з конфіденціною інформацією, допоможуть підібрати ефективні методи протидії загрозам інформаційній безпеці.

Отже, забезпечення інформаційної безпеки підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Література

1. Вітер С.А., Світлишин І.І. Захист облікової інформації та кібербезпека підприємства. Економіка і суспільство. 2017. №1. С.497-502.
URL:http://www.economyandsociety.in.ua/journal/11_ukr/80.pdf
2. Організаційне забезпечення інформаційної безпеки.
URL:http://zi.vntu.edu.ua/uploads/NMKD///OZIB/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%97.pdf
3. Копитко М.І. Менеджмент інформаційних ресурсів та інформаційна безпека підприємств. навч.-метод. посібник. Львів: Ліга-Прес, 2016. 172 с.
URL:http://dspace.lvduvs.edu.ua/bitstream/1234567890/669/1/%D0%9A%D0%BE%D0%BF%D0%B8%D1%82%D0%BA%D0%BE%20%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D1%96%D0%B2%20%D0%BD%D0%B0%D0%B2%D1%87%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1.pdf

МЕТОДИЧНІ ПІДХОДИ ДО АНАЛІЗУ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ВИЯВЛЕННЯ ОЗНАК КОМП'ЮТЕРНИХ АТАК

Поляков Д. А.- Державний університет телекомунікацій

В наш час Інтернет розвивається дуже швидко, що зумовлює перехід на електронні форми зберігання і передачі інформації, активне впровадження в повсякденне життя електронних форм платежів і багато іншого.

Разом з цим розвивається і змінюється кіберзлочинність, тому за останні 30 років багато речей встигли розвинутись і практично зникнути. Десять-двадцять років тому

кіберзлочинність у більшості випадків була “кібервандалізмом” (сайти знищували просто заради того, щоб комусь щось довести). А зараз більшість злочинів в Інтернеті — економічно мотивована. Так само злочинність еволюціонувала від дій одиноких аматорів та груп “одного дня” до багатошарових структур, дії кожного з прошарків яких несуть реальну небезпеку [1].

Члени організованих угруповань можуть користуватися програмним забезпеченням «державних» хакерів, а «державні» хакери попутно можуть викрадати гроші з банків держави, проти якої йде спецоперація. А якщо інструментарій один раз виклали в мережу, то ним починає користуватися вся спільнота, від професіоналів високого рівня до “скріпткідді”. Все це піднімає ціну кібербезпеки для бізнесу — як і в випадку інших злочинів, подолання наслідків зламів обходиться значно дорожче, ніж їхнє попередження чи навіть те, що злодії можуть вкрасти (а якщо порівняти ціну виконання таких дій із ціною подолання наслідків, то тут різниця, як мінімум, у два порядки).

З останніх новин, кіберзлочинні угруповання з Китаю, Північної Кореї і Росії активно експлуатують тему пандемії коронавіруса (COVID-19) і використовують фішингові листи для зараження жертв шкідливим програмним забезпеченням (ПЗ) і отримання доступу до їх систем [2].

Першим угрупованням, яке використало тему коронавіруса в якості приманки, була група Hades [2].

Імовірно, злочинці діють з Росії і пов'язані з APT28 (Fancy Bear). За словами фахівців з компанії QiAnXin, Hades провела шкідливу кампанію в середині лютого, в ході якої розміщувала троянський бекдор в документах, замаскованих під електронні листи від Центру громадської охорони здоров'я Міністерства охорони здоров'я України [2].

Наступне угруповання, що використало COVID-19 для обману своїх жертв, діяло з Північної Кореї. Як відзначили експерти з південнокорейської компанії IssueMakersLab, група північнокорейських злочинців також розмістила шкідливе ПО всередині документів, в яких детально описується реакція Південної Кореї на епідемію COVID-19. Передбачається, що документи були відправлені південнокорейським чиновникам [2].

Найбільше шкідливих кампаній з використанням теми коронавіруса прийшло з Китаю. Перша з двох атак сталася на початку березня. В'єтнамська фірма з кібербезпеки VinCSS виявила, що злочинна група Mustang Panda поширює електронні листи з шкідливим файлом RAR, нібито призначеним для передачі повідомлення про спалах коронавіруса від прем'єр-міністра В'єтнаму [2].

Компанія CheckPoint зафіксувала злочинну діяльність іншою китайською групою під назвою Vicious Panda. Зловмисники націлилися на урядові організації Монголії, відправляючи документи з інформацією про поширеність нових коронавірусних інфекцій [2].

Таким чином, аналіз даних впливу подій, повязаних з поширенням у світі COVID-19 у світі, показав:

- безпека мереж і мережевих сервісів стала дійсно нагальною проблемою практично кожного користувача, установи або підприємства;
- подальше дослідження повинно бути спрямовано на пошук, розробку і використання ефективних методичних підходів підвищення рівня інформаційної безпеки у напрямку аналізу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак.

Література

1. Побокін М. Кіберзлочинність та кібервійна: хто і як може атакувати вас. ZDNet. - Електронний ресурс. Режим доступу: https://cybercalm.org/analytics/kiberzlochynnist-ta-kibervijna-hto-i-yak-mozhe-atakuvaty-vas/.
2. Киберпреступники в ходе атак рассылают жертвам письма на тему COVID-19/.- Электронный ресурс. Режим доступа: https://www.securitylab.ru/news/505889.php.

ВИМОГИ ДО МОДЕЛЮВАННЯ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Воробйов О.Ю. - Державний університет телекомунікацій

Моделювання передбачає створення моделі і її дослідження (аналіз). Модель це опис або фізичний аналог будь-якого об'єкту, в тому числі системи захисту інформації та її елементів в будь-якій організації. Система захисту інформації підприємства функціонує в умовах впливу безлічі зовнішніх і внутрішніх факторів середовища на виробничу його діяльність, серед яких відповідальне місце займає вплив загроз на безпеку інформації та вжиття заходів щодо підвищення її захисту і в цілому - вплив на ефективність вирішення завдань управління організацією. Загроза – це сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення конфіденційності, доступності та (або) цілісності інформації.

Моделювання загрози - це ітеративний процес, який полягає у визначенні захищуваних активів, визначення того, що кожна програма робить щодо захисту цих активів, створення профілів безпеки для кожної програми, визначення потенційних загроз, визначення пріоритетів потенційних загроз та документування побічних явищ та дій, здійснених у кожній із них [1].

Моделювання процесів порушення інформаційної безпеки завжди здійснюють на основі розгляду логічної послідовності: «загроза - джерело загрози - метод її реалізації – вразливість від загроз – наслідки її у вигляді наступу збитків». Загроза завжди виступа тісною сполучною ланкою в цьому ланцюзі елементів. Якість моделювання загрози визначає ефективність моделювання процесів порушення інформаційної безпеки будь-якої організації.

В роботі [2] приведені основні загрози інформаційній безпеці підприємства :

• втрата (порушення) конфіденційності інформації та ресурсів, тобто розкриття змісту інформаційного ресурсу несанкціонованим користувачем (зловмисником);

• втрата (порушення) цілісності інформації та ресурсів внаслідок впливів як природного, так і штучного характеру;

• втрата або неякісна доступність до інформації та ресурсів підприємства, можливість доступу до інформації зловмисників;

• неякісна спостережливість власників та/або користувачів за інформацією та ресурсами.

Первинний аналіз наведеного переліку загроз безпеці інформації, показує, що для забезпечення комплексної безпеки необхідне прийняття як організаційних, так і технічних рішень. Такий підхід дозволяє диференційовано підійти до розподілу матеріальних ресурсів, виділених на забезпечення інформаційної безпеки. Необхідно відзначити, що оцінити вагові коефіцієнти кожної загрози досить важко через високу змінність їх проявів і відсутності зрозумілої статистики з цього питання. Тому в сучасній літературі можна знайти різні шкали оцінок. Разом з тим, на основі аналізу, проведеного різними фахівцями в області комп'ютерних злочинів [3,4] , за частотою прояву загрози безпеки можна розставити так:

- крадіжка (копіювання) програмного забезпечення (ПЗ);
- підміна (несанкціоноване введення) інформації;
- знищення (руйнування) даних на носіях інформації;
- порушення нормальної роботи (переривання) в результаті вірусних атак;
- модифікація (зміна) даних на носіях інформації;
- перехват (несанкціоноване вилучення) інформації;
- крадіжка (несанкціоноване копіювання) ресурсів;
- порушення нормальної роботи (перевантаження) каналів зв’язку;
- непередбачені втрати.

Для простоти використання при побудові моделі можна вважати, що кожна загроза себе колись проявить, тому всі вони однаково рівні між собою.

При моделюванні загроз необхідно враховувати ще те, що система захисту інформації, як і будь-яка складна система, описується наступними основними параметрами: цілі і завдання; входи і виходи системи; процеси всередині системи, що забезпечують перетворення входів в виходи. Входами такої системи захисту інформації є загрози інформації. Виходами - заходи, які потрібно застосувати для запобігання загрозам або для зниження їх до необхідного рівня.

При моделюванні загроз повинні також виявлятися, аналізуватися і визначатися ризики (ймовірності) загрози, оцінюватися очікуваний від їх реалізації потенційний збиток і ранжування загроз по потенційному збитку.

Рівень ризику інформаційної безпеки підприємства, як кількісний показник, може визначатися рівнем шкоди, що завдається підприємству при реалізації загроз. Рівень шкоди може бути представлений у вигляді якісної характеристики або кількісного показника. Збиток может бути заподіяній будь-ким по різним причинам (злочин, вина або недбалість), або- бути наслідком незалежних від нікого проявів. Збудовані моделі загроз повинні наглядно демонструвати можливості систем захисту інформації підприємства від актуальних видів загроз усіма доступними способами забезпечення її інформаційної безпеки.

При складанні моделі загроз вже зараз використовуються різні варіанти існуючих моделей, які розроблені фахівцями в області захисту інформації державних і недержавних установ. У інформаційних системах підприємств може бути різний спектр загроз, який визначається особливостями конкретної системи і характером можливих дій джерела загрози, тому універсального підходу до створення моделі загроз на данний час не існує.

Література

1. Е. Степченко, В.В. Ерохин, Д.А. Погонышева "Безопасность информационных систем : Учебное пособие. 2016. 184 с.

2. Різник Н. С., Корецька Н. І. Теорії та змістово-типологічні характеристики безпеки підприємства / Н. С. Різник, Н. І. Корецька // Економічний форум. – 2013. – № 1. – 486 с. – С. 238–243

3. Антонюк А.О. Моделювання систем захисту інформації: монографія.-Ірпінь: Національний університет ДПС України, 2015.-273 с.

4. Щеглов А.Ю. Моделювання загрози безпеки інформаційної системи // Захист інформації: основи теорії. підручник, 2018. URL: https://stud.com.ua/180225/informatika/modelyuvannya_zagrozi_bezpeki_informatsiynoyi_sistemi.

ОРГАНІЗАЦІЯ МОНІТОРИНГУ ЗАГРОЗ ФУНКЦІОНУВАННЮ ПІДПРИЄМСТВА

Якушев І. А., Іванченко Б. Т. - Державний університет телекомунікацій

Сучасна соціально-економічна і політична нестабільність в Україні тісно пов'язана з недостатньою розвиненістю механізмів виявлення та попередження всіх видів загроз як національній безпеці держави так і для окремих підприємств, з подальшим своєчасним усуненням негативних наслідків після них.

Одним з ефективних механізмів вирішення зазначених проблем є проведення комплексного моніторингу загроз, організованого на принципах науковості та системності.

В інформаційній сфері моніторинг на підприємстві може розглядатися як система збору, обробки, зберігання і розповсюдження інформації про стан виробничих процесів в

будь-який момент часу, як джерело для планування і прогнозування розвитку, так і для забезпечення ефективності управління інформаційною безпекою (ІБ) підприємства.

Ефективність моніторингу вирішальним чином залежить від правильної його організації, яка повинна полягати в попередньому вивченні ситуації, аналізі можливих небезпечних впливів, проведенні вимірювань, які дозволяють виявити проблему і підготувати адекватні рішення щодо їх попередження або нейтралізації та неприпустимості нанесення шкоди .

В організації моніторингу повинні бути виконані, перш за все, вимоги (принципи) до інформації: об'єктивності (повинна бути максимально формалізована і легко перевірена) та адекватності (повинна враховувати вплив змін від різних зовнішніх умов на досягнення поставлених цілей).

Моніторинг підприємства завжди асоціюється з проведенням його контролю, який повинен бути спрямований на забезпечення основних показників ефективності на всіх етапах управління підприємством, у тому числі і при забезпеченні ІБ. У зв'язку з цим метою контролю на підприємстві є виявлення можливих відхилень від запланованих показників, встановлення причин цих відхилень і розробка заходів щодо їх усунення.

При побудові системи контролю на підприємстві рекомендується встановлювати контроль в три етапи: попередній, поточний, підсумковий. Встановлення такого контролю обумовлено необхідністю підвищення адаптивності підприємства до змін зовнішнього і внутрішнього середовища, особливо в умовах зростання загроз їх інформаційній безпеці

Попередній контроль повинен здійснюватися:

- при формуванні цілей (вибір, перевірка на обґрунтованість і узгодженість, адекватність відповідності кількісних показників, облік обмежень і прогнозу змін).

- при плануванні (обґрунтованість завдань, перевірка повноти і узгодженості заходів, перетворення планових величин в контрольовані параметри, встановлення допустимих меж відхилень контрольованих величин і т.д.)

Поточний контроль необхідно проводити при організації виконання запланованих заходів та реалізації поставлених цілей.

На етапі підсумкового контролю діяльності підприємства оцінюються остаточні результати по досягненню підприємством поставлених цілей і розробляються заходи щодо ліквідації виявлених відхилень і недопущення в майбутньому.

Всі види контролю містять в собі аналіз і вимір кількісних і якісних характеристик (показників) діяльності підприємства, а також виявлення причин відхилень контрольних величин від планових (нормативних) значень.

Автоматизований і безперервний моніторинг ІБ, об'єднаний з усіма видами контролю є головною умовою швидкого виявлення та усунення загроз в інформаційній системі (ІС). Вже є досвід [1] створення рішень на базі продукту HP ArcSight, як спеціалізованої системи моніторингу (в західній термінології різновид SIEM), призначеної для збору, обробки, кореляції і реагування на події ІБ з єдиного центру управління. При цьому регулярний моніторинг стану безпеки ІС (часто в режимі реального часу) спрямований на: виявлення і прогнозування подій та інцидентів ІБ; оцінку рівня поточної захищеності ІС; прийняття рішень з управління ІБ.

Архітектура SIEM, як правило реалізується і включає в себе сервер бази даних, сервер обробки повідомлень і консоль управління системою.

Таким чином, на основі таких систем моніторингу можуть створюватися повноцінні центри управління інформаційною безпекою (SOC), що є актуальним в сучасних умовах зростання атак і загроз на інформаційні ресурси підприємств, і в той же час - представляти цінний напрямок для проведення подальших досліджень щодо їх вдосконалення.

Література

1. Оладько В.С. Цели и задачи мониторинга безопасности информационной системы // В.С. Оладько, А.И. Пушкарская, Е.А. Витенбург Международный научный журнал «Интернаука» // № 4 (26), 1 т., 2017 .- С. 49-51.
2. Тимофєєв Д. С. Впровадження систем моніторингу інформаційної безпеки на підприємстві // Д.С. Тимофєєв, О.В. Стародубець /- м. Дніпро, Державний ВНЗ «Національний гірничий університет», 2017.
http://ir.nmu.org.ua/bitstream/handle/123456789/150647/starodubec_timofeev.pdf?sequence=1

НЕОБХІДНІСТЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Коваленко Н. І. –Державний університет телекомунікацій

Останні півтора десятиріччя одним із головних факторів, що прискорює формування і розвиток суспільства, є інформаційні технології, які надають певні преференції, а також створюють умови для втрати інформації, тому забезпечення безпеки суб'єктів ринку споживання інформації є актуальною проблемою. Інформаційні технології являються не лише глобальним засобом комунікацій без територіальних і національних кордонів, але й ефективним інструментом ведення бізнесу, досліджень, впливу на аудиторію.

Практика свідчить, що інформаційні інтернет-технології урівнюють шанси на успіх малих і великих підприємств, тих, хто міцно закріпився на ринку, і новачків. Це стало можливим тому, що витрати на їх застосування є невеликими, використовуються доступні й фактично стандартизовані інструменти, які надають можливість забезпечити недосяжну за інших умов широту охоплення і при цьому зберегти адресність впливу на цільову аудиторію, забезпечується фактично миттєвий доступ на ринок будь-якої країни чи регіону, можна у реальному масштабі часу оцінювати ефективність бізнесу тощо.

Однак, розвиток інформаційних технологій, також розкриває безліч можливостей для здійснення інформаційних махінацій та шахрайства. Тому особливо значного поширення набуває актуальність розвитку та застосування інформаційної безпеки для захисту розвитку діяльності підприємства і практично-орієнтованого інструментарію ведення бізнесу.

У висновках п'ятого щорічного дослідження корпоративних ризиків «Барометр ризиків Allianz 2016» [1] зазначається, що головним ризиком для підприємств на глобальному рівні четвертий рік поспіль залишаються перерви у виробництві і ланцюгу поставок. Однак більшість компаній стурбовані, що втрати, понесені у результаті перерв у виробництві, які зазвичай відбуваються внаслідок завдання шкоди майну, в майбутньому будуть все частіше зумовлюватися кібератаками, технічними збоями та геополітичною нестабільністю. Стурбованість бізнесу викликає й інша глобальна сфера – це інциденти у кіберпросторі, що включають кіберзлочини або несанкціоновані втручання в бази даних, а також технічні збої в інформаційно-комунікативних системах [2, с.138-139].

Менеджмент вітчизняних підприємств недостатньо приділяє уваги захисту інформаційно-комунікативних систем, створюючи небезпечні ситуації з забезпечення безперервності та беззбитковості бізнесу. Головними причинами є неусвідомлення можливих наслідків кібератак та значні капіталовкладення на створення системи захисту інформаційних ресурсів.

Наслідки втрати інформації можуть мати катастрофічний характер, а саме [2]: зменшення вартості капіталу підприємства; труднощі залучення інвестицій; розрив (або погіршення) ділових відносин із партнерами; зрив переговорів, втрата вигідних контрактів; невиконання договірних зобов'язань; відмова від рішень, які стали неефективними через розголос інформації; втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію; зниження цін або обсягів реалізації; нанесення шкоди

авторитету та діловій репутації фірми; більш жорсткі умови отримання кредитів; труднощі в постачанні та придбанні устаткування тощо.

Отже, уникненню цих проблем, які можуть прийняти системний характер та призвести до банкрутства, є налагодження дієвих заходів із забезпечення інформаційної безпеки підприємства, знаходження ефективних управлінських рішень щодо збалансування х між витратами та вигодами.

Розробка дієвої стратегії формування витрат на забезпечення інформаційної безпеки підприємства із застосуванням сучасних технологій та інструментів, які з'явилися останнім часом і стрімко поширюються, повинна бути метою кожного сучасного підприємства.

Література

1. Top 10 Global Business Risks for 2016: URL: http://www.agcs.allianz.com/assets/PDFs/Reports/ AllianzRiskBarometer 2016.pdf.
2. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету*. 2016. №24-2. С.137-140.

ФОРМУВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ ЯК ЧИННИК ЗАПОБІГАННЯ ПОРУШЕННЯМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мужанова Т.М., к.держ.упр., Мосійчук В.М., Клименко О.І. – Державний університет телекомунікацій

Найкращий вибір керівника – це лояльний працівник. Лояльність – задоволеність працівника умовами праці, винагородою, професійним ростом і перспективами, колективом, рівнем захисту від зовнішніх загроз.

Підприємства, які дбають про довгострокові перспективи розвитку, мають сприяти зростанню лояльності персоналу як основного чинника підвищення продуктивності праці і, в результаті – прибутковості бізнесу. Також лояльність персоналу є «наріжним каменем» у забезпеченні інформаційної безпеки підприємства, оскільки лояльний працівник усвідомлено виконує свою роботу відповідно до цілей і завдань компанії та на її користь, а також дотримується норм, правил і зобов'язань, встановлених у компанії.

Важливість лояльності для бізнесу підтверджується багатьма дослідженнями. За даними американських дослідників, організації з високолояльними працівниками за три роки принесли своїм акціонерам 112% прибутку, організації з середнім рівнем лояльності – 90%, а з низькими показниками лояльності – 76% [2].

Для підвищення лояльності персоналу доцільно здійснювати комплекс заходів, серед яких виділяють такі: забезпечення сприятливих умов праці та позитивного психологічного клімату в колективі, розвиток корпоративної культури й ефективної системи мотивації [3].

Умови праці є однією з передумов стабільної продуктивності праці. За сприятливих умов праці працездатність людини підвищується, тому що немає потреби у витрачанні сил та здоров'я на захист організму від негативного впливу шкідливих виробничих факторів. У результаті досліджень з'ясовано, що заходи з покращення умов праці підвищують її продуктивність на 15–20 % [1].

Створення й підтримання сприятливого психологічного клімату є необхідним, оскільки внаслідок поганого настрою ефективність роботи колективу знижується приблизно в 1,5 рази. На психологічний клімат можна впливати через сприяння згуртованості колективу; забезпечення сумісності співробітників; створення позитивної психологічної атмосфери; формування колективних думок і настрою, а також спільних традицій.

Формування корпоративної культури як важливого чинника лояльності колективу здійснюється через формування належних норм поведінки персоналу у процесі трудової діяльності, оволодіння працівниками необхідними професійними знаннями, вміннями і

навичками, культивування бажаних відносин, ставлення до колег і керівників, заохочення комунікації з метою пропагування й підтримки загальних цінностей, традицій, місії компанії.

У формуванні лояльного працівника значну роль відіграють заходи матеріального стимулювання, насамперед справедливе матеріальне заохочення, достатній соціальний захист і медичне страхування, а також методи нематеріальної мотивації.

Отже, заходи зі зміцнення лояльності персоналу є необхідними на підприємстві. Вони сприятимуть зростанню якості і продуктивності праці, відповідальності працівників, посиленню згуртованості, дисциплінованості й мотивації трудового колективу і, як наслідок, матимуть наслідком підвищення рівня забезпечення інформаційної безпеки підприємства.

Література

1. Гринюк Т. Ю. Сучасні проблеми поліпшення умов праці на підприємстві. Психолого-педагогічні основи гуманізації навчально-виховного процесу в школі та ВНЗ : зб. наук. пр. Рівне. 2014. Вип. 1. С. 121-127.
2. Коваленко Д. В. Методологічні основи соціологічного виміру лояльності персоналу організації. Соціологія майбутнього: науковий журнал з проблем соціології молоді та студентства. 2010. № 1. С. 13-20.
3. Маренич А.І., Мехеда Н.Г. Виявлення та запобігання загроз кадровій безпеці. Фінансовий простір. 2011. № 3 (3). С. 127-132.

ПОЛІТИКА БЕЗПЕКИ ЯК ОСНОВА УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Коваленко О. О., Бородін Р. Р. -Державний університет телекомунікацій

Політика безпеки підприємства (англ. organizational security policies) – сукупність керівних принципів, правил, процедур і практичних прийомів в галузі безпеки, які регулюють управління, захист і розподіл цінної інформації. У загальному випадку такий набір правил являє собою певну функціональність програмного продукту, який необхідний для його використання в конкретній організації. Якщо підходити до політики безпеки більш формально, то вона є набір якихось вимог до функціональності системи захисту, закріплених у відомчих документах. Наприклад, у фінансових організаціях найчастіше прийнято, щоб у продукті передбачалося присутність кількох адміністративних ролей: адміністратор, аудитор і оператор системи захисту. Таке рольове управління інформаційною безпекою – радше данина традиції і теоретично дозволяє уникнути “змови” адміністратора і зловмисника з числа користувачів. Для того щоб включити дану функціональність продукту в профіль захисту, найдоцільніше ввести відповідну політику безпеки. Політика безпеки залежить від:

- конкретної технології обробки інформації;
- використаних технічних і програмних засобів;
- розташування організації;

Головною причиною появи політики безпеки є вимога наявності такого документа від регулятора – організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності. Крім того, певні вимоги (рекомендації) пред’являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства – позиції в рейтингу, рівень надійності і т.д. Наявність політики є ознакою зрілості підприємства в питаннях інформаційної безпеки.

Сама по собі наявність документа “Політика інформаційної безпеки” не принесе істотної користі підприємству. Важливо, щоб політика безпеки була ефективною. Досвід показує, що неефективні політики безпеки можна розділити на добре сформульовані, але не практичні і на практичні, але погано сформульовані. Перша категорія найчастіше зустрічається у випадках, коли фахівці з питань безпеки підприємства недовго думаючи беруть готову політику (скажімо, з Інтернету) і, провівши мінімальні зміни, затверджують її для свого підприємства. Оскільки загальні принципи безпеки у різних підприємств, навіть різних галузей, можуть бути дуже схожі, такий підхід досить широко поширений. Однак його використання може привести до проблем, якщо від політики верхнього рівня знадобиться спуститися до документів нижнього рівня – стандартам, процедурам, методикам і т.д. Оскільки логіка, структура та ідеї вихідної політики були сформульовані для іншого підприємства, можливе виникнення серйозних труднощів, навіть протиріч в інших документах. Політики другої категорії зазвичай з’являються у випадках, коли виникає необхідність вирішити нагальні завдання.

Отже, створення ефективної політики інформаційної безпеки дозволить підприємству не просто створити стрункy систему нормативних документів, але і принесе певні фінансові переваги, наприклад, зберігши інвестиції або запобігши неефективним вкладенням коштів.

Література

1. Політика безпеки. URL: https://wiki.tntu.edu.ua

ЗАГРОЗИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Крочак Р.П. - Державний університет телекомунікацій

В даний час питання використання електронних документів і переходу до електронного документообігу придбали дуже велике значення. Потреба в ефективному управлінні електронними документами призвела до створення систем електронного документообігу (СЕД). Однак при переході до електронного документообігу виникає гостра необхідність в його захисті.

Загрози СЕД можна згрупувати по порушенням властивостей безпеки, до яких належать: загроза конфіденційності; загроза цілісності; загроза доступності.

В цілому СЕД включає в себе три типи компонентів: сервери; робочі місця; канали зв'язку.

За вищеописаної моделі можна скласти список загроз несанкціонованого доступу до СЕД, метою яких є порушення конфіденційності інформації, що зберігається. До даних порушень відносяться: погроза робочим місцям; загроза серверу ОС; загроза серверу автоматизованої СЕД (АСЕД); загроза серверу баз даних; загроза каналам зв'язку між компонентами системи [1].

Для зовнішнього ЕД додатковими вимогами до комплексної системи захисту є: обов'язкова наявність засобів антивірусного захисту з автоматично оновлюємим списком шкідливих програм; наявність засобів ідентифікації атак з реалізованим алгоритмом дій у відповідь на атаки; наявність механізму контролю коректності завантажених в пам'ять комп'ютера даних; наявність механізму запобігання перевантаження СЕД від множинних запитів; наявність засобів запобігання зовнішнього сканування СЕД.

З додаткових вимог до захисту внутрішнього ЕД можна виділити наступні: наявність механізму перевірки правильності задання паролів для доступу до ресурсів, що захищаються; механізму ідентифікації атак на засоби аутентифікації, з реалізованим алгоритмом дій у відповідь; наявність механізму контролю цілісності використовуваного ПЗ; наявність механізму автоматичного оновлення ПЗ; наявність засобів, керуючих правами доступу до

різноманітних послуг та сервісів; наявність засобів запобігання внутрішнього сканування СЕД [1].

Отже, врахування вірогідних загроз надає можливість забезпечити безпечне функціонування електронного документообігу підприємства та дозволяє зберегти інформаційну сумісність всіх його складових елементів: автоматизоване управління процесами, системну взаємодію служб підприємства, що залучаються для забезпечення захисту інформації. Так забезпечується найбільш ефективний захист СЕД підприємства.

Література

1. Бурячок В. Л., Толюпа С.В., Семко В.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ: ДУТ - КНУ, 2016. 178 с.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВ

Рожко В. Г., Жижура Г. О. - Державний університет телекомунікацій

Стрімкий розвиток інформаційних технологій, розширення глобального інформаційного середовища, широке застосування засобів обміну інформацією, всеохоплююча автоматизація всіх сфер життєдіяльності зумовлюють актуальність дослідження питань безпеки інформаційної інфраструктури. Забезпечення ефективного захисту інформації є надзвичайно актуальним і для установ банківської сфери, де щоденно оброблюється великий обсяг інформації різного рівня конфіденційності. Ця інформація в більшості випадків і виступає об’єктом дій конкурентів, що і обумовлює загострення питань захисту інформації від її незаконного використання і несанкціонованого доступу до неї.

З метою підвищення рівня ефективності управління інформаційною безпекою банківських установ необхідно визначити поняття та сутність інформаційної безпеки банків, проаналізувати актуальні загрози інформаційній безпеці в банківській сфері та обрати актуальні для банківської сфери методи та засоби захисту інформації.

У процесі розробки концепції управління інформаційною безпекою банківської установи варто виділити основні процеси функціонування банку і виключити можливість витоку інформації, її несанкціонованого використання, нанесення збитків, упущення вигоди з боку всіх зацікавлених сторін і в напрямі досягнення основних цілей банківської діяльності. Реалізація цих положень гармонійно вписується в концепцію корпоративного управління банківською діяльністю, до якої сьогодні залучаються дедалі більше банків.

Метою діяльності банку щодо забезпечення інформаційної безпеки є зниження загроз інформаційній безпеці до прийнятного для банку рівня. А головним критерієм ефективності та якості інформаційної безпеки банку є стійкість його фінансового та економічного розвитку згідно з планами і завданнями незалежно від зміни ситуації.

Література

1. Світлична В.Ю. Забезпечення інформаційної безпеки банківських установ. *Кримський економічний вісник*. 2014. №1 (08). Част. ІІ. С.172-175.
2. Ахрамович В.М. Кібербезпека банківських та комерційних структур: Навч. посібник Київ:ДУТ, 2019. 163 с.

АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Хімей О.І. - Державний університет телекомунікацій

Аудит інформаційної безпеки це незалежна оцінка поточного стану системи інформаційної безпеки, що встановлює рівень її відповідності певним критеріям і надання результатів у вигляді рекомендацій поточного стану захищеності інформаційної системи, що дозволяє систематизувати загрози ІБ і запропонувати рекомендації щодо їх усунення [1].

До основних завдань, що вирішуються в ході аудиту захищеності інформаційної системи можна віднести наступні:

аналіз структури, функцій, використовуваних технологій автоматизованої обробки і передачі інформації в інформаційній системі, аналіз бізнес-процесів, нормативно-розпорядчої та технічної документації;

виявлення значимих загроз інформаційній безпеці та шляхів їх реалізації, виявлення і ранжування за ступенем небезпеки існуючих вразливостей технологічного та організаційного характеру в інформаційній системі;

складання неформальної моделі порушника, застосування методики активного аудиту для перевірки можливості реалізації порушником виявлених загроз інформаційній безпеці;

проведення тесту на проникнення по зовнішньому периметру IP-адрес, перевірка можливості проникнення в інформаційну систему за допомогою методів соціальної інженерії;

аналіз та оцінка ризиків, пов'язаних із загрозами безпеці інформаційних ресурсів;

оцінка системи управління інформаційною безпекою на відповідність вимогам стандарту ДСТУ ISO/IEC 27001-2006, ISO/IEC 27006-2011, та розробка рекомендацій щодо вдосконалення системи управління інформаційною безпекою;

розробка пропозицій та рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів забезпечення інформаційної безпеки.

Аудит інформаційної безпеки складається з наступних етапів [2]:

ініціювання робіт і планування;

обстеження та збір інформації;

пошук вразливостей і невідповідностей;

вироблення рекомендацій та підготовка звітних документів.

Результатом аудиту інформаційної безпеки є створення документа, який містить детальну інформацію про:

усіх виявлених вразливостей об'єкта аудиту;

критичні знайдені вразливості;

наслідок у разі реалізації загроз;

рекомендації щодо усунення вразливостей.

На підставі результатів аудиту інформаційної безпеки підприємство зможе побудувати систему безпеки, мінімізувати можливі ризики інформаційної безпеки, а також підвищити свій авторитет в очах партнерів і клієнтів.

Аудит інформаційної безпеки дозволить керівництву підприємства або організації побачити реальний стан інформаційних активів і оцінити їх захищеність.

Література

1. А.П. Курило Аудит информационной безопасности. — 2006.
2. Власова Л.А. Защита информации. – 2007.

ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ

Попов В.С. - Державний університет телекомунікацій

Сучасними тенденціями розвитку інформаційних технологій є яскраво виражений перехід у бік створення корпоративних інформаційних систем. При цьому основною характеристикою цих систем є розмежування доступу співробітникам корпорації до інформаційних і інших ресурсів обчислювальної системи. Причому дані тенденції виявляються практично для всіх рівнів ієрархії сучасних інформаційних технологій, починаючи з архітектурного рівня в цілому (Internet і Intranet), включаючи мережеві технології (наприклад, IP v.4.0 і IP Sec), і закінчуючи рівнем загальносистемних засобів (ОС, СУБД) та прикладних програм: текстові редактори і текстові процеси, електронні таблиці, бази даних, графічні пакети, системи штучного інтелекту й експертні системи, навчальні програми системи мультимедіа, комп'ютерні ігри та розваги [1].

Масштаби застосування інформаційних технологій стали такі, що поряд із проблемами продуктивності, надійності і стійкості функціонування інформаційних систем, гостро постає проблема захисту. Інший аспект наведеної статистики - це можливість локалізації загроз корпоративної інформації, так як більша їх частина пов'язана з загрозою несанкціонованого доступу (НСД), що виходить від самих співробітників компанії. При цьому слід враховувати і мережеві ресурси, до яких співробітник має доступ зі свого комп'ютера в рамках своєї службової діяльності. У зв'язку з цим саме комп'ютер (особливо що знаходиться в складі мережі) слід в першу чергу розглядати як об'єкт захисту, а кінцевого користувача - в якості її найбільш ймовірного потенційного порушника. Як наслідок, під сумнів ставиться обгрунтованість концепції реалізованої системи захисту в сучасних універсальних ОС. Ця система захисту полягає в побудові розподіленої схеми адміністрування механізмів захисту, елементами якої, крім адміністратора, виступають користувачі, які мають можливість призначати і змінювати права доступу до створених ними файловим об'єктам [2].

На практиці сьогодні існує два підходи до забезпечення комп'ютерної безпеки:

використання тільки вбудованих в ОС засобів захисту;

застосування, поряд з вбудованими, додаткових механізмів захисту. Цей підхід полягає у використанні так званих технічних засобів додаткового захисту - програмних, або програмно-апаратних комплексів, що встановлюються на захищені об'єкти.

Існуюча статистика помилок, виявлених в ОС, а також відомості про недостатню ефективність вбудованих в ОС механізмів захисту, змушує фахівців сумніватися в досягненні гарантованого захисту від НСД, при використанні вбудованих механізмів, і все більшу увагу приділяти засобам додаткової захисту інформації. Хороша система захисту - це свого роду "конструктор", в якому закладені механізми протидії як явним, так і прихованим загрозам інформаційної безпеки. Щоб досягти необхідного рівня безпеки об'єктів, що захищаються, адміністратор повинен не тільки знати і розуміти можливості механізмів захисту, а й уміло їх налаштовувати, стосовно до безперервних загроз.

Найважливішою умовою захищеності комп'ютерної інформації є кваліфікація адміністраторів безпеки і співробітників експлуатуючих служб, яка, принаймні, не повинна поступатися кваліфікації зловмисників. В іншому випадку не допоможуть ніякі засоби захисту (те ж, до речі кажучи, відноситься і до розробників засобів захисту і захищених інформаційних систем).

Література

1. Ізбачков Ю. С., Петров В. Н. «Інформаційні системи: Підручник для вузів. – 2006.
2. Горбунов А., Чуменко В., Вибір раціональної структури засобів захисту інформації в АСУ.

Режим доступу: http://kiev-security.org.ua.

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПРИ РЕАЛІЗАЦІЇ ТА ВИКОРИСТАННІ МОБІЛЬНИХ БІЗНЕС-РІШЕНЬ НА ПІДПРИЄМСТВІ

Крівєнкова Г.М. - Державний університет телекомунікацій

На даний час організація режиму інформаційної безпеки стає критично важливим стратегічним чинником розвитку будь-якої компанії. При цьому, як правило, основна увага приділяється вимогам і рекомендаціям відповідної нормативно-методичної бази в галузі захисту інформації. Разом з тим багато провідних компаній сьогодні використовують деякі додаткові ініціативи, спрямовані на забезпечення стійкості і стабільності функціонування корпоративних інформаційних систем для підтримки безперервності бізнесу в цілому.

Однією з таких ініціатив є використання мобільних пристроїв для ведення бізнесу. На даний час мобільні пристрої стали поширеним засобом доступу до інформації, додатків та ведення бізнесу, в той же час створюючи нові можливості загроз.

До головних загроз для мобільних пристроїв можна віднести:

а) Атаки через Web-додатки та мережі.

б) Шкідливе ПЗ.

в) Атаки з використанням соціальної інженерії. Іншими словами, фішинг або прицільні атаки - являють собою психологічні прийоми з метою обману користувачів. Вони змушують користувача розкрити секретну інформацію або встановити зловмисне ПЗ.

г) Захоплення IT-ресурсів.

д) Втрата даних.

е) Загрози цілісності даних.

є) Загроза «відмова в обслуговуванні».

ж) Порушення зв'язку внаслідок впливу природних або штучних ненавмисних перешкод, виходу з ладу апаратури зв'язку, перевантаження мережі та інших причин.

з) Навмисне порушення зв'язку, обумовлене застосуванням методів радіоелектронної протидії, викликають, блокування (глушіння) мобільних пристроїв.

и) Контроль місцезнаходження абонента.

і) Порушення безпеки мобільних транзакцій (m-транзакцій).

Аналіз загроз показав, що основною загрозою для мобільних пристроїв є шкідливе програмне забезпечення (ПЗ). Дослідження, проведене лабораторією G Data SecurityLabs, показує, що доля вірусів для смартфонів і планшетних комп'ютерів збільшилася на 140% у співвідношенні з загальною кількістю шкідливого ПЗ [1]. Також експерти відзначають особливу активність з боку крос-платформенних троянських програм, які на даний момент домінують на фоні інших загроз. Більшість з них були створені для розповсюдження спаму та іншої нелегальної діяльності, яку ведуть електронні шахраї. Збільшення частки подібних злочинів лише показує, що нелегальний ринок шкідливих програм знаходиться у своєму зеніті [2].

Література

1. Дослідження компанії IDC. – Режим доступу до ресурсу: http://www.idc.com/
2. Дослідження компанії G Data SecurityLabs. – Режим доступа к ресурсу: http://ru.gdatasoftware.com/security-labs

РОЗРОБКА ЗАХОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ОРГАНІЗАЦІЇ

Величенко Л.О. - Державний університет телекомунікацій

Сучасний рівень розвитку інформаційних технологій висуває на передній план нові вимоги зокрема до побудови систем захисту персональних даних та забезпечення інформаційної безпеки в організації.

З стрімким розвитком інформаційних технологій перед організаціями все гостріше постає проблема не тільки забезпечення надійного захисту інформації від несанкціонованого доступу загалом, але й створення ефективної системи захисту персональних даних (СЗПДн) зокрема.

Створення такої системи дозволило б реально і адекватно захистити ПДн в організації шляхом створення [1]:

юридично обґрунтованої внутрішньої документації, яка дозволяє розмежувати відповідальність між посадовими особами та виконавцями, які безпосередньо використовують ПДн в повсякденній діяльності;

процесів обробки, зберігання, передачі та знищення ПДн в організації і в ІС зокрема;

дієвих заходів захисту ПДн відповідно до ризиків в конкретній організації (або в ІС).

Модель системи захисту (і обробки) ПДн дозволить:

реалізувати процеси обробки та обміну ПДн з урахуванням особливостей бізнес-процесів конкретної організації;

розрахувати і впровадити достатні та адекватні ризикам заходи щодо захисту ПДн.

Етапи впровадження СЗПДн:

1) Інвентаризація та підготовчі дії до впровадження СЗПДн.

Вивчення стандартів (міжнародних, державних, галузевих) фахівцями ІБ;

Проведення інвентаризації всіх ПДн;

Інвентаризація баз ПДн.

2) Визначення поточного стану СЗПДн.

Визначення рівня зрілості організації в області ІБ;

Підвищення кваліфікації та перепідготовка фахівців в ІБ;

Підготовка звіту, щодо подальшого напрямку розвитку СЗПДн в організації.

3) Визначення заходів захисту ПДн.

Розробка регламентної документації.

Проектування майбутньої СЗПДн.

4) Впровадження СЗПДн.

Впровадження технічних засобів захисту інформації;

Ознайомлення персоналу з політикою ІБ та інструкціями щодо забезпечення ІБ.

Атестація системи (якщо потрібно).

Реєстрація баз у Держреєстрі.

Таким чином, створення СЗПДн в організації слід починати з підготовки внутрішньої нормативно-правової бази та ідентифікації баз ПДн та самих ПДн [2]. Метою побудови СЗПДн є запобігання або зниження шкоди через втрати внаслідок реалізації загроз ПДн та іншій цінній інформації організації, що захищається. Завдання СЗПДн полягають у своєчасному виявленні, усуненні загроз ПДн та створенні механізму та умов оперативного реагування на загрози безпеки в різних ситуаціях їх прояву.

Література

1. Зубок М.І.,Яременко С.М. Безпека банківської діяльності. - 2012.
2. В.А. Трайнёв, А.А. Федулов Информационная безопасность. - 2005.

РОЗРОБКА МЕТОДИКИ АНАЛІЗУ ТА ОЦІНКИ ЗАГРОЗ ЦЕНТРА ОБРОБКИ ДАНИХ

Величенко В.О. - Державний університет телекомунікацій

Система забезпечення інформаційної безпеки центру обробки даних (СЗІБ ЦОД) призначена для забезпечення заданого стану інформаційної безпеки системи ЦОД шляхом моніторингу інформаційної безпеки системи ЦОД і управління, як спеціальними, так і вбудованими в функціонал програмно [1]. СЗІБ ЦОД повинна забезпечувати виконання вимог щодо інформаційної безпеки для технічних і програмних засобів, на яких побудована сама система і для суміжних з нею систем.

Разом з тим в організаціях неодноразово виникали випадки втрати даних, викликані несанкціонованим доступом до ключової інформації. З метою ліквідації можливості загроз, що впливають на цілісність і захищеність даних, необхідно провести аналіз і розрахунки можливих загроз інформаційної безпеки ЦОД.

Для найбільш ефективного функціонування СЗІБ необхідно визначити наступні параметри:

системне програмне забезпечення;

базова платформа системи забезпечення інформаційної безпеки;

базова платформа центру управління системи забезпечення інформаційної безпеки.

Система забезпечення інформаційної безпеки повинна вирішувати такі завдання з метою протидії основним загрозам ІБ [2]:

управління доступом користувачів до ресурсів АІС;

захист даних, що передаються по каналах зв'язку;

реєстрацію, збір, зберігання, обробка і видача відомостей про всі події, що відбуваються в системі і мають відношення до її безпеки технічними засобами забезпечення інформаційної безпеки на кожному рівні системи ЦОД;

контроль роботи користувачів системи з боку адміністрації та оперативне оповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

забезпечення замкнутої середовища перевіреного програмного забезпечення з метою захисту від безконтрольного впровадження в систему потенційно небезпечних програм (в яких можуть міститися шкідливі закладки або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження і поширення комп'ютерних вірусів;

контроль і підтримку цілісності критичних ресурсів системи захисту; управління засобами захисту;

розробка моделі загроз інформаційній безпеці ЦОД.

У висновку, слід зазначити, що роботи зі створення СЗІБ повинні виконуватися відповідно до державних та міжнародних стандартів по проектній технології, яка включає в себе всі стадії життєвого циклу автоматизованої системи.

Література

1. Бичуяров Т.А. Безопасность корпоративных сетей. - 2008.
2. Ефимов П. Концепция обеспечения безопасности информационных технологий. - 2005 г.

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Зіновський Р.О. - Державний університет телекомунікацій

Інформаційна безпека, як і захист інформації, завдання комплексне, спрямована на забезпечення безпеки, що реалізується впровадженням системи безпеки. Проблема захисту інформації є багатоплановою і комплексною і охоплює ряд важливих завдань. Проблеми інформаційної безпеки постійно поглиблюються процесами проникнення в усі сфери

суспільства технічних засобів обробки і передачі даних і, насамперед, обчислювальних систем.

На сьогоднішній день сформульовано три базові принципи, які повинна забезпечувати інформаційна безпека: цілісність даних - захист від збоїв, що ведуть до втрати інформації, а також зашита від неавторизованого створення або знищення даних; конфіденційність інформації; доступність інформації для всіх авторизованих користувачів [1].

При розробці комп'ютерних систем, вихід з ладу або помилки в роботі яких можуть призвести до тяжких наслідків, питання комп'ютерної безпеки стають першочерговими. Відомо багато заходів, спрямованих на забезпечення комп'ютерної безпеки, основними серед них є технічні, організаційні і правові. Забезпечення безпеки інформації – дорога справа, і не тільки через витрати на закупівлю або установку засобів захисту, але також через те, що важко кваліфіковано визначити межі розумної безпеки та забезпечити відповідне підтримку системи в працездатному стані. Усі вищенаведені твердження зумовили вибір теми дослідження, а також вказують на її актуальність для надання практичних рекомендацій по удосконалення організаційно-технічного забезпечення захисту інформації на підприємстві.

Проведений аналіз існуючих методик (послідовностей) робіт зі створення системи захисту інформації дозволяє виділити наступні етапи [2]:

визначення інформаційних і технічних ресурсів, а також об'єктів інформаційної системи, що підлягають захисту;

виявлення повної множини потенційно можливих загроз і каналів витоку інформації;

проведення оцінки вразливості і ризиків інформації (ресурсів ІС) при наявній множині погроз і каналів витоку;

визначення вимог до системи захисту інформації;

здійснення вибору засобів захисту інформації і їхніх характеристик;

впровадження й організація використання обраних методів і засобів захисту.

здійснення контролю цілісності і керування системою захисту.

Тому на підприємстві необхідно створити службу інформаційної безпеки, яка включала б керівника, відділ програмно-апаратного захисту інформації, підрозділ конфіденційного діловодства, підрозділ інженерно-технічного захисту інформації.

Література

1. Богуш В. Інформаційна безпека держави. "МК-Прес", 2005.

2. Бурцева К. Підвищення рівня інформаційної безпеки за допомогою організаційних заходів на комерційних підприємствах. – Режим доступу: ir.nmu.org.ua/jspui/bitstream/123456789/1673/1/6.pdf.

СИСТЕМА КОНТРОЛЮ ЦІЛІСНОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Шилан А.О. - Державний університет телекомунікацій

Захист інформації є ключовим завданням в сучасних умовах взаємодії глобальних і корпоративних комп'ютерних мереж. У реальному світі багато уваги приділяється фізичній безпеці, а в світі електронного обміну інформацією необхідно піклуватися також про засоби захисту даних. Ускладнення методів і засобів організації машинної обробки, повсюдне використання глобальної мережі Інтернет призводить до того, що інформація стає все більш вразливою. Цьому сприяють такі чинники, як постійно зростаючі обсяги оброблюваних даних, накопичення і зберігання даних в обмежених місцях, постійне розширення кола користувачів, що мають доступ до ресурсів, програм і даних, недостатній рівень захисту апаратних і програмних засобів комп'ютерів і комунікаційних систем тощо.

Захист даних з допомогою шифрування - одне з можливих рішень проблеми безпеки.

Зашифровані дані стають доступними тільки тим, хто знає як їх розшифрувати, і тому викрадення зашифрованих даних не має сенсу для несанкціонованих користувачів [1].

На даний час криптографічні методи забезпечення конфіденційності і цілісності даних є найсучаснішими і найкращими методами. Задачі щодо розробки нових і вдосконалення існуючих криптографічних методів захисту інформації завжди будуть актуальними.

Незалежно від способу реалізації для сучасних криптографічних систем захисту сформульовані такі загальноприйняті вимоги [2]:

зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;

шифр повинен бути стійким навіть у разі, якщо порушнику відома досить велика кількість вихідних даних і відповідних їм зашифрованих даних;

незначна зміна ключа або вихідного тексту повинна приводити до істотної зміни виду зашифрованого тексту;

структурні елементи алгоритму шифрування повинні бути незмінними;

шифртекст не повинен значно перевищувати за обсягом вихідну інформацію;

додаткові біти, що вводяться в повідомлення в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

помилки, що виникають при шифруванні, не повинні призводити до спотворень і втрат інформації;

не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуються в процесі шифрування;

будь-який ключ з безлічі можливих повинен забезпечувати рівну крипостійкість (забезпечення лінійного (однорідного) простору ключів);

час шифрування не повинен бути великим;

вартість шифрування повинна бути узгоджена з вартістю шифруємої інформації.

Таким чином, закономірним є те, що у багатьох надійних системах комп'ютерної безпеки основним механізмом захисту даних від НСД є використання криптографічних алгоритмів. Нажаль, не всі вони забезпечують необхідну швидкість перетворення даних і майже всі мають ряд недоліків. Усе це разом із стрімким розвитком КТ може сприяти проведенню все більшої кількості атак, а як наслідок – можливого їх злому. Не дивлячись на різноманіття існуючих криптографічних алгоритмів, дослідження, спрямовані на розробку нових та удосконалення вже існуючих, ніколи не втратять своєї актуальності.

Література

1. С.Г. Баричев, Р.Е. Серов, Основы современной криптографии: Учеб. пособие. - М.: Горячая линия - Телеком, 2002.

2. Лапонина О.Р. Криптографические основы безопасности. — М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2004.

ЗАСТОСУВАННЯ БІОМЕТРИЧНИХ МЕТОДІВ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ НА ОБ’ЄКТ

Корнієнко В.А. - Державний університет телекомунікацій

Рано чи пізно, на будь-якому сучасному підприємстві виникає проблема обмеження доступу сторонніх осіб на територію підприємства або в приміщення. У будь-якому офісі є місця, куди не повинні заходити звичайні відвідувачі (бухгалтерія, склад та ін.) і будь-який керівник прагне контролювати дисципліну співробітників і їх доступ в кабінети і приміщення підприємства або офісу.

В наш час будь-яка організація, що має в своєму розпорядженні конфіденційну чи секретну інформацію, зобов’язана мати систему контролю доступу.

Системи контролю та управління доступом (СКУД) знаходять широке застосування у сфері забезпечення безпеки та зарекомендували себе як надійні, гнучкі і функціональні. У переліку розроблених різними компаніями продуктів для системи контролю управління доступом містяться контролери з централізованою архітектурою, аналогові і цифрові панелі охоронної сигналізації, релейні модулі, зчитувачі і проміжні блоки з власною пам'яттю і вбудованою логікою, здатні працювати автономно, цифрові і аналогові інтерфейси управління кінцевими пристроями і ін. З допомогою контролера система може управляти різними виконавчими пристроями (електромеханічний замок, турнікет, автоматичні ворота та ін.) [1].

Устаткування систем контролю і управління доступом ділиться на автономні і мережеві системи. Автономні системи контролю доступу мають зчитувачі того або іншого типу, або клавіатуру для набору коду і контролер, що пам'ятає легальні коди та керує замком або іншим виконавчим механізмом.

Мережеві системи контролю доступу включають декілька зчитувачів і один або декілька контролерів. З використанням додаткових інтерфейсних модулів можливе підключення будь-яких зчитувачів.

Крім вирішення питань контролю доступу, система здійснює облік робочого часу співробітників, що приводить до підвищення трудової дисципліни і мотивації персоналу. Існують також автономні системи контролю доступу з накопиченням інформації про всі переміщення через точку контролю (двері, шлагбаум, турнікет) - час, дата, ідентифікаційний номер Proximity- або smart- карти або брелка Touch Memory. Вся інформація зберігається в пам'яті контролера [2]. СКУД дозволяє автоматично контролювати вхід людей в будівлю або приміщення і вихід з нього, а також в'їзд автотранспорту на територію і виїзд. Таким чином, установка СКУД просто необхідна тим, хто приділяє належну увагу безпеці. Мережеві системи поєднують в собі функції контролю і управління доступом і охоронної сигналізації, що дозволяє забезпечити комплексний захист об'єкту без використання додаткових засобів.

СКУД дозволить запобігти доступу небажаних осіб, а співробітникам точно вказати ті приміщення, в які вони мають право доступу. Складніша система дозволить, крім обмеження доступу, призначити кожному співробітникові індивідуальний часовий графік роботи, зберегти і потім проглянути інформацію про події за день. Системи можуть працювати в автономному режимі і під управлінням комп'ютера. СКУД дозволить створити системи контролю доступу будь-якої складності з можливістю контролю і управління проходу співробітників в різні приміщення.

Література

1. Ушмаєв О.С. Реалізація біометричної системи в правоохоронних системах, 2007.
2. Biometric terminals add security to a variety of processes [Електронний ресурс] – Режим доступу до ресурсу: www.bioscrypt.com.

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Сколота В.В. - Державний університет телекомунікацій

Сучасними тенденціями розвитку інформаційних технологій є яскраво виражений перехід у бік створення корпоративних інформаційних систем. При цьому основною характеристикою цих систем є розмежування доступу співробітникам корпорації до інформаційних і інших ресурсів обчислювальної системи. Причому дані тенденції виявляються практично для всіх рівнів ієрархії сучасних інформаційних технологій, починаючи з архітектурного рівня в цілому (Internet і Intranet), включаючи мережеві технології (наприклад, IP v.4.0 і IP Sec), і закінчуючи рівнем загальносистемних засобів (ОС, СУБД) та прикладних програм: текстові редактори і текстові процеси, електронні таблиці, бази даних, графічні

пакети, системи штучного інтелекту й експертні системи, навчальні програми системи мультимедіа, комп’ютерні ігри та розваги [1].

Масштаби застосування інформаційних технологій стали такі, що поряд із проблемами продуктивності, надійності і стійкості функціонування інформаційних систем, гостро постає проблема захисту. Інший аспект наведеної статистики - це можливість локалізації загроз корпоративної інформації, так як більша їх частина пов'язана з загрозою несанкціонованого доступу (НСД), що виходить від самих співробітників компанії. При цьому слід враховувати і мережеві ресурси, до яких співробітник має доступ зі свого комп'ютера в рамках своєї службової діяльності. У зв'язку з цим саме комп'ютер (особливо що знаходиться в складі мережі) слід в першу чергу розглядати як об'єкт захисту, а кінцевого користувача - в якості її найбільш ймовірного потенційного порушника. Як наслідок, під сумнів ставиться обгрунтованість концепції реалізованої системи захисту в сучасних універсальних ОС. Ця система захисту полягає в побудові розподіленої схеми адміністрування механізмів захисту, елементами якої, крім адміністратора, виступають користувачі, які мають можливість призначати і змінювати права доступу до створених ними файловим об'єктам.

Для запобігання проникнення зловмисника до інформації застосовують різні методи захисту, в тому числі, регулювання використання всіх інформаційних ресурсів, проведення заходів з виявлення каналів витоку, фізичний пошук, візуальній огляд та інше.

Крім того, технології застосування кодів і розмежування доступу до ресурсів в сучасних умовах переслідують мету захисту інформації, скорочення трудовитрат і забезпечення швидкої обробки, економії комп’ютерної пам’яті.

Наслідком зростаючого останнім часом значення інформації стали високі вимоги до конфіденційності даних. Система управління базами даних, особливо реляційні, стали домінуючим інструментом цій області [2]. Забезпечення інформаційної безпеки СУБД набуває вирішального значення при виборі конкретного засобу забезпечення необхідного рівня безпеки організації в цілому.

Література

1. Ізбачков Ю. С., Петров В. Н. «Інформаційні системи: Підручник для Вузів, 2» / Ю. С. Ізбачков, В. Н. Петров. - Вид. СПб.: Питер, 2006

2. Кузнєцов С. Д. «Основи баз даних.» - 2-е вид / С. Д. Кузнєцов. - М.: Інтернет-Університет ІТ; Біном. Лабораторія знань, 2007.

ТЕХНОЛОГІЇ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

Легомінова С.В., д.е.н., доц., Ільченко О. О. – Державний університет телекомунікацій

Процес успішного функціонування підприємства залежить від прийняття якісних і своєчасних управлінських рішень, які формуються на основі ретельного та всебічного аналізу інформації, що надходить як з внутрішнього, так і з зовнішнього середовища, а також від технологій управління.

До визначення технології управління різні автори мають свою точку зору, що відображено в табл.1.

Таблиця 1

Підходи до визначення сутності технології управління

Автори	Визначення
Б.Ш. Рапопорт [1]	Технологія управління як процес - це механізм,

	структура і послідовність взаємодії в часі і просторі людей за допомогою документів і технічних засобів при перетворенні інформації з метою управління діяльністю. Технологія управління як наука - це вчення про закономірності побудови раціональних технологічних процесів управління. Технологія управління як документ - це зафіксоване на будь-якому носії опис процесів управління
В.Ф. Комаров [2]	Способи практичного застосування сучасних наукових методів і засобів прийняття рішень
В.К. Скляренко, О.І. Волков [3]	Набір засобів і методів здійснення управлінських дій, що включає методи і засоби збору та обробки інформації, прийоми ефективного впливу на працівників, принципи, закони і закономірності організації і управління, системи контролю
Р.М. Грант [4]	Здібності компанії зі створення принципів і моделей взаємодії між працівниками, а також між працівниками та іншими ресурсами.
Ракша Н. В.[5, с. 86]	певний порядок здійснення процесу управління, який обумовлює послідовність та умови прийняття управлінських рішень і визначає найефективніші методи та інструменти їх впровадження на практиці.
Економічна енциклопедія [6, с. 627]	поєднання, послідовність, взаємозв'язок організаційних, інформаційних, розрахунково-обчислювальних та інших операцій і процедур у процесі здійснення управлінських функцій.
Василенко В. О. [7]	комплекс послідовно здійснюваних заходів попередження, профілактики, подолання кризи, зниження рівня її негативних наслідкі.
Смирнов Э. А. [8]	послідовність виконання управлінських функцій (планування, організації, мотивації, контролю), методів і процесів управління з метою оптимізації управлінського впливу для досягнення загальних та конкретних цілей організації.
Соболев В. Г. [9]	сукупність методів, прийомів, засобів, способів, інструментів, застосування яких повинно забезпечувати очікуваний результат.
Семенчук А. О. [10, с. 141]	інструмент, який є найбільш ефективним за обставин, що вимагають масштабних змін, які забезпечать ефективне використання ресурсів (сировинних, трудових, матеріальних) і покращення показників виробничо-господарської діяльності підприємства.

За приведеними прикладами можна зазначити, що технології управління відрізняються одна від одної в залежності від підходів застосування та мети використання, а

саме: чи це процес, чи послідовність дій, чи інструмент, засіб або метод використання, операція чи процедура.

Сучасні чинники, що визначають доцільність технологізації управління:

- поява нових виробничих технологій і скорочення життєвого циклу продуктів;
- інформатизація різних сфер діяльності;
- глобалізація, що проявляється в ускладненні умов конкуренції і зростаючої економічної взаємозалежності країн та територій;
- ускладнення зв'язків між організаціями;
- необхідність пристосування продукту до споживача.

Одним з ключових чинників успішності технологій управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC 27001.

Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

Система управління інформаційною безпекою забезпечує вибір адекватних і пропорційних методів і засобів контролю та захисту інформації тим самим, довіру зацікавлених сторін. Проте слід брати увагу також на інші стандарти у сфері інформаційної безпеки. На даний момент у світовій практиці використовується велика кількість стандартів, методик та інших документів, що регламентують процеси управління інформаційною безпекою, наприклад ISM3, COBIT, ITIL / ITSM, BSI-100-2, ISO13335-4, CRAMM, ISO15408. Але варто звернути увагу, що всі вони сумісні з ISO 27001, а також подібні до нього.

Література

1. Рапопорт В.Ш. Диагностика управления: Практический опыт и рекомендации. Москва: Экономика, 1988. 127 с.
2. Комаров В.Ф. Управленческие имитационные игры. Новосибирск: Наука. Сиб. отделение, 1989. 272 с.
3. Экономика фирмы: Словарь-справочник / Н.Б. Акуленко [и др.]; под ред. В.К. Скляренко, О.И. Волкова. Москва: ИНФРА-М, 2000. 398 с.
4. Грант Р.М. Ресурсная теория конкурентных преимуществ: практические выводы для формулирования стратегии. *Вестник СПбГУ*. 2003. Сер. 8, вып. 3. С. 47–75.
5. Ракша Н. В. Роль інноваційних технологій в управлінні підприємством. *Інноваційна економіка*. 2012. № 9 (35). С. 86–89.
6. Економічна енциклопедія : у трьох томах. Т. 3 / ред. кол. С. В. Мочерний (відп. ред.) та ін. Київ: Видавничий центр "Академія", 2002. – 952 с.
7. Василенко В. О. Антикризове управління підприємством. Київ: ЦУЛ, 2003. –503 с.
8. Смирнов Э. А. Управленческие технологии как объект функционального аудита. URL: http://www.cfin.ru/press/management /1998-6/10.shtml.
9. Соболев В. Г. Технологии эффективного управления персоналом. *Управління розвитком*. 2011. № 21 (118). С. 162–164.
10. Семенчук А. О. Реконверсійна технологія управління конкурентними перевагами підприємства. *Актуальні проблеми економіки*. 2010. № 4 (106). С. 138–143.
11. ISO 27001.URL: (https://ua.ikmj.com/isms/)

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ВІДПОВІДНО ДО СТАНДАРТУ ISO 27002

Мужанова Т. М., к.держ.упр., Стегнієнко А. Д. –
Державний університет телекомунікацій

З розвитком інформаційної сфери захист інформації стає одним з найголовніших питань на підприємстві. Відсутність або слабка організація інформаційної безпеки дають зловмисникам можливості нанести велику шкоду інформаційним ресурсам та інфраструктурі компанії. Тому актуальним питанням є вироблення і застосування методики організації захисту інформації підприємства.

У цьому контексті важливу роль відіграє стандарт ISO 27002 «Звіт практик для управління інформаційною безпекою» [2], який, на відміну від інших стандартів серії ISO/IEC 27000, не містить детальних консультацій або вимог до різних аспектів загального процесу управління інформаційною безпекою, а дає настанови стосовно широкого діапазону заходів інформаційної безпеки, які використовує велика кількість різних організацій.

Стандарт ISO 27002 містить перелік заходів і засобів управління інформаційною безпекою, які обираються на основі оцінки ризиків. Ці заходи наведені не у вигляді вимог, а подані разом з детальним поясненням передового досвіду їх застосування.

Даний стандарт розроблено для використання організаціями, які мають на меті:

a) визначити заходи безпеки в межах процесу впровадження СУІБ на основі ISO/IEC 27001 [1];

b) впровадити загальноприйняті заходи інформаційної безпеки;

c) розробити власні настанови щодо управління інформаційною безпекою.

Стандарт ISO 27002 містить 14 розділів заходів безпеки, серед яких розробка політики інформаційної безпеки, управління активами, робота з персоналом, безпека операцій та мереж, контроль доступу, фізична безпека, управління ризиками та інцидентами, аудит інформаційної безпеки та інші. Розділи загалом охоплюють 35 основних категорій безпеки та 114 заходів безпеки. Кожний розділ, який визначає заходи безпеки, містить одну чи більшу кількість основних категорій безпеки.

Порядок розділів у стандарті не означає їх важливості. Залежно від обставин заходи безпеки будь-якого чи всіх розділів можуть бути важливими, тому кожна організація, яка застосовує цей стандарт, повинна ідентифікувати заходи безпеки, які використовує, для розуміння їх важливості та необхідності їх застосування до конкретного бізнес-процесу.

Заходи безпеки можна вибирати з цього стандарту або інших наборів заходів безпеки, або, за потреби, можна спроектувати нові заходи безпеки для задоволення специфічних потреб. Вибір заходів безпеки залежить від управлінських рішень, основаних на критеріях прийняття ризиків, варіантах оброблення ризиків та загальному підході до управління ризиками, який застосовується в організації, а також він має відповідати всьому чинному національному й міжнародному законодавству та нормативним документам. Вибір заходів безпеки має також залежати від способу взаємодії цих заходів безпеки для забезпечення кращого захисту.

Таким чином, стандарт ISO 27002 є важливим для впровадження ефективної СУІБ підприємства, оскільки містить зібрання найкращих практик реалізації заходів безпеки. Подані в стандарті настанови стосуються широкого діапазону заходів інформаційної безпеки і можуть бути використані різними організаціями та підприємствами.

Література

1. ISO/IEC 27001:2013 [ISO/IEC 27001:2013] Information technology - Security techniques - Information security management systems – Requirements. 23 p.
2. ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management. 115 p.

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Романов М. В., Кавун А. В. - Державний університет телекомунікації

Розвиток кіберзагроз зростає с кожним днем. Тому варто міцно забезпечити захист інформаційної безпеки на підприємстві. Підприємства розширюються та розширюють як перелік послуг, так і масштабність інформаційно-телекомунікаційних систем. Зростає кількість загроз та вразливостей, з якими потрібно взаємодіяти.

Сьогодні кожне підприємство повинно визначити, які механізми захисту варто впровадити в організацію його інформаційної безпеки для того, щоб максимально знизити ризики збитку та витоку інформацію з підприємства. Це дуже важливо в наш час, тому що може привезти до багатомільйонних збитків і до величезних катастроф. Наприклад до знеструмлення міста або припинення банківських послуг. Тому важливо своєчасно створити комплексну систему захисту інформації та регулярно підтримувати і розвивати від нових загроз.

Організовуючи захист інформаційної безпеки на підприємстві, варто пам’ятати, що основні загрози йдуть через мережу та фізичний доступ.

Для забезпечення захисту мережі необхідно:

а) мережа локальна – забезпечити потік інформації на підприємстві тим співробітникам, яким вона необхідна та які мають до неї доступ, та надати захист цій інформації такими атрибутами як “читання”, “зміна” або “видалення”;

б) мережа зовнішня – встановити файрвол, та його надійно налаштувати; закрити уразливі та підозрілі порти; регулярно оновлювати налаштування файрвола та аналізувати потік трафіку (куди він рухається та в якому об’ємі).

Для забезпечення захисту фізичного доступу необхідно:

а) встановити антивірусну програму на всі комп’ютери підприємства (можна встановити також більш функціональні програми-антивируси – “доктор”, “ревізор” або “сторож”);

б) захистити жорсткі диски шифрування – обрати програму з відкритим початковим кодом, обрати типи шифрування такі як на стрічку та на контейнер (залежно від мети), захиститись від природних явищ таких як повінь, падіння, перенапруження тощо;

в) налаштувати політику безпеки операційної системи яка зможе - виконувати такі “функції реєстрація й облік (аудит)”, “розмежування доступу”, “контроль навантаження системи”, “ідентифікація й автентифікація”, “резервне копіювання”, “криптографічні функції”

При застосування відповідних механізмів захисту рівень забезпечення інформаційної безпеки на підприємстві зростає, що знижує ризик одержання збитків та витоку інформації.

Література

1. В.Г. Олифер, Н.А. Олифер. Компьютерные сети, принципы, технологии, протоколы 2-е издание. СПБ. 2006. 816 с.

2. Владимир Шаньгин. Информационная безопасность и защита информации. ДМК Пресс 2016. 173с.

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ДОДАТКАХ ДЛЯ МОБІЛЬНИХ СИСТЕМ

Лаврік Д.Ю. –Державний університет телекомунікацій

Мобільні телефони в сучасному світі є не просто засобом зв'язку, а пристроєм, який містить вразливі персональні дані, несанкціонований доступ до яких може привести до непередбачуваних результатів.

Відповідно до останніх даних дослідницької компанії eMarketer [1], що спеціалізується на аналізі ринку високих технологій, смартфонами вже користується чверть світового населення. Це близько 2 млрд. людей. І тенденція зростання користувачів мобільних пристроїв продовжується. На рис. 1 представлена динаміка зростання числа користувачів смартфонів в період з 2015 по 2018 року з прогнозом на 2019-2020 р.

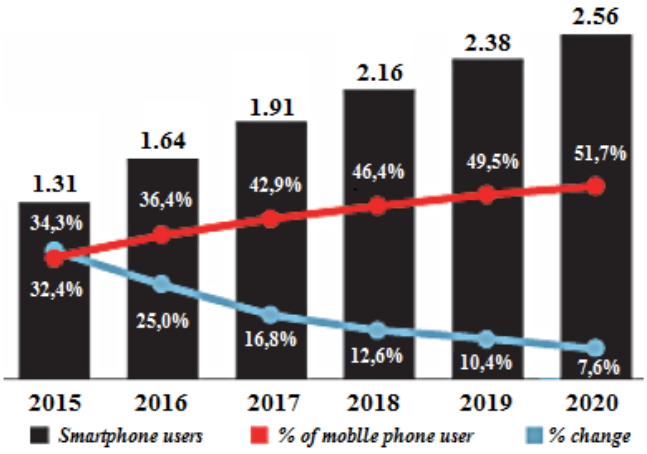

Рис.1 Динаміка зростання числа користувачів смартфонів

Мобільні телефони в сучасному світі є не просто засобом зв'язку, а пристроєм, який утримує вразливі персональні дані: номери кредитних карт, електронну пошту, геолокаційні відомості [2], профілі в соціальних мережах, засоби віддаленого доступу і управління підприємством, фотографії, видео і т. д. Несанкціонований доступ до таких чутливих даними може призвести до критичної ситуації. Тим часом, ринок мобільних додатків зростає з великою швидкістю, а користувачі особливо не замислюються про те, які дозволи вони надають додаткам, встановлюючи їх на свій смартфон, а також про наслідки, які можуть настати. Останній звіт компанії Digital Secuirty про дослідження додатків мобільного банкінгу показав, що всі вони містять, принаймні, одну уразливість, яка дозволяє або перехопити дані, що передаються між клієнтом і сервером, або безпосередньо експлуатувати уразливості пристрою і самого мобільного застосування [3].

Проблеми безпеки стосуються не тільки банківського сектора. Ігри на мобільних пристроях, безліч інших популярних додатків можуть бути потенційно небезпечними. Наприклад, популярний додаток «Відео у Watch», розміщене на майданчику Google Play і має досить високий рейтинг (4,5 з 5), а також понад 500 тисяч завантажень, зовсім викрадала ідентифікаційні дані користувачів, що призводило до втрати доступу до профілю в соціальній мережі.

Отже, що існує реальна необхідність оцінити поточний стан інформаційної безпеки найбільш поширених мобільних операційних систем, систематизувати основні загрози і уразливості мобільних додатків і скласти детальний підхід до розробки методики з оцінювання загроз інформаційній безпеці в додатках для мобільних систем.

Література

1. Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2016.
2. Михайлов Д. М. Исследование уязвимости мобильных устройств систем Apple и Google/ Д. М. Михайлов, А. В. Зуйков, И. Ю. Жуков и др. // Спецтехника и связь, 2017, № 6. С. 38-40.
3. Корниенко А. А. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте / А. А. Корниенко, С. Е. Ададуров, А. П. Глухов. М.: УМЦ ЖДТ, 2014. 440 с.

ОСНОВНІ ПІДХОДИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Новіков А.М. – Державний університет телекомунікацій

У сучасному суспільстві перед кожним підприємством постає питання про організацію системи захисту інформації, яка б дозволила у повній мірі забезпечити безпеку функціонування інформаційно-телекомунікаційної системи (ІТС). Ефективність захисту інформації залежить від підходу до її організації та правильного вибору методів оцінки ризиків інформаційної безпеки.

В даний час практично всі організацій в тій чи іншій мірі використовують як глобальні, так і локальні мережі. Уявімо, що компанія складається з великого числа підрозділів, які територіально розташовані на значних відстанях один від одного. Розташування окремих структурних підрозділів компанії може бути в межах як міста, країни так і всього світу. Для того щоб організація працювала як єдине ціле, всі її віддалені офіси повинні взаємодіяти між собою. На допомогу якраз і приходять інформаційно-телекомунікаційні системи.

З розвитком ІТС гостро постає проблема забезпечення інформаційної безпеки та технічного захисту інформаційних ресурсів в автоматизованих системах (АС). Одним з важливих організаційних заходів захисту інформації в АС є визначення переліку загроз інформації, які порушують її властивості – конфіденційність, цілісність та доступність. Перелік загроз, у свою чергу, пов'язаний з уразливістю таких систем. Ці два фундаментальні поняття лежать в основі теорії оцінювання ризиків як одного з найважливіших етапів побудови підсистеми захисту інформації [1].

Визначення терміну «інформаційна безпека» (ІБ) у більш вузькому значенні має характер процесу забезпечення конфіденційності, цілісності та доступності. Існує досить великий клас систем обробки інформації, під час розробці яких фактор безпеки відіграє першорядну роль (наприклад, енергетичні, банківські, інформаційні, медичні, економічні та лінгвістичні системи). Одним з важливих організаційних заходів захисту інформації в АС є визначення переліку загроз інформації, які порушують її властивості – конфіденційність, цілісність та доступність. Одна або декілька загроз можуть використовувати ряд уразливостей інформації. Будь-яка зміна загроз та уразливостей може мати значний вплив на ІБ. Раннє виявлення або знання про ці зміни збільшує можливості щодо прийняття необхідних заходів для обробки ризику та забезпечення безпеки ІТС у цілому. Це досягається за рахунок інструментальних методів визначення ризиків інформаційної безпеки в ІТС.

Відповідно до стандартів ISO/IEC 27005 та ISO/IEC TR 13335-2 оцінювання ризиків включає такі етапи [2, 3]:

1. Оцінку ймовірності можливих загроз і уразливостей.
2. Розрахунок ступеню впливу, який може мати загрозу на кожен актив.
3. Визначення кількісної (виміряної) або якісної (описуваної) вартості ризику.

Оцінювання ризиків полягає у визначенні кількісних та якісних показників, формуванні реєстру ризиків та ранжируванні ризиків.

Більш поширені способи оцінки інформаційних ризиків використовують змішані методи оцінки, які включають кількісні та якісні показники.

Як показує огляд інформаційних джерел, у галузі оцінки та управління інформаційними ризиками в ІТС на даний момент переважають інструментальні засоби їх оцінки такі, як CRAMM, Risk Watch, ГРИФ 2006, NIST, COBRA, OCTAVE.

Література

1. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз :монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 213 с.
2. Корнієнко Б. Я. Прикладні програми управління інформаційними ризиками / Б. Я. Корнієнко, Ю. О. Максімов, Н. М. Марутовська // Захист інформації. — К. : Науково-практичний журнал, 2012. — Вип. 4. — С. 60–64.
3. . Бучик С. С. Методика оцінювання інформаційних ризиків в автоматизованій системі / С. С. Бучик, С. В. Мельник // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем : зб. наук. праць. — Житомир: ЖВІ ДУТ, 2015. — Вип. 11. — С. 33–43.

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ІНТЕРНЕТ-БАНКІНГУ

Ляшок Б.О. - Державний університет телекомунікацій

Застосування сучасних досягнень інформаційних і телекомунікаційних технологій для надання банківських електронних послуг ставить підвищені вимоги до організації систем захисту банківської інформації [1]. Тому банкірам необхідно знати про найпоширеніші

можливі загрози для сучасних інформаційних систем та про уразливі місця, які ці загрози звичайно використовують, для того щоб обирати найекономічніші засоби забезпечення безпеки [2]. Незнання цього веде до перевитрати засобів і, що ще гірше, до концентрації ресурсів там, де вони не особливо потрібні.

Мережа VPN гарантує успішне ведення справ за допомогою Інтернет-технологій, тому клієнти і партнери банку можуть активно використовувати Інтернет у своїй діяльності, але вони мають розуміти особливості використання мережі VPN, яка може надати їм оперативну конфіденційну інформацію, даючи можливість швидко оформляти замовлення забезпечуючи повноцінну участь у спільних проектах.

Сучасні засоби захисту інформації, що передається через мережу, дають змогу ідентифікувати користувача, а також забезпечити достатній рівень безпеки даних. Однак відповідна вітчизняна і закордонна юридична база не має достатньої практики використання технології захисту інформації і поки що має декларативний характер.

Щодо суб'єктивних чинників категорію "інформаційна безпека" розглядають в Україні і за кордоном переважно відокремлено, в організаційно-управлінському та інженерно-технологічному аспектах, що не зовсім правильно і в майбутньому може спричинити неправильне формування державної політики.

Зазначені аспекти є важливими у системі організації захисту інформації, але без правового аспекту вони не можуть претендувати на системність і комплексність безпеки. Невідповідність чинного законодавства сучасним вимогам є однією з основних проблем розвитку законодавства щодо захисту інформації, що за наявності в нашій державі потужного науково-технічного потенціалу не може сприяти його ефективному використанню. Важливою складовою нормативно-правових засобів є морально-етичні аспекти захисту, які реалізують у вигляді різноманітних норм, що традиційно сформувалися в кожній державі або в суспільстві.

Література

1. Адамик Б.П., Литвин І.С., Ткачук В.О. Інформаційні технології у банківській сфері: Навч. посіб. – К.: Знання, 2008.

2. Олійник А.В., Шацька В.М. Інформаційні технології у фінансових установах: Навчальний посібник. – Львів: “Новий Світ-2000”, 2007.

ЗАГРОЗИ ІНФОРМАЦІЇ, ЯКІ ВИНИКАЮТЬ В ПРОЦЕСІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

Ільніцький А.Ю. - Державний університет телекомунікацій

Одне з основних завдань сучасної ділової діяльності полягає в тому, щоб забезпечити безпеку своїх інформаційних активів. Комерційні й технологічні секрети, конфіденційні документи, персональні дані персоналу й клієнтів організації - всю цю класифіковану інформацію необхідно захистити від самих різних загроз.

Найнебезпечнішою загрозою щодо цього є витік конфіденційної інформації. За останні роки актуальність цієї загрози зросла настільки, що сьогодні крадіжка класифікованих відомостей стабільно посідає перші місця у всіх рейтингах загроз IT-безпеки [1].

Всі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи:

загрози, обумовлені діями суб'єкта (антропогенні загрози);

загрози, обумовлені технічними засобами (техногенні загрози);

загрози, обумовлені стихійними джерелами.

Виходячи із даних антирейдерського союзу підприємців України:

82% загроз реалізується власними співробітниками фірми або при їх прямій чи опосередкованій участі;

17% загроз реалізується ззовні підприємства;

1% загроз реалізується випадково.

Найпоширеніші фактори розголошення співробітниками інформації з обмеженим доступом є [2]:

надмірна балакучість співробітників (32%);

прагнення співробітників заробляти гроші будь-якими способами та за будь-яку ціну (24%);

відсутність на фірмі служби безпеки(14%);

звичка співробітників фірми ділитися один з одним (традиційний обмін досвідом) (12%);

безконтрольне використання інформаційних систем (10%);

наявність можливостей виникнення серед співробітників конфліктних ситуацій: відсутність психологічної сумісності, випадковий підбір кадрів, відсутність роботи по згуртованості колективу і т.д. (8%).

Як видно, розголошення співробітниками інформації з обмеженим доступом найчастіше здійснюється через те, що керівництво компаній не приділяє уваги загрозам витоку інформації, пов'язаним з персоналом. Для кращого розуміння можливостей витоку інформації та визначення способів його попередження слід провести класифікацію самих порушників та класифікацію загроз, пов'язаних з ними.

Існує декілька різних класифікацій внутрішніх порушників, яких звикли називати інсайдерами. Інсайдерами є ті співробітники, що працюючи на підприємстві являються порушниками правил цього підприємства.

Створення служби захисту інформації підприємства дозволить зменшити виток інформації з використанням IT-технологій.

Література

1. Кукаркін О.Б. Електронний документообіг та захист інформації: навч. посіб. // – К.: НАДУ, 2015. – 84 с. http://academy.gov.ua/infpol/pages/dop/2/files/dcc74a43-a939-4314-8f50-f6b1e80cf498.pdf

2. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с. https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf

ВИМОГИ ЗАКОНОДАВСТВА ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Шак Д.О. - Державний університет телекомунікацій

Основи захисту інформації розробляються органами державної влади, виходячи з умов забезпечення інформаційної безпеки зокрема і національної безпеки України в цілому.

Відповідно до ст. 20, 21 Закону України «Про інформацію» [1], вся інформація за режимом доступу поділяється на відкриту та інформацію з обмеженим доступом (ІзОД).

ІзОД є конфіденційна, таємна та службова інформація [1]. Такий розподіл по режимах доступу здійснюється винятково на підставі ступеня конфіденційності інформації.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [1].

В умовах інформатизації країни, розвитку інформаційних технологій, інформаційні ресурси (сукупність документів у інформаційних системах) формуються у всіх сферах діяльності, і насамперед: в політичній, військовій, економічній, науково-технічній, тому інформаційну безпеку слід розглядати як комплексний показник національної безпеки. Цим визначається її важливе місце і одна з провідних ролей в системі національної безпеки країни в сучасних умовах [2].

Згідно із Законом України «Про захист персональних даних» об'єктами захисту є персональні дані, які обробляються в базах персональних даних. Персональні дані за режимом доступу є ІзОД [3]. Відповідно до ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» «Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством» [4].

Відповідно до вимог законодавства України [1-5], для забезпечення конфіденційності, доступності, цілісності та спостереженості зазначеної інформації в кожній автоматизованій системі має створюватися комплексна система захисту інформації.

Література

3. Закони України «Про інформацію». – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2657-12.

4. Концепція технічного захисту інформації в Україні № 1126 від 8.10.1997 р. – Із змінами, внесеними згідно з Постановою Кабінету Міністрів України № 938 від 07.09.2011. – (Серія видань «Законодавство України»).

5. Закони України «Про захист персональних даних». Режим доступу: http://zakon5.rada.gov.ua/laws/show/2297-17.

6. Закони України «Про захист інформації в інформаційно-телекомунікаційних системах». Режим доступу: http://zakon5.rada.gov.ua/laws/show/80/94-вр.

7. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

І. В. Мордас, к.е.н, доц., Я. В. Байда -Державний університет телекомунікацій

Захист інформації є одним з найновітніших і динамічно розвинених напрямів сучасної науки і техніки, що сформовані на базі наукоємних технологій. Питання захисту інформаційних ресурсів широко використовуються в різних галузях, скрізь, де потрібне зберігання й передавання інформації для різноманітних інформаційних систем суспільства. Це зумовлено досить високою комерційною вартістю інформації та постійно зростаючими обсягами інформаційних потоків, які необхідно передавати на великі відстані без втрати або спотворення корисної інформації.

У сучасних умовах інформаційної ери XXI ст. інформаційна безпека відіграє все більш вагому роль, а питання її забезпечення стають дедалі гострішими. Стрімке впровадження інформаційних технологій у всі сфери життєдіяльності суспільства та

розвиток економіки актуалізує питання визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки.

Інформація визначається як рушійна сила та домінуюча галузь, яка ставить собі за завдання впровадження провідних інформаційних технологій у всі сфери суспільної діяльності. Через те, що питання інформаційної безпеки посідає важливе місце у системі забезпечення безпеки як однієї окремо взятої країни, так і світу в цілому, дослідженням інформаційної безпеки займається ряд вітчизняних та закордонних дослідників, а також велика кількість державних та недержавних наукових установ, дослідницьких та аналітичних центрів (див. табл.1.)

Таблиця 1.

Сучасні підходи до трактування поняття «інформаційна безпека»

Вчений	Короткий зміст поняття
В. Богуш	Стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз [1].
В.А. Ліпкан, В.А. Авраменко	Стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації.
Р. Калюжний	Стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави.
Н.Р. Нижник, Я.М. Жарков, В.Т. Білоус	Стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни.
Б.А. Кормич	Захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [2].
О.І. Барановський	Стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій.

Отже, інформаційна безпека є однією з складових стійкого розвитку всієї держави, а процес забезпечення інформаційної безпеки необхідно розуміти як одне з глобальних і пріоритетних завдань державних органів, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

Разом з тим, варто визначити основний зміст, інструменти, завдання, порядок реалізації та нормативне регулювання інформаційної безпеки, які полягають у наступному:

1. Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері.

2. Інструментом реалізації державної політики інформаційної безпеки виступає система забезпечення інформаційної безпеки. Остання представляє собою організаційне поєднання заходів (інформаційного, адміністративного, управлінського, методологічного характеру), які спрямовані на забезпечення інформаційної безпеки особистості, суспільства та держави.

3. Завданнями системи забезпечення інформаційної безпеки є:

- моніторинг, прогнозування реалізації дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави;
- здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення;
- створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки;
- вдосконалення державної політики розвитку інформаційної сфери (створення сприятливих умов розвитку національної інформаційної інфраструктури, впровадження новітніх технологій у цій сфері);
- забезпечення інформаційно-аналітичного потенціалу країни.

4. Перелік функцій системи забезпечення інформаційної безпеки держави удосконалення нормативно-правового поля регулювання розвитку інформаційних ресурсів; оптимізація державної політики інформатизації; регулювання інформаційного співробітництва; контроль за встановленим порядком і правилами формування і використання інформаційних ресурсів.

Література

1. Богуш В. Інформаційна безпека держави / В. Богуш, О. Юдін. – К.: “МК-Прес”, 2005. – 432 с.
2. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник / Б.А. Кормич. – К.: Кондор, 2004. – 384 с.

СУТНІСТЬ МЕТОДУ АНАЛІЗУ СОЦІАЛЬНОЇ МЕРЕЖІ ПРОГРАМНОГО КОМПЛЕКСУ IBM I2 ANALYST'S NOTEBOOK

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

ТЕХНОЛОГІЯ УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ ESET SECURITY MANAGEMENT CENTER

Гахов С.О.
Спірін Родіон Олегович, БСДМ-71
Державний університет телекомунікацій,
м. Київ

Розглянуто зміст технології управління захистом кінцевих точок корпоративної інформаційної системи на базі ESET Security Management Center. Визначено мету і основні завдання щодо управління захистом кінцевих точок інформаційних систем підприємства. Розроблено рекомендації щодо управління захистом кінцевих точок корпоративної інформаційної системи.

В останній час спостерігається швидкий ріст числа руйнівних атак, таких як ransomware. Відбувається широке застосування безфайлових методів зараження шкідливим програмним забезпеченням комп'ютерів. Відмічається дефіцит навичок кібербезпеки у користувачів інформаційних систем та фахівців із кібербезпеки. Це тільки кілька проблем, які призвели до появи нових рішень щодо забезпечення безпеки кінцевих точок [1].

В останній час відбувся перехід від рішень безпеки кінцевих точок, керованих у локальній мережі (LAN-managed endpoint security solutions), до хмарних рішень. Продукти, що розгортаються та поставляються у хмарі, зменшують навантаження на обслуговування рішень EPP (Endpoint Protection Platform), зокрема, вирішується найважливіше завдання щодо їх оновлень. Однак не всі хмарні рішення в повній мірі використовують переваги сучасних хмарних архітектур для надання адаптивних та розширюваних рішень для протидії загрозам, які постійно змінюються.

Інтеграція можливостей виявлення та парирування загрозам під час захисту кінцевих точок відбувається шляхом реалізації множини функцій захисту одним агентом та консоллю. Рішення EDR (Endpoint Detection and Response) забезпечують видимість реакції на критичні інциденти, пошук, можливість "полювання на загрозу" та, що найголовніше, кращу здатність їх виявлення, яка базується на моделюванні поведінки, а не за допомогою тільки індикаторів компрометації.

Вимога щодо навичок застосування рішень EDR для більшості підприємств та організацій є перешкодою. В результаті вендори все частіше пропонують поєднання продуктів і послуг, починаючи від легкого реагування на інциденти і моніторингу і закінчуючи повністю керованими службами виявлення і реагування та консультативного реагування на інциденти.

Рішення EDR все більшою мірою забезпечують управління додатками і пристроями, управління вразливостями, конфігураціями та виправленнями. Широко використовуються портали співтовариства, де адміністратори та особи, які реагують на інциденти, можуть обмінюватися даними щодо проактивного виявлення (proactive detection) і реактивного "полювання на загрози" (reactive hunting) [1].

Вищенаведені аргументи актуалізують дослідження щодо управління захистом кінцевих точок корпоративної інформаційної системи на базі ESET Security Management Center. 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 [2].

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.

Для ефективного управління великими та середніми мережами (до 1000 клієнтів) зазвичай досить одного комп'ютера, на якому встановлений один сервер ESET Security Management Center (ESMC) з усіма компонентами (наданий веб-сервер, база даних тощо). Це можна сприймати як один сервер або автономний продукт. Всі керовані клієнти підключаються безпосередньо до сервера ESMC за допомогою агента ESET Management. Адміністратор може підключитися до веб-консолі ESMC в веб-браузері на будь-якому комп'ютері в мережі або запустити веб-консоль безпосередньо на сервері ESMC.

Щоб повністю розгорнути портфель рішень безпеки ESET, потрібно встановити наступні компоненти: ESMC Server (управляє обміном даними з клієнтськими комп'ютерами); веб-консоль ESMC (інтерфейс для сервера ESMC); агент ESET Management (розгортається на клієнтських комп'ютерах, обмінюється даними з сервером ESMC).

Таким чином, сучасні підходи базуються на комплексному захисті кінцевих точок 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. Sophos is a Leader in the Endpoint Protection Platform Magic Quadrant again [Електронний ресурс] – Режим доступу: https://www.gartner.com/technology/media-products/newsletters/sophos/1-671OHZP/gartner.html.
2. ESET Security Management Center. Guide for Small and Medium-sized Businesses [Електронний ресурс] – Режим доступу: https://download.eset.com/com/eset/apps/business/era/allinone/latest/eset_esmc_7_esmc_smb_enu.pdf.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Власенко В.О.
Філімонов Роман Олександрович, БСДМ-71
Державний університет телекомунікацій,

м. Київ

Розглянуто зміст технології забезпечення фізичного захисту інформації на об'єктах інформаційної діяльності. Визначено мету і основні завдання щодо забезпечення фізичного захисту інформації на об'єктах інформаційної діяльності підприємства. Розроблено рекомендації щодо застосування технології фізичного захисту інформації на об'єктах інформаційної діяльності.

У загальному комплексі заходів щодо забезпечення національної безпеки України в інформаційній сфері особливо важливе місце займає захист інформації, який безпосередньо призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в інформаційно-телекомунікаційних системах, циркулює на об'єктах інформаційної діяльності і становить державну та іншу передбачену законом таємницю, віднесена до конфіденційної інформації, вимога щодо захисту якої встановлена законом, або є відкритою і спрямованою на реалізацію законних прав та інтересів особи, суспільства, держави [1].

З урахуванням важливості захисту інформації для забезпечення національної безпеки в інформаційній сфері в Україні формування та розвиток державної системи захисту інформації, що призначена забезпечувати цілеспрямовану організацію і координацію діяльності в цій сфері. Як кожна організаційно-технічна система вона складається з трьох основних компонентів: нормативно-правової бази, організаційної інфраструктури та матеріально-технічної бази.

Інформація та інформаційні системи підприємств, мережеве оточення, у яких вони функціонують, є невід'ємними складовими сучасного бізнес-середовища. Їх доступність, цілісність і конфіденційність можуть мати вирішальне значення для забезпечення конкурентоспроможності підприємства, руху коштів, рентабельності, відповідності правовим нормам і стандартам. Водночас, унаслідок посилення залежності підприємств від інформаційних, комунікаційних систем і сервісів вони стають вразливішими до порушень режиму безпеки.

Поширення інформаційних і комунікаційних систем надає все нові можливості несанкціонованого доступу до інформаційних ресурсів, а тенденція переходу на розподілені обчислювальні системи обмежує можливості фахівців централізовано контролювати інформаційні системи та мережеве оточення.

Порушення режиму безпеки інформаційних систем може істотно ускладнити реалізацію виробничих завдань, тому вирішення проблеми формування ефективної системи захисту інформації набуває дуже важливого значення. Вимогою сьогодення є необхідність вирішення питань фізичної безпеки.

Захист інформації – це діяльність (процес), спрямована на запобігання витоку інформації, що захищається, проти несанкціонованих і ненавмисних дій порушників інформаційної безпеки на об'єктах інформаційної діяльності підприємства.

Водночас, фізичний захист інформації – захист інформації (процес) шляхом застосування організаційних заходів та сукупності засобів, що

створюють перешкоди для проникнення або доступу неуповноважених фізичних осіб до об’єкта захисту.

Організаційні заходи щодо забезпечення фізичного ЗІ передбачають встановлення режимних, тимчасових, територіальних, просторових обмежень на умови використання та розпорядок роботи об’єкта інформаційної діяльності підприємства.

Серед іншого, спосіб захисту інформації – це порядок і правила застосування певних принципів і засобів ЗІ. За цього застосовують засіб фізичного захисту – це такий засіб захисту інформації, який призначений чи використовується для забезпечення фізичного захисту об’єкта інформаційної діяльності підприємства.

Досягти результатів вирішення завдання фізичного захисту інформації на об’єкті інформаційної діяльності підприємства можна тільки завдяки системному підходу та комплексним різних методів та засобів даного виду захисту.

Література

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

ТЕХНОЛОГІЇ ТА МЕХАНІЗМИ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ

Ісаченко Анастасія Віталіївна, студент 125 кібербезпека
Державний університет телекомунікацій,
м.Київ

Безпека інформації має велике значення для забезпечення життєво-важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби. Однією з потенційних загроз для інформації слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.[1]

На сьогоднішній день рішення проблеми інформаційної безпеки вже розглядаються на державному рівні, що підтверджується нормативно-правовими і організаційними документами. Одним із важливих аспектів сучасного інформаційного простору є спеціальні цифрові носії інформації, що широко використовуються в наш час.[1][2]

Дослідження безпеки збереження інформації на цифрових носіях показує, що використання різних методів захисту не відповідає множині характерних сучасних загроз. Тому виникає необхідність проаналізувати та узагальнити можливі технічні рішення цього питання.

Вивчення питань захисту інформації з використанням цифрових носіїв визначається повсюдним поширенням комп'ютерних інформаційних, банківських, ідентифікаціфних, платіжних та інших видів систем, а також

окремих прикладних програм, які використовують інтелектуальні карти (ІК) як засіб зберігання і обробки персональних даних користувачів комп'ютерних систем.

Для виконання важливих дій, а саме контролю та управління державними чи приватними інформаційними ресурсами, використовується електронний документообіг. Вимогою такого методу управління є безпека та цілісність інформації що циркулює в інформаційній системі. Основним та найголовнішим завданням є забезпечення стійкості та унеможливлення компроментації, модефікації чи спотворення критично важливих даних . Методика безпечного зберігання даних повинна опиратися комплекс заходів, що спрямовані на унеможливлення розкриття інформації стороннім особам, а також бути здатною реалізувати своє функціонування не 4 тільки в повсякденних умовах, але і в критичних ситуаціях.[3]

Структура смарт-карток дуже відрізняється від своїх попередників, пластикових карток. Наявність мікропроцесора дозволяє виконувати різноманітні задачі, а наявність інтегральної мікросхеми збільшує захист від злому. Наявність мікропроцесора дозволяє організувати не тільки управління пам’яттю, але і захист деяких областей пам'яті.[4][5]

Програмування пам'яті смарт-карток здійснюється за допомогою спеціальних інструментальних пакетів, що включають транслятор текстів програм з мов високого рівня і асемблера в коди мікропроцесора смарт-картки, а також програмний емулятор мікропроцесорної системи смарт-картки для налагодження і тестування програмного забезпечення.[6]

Найбільш поширеними напрямами захисту смарт-карток вважаються таки:[7]

- захист від фізичного втручання;
- криптографічні механізми захисту;
- апаратно-програмовані засоби.

Жоден з методів захисту не може самостійно забезпечити максимальний захист, тому необхідно розглядати обґрунтовані комплексні рішення, що повіни скласти рекомендаційну основу для створення методики зменшення ризику втрати інформації на цифрових носіях.

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. *Пластиковые карты на интегральных микросхемах - стандартизованные технические условия для платёжных систем. EMV, 1994. - Перевод с англ. фирмы «Анкад», 2011.*
5. *Лубенская Т.В., Мартынова В.В., Скородумов Б.И. Безопасность информации в системах электронных платежей с пластиковыми карточками, 2015.*
6. *Абакумов В.Г. Методи захисту пластикових карт / В.Г. Абакумов, Л.В. Ратомська // Друга конференція молодих вчених «Електроніка – 2009»: збірник статей. – К., 2009. – Ч. 2. – С. 61-68.*
7. *Дичка І.А. Зберігання інформації у вигляді багатокольорових штрихових кодів та їх обробка / Дичка І.А. – К. : ІВЦ «Видавництво “Політехніка”»», 2003. – 340 с.*

НЕОБХІДНІСТЬ ЗАСТОСУВАННЯ ПРИВАТНИХ МЕРЕЖ У РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

Гайдур Г.І.
Турко С.О., БСЗМ-71
Державний університет телекомунікацій,
м.Київ

Постановка проблеми.

Сучасний розвиток інформаційних технологій і, зокрема, мережі Internet, приводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу. Віртуальні приватні мережі (VPN) - це технологія, яка поєднує довірені мережі, вузли й користувачів в єдину віртуальну мережу, що забезпечує конфіденційність і цілісність інформації, яка циркулює в ній.

Мета **матеріалу**.

Дослідження необхідності впровадження і використання технологій VPN в розподілених корпоративних мережах.

Основні матеріали дослідження *Корпоративна мережа(КМ)* **-** *взаємозалежна сукупність мереж, служб передачі даних і телеслужб, призначена для надання єдиного захищеного мережного простору обмеженому рамками корпорації колу користувачів.*

Основними особливостями КМ є:

1. Використання того ж інструментарію, що й при роботі з мережею передачі даних загального користування.

2. Доступ до інформації надається тільки обмеженій групі клієнтів у внутрішній мережі організації. Внутрішня мережа представляє із себе локальну мережу, відділену від глобальних мереж міжмережевими екранами (МЕ).

3. Циркуляція інформації трьох типів: офіційна (поширення якої офіційно санкціонується й заохочується на рівні організації), проектна або групова (призначена для використання окремою групою співробітників, як правило, підлягає захисту) і неофіційна (особиста папка або каталог на сервері, що слугують сховищем статей, заміток і ідей, з якими можна поділитися з іншими співробітниками підприємства в спільних інтересах для обміну зауваженнями або якихось інших цілей).[2]

4. Наявність централізованої системи керування корпоративною мережею.

КМ дозволяє ефективно об'єднати територіально розділені підрозділи компанії. Єдина мережа забезпечує широкий спектр можливостей:

- *охоплення всіх робочих місць підприємства в on-line режимі;*

- *віддалений доступ до ресурсів корпоративної мережі;*
- *доступ в Інтернет;*
- *розсилання великих обсягів даних по одному або багатьом адресам та ін. [1]*

Завдання створення комп'ютерної мережі підприємства в межах однієї будівлі може бути вирішується відносно легко і без значних затрат. Якщо ж інфраструктура корпорації включає в себе географічно розподілені підрозділи, то об'єднання їх в одну мережу є досить складним і затратним завданням. Використання технології VPN дозволяє *отримати дешеві, доступні і захищені канали.Так як при застосуванні* VPN *весь потік інформації, переданий по загальнодоступних мережах, шифрується.*

Розглянемо детальніше всі переваги використання VPN у розподілених корпоративних мережах .

1. ***Простота використання****.* Це програмне забезпечення, що легко встановлюється іне вимагає практично ніяких налаштувань, забезпечує безпеку як окремого комп'ютера в локальній мережі, так і локальної мережі в цілому.

2. ***Використання механізмів сповіщень і авторегістрації.*** При включенні в мережу VPN чергового мережного ресурсу механізми сповіщень і авторегістрації забезпечують миттєве налаштування всіх компонентів VPN.

3. ***Відсутність будь-яких обмежень на кількість одночасних з'єднань по VPN.*** Рішення ідеально працює одночасно і в локальній мережі, і при взаємодії із зовнішніми ресурсами. Відсутні будь-які обмеження на кількість одночасних з'єднань по VPN. Забезпечується підтримка стандартних служб імен (DNS, WINS).

4. ***Мобільність.*** Мобільний користувач може працювати при будь-яких переміщеннях, навіть якщо у нього на комп'ютері розміщені серверні служби (за рахунок підтримки технології динамічного DNS).

5. ***Простота підключення партнерів або клієнтів до своїх ресурсів.*** При підключенні партнерів або клієнтів до своїх ресурсів:

а. організується точкове їх підключення до заданого ресурсу по заданих протоколах з криптографічною аутентифікацією трафіку, не залежною від IPадреси джерела;

b. за рахунок формування кожним модулем VPN унікальних віртуальних адрес не потрібне узгодження адрес взаємодіючих мереж; система дозволяє об'єднувати
в VPN-вузли з однаковими IP-адресами.

6. ***Безперебійність роботи мережі VPN при наявності в мережах NAT-пристроїв.*** Присутні в мережях NAT-пристрої не порушують безперебійність роботи мережі VPN. Доступ до вузлів, що знаходяться за NAT-пристроями, можливий як шляхом налаштування правил пропуску UDP-пакетів по заданому порту, так і за рахунок спеціальних механізмів підтримки автоматично створюваних на NAT-пристрої динамічних правил.

7. ***Забезпечення проходження між собою прямого трафіку при будь-яких конфігураціях.*** Модулі VPN забезпечують проходження між собою прямого трафіку при будь-яких конфігураціях, без перешифрування на проміжних вузлах.

8. ***Менша вартість.*** За наявності каскадів подвійне шифрування трафіку і, відповідно, його подвійна інкапсуляція не проводяться, що виключає витрати, пов'язані з цим.

9. ***Підвищена надійність і безпека функціонування інформаційних систем.*** Використовування симетричної ключової структури і наявність системи автоматичного розподілу ключів значно підвищують надійність і безпеку функціонування інформаційних систем .

10. ***Можливість підтримки інфраструктури електронного цифрового підпису.*** В системі присутні всі необхідні рішення для підтримки інфраструктури електронного цифрового підпису.

Висновки. В роботі розглянуто та визначено переваги технологій VPN. Обґрунтовано необхідністі впровадження і використання технологій VPN в розподілених корпоративних мережах.

Список літератури

1. Биячуев Т.А. / под ред. Л.Г.Осовецкого. Безопасность корпоративных сетей. – СПб: СПб ГУ ИТМО,2004.- 161 с..

2. С. Браун. Виртуальные частные сети.. – Лори, 2001– 503 с

3. Запечников С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей — №10, 2003, 248 с.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети – 2006, 958 с.

5. Таненбаум Э. Компьютерные сети. – 2003, 992 с.

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Ісаєв Дмитро Олександрович, БСД-43
Державний університет телекомунікацій, м.Київ

Корпоративні інформаційні системи міцно увійшли в наше життя. У сучасному світі досить складно уявити собі підприємство, яке успішно розвивається і керується без участі такої системи. У зв'язку з тим, що в корпоративних інформаційних системах зберігається інформація, порушення цілісності або конфіденційності якої може привести до краху цілого підприємства гостро стоїть питання про захист інформації в корпоративних інформаційних системах. Причому мова йде не тільки про запобігання витоку корпоративної інформації, зниження обсягів паразитного трафіку і відбитті атак на ресурси компанії, але і про оптимізацію роботи системи в цілому. Захист систем даного типу має спиратися на аналізі основних можливих вразливостей.

Корпоративна інформаційна система являє собою складну структуру, в якій об'єднані різні сервіси, необхідні для функціонування компанії. Ця структура постійно змінюється – з'являються нові елементи, змінюється конфігурація існуючих. У міру зростання системи забезпечення інформаційної безпеки і захист критично важливих для бізнесу ресурсів стають все більш складним завданням. В даній роботі представлені результати проектів з аналізу захищеності корпоративних інформаційних систем.Вразливість визначається в стандарті ISO 27002 як «слабкість активу або групи активів, які можуть бути використані однією або кількома загрозами» [1].

Управління вразливістю – це процес, в якому знаходяться вразливості в IT виявлено та оцінено ризики цих вразливих місць. Ця оцінка призводить до виправлення вразливих місць та усунення ризику або офіційного прийняття ризику з боку управління організацією.

Термін управління вразливістю часто плутають із скануванням вразливості. Незважаючи на те, що обидва пов'язані між собою, між ними є важлива різниця. Сканування вразливості полягає у використанні комп'ютерної програми для виявлення вразливості в мережі, комп'ютерна інфраструктура або програми. Управління вразливістю – це обробляти сканування вразливості, також враховуючи інші аспекти, такі як прийняття ризику, усунення та ін.

Зростаюче зростання кіберзлочинності та пов'язані з цим ризики примушують найбільше організації приділяти більше уваги інформаційній безпеці. Вразливість процес управління повинен бути частиною зусиль організації з контролю інформації ризики для безпеки. Цей процес дозволить організації отримувати постійний огляд вразливості в їх IT-середовищі та пов'язані з ними ризики. Тільки виявити та пом'якшити вразливості в IT-середовищі може організація не допускати проникнення зловмисників у їхні мережі та крадіжки інформації [2].

Nessus забезпечує багато функціональності та можливостей в одному інструменті. Порівняно з іншими інструментами мережевого сканування, він досить зручний у користуванні, мав плагіни, які легко оновлювати, та має чудові інструменти звітування для верхнього управління. Використання цього інструменту та побачення вразливих місць допоможуть вам отримати знання про ваші системи, а також навчать їх захищати. Нові вразливості випускаються майже щодня, і для того, щоб забезпечити постійну безпеку ваших систем, вам доведеться їх регулярно сканувати. Майте на увазі, що пошук уразливостей, перш ніж хакери скористаються ними, – це перший перший крок у забезпеченні безпеки ваших систем.

Організації опиняються під тиском, змушених швидко реагувати на динамічно зростаючу кількість загроз кібербезпеки. Оскільки зловмисники використовують життєвий цикл нападу, організації також були змушені придумати життєвий цикл управління вразливістю. Життєвий цикл управління вразливістю призначений для швидкого протидії зусиллям, які докладаються зловмисниками. У цій роботі розглянуто життєвий цикл управління вразливістю з точки зору вразливості стратегія управління.

Він пройшов етапи створення запасів активів, управління потоком інформації, оцінка ризиків, оцінка вразливих ситуацій, звітність та усунення та, нарешті, планування відповідних заходів. Це пояснило важливість кожного кроку на етапі управління вразливістю та те, як слід їх виконувати. Інвентаризація активів була описана як важлива для стратегії, оскільки саме в ній перераховані всі подробиці про хости, щоб допомогти в ретельній санітарії всіх машин, які можуть мати вразливі місця. Важливою функцією кроку управління інформацією є швидке та надійне поширення інформації також було висвітлено, а також інструменти, які зазвичай використовуються для його досягнення [3].

Життєвий цикл кожної операційної системи починається при випуску продукту на ринок і закінчується, коли її підтримка припиняється. Знання основних дат життєвого циклу допомагає в прийнятті рішень про час установки нової версії або внесення інших змін до використовувані програми.

Типовий життєвий цикл для ОС сімейства Windows виглядає наступним чином:

- Випуск ОС.
- Основна підтримка (~ 5 років).
- Розширена підтримка (~ 5 років).
- Закінчення розширеної підтримки.

Строго кажучи, життєвий цикл, операційної системи не закінчується після закінчення розширеної підтримки - вона продовжить виконувати свої функції, в той же час ми настійно рекомендуємо відмовитися від використання

застарілих версій ОС і перейти на новішу версію, не чекаючи закінчення періоду розширеної підтримки.

Таким чином, реалізація методів та засобів захисту **корпоративної інформаційної системи на основі рішення Nessus Professional, забезпечить ефективний захист інформації та кібербезпеку корпоративної інформаційної системи підприємства** [4].

Література:

1) КОРПОРАТИВНІ ІНФОРМАЦІЙНІ СИСТЕМИ – Інформаційні технології автоматизації управління в масштабах корпорації. [Електронний ресурс] – Режим доступу до ресурсу: https://pidruchniki.com/74260/informatika/korporativni_informatsiyni_sistemi

2) Аналіз вразливостей корпоративних інформаційних систем. [Електронний ресурс] – Режим доступу до ресурсу: http://jrnl.nau.edu.ua/index.php/ZI/article/view/12453

3) Tenable – The Cyber Exposure Company. [Електронний ресурс] – Режим доступу: https://www.tenable.com/products/nessus/nessus-professional

4) Implementing a vulnerability management. [Електронний ресурс] – Режим доступу: https://www.sans.org/reading-room/whitepapers/threats/paper/34180

МЕТОДИКА ОЦІНКИ МЕХАНІЗМІВ ЗАХИСТУ ІНФОРМАЦІЇ НА СМАРТ-КАРТКАХ З ДВОФАКТОРНОЮ АВТЕНТИФІКАЦІЄЮ

Кузовенкова Ліна Олександрівна, БСЗМ-71
Державний університет
телекомунікацій,
м.Київ

У процесі розвитку суспільства різних країн поступово переходять від традиційних форм збереження цінних інформаційних даних (паперових документів суворої звітності) і цінних паперів (грошей, векселів) до їх електронних аналогів, коли вони повинні існувати як в паперовому, так і в електронному вигляді або до гібридних документів, наприклад, паперового чи пластикового паспорта, який містить біометричні дані та інші цифрові дані про людину на мікрочіпі, що вміщений у паспорт.

Важливою категорією існування як для людини так і для суспільства є безпека. Безпека – стан, при якому кому-небудь, чому-небудь не загрожує будь-що (небезпека, загрози будь-якого виду).

Однією з головних функцій будь-якої держави є забезпечення національної безпеки. Національна безпека – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам. Інформаційна безпека є складовою національної безпеки, яка визначена Конституцією України.[1]

На сьогоднішній день постала необхідність у перенесенні та використанні всіх цінних документів, паперів, грошей у електронний вигляд на спеціальні цифрові носії інформації. Повністю розкривається потенціал СЦН, якщо засоби їх зберігання мають можливість організації спеціального захищеного інтерфейсу роботи з СЦН, тобто мають певні обчислювальні можливості. Найбільш зручними портативними носіями СЦН є смарт- картки

(інтелектуальні пластикові картки з пам'яттю), токени, кишенькові комп'ютери (або близькі до них за функціональністю смартфони). В останній час як самостійні пристрої збереження СЦН можуть розглядатися засоби реалізації технології електронного паперу.

Ще зовсім нещодавно було маловідомим, незвичним явищем використання смарт-карток. Смарт-картки ширше і входять до найрізноманітніших сфер життя. Володіючи цілим рядом привабливих для користувачів властивостей, вони витісняють традиційні технології і знаходять все нові і нові області застосування.

Впровадження та використання технологій і методів захисту інформації на спеціальних інтелектуальних цифрових носіях, що містять інформацію, яка є основою для створення систем електронного документообігу, електронної торгівлі та електронного бізнесу (електронні гроші, електронні цінні папери), спеціалізовану інформацію для ідентифікації та автентифікації суб'єктів цих систем (наприклад, цифрові паспорти) та спеціальну службову інформацію, яка визначає захищену взаємодію з цим електронним документом.

Не менш важливим є захищеність цих смарт-карток неможливо створити смарт-картку, яку не можна буде взламати, питання стоїть тільки в тому скільки ресурсів буде витрачено. Використання криптографії значно підвищує захист інформації на смарт-картках. Найкращим методом захисту є двофакторна автентифікація, крадіжка інформації на якій потребує дуже великих ресурсів.[2]

Цю методику можна використовувати як на державних об’єктах для підвищення захисту інформації так і на цивільних підприємствах та при державних експертизах.

Література:

1. ДСТУ 4145-2002. Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка. Київ:-Держстандарт України, 2003.
2. Anderson R.J., The Formal Verification of a Payment System.

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ МОЖЛИВОСТЕЙ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Смолєв Євген Сергійович, БСД-43
Державний університет
телекомунікацій,
м.Київ

З кожним новим витоком даних або кібератакою складність навколо виявлення та реагування на загрози зростає, а тиск на спеціалістів кібербезпеки підприємств посилюється. Річ у тому, що виявлення загроз є складним, і згідно з недавнім опитуванням ESG Research 2019 року, цей процес стає лише важчим. Частково за підтримки Symantec, опитування ESG серед керівників кібербезпеки підприємств, виявило, що понад три чверті (76%) спеціалістів вважають, що виявлення загрози та реагування на інцидент сьогодні складніші, ніж це було лише два роки тому [1]. Проблема полягає в тому, що кібератаки продовжують зростати в обсязі та витонченості. Простіше кажучи, вони ніколи не закінчуються, і вони продовжують вдосконалюватися для збільшення своєї ефективності та ускладнення виявлення.

З метою розробити рекомендації щодо підвищення можливостей виявлення загроз корпоративній інформаційній системі були виконані наступні завдання: -досліджено зміст виявлення загроз корпоративній інформаційній системі; - проаналізовано зміст бази знань MITRE ATT&CK та визначено можливості її застосування; - досліджено можливості застосування SIEM-системи та програмного комплексу IBM QRadar Use Case Manager.

Загрози інформаційної (комп'ютерної) безпеки – це різні дії, які можуть привести до порушень стану захисту інформації. Іншими словами – це потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам. Основні джерела загроз – хакери, намагаються отримати доступ до систем організацій з метою крадіжки даних, коштів або виведення з ладу обладнання.

Превентивні заходи вже давно є сприятливим методом, щоб запобігти шкоди нанесеної організаціям кіберзлочинцями. Але наскільки ефективною не була б профілактика – цього вже недостатньо. Оскільки кіберзагрози швидко поширюються і стають складнішими, старих способів забезпечення кібербезпеки більше не вистачить. Хоча попереджувальний рівень все ще має важливе значення для зупинки більшості загроз, організації більше не можуть розраховувати лише на запобіжний шар – рішучий нападник знайде спосіб зламати навіть найбезпечнішу систему.

В останні пару років спеціалісти Positive Technoligies відзначали, що парадигма забезпечення інформаційної безпеки почала змінюватися і все більше компаній приходять до розуміння, що побудова захисту, яку не можна зламати – утопічно за своєю суттю. Левова частка систем або вже зламана, або може виявитися зламаною, і головне завдання будь-якої системи безпеки – максимально швидко виявити атаку та атакуючого в системі, скоротити вікно його можливостей настільки, щоб він не встиг завдати непоправної шкоди (тобто сьогодні мова йде про так звану ability to detect). У зв'язку з цим спостерігається зростання потреби високоінтелектуальних засобів захисту, що дозволяють вирішувати завдання по своєчасному виявленню атак і інцидентів. Зокрема, мова йде про системи класу security information and event management (SIEM), network traffic analysis (NTA), комплексні antiAPT рішення. За підсумками 2019 року спостерігалося майже триразове зростання інтересу до технологій такого типу [2].

SIEM є не лише потужним інструментом системи інформаційної безпеки, але й IT-системи в цілому. Системи даного класу дозволяють домогтися практично повної автоматизації процесу виявлення загроз, тим самим змістивши акцент уваги на критичні загрози, дозволяє працювати не з подіями, а з інцидентами, своєчасно виявляти аномалії та ризики, забезпечує безперервність роботи IT-сервісів шляхом грамотного налаштування кореляційних механізмів, що, в сукупності, дозволяє істотно скоротити можливі фінансові втрати.

Очевидно, що інструментарій даної системи дозволить істотно прискорити процес розбору інциденту, проте основним завданням SIEM є

своєчасне виявлення, оперативне реагування та запобігання загрозам. Для цього необхідно складання правил кореляції з урахуванням актуальних для компанії ризиків, а також постійна актуалізація самих правил фахівцями. Як і в випадку систем IDS, типова загроза буде реалізована, якщо не створити правило, що дозволяє цю загрозу виявити.

Однак, SIEM має перевагу перед системами виявлення вторгнень, яка полягає в можливості загального опису властивостей загроз і використанні накопиченої статистики для відстеження відхилення інформаційних систем і трафіку від нормальної поведінки. У найпростішому випадку в SIEM-системах правила представлені в форматі RBR Rule Based Reasoning і містять набір умов, тригери, лічильники, сценарій дій.

В цілому система класу SIEM здатна виявляти факти мережевих атак у внутрішньому і зовнішньому периметрах, вірусні епідемії або окремі зараження шкідливим програмним забезпеченням, спроби несанкціонованого доступу до конфіденційної інформації, шахрайство, а також визначати помилки і збої в роботі інформаційних систем, уразливості, помилки конфігурацій в засобах захисту та інформаційних системах.

Однак, слід уточнити, що SIEM, як і інші системи ІБ, не є панацеєю. Як мінімум з огляду на те, що впровадження даної системи є складним, дорогим і тривалим за часом проектом, а для її експлуатації необхідна наявність кваліфікованого фахівця, який забезпечить контроль безперервності збору подій, управління правилами кореляції, а також буде коригувати і оновлювати правила згідно із змінами в самій інфраструктурі. Установка SIEM в стані “як є”, з активацією вбудованих правил кореляції і обмеженого набору шаблонів, без належного управління та контролю, призведе до нераціональної витрати бюджетних коштів.

Що стосується виявлення та пом’якшення загроз, швидкість має вирішальне значення. Програми безпеки повинні бути в змозі швидко та ефективно виявляти загрози, щоб зловмисники не мали достатньо часу для отримання доступу до конфіденційних даних. Оборонні програми бізнесу в ідеалі можуть зупинити більшість загроз, тому що часто про них знали раніше – це означає, що вони повинні знати, як боротися з ними. Ці загрози вважаються “відомими” загрозами. Однак існують додаткові “невідомі” загрози, які організація прагне виявити. Це означає, що організація раніше не стикалася з ними, можливо, тому, що зловмисник використовує абсолютно нові методи або технології.

У арсеналі захисту є кілька методів, які допоможуть у виявленні загроз [3]: -розвідка; -аналіз поведінки користувачів і поведінки зловмисників; -встановлення пасток для зловмисників; -проведення пошуку загрози.

Успішне та всебічне виявлення загрози вимагає розуміння загальноприйнятих методів боротьби із супротивниками, які можуть особливо загрожувати організації. Зважаючи на це, обсяг та широта тактик нападу роблять майже неможливим моніторинг кожного типу атаки. Саме з цих причин MITRE розробила фреймворк ATT & CK.

Фреймворк ATT & CK широко визнане авторитетне джерело, що аналізує поведінку та методи, якими хакери сьогодні користуються проти організацій. Це не тільки усуває неоднозначність і забезпечує загальну лексику для професіоналів галузі для обговорення та співпраці щодо боротьби з цими протиборчими методами, але також має практичне застосування для команд із безпеки.

ATT & CK використовує 12 різних тактичних категорій для опису поведінки супротивника:
початковий доступ; виконання; закріплення в системі; ескалація привілеїв; ухилення від захисту; доступ до довірених даних; дослідження системи; бічне переміщення; збір даних; ексфільтрація; командування та управління; вплив.

Ці категорії індексуються і детально розбиваються на точні кроки та методи, якими користуються хакери, що полегшує командам розуміння дій, які можуть бути використані проти певної платформи. Щоб піти на крок далі, MITRE також використовує розвідувальні дані про кіберзагрози, що документують профілі поведінки супротивника, щоб документувати, які групи нападів використовують які методи.

IBM QRadar Use Case Manager – це додаток, що допомагає забезпечити оптимальне налаштування QRadar для точного виявлення загроз у всьому ланцюзі атак. Неважливо чи взаємодія з правилами в QRadar відбувається щодня чи нові дані для виявлення загроз завантажуються з IBM Security App Exchange. Для допомоги в управлінні правилами Use Case Manager надає розширений набір інструментів та можливостей.

QRadar Use Case Manager включає провідник правил, який пропонує гнучкі звіти, пов’язані з правилами. QRadar Use Case Manager також постачається з додатком Cyber Advisory Framework Mapping для розкриття заздалегідь визначених відображень системних правил та для того, щоб допомогти зіставити власні правила до тактик та методів, що використовуються у фреймворку MITRE ATT & CK. Деякі з основних функцій додатка включають: -дослідження кореляційних правил SIEM системи за допомогою візуалізації та згенерованих звітів; -налаштування власного оточення на основі вбудованого аналізу; -візуалізацію покриття загроз у рамках MITRE ATT & CK.

Однією з особливостей використання бази знань MITRE ATT&CK в середовищі IBM QRadar Use Case Manager є візуалізація правил, будівельних блоків та технік MITRE ATT & CK в IBM QRadar. Після організації звіту про правила можна візуалізувати дані за допомогою діаграм та теплових карт.

Проведення аналітики для виявлення методів ATT & CK може відрізнятися від того, як спеціалісти з безпеки звикли до виявлення. Замість того, щоб визначати речі, які, як відомо, погані, і блокувати їх, аналітика на основі ATT & CK передбачає збір даних журналу та подій про речі, які відбуваються у системах, і використовує їх для виявлення підозрілої поведінки, описаної в ATT & CK.

Запобігання використання зловмисниками технік є критично важливим. Реалізація детективного контролю також важлива, оскільки для глибокої

оборони потрібний багатошаровий захист від будь-якої заданої загрози та, як згадувалося раніше, не можливо запобігти реалізації всіх тактик. Тому ATT & CK надає широкі вказівки щодо того, як виявити використання методик зловмисниками з журналами та іншими джерелами аналітики безпеки у розпорядженні організації.

Основні кроки для проведення аналітики з використанням фреймворку включають [4]: -розуміння можливостей для отримання даних та пошуку; -збір даних в платформу для дослідження (наприклад SIEM); -проведення аналітики.

Таким чином В роботі досліджено зміст виявлення загроз та проаналізовані науково-технічні дані. Завдяки даному етапу вдалося визначити основні типи та джерела загроз корпоративній інформаційній системі. Була встановлена необхідність виявлення загроз для уникнення збитків.

Проаналізувавши наявні методи та засоби виявлення загроз була встановлена необхідність швидкого реагування, для виявлення атакуючого в системі, щоб він не встиг завдати непоправної шкоди. У зв'язку з цим зростає потреба у високоінтелектуальних засобах захисту таких, як SIEM-система, що дозволяють вирішувати завдання по своєчасному виявленню атак.

Були визначені можливості програмного комплексу IBM QRadar Use Case Manager та основні функції даного програмного комплексу щодо виявлення загроз.

Джерела:

1. The Growing Challenges of Threat Detection and Response [Електронний ресурс] – Режим доступу: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/growing-challenges-threat-detection-and-response.

2. Кибербезопасность 2019-2020. Тренды и прогнозы [Електронний ресурс] – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020.

3. Threat Detection [Електронний ресурс] – Режим доступу: https://www.rapid7.com/fundamentals/threat-detection.

4. Getting started with ATT&CK [Електронний ресурс] – Режим доступу: https://www.mitre.org/sites/default/files/publications/mitre-getting-started-with-attack-october-2019.pdf.

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПРИКЛАДІ MCAFEE SECURITY ENDPOINT

Хотінь Кароліна Юріївна
Державний університет телекомунікацій,
м.Київ

На сьогодняшній день існує багато типів кібератак. У зв'язку із цим, зростає необхідність в тому, щоб не тільки зупиняти ці кібератаки, а й запобігати їх появи. Тому дуже важливо, аби кожна корпоративна інформаційна система підприємства (незалежно від його розмірів) мала змогу захиститися від них шляхом добре розробленного програмного забезпечення та кваліфікованих кадрів.

Кінцеві станції завжди були якщо не головним, то одним із основних джерел загроз інформаційній безпеці підприємства. При цьому саме поняття «кінцевої станції» істотно розширилося за останні кілька років, особливо з розвитком мобільних платформ.Зараз в область визначення «кінцевої станції» входять не тільки персональні комп'ютери користувачів і

корпоративні сервера, але і мобільні пристрої (ноутбуки, смартфони, планшети) та пристрої IoT (Internet of Things).

У реаліях сьогоднішнього дня організаціям необхідна грамотна оцінка найбільш актуальних загроз для їх інформаційних систем, а також аналіз фінансових і репутаційних ризиків від можливих дій зловмисників.

Основними *проблемами* [1] забезпечення кібербезпеки на підприємствах вважають:

недостатня кваліфікованість кадрів на підприємствах;

невміння запобігати та протидіяти кібератакам та шкідливому ПЗ;

неправильне використання захисного програмного забезпечення;

відсутність розроблення стратегічно правильних засобів захисту інформації в корпоративній системі;

неправильний підхід або відсутність управління ризиками;

крадіжка інформації через підключені пристрої.

Вирішення цих проблем спрямоване на мінімізацію ймовірності таких загроз інформаційній безпеці (ІБ), як несанкціоновані дії з даними, атаки на канал передачі інформації між централізованими ресурсами і кінцевою точкою, авторизація іншої людини під ім'ям справжнього користувача. Використовувані для цього засоби захисту досить добре відомі. Це антивіруси, засоби аутентифікації (скажімо, електронний підпис), засоби захисту каналу (наприклад, VPN). Для мобільних точок доступу додатково буде потрібно встановити засоби криптографічного захисту даних, що розташовуються на носіях інформації (перш за все на знімних - наприклад, флешках), і персональний міжмережевий екран.

Тож, подивимось на існуючі засоби захисту кінцевих точок корпоративної інформаційної системи. За даними «магічного квадранта» Gartner [2] (дослідницька компанія, що спеціалізується на ринку інформаційних технологій) за 2016 рік, лідерами ринку систем захисту кінцевих точок є компанії Symantec, Sophos, Intel Security, Trend Micro, «Лабораторія Касперського» та *McAfee*.

Розглянемо детальніше такий продукт як McAfee.

Саме для захисту кінцевих точок був розроблений окремий програмний комплекс *McAfee Endpoint Security* [3].

Що забезпечує даний продукт? Відповідь очевидна! Даний продукт забезпечує захист кінцевих точок корпоративної мережі та проводить збір інформації про стан безпеки системи у режимі реального часу. У випадку, коли

атака вже відбулась, програмне забезпечення McAfee реагує на всі компоненти та процеси, щоб заблокувати атаку, повідомляти вас та записувати інцидент.

Програмний комплекс McAfee Endpoint Security *включає* в себе такі модулі:

«Threat prevention» (попередження загроз) – захищає користувача від зловмисного програмного забезпечення заздалегідь визначеними діями для виявлення зловмисних програм та підозрілих предметів;

«Firewall» (міжмережевий екран) - фільтрує вхідний та вихідний мережевий трафік, щоб дозволити або заблокувати трафік, згідно з тим, як це визначено у правилах. Кожне з правил визначає набір умов, яким повинен відповідати мережевий трафік і виконувати дії згідно з пов'язаним правилом;

«Web Control» (контроль інтернету) - здійснює моніторинг кожного веб-сайту, до якого користувач отримує доступ або просто переглядає, та перевіряє його рейтинги безпеки задля того, аби дозволити чи заблокувати сайт згідно з конфігурацією політики безпеки підприємства;

«Adaptive threat protection» (адаптивний захист від загроз) - перевіряє вміст у середовищі підприємства та визначає, які дії слід зробити, на основі репутації файлів, правил та порогових значень репутації.

Кожний з цих модулів доповнюють один одного, тому використання кожного з них у комплексі забезпечує захист кінцевих точок на підприємстві.

Отже, виходячи з цього, ми можемо зробити висновок, що захист кінцевих точок-це дуже важливий крок, який гарантує безпеку корпоративній інформаційній системі, якщо притримуватися правил забезпечення безпеки та використовувати надійний програмний продукт.

Література:

1. «Захист кінцевих точок в сучасних умовах: інструменти та основні проблеми» [Електронний ресурс] / Михайло Кондрашин // Компьютерное Обозрение- 2019. - Режим доступу до ресурсу: https://ko.com.ua/zashhita_konechnyh_tochek_v_sovremennyh_usloviyah_instrumenty_i_osnovnye_problemy_129548 ;

2. «Системи захисту кінцевих точок за даними магічного квадранта» [Електронний ресурс] - Режим доступу до ресурсу:http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B_%D0%BA%D0%BE%D0%BD%D0%B5%D1%87%D0%BD%D1%8B%D1%85_%D1%82%D0%BE%D1%87%D0%B5%D0%BA_(Endpoint_Protection_Platform,_EPP) ;

3. Огляд продукту McAfee Endpoint Security [Електронний ресурс] - Режим доступу до ресурсу: https://www.mcafee.com/enterprise/ru-ru/products/endpoint-security.html.

ПРОБЛЕМА ВИБОРУ ОПТИМАЛЬНОГО ПІДХОДУ ДЛЯ МОДЕЛЮВАННЯ ЗАГРОЗ ВЕБ-ДОДАТКІВ

Хмелевський Р.М.
Юдінцев Олег Володимирович, студент БСДМ-71
Державний Університет Телекомунікацій
м. Київ

В умовах сьогодення актуальним є питання впровадження новітніх практик детектування проблем безпеки веб-додатків на ранніх стадіях циклу розробки. Стрімке кількісне та гетерогенне зростання веб-середовища обумовлює відповідне розширення кола ризиків – від витоку персональних даних аж до актів кібер-тероризму. У сучасних реаліях безпека, поряд з іншими атрибутами якості, стала головною вимогою для всіх веб-додатків. Створення безпечного програмного засобу для веб-середовища неможливе без бачення та розуміння threat landscape – множини актуальних загроз з урахуванням архітектури системи та відповідного стеку технологій. В свою чергу, ефективне впровадження безпеки у стандартизований цикл розробки програмних засобів (SDLC) передбачає якнайшвидшу ідентифікацію можливих загроз задля мінімізації ризиків бізнес-процесів, адже вартість виправлення знайдених дефектів зростає в залежності від часу.

Первинним етапом для оцінки безпеки програмного забезпечення є моделювання загроз. Моделювання загроз може застосовуватись до широкого кола систем організації, включаючи бізнес-процеси, мережеву інфраструктуру, розподілені підсистеми, програмні сервіси тощо. Існує декілька методологічних підходів побудови профілю загроз, проте всі вони спрямовані на інформаційну систему в цілому, а не на аналіз безпеки веб-додатків.

Методика TRIKE направлена на забезпечення відповідності процесам аудиту та базується на управлінні кібер-ризиками.[1] Підхід засновано на концепції «моделі вимог», яка гарантує, що визначений рівень ризику для кожного активу інформаційної системи є суб'єктивно допустимим для різних зацікавлених сторін. Множина вимог має бути розділена відповідно до ресурсів системи, з якими будуть взаємодіяти агенти з різними рівнями доступу. Бізнес-сторона має визначити допустимий рівень ризику для кожного з класів активів системи, створюючи «модель вимог». Подальший аналіз створеної моделі дозволяє побудувати профіль можливих загроз із визначенням контр-заходів, необхідних для мінімізації відповідних ризиків. Кінцевим результатом є модель ризику, яка враховує наявні активи інформаційної системи, ролі та дії користувачів, а також схильність до потенційних загроз.[2]

Головними недоліками методу Trike є недостатня формалізація, неналежна підтримка розвитку, та майже повна відсутність документації. Крім іншого, в якості недоліків можна навести низький рівень адаптації відповідно до методології Agile та проблемне масштабування.

Методологія моделювання загроз OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) орієнтована на оцінку операційних (нетехнічних) ризиків та практик безпеки.[3] Ця методологія використовує ізольований підхід, який передбачає, що створення та реалізація стратегій безпеки відбувається безпосередньо внутрішнім департаментом інформаційних технологій підприємства.

Метод OCTAVE виявляє свою ефективність при побудові корпоративної культури безпеки з урахуванням ризиків, оскільки легко налаштовується відповідно до конкретної політики безпеки організації.[4] Водночас, головним недоліком OCTAVE є відсутність масштабованості при нарощувані

функціональних можливостей інформаційної системи, внаслідок чого процес контролю моделі стає некерованим. Хоча підхід OCTAVE забезпечує надійний ресурс-орієнтований аналіз організаційних ризиків, об’єм супроводжуючої документації може стати критичним.[5]

Моделювання загроз згідно підходу PASTA – це процес з 7 етапів, орієнтований на властиві корпоративній системі ризики, межі довіри між компонентами та шаблони атак.[6] Особливість підходу PASTA полягає у орієнтації на ризик, заснований на фактичних даних. Підхід представляє собою процес узгодження бізнес цілей з технічними вимогами задля побудови комплексної стратегії зниження ризиків для підприємства. PASTA дозволяє експертам з інформаційної безпеки краще зрозуміти погляд зловмисного користувача на інфраструктуру організації та розробити процеси управління загрозами, їх ідентифікації та оцінки.

Дана методологія найкраще підходить для організацій, які хочуть узгодити моделювання загроз зі стратегічними бізнес цілями, оскільки вона включає аналіз впливу на бізнес в якості невід'ємної частини процесу. Недоліками є низький рівень адаптування для технічних сторін бізнес-процесу та складність можливої автоматизації. Фокусування методики PASTA на оцінці бізнес-ризиків робить її в першу чергу практикою стратегічного бізнес-управління для відповідних ключових осіб, а не практикою впровадження безпеки у розробку програмного забезпечення підприємства.

Задум підходу VAST (акронім Visual, Agile, Simple Threat modeling) полягав в усуненні обмежень інших методологій моделювання загроз. Основний принцип VAST полягає в масштабуванні процесу по всій інфраструктурі та по всьому циклу розробки системи із інтеграцією у методологію гнучкої розробки програмного забезпечення Agile. Мета VAST – надати рекомендації усім зацікавленим сторонам, включаючи менеджмент, розробників та департамент з інформаційної безпеки.[7]

Основні переваги підходу – це масштабування та тісна інтеграція з методологією розробки ПЗ. Масштабування передбачає співпрацю зацікавлених сторін із використанням різних навичок та знань для визначення пріоритетних задач зниження ризиків, інтеграція з Agile формує основу для спільного процесу моделювання загроз. Недоліком методу VAST є загальна складність розгортання, занадто тісна інтеграція із комерційним програмним продуктом автоматизації «Threat Modeler»[8], а також мала доступність публічної документації.

Підхід STRIDE, який було розроблено у 1999 році та вперше впроваджено у компанії Microsoft, до сьогодні залишається найбільш вживаною та одночасно простою методологією моделювання загроз. В основу STRIDE покладено декомпозицію системи шляхом побудови діаграми потоків даних (DFD), за допомогою якої деталізовано ідентифікуються об’єкти, процеси та граничні межі системи.[9] Слід зазначити, що акуратність побудови діаграми потоків даних значною мірою визначає ефективність подальшого моделювання загроз.[8] Наступним кроком є процес пошуку потенційних загроз, для якого

STRIDE використовує множину з шести класів відомих загроз, що відображається у назві методу: Spoofing (identity), Tampering (data), Repudiation, Information disclosure, Denial of service, Elevation of privileges. Акронім, що закладено у назві методу, можна використовувати в якості мнемоніки для ідентифікації загроз, аналізуючи побудовану за допомогою DFD системну декомпозицію.[2][10] Після виявлення потенційних загроз та визначення стратегії контр-заходів, процес моделювання має бути задокументовано.[8][11]

Метод STRIDE є найбільш простим у застосуванні та демонструє помірно низький рівень хибних спрацювань (false negatives).[12]

Для вибору оптимального методу моделювання загроз необхідно опиратися на область застосування, ресурси часу для розгортання, наявний досвід аналізу ризиків та ступінь залучення зацікавлених сторін. Всі наведені методології дозволяють вирішити дві основні задачі моделювання загроз – імплементацію безпеки на ранньому етапі циклу розробки ПЗ та визначення відповідних запобіжних заходів задля зменшення ризиків, пов’язаних із потенційними загрозами. Водночас, лише деякі методології (OCTAVE, Trike, PASTA, VAST) передбачають пріоритезацію зусиль із зменшення загроз та безпосередньо сприяють управлінню ризиками у бізнес-перспективі. Разом з тим, комплексність перерахованих підходів у порівнянні із методологією STRIDE робить останню найбільш оптимальним варіантом для побудови та інтеграції практики моделювання загроз у цикл розробки систем на основі веб-технологій.

Література:

1. Eddington, Michael, Brenda Larcom, and Eleanor Saitta, 2005. Trike v1 Methodology Document http://octotrike.org
2. Shostack A. Threat Modeling: Designing for Security / Adam Shostack. – Wiley, 2014.
3. Alberts, Christopher. Introduction to the OCTAVE® Approach. Software Engineering Institute, Carnegie Mellon: Pittsburg, 2003.
4. Eaton John W. Octave / John W. Eaton. https://octave.org/doc/interpreter/
5. Stanganelli, J. Selecting a Threat Risk Model for Your Organization, Part Two. eSecurity Planet. September 27, 2016. https://www.esecurityplanet.com/network-security/selecting-a-threat-risk-model-for-your-organization-part-two.html
6. Ucedavélez, Tony and Marco M. Morana. Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis. John Wiley & Sons: Hobekin, 2015.
7. Beyst, B. Which Threat Modeling Method. ThreatModeler. April 15, 2016. https://threatmodeler.com/2016/04/15/threat-modeling-method/
8. Mead, N.; Shull, F.; Vemuru, K.; & Villadsen, O. A Hybrid Threat Modeling Method. Software Engineering Institute, Carnegie Mellon University, 2018. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=516617
9. Hernan, S.; Lambert, S.; Shostack, A.; & Ostwald, T. Uncover Security Design Flaws Using the STRIDE Approach. MSDN Magazine, 2006.
10. Karahasanovic, A.; Kleberger, P.; & Almgren, M. Adapting Threat Modeling Methods for the Automotive Industry. In Proceedings of the 15th ESCAR Conference, 2017.
11. Sion, L.; Yskout, K.; Van Landuyt, D.; & Joosen, W. Solution-aware data flow diagrams for security threat modeling. P.1425-1432. In Proceedings of the 33rd Annual ACM Sympo-sium on Applied Computing, 2018.
12. Scandariato, R.; Wuyts, K.; & Joosen, W. A descriptive study of Microsoft’s threat modeling technique. Requirements Engineering. Volume 20. Number 2, 2015. P.163–180.

ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМИ «РОЗУМНИЙ ДІМ»

Козачок В.А.,
Коновалов О.Г. студент БСЗМ 71

Система «Розумний будинок» (далі – Система) - це об'єднані між собою інтелектуальні пристрої, які створюють людині комфортні і безпечні умови життя виконуючи частину роботи замість неї. Людина фактично перекладає на Систему частину своїх буденних справ (керування інженерними системами - опаленням, освітленням, водопостачанням, кондиціюванням, доступом в приміщення, розвагами, мультимедіа, безпекою тощо). Однак така інтеграція людини і штучного інтелекту може бути небезпечною. При роботі в штатному режимі, якісна інтелектуальна система працює безпомилково і ефективно, але при не коректному функціонуванні або відмові, функції перестають виконуватись і це може дати негативні наслідки.

Тенденція перекладання на інтелектуальну систему важливих функцій, які раніше виконувались людьми з використанням надійних механічних засобів, створює певні ризики негативних подій для користувачів «розумних будинків». Для мінімізації зазначених ризиків при створенні «розумних будинків» слід враховувати деякі аспекти.

Розумні будинки – це відносно нова галузь, в якій ще не напрацьовано сталих вимог і стандартів по ергономічності, якості, безпеці. Компанії на свій розсуд проектують, монтують та позиціонують свої продукти. Користувач очікує, що Система буде працювати безпроблемно і саме так, як декларував виробник. Натомість багатофункціональні системи на виході стають досить складними, інтерфейси заплутаними, їхня настройка потребує суттєвих зусиль, а деякі функції реалізуються не в повній мірі або не виконуються повністю. Іноді замовникам часто доводиться витрачати багато часу і сил, щоб «розумний будинок» запрацював належним чином. Виникає розбіжність очікувань і реальності.

Наприклад розглянемо такі важливі функції Системи, як виведення сигналів від охоронної та пожежної сигналізації на пульти централізованого нагляду. Наявність зазначених опцій обов'язково декларується монтажними організаціями і можливість встановлення охоронних та пожежних датчиків і включення тривожного оповіщення у приміщеннях будівлі з передаванням сигналів про спрацювання сигналізації на охоронні та пожежні пульти існує. Але переважна більшість поважних, добре зарекомендувавших себе охоронних організацій, які дають гарантії на свої послуги по-перше, працюють на власному обладнанні, мають свої стандарти облаштування об'єктів і можуть не погодитись підключати змонтовані чужі об'єктові пристрої Системи з причини безпеки власних пультів та надійності чужого обладнання. По-друге охоронні датчики Системи можуть конфліктувати з обладнанням пультової частини. Охоронні підприємства в своїй переважній більшості, більш за все, не погодяться зробити свої пульти частиною "розумного дому" та інтернету речей з міркувань безпеки пультових пристроїв від вразливостей віддаленого доступу.

Що стосується виведення сигналів "Пожежа" на пожежні пульти, то згідно законодавства України, всі пристрої, які включаються в систему пожежного спостерігання, а ними мають стати пожежні датчики системи "розумний будинок", повинні бути сертифіковані державними органами сертифікації. З цієї причини фірми, які ведуть пожежне спостереження, не виводять сигнали з не сертифікованого обладнання на свої пульти. Крім того,

всі вище викладені зауваження щодо сумісності обладнання і ризиків віддаленого доступу до охоронних пультів, стосуються і пультів пожежного спостерігання.

Зважаючи на зазначене, безпекові функції автоматичного передавання сигналів тривоги можуть бути виконані тільки локально, в межах простору, що охороняється, а тривожні сповіщення у відповідні служби, можуть бути передані тільки «вручну», телефоном, за номерами «101» та «102».

Окремо розгляду потребує питання архітектури включення в «розумний будинок» такого потенційно-небезпечного інженерного обладнання, як сауна. Зважаючи на те, що зазначена підсистема є пожежонебезпечною, навіть у штатному режимі роботи, вона має бути запроектована і змонтована за розподіленою схемою, як окрема підсистема. Функція увімкнення її в роботу повинна здійснюватись вручну, безпосередньо з самого будинку. Це унеможливить віддалене, зловмисне включення сауни та маніпулювання режимами роботи її нагрівальних елементів в разі отримання зловмисниками несанкціонованого доступу до керування центральним процесором (тривала штатна робота нагрівальних елементів в певних режимах, може створювати вибухо- та пожежонебезпечні стани). З усіх функцій автоматизації сауни, бажано залишити тільки її автоматичне вимкнення та аналоговий сигнал сповіщення про режими її роботи.

Список літератури:
1. М. Э. Сопер. Практические советы и решения по созданию «Умного дома» М. Э. Сопер. – М.: НТ Пресс, 2007; Ярочкин В.И. Информационная безопасность. – М.: Изд–во «Академический проект», 2004. – 640 с.
2. .ДСТУ EN 50136-1:2014 Системи тривожної сигналізації. Системи передавання тривожних сповіщень та устаткування. Частина 1. Загальні вимоги до систем передавання тривожних сповіщень (EN 50136-1:2012, IDT)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ДОКУМЕТІВ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕТООБІГУ

Довженко Н.М.
Кудлій Олексій Олександрович, студент БСДМ-71
Державний університет
Телекомкунікацій
м. Київ

В умовах розвитку електронного самоврядування в Україні є актуальним питанням забезпечення безпеки електронних ресурсів. Так як управління відбувається за рахунок розпорядчих документів, забезпечення безпеки електронних документів посідає особливе місце.

З метою розуміння підходу до забезпечення безпеки електронних документів необхідно проаналізувати нормативно-правові акти пов’язані з забезпеченням безпеки електронних документів, загрози які відносяться до електронних документів і методи та засоби забезпечення безпеки електронних документів.

В Україні існують нормативні документи які визначають загальні засади електронних документів та електронного документообігу [1], правила забезпечення захисту інформації в інформаційно-телекомунікаційних системах [2]. Ці закони регулюють правила використання електронних документів.

Під загрозою інформаційній безпеці розуміють сукупність умов та факторів, що створюють небезпеку життєво важливим інтересам суспільства, держави та особистості. Загалом під загрозою інформаційній безпеці визначають потенційно можливу подію, дію, процес або явище, що може призвести до нанесення шкоди системі. Загрози кібербезпеці актуалізуються через дію таких чинників: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [3].

Розглянемо загрози які базуються на властивостях інформації. Її можна розділити на: порушення конфіденційності, порушення цілісності, порушення доступності інформації. Загрози порушення конфіденційності інформації, у результаті реалізації яких інформація стає доступною суб’єкту, що не володіє повноваженнями для ознайомлення з нею. Загрози порушення цілісності інформації, до яких відноситься будь-яке зловмисне спотворення інформації, яка обробляється з використанням інформаційної системи. Загрози порушення доступності інформації, що виникають у тих випадках, коли доступ до деякого ресурсу ІС для легальних користувачів блокується.

Можна виділити такі основні рівні забезпечення безпеки електронних документів: законодавчий, адміністративний, програмно-технічний рівень [4].

Законодавчий рівень протидії загрозам є найважливішим для забезпечення інформаційної безпеки. Розробка та прийняття законодавчих актів створюють умови для безпечного використання інформаційно-комунікаційних технологій, доступу до інформації, захисту інформації від несанкціонованого доступу.

Головна мета заходів адміністративного рівня є сформування програми робіт в області інформаційної безпеки й забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ. Політика безпеки є основою для адміністративного рівня. Під політикою безпеки ми будемо розуміти сукупність документованих розв'язків, прийнятих керівництвом організації й спрямованих на захист інформації й асоційованих з нею ресурсів.

Програмно-технічний рівень протидії загрозам електронного документу включає такі механізми захисту: ідентифікація і аутентифікація користувачів; управління доступом; протоколювання і аудит; криптографія; екранування каналів зв’язку; забезпечення високої доступності тощо. Основні положення програмно-технічного рівня забезпечення безпеки електронного документу можна розділити на: управління доступом до системи електронного документообігу; спостережливість за доступом до системи електронного

документообігу та діями над електронними документами; аудит систем пов’язаних з електронним документом [5].

Забезпечення безпеки електронних документів здійснюється також за допомогою комплексних систем електронного документообігу. Яка має підтримувати функції: розмежування прав доступу на рівні: функціональних модулів, функцій, групи операцій, окремих операцій, атрибутів реєстраційної картки, групи документів, окремих документів; ідентифікація користувачів як за логіном і паролем, так і за допомогою кваліфікованого електронного підпису; автоматичний запит повторної аутентифікації користувача через визначений період перерви у роботі з системою; можливість блокування облікового запису; протоколювання дій користувачів у захищеному журналі.

Література:

1. Про електронні документи та електронний документообіг [Текст]:Закон України 851-IV від 7 листопада 2018 р. / Верховна Рада України // Відомості Верховної Ради України. – 2003. – № 36.– ст.275

2. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах послуг [Текст]: Постанова Кабінету Міністрів України 373-2006-п від 13 жовтня 2011 р. / Кабінет Міністрів України // Відомості Кабінету Міністрів України. – 2006. – № 373

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Текст]: Указ Президента України 96/2016 від 15 березня 2016 р.

4. Хошаба О. Захист інформації в системах електронного урядування / [О.М. Хошаба]. – К.: ФОП Москаленко О. М., 2017. – 72 с.

5. . Кукарін О. Електронний документообіг та захист інформації / Олександр Кукарін – К. : НАДУ, 2015. – 84 с.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ 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. Межуревский В.Ф. Анализ применения технологий мониторинга компютерных сетей [Електронний ресурс] – Режим доступу: https://cyberleninka.ru/article/n/analiz-primeneniya-tehnologiy-monitoringa-kompyuternyh-setey

2. Дрейман И.А., Капуста А.П. Мониторинг и управление сетью передачи данных [Електронний ресурс] – Режим доступу: http://elib.sfu-kras.ru/handle/2311/6919

3. Zabbix Documentation 4.4: Руководство по Zabbix [Електронний ресурс] – Режим доступу: https://www.zabbix.com/documentation/4.4/ru/manual/

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/