ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИУТУ ЗАХИСТУ ІНФОРМАЦІЇ

ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

Тези доповідей

24 жовтня 2019
м. Київ

ЗМІСТ

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ: ЗМІ ЯК ФАКТОР ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

Бржевський Микита В'ячеславович

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

Розглянуто поняття інформаційної війни та інформаційна операція. Наведено задачі інформаційних операцій, які полягають в маніпулюванні масовою свідомістю. Серед потенційних загроз в інформаційній сфері відзначаються ризики і загрози інформаційних впливів. Для реалізації негативних інформаційних та психологічних впливів використовується весь спектр засобів масової інформації. Перераховані фактори інформаційно-психологічного ризику, об'єкти та суб'єкти інформаційно-психологічного захисту.

У сучасному світі внаслідок постійного зростання значення інформації індустрія її одержання, обробки, реєстрації, передачі та поширення стає однією з провідних галузей діяльності людства, куди з кожним роком вкладають усе більші кошти. Інформація стає найважливішим стратегічним ресурсом, брак якого призводить до істотних втрат у всіх сферах життя.

На жаль, сьогодні як ніколи є актуальним поняття «інформаційна війна». Всі ми мимоволі стаємо свідками та учасниками різних інформаційних протиборств - чи то передвиборних перегонів, чи то спроб рейдерських атак, чи то просто просування деяких товарів і послуг у конкурентному середовищі. У класичному розумінні інформаційна війна - це одна з форм інформаційного протиборства, комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не відповідають їхнім інтересам, а також, природно, захист від подібних впливів.

Основні методи інформаційної війни є блокування або перекручування інформаційних потоків і процесів прийняття рішень супротивником [1].

Термін «інформаційна операція», який останнім часом застосовується усе ширше, відповідає компоненті інформаційних протистоянь, зміст якої

спрямовано на реалізацію попередньо спланованих інформаційно-психологічних впливів на ворожу, дружню або нейтральну аудиторію шляхом впливу на установки та поведінку для досягнення заздалегідь визначених цілей.

Основна задача інформаційних операцій полягає в маніпулюванні масовою свідомістю з такими цілями, як, наприклад:

- внесення в суспільну свідомість і свідомість окремих людей визначених ідей і поглядів;
- дезорієнтація людей та їхня дезінформація;
- ослаблення визначених переконань людей, основ суспільства;
- залякування мас.

Серед потенційних загроз в інформаційній сфері відзначаються й ризики інформаційних впливів: прагнення маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [2].

Основними реальними і потенційними загрозами в інформаційній безпеці країни у внутрішньополітичній сфері є

- деструктивні інформаційні впливи
- поширення суб'єктами інформаційної діяльності перекручувань, недостовірної та упередженої інформації [3].

Для реалізації негативних інформаційно-психологічних впливів використовується весь спектр ЗМІ. Комплексне застосування цих засобів забезпечує ефективну реалізацію всього спектра негативного інформаційно-психологічного впливу, а саме: дезінформації, маніпулювання, пропаганди, шантажу, поширення слухів, компрометації, дискредитації, провокації, кризового керування.

До факторів інформаційно-психологічного ризику слід віднести:

- неповну або недостовірну інформацію у ЗМІ;
- надмірний обсяг і хаотичність інформації, яка циркулює в суспільстві;
- технологічні помилки щодо введення, збереження й обробки даних в інформаційних системах;
- штучне або природне перекручування інформації в процесі її відбору для аналізу й використання у ході прийняття відповідальних державних рішень.

Основними об'єктами інформаційно-психологічних загроз у сфері масової свідомості є:

- спільні інтереси великих мас громадян (соціальних груп або національних утворень, населення країни в цілому), які можна назвати груповими асоціаціями;
- культурні, духовні й моральні цінності, які сповідуються груповими асоціаціями.

Суб'єктами інформаційно-психологічного захисту можуть бути:

- сама людина з її внутрішніми психологічними можливостями щодо самозахисту;
- соціальні групи й співтовариства, які надають особистості підтримку й допомогу психологічними засобами;

- держава й суспільство, які підтримують або допомагають громадянину через діяльність певних соціальних інститутів [4].

Нові можливості для захисту інтересів держави дає відповідне використання сучасних методів і засобів збору, передачі, обробки і захисту інформації. Найбільшої ефективності вони досягають у разі об'єднання національних інформаційних систем і телекомунікаційних мереж у загальну інформаційно-телекомунікаційну інфраструктуру зі спільними системами інформаційної протидії негативним зовнішнім впливам.

Література:

1. Information operations roadmap. – DoD US, 30 october 2003. – 78 p.
2. Закон України «Про основи національної безпеки» від 7 серрня 2015 р.
3. Доктрина інформаційної безпеки №47/2017 від 25 лютого 2017 р.
4. В.Г. Головань. Інформаційна безпека держави: аспекти інформаційно-психологічних загроз / В.Г. Головань, О.М. Дроздов, В.В. Сергєєв, В.М. Герасимов // Збірник наукових праць ЖВІНАУ. Випуск 5, 2011. – С. 33-41

Теоретичні аспекти створення методики протидії соціальному інжинірингу

Гайдур Г.І.,
Біленко А.А.
студент групи БСДМ-61

В контексті інформаційних технологій соціальна інженерія - це загальна кількість підходів щодо прикладних соціальних наук, які орієнтовані на спрямовану зміну організаційних структур, які визначають людську поведінку і надають контроль за нею. Також це комплексний підхід до навчання і можливих змін соціальної реальності, що засновано на застосуванні інженерного підходу і наукових технологій. Соціальна інженерія застосовується для збору відомостей про мету підприємства, отримання конфіденційної інформації, прямого доступу до системи. Тож створення методики протидії на підприємства є доцільним та має важливий аспект забезпечення протидії таких атак.

Важливим фактором протидії соціальному інжинирінку є підготовка прцівникив до таких атак. Ніякі технічні заходи захисту інформації практично не допоможуть захиститися від соціального інжинірингу. Пов'язано це з тим, що соціальні інженери використовують слабкості нетехнічних засобів, а як говорилося, людський фактор. У зв'язку з цим, єдиний спосіб протидіяти соціальним інженерам - це постійна і правильна робота з персоналом [1].

Для підвищення безпеки в організації, весь час повинні проводитися спеціальні навчання, постійно контролюватися рівень знань у співробітників, має проводитися тестування, а так само відбуватися внутрішні диверсії, які дозволять виявити рівень підготовленості співробітників в реальних умовах.

Найважливіший момент в підготовці користувачів, на який слід вказати увагу - це те, що навчання - це циклічний процес, який повинен повторюватися з періодичністю в часі.

Форма навчання може складатися з таких видів, як:

1. Теоретичні заняття.
2. Практикум.
3. Онлайн-семінари.
4. Рольові ігри (тобто створення моделі атаки).

Для того щоб створити методику навчання персоналу, яка буде працювати, необхідно зрозуміти, чому люди вразливі для атак. Для виявлення цих тенденцій, необхідно звернути на них увагу завдяки дискусії - цим можна допомогти співробітникам зрозуміти, як соціальний інженер може маніпулювати людьми.

Розробку протидій соціальному інжинірингу необхідно почати з створення групи людей, які будуть відповідати за безпеку. Вони повинні відповідати за розробку політик і процедур безпеки, які повинні бути спрямовані на захист окремих співробітників і мережі організації в цілому. Ця група повинна включати в себе співробітників з різних відділів [2, 3].

До завдань цієї групи повинні входити такі речі як:

1. Забезпечення підтримки політик і процедур безпеки.
2. Допомога в розробці навчально-методичних матеріалів для співробітників .

Співробітник, відповідальний за розробку програми інформаційної безпеки повинен виробити специфічні вимоги для окремих груп співробітників, що беруть участь в роботі з інформацією, яка обробляється організацією. Тренінги повинні проводитися для всіх груп персоналу.

Розробка методики підвищення обізнаності персоналу у питаннях протидії методам соціальної інженерії включає в себе такі складові:

1 Розробка методичних вказівок для підвищення рівня обізнаності персоналу у питаннях протидії методам соціальної інженерії.

2 Розробка шаблону опитувальника як метрики ефективності методики обізнаності та способу виявлення слабких сторін обізнаності персоналу для подальшого навчання їх у цьому напрямку.

Таким чином, навчання персоналу буде проходити кілька разів на рік.

Література

1. Гаврилов А. Социальный инжиниринг в действии / А. Гаврилов // Безопасность. – 2015. - №3. – с. 118-122.

2. Безмалый В. Психология на службе хакеров [Электронный ресурс] : < http://www.bibliofond.ru/view.aspx?id=67351> (07.09.18).

3. Соколов В.В., Курбанмурадов Д..М. Методика протидії соціальному інжинірингу на об’єктах інформаційної діяльності. Кібербезпека: освіта та наука. №1(1). – 2018. – ст.6-16.

Мельник М. О.
Студент БСДМ-61
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

ІНФОРМАЦІЙНІ АТАКИ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СКЛАДНИХ СОЦІОТЕХНІЧНИХ СИСТЕМ

В даній статті розглянуто соціотехнічні системи, складовою яких є людина-оператор, знання, уміння, настрої, ціннісні переваги й ставлення до виконуваних обов'язків які у взаємодії з технічним пристроєм у процесі. Розглянуті інформаційні атаки та їх методи реалізації, які представляють велику загрозу для інформаційно-технологічного сектору і вчасності для складних соціотехнічних систем. Проаналізовані та виявлені такі актуальні загрози: цільові атака, соціальна інженерія та її наслідок соціотехнічні атаки. Підкреслені методи та рішення захисту від цих загроз.

Людський процес існування в наш час повністю пов'язаний зі складними соціотехнічними системами. Всюди є взаємодія людини та технологій. Через певну людську природу процеси складних соціотехнічних систем потребують забезпечення безпеки. Існує безліч загроз, безліч методів проведення і реалізації інформаційних атак на наш спосіб життя. Такі загрози виходять навіть на рівень Держави. Статистика здійснених атак по всьому світу в економічних, політичних та інших секторах тільки зростає. Навіть на звичайних людей, майже кожний день, здійснюються інформаційні атаки шляхом соціальної інженерії, що призводить до масових шахрайств. Проте справжнє число атак ми не дізнаємось, тому що більшість компаній та корпорацій приховують факти того, що на них була здійснена інформаційна атака. Наша країна потребує сучасних рішень та методів забезпечення безпеки від інформаційних атак. Потрібні спеціалісти високого рівня, для того щоб вони могли передати свій досвід та знання іншим. Також потрібні фінансові та технічні ресурси для реалізації кібербезпеки.

Розробники концепції соціотехнічних систем — англійські вчені Е. Тріст та К. Бемфорт, які досліджували процеси механізації добування вугілля у Великобританії[1, 95; 96 с.]. Їхні пошуки завершилися встановленням взаємозв'язку та взаємної зумовленості обох частин цілісної системи — технічної, що охоплює в собі інструменти й обладнання, та соціальної, утворюваної сукупністю людей, відношень між ними й сформованих інституціональних установок.

Загалом під системою слід розуміти цілісність взаємопов'язаних елементів та взаємозв'язків між ними, яким притаманні певні властивості, мета, цілі та функції. Головні характеристики соціотехнічної системи такі:

- організаційна філософія, що базується на розумінні працівниками своїх цілей і призначення підприємства, на їхній постійній готовності поділити

з адміністрацією всю повноту відповідальності за результати господарської діяльності;

- організаційна структура управління, що забезпечує рядовим робітникам та службовцям реальні права щодо участі в керуванні;
- новий підхід до розробки робочих місць і визначення ролі виконавця в процесі ухвалення управлінських рішень;
- нова схема розміщення обладнання, яка має відповідати потребам перспективної форми організації праці, забезпечуючи прискорене проходження матеріальних потоків на виробництві;
- нові форми й методи підготовки та перепідготовки кадрів, що спираються на гнучку кадрову політику, спрямовану на гарантування зайнятості;
- нові критерії в оцінюванні економічної ефективності використання сучасних технологій та здійснення капіталовкладень у розвиток виробництва.

Складну соціотехнічну систему можна назвати сучасним алгоритмом людського життя. І для такого життя, в наш час високих інформаційних технологій, існують загрози у вигляді різних інформаційних атак.

Можна підкреслити основні загрози, такі як: цільова атака, соціальна інженерія, соціотехнічна атака. Цільові атаки — це атаки, спеціально націлені на одну людину, компанію або групу компаній, які проводяться тихо і непомітно(2). Це не масові атаки, оскільки їх мета не вразити якомога більше комп'ютерів. Небезпека полягає саме в «замовному» характері такого роду атак, які спеціально розробляються для обману своїх потенційних жертв. Даний вид інформаційної атаки як правило реалізується завжди успішно. Цілеспрямовані атаки зазвичай добре сплановані та включають кілька етапів — від розвідки й впровадження до знищення слідів присутності. Як правило, в результаті цілеспрямованої атаки зловмисники закріплюються в інфраструктурі жертви та залишаються непоміченими протягом місяців або навіть років. Протягом усього цього часу вони мають доступ до всієї корпоративної інформації.

Соціальна інженерія використовується для проведення розвідки інформаційних телекомунікаційних систем та характеризується специфічними механізмами — способами й методами, а також силами та засобами, залученими у процесах збору або добування інформації[1, 112 с.]. Головні способи ведення розвідки — розвідка систем телекомунікацій, мережна розвідка та кіберрозвідка. Ці види розвідки мають на меті систематичний пошук, збір та добування різноманітних даних про об’єкти атак. Після соціальної інженерії проводять соціотехнічні атаки. Їхня мета це отримати несанкціонований доступ до захищених інформаційних систем(паролі, персональні дані тощо).

З поміж сучасних і дієвих засобів захисту від інформаційних атак можна виділити Deception та SOC. Deception — це одна з нових технологій інформаційної безпеки, яка призначена для боротьби з цільовими атаками, атаками нульового дня і шкідливим програмним забезпеченням(3). Технологія базується на спеціальній, паралельній мережі замаскованих мережевих пасток і приманок, розкиданої по всій IT-інфраструктурі, що дозволяє виявляти атаки на етапі поширення, коли хакери починають досліджувати мережу і захоплювати її.

Deception забезпечить: виявлення в режимі реального часу цілеспрямованих атак і атак нульового дня, захист реальних IT-активів шляхом перемикання активності нападників на «пастки», захист цінних даних від «шифрувальників», збір інформації про дії зловмисників, відсутність помилкових спрацьовувань.

Питаннями побудови Security Operation Center(SOC) цікавляться практично всі представники світової економіки: від страхових компаній і банків до великих промислових підприємств. SOC є одним з ключових компонентів підрозділів інформаційної безпеки будь-якої організації. В першу чергу він націлений на моніторинг, детектування й оперативну реакцію на інциденти, і як наслідок, на скорочення шкоди та фінансових втрат, до яких той чи інший інцидент може призвести(4). SOC — це не тільки технічні засоби. Це команда, завдання якої виявляти, аналізувати, реагувати, повідомляти про виникнення і запобігати інцидентам інформаційної безпеки. Ще один важливий компонент SOC — це процеси, оскільки мається на увазі взаємодія між співробітниками підрозділу, відповідального за моніторинг і реагування на інциденти, а також між різними підрозділами. Від того, наскільки якісно збудовані ці процеси, буде залежати ефективність роботи SOC. Технічні засоби є лише інструментами, які дозволяють автоматизувати частину процесів, які функціонують. SOC є хорошим варіантом забезпечення безпеки. Він працює в режимі 24/7, завдяки технічним інструментам та SIEM(Security information and event management) системі здійснюється моніторинг наших робочих систем. Команда спеціалістів постійно на місці й проводять аналітичну та технічну роботу.

Складні соціотехнічні системи містять ті елементи «людського фактора», які впливають на кожного окремого індивіда та на групи людей, зокрема у плані їхнього ставлення до роботи, на організаційну культуру, на керівництво та управління в цілому. «Людський фактор» являється слабким та найбажанішим об’єктом для цільових і соціотехнічних атак. Є велика потреба для посилення саме соціального сектору в кібербезпеці. А також розвивати й технічні засоби захисту, тому що технічний прогрес дуже стрімкий. Кіберзлочинність не стоїть на місці, вона з кожним днем стає розумнішою, хитрішою і розвиненою в технічних засобах.

Література:

1.В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа «ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: СОЦІОТЕХНІЧНИЙ АСПЕКТ» [Електронний ресурс]: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

2.Основы социотехники [Електронний ресурс]: https://www.securitylab.ru/analytics/216202.php

3.Deception – ловушки для хакеров [Електронний ресурс]: https://itprotect.ru/all-services/solutions/traps

4.Як швидко запустити свій Security Operation Center (SOC) [Електронний ресурс]: https://www.antimalware.ru/analytics/Technology_Analysis/How_fast_run_SOC_Security_Operation_Center

БЕЗПЕКА КОНТЕЙНЕРІВ DOCKER. КРАЩІ ПРАКТИКИ

Седлецький Денис Володимирович

Останніми роками використання Docker стає більш поширеним явищем, тому безпека контейнерів стає критичним фактором для підприємств та організацій, які використовують контейнери для розробки та запуску свого продукту. Зважаючи на те, що контейнери набагато складніші, ніж віртуальні машини та інші подібні технології розгортання, які широко використовувались до появи Docker, навчання безпеці контейнерів Docker також може стати випробуванням.

До появи Docker більшість організацій використовували віртуальні машини або звичайні фізичні сервери для розміщення свої додатків. З точки зору безпеки, ці технології відносно прості. Вам потрібно зосередитись лише на двох шарах (хост-середовище та додаток) задля забезпечення надійного розгортання та контролю за подіями, що стосуються безпеки. Також зазвичай не потрібно дуже хвилюватися щодо API, складних конфігурацій зберігання даних або мереж, оскільки вони, як правило, не є основною частиною розгортання віртуальної машини чи фізичного сервера.

Захист контейнерів Docker є складнішим, багато в чому тому, що в типовому середовищі Docker є набагато більше змінних частин. Ці частини включають:

- Ваші контейнери. Напевно, у вас є кілька зображень контейнерів Docker, кожен з яких розміщує окремі мікросервіси. Напевно, у вас також є кілька примірників кожного зображення, що працює в даний момент часу. Кожне із цих зображень та екземплярів потрібно захищати та контролювати окремо.
- Служба Docker, яку потрібно захистити, щоб зберігати підконтрольні їй контейнери в безпеці.

- Хост-сервер, який може бути фізичним сервером або віртуальною машиною.
- Якщо ви розміщуєте ваші контейнери в хмарі (за допомогою AWS, Google Cloud і т.п.), це ще один шар для захисту.
- Мережі та API, що полегшують зв'язок між контейнерами.
- Системи зберігання даних, які існують ззовні від ваших контейнерів.

Безпека Docker справді складніша, ніж інші стратегії безпеки. Нижче наведено кілька кращих практик, які можуть стати у нагоді.

1. Встановлення квот на ресурси

Одна зручна річ, яку в Docker легко зробити - це налаштування квот на ресурси на основі контейнерів. Квоти дозволяють обмежити об'єм пам'яті та ресурсів процесора, які контейнер може споживати. Квоти на ресурси легко встановити за допомогою опцій командного рядка.

Ця функція корисна з кількох причин. По-перше, це допоможе запобігти випадкам, коли один контейнер чи додаток споживає занадто багато системних ресурсів, що призводить до зависання системи. По-друге, це підвищує безпеку, не даючи скомпрометованому контейнерові споживати велику кількість системних ресурсів з метою порушення роботи сервісу чи виконання шкідливих дій.

2. Не запускайте Docker з правами root

Ви втомилися і не хочете боротися з налаштуваннями дозволів, щоб програма працювала належним чином, тому просто запускаєте її від імені root, щоб не турбуватися про обмеження дозволу. Це може бути прийнятним лише в тестовому середовищі Docker, якщо ви вчитеся вперше використовувати Docker, але у продуктивних системах не існує вагомих причин дозволити контейнеру працювати з правами суперкористувача.

Дотримуватись цієї рекомендації досить легко, оскільки Docker не запускає контейнери як root за замовчуванням. Тому, як правило, нічого не потрібно змінювати в конфігурації, щоб запобігти виконанню з правами суперкористувача. Для додаткової безпеки Docker, при використанні Kubernetes для адміністрування ваших контейнерів, ви можете не допустити запуску контейнерів як root (навіть якщо адміністратор намагається вручну запустити контейнер з правами суперкористувача), використовуючи директиву MustRunAsNonRoot в політиці безпеки.

3. Захистіть регістри своїх контейнерів

Регістри контейнерів є причиною такої потужності Docker. Вони полегшують налаштування центрального сховища, з якого ви можете завантажувати образи контейнерів за допомогою кількох натискань клавіш. Однак простота та зручність регістрів контейнерів можуть створювати ризики безпеки, якщо ви не можете оцінити контекст безпеки регістру, який ви використовуєте. За ідеальних умов, ви будете використовувати регістр, такий

як Docker Trusted Registry, який можна встановити за власним брандмауером, щоб зменшити рівень ризику.

4. Використовуйте надійні, безпечні образи

Говорячи про регістри, ви також повинні бути впевнені, що образи контейнерів, які ви отримуєте, надходять із надійного джерела. Це може здатися надто очевидним, але, враховуючи, що існує стільки загальнодоступних образів контейнерів, які можна швидко завантажити, ви можете отримати образ з недовіреного джерела. З цієї причини слід додати до чорного списку публічні регістри контейнерів, окрім надійних офіційних сховищ, таких як Docker Hub.

Ви також можете скористатися інструментами сканування образів, щоб виявити деякі відомі вразливості в межах Docker-образів. У більшості регістрів контейнерів є вбудовані засоби сканування. Деякі з них, наприклад Clair, можуть використовуватися окремо від регістру для сканування окремих зображень.

5. Визначте джерело свого коду

Слід мати на увазі, що образи Docker зазвичай містять поєднання оригінального коду та пакетів зі сторонніх джерел. Таким чином, навіть якщо конкретний образ, який ви завантажуєте, походить з надійного регістру, він може містити пакети з інших джерел, яким не можна довіряти.

У цьому контексті є корисними інструменти аналізу вихідного коду. Завантажуючи джерела всіх пакетів у ваших образах Docker та скануючи їх, щоб визначити, звідки походить код, ви можете визначити, чи містить будь-який з кодів, включених у ваші образи контейнера, відомі вразливості безпеки. В якості додаткової переваги, аналіз вихідного коду також допомагає вам дотримуватися ліцензійних вимог, що стосуються сторонніх кодів.

6. Безпека API та мережі

Як зазначалося вище, контейнери Docker зазвичай покладаються на API та мережі для комунікації один з одним. Ось чому важливо переконатися, що ваші API та мережеві архітектури спроектовані надійно, а також ви відстежуєте використання API та мережеву активність на предмет аномалій, які можуть свідчити про вторгнення. Тож, основне повідомлення тут полягає в тому, що безпека API та мережі є особливо важливими при використанні Docker, тому ними не слід нехтувати.

Висновок

Docker - це досить складний інструмент, і не існує універсального методу, який можна використовувати для підтримки безпеки контейнерів Docker. Натомість ви повинні цілісно подумати про способи забезпечення безпеки своїх контейнерів Docker та засоби підвищення безпеки середовища для контейнерів на кількох рівнях. Це єдиний спосіб переконатися, що ви можете скористатись усіма перевагами контейнерів Docker, не піддаючи себе ризикам безпеки.

Література

1. IT-ресурс “Computerworld”. URL: https://www.computerworld.com/
2. IT-ресурс “White Source”. URL: https://resources.whitesourcesoftware.com/blog-whitesource/

ПРОБЛЕМИ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Герега Ілля Дмитрович

Розглянуто основні поняття електронного документу та документообігу, об’єкти захисту інформації в СЕД та способи їх захисту, виділено основні загрози систем електронного документообігу, наведено статистику втрат інформації в СЕД, запропоновано рекомендації щодо організації захищеного електронного документообігу.

Нині, в епоху розвитку інформаційних та автоматизованих систем управління, дедалі більше підприємств в Україні відмовляються від традиційного – паперового документообігу. Розвитку ідей «держави в смартфоні» посприяв, перш за все, розвиток електронного документообігу. Електронний документообіг є сучасну технологію, яка дозволяє не тільки розвиватися, а й значно спрощувати всі процеси на підприємстві.

Проблема, пов'язана з автоматизацією обміну інформації в компаніях, стала однією з найпоширеніших в нашій країні. Дане твердження можна підтвердити наступними даними. За оцінкою Siemens Business Services, до 80% свого робочого часу керівник витрачає на роботу з інформацією, до 30% робочого часу співробітників йде на створення, пошук, узгодження і відправлення документів, кожен внутрішній документ копіюється, в середньому, до 20 разів і до 15% корпоративних документів безповоротно втрачається. Існують також оцінки, що на роботу з документами доводиться витрачати до 40% трудових ресурсів і до 15% корпоративних доходів. Саме тому ефективність управління підприємствами та організаціями не в останню чергу залежить від коректного рішення задач оперативного і якісного формування електронних документів, контролю їх виконання, а також продуманої організації їх зберігання, пошуку і використання. Поняття електронного документообігу в Україні визначено Законом України «Про електронні документи та електронний документообіг» від 22 травня 2003 року №851-IV та полягає у наступному:

«Електронний документообіг (обіг електронних документів) це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів».

Тобто, електронний документообіг – це така інформаційна система, яка сприяє більш раціональному і простому використанню даних компанії. У неї включені такі складові, як відповідне програмне забезпечення, електронна пошта, що дає можливість оперативно зв'язуватися з підлеглими, Інтернет і багато іншого. Потреба в ефективному управлінні електронними документами призвела до створення та розвитку систем електронного документообігу.

Система електронного документообігу (СЕД) - комп'ютерна програма, яка дозволяє організувати роботу з електронними документами, а також взаємодія між співробітниками. Базовим елементом будь-якої СЕД є документ, всередині системи це може бути, наприклад; файл або запис в базі даних. Говорячи про захищений документообіг, часто мають на увазі саме захист документів, захист тієї інформації, яку вони в собі несуть. Однак насправді необхідний захист всієї системи електронного документообігу, а не тільки даних всередині неї. Це означає, що потрібно захистити працездатність СЕД, забезпечити швидке відновлення після ушкоджень, збоїв і навіть після знищення. Тому до питань організації захисту системи електронного документообігу необхідно підходити комплексно, що означає захист на всіх рівнях СЕД, починаючи від фізичних носіїв інформації, даних на них та закінчуючи організаційними заходами. Отже, необхідний захист:

- апаратних елементів системи. Це комп'ютери, сервери, елементи комп'ютерної мережі та мережеве обладнання;
- файлів системи. Це файли програмного забезпечення та бази даних. У разі їх незахищеності з'являється можливість впливу зловмисника на файли СЕД.
- захист документів і інформації, що знаходяться всередині системи.

Використовуючи такий підхід, можна побудувати систему, захищену на всіх рівнях, з рубежами оборони від загроз на кожному рівні. Вартість такого захисту може зрівнятися з вартістю самої СЕД, тому потрібно шукати розумний баланс між безпекою та вартістю. Всі загрози для системи електронного документообігу можна поділити на наступні:

- загроза цілісності - пошкодження і знищення інформації, спотворення інформації - як ненавмисне в разі помилок і збоїв, так і зловмисне;
- загроза конфіденційності - це будь-яке порушення конфіденційності, в тому числі крадіжка, перехоплення інформації, зміни маршрутів слідування;
- загроза працездатності системи - всілякі загрози, реалізація яких призведе до порушення або припинення роботи системи, сюди входять як умисні атаки, так і помилки користувачів, а також збої в обладнанні та програмному забезпеченні.

Можна виділити кілька, основних, груп джерел загроз: легальні користувачі системи, адміністративний IT - персонал, зовнішні зловмисники. Згідно з численними дослідженнями, від 70 до 80% втрат від злочинів припадають на атаки зсередини. Особливу групу становить адміністративний IT - персонал, або персонал служби IT - безпеки. Ця група, як правило, має не

обмежені повноваження і доступ до сховищ даних, тому до неї потрібно ставитися з особливою увагою. Вони не тільки мають великі повноваження, але і найбільш кваліфіковані в питаннях безпеки та інформаційних можливостей. Згідно зі статистикою, втрати важливої інформації в 45% випадків припадають на фізичні причини (відмова апаратури, стихійні лиха і т. П.), 35% обумовлені помилками користувачів і менш 20% - дією шкідливих програм і зловмисників. Безпечний доступ до даних усередині СЕД забезпечується автентифікацією і розмежуванням прав доступу до об'єктів. В СЕД можуть використовуватися різні методи автентифікації. Найпоширеніший з них - застосування багаторазових паролів. Шифровані значення паролів зазвичай зберігаються на сервері в спеціальній базі даних користувачів. Однак надійність даного методу сильно знижує людський фактор. Навіть якщо користувач використовує правильно згенерований пароль, іноді його можна виявити записаним на листку паперу в столі або під клавіатурою. Також існує безліч рішень для майнової автентифікації користувача: це USB-ключі, смарт-карти, магнітні карти, дискети та компакт-диски. Тут також не виключено вплив людського фактора, але зловмисникові необхідно не тільки отримати сам ключ, а й дізнатися PIN-код. Розмежування прав доступу до об'єктів системи електронного документообігу, може бути реалізовано виходячи з різних принципів:

- завдання користувачів і груп, що мають право читання, редагування або видалення всього документа, включаючи приєднані файли і реквізити;
- мандатний доступ по групах, коли доступ до даних, надається відповідно до фіксованих рівнями повноважень груп користувачів;
- розмежування доступу до різних частин документів, наприклад до різних приєднаним файлів, груп реквізитів, полях реєстраційних карток, доручень по документу.

Серед методів розмежування доступу можна виділити:

- завдання доступу на рівні серверної бази даних;
- обмеження доступу на рівні інтерфейсу, коли ряд дій не може бути виконаний через призначений для користувача інтерфейс, але доступний в разі написання окремої програми.

Забезпечення конфіденційності інформації здійснюється с допомогою криптографічних методів захисту даних. Їх застосування дозволяє не порушити конфіденційність документа навіть в разі його попадання в руки стороннього особи. Будь-який криптографічний алгоритм має таку властивість, як криптостійкість, тобто і його захисту є межа. Немає шифрів, які не можна було б зламати, - це питання тільки часу і коштів. Ті алгоритми які ще кілька років тому вважалися надійними сьогодні вже успішно зламуються. Тому для забезпечення конфіденційності слід переконатися, що за час, витрачений на злом зашифрованою інформацією, вона або безнадійно застаріє, або кошти, витрачені на її злом, перевершать вартість самої інформації.

При організації електронного документообігу необхідно забезпечити юридичну значимість електронних документів відповідно до законодавства. Це завдання можна вирішити, використовуючи систему електронного цифрового підпису (ЕЦП) та інфраструктуру управління відкритими ключами PKI. Основний принцип роботи ЕЦП заснований на технології шифрування з асиметричним ключем, при якій ключі для шифрування і розшифрування даних різні: є закритий ключ, який дозволяє зашифрувати інформацію, і відкритий ключ, за допомогою якого можна цю інформацію розшифрувати, але з його допомогою неможливо зашифрувати цю інформацію. Таким чином, власник цифрового підпису повинен володіти закритим ключем і не допускати його передачу інші особам, а відкритий ключ може поширюватися публічно для перевірки справжності цифрового підпису, отриманого за допомогою закритого ключа. В Україні правовий статус ЕЦП визначається та регулюється Законом України «Про електронний цифровий підпис» № 2155-VIII, а механізм цифрового підписування установлений Державним Стандартом України 4145-2002.

Висновки

При формуванні захисту електронного документообігу необхідно об'єктивно оцінити можливі загрози і ризики СЕД і величину можливих втрат від реалізованих загроз. Захист СЕД не зводиться тільки лише до захисту документів і розмежування доступу до них. Необхідно забезпечити захист апаратних засобів, системи, персональних комп'ютерів, принтерів і інших пристроїв; захист мережевий середовища, в якому функціонує система; захист каналів передачі даних і мережевого обладнання. На кожному рівні захисту важливу роль відіграє комплекс організаційних заходів (інструктаж, підготовка персоналу до роботи з конфіденційною інформацією). Захист системи електронного документообігу повинна бути комплексною.

Література

1. «Про електронні документи та електронний документообіг» : Закон України №851-IV від 22 травня 2003 р. / Відомості Верховної Ради України (ВВР), 2003, № 36, ст.275.
2. «Про електронний цифровий підпис» : Закон України № 2155-VIII від 05 жовтня 2017 р. / Відомості Верховної Ради України (ВВР), 2017, № 45, ст.400.
3. Електронний документообіг [Електронний ресурс] Режим доступу: World Wide Web. – URL: http://documentooborot.com/

КОНЦЕПТУАЛЬНІ ОСНОВИ ПРОВЕДЕННЯ КОМПЛЕКСНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

к.т.н., с.н.с. Ю.М. Щебланін
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій

В наш час неможливо представити існування людини, підприємства (організації), компанії та взагалі Держави без використання сучасних рішень в сфері інформаційних технологій (ІТ). На сьогодні багато компаній вирішують задачі створення системи інформаційної безпеки (ІБ) їх ІТ- інфраструктури, яка б відповідала всім стандартам в області ІБ і сучасним вимогам захисту інформації за параметрами конфіденційності, цілісності та доступності. Це важливо не лише для «молодих» компаній, що розвивають свій бізнес з використанням сучасних технологій управління, а й для підприємств і організацій, що давно працюють на ринку, яким необхідно модернізувати існуючу у них систему ІБ.

Одним із напрямків вирішення зазначеного питання є проведення аудиту ІБ який може надати об'єктивну оцінку захищеності будь якого підприємства або установи, а також попередити реалізацію потенційних загроз. Результат перевірки є основою для розробки подальшої стратегії та розвитку ІБ.

Основними видами аудиту ІБ є [1 с.10, 2]:

- експертний аудит ІБ, під час якого виявляються недоліки у системі заходів захисту інформації на основі досвіду експертів, що беруть участь у процедурі аудиту;
- аудит ІБ на відповідність міжнародним стандартам, наприклад, стандартам ISO/IEC 27001, Cobit та ін.;
- активний аудит, головним завданням якого є оперативне виявлення підозрілої активності і надання засобів для автоматичного реагування на неї. Під підозрілою активністю розуміють поведінку користувача або компоненти інформаційної системи, яка є зловмисною (відповідно до заздалегідь визначеної політики безпеки) або нетиповою (згідно з прийнятими критеріями);
- комплексний аудит, що включає в себе всі перераховані вище форми проведення обстеження.

Комплексний аудит інформаційної безпеки підприємства - це комплекс організаційно-технічних заходів, що проводяться незалежними експертами, з оцінки функціонування існуючої системи забезпечення ІБ замовника.

В якості об'єкта аудиту може виступати як ІТ-інфраструктура підприємства в цілому так і її окремі складові, що забезпечують обробку зберігання та передачу інформації з дотриманням вимог до захисту інформації.

Метою проведення комплексного аудиту є перевірка системи ІБ замовника на відповідність існуючим стандартам і нормативним документам в

області захисту інформації та розробка рекомендацій щодо усунення виявлених невідповідностей.

Комплексний аудит ІБ підприємства включає проведення:

- мережевого аудиту (аналіз захищеності корпоративної інформаційно-телекомунікаційної системи);
- аудиту ІБ підприємства (аналіз захищеності системи забезпечення ІБ).

Основними завданнями аудиту інформаційно-телекомунікаційної системи (ІТС) є:

- незалежна оцінка поточного стану ІБ ІТС підприємства;
- визначення і усунення вразливостей ІТС;
- техніко-економічне обґрунтування механізмів забезпечення безпеки;
- забезпечення відповідності використовуваних засобів і комплексів технічного захисту інформації вимогам чинного законодавства (міжнародним стандартам);
- мінімізація збитків від потенційних вразливостей;
- оптимізація мережевої інфраструктури;
- навчання спеціалістів замовника.

Основними завданнями аудиту ІБ підприємства є:

- планування (проектування) системи забезпечення ІБ;
- обстеження, документування та збір інформації;
- аналіз отриманих даних і загроз безпеці;
- розробка рекомендацій;
- підготовка та затвердження звітних документів.

Сертифіковані фахівці, які проводять аудит можуть використовувати методику проведення аудиту, яка включає:

- методи аналізу захищеності системи ІБ, включаючи тест на проникнення, аналіз конфігурації засобів захисту інформації, аналіз сценаріїв здійснення потенційних атак;
- проведення анкетування співробітників підприємства;
- документування системи ІБ і аналіз ризиків;
- аналіз організаційно-нормативної бази підприємства по забезпеченню режиму ІБ;
- оцінка процесів забезпечення ІБ на підприємстві, кваліфікації співробітників, знання співробітниками своїх посадових обов'язків і рівня їх обізнаності в питаннях ІБ;
- оцінка достатності фізичних механізмів безпеки та ін.

За результатами проведення аудиту готується звіт про поточний стан ІБ підприємства, який містить розгорнуті рекомендації щодо оптимізації (розробки та впровадження) системи забезпечення ІБ як за рахунок організаційних заходів, так і за рахунок застосування спеціальних засобів захисту інформації з оцінкою можливостей використання наявних програмних і технічних засобів.

При цьому у звіті має бути відображено:

- короткий опис об'єкта обстеження;

- виявлені загрози та вразливості ІБ замовника;
- якісний аналіз виявлених загроз і вразливостей;
- оцінку наслідків реалізації загроз (інформаційних ризиків);
- рекомендації щодо усунення вразливостей, мінімізації або ліквідації загроз (зниження, усунення інформаційних ризиків);

- визначення категорій інформаційних ресурсів, що обробляються та вимог щодо забезпечення їх конфіденційності, цілісності та доступності;
- оцінку рівня кваліфікації персоналу щодо забезпечення ІБ;
- оцінку стану захищеності об’єкту обстеження;
- пропозиції щодо вдосконалення системи ІБ замовника.

Зазначені пункти звіту можуть поєднуватись або розширюватись з проведенням більш глибокої деталізації, все це залежить від обєму послуг з проведення аудиту, які визначив замовник та рішення особи яка проводить аудит.

ЛІТЕРАТУРА

1. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

2. Ю.М. Щебланін Аналіз використання моделей зрілості процесів в ході оцінювання рівня інформаційної безпеки / Ю.М. Щебланін, А.Б. Гребенніков // Сучасний захист інформації. – 2018. – № 1(33). – С. 33–38.

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Колісник Денис Русланович

Захист інформаційних систем від загроз в даний час є одним з найбільш актуальних завдань в області захисту інформації. Щорічні втрати від комп'ютерних вразливостей оцінюються в десятки і сотні мільярдів доларів. Вразливості в інформаційній системі є в даний час однією з найбільш значущих загроз інформаційної безпеки. Високі вимоги до оперативності інформаційних процесів в різних областях діяльності сучасного суспільства, а також розширення можливостей мережевої побудови інформаційних систем і впровадження методів розподіленої обробки даних за рахунок реалізації мережевого доступу до обчислювальних засобів призвело до інтегрування систем обробки інформації і систем її обміну. Результатом такого інтегрування стало створення інформаційних систем.

Інформація та інформаційні системи (ІС) 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 до переходу на розподілені обчислювальні системи обмежує

можливості фахівців централізовано контролювати ІС та мережеве оточення [1].

Порушення режиму безпеки ІС може істотно ускладнити реалізацію виробничих завдань, тому вирішення проблеми формування ефективної системи захисту інформації (ЗІ) набуває дуже важливого значення. Це пояснюється тим, що у процесах розроблення й удосконалення систем ЗІ є чимало недостатньо вивчених і досліджених аспектів, які можуть негативно впливати на показники ефективності та надійності функціонування системи безпеки загалом. Вимогою сьогодення є необхідність вирішення питань фізичної безпеки, управління інцидентами, виконання законодавчих актів, стандартів, настанов. Останнім часом спостерігається тенденція до збільшення кількості порушень в області комп'ютерних злочинів, 2018 рік став роком апаратних вразливостей, їх поява в серйозних сценаріях атак змусила підприємства переосмислити підхід до безпеки своїх систем в цілому. Беручи до уваги різноманітність загроз і складність сучасної мережі, реалізація рішення для захисту потребує глибоких знань і досвіду.

Мережеві сканери є актуальними засобами для виявлення вразливостей в корпоративній інформаційній системі. Вони призначені для виявлення виключно відомих вразливостей, опис яких є у базі даних. У цьому вони подібні антивірусним системам, яким для ефективної роботи необхідно постійно оновлювати базу даних сигнатур [2]. Найбільшого розповсюдження набули засоби аналізу захищеності мережевих сервісів і протоколів. Крім виявлення вразливостей за допомогою засобів аналізу захищеності, можна швидко визначати всі вузли корпоративної мережі, доступні у момент проведення тестування, виявити всі використовувані в ній сервіси і протоколи, їх налаштування і можливості для виконання несанкціонованої дії. Також ці засоби розробляють рекомендації та заходи, які дозволяють ліквідувати виявлені недоліки.

Література

1. Киричок Р.В. Тест на проникнення як імітаційний підхід до аналізу захищенності корпоративних інформаційних систем. Киричок Р.В. // Сучасний захист інформації – 2018. – № 2. – С. 53-58.
2. COMPARE NESSUS WITH INDUSTRY VULNERABILITY ASSESSMENT SOLUTIONS // [Електронний ресурс]. Режим доступу: World Wide Web. – URL: https://www.ibm.com/security/data-breach

ПОШИРЕНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ «РОЗУМНІЙ БУДИНОК»

Семенова Інна Дмитрівна

На сьогоднішній день Інтернет речей один з найбільш перспективних напрямків розвитку технологій. IoT (Interenet of Things (англ.) – Інтернет речей) застосовується неймовірно широко - від спрощення щоденної рутини кожної людини, до автоматизації виробництва. Однією з гілок Інтернету речей є система "Розумний будинок", яка дозволяє інтегрувати набір самостійних технологій, таких як керування світлом, кліматом, шторами, охоронною системою, в єдину систему управління будинком (офісом, заводом) за допомогою системної інтеграції на базі, як правило, певної технології (KNX, Crestron і т.д.). Але, як і будь-яка мережева технологія, «Розумний будинок» схильний до всіляких ризиків інформаційної безпеки, таких як порушення цілісності, доступності , конфіденційності, тощо, розглянемо деякі, найбільш характерн,і уразливості.

Розглянемо, як в цілому будується система розумного будинку:

1. Обирається одна (інколи 2) технології на базі яких буде будуватися система, це може бути шинна або мережева технологія, у сучасному світі, майже завжди, використовується мережева. В результаті чітко визначаються протоколи комунікації між пристроями у системі.

2. Проектується система - формально або не формально перелічується усе, чим потрібно керувати, зазвичай це світло, штори, клімат, охоронна система (фізичний периметр, система протизатоплення, відеоспостереження, контроль доступу).

3. Етап програмування.

4. Впровадження системи до вже існуючої мережі або побудова мережі з врахуванням «Розумного будинку».

Одразу можна побачити, що більше всього проблем, з точки зору інформаційної безпеки буде з недоліками та уразливостями безпосередньо технологій інтеграції та мережевими уразливостями. Не варто відмежовувати їх один від одного, оскільки вони нероздільно взаємопов’язані.

Першою, і найбільш поширеною проблемою системи розумного будинку є слабке або, навіть, відсутнє шифрування, загалом, це вирішується використанням примусового шифрування в усій мережі або підбором обладнання з таким функціоналом.

Друге, неправильно налаштоване віддалене підключення. Як правило, використовується VPN-підключення зі стандартнім налаштуванням, або «пере направлення портів», знову ж таки, зі стандартними відкритими портами. Подібне нехтування може призвести до того, що, хто завгодно зможе підключитися до керування системою. Проблема вирішується використанням нестандартних портів, або використанням SSL-сертифікатів, або використанням 2 факторної автентифікації.

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

Четверте, маскування під легітимною MAC адресою - зловмисник знаходиться в мережі з параметрами дозволеного пристрою, це дозволяє перехоплювати певну інформацію або «підставити» пристрій – власник буде

вважати, що це його пристрій «збожеволів» та атакує мережу. Найпростіше рішення – гарантована авторизація пристроїв у мережі після кожного перепідключення.

П’яте, порушення електропостачання – нажаль, дуже часто, власники або інтегратори нехтують необхідністю встановлення пристрою гарантованого електропостачання або генератора. Перебої можуть призвести до виходу зі строю елементів системи, порушенню роботи програми автоматизації, відключенню або збоям в роботі ППК – усе це може призвести до нелегітимного доступу, як до інформації, що циркулює в системі, так і безпосередньо до об’єкту. Проблема вирішується встановленням пристрою гарантованого живлення або незалежного джерела електропостачання.

Висновки: На сьогоднішній день системи IoT не є цілком захищеними, як результат, система розумного будинку також. Це відносно молода технологія, яка активно розвивається зараз, тому необхідно дуже прискіпливо підбирати обладнання, налаштовувати систему та будувати архітектуру мережі. Адже, навіть невеличка помилка може призвести до втрати надзвичайної кількості конфіденціальної інформації.

Література

1. https://sites.google.com/site/theocsic/technologies/securitynet/dhcp-spoofing
2. *В. Архипов «Системы для интеллектуального здания»*
3. https://xakep.ru/2002/01/24/14341/

ВІРУСИ ТА ЇХ ВПЛИВ НА ВИТОКИ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Цесарський Валерій Андрійович

Анотація

Захист інформації неможливо регламентувати через різноманітність існуючих видів інформації, що обробляється. Конкретні заходи визначаються виробничими, фінансовими та іншими можливостями підприємства, обсягом конфіденційної інформації та її значущістю. Система заходів, спрямована на недопущення несанкціонованого доступу до інформації, її модифікації, втрати, знищення, порушення цілісності тощо. Одним із видів захисту персональних даних є встановлення антивірусної програми. Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Актуальність даної теми обумовлена високими темпами захисту комп’ютерних мереж від впливу різних шкідливих програм, метою яких є пошкодження комп’ютера і системи та володіння конфіденційними даними користувача.

На сьогоднішній день захист інформації передбачає систему заходів, спрямованих на недопущення несанкціонованого доступу до інформації, її

модифікації, втрати, знищення, порушення цілісності тощо, а контроль за національним інформаційним простором – заходи щодо мінімізації збитків від здійснення як іноземними державами, так і внутрішніми організаціями підривних психологічних операцій. Рівень захисту визначають для кожного певного виду інформації окремо. Одним із видів захисту персональних даних є встановлення антивірусної програми [4].

Оскільки віруси не виникають самі по собі в результаті електромагнітних колізій, а створюються людьми, то для відповіді на це питання слід розібратися в психології тих індивідуумів, які створюють "шкідливе" програмне забезпечення, у побуті називається "вірусами". Найбільш ймовірними причинами створення і розповсюдження шкідливого програмного забезпечення є шахрайство та хуліганство [4].

Комп'ютерний вірус - це шкідливий саморозповсюджуємий в інформаційному середовищі програмний код. Він може впроваджуватися в виконувані і командні файли програм, поширюватися через завантажувальні сектори жорстких дисків, документи офісних додатків, через електронну пошту, web-сайти тощо. Основну масу вірусів створюють студенти та школярі, які тільки що вивчивши мову асемблера, хочуть спробувати свої сили [4].

Другу групу складають також молоді люди (частіше - студенти), які ще не повністю оволоділи мистецтвом програмування, але вже вирішили присвятити себе написанню та розповсюдженню вірусів. Як правило, вони створюють численні модифікації "класичних" вірусів, або віруси вкрай примітивні і з великою кількістю помилок [4].

Третя група авторів вірусів - "дослідники". Ця група складається з талановитих програмістів, які займаються винаходом принципово нових методів зараження, приховування, протидії антивірусам і т.д. Ці програмісти пишуть віруси не заради власне вірусів, а швидше ради "дослідження" потенціалів "комп'ютерної вірусології" [4].

При зараженні комп'ютера вірусом важливо його знайти, для цього слід знати основні ознаки його прояву:
- припинення роботи або неправильна робота раніше успішно функціонуючих програм;
- повільна робота комп'ютера;
- неможливість завантаження операційної системи;
- зникнення файлів і каталогів або перекручування їхнього вмісту;
- зміна розміру файлів або збільшення кількості файлів на диску;
- істотне зменшення розміру вільної оперативної пам'яті;
- часті зависання і збої в роботі комп'ютера [3].

На сьогоднішній день відомі десятки тисяч різних вірусів. Їх можна класифікувати за такими ознаками:
- середовище проживання;
- спосіб зараження середовища перебування;
- ступінь впливу;
- особливості алгоритму [2].

У залежності від середовища перебування віруси ділять на:
- мережеві - поширюються по різним комп'ютерним мережам;
- файлові - вражають файли з розширенням com, exe, рідше sys або оверлейні модулі exe файлів;
- завантажувальні - отримують управління на етапі ініціалізації комп'ютера, ще до початку завантаження ОС;
- файлово-завантажувальні - комбіновані віруси, які об'єднують властивості файлових і завантажувальних [3].

За способом зараження середовища перебування віруси діляться на:
- резидентні - при зараженні (інфікуванні) комп'ютера залишає в оперативній пам'яті свою резидентну частину, яка потім перехоплює звернення ОС до об'єктів зараження (файлів, завантажувальних секторів дисків і т. п.) і впроваджується в них;
- нерезидентні - не заражають пам'ять комп'ютера і є активними обмежений час [2].

За ступенем впливу віруси можна розділити на:
- безпечні - не заважають роботі комп'ютера, але зменшують обсяг вільної оперативної пам'яті і пам'яті на дисках, дії таких вірусів виявляються в яких-небудь графічних або звукових ефектах;
- небезпечні - можуть призвести до різних порушень в роботі комп'ютера;
- особливо небезпечні - їх вплив може привести до втрати програм, знищення даних, стирання інформації в системних областях диска [2].

Крім вірусів прийнято виділяти ще, принаймні, три види шкідливих програм. Це троянські програми, логічні бомби і програми-черв'яки [1].

Антивірус - це спеціалізована програма, призначена для захисту операційної системи від вірусів, шпигунських програм, хакерських атак і іншого несанкціонованого доступу з метою крадіжки цінних особистих даних. Антивірусні програми можна розділити на кілька типів:
- детектори - виявляють віруси;
- доктора (Фагі. Фаг) - це програми, які здатні не тільки виявити, а й знищити вірус, тобто видалити його код із заражених програм і відновити їх працездатність (якщо можливо);
- ревізори - контролюють можливі шляхи розповсюдження програм-вірусів і зараження комп'ютерів;
- вакцини - антивірусні програми, що ведуть себе подібно вірусам, але не завдають шкоди [1].

На переконання експертів, завдання забезпечення інформаційної безпеки повинно вирішуватися системно. Це означає, що різні засоби захисту (апаратні, програмні, фізичні, організаційні і т. д.) мають застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні "знати" про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз [3].

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками,

що зберігаються в антивірусній базі. Захист від вірусів може бути встановлений на робочі станції, файлові і поштові сервери, міжмережеві екрани. Своєчасне виявлення заражених вірусами файлів і дисків, повне знищення виявлених вірусів на кожному комп'ютері дозволяють уникнути поширення вірусної епідемії на інші комп'ютери [4].

Головною зброєю в боротьбі з вірусами є антивірусні програми. Вони дозволяють не тільки виявити віруси, що використовують різні методи маскування, але і видалити їх з комп'ютера [3].

З усього вищесказаного можна сміливо зробити висновок, що необхідність захисту від комп'ютерних вірусів на даний момент стоїть на першому місці. Якщо правильно вибирати антивірусне програмне забезпечення та регулярно оновлювати його, можна уникнути зараження вірусом і відповідно всіх його наслідків.

Перелік використаної літератури:

1. Інформатика – базовий курс. – Доступний зhttp://www.zhu.edu.ua/mk_school/mod/.
2. Антивіруси та їх види. – Доступний з http://vadimkoshka.blogspot.com/.
3. Всі загрози. – Доступний з http://www.viruslist.com.
4. Всеосвіта. Поняття комп’ютерного вірусу. – Доступний з https://vseosvita.ua/library/tema-ponatta-komputernogo-virusu-istoria-ta-klasifikacia-virusiv-i-troanskih-program-priznacenna-princip-dii-ta-klasifikacia-antivirusnih-program-81906.html.

АНАЛІЗ ОСОБЛИВОСТЕЙ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ З КОМУТАЦІЄЮ ПАКЕТІВ

Штомпель М.А., Штомпель Т.В.

Показано, що при забезпеченні інформаційної безпеки телекомунікаційних мереж з комутацією пакетів важливу роль відіграє питання виявлення атак. Представлено класифікацію систем виявлення вторгнень в залежності від місця їх розташування у телекомунікаційній мережі. Наведено відомості щодо основних підходів та методів, що можуть бути використані при технічній реалізації модулю виявлення атак. Показано, що реалізація даного модулю на основі технологій машинного навчання характеризується хорошими показниками ефективності.

Необхідність впровадження сучасних інформаційних послуг призводить до широкого розповсюдження телекомунікаційних мереж з комутацією пакетів, що побудовані на основі стеку протоколів TCP/IP. При цьому постійно зростають вимоги щодо забезпечення рівня інформаційної безпеки у даних телекомунікаційних мережах [1, с. 10].

Однією з актуальних задач при організації захищеної передачі даних у телекомунікаційних мережах на основі стеку протоколів TCP/IP є виявлення атак та запобігання їх впливу на працездатність мережі. Для цього

використовуються системи виявлення вторгнень, які можна розділити на такі види: мережеві системи виявлення вторгнень, що розташовуються на межі двох мереж; системи виявлення вторгнень окремого вузла, що аналізують потік даних, який надходить на конкретний сервер; системи виявлення вторгнень хосту, що розгортаються на заданому хості мережі [2, с. 254].

Ефективність систем виявлення вторгнень залежить від компонентного складу та технологій, що використовуються при їх технічній реалізації. При цьому ключову роль при побудові даних систем відіграє модуль виявлення атак, що може бути реалізований з використанням різних підходів та процедур. У [3, с. 102] проаналізовано підходи до аналізу даних на основі експертної оцінки та машинного навчання. Показано, що для вирішення задачі виявлення атак можуть бути використані методи, що засновані на математичному апараті статистичного аналізу, кластерного аналізу, нейронних мереж, імунних мереж, опорних векторів, експертних систем та сигнатур. За результатами аналізу визначено, що застосування технологій машинного навчання при реалізації модулю виявлення атак дозволяє отримати достатньо хороші показники ефективності. Перспективним напрямом подальших досліджень є отримання кількісних показників щодо обчислювальної складності технічної реалізації модулю виявлення атак на основі різних процедур машинного навчання.

Перелік використаної літератури

1. Толюпа, С.В. Побудова мультисервісних мереж на концепції NGN та проблеми захисту інформації в них / С.В. Толюпа, Н.І. Кунах // Наукові записки Українського науково-дослідного інституту зв'язку. – К: УНДІЗ, 2011. – № 3(19). – С. 10 – 15.

2. Скабцов, Н. Аудит безопасности информационных систем [Текст] / Н. Скабцов. – СПб.: Питер, 2018. – 272 с.

3. Рубан, І.В. Класифікація методів виявлення аномалій в інформаційних системах [Текст] / І.В. Рубан, В.О. Мартовицький, С.О. Партика // Системи озброєння і військова техніка. – Х: ХНУПС ім. І. Кожедуба, 2016. – № 3(47). – С. 100 – 105.

АНАЛІЗ КЛАСИФІКАЦІЙ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Бржевська Зореслава Михайлівна
Державний університет телекомунікацій, м. Київ

Розглянуто дефініція загрози інформаційної безпеки. Проаналізовано Проект концепції інформаційної безпеки України, Закони України «Про основи національної безпеки України», «Про Основні засади розвитку інформаційного суспільства в України на 2007-2015 роки», Доктрину інформаційної безпеки. Встановлено, що Проект Концепції інформаційної безпеки України, поряд з Доктриною визначають множину загроз інформаційній безпеці держави, які мали прояв в інформаційному просторі.

У загальному випадку під загрозою ІБ будемо розуміти дефініцію, сформульовану у підготовленому Проекті Концепції інформаційної безпеки України [1].

Закон України “Про основи національної безпеки України” визначає, що загрози національній безпеці України в інформаційній сфері зводяться до [2] : обмеження свободи слова і доступу до публічної інформації; поширення у ЗМІ культу насильства, жорстокості, порнографії; комп’ютерної злочинності та тероризму; розголошення інформації з обмеженим доступом; маніпулювання суспільною думкою.

Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки” безпосередньо не визначає види загроз ІБД, але встановлює напрямки їх реалізації [3].

У Доктрині інформаційної безпеки України уточнено перелік актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері в умовах збройної агресії Російської Федерації [4].

Запропонований експертною радою при Міністерстві інформаційної політики України (МІПУ) Проект Концепції інформаційної безпеки України [1] формулює засади функціонування СЗІБД. Даний документ, поряд з Доктриною, визначає множину загроз ІБД, які мали прояв у національному інформаційному просторі.

Комунікативні загрози ІБД пов’язані з реалізацією потреб особи, суспільства і держави щодо створення, споживання, розповсюдження та розвитку національного стратегічного контенту. Технологічні загрози ІБД проявляються під час функціонування та забезпечення захисту кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну складову державного інформаційного простору [1].

Таким чином, в Україні, як і у всьому світі, прослідковується поступове збільшення кількості нових і доопрацьованих нормативно-правових документів у сфері ІБД, які закріплюють фундаментальні засади формування, захисту та сталого розвитку національного інформаційного простору. При цьому відмінність у способах визначення видів загроз ІБД пояснюється різними цілями систематизації та вибором ознак.

Список використаних джерел:

1. Міністерство інформаційної політики України. (2015, Черв. 5). Проект Концепції інформаційної безпеки України. [Електронний ресурс]. Доступно: http://mip.gov.ua/documents/30.html. Дата звернення: Лист. 07, 2017.

2. Верховна Рада України. (2003, Черв. 19). Закон України № 964-15, Про основи національної безпеки України. [Електронний ресурс]. Доступно: http://zakon2.rada.gov.ua/laws/show/964-15. Дата звернення: Лист. 07, 2017.

3. Верховна Рада України. (2007, Січ. 09). Закон України №537-16, Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. [Електронний ресурс]. Доступно: http://zakon4.rada.gov.ua/laws/show/537-16.

4. Офіційне представництво Президента України. (2017, Лют. 25). Указ Президента України №47/2017, Доктрина інформаційної безпеки України. [Електронний ресурс]. Доступно: http://www.president.gov.ua/documents/472017-21374.

ІНСАЙДЕРСЬКА ЗАГРОЗА ЯК ОДНА З АКТУАЛЬНИХ ПРОБЛЕМ

КІБЕРБЕЗПЕКИ. ОСНОВНІ МЕТОДИ ВИЯВЛЕННЯ

Коваленко Сергій Володимирович

Розвиток новітніх технологій та потреби бізнесу спричинили прорив в створенні інформаційних систем та появу корпоративних інформаційних систем. Однак, в свою чергу, це стало приводом для появи нового типу загроз – внутрішня (інсайдерська) загроза. Великі інсайдерські загрози стали заголовками в останні роки, і дослідження показують, що майже 60% атак походять від зловмисних або випадкових інсайдерських дій. В результаті організації можуть зіткнутися зі значною втратою даних. Саме для протидії цьому було створено як малі рішення кібербезпеки, так і масштабні системи, які здатні шляхом моніторингу дій користувачів виявляти підозрілу активність, яка може вилитися в інсайдерську діяльність.

Пошук внутрішнього порушника інформаційної безпеки є одним з пріоритетних напрямків в роботі служби безпеки організацій. Внутрішній порушник має відомості про роботу комп'ютерної системи, вірогідно знайомий з співробітниками, що обслуговують і адмініструють КС, має ряд дозволів на доступ до внутрішньої інформації, може знати парольну інформацію колег, має фізичний доступ до деяких комп'ютерів. Крім того, внутрішній порушник менш обмежений в діях засобами захисту інформації на відміну від зовнішнього порушника.

Інсайдерські дії негативно впливають на систему, з якою вони працюють. Видами шкідливих дій можуть бути: крадіжка інтелектуальної власності, IT-саботаж, шахрайство (крадіжка конфіденційних даних), шпигунство, випадкові ненавмисні дії тощо. З’ясовано, що особливість виявлення інсайдерів полягає в тому, що, як правило, їхні дії не спрямовані на подолання засобів або систем захисту інформації, так як останні просто не діють на них. Інсайдери діють в рамках наданих їм повноважень і використовують наявні у них знання і інформацію про КС для нанесення шкоди.

З’ясовано, що на даний момент існує декілька загальних методів виявлення внутрішньої (інсайдерської) загрози в корпоративних інформаційних системах:

1. Data leakage protection (DLP-системи).

На даний момент існує досить велика кількість dlp-систем [1] (data leakage protection - система запобігання витокам інформації) або їм подібних програм, що дозволяють виявляти витік конфіденційної інформації та нелояльних співробітників.

DLP-системи ґрунтуються на перехопленні інформації, переданої користувачем комп'ютерною мережею та на периферійні пристрої (принтери, USB-носії тощо). В окремих випадках система може контролювати роботу самого користувача – здійснювати перехоплення клавіатури, знімків екрану та ін.

Виділяються кілька типів DLP-систем.

Перший – шлюзові DLP-системи, які встановлюються на центральних вузлах локальної мережі. При такому підключенні DLP-система залишається прихованою від користувачів КС. Інформація на сервер DLP-системи надходить або з комутатора (або спеціально налаштованого маршрутизатора), або безпосередньо програмно з сервісу комп’ютерної системи (КС) (агент DLP-

системи встановлюється на один сервер з сервісом КС, наприклад з проксі-сервером, і передає інформацію на DLP- сервер).

Другий тип DLP-систем – хостові системи, тобто системи, що встановлюються безпосередньо на ПК користувача.

Комбіновані системи використовують обидва типи установок. На сьогодні комбіновані системи набули найбільшого поширення.

Існує кілька видів обробки перехопленої і приведеної до загального формату інформації. Мета обробки – серед потоку даних знайти надходження конфіденційної інформації.

Основні використовувані алгоритми:

1) Пошук за регулярними виразами (перехоплення даних певного формату, наприклад номер паспорта, ПІБ і т. д.).

2) Пошук подібних (цифрові відбитки і т. д.) - пошук певних шаблонів в документах.

3) Сигнатурний аналіз (пошук входжень тексту).

4) Лінгвістичний пошук (пошук з урахуванням особливостей мови і мовних виразів).

5) Розпізнавання тексту із зображень і подальший аналіз і ін.

Проте такими системами не запобігти загроз цілісності та доступності конфіденційної інформації. Крім того, використання DLP-систем обмежено на законодавчому рівні (таємниця листування, таємниця особистого життя та ін.). В наш час компаніям при впровадженні DLP слід отримати юридичну консультацію і провести ряд організаційних заходів.

2. Honeypot.

До засобів виявлення порушника відносяться системи «honeypot» (з англ. - «горщик з медом»). Honeypot – це муляж будь-якої частини КС, наприклад СУБД, мережевого сервісу або виділеного сервера. Honeypot повинен бути невідомий користувачам КС. Основна мета honeypot – привернути увагу порушника. Honeypot спрацьовує і сигналізує адміністратору системи про обстеження або спробу злому муляжу. Honeypot може реалізовуватися як на окремому фізичному сервері, так і у віртуальному середовищі [2].

До переваг honeypot відносяться: мале число помилкових спрацьовувань в порівнянні з «традиційними» засобами захисту інформації (будь-яке звернення до honeypot вже є тривожним знаком), перехоплення невідомих раніше атак, велика гнучкість, що дозволяє адаптувати honeypot до будь-якої КС, мінімальна кількість програмно-апаратних ресурсів навіть для великої КС.

Для створення цієї «інсайдерської пастки» в мережі використовують Honeynet, який являє собою об'єднання двох і більше фізичних honeypot в одну мережу. Однією з вимог побудови honeynet є схожість елементів honeynet с вузлами, використовуваними в КС: базами даних, веб-серверами і т. д. Усі звернення до елементів honeynet фіксуються і досліджуються фахівцями. Таким чином, honeynet дозволяє досліджувати дії, прийоми і тактику порушника.

Крім honeypot використовуються і так звані honeytoken. Honeytoken, на відміну від honeypot, не передбачає наявність апаратної частини. Honeytoken

являє собою своєрідну приманку: інформацію, яка може зацікавити зловмисника. При цьому в дійсності вона не є цінною для організації. Інформація подається у вигляді файлу, запису в базі даних, пари логін/пароль таким чином, щоб переміщення honeytoken можна було відстежувати. До honeytoken створюється вільний доступ. Відстеження переміщень проводиться за допомогою міток, що перехоплюються системами виявлення вторгнень. Про кожне переміщення сповіщується адміністратор безпеки.

3. Security Information and Event Management.

SIEM-системи (англ. Security Information and Event Management) - системи, що складаються з агентів, що встановлюються на різних частинах КС, механізму, що приводить дані до єдиної форми, і механізму, що аналізує отримані від агентів дані. SIEM-система використовується при керуванні ризиками ІБ, виявленні порушення ІБ, аналізі та розборі інциденту ІБ, створенні рекомендацій щодо протидії порушникам в разі виявлення загрози ІБ[3].

Основне завдання SIEM-системи - фіксувати події, що відбуваються в КС, і сповіщати співробітника служби ІБ про події, що передували атаці на КС.

У SIEM-системах використовується велика кількість різних математичних алгоритмів для обробки та аналізу отриманих подій. SIEM-система здатна виявляти: відому і описану правилами загрозу, типову загрозу, аномальну поведінку користувачів, відхилення від жорстко заданих правил роботи в КС, причинно-наслідковий зв'язок між подіями (при використанні алгоритмів кореляції на основі графів, статистичних методів, байєсівської ймовірності).

Навіть без використання спеціальних алгоритмів деякі події, перехоплені SIEM-системою, можуть безпосередньо сигналізувати про інсайдерську атаку. Наприклад: подключення до комп'ютерної мережі через VPN у позаробочий час, збільшення мережевої активності та ін.

4. Програми tripwire .

Одним із способів виявлення порушника є програми tripwire (пер. з англ. - «загородження», «натягнутий дріт»), які відстежують зміни в конфігураційних і інших файлах і сповіщають про це адміністратора КС. При першому запуску система обчислює хеш-функції від важливих файлів КС і далі до заданого адміністратором періодом відстежує зміни в файлах.

Описавши системи виявлення внутрішньої загрози, було прослідковано залежність між напрямком шкідливої діяльності інсайдерів і типів комплексів засобів та систем захисту [4]:

1. Крадіжка інтелектуальної власності:

DLP-система – здійснює контроль периферійних пристроїв: виведення документів на друк, на зовнішні носії, на мережеві засоби, наприклад Bluetooth, і ін .;

SIEM-система – фіксує аномальну активність користувача, наприклад: збільшення числа звернень до певних документів, числа документів, які надсилаються на друк, електронною поштою, спроби підбору паролів і ін.

2. IT-саботаж:

SIEM-система: найбільш вірогідною дією порушника в такому випадку є створення «бекдорів» і логічних бомб. SIEM-система, завдяки вбудованим алгоритмам графів атак, сигнатурним правилам і правилам кореляції, заданим згідно з політикою ІБ, здатна виявляти подібні загрози;

програми tripwire сповіщають про зміну системних файлів, які можуть залишатися непоміченими тривалий час до перезавантаження сервісу або сервера.

3. Шахрайство, крадіжка даних: аналогічно п. 1, але при цьому DLP-система повинна бути налаштована на перехоплення специфічних видів даних, наприклад фінансових даних, персональних данних і т. д.

4. Шпигунство:

honeypot, honeytoken - при активному пошуку конфіденційних даних зловмисник може знайти, наприклад, файл із спеціально підготовленою парою логін-пароль, вигаданими персональними даними, вигаданої службовою інформацією. Будь-яке використання такого файлу розцінюється як інсайдерська діяльність;

DLP-система: результати шпигунства можуть бути відправлені засобами корпоративної КС;

SM-система: виявлення аномалій в роботі користувачів - збільшень числа звернень до певних документів, збільшень обсягів, переданих по Мережі.

5. Випадкові, ненавмисні дії:

SIEM-система: виявлення відхилень від заданих режимів роботи;

DLP-системи виявляють передачу конфіденційних даних, відправлених помилково.

Література

1. DLP-системи [Електронний ресурс] – Режим доступу: World Wide Web. – https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/
2. Spitzner L. Honeypots: Catching the Insider Threat // Computer-Security Application Conference, 2003. Proceesings, 19th Annual. 2003. P. 170–179.
3. SIEM-системи [Електронний ресурс] – Режим доступу: World Wide Web. – https://itprotect.ru/all-services/solutions/siem
4. Maybury M., Chase P., Cheikes B., Brackney D., Matzner S., Hetherington T., Wood B., Sibley C., Marin J., Longstaff T., et al. Analysis and Detection of Malicious Insiders // International Conference of Intelligence Analysis. McLean. VA. 2005.

АКТУАЛЬНІ ПРОБЛЕМИ ЗАХИЩЕНОСТІ ХМАРНИХ ТЕХНОЛОГІЙ

Бойко Олексій Петрович
студент магістратури
ННІ захисту інформації
Державного

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

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

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

Основними загрозами на сьогодні для хмарних технологій на сьогодні є:

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

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

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

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

Серед нападів, які зазнали респонденти в опитуванні хмарної безпеки в

2019 році, найчастішим методом нападу було викрадення облікових записів або облікових даних. Погані конфігурації, що ведуть до публічного впливу, були другими, а привілейовані зловживання користувачами - третіми. Інші методи, що повторюються, включають невпевнений компроміс із інтерфейсом, тіньові IT (несанкціоновані зловмисне програмне забезпечення службовців), атаки "відмова в обслуговуванні" та ексфільтрацію даних із певного хмарного додатка [2].

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

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

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

МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Костюк Петро Петрович

Анотація. Технологія блокчейн стає однією із головних рушійних сил інновацій в глобальній економіці. Її впровадження матиме величезний вплив на те як діють підприємства та уряди і на те як люди організовують своє повсякденне життя. Індустрія фінансових послуг на даний момент зазнає найбільшого впливу блокчейн-революції, а фінансові інституції є одними з найперших користувачів технології. У той же час, сфера морських перевезень, як доволі традиційна індустрія, поки що не має багато прикладів застосування блокчейну, але ця технологія здатна суттєво змінити цю галузь.

Останнім часом все частіше можна почути про технологію Blockchain. В чому ж суть технології та які перспективи її використання?

Blockchain можна описати як публічну базу даних всіх транзакцій, які коли-небудь були зроблені в системі. Вперше термін з'явився як назва розподіленої бази даних, реалізованої в криптовалюті «біткойн».

Коротко роботу блокчейн можна було б описати так: цифрові записи об'єднуються в «блоки». На наступному кроці блоки алгоритмічно зв'язуються в «ланцюжки». Кожен блок пов'язаний з попереднім і містить в собі набір записів. Процес шифрування, відомий як хешування, виконується великою кількістю різних комп'ютерів, що працюють в одній мережі. Якщо всі компютери мережі в результаті розрахунків отримують однаковий результат, то блоку присвоюється унікальний цифровий підпис. Таким чином підробити його неможливо. До нього можна тільки додавати нові записи. Важливо врахувати те, що реєстр оновлюється на всіх комп'ютерах в мережі одночасно.

Така технологія роботи для розподілених баз даних практично унеможливлює злам, адже для цього необхідно було б отримати доступ до всіх компютерів мережі одночасно. Разом з тим технологія є гнучкою в сенсі забезпечення публічності роботи компютерних систем.

Загалом типізувати блокчейн можна наступним чином [1]:

- Відкритий блокчейн (англ. Public blockchain) – блокчейн, в якому не існує обмежень на читання даних блоків і обмежень на відсилання транзакцій для включення в блокчейн.
- Закритий блокчейн (англ. Private blockchain) – блокчейн, в якому прямий доступ до даних і до відправки транзакцій обмежений певним вузьким колом організацій.
- Загальнодоступний блокчейн (англ. Permissionless blockchain) – блокчейн, в якому не існує обмежень на особистість обробників транзакцій.
- Ексклюзивний блокчейн (англ. Permissioned blockchain) – блокчейн, в якому обробка транзакцій здійснюється певним списком суб'єктів особистості яких встановлено.

Сьогодні активними користувачами цієї технології є криптовалюти, зокрема найвідоміша з них – біткойн. Ринок криптовалют швидко розвивається, так максимальна капіталізація ринку криптовалют складала 160 млрд. доларів, а курс біткойн перетнув відмітку 5000 доларів [3]. Проте це не єдине ефективне застосування цієї технології, зокрема, ринок стартапів на базі використання технології блокчейн, за оцінками експертів, залучить у 2017 році інвестицій на суму 3 млрд. доларів, що робить технологію альтернативою традиційним венчурним інвестиціям.

Варто звернути увагу, що використання технології блокчейн викликає зацікавлення і в Україні. Так стало відомо, що Україна уклала угоду з міжнародною технологічною компанією Bitfury Group про переведення всіх електронних державних даних на блокчейн [2].

Таким чином стає зрозуміло, що технологія блокчейн до певної міри революційна та може бути використана в різних сферах діяльності суспільства. Зокрема, мова йде про такі реалізації як: медіа платформи, криптовалюти, різного роду реєстри як корпоративного так і державного значення тощо.

Необхідно також відзначити, що існують певні проблеми щодо застосування цієї технології, зокрема, подвійного витрачання та зростання складності мережі.

.Ключові слова: Блокчейн, обробка даних, захист інформації.

Література

https://forklog.com/issledovanie-bitfury-sochetanie-otkrytyh-i-eksklyuzivnyh-blokchejnov-effektivnyj-put-razvitiya-kriptotehnologij/.http://www.espertech.com/esper

https://hightech.fm/2017/04/14/us-ukraine-bitfury-blockchain.

Melanie Swan. Blockchain: Blueprint for a New Economy. – 2015. – 152 p.

ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ ІЗ ЗАХИСТОМ ІНФОРМАЦІЇ В КАБЕЛЬНИХ СИСТЕМАХ ЗВ'ЯЗКУ

Жук Олександр Олександрович *студент Державного Університету Телекомунікацій.*

В даній роботі були розглянуті можливі загрози для комунікаційних систем зв'язку. Також були надані рекомендації для захисту від впливу внутрішніх і зовнішніх втручань та загроз навмисного, природного або штучного характеру для кабельних систем зв'зку. При дотриманні наданих рекомендацій, можна захистити циркулюючу інформацію в кабельних системах зв'язку від окремих загроз витоку та перехоплення.

Інформація, на даний момент, є одним з найцінніших скарбів, який бажають отримати зловмисники, саме тому найголовнішою метою є забезпечення інформаційної безпеки в комунікаційних системах зв'язку. Кабельна система зв'язку, як відомо - це ієрархічна система, що включає в себе всі необхідні компоненти для створення середовища передачі інформації..

Однією з найскладніших і витратних складових телекомунікаційних систем є лінії зв'язку (ЛЗ), якими передаються інформаційні сигнали від одного абонента (станції, передавача, регенератора) іншому (станції, приймачу, регенератору) та у зворотному напрямку.[1, с. 137] Вони є невід'ємною частиною всього комплексу засобів, що забезпечують діяльність будь-якого підприємства, тому і рішення проблем безпеки неминуче зачіпає процес безпечного функціонування ЛЗ.

До ліній зв'язку висувають такі вимоги:

- велика інформаційна ємність (пропускна здатність);
- мале загасання, завдяки чому забезпечується більша відстань одного інтервалу зв'язку;
- захищеність лінії від взаємних і зовнішніх електромагнітних впливів;
- захищеність від механічних пошкоджень і температурних коливань;
- стабільність електричних параметрів у часі;
- мінімальні витрати під час будівництва й експлуатації лінії.

У першому чергу мова йде про захист кабельних ЛЗ від несанкціонованого доступу до інформації, що передається по мережі.

Технічні засоби протидії передбачають застосування спеціальних пристроїв захисту, що обмежують можливості нелегальних абонентів з доступу до ліній зв’язку. Вони поділяються на активні і пасивні.

Пасивні пристрої захисту призначені для реєстрації факту приєднання і несанкціонованого використання лінії.

Активні пристрої захисту передбачають втручання в процес установлення і проведення несанкціонованого зв’язку. Наприклад, так звані індикатори приєднання і обривання лінії.

Для захисту від перехоплення паразитного електромагнітного проміння і наведень телефонних апаратів, телексів та факсів рекомендується використовувати або спеціально розроблену техніку зв'язку, або організувати просторове електромагнітне зашумлення в діапазонах частот випромінювання.

Канальне шифрування являє собою дуже ефективний засіб захисту інформації в мережах зв’язку. Оскільки шифруванню підлягають всі дані, передані від одного вузла мережі до іншого, у криптоаналітика немає ніякої додаткової інформації про те, хто служить джерелом цих даних, кому вони призначені, яка їхня структура і т. д. А якщо ще подбати і про те, щоб, поки канал простоює, передавати по ньому випадкову бітову послідовність, сторонній спостерігач не зможе навіть сказати, де починається і де закінчується текст переданого повідомлення.

Канали витоку інформації кабельних систем зв’язку представляють не тільки допоміжні засоби, що виходять за межі контрольованої зони, а також сторонні дроти і кабелі, до них не відносяться, але що проходять через приміщення, де встановлені основні і допоміжні технічні засоби, металеві труби систем опалення, водопостачання та інші струмопровідні металоконструкції. Залежно від способів перехоплення, від фізичної природи виникнення сигналів, а також середовища їх поширення технічні канали витоку інформації можна розділити на електромагнітні, електричні і параметричні[2, с. 20].

Невід'ємною частиною захисту інформації в кабельних системах зв'язку від витоку є технічний контроль, який призначений для оцінки ефективності та надійності прийнятих заходів захисту. Без якісного технічного контролю неможливо реалізувати надійне закриття каналів витоку інформації.

Технічний захист інформації в кабельних системах передачі даних повинна здійснюватися в суворій відповідності з нормативними документами[3, с. 20]. Тому належну увагу треба приділяти комплексним системам технічних засобів захисту інформації, що циркулюють в телекомунікаційних системах.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О.// Телекомунікаційні системи та мережі. Том 1. Структура й основні функції. 2018. -137ст.
2. А.В. Зайчук// Науково-технічний журнал "ЗАХИСТ ІНФОРМАЦІЇ" №4 2003. - 20 ст.
3. В.С. СолодкийВ.А. Тимофеев.Технические средства защиты информации с ограниченным доступом// Харьковский национальный университет радиоэлектроники, 2013. -20 ст.

ЗАХИСТ ІНФОРМАЦІЇ В БАНКІВСЬКИХ СИСТЕМАХ ТА НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Реков Дмитро Валерійович *студент Державного Університету Телекомунікацій.*

В даній роботі були розглянуті можливі загрози в банківських системах та на об'єктах інформаційної діяльності. Також були наданні рекомендації для захисту від впливу внутрішніх і зовнішніх загроз. При дотриманні наданих рекомендацій дозволяє на ранній стадії проектування вибрати оптимальний варіант захисту інформації.

Захист інформації має величезне значення у повсякденному житті, тим більше в банківських системах (БС) та на об'єктах інформаційної діяльності (ОІД). Сучасні інформаційні системи мають складну структуру. Вони містять додатки, що працюють у взаємодії з різними операційними системами, встановленими на комп'ютерах, об'єднаних в локальну мережу, часто пов'язану тим чи іншим чином з сегментом глобальної мережі. Забезпечення безпеки такої системи вимагає проведення цілого комплексу заходів відповідно до розробленої на підприємстві політикою інформаційної безпеки. В БС фінансові дані являють собою найбільш бажану ціль для кіберзлочинців. Дані які використовують фінансові установи для отримання грошового прибутку мають особливе значення тому банківські установи завжди знаходяться під загрозою кібернетичних атак.

Для забезпечення захисту інформації на ОІД та в БС є створення необхідних умов для захисту конфіденційної, службової або таємної інформації. Все починається з підготовки приміщення. При цьому, вже на стадії проектування та будівництва нових і реконструкції (ремонту) існуючих приміщень, необхідно визначити вищий ступень обмеження доступу до інформації, яка циркулюватиме на об'єктах, і у яких приміщеннях конкретно[1]. Для захисту важливих об'єктів є необхідним створення комплексу інженерно-технічних засобів охорони. Особливо важливим є аналіз вразливості ОІД, предмет захисту, загрози безпеки та оцінювання можливої шкоди. Необхідний комплексний науковий підхід до створення систем захисту та мати різні варіанти побудови комплексу інженерно-технічних засобів охорони з оцінкою її вартості. Такий підхід допоможе уникнути більшість помилок та зменшити витрати.

Метою також є аналіз захищеності від кібератак та створення рекомендацій щодо їх уникнення. Законодавство України визначає: «Кібератака — спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в

комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [2]. З цього слід зрозуміти, що будь-яка вразливість БС може призвести до успішної кібератаки на організацію.

Нажаль кількість кібератак які стосуються фінансових даних збільшується з кожним роком в Україні, трохи менше половини банків та платіжних організацій а саме 48% вирішили, що краще боротися з наслідками кібератак ніж створювати нові розробки захисту даних.

Для забезпечення ефективного захисту необхідно використовувати комплекс програмних та апаратних засобів. Використовування послуг спеціалізованих компаній, які захищають дані від DDoS-атак, підключившись до хмарних сервісів. Використовувати сайти які написані на мові Java вони є менш вразливими до загроз згідно дослідження компанії Positive Technologies. POS-термінали повинні забезпеченні спеціальним програмним забезпеченням для уникнення загроз. Необхідні роботи с персоналом такі як контроль відвідуваних сайтів і якими додатками користуються співробітники організації. Також необхідні курси для безпечної роботи в інтернеті, інформування про можливі загрози.

Таким чином, створення ефективного комплексу захисту інформації в БС та на ОІД потребую проведення аналізу вразливостей на стадії проектування і повинна базуватися на науковому підході. Захист інформації та інформаційна безпека повинні бути на високому для запобіганню кібератак. Без знання та кваліфікованого застосування сучасних технологій, стандартів, протоколів і засобів захисту інформації неможливо досягти необхідного рівня інформаційної безпеки комп'ютерних систем і мереж.

Література

1)https://tzi.ua/ua/planuvannya_zahodv_z_tehnchnogo_zahistu_movno_nformac_pd_chas_budvnictva_novih_rekonstrukc_remontu_snuyuchih_primshhen.html
2)https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA

Дослідження принципів роботи технологій VPN

Шиян Д.Г. БСДМ-61

На сьогоднішній день один із популярних та найлегших способів для забезпечення анонімності в Інтернеті це мережа під назвою Virtual Private Network

VPN – загальна назва віртуальної приватної мережі, що створюються поверх інших мереж. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами – внутрішніми сайтами, базами,

принтерами. Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Принцип роботи мережі

VPN-з'єднання завжди складається з каналу типу “точка-точка”, також відомого під назвою “тунель”. Тунель створюється в незахищеній мережі, в якості якої найчастіше виступає Інтернет. З'єднання “точка-точка” має на увазі, що воно завжди встановлюється між двома комп'ютерами, які називаються “вузлами”. Кожен вузол відповідає за шифрування даних до того, як вони потраплять в тунель, і розшифрування цих даних відбудеться після того, як вони покинуть тунель. Після підключення до VPN-сервера всі дані починають передаватися між вашим ПК і сервером взашифрованому вигляді. Уже з VPN-сервера всі дані передаються до зовнішніх ресурсів, які були запитані.

Призначення даної мережі

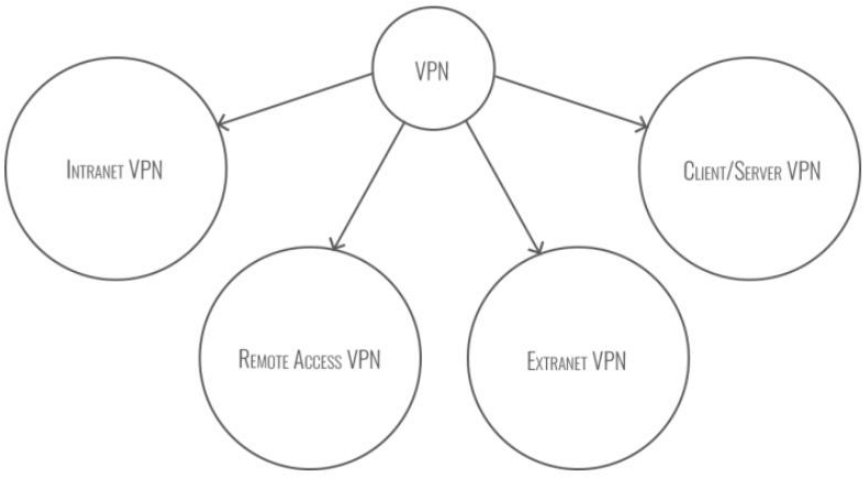
1. Захист від крадіїв. Багато людей люблять відвідувати кафе і сидіти там в Інтернеті через Wi-Fi або часто подорожують і підключаються до відкритих Wi-Fi точок. Злочинець, який сидить за сусіднім столиком, не зможе перехопити дані кредитної карти з CVV кодом, або не вкраде пароль від платіжної системи разом грошима.
2. Захист від спостереження. Якщо людина цінуєте своє приватне життя і їй неприємний той факт, що будь-який системний адміністратор провайдра має доступ до відвіданих вами сайтів, або з яких електронних платіжних системам ви поповнюєте чи знімаєте великі суми грошей. Провайдер більше не буде знати, які сайти ви відвідуєте, а сайти не будуть знати, хто їх відвідав.
3. Кожна людина хоче бачити Інтернет таким, яким він повинен бути – відвідувати сайти без обмежень. Також не рідкість, коли блокуються певні сторінки або розділи, а провайдер не розбираючись блокують весь сайт. Також в список заблокованих сайтів може потрапити ваш улюблений сайт або сервіси які надає привілеї, бонуси, знижки конкретним країнам. За допомогою VPN можна стати резидентом даної країни.

VPN – це теж бізнес, якому потрібні гроші на обладнання,

техобслуговування і зарплату співробітникам.
Безкоштовні і дуже популярні сервіси викрили в тому, що вони продають дані своїх користувачів стороннім організаціям. Найчастіше безкоштовні сервіси навіть не приховують передачу інформації третім особам, тому що безкоштовний продукт завжди притупляє пильність користувачів. Такі користувачі скоріше всього не читають умови надання послуги і не ставлять запитань.
Якщо VPN платний тоді зрозуміло де беруться гроші. Платні VPN не зацікавлені в продажу даних, так, як дорожать своїми користувачами і репутацією.

VPN поділяється на такі види:

1. Intranet VPN. Такий варіант дозволяє об'єднати кілька філіалів організації. Передача даних здійснюється по відкритих каналах. Інтернет може використовуватися для звичайних компаній і для мобільних офісів. Але слід мати на увазі, що такий спосіб передбачає установку серверів у всіх офісах.
2. Extranet VPN. Доступ до інформації підприємства надається клієнтам і іншим зовнішнім користувачам. При цьому їх можливості по використанню системи помітно обмежені. Не призначені для абонентів файли надійно захищаються засобами шифрування. Це відповідне рішення для фірм, яким необхідно забезпечити своїм клієнтам доступ до певних відомостей.
3. Remote Access. У цьому випадку створюється захищений канал міжофісом і віддаленим користувачем, що підключаються до ресурсів підприємства з домашнього ПК через Інтернет. Подібні системи прості в побудові, але менш безпечні, ніж їх аналоги, вони використовуються підприємствами з великою кількістю віддалених співробітників.
4. Client / Server. Цей варіант дозволяє обмінюватися даними між декількома вузлами всередині одного сегмента. Він користується найбільшою популярністю у організацій, яким необхідно в рамках однієї фізичної мережі створити кілька логічних, для захисту трафіку під час поділу використовується шифрування.



Висновки. Було досліджено принципи роботи мережі VPN, основне її призначення, види та недоліки даної технології.

Список літератури.

1. VPN [Електронний ресурс].
https://ru.wikipedia.org/wiki/VPN
2. Принцип роботи мережі VPN [Електронний ресурс].
https://lifehacker.ru/2016/05/12/mify-o-vpn/
4. Що таке VPN [Електронний ресурс].
http://tersukr.ru/rizne/8813-shho-take-vpn.html
5. Організація корпоративних мереж [Електронний ресурс].
https://www.kp.ru/guide/korporativnaja-set.html

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Шиян Д.Г. БСДМ-61

Сьогодні на другому місці за негативним впливом для світової спільноти після природних катаклізмів перебувають кібератаки (рік тому технологічні ризики разом із кіберзлочинністю займали третє місце). Це зазначено в щорічній доповіді експертів Всесвітнього економічного форуму в Давосі про глобальні ризики у світі під назвою “Global Risks Report 2018”, яка опублікована в січні 2018 року [1]. Виходячи з концептів документу ризики кібербезпеки постійно зростають, як у їх поширеності, так і руйнівному потенціалі. Наприклад, кількість кібератак на підприємства у світі подвоїлася протягом п’яти останніх років, а інциденти, які колись розглядалися як надзвичайні, сьогодні стають все більш розповсюдженими. Також зростають збитки від кіберзлочинів, які відповідно до звіту компанії McAfee і Центру стратегічних і міжнародних досліджень (CSIS) склали у 2018 році близько 600 млрд доларів [2].

Новою загрозою для кібербезпеки є створення кібервійськ, які здатні впливати на інфраструктуру «противників», що створюються багатьох країнах. Генеральний секретар ООН Антоніу Ґутерріша під час виступу в Лісабонському університеті 19 лютого 2018 року застеріг: «Наступна війна почнеться з масової кібератаки з метою знищення військового потенціалу і паралічу базової інфраструктури, такої як електричні мережі» [3]. Ґутерріш закликав світову спільноту до об’єднання з метою мінімізації впливу кібервоєн на життя цивільних громадян та запропонував створити в ООН платформу, на базі якої вчені, урядовці та інші особи могли б розробити

правила «для забезпечення більш гуманного характеру» щодо вирішення будь-якого конфлікту, пов'язаного з інформаційними технологіями.
В Україні світові тенденції кіберзагроз посилюються внаслідок гібридної війни, під час якої об'єкти критичної інфраструктури стають мішенями, на яких випробовуються все нові технології кібератак, зокрема кібератаки Petya, NotPetya були зорієнтовані на українські підприємства.
Останнім часом для захисту вітчизняного кіберпростору були розроблені та прийняті ряд важливих нормативно-правових актів, серед яких слід зазначити Стратегію кібербезпеки України, Рішення РНБО України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», Закон України «Про основні засади кібербезпеки України» та інші документи у сфері кібербезпеки.
Водночас украй важливим є не тільки прийняття відповідних нормативно-правових актів, але й упровадження їх положень у практичну діяльність суб'єктів, задіяних у забезпеченні кібербезпеки. Зокрема конкретні заходи для усіх основних суб'єктів забезпечення кібербезпеки та терміни їх реалізації визначені в Плані заходів на 2018 рік з реалізації Стратегії кібербезпеки України, який затверджений розпорядженням Кабінету Міністрів України від 10 березня 2017 р. № 155-р.
Слід зазначити, що лише після потужних кібератак на критичні інфраструктури в грудні 2016 року та у 2017 році державними органами проведено значну роботу із зміцнення кібербезпеки. Але, на жаль, на початок 2018 року залишається невиконаною ще низка важливих заходів, особливо тих, що стосуються об'єктів критичної інфраструктури, зокрема:
– не визначений перелік об'єктів критичної інфраструктури України;
– не внесено до Верховної Ради України проект Закону України "Про критичну інфраструктуру та її захист"; не в повному обсязі імплементуються Директива 2008/114/ЕС [4] щодо захисту критичної інфраструктури, зокрема з питань кібербезпеки та кіберзахисту об'єктів критичної інфраструктури, Директива ЄС 2013/40/EU від 12 серпня 2013 року [5] щодо кібератак на інформаційні системи та Директива ЄС 2016/1148 від 6 липня 2016 року про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем [6].
Слід також вказати, що жодна країна не може самостійно протистояти проблемам кібербезпеки, а тому необхідна тісна співпраця на міжнародному рівні з європейськими та структурами країн НАТО. Поряд із цим слід підвищувати рівень державно-приватної взаємодії в галузі кібербезпеки, та, як це зазначено в Рекомендаціях Європейського центру протидії кіберзлочинності (European Cybercrime Centre - EC3) «Оцінка загроз організованої злочинності в Інтернеті», в зв'язку з тим, що сектори критичної інфраструктури є досить вразливими до руйнівних кібератак, необхідно забезпечити їх більш досвідченими та підготовленими співробітниками та відповідним обладнанням, щоб протидіяти кібератакам [7].

Висновок:
Виконання зазначених заходів сприятиме забезпеченню необхідного рівня кібербезпеки України та надасть можливість отримати значні переваги від впровадження інформаційних технологій в усі сфери суспільного життя.

Список літератури.
1. Global Risks Report 2018”

http: www.weforum.org.
2. Збитки світової економіки від хакерів досягли $ 600 млрд : https://ua.korrespondent.net/world/3943548-zbytky-svitovoi-ekonomiky-vid-khakerivdosiahly-600-mlrd
3. Генсекретар ООН закликав до глобальної боротьби проти кібервоєн : https://www.radiosvoboda.org/a/news/29049044.html.
4. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32008L0114.
5. DIRECTIVE 2013/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council
Framework Decision 2005/222/JHA

http://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A32013L0040.
6. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of
network and information systems across the Union

http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.EN
7. Internet Organised Crime Threat Assessment (IOCTA) 2017 https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crimethreat-assessment-iocta-2017.

ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ПО КІБЕРБЕЗПЕЦІ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Шиян Д.Г. БСДМ-61

В умовах протистояння України зовнішній агресії, становлення її як демократичної держави, прагнення щодо вступу до європейських та євроатлантичних структур, кількість та якість загроз і небезпек, спрямованих проти України, суттєво збільшуються. Виходячи з цього, проблематика національної безпеки стає особливо актуальною та гостро ставить питання про «розвиток системи підготовки кадрів для потреб органів сектору безпеки і оборони України та розвиток науково-виробничого потенціалу такої системи» [1].

Для України, як на наш погляд, одною із головних проблем залишається при цьому саме незадовільне кадрове забезпечення фахівцями із кіберзахисту та їх розподілення на працевлаштування.

Про таке свідчать матеріали аналітичної доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України», а також результати аудиту нещодавно виведених з обігу стандартів вищої освіти у галузі знань «Інформаційна безпека», які показали, що професійні компетентності, задекларовані в цих галузевих стандартах, неповною мірою враховують стан та перспективу розвитку методів і засобів забезпечення кібербезпеки. Імовірно, саме це стало відправною точкою для прийняття постанови Кабінету Міністрів України від 29 квітня 2015 року № 266, яка внесла зміни до «Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» та визначила для України лише одну безпекову спеціальність – 125 «кібербезпека». Виходячи з цього та з врахуванням вимог Закону України «Про вищу освіту» стають актуальними питання щодо змісту, обсягу та оцінювання якості змісту і результатів освітньої діяльності вищих навчальних закладів (ВНЗ) за спеціальністю «кібербезпека» [2], запровадження спеціалізацій, що відповідають спеціальностям колишньої галузі знань «інформаційна безпека», розроблення нових освітніх програм та проведення їх акредитації. Формування професійної компетентності майбутніх фахівців кібернетичної безпеки розглядається при цьому, як трирівневий педагогічний процес, який відповідно до вимог закону України «Про вищу освіту» включає послідовну й неперервну фахову підготовку відповідно до Галузевих стандартів вищої освіти на першому (бакалаврському) і другому (магістерському) освітньо-професійних та третьому (доктор філософії) освітньо-науковому рівнях й здійснюється у вищих навчальних закладах III – IV рівнів акредитації або у спеціалізованих структурних підрозділах – навчально-наукових інститутах. Підготовка фахівців в галузі кібернетичної та інформаційної безпеки ведеться у багатьох ВНЗ України, але мало які з них відстежують працевлаштування своїх випускників. Тому існує велика ймовірність використання знань, отриманих у вишах, проти суспільства та держави у основних сферах життєдіяльності України [3].

Зважаючи, що останнім часом інформаційні технології все частіше

використовуються для досягнення воєнно-політичних цілей, втручання у внутрішні справи суверенних держав та порушення суспільного порядку, здійснення актів агресії проти інших держав, здійснення деструктивного впливу на об'єкти критичної інфраструктури, то це дає можливість застосування проти нашої держави низки кібератак і кібероперацій, які можуть призвести до проблем, пов'язаних із забезпеченням безперебійного функціонування об'єктів критичної інфраструктури, цілісності та конфіденційності інформації, а також її збереження, тобто всього того, з чим вже зіштовхнулась більшість країн Заходу – залишається актуальною. З метою убезпечення від таких дій постає потреба у проведенні, перш за все, інформаційно-пропагандистської кампанії про значимість проблематики інформаційної та кібербезпеки, а також підвищенні компетентності фахівців різних сфер діяльності з цих питань. При цьому за доцільне вбачається фахову підготовку фахівців з інформаційної і кібербезпеки для потреб як силових структур та органів державного управління, так і виробничої та банківської сфери проводити у єдиній системі освіти України, а спеціальну підготовку офіцерського складу ЗС України та інших силових структур із загальних питань – в системі командирської підготовки та на курсах підвищення кваліфікації [4].

Таким чином, автори вважають, що необхідно посилити контроль за працевлаштуванням випускників ВНЗ. Перевіряти куди вони йдуть, в державні чи приватні структури, де ті знаходяться і кому підпорядковуються. При вступі абітурієнтів до навчального закладу на спеціальності, пов'язані з інформаційною та кібернетичною безпекою, необхідно проводити додатково профвідбір (наприклад, тести) за моральнопсихологічними якостями, тому що не дивлячись на підвищення в останні
роки патріотизму, все одно є велике бажання молоді переїхати і попрацювати за кордоном. Тим паче, що знання іноземних мов є також пріоритетною програмою нашої держави. Таким чином ми можемо просто готувати за держбюджетні кошти кадри, які не тільки ніколи не будуть приносити користі Україні, а у деяких випадках навіть можуть шкодити.

Література

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня
2016 р. №96/2016 [Електронний ресурс]. - Режим доступу: http://www.president.gov.ua/documents/962016-19836.
2. «Про вищу освіту». Закон України від 1.07.2014 року № 1556-VII.
3. Buryachok V., Bogush V. Guidelines for the development and implementation training profile «cyber security» in Ukraine // Ukrainian Scientific Journal of Information
Security, 2014, vol. 20, issue 2, p. 126-131.
4. В.Л. Бурячок, І.Р. Пархомей, М.М. Степанов, В.Б.Толубко Проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки

галузі знань
«інформаційні технології». Сучасний захист інформації. № 2, 2016.

АКТУАЛЬНІСТЬ ПРОБЛЕМИ ФІШИНГУ В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОГО ЗАХИСТУ

Волков Микита Валерійович
студент магістратури ННІ захисту інформації
Державного університету телекомунікацій

З зростом нових технологій зростає і кількість можливих видів шахрайства та злочинів. Так само сталося і з появою світової мережі Інтернет – потік нових видів крадіжок не змусив себе довго чекати. Одним із таких видів являється фішинг – вид шахрайства , заснований на виманюванні персональних даних користувача за для отримання вигоди зловмисником. За останні роки він все більше набуває популярності , і тому – дуже важливо акцентувати увагу на ньому.

Актуальність даної теми спричинена не тільки різким підвищенням кількості атак даним методом, але й різким зростанням рівня технологій, що опосередковано сприяли цьому та великим рівнем успішності даних атак, що говорить про пробіли в схемах безпеки компаній та про низький рівень освіченості серед користувачів мережі Інтернет.

Таким чином, необхідно звернути увагу на можливі види фішинг-атак, а саме:

- Особисті або ділові електронні листи;
- Текстові повідомлення та інші послуги обміну повідомленнями;
- Реклама (пов'язані URL-адреси) на веб-сайтах і в додатках;
- Голосові фішинг-дзвінки (шахрайські продажі чи дзвінки щодо підтримки, які бажають придбати або перевірити особисту інформацію) [1];

Важливо усвідомлювати той факт , що потенційною жертвою фішинг-атак може стати кожен із нас – не потрібно приміряти бірки на когось іншого, адже за статистикою сайту retruster.com за 2019 рік 15% людей, які успішно «виловлюються», будуть націлені хоча б ще один раз протягом року [2], 76% підприємств повідомили, що стали жертвою фішинг-атаки за останній рік [2] , а всього на кібер-атаки в 2019 році доля фішингу складає 90 % [2].

Згідно з звітом постачальника безпеки, змістовна версія якого надана веб-ресурсом techrepublic.com, кількість світових фішинг-атак, виявлених Касперським, становила 129,9 млн. Протягом другого кварталу 2019 року [3].

Найбільша частка спаму спостерігалась у травні - 58,7%. Китай у всьому світі найбільшим джерелом спаму становив 23,7%, далі США - 13,8%, Росія -

4,8% та Бразилія - 4,6%. За квартал Касперський виявив загалом 43,9 мільйонів зловмисних вкладень електронної пошти [3].

Найбільше число фішинг-атак зазнало Греція - 26,2%, за нею - Венесуела, Бразилія, Австралія та Португалія. Щодо галузей та організацій, банки отримали найбільший відсоток фішингових електронних листів - 30,7%, далі - платіжні системи на рівні 20,1%, глобальні Інтернет-портали - 18% та соціальні мережі - 9% [3].

Для забезпечення більш високого рівня інформаційної безпеки , рекомендовано виконувати наступні дії [3]:

- Завжди перевіряйте адресу посилання та електронну пошту відправника, перш ніж натискати підозрілі електронні листи.
- Перевірте, чи адреса посилання може бути помічена в електронному листі та чи збігається з фактичною гіперпосиланням. Це можна перевірити, наведення курсор миші на посилання.
- Не завантажуйте та не відкривайте вкладення електронної пошти, які надходять з незнайомих адрес електронної пошти, перш ніж сканувати їх із рішенням безпеки. Якщо електронний лист здається законним, найкраще перевірити його, перейшовши на веб-сайт організації, яка його нібито надіслала.
- Ніколи не діліться вашими конфіденційними даними, такими як логіни та паролі, дані банківської картки тощо, з третьою стороною. Офіційні компанії ніколи не запитуватимуть такі дані електронною поштою.
- Використовуйте надійне рішення щодо безпеки з використанням анти-фішингових технологій, що базуються на поведінці, для виявлення та блокування як спам, так і фішинг-атак та ініціювання шкідливих файлів.

Отже , враховуючи наданий матеріал можна зробити висновок , що проблема фішинг-атак на сьогодні займає дуже важливу нішу в можливості забезпечення інформаційної безпеки та безперечно являється актуальною проблемою для кібербезпеки в цілому.

1. https://zvelo.com/news/phishing-2019-most-significant-security-challenge/
2. https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html

https://www.techrepublic.com/article/phishing-attacks-jump-by-21-in-latest-quarter-says-kaspersky/

НЕОБХІДНІСТЬ ВПРОВАДЖЕННЯ СИСТЕМ ДОСТУПУ ДО ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ ЗАСОБІВ ІДЕНТИФІКАЦІЇ

Бондар Олександр Павлович

В даній роботі освітлена проблема значного розвитку комп'ютерних систем, який потребує відповідного розвитку способів захисту від несанкціонованого доступу до інформації. Обґрунтована необхідність удосконалення систем

ідентифікації особи через впровадження біометричних технологій та актуальність такого підходу.

У сучасному світі комп’ютерні мережі розвиваються з величезною швидкістю. Швидке зниження вартості коштів обчислювальної техніки привело до різкого розширення сфер її застосування. Без комп'ютерів тепер неможлива будь-яка виробнича і управлінська діяльність, вони широко використовуються в медицині, освіті і багатьох інших сферах людської діяльності. Автоматизовані системи керують технологічними процесами на підприємствах, виконують фінансові операції, обробляють секретну і конфіденційну інформацію.

Комерційні, юридичні і лікарські таємниці та навіть державні секрети все частіше довіряються комп'ютеру, який, як правило, підключений до локальних і корпоративних мереж. Все більше компаній стикаються з необхідністю запобігти несанкціонованому доступу до своїх систем і захистити транзакції в електронному бізнесі.

Підкомітет ООН зі злочинності ставить цю проблему в один ряд з тероризмом і наркотичним бізнесом. Щорічні втрати від кіберзлочинності в Європі і Америці становлять кілька десятків мільярдів доларів. При цьому в дев'яноста відсотках випадків не вдається вийти на слід злочинця.

Головною причиною цього є те, що основним способом ідентифікації користувача у комп’ютерній мережі до сих пір є вказівка його мережевого імені і пароля. Для вирішення цієї проблеми необхідно відмовитися від застарілих методів ідентифікації.

Саме тому актуальність біометричних систем доступу до інформації на даний момент є дуже значною. Біометричне розпізнавання об'єкту засноване на порівнянні фізіологічних (відбитки пальців, структура сітківки ока, форма руки, теплова картина) або психологічних (особливості підпису або введення тексту з клавіатури, динамічні параметри письма) особливостей цього об'єкта з його характеристиками, що зберігаються в базі даних системи. В порівнянні з паролями і картками доступу, така система забезпечує набагато надійніший захист від несанкціонованого доступу до інформації [1].

Впровадження біометричної системи доступу потребує внесення змін в існуючий режим роботи. Можливо, необхідно внести зміни в штатний розклад: ввести нові посадові одиниці або скоротити деякі посади, змінити обов’язки робітників. Якщо обирати між біометричними методами ідентифікації для корпоративних цілей, то доцільно використовувати таку систему доступу до об’єкту, що ґрунтується на ідентифікації за відбитками пальців. Вона є найбільш розповсюдженою серед біометричних систем захисту та її впровадження не потребує багато коштів.

Звісно, системи доступу, що працюють на основі біометрії людини, коштують дорожче за класичні, застарілі варіанти контролю доступу, але приносять власнику безперечну користь: вони не лише надають набагато більший рівень захисту, але й демонструють належну увагу компанії до питань безпеки.

Проте більшість корпоративних користувачів, схоже, ще не усвідомили потенційних можливостей біометричних методів ідентифікації повною мірою. Та все ж таки нові технології все активніше проникають на корпоративний ринок. Вже сьогодні існують десятки тисяч комп'ютеризованих місць, сховищ, дослідницьких лабораторій, банків крові, банкоматів, військових споруд, доступ до яких контролюється пристроями, що сканують унікальні фізіологічні або психологічні характеристики індивідуума.

Ми вже спостерігаємо тенденції впровадження новітніх систем, законів та правил в нашій країні, зокрема перехід до біометричних паспортів як засобів ідентифікації особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Синіцин І. М., Ушмаєв О. С. Метрологічні і біометричні технології та системи, 2008. -15с.

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

Бортник Олексій Сергійович

Анотація

Робота містить актуальні проблеми кібербезпеки нашої держави, було наведено рекомендації щодо покращення кіберструктури держави, проведені порівняння розвитку кібербезпеки з міжнародним досвідом та іншими державами.

Ключові слова: кіберпростір, кібербезпека, кіберінциденти, міжнародні стандарти.

Аннотация

Работа содержит актуальные проблемы кибербезопасности нашего государства, были приведены рекомендации по улучшению киберструктуры государства, проведены сравнения развития кибербезопасности с международным опытом и другими государствами.

Ключевые слова: киберпространство, кибербезопасность, киберинциденты, международные стандарты.

Abstract

The work contains topical problems of cyber security of our country, the recommendations on improvement of the cyber structure of the state were given, comparisons of the development of cyber security with international experience and other states were made.

Keywords: cyberspace, cybersecurity, cybercidents, international standards.

Не поширюються індикатори атак і зразки шкідливого коду, щоб інші організації могли перевірити свої мережі і визначити, чи було у них вторгнення.

Не розробляються «Advisories» — керівництво по протистоянню і реагуванню на кібератаки.

Не надається допомога по викоріненню порушників з мереж організацій. А це дуже складний і тривалий процес, який може зайняти місяці, і вимагає методологічної підтримки. (Наприклад багато держорганізацій, які

були атаковані, залишилися без підтримки з точки зору вичищення їх мереж від хакерів. І хакери все ще присутні в мережах цих організацій).

Держспецзв'язок повинен дати організаціям інструменти, які дозволять їм зрозуміти чи скомпрометовані їх мережі, а також навчити організації реагувати на кібератаки.

Держспецзв'язок повинен аналізувати зразки хакерських інструментів з недавніх атак, і публікувати керівництва з пошуку ознак вторгнення, протистояння і викорінювання хакерів, як це роблять за кордоном.

Держава повинна допомагати організаціям готуватися до атак, а також допомагати проводити стримування і викорінення зловмисників з комп'ютерних мереж організацій, які піддалися атаці.

Якщо порівнювати нашу ситуацію з міжнародним досвідом, у нас не вистачає найважливіших елементів управління кібербезпекою, а створений при РНБО координаційний центр працює неефективно.

У країні відсутнє централізоване управління силами реагування на кіберінциденти і уповноваженими держорганами. Має місце лише "координація", але і вона неефективна. Наскільки мені відомо, координаційний центр зараз лише розробляє механізми координації і цей процес в зародковому стані.

Державі необхідна система управління, яка дозволить централізовано оперативно керувати діями уповноважених силових структур (Армія, Поліція, Держспецзв'язкок, СБУ) в разі кібератак, а також залучати волонтерів і бізнес партнерів, якщо потрібна підтримка.

На рівні міністерств також необхідно визначити відповідальних за кібербезпеку у відповідних галузях.

Зараз багато керівників відмовляються визнавати свою відповідальність: мовляв, якщо є комплексна система захисту інформації, КСЗІ — відповідає Держспецзв'язку. Це не правильно.

Крім CERT-UA, необхідні галузеві CERTи, і центри обміну інформацією про атаки ISAC (Information Sharing and Analysis Centers).

У деяких країнах є окремі CERT-и з безпеки АСУТП і SCADA-систем. Ці організації можуть створюватися як профільними міністерствами в галузях, де є критична інфраструктури, так і компаніями-учасниками ринку.

У нас також не визначена роль галузевих регуляторів в частині кібербезпеки.

За кордоном багато питань кібербезпеки регламентовані саме галузевими регуляторами, тому що ніхто крім них не знає краще особливості їх галузі. Приклад галузевого регулятора - NERC в США для енергетики, або Ofcom в

UK для телекомунікаційного і медіа сектора. Є готові галузеві стандарти кібербезпеки для різних галузей, які можна використовувати в Україні для тієї чи іншої критичною галузі.

Необхідно впровадити міжнародні стандарти замість КСЗІ.

Система КСЗІ показує свою неефективність. Необхідний перехід до міжнародних, ризик-орієнтованих стандартів і кращим практикам — ISO-27000 і NIST.

Відповідність стандартам повинні підтверджувати не аудитори, акредитовані державою - а компанії, що мають у себе фахівців, що володіють міжнародною сертифікацією по IT-аудиту та кібербезпеки. Міжнародна акредитація, замість державної, дозволить запобігти можливим зловживанням з боку чиновників і забезпечити високу якість аудиту.

Вищі навчальні заклади повинні готувати студентів за міжнародними стандартами, а міжнародні професійні сертифікації повинні бути визнані в Україні.

Важливе питання — освіта. В Україні повинні бути визнані на державному рівні міжнародні сертифікації по Форензік, кібербезпеці, IT-аудиту, IT-управління. А вузи, нарешті, повинні почати готувати фахівців за міжнародними стандартами, а не по захисту інформації відповідно до КСЗІ.

Потрібно вибудувати діалог між владою, професійним співтовариством і бізнесом з питань кібербезпеки.

Бракує працюючої програми державно-приватного партнерства. Держава дуже слабо інформує бізнес і громадян про свої плани, про те, що відбувається. Багато стратегічно важливих питань обговорюються і вирішуються кулуарно.

Бізнес-партнерів і волонтерів не залучають, якщо державі потрібна допомога — для цього немає механізмів. Бізнес і громадяни також не можуть розраховувати на отримання кваліфікованої допомоги від держави по кіберпитанням.

Необхідно налагодити взаємодію з міжнародними організаціями, центрами обміну інформацією про атаки. Від представників деяких з цих організацій ми знаємо, що зараз взаємодія не на висоті.

Впровадження кібербезпеки вимагає комплексного, трансформаційного підходу, який повинен управлятися зовнішніми експертами, незалежними від інтересів політичних партій.

Чому потрібен комплексний підхід?

Проекти, які потрібно запустити, не повинні обмежуватися чотирма силовими відомствами. Вони повинні охопити також всі органи державної

влади, міністерства, де є критична інфраструктура, приватні компанії, академічний сектор, громадян.

Проекти та ініціативи повинні бути взаємопов'язані і об'єднані в єдину програму. Така програма повинна централізовано управлятися, прогрес повинен відслідковуватися щотижня, а то й щодня.

Повинен бути створений «Трансформаційний Офіс» з кібербезпеки, подібний «Офісу Реформ».

Перелік посилань

1. Сучасні тренди кібербезпекової політики: висновки для України [Електронний ресурс] — Режим доступу : http://old2.niss.gov.ua/articles/294/
2. Про проблеми в сфері кібербезпеки в Україні [Електронний ресурс] — Режим доступу : https://www.pravda.com.ua/columns/2017/02/15/7135442/
3. Про основні засади забезпечення кібербезпеки України Закон від 05.10.2017 № 2163-VIII [Електронний ресурс] — Режим доступу : http://zakon5.rada.gov.ua/laws/show/2163-19
4. Ukraine Cybersecurity Cooperation Act of 2017 [Electronic resource]. – Mode of Access : https://www.congress.gov/bill/115th-congress/house-bill/1997

ТЕХНІЧНІ ЗАСОБИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ ЯК ЗАСОБИ ЗАХИСТУ ВІД ВИТОКУ ІНФОРМАЦІЇ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ

к.т.н. Котенко А.М.
Гармаш А.О. СЗДМ - 61
Держаний університет телекомунікацій
м. Київ

У статті розглядається склад технічної системи охорони та її призначення. Розглянуто типи датчиків ,що використовуються в системі охорони. Показано склад матеріально-речового каналу. Грунтуючись на проведеному аналізі зроблено висновок про доцільність використання технічних систем охорони для запобігання витоку інформації матеріально-речовим каналом.

Технічними засобами виявлення є комплекс технічних засобів охоронної сигналізації, що включає в себе сповіщувачі, що встановлюються безпосередньо на об'єктах, які охороняються, що включаються в шлейф і призначені для виявлення проникнення, спроби проникнення або фізичного впливу, що перевищує нормований рівень, і формування тривожного сповіщення.

Засоби виявлення (охоронні сповіщувачі) за принципом дії поділяються на [1, с. 25]:

- електроконтактні і омічні (обривні);
- магнітоконтактні (герконові);
- ударноконтактні;
- п’єзоелектричні (вібраційні);

- ємнісні або індуктивні (параметричні);
- радіохвильові (СВЧ-сповіщувачі);
- ультразвукові;
- оптично-електронні (інфрачервоні) активні і пасивні;
- комбіновані (які поєднують декілька різних принципів дії, наприклад, пасивний інфрачервоний і СВЧ);

За видом зони виявлення, що контролюється сповіщувачем:

- крапкові;
- лінійні;
- поверхневі;
- об'ємні.

Будь-які технічні засоби мають своє маркування, що містить основну інформацію про їх призначення і область застосування. Засоби охоронної і охоронно- пожежної сигналізації маркуються аналогічно пожежній сигналізації, а основна відмінність полягає в зашифрованих відомостях, що визначають принцип дії датчиків виявлення.

До технічних засобів виявлення охоронної сигналізації відносяться спеціальні датчики, призначені для фіксації факту несанкціонованого доступу на територію, що охороняється, і передачі сигналу тривоги.

Датчик - чутливий елемент, що перетворює параметр, який контролюється, в електричний сигнал.

У системах охоронної сигналізації використовуються датчики наступних типів [2, с. 34]:

- пасивні інфрачервоні датчики рушення;
- датчики розбиття скла;
- активні інфрачервоні датчики рушення і присутності;
- мікрохвильові датчики;
- ультразвукові датчики;
- магнітні (герконові) датчики;

Розглянемо що являє собою матеріально-речовий канал витоку інформації. Джерелами і носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин [3, с. 156]. Витік інформації в цих каналах супроводжується фізичним переміщенням людей та матеріальних тіл з інформацією за межами контрольованої зони. Основними джерелами інформації матеріально-речового каналу витоку інформації є наступні:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, що ведуться в організації;

- відходи діловодства та видавничої діяльності в організації, в тому числі використана копіювальний папір, забраковані листи при оформленні документів і їх розмноженні;

- жорсткі диски ПЕОМ, оптичні диски, флеш-носії, що містять інформацію з обмеженим доступом ;

- бракована продукція і її елементи;

Перенесення інформації в цьому каналі за межі контрольованої зони можливо наступними суб'єктами і об'єктами:

- співробітниками організації;

- сторонніми особами (злочинцями).

Технічні системи охорони призначені для виявлення людини-порушника у контрольованому просторі.

З цього слідує висновок, що технічні системи охорони дозволяють протидіяти витоку інформації на об’єктах інформаційної діяльності матеріально-речовим каналом.

Перелік використаної літератури.

1. Христич В. В., Дерев'янко О. А., Бондаренко С. М., Антошкін О. А. Системи пожежної та охоронної сигналізації.
2. Погребенник В.Д., Політило Р.В., 2008. Принципи побудови систем охоронної сигналізаці.
3. Хорев А.А. Захист інформації та інформації від витоку по технічним каналам. Ч.1. Технічні канали витоку інформації. Навчальний посібник. — 1998. — 320 с.

ЗАХИСТ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Поночовний А. М. СЗДМ - 61
Державний університет телекомунікації
Київ

Теза присвячена захисту акустичної інформації на об’єктах інформаційної діяльності. Розглянуто поняття мовного сигналу. Розглянуто причини появи акустичного каналу витоку інформації. Приводиться класифікація акустичних каналів витоку інформації. Для захисту інформації від витоку акустичним каналом використовується комплекс технічного захисту інформації від витоку технічними каналами.

Захист мовної інформації – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини).

Мовний сигнал – складний фізичний процес, пов'язаний зі зміною акустичних параметрів, які містять інформацію про зміст повідомлення. Енергія мовного сигналу зосереджена в діапазоні 300 - 4000 Гц. У своєму первісному вигляді мовний сигнал в приміщенні присутній у вигляді акустичних і вібраційних коливань [1, с. 45].

Залежно від середовища поширення сигналів і способів їх перехоплення технічні канали витоку мовної інформації можна розділити на [2, с. 134]:

- акустичні- за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали);

- вібраційні (віброакутсичні) - за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи вібрації (огороджувальні конструкції (стіни, стелі, підлоги, вікна, двері, короба вентиляційних систем тощо), інженерні комунікації (труби водопостачання, опалення, кондиціонування тощо));

- акустоелектричні- за рахунок впливу звукових коливань на ДТЗС (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля,створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цимелементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»);

- оптико-електронні (лазерні канали) канали - за рахунок приймання та демодуляції відбитого від вібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання;

- параметричні - за рахунок впливу звукових коливань на ОТЗ і ДТЗС (за рахунок паразитної модуляції інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори, за рахунок утворення вторинних радіохвиль, при «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу);

При проведенні робіт із технічного захисту інформації одночасно, з використанням одних і тих же приладів, методик та спеціалістів можуть здійснюватися заходи із захисту декількох каналів витоку інформації. Так, при проведенні робіт із захисту інформації від витоку акустичним каналом можуть проводитися роботи із захисту інформації від витоку віброакустичним і оптоелектронним каналами. Аналогічним чином здійснюються роботи із захисту інформації від витоку акустоелектричним та параметричним каналами побічних електромагнітних випромінювань та наводок (канали побічних електромагнітних випромінювань та наводок).

Виходячи з цього види роботи з технічного захисту інформації доцільно проводити за наступними напрямками [2, с. 178]:

- захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами;

- захист інформації від витоку акустоелектричними та параметричними каналами;

- захист інформації від витоку через закладні пристрої.

Для захисту мовної інформації з обмеженим доступом від витоку технічними каналами на об’єктах інформаційної діяльності створюється комплекс ТЗІ [3, с. 2].

Результатом проведення всіх вище перерахованих заходів є випробування та атестація. КТЗІ [3, с. 3].

Перелік використаної літератури.

1. Системи та пристрої інформаційної безпеки. Навчальний посібник / під ред. проф. В.А.Хорошко / Співавтори: А.П.Провозин, О.В.Рыбальский, В.А.Хорошко, Д.В.Чирков. – К.: ДУИКТ, 2007 р.

2. Методи та засоби захисту інформації. В 2-х томах / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко, Під ред. В.А.Хорошко. – К.: Арий, 2008.– Том ІІ. Інформаційна безпека. – 344 с.

3. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

ОСНОВНІ ПРОБЛЕМИ ТА РІШЕННЯ КІБЕРБЕЗПЕКИ, З ЯКИМИ СТИКАЮТЬСЯ КОМПАНІЇ

Овчиннік Сергій Олександрович

Державний Університет Телекомунікацій

Навчально-науковий інститут захисту інформації

Кафедра Системи інформаційного та кібернетичного захисту

Інтернет не тільки змінив способи ведення бізнесу компаніями, але і істотно змінив ставлення людей з їх конфіденційною інформацією. Хоча ця інформація колись була надійно заблокована (більш-менш), сьогодні велику її частину можна знайти десь в Інтернеті. Оскільки все більше людей використовують мережеві сервіси для розваг, управляють своїми фінансами і виконують свою роботу, кібератаки, спрямовані на збір і використання цінних даних, стають все більш поширеним явищем, в результаті чого всі піддаються ризику впливу Інтернету.

Кіберзлочинці постійно ставлять нові завдання перед професіоналами в області кібербезпеки. Ось деякі з головних проблем кібербезпеки:

1. **IoT-атаки**. з усіма пристроями IoT, які з'являються по 20 доларів за штуку, їх безпека не може бути нічим іншим, як катастрофою. Ми почали бачити те, що називається IoT Botnets. Звичайні ботнети - це група комп'ютерів, до яких зловмисник отримував доступ і контролював їх без відома їх власників. Їх можна колективно контролювати через центр управління та контролю, який контролює хакер. Ботнет IoT полягає не тільки зі спеціалізованих комп'ютерів, але також з моніторів серцевих імплантатів, механічних датчиків, побутових і промислових приладів і інших пристроїв, оснащених IP-адресами і можливістю передачі даних по мережі..

2. **БЛОКЧЕЙН**: «Блокчейн - це вічний цифровий розподілений журнал економічних транзакцій, який може бути запрограмований для запису не тільки фінансових операцій, але і практично все, що має цінність«, - Дон і

Алекс Тепскотт (Don & Alex Tapscott), автори «Революція блокчейна» (2016р).

Блокчейн зруйнував практично всі галузі. Досить складно зрозуміти переваги або проблеми блокчейна в області кібербезпеки.

Інтеграція кібербезпеки і блокчейна принесе багато змін в традиційні підходи кібербезпеки. Як фахівці з кібербезпеки адаптуються до цих змін, буде цікаво подивитися.

3. **ЗАГРОЗИ**: майже все електронне обладнання в нашому будинку підключено до Інтернету. Перевага цього полягає в тому, що ви можете перемикати телевізійні канали за допомогою мобільного телефону, а також використовувати мобільний телефон для замовлення їжі.

Ця взаємопов'язаність робить користувача дуже вразливим для кібератак. Це величезний ризик або проблема кібербезпеки, яку професіонали постійно намагаються усунути, додавши кілька рівнів перевірок, паролів, двофакторної аутентифікації, сеансів тайм-ауту і т. д.

4. **Вимагачі**: масштаби вимагачів майже подвоїлися за останнє десятиліття. Мета вимагачів - повністю вкрасти конфіденційні бізнес-дані. Компанія не може отримати ці дані.

Єдиний спосіб повернути дані - заплатити зловмисникам солідну суму грошей. Фахівці з кібербезпеки стикаються з проблемою захисту бізнес-даних від шкідливих програм і здирників.

Висновки:

Основна мета будь-якої кібератаки - дістати несанкціонований доступ до чогось цінного, це можуть бути дані, інтелектуальна власність, базова мережа або комп'ютери користувачів. Всі поточні проблеми кібербезпеки не нові, але вони прийняли більш небезпечні форми через доступність нових технологій.

Гарна новина полягає в тому, що працювати з цією областю складніше і легше, ніж кілька років тому. Інструменти захисту стали набагато краще е виявленні і складанні звітів, ніж будь-коли раніше, але наступальні інструменти і уразливості також набагато більш витончені, ніж ми мали затверджувати. Тим не менш, це дуже складне поле для гри.

КІБЕРБЕЗПЕКА В УКРАЇНІ

Василенко О. Є.

Шлях, яким рухається Україна у розбудові власної кібербезпеки, потребує докорінних та невідкладних змін. Це не лише точка зору лідерів думок вітчизняного кіберзахисту.Необхідність змін підтверджена атаками на об'єкти критичної інфраструктури, сумнозвісним NotPetya та багатьма

іншими інцидентами, які протягом останніх років створили Україні сумнівну репутацію одного з головних кіберполігонів.

Неефективна нормативна база та система управління, аналіз першопричин призводить до цілої низки системних проблем у галузі, ігнорувати які з кожним наступним інцидентом стає дедалі важче. Одна з головних – неефективна нормативна база та система управління. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та серія нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі. Більше того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати так звану Комплексну систему захисту інформації (КСЗІ). Вона, окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність.

Низька готовність реагувати на кібератакит а інша і не менш важлива проблема – неготовність реагувати на кіберінциденти. Більшість компаній все ще не готові організаційно до нових хвиль кібератак та не мають підготовлених в достатній мірі фахівців у своєму штаті. Відсутнє й централізоване управління силами реагування на кіберінциденти на загальнодержавному рівні. А якщо спуститися на щабель нижче – від державних структур та приватних компаній до пересічних громадян – то ситуація ще гірша. Рівень обізнаності українців з питань кібербезпеки залишає бажати кращого. Державна програма для заповнення цієї прогалини в Україні наразі, на жаль, відсутня.

Загалом управління кібербезпекою в Україні на державному рівні важко назвати ефективним. Національна система кібербезпеки обмежується переважно участю в ній силових органів (Нацполіція, СБУ, Держспецзв'язок тощо). Приватний бізнес та кіберспільнота до вирішення важливих питань майже не залучаються. Відсутній трансформаційний підхід до управління національною кібербезпекою, що передбачає наявність організації, яка керує впровадженням програми з кібербезпеки, та регулярного контролю за процесом впровадження. До того ж, через специфіку багатьох галузей (охорона здоров'я, енергетика, телекомунікації тощо) існує гостра потреба в окремих галузевих стандартах з кіберзахисту.

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

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

Підсумовуючи викладене, можна констатувати, що потрібний перехід на міжнародні стандарти кібербезпеки, в тому числі галузеві, визначення чітких критеріїв об'єктів критичної інфраструктури, навчання для організацій

громадян та формування культури кібербезпеки в суспільстві та визнання міжнародних сертифікацій, запровадження обов'язкової міжнародної сертифікації для посадовців, які займаються кібербезпекою та аудитом а також створення національної експертної ради з кібербезпеки.

Література

1. ЯНКОВСЬКИЙ О. Україні потрібна нова кіберстратегія [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.pravda.com.ua/columns/2019/09/14/7226291/

Зозуля Олександр Юрійович
студент групи ТСДМ-62
Державного Університету Телекомунікацій
м.Київ

БЕЗПЕКА В МЕРЕЖАХ ЗВ'ЯЗКУ 4G

4G – стандарт четвертого покоління мобільного радіозв'язку, який дозволяє забезпечити швидкість завантаження даних до 326 Мбіт/с, а швидкість віддачі даних до 172 Мбіт/с, з ще меншою затримкою передачі даних, ніж у попередника 3G. Мережі 4G стали розроблятися ще в 2000-х роках, а впроваджувати їх почали тільки з 2010-го року.

Безпека більшості мереж мобільного зв'язку знаходиться на низькому рівні. LTE-технолігія, зазвичай позиціонується як мережа 4G, є стандартом для безпровідної високошвидкісної передачі даних для мобільних телефонів, пристроїв та терміналів збору та обробки даних. Технологія покоління мобільного зв'язку LTE вже впроваджена в багатьох країнах світу та поступово впроваджується в інших країнах. Технологія LTE повністю заснована на протоколі IP. Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Це технологія кодового розподілення сигналу CDMA, технологія цифрового мобільного зв'язку GSM/GPRS, заснована на тимчасовому розподіленні сигналу, і стандарт радіо-Ethernet під назвою WiMAX, який передбачає динамічне розподілення ресурсу базової станції між абонентами. Всі вони внесли свій вклад в специфікацію LTE, також реалізований в двох основних варіантах: технологія з дуплексним частотним розподіленням FDD (Frequency Division Duplex) та тимчасовим розподіленням TDD (Time Division Duplex). Опора на більшість різноманітних технологій ускладнює пошук вразливостей в LTE, що дуже добре з точки безпеки. Так як стандарти LTE та LTE Advanced – це всього вдосконалені стандарти мобільного зв'язку 3G, то ніяких принципово нових погроз безпеки для даного виду комунікації не з'явилося. Але акценти в

моделюванні погроз технології LTE трохи змістилися. Тепер всі погрози зв'язані з протоколом IP. Якщо в мережах 3G голосовий трафік та дані передавалися по двом різним мережам – по мережі з комутацією каналів та по мережі даних, то в мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) по протоколу IP.

Не можна забувати і про обмеження LTE. Наприклад, збільшення швидкості підключення обертається зазвичай зменшенням радіусу дії базової станції – в середньому для LTE він складає 5 кілометрів, хоча залежить від використовуванного частотного діапазону. Із-за цього базових станцій в мережі стає більше і розташовані вони мають бути ближче один до одного. В результаті метод визначення місцезнаходження абоненту по сигналам базових станцій буде працювати точніше. З однієї сторони, це добре – оператор буде точніше знати місцезнаходження абоненту. З іншої сторони – сервіси геопозиціонування можливо використовувати і для слідкування за абонентом, що створює небезпеку нових загроз.

Також треба врахувати, що базові станції в LTE стали більш інтелектуальними і самостійними – вони отримали можливість маршрутизувати трафік. «Особливість мережі 4G в тому, що з її архітектури зникло поняття контролювання радіомережі (RNC), який в технології 3G виконував основну функцію по управлінню комунікаціонними ресурсами.

Перша загроза для технології LTE – це DDos атаки (Distributed Denial of Service) на мережу. Це така атака на обчислювальну систему з метою довести її до відмовлення роботи, тобто створення таких умов, при яких сумлінні користувачі системи не зможуть отримати доступ до представлених системних ресурсів, або цей доступ буде утруднений.

Друга загроза для цієї технології – це вірусні атаки. Хоча таким атакам схильні пристрої, а не мережа, технологія LTE збільшує швидкість розповсюдження шкідливих програм, так як сам цей стандарт є високошвидкісним. Труднощі розпочинаються при встановленні користувачами додаткових прошивок, або при отриманні повного доступу до мобільного пристрою, коли при невірній конфігурації зловмисниками стають доступними всі ресурси телефону через той самий протокол SSH (Secure SHell).

Третя загроза – атаки на додаткові сервіси. Технологія LTE розроблялася не тільки для забезпечення доступу до інтернету мобільних користувачів, а скоріше як платформа для впровадження нових послуг: відео, ігрові та багато інших. Ці сервіси можуть бути також вразливі для самих різноманітних атак – як з інтернету, так і з мобільної мережі. Скоріш за все, атакував один з сервісів, зловмисники зможуть впровадити в клієнтські пристрої небезпечні програми.

Загроза користувачам LTE може виходити і від сервісів двійного призначення. Мобільні оператори мають так багато цінної інформації про абонентів. Таким прикладом є сервіси пошуку місцезнаходження. З однієї сторони, такі сервіси можливо використовувати для пошуку свого та місцезнаходження інших людей, для зручності добиратися до пункту призначення, але з іншої сторони – їх також можливо використовувати для

незаконного стеження за абонентом. З поширення інтелектуальних пристроїв число потенційно небезпечних сервісів буде тільки зростати. Взлом такого сервісу дозволить зловмисникам отримати доступ до цінної інформації провайдера і построїти нові схеми злочинів і незаконного отримання фінансів. Цей список загроз не повний, зв'язаних з появою LTE, але це одні з основних загроз.

Розробники мобільної технології LTE все ж таки подбали і про її захист. В LTE використовується майже така ж сама модель безпеки, як і в ранніх версіях мобільного зв'язку. Хоча архітектура мережі змінилася, загальні принципи захисту залишилися колишніми. Якщо в колишніх версіях мобільної мережі за безпеку відповідав RNC, то тепер його немає, безпека покладена на базові станції, які стали більш інтелектуальними. Всі функції захисту в LTE об'єднанні стандартом і мають на увазі захист на декількох рівнях.

В LTE зберігаються і методи аутентифікації користувачів по прив'язці до карти USIM, так як в традиційному мобільному зв'язку: користувач може заблокувати доступ до телефону по PIN-коду. Передбачені і нові функціональні можливості для нових сценаріїв, включених міжмашинної взаємодії (M2M) і однократну аутентифікацію (SSO). Крім того, передбачений захист від несанкціонованих з'єднань поверх мультимедійної IP-мережі IMS. Цілком можливо, що використовувана в мобільній мережі більш краща система аутинтефікації допоможе і в інтернеті покращити систему безпеки.

Література:

1. Інтернет-ресурс «ITC» - https://itc.ua
2. Інтернет-ресурс «Confident» - http://www.confident.org.ua
3. Інтернет-ресурс «1234g» - http://1234g.ru/4g/lte/
4. Інформаційний інтернет-ресурс, проект «IT Захист» - http://itzashita.ru/

Світіна Ольга Сергіївна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в т.ч. персональні дані громадян.

Комплексна система захисту інформації (далі КСЗІ) – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.
Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

У процес створення КСЗІ залучаються такі сторони:

- організація, для якої здійснюється побудова КСЗІ (Замовник);
- організація, що здійснює заходи з побудови КСЗІ (Виконавець);
- Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку) (Контролюючий орган);
- організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);
- організація, що в разі необхідності залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єктом захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання. Матеріальними носіями інформації є сигнали. По своїй фізичній природі інформаційні сигнали можна розділити на такі види: електричні, електромагнітні, акустичні, а також їх комбінації. Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань, причому інформація, яка підлягає захисту, міститься в їх змінних параметрах. Залежно від природи, інформаційні сигнали поширюються в певних фізичних середовищах. Середовища можуть бути газовими, рідинними і твердими. Наприклад, повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, заземлення та інші. Залежно від виду та форми подання інформаційних сигналів, які циркулюють в інформаційно-телекомунікаційній системі (ІТС), у тому числі і в автоматизованих системах (АС), при побудові КСЗІ можуть використовуватися різні засоби захисту.

У побудові КСЗІ можна виділити наступні етапи:

- підготовка організаційно-розпорядчої документації.
- обстеження інформаційної інфраструктури Замовника.
- розробка "Технічного завдання на створення КСЗІ".
- розробка "Плану захисту інформації".
- розробка "Технічного проекту на створення КСЗІ".
- приведення інформаційної інфраструктури Замовника у відповідність з "Технічним проектом на створення КСЗІ".
- розробка "Експлуатаційної документації на КСЗІ".
- впровадження КСЗІ.
- випробування КСЗІ.

Виконавцем робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі може бути суб’єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення КСЗІ. Для проведення інших видів робіт з ТЗІ, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії. Якщо для створення КСЗІ необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензію на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

Література:

1. *Харченко В. С. Інформаційна безпека. Глосарій. — К.: КНТ, 2005.*
2. *Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005.-432 с.*
3. *Борсуковский Ю. Подходы и решения : Информационная безопасность // Мир денег. - 2001. - № 5. - С. 41-42*

4. *Інформаційна безпека України: проблеми та шляхи їх вирішення // Національна безпека і оборона. - 2001. - № 1. - С. 60-69*
5. *http://altersign.com.ua/*
6. *http://www.dsszzi.gov.ua/dsszzi/control/uk/index*

Світіна Ольга Сергіївна

Державний університет телекомунікацій

Навчально-науковий інститут захисту інформації

м. Київ

БЕЗПЕКА БАЗ ДАНИХ

Атаки на сховища і БД є одними з найнебезпечніших для підприємств і організацій. Згідно зі статистикою компанії infowatch, в останні роки кількість витоків даних в світі неухильно зростає, при цьому на 2018 – поч. 2019 року понад тридцять відсотків з них припадають на зовнішніх порушників і більше шістдесяти виконано за участю співробітників організації. Навіть якщо припустити, що в ряді випадків витік включала дані, до яких співробітник має легальний доступ, кожен третій випадок припадав на зовнішню атаку. Обсяг скомпрометованих в світі в результаті витоків записів даних, в тому числі номерів соціального страхування, реквізитів пластикових карт та іншої критично важливої інформації, на кінець 2018 року складав 13,3 млрд записів.

Питання комплексної безпеки БД привертають увагу дослідників, їм щорічно присвячується ряд робіт як в Україні, так і за кордоном. Можна відзначити дослідження, в якому розглядаються підходи до забезпечення конфіденційності, цілісності та доступності СУБД, запобігання, визначення та подолання атак. Пропонуються підходи до забезпечення мандатної і рольового дискреційного доступу до реляційного сервера. З усіх моделей безпеки найзручнішою для користувачів є рольова модель, проте вона найскладніша для адміністрування. За допомогою мандатної моделі можна створювати багаторівневі системи захисту. Найпростішою моделлю є дискреційна, але вона може виявитися надмірно детальною. Методи ідентифікації та аутентифікації користувача (внутрішня, зовнішня, біометрична і парольна). З усіх схем аутентифікації найчастіше використовується парольний захист, зважаючи на дешевизну і простоту. Часто використовується зовнішня аутентифікація за допомогою парольного захисту ОС, оскільки це зручно для користувачів. Досить поширеною є аутентифікація за допомогою токенів. Перспективною є біометрична аутентифікація Запроваджуються методи посиленої безпеки СУБД: криптографія, управління безпекою засобами мови SQL. У сучасних

СУБД широко використовується прозоре шифрування, оскільки при цьому дані завжди зашифровані, хоча це створює додаткове навантаження на центральний процесор. Окрім цього, при прозорому шифруванні користувачу не треба змінювати свої програми. Спільне використання симетричних і асиметричних методів шифрування підвищує ефективність СУБД та зменшує їх завантаженість. Обов'язковою частиною системи без- пеки СУБД є системи резервного копіювання (відновлення) і аудиту. Резервне копіювання і відновлення в сучасних СУБД може здійснюватися через графічний інтерфейс, а також за допомогою команд SQL. Мова SQL відіграє важливу роль у захисті СУБД. За допомогою команд SQL можна виконувати практично всі аспекти за- хисту СУБД. Для ефективного захисту БД в СУБД потрібен комплексний, систематичний підхід, необхідне поєднання різних сервісів безпеки та їх механізмів.

В архітектурному плані виділяють наступні підходи:

- повний доступ всіх користувачів до серверу БД;
- поділ користувачів на довірених і частково довірених засобами СУБД (системи управління БД);
- введення системи аудиту (логів дій користувачів) засобами СУБД;
- введення шифрування даних; винос коштів аутентифікації за межі СУБД в операційні системи і проміжне ПО; відмова від повністю довіреної адміністратора даних.

Список основних вразливостей СУБД не зазнав істотних змін за останні роки. Проаналізувавши засоби забезпечення безпеки СУБД, архітектуру БД, відомі уразливості і інциденти безпеки, можна виділити наступні причини виникнення такої ситуації:

- проблемами безпеки серйозно займаються тільки великі виробники;
- програмісти баз даних, прикладні програмісти і адміністратори не приділяють належної уваги питанням безпеки;
- різні масштаби і види збережених даних вимагають різних підходів до безпеки;
- різні СУБД використовують різні мовні конструкції для доступу до даних, організованих на основі однієї і тієї ж моделі;
- з'являються нові види і моделі зберігання даних.

Багато уразливості зберігають актуальність за рахунок неуваги або незнання адміністраторами систем баз даних питань безпеки. Наприклад, прості SQL-ін'єкції широко експлуатуються сьогодні по відношенню до різних web-додатків, в яких не приділяється достатньої уваги вхідних даних запитів.

Проте, введення засобів захисту як реакції на загрози не забезпечує захист від нових способів атак і формує розрізнене уявлення про саму проблему забезпечення безпеки. З одного боку, великі компанії можуть виділити

достатню кількість коштів забезпечення безпеки для своїх продуктів, з іншого боку, саме з цієї причини є велика кількість різнорідних рішень, відсутнє розуміння комплексної безпеки даних (і її компоненти відрізняються від виробника до виробника), немає загального, єдиного підходу до безпеки сховищ даних і, як наслідок, можливості. Ускладнюються прогнозування майбутніх атак і перспективна розробка захисних механізмів, для багатьох систем зберігається актуальність вже давно відомих атак, ускладнюється підготовка фахівців з безпеки.

Саме розробка програмних засобів перспективної захисту (на випередження зловмисника), забезпечення можливості впровадження такої технології представляються авторам статті найбільш актуальними завданнями на поточному етапі.

Незалежними від даних можна назвати наступні вимоги до безпечної системі БД:

Функціонування в довіреної середовищі

Під довіреної середовищем слід розуміти інфраструктуру підприємства і її захисні механізми, обумовлені політиками безпеки. Таким чином, мова йде про функціонування СУБД відповідно до правил безпеки, що застосовуються і до всіх інших систем підприємства.

Організація фізичної безпеки файлів даних

Вимоги до фізичної безпеки файлів даних СУБД в цілому не відрізняються від вимог, що застосовуються до будь-яких інших файлів користувачів і додатків.

Організація безпечної і актуальною настройки СУБД

Дана вимога включає в себе загальні завдання забезпечення безпеки, такі як своєчасна установка оновлень, відключення невикористовуваних функцій або застосування ефективної політики паролів.

Наступні вимоги можна назвати залежними від даних:

Безпека призначеного для користувача ПО

Сюди можна віднести завдання побудови безпечних інтерфейсів і механізмів доступу до даних.

Безпечна організація і робота з даними

Питання організації даних і управління ними є ключовим в системах зберігання інформації. У цю область входять завдання організації даних з контролем цілісності та інші, специфічні для СУБД проблеми безпеки.

Фактично це завдання включає в себе основний обсяг залежать від даних вразливостей і захисту від них.

В кінцевому випадку усі системи захисту зловмисники можуть «обійти» тільки через недбалість самих працівників, які не дотримуються регламенту політики безпеки персональних даних, платіжних систем та інших, які мають конфіденційну, службову або таємну інформацію з обмеженим доступом. Шукаючи і використовуючи вразливості СУБД зловмисники можуть навіть за допомогою Google Dorks викрасти особисту інформацію, яку ідентифікує пошукова система, про фізичну чи юридичну особу, згодом використавши це у своїх цілях. І все це через недолугість користувачів. На більш захищені системи винаходять більш руйнівні методи атак.

Література:

1. *http://www.tadviser.ru/index.php/*
2. *irbis-nbuv.gov.ua/.../cgiirbis_64.exe?*
3. http://www.swsys.ru/index.php?page=article&id=4175&lang
4. https://tproger.ru/articles/db-security-basics/

ПРОАКТИВНІ МЕТОДИ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ПРИМАНОК

Довгуша Ігор Михайлович

Проблеми кібербезпеки з кожним днем стають все більш актуальними для кожної організації, особливо в сучасних реаліях коли комп'ютерні мережі стрімко розростаються та звичних нам інструментів по забезпеченню інформаційної безпеки вже не вистачає. Традиційні (активні) підходи до безпеки полягають в тому, щоб забезпечити сильний захист периметру для запобігання кіберінцидентам, а реакція на загрози проводиться на події, які вже безпосередньо відбулись. Але не всі організації приділяють увагу проактивним методам захисту мережі, як можуть значно посилити загальний рівень кібербезпеки та зупиняти атаки ще до їх фактичного початку.

Проактивні методи захисту базуються на розвідці, яка залежить від комплексної оцінки кібербезпеки в організації. В цьому методі поєднується так зване "полювання на загрози" та моніторинг всієї мережі для того щоб отримати інформацію про стан захищеності систем та дізнатись про можливі вектори атаки. Враховуючи характер та потреби компанії, можна легко виявити та усунути слабкі місця в мережі до того, як атака буде проведена, а також визначити області для майбутніх інвестицій для підвищення загальної безпеки.

Проактивна розвідка може підвищити стійкість проти цільових атак (APT), пом'якшити наслідки та забезпечити найменшу можливу поверхню для атак нульового дня. Одним з інструментів проактивного виду захисту є приманки (honeypot). Honeypot - це система, яка створена з єдиною метою – бути атакованою, вона призначена для експлуатації, злому та зараження шкідливим програмним забезпеченням.

Є дві дуже вагомі причини, чому слід використовувати цей інструмент в своїй інфраструктурі.

По-перше, в той час коли під удар ставляться приманки ви виграєте час для захисту своєї основної інфраструктури.

По-друге, за допомогою цього інструменту можна з'ясувати хто проводить атаку та методи, які використовуються, що може дати уявлення про можливі типи подальших атак та таким чином продумати подальші дії та методи захисту.

Існує багато різних типів приманок з різними алгоритмати роботи та можливостями. Ви можете створити цілу фіктивну систему з цілою мережевою топологією, якщо бажаєте. У вас може бути безліч різних хостів, ви можете включати широкий спектр сервісів і навіть різні операційні системи. Іншими словами ви маєте змогу налаштувати цілу систему так, щоб вона виглядала справжньою.

Можна виділити наступні переваги використання приманок:

1. Можливість спостерігати за діями хакерів та збирати дані про їх поведінку;
2. Можливість збирати дані щодо можливих векторів проведення атак;
3. Створення моделі порушника для конкректної організації;
4. Приманки дають змогу виявити атаку на ранньому етапі;
5. Робить розвідку мережі для хакерів не такою ефективною;
6. Виявлення нових методів атак та збір інформації про шкідливе програмне забезпечення.

Таким чином, слід відзначити, що Honeypot є гнучкою технологією, яка може бути застосована в безлічі ситуацій. Приманки мають цілий ряд переваг і можуть послужити прекрасним доповненням іншим системам захисту, виконуючи такі функції як виявлення, попередження і протидія несанкціонованому доступу до мережі та протиправної активності в ній. Також технологія Honeypot може знайти своє застосування як важливий засіб по дослідженню нових методів та засобів, які використовуються зловмисниками для несанкціонованого доступу до інформаційних систем і дослідження шкідливого програмного забезпечення, його принципів роботи та механізмів розповсюдження.

Література

[1]https://en.wikipedia.org/wiki/Deception_technology
[2]https://www.fortinet.com/blog/industry-trends/reactive-vs--proactive-cybersecurity--5-reasons-why-traditional-.html
[3]https://www.finextra.com/blogposting/15308/active-proactive-or-reactive-assessing-your-cyber-security-posture
[4]https://www.webtitan.com/blog/honeypots-how-far-can-you-go-in-wasting-a-hackers-time/

АНАЛІЗ ІСНУЮЧИХ ПРОБЛЕМ ЗАХИСТУ КІНЦЕВИХ ТОЧОК

Скринник Владислав Сергійович

Фахівці в області інформаційної безпеки все частіше звертають увагу на те, що зловмисники майже завжди шукають можливості для експлуатації вразливостей кінцевих точок, і тому багато хто з них ставлять захист кінцевих точок на чільне місце при реалізації своїх програм з інформаційної безпеки. Для багатьох організацій захист привілейованих облікових записів крутиться навколо передачі прав. Внаслідок цього бізнес-користувачі та IT-адміністратори часто отримують більше прав, ніж їм необхідно, створюючи при цьому великий і часто експлуатований пролом у захисті.

Розглянемо основні проблеми при побудові захисту кінцевих точок:

Проблема 1. Ландшафт загроз постійно змінюється. У спробах обійти систему інформаційної безпеки організацій кіберзлочинці постійно змінюють тактику. В даний час більшість професіоналів в області інформаційної безпеки розуміють, що наявність прогалин неминуче. Зловмисник буде обходити існуючі системи безпеки і переміщатися по мережі, здійснюючи крадіжку параметрів доступу і підвищуючи права, поки не знайде конфіденційну інформацію для крадіжки або шифрування з метою отримання викупу. Визначення типу загрози і миттєвий відповідь на неї зараз є найважливішими компонентами будь-якої системи безпеки.

Проблема 2. Привілейовані облікові записи є важливим вектором атаки. Облікові записи з правами локального адміністратора є популярним вектором атаки, адже вони існують на кожній кінцевій точці і сервері всередині оточення. А індивідуальні користувальницькі облікові записи - на тих же самих машинах, - які мають права адміністратора, тільки збільшують можливості атакуючого.

Проблема 3. Складно знайти баланс між захистом і продуктивністю Незважаючи на те, що вважається хорошою практикою відбирати адміністративні права у бізнес-користувачів, багато організацій насправді не поспішають проводити такі зміни. Без всіх адміністративних прав у бізнес-користувачів можуть виникати проблеми з виконанням деяких завдань або запуском певних програм, які їм потрібні для виконання повсякденних ролей. Наприклад, користувачеві може знадобитися використовувати додаток для робочих потреб, яке для запуску вимагає певні права. Або користувачеві можуть знадобитися певні права для установки або оновлення авторизованого довіреної програми. Якщо повністю відібрати адміністративні права у цих користувачів, вони будуть змушені телефонувати на підтримку кожного разу, коли їм потрібні такі права лише для того, щоб мати можливість виконувати щоденну роботу.

Проблема 4. Занадто малі права можуть привести до «повзучості» прав і зростання ризиків. Коли організації вирішуються відібрати всі адміністративні права у бізнес-користувачів, IT-відділ буде періодично повертати ці права назад, щоб користувачі могли здійснювати певні дії. Наприклад, багато застарілі або зроблені самостійно «на коліні» програми, які використовуються в IT-середовищах, вимагають права для запуску, як вимагають їх і багато

комерційних вузькоспеціалізовані програми. IT-відділи повинні видавати права локального адміністратора цим користувачам для запуску таких додатків. Так як ці права були повернуті, вони рідко знову відбираються, і з часом це може призводити до того, що в організаціях майже всі користувачі мають права локальних адміністраторів. Ця «повзучість» прав повторно відкриває лазівки в безпеці, пов'язані з надмірними адміністративними правами, і знову робить організації, які зазвичай думають, що добре захищені, більш уразливими до погроз.

Проблема 5. Занадто багато прав можуть збільшити ризик шкоди від інсайдерів і складних загроз. На додаток до компромісу продуктивності, пов'язаного з обмеженням прав бізнес-користувачів, багато організацій також не поспішають обмежувати права IT-адміністраторів на серверах Windows. За ідеальних налаштуваннях системні адміністратори, власники додатків і адміністратори бази даних мають кожен свій набір дозволів на кожному сервері, до якого у них є доступ. На практиці цей поділ зон відповідальності може бути складно організувати, і у адміністраторів залишається істотно більше прав, ніж їм дійсно необхідно для роботи. Без політики прав на основі ролей для поділу зон відповідальності IT-адміністраторів чутливі системи можуть бути легко пошкоджені недосвідченими користувачами, їм може бути завдано шкоди інсайдерами-зловмисниками або вони можуть бути скомпрометовані досвідченими кіберзлочинцями, які отримують неавторизований доступ до привілейованих облікових записів.

Проблема 6. На кожній машині завжди буде обліковий запис «Адміністратор» Так вже вийшло, що на всіх кінцевих точках і серверах є користувач Адміністратор, root або іншого облікового запису того ж рівня, яка дозволяє будь-якому користувачеві мати адміністраторськими правами над машиною. Навіть якщо ви видалите адміністраторські права у індивідуальній облікового запису користувача, повноцінні облікові записи з ім'ям Адміністратор все ще залишаються. «Погані» політики управління паролями для таких облікових записів можуть привести при використанні однакових паролів на багатьох системах, що полегшує завдання для зловмисників, котрі скомпрометували одну систему, пересуватися по всьому оточенню - підвищуючи права, здійснюючи крадіжку даних і завдаючи шкоди системам на своєму шляху.

Проблема 7. Незважаючи на обмежені права деякі шкідливі програми все ще можуть проникнути. Обмежуючи права до рівня тих, які абсолютно необхідні, організації можуть обмежити ймовірну поверхню атак і заблокувати шкідливі програми, які намагаються використовувати права для установки шкідливих програм або принести шкоду машині. Проблема в тому, що не всім шкідливим програмам потрібні права для запуску, і в міру того, як зловмисники все більше дізнаються про обхід захисних механізмів, організації стають все більш уразливими до таких типів шкідливих програм. Практика показує, що більшість складних атак починаються з надсилання електронних листів на адресу непривілейованих бізнес-користувачів, а кампанія за все з 10

електронних листів зазвичай дає свої плоди в більш ніж 90% випадків, коли принаймні одна людина стає жертвою злочинця. У таких пуш-атаках можуть використовуватися дуже витончені шкідливі програми, і т.д. Вони знаходяться всередині мережі, вони можуть компрометувати машини, скоювати крадіжки даних, захоплювати параметри доступу або завдавати шкоди системам, абсолютно не використовуючи ніяких адміністраторських прав.

Проблема 8. Складно достовірно відстежити, які програми знаходяться в оточенні, і зрозуміти, які з них хороші, а які погані. Згідно з дослідженням кінцевих точок співробітників, проведеного компанією CyberArk, досить часто можна знайти більше 20 тис. Різних додатків на одному підприємстві, що говорить про те, що шкідливі програми можуть легко сховатися від очей, тому IT-відділи просто не володіють достатнім часом, щоб вручну все аналізувати. У таких масштабах визначити, яка програма хороша, погана або невідома - завдання, яке видається неможливим для вирішення або ж буде коштувати нечуваних грошей. Ще більше ускладнює справу те, що крім очевидно необхідних і очевидно підозрілих додатків існують десятки таких, для яких все не очевидно, і адміністратори просто не володіють достатнім часом для того, щоб впоратися з процесом рознесення додатків за категоріями. Це призводить до того, що традиційна технологія білого списку, яка входить в функціональність багатьох продуктів для захисту кінцевих точок, де-факто стає застарілою.

Висновки: На сьогоднішній день у підприємствах існують неефективні корпоративні рішення захисту кінцевих точок наступного покоління. Їх підхід полягає в тому, щоб показати, що існують шкідливі програми, які не виявляються такими рішеннями безпеки при їх завантаженні на комп'ютер або в момент спроби їх запуску. Проблема з такими демонстраціями полягає в тому, що автори розраховують зупинити шкідливі файли до їх запуску. Але це помилка. Вона показує явне нерозуміння цієї нової моделі захисту, заснованої на безперервному моніторингу всіх активних процесів. Щоб бути дійсно ефективним, рішення наступного покоління повинно надавати безперервну захист від усіх типів атак.

Література

1. Незалежний інформаційно-аналітичний центр з інформаційної безпеки [Електронний ресурс] / Шабанов І. – Режим доступу: https://www.anti-malware.ru
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. 4-е изд. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2012. – 943 с.

ХАРАКТЕРИСТИКА ТА ОСНОВНІ ВИМОГИ ДО СКЛАДОВИХ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Омельченко М.О., СЗДМ-51

Державний університет телекомунікацій

З найдавніших часів питання забезпечення безпеки життя людини в її повсякденній діяльності було і залишається відкритим, фактори ризику різного роду впливів що року поповнюються новими загрозами це стосується - навколишнього середовища проживання людини, захисту житла, захист від негативних природних явищ, забезпечення безпеки промислів і виробництва, виробів для споживання і закінчуючи захистом людини від людини.

Однак створення загроз спонукало світ до створення «індустрії безпеки» - це малі або великі колективи різного роду фахівців, які в свою чергу розробляють засоби нападу і засоби захисту включаючи такі напрямки, як законодавство і способи ухилення від його виконання, засоби економічної розвідки, промислового шпигунства, електронної розвідки і захисту інформації, фізичного впливу на людину, будівлю і споруду, пожежної та охоронної сигналізації, відеоспостереження (ВС), систем контролю управління доступом (СКУД) та ін. Такі органи забезпечення безпеки можуть надавати послуги захисту як за допомогою однієї автономної системи охорони (пожежна, охоронна сигналізація, відеоспостереження, система контролю управління доступом та ін.) так і створювати абсолютно новий етап в побудові системи безпеки – інтеграцію.

Більш складні умови захисту провокують застосування і розробку більш складних охоронних комплексів. На тлі розвитку ринку виникла необхідність інтеграції всіляких підсистем в одну єдину монолітну систему безпеки, яка може вирішувати весь спектр поставлених завдань - інтегрована система безпеки.

Інтегрована система безпеки (ІСБ) – є спільне використання ресурсів підсистем (пожежної та охоронної сигналізації, відеоспостереження, систем контролю управління доступом та іншого), в результаті чого система як ціле набуває нових якісних властивостей, на відміну від автономної роботи підсистем [1].

Не дивлячись на те, що ринок пропонує широкий асортимент моносистем безпеки, які працюють окремо від інших складових технічної охорони, жодна з них не здатна повністю захистити інтереси об’єкта інформаційної діяльності (ОІД), що охороняється. Тому більш ефективною у захисті безпеки є інтегровані системи безпеки, які складаються не тільки з підсистем, а й з власних каналів зв'язку, баз даних, алгоритмів роботи та програмного забезпечення.

Основні напрями визначаються наступними вимогами:

1. Зниження ролі людини в процесі забезпечення безпеки за рахунок підвищення інтелектуальності систем;

2. Зниження рівня помилкових спрацьовувань за рахунок більш тісного використання підсистем;

3. Вимога відкритості. Розробники ІСБ повинні забезпечити замовнику за допомогою відкритих протоколів можливості підключення систем і устаткування інших виробників і гнучкого настроювання ІСБ під свої потреби.

Реалізація зазначених вимог з одного боку дозволить збільшити ефективність систем безпеки, знизити людський фактор, з іншого - зробить побудову інтегрованих систем більш прозорою.

Оскільки сучасність вимагає більш удосконалених та ефективних засобів захисту інформації на ОІД, можна вважати, що тема роботи, яка присвячена питанням підвищення рівня захисту на ОІД за рахунок використання ІСБ, як високоефективного методу є актуальною науковою задачею.

Об'єднання різних підсистем в рамках єдиної ІСБ дозволяє вирішувати питання комплексного забезпечення безпеки об'єкта максимально ефективно саме за рахунок їх взаємодії та обміну інформацією. Можна сказати по-іншому: окремі підсистеми як би доповнюють один одного, допомагаючи в кінцевому підсумку вирішити спільне завдання - забезпечення безпеки.

Інтеграція системи в єдине рішення дозволяє забезпечити комплексний захист об'єктів це дає можливість:

- мінімізувати витрати на оснащення об'єкта за рахунок інтеграції систем і використання існуючої інфраструктури;
- об'єднати всі системи безпеки об'єкта в єдине інформаційне середовище, з єдиною базою даних і єдиним підходом до аналізу подій і прийняття рішень;
- задавати різноманітні алгоритми взаємодії систем за сигналами один одного: включення камер і запис, замикання / відмикання дверей, включення систем пожежогасіння, сирен і т.д., і забезпечити тим самим значний приріст функціональності комплексу;
- автоматизувати прийняття рішень для типових ситуацій;
- вести комплексний автоматизований аналіз даних щодо подій всього комплексу, включаючи порівняльний аналіз показань різних систем за обраними подій і т.д. (Наприклад дані відеоспостереження, охоронної сигналізації та системи контролю доступу);
- забезпечити оперативне надання керівництву достовірних даних;
- оперативно сповіщати персонал служби безпеки і координувати їх дії;

- знизити кількість інформації, що надходить до оператора, і зробити її більш наочною;
- значно зменшити ймовірність помилкових дій оператора;
- мінімізувати залежність системи від конкретного виконавця і негативні впливи людського чинника.

Склад кожної конкретної інтегрованої системи безпеки може змінюватися - доповнюватися якимись новими підсистемами, або навпаки виключати їх із загального списку. Це залежить від конкретних завдань, визначених на етапі проектування виходячи із можливостей та потреб окремо взятого ОІД. Базовий набір підсистем, що входять в інтегровану систему безпеки можна представити таким чином:

- Система охоронної сигналізації;
- Система пожежної сигналізації;
- Система контролю і управління доступом – СКУД;
- Система відеоспостереження;
- Система периметрової безпеки.

Переваги ІСБ:

- Можливість інтеграції довільного обладнання. Провести інтеграцію можливо як при наявності відкритих загальнодоступних ПЗ, так і на апаратному або транспортному рівні, коли ПЗ для обладнання не існує або воно з якихось причин недоступне.
- Великий набір можливостей взаємодії устаткування між собою.
- Можливість розробки особливих характеристик програмного забезпечення в процесі інтеграції.

Недоліки ІСБ:

- Необхідні додаткові ресурси на інтеграцію нового обладнання та на оновлення драйверів при зміні версій прошивок і обладнання. Це можливо тільки у випадку, якщо замовнику необхідно інтегрувати нове обладнання, яке до нього не було інтегровано.
- Іноді доводиться дублювати функціональні можливості в декількох місцях одночасно. Наприклад, ведення бази даних пропусків в інтегрованій системі і у вихідній базі підсистеми контролю і управління доступом.

Література:

1. Интеграция как новый подход к построению систем безопасности. [Електронний ресурс] / Журавлев С.П. //Журнал научных публикаций аспирантов и докторантов. - 2006 – 1с.

СПОСОБИ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЇ В КОНЦЕПІЇ ІНТЕРНЕТУ РЕЧЕЙ ЩО ЗАСТОСОВУЄТЬСЯ В МЕДИЦИНІ

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

Інтернет речей — концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.[1]

В медицині, ця концепція використовується в пристроях для спостереження за станом хворих та навіть кардіостимуляторах. Що може нести пряму загрозу життю людині. Прикладом можуть слугувати пристрої для автоматичної оцінки кількості цукру в крові та введення інсуліну або кардіостимулятори, роботу яких, зловмисник при бажанні може порушити і навіть зупинити. Подібна вразливість була виявлена в обладнанні компанії «St. Jude Medical».[2]

В цілому, можна виділити такі методи захисту:

1) Захист має забезпечуватися ще на етапі розробки програми, тобто код має бути захищеним, без можливості його редагування
2) Мають використовуватися тільки захищені канали передачі даних або спеціалізоване обладнання для взаємодії з пристроями та, наприклад, багатофакторна взаємна аутентифікація обох пристроїв.
3) використовувати стійкі та унікальні коди доступів(паролі).
4) Загалом, усі дані мають зберігатися тільки в зашифрованому вигляді.
5) «бекдор» повинен бути відсутнім, саме ж ПЗ(програмне забезпечення) якщо і має оновлюватися, то тільки при фізичному контакті з обладнанням, а не по «повітрю».
6) У конкретному випадку з кадіостимуляторами та подібним обладнанням, доцільно було б звести його функціонал до мінімуму, наприклад, щоб передавалися дані моніторингу без можливості проведення будь-яких дій віддалено або автоматизовано. Витік

інформації не призведе до таких фатальних наслідків, як зупинка роботи медичного обладнання.

ЛІТЕРАТУРА

1. Визначення інтернету речей.Історія, технології та проблеми [Электроний ресурс] - Режим доступа до статті: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9
2. Вразливі карідостимулятори [Электроний ресурс] - Режим доступа до статті: https://xakep.ru/2017/01/11/st-jude-patch/
3. Приклади застосування інтернету речей у догляді за здоров'ям [Электроний ресурс] - Режим доступа до статті: https://econsultancy.com/internet-of-things-healthcare/

ПРОБЛЕМАТИКА СТВОРЕННЯ ЦЕНТРІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (SOC)

Рижков Дмитро Олегович

Останні роки у сфері інформаційної безпеки ознаменувалися появою принципово новими загрозами і спонукають нас до впровадження ефективних рішень із реагування та протидії ним. ІБ суспільство прийшло до того, що необхідно впроваджувати заходи із постійного моніторингу та реагування на загрози. SOC – це концепція використання систем агрегації подій, управління ризиками та організаційних заходів задля забезпечення постійного процесу безпеки. Однак SOC не є лише інструментальним рішенням і його створення і розвиток має безліч «підводних каменів».

Постійний розвиток загроз інформаційній безпеці та поява безлічі нових програмних, апаратних та організаційних рішень у сфері безпеки привели цілі IT та ІБ індустрії до необхідності впровадження рішень, що агрегуватимуть усю циркулюючу в мережі підприємства інформацію та допомагатимуть проводити моніторинг, аналітику та реагування на інциденти. В результаті з’явилися SIEM-системи – Системи управління подіями та інцидентами, – той самий багатофункціональний агрегатор. Однак він є лише активним засобом забезпечуючи можливість перегляду уже результуючої інформації, тому одразу ж постає питання забезпечення «проактивності» безпеки, яке вирішується впровадженням засобів управління вразливостями(сканери) та ризиками, що також вдало інтегруються у SIEM.

Підприємство, що задовольнило свої потреби у вищезгаданих рішеннях спіткає себе на новий багаторічний квест, що складається із повноцінного впровадження рішень у всій інформаційній інфраструктурі компанії, інтеграції всіх IT-систем у ці рішення, розробки процедур із реагування на інциденти, підтримки функціонування системи, управління вразливостями і ризиками і багато іншого. Відповідні функції бере на себе команда, що в сучасності називається **SOC** (Security Operation Center).

Необхідність появи відповідних структур виправдана і наразі кожне підприємство, незалежно від форми власності, прагне до створення такого центру самостійно, або ж звернувшись за допомогою до спеціалізованих компаній, що постачають послуги **SOC as a service**, забираючи на себе усі процеси із адміністрування, моніторингу на реагування на інциденти. Крім того, відповідних кроків від підприємств очікує держава, затверджуючи законодавчо[1] необхідність забезпечення низки аспектів інформаційної безпеки, що задовольняються зокрема функціоналом SIEM та сканерів вразливості. В свою чергу це призводить до необхідності появи відповідних кадрів і формування команд моніторингу і реагування.

Найбільш складно усі кроки із побудови SOC даються організаціям, що прагнуть створити та керувати ним самостійно, як наприклад об'єкти критичної інфраструктури. Функції центру реагування зазвичай покладаються на підрозділи інформаційної безпеки, що здебільшого не займаються безпосереднім адмініструванням системної та мережевої інфраструктур і тому задачі із налаштування джерел даних до їх передачі до SIEM покладаються на IT-підрозділи. Водночас існує проблема, пов'язана із тим, що один підрозділ не розуміє цілей іншого[2,с.46], далеко не завжди налагоджується необхідний рівень комунікації і навіть існує ризик виникнення конфліктних ситуацій між підрозділами, що ніяк не сприяють розвитку та побудові нормального SOC. Виконуючи вимоги із забезпечення належного рівня інформаційної безпеки, підрозділи ІБ впроваджують рішення,які призначені для суттєвого покращення безпечності, але водночас вони знижують зручність використання IT-систем, що також не сприяє «теплим» відносинам між колективами.

Окрім вищезазначених проблем є і така, що пов'язана із неправильним уявленням організацій про те, що наявність SIEM одразу ж дорівнює появі SOC[3]. Це є найбільша омана, адже SIEM та інші програмно-апаратні рішення це лише інструментарій, а Центр реагування складається також із інших складових – спеціалістів та процесів.

Кадри: люди, що мають знання певного переліку систем, ОС, ПЗ, БД на рівні адміністрування, телекомунікаційних мереж, знають як проводити моніторинг та аналітику, реагувати на інциденти. В ідеалі ними мають бути люди із відповідним досвідом понад 2 роки або ж ті, кого можна навчити цьому забезпечуючи навчання певних аспектів роботи. Непоганим підходом є «змішування» більш досвідчених кадрів із менш досвідченими або ж початківцями, для підготовки заміни, адже високо досвідчені спеціалісти зазвичай ненадовго залишаються.

Процеси: сукупність організаційних та технічних процедур, що забезпечують підтримку інфраструктури, моніторинг, розслідування інцидентів та постійний розвиток, оновлення і розробка нових політик і заходів безпеки.

У вирішенні всіх цих проблем має бути зацікавлене, у першу чергу, керівництво підприємством, слідкуючи за якістю взаємодії підрозділів, що залучаються до побудови і розвитку SOC, надаючи необхідне забезпечення, що необхідне для виконання SOC-командою своїх задач, окрім того, воно має бути зацікавленим у тому, щоб завдання виконували кваліфіковані кадри і, у разі потреби, була готова забезпечити отримання персоналом нових знань, хоча б мінімально необхідних для виконання їх обов'язків. Якщо мова йде про критично важливі об'єкти та установи, то державі варто замислитись забезпечувати щонайменш якісною консультаційною допомогою та сприяти вирішенню питань побудови і розвитку центрів реагування.

Література

1. Постанова КМУ № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 р. Додаток «ПЕРЕЛІК базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури». Пункти 7,19,22.
2. Carson Zimmerman, The MITRE Corporation. Ten Strategies of a World-Class Cybersecurity Operations Center. October 2014.
3. https://habr.com/ru/company/softline/blog/423965/

КАНАЛИ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Панченко В.Г., УБДМ-61

Державний Університет Телекомунікацій

Модель порушника, яка використовується в цій тезі, передбачає, що в якості потенційних зловмисників можуть виступати співробітники компанії, які для виконання своїх функціональних обов'язків мають легальний доступ до конфіденційної інформації. Метою такого роду порушників є передача інформації за межі автоматизованих систем (далі АС) з метою її подальшого несанкціонованого використання - продажу, опублікування її у відкритому доступі і т.д. В цьому випадку можна виділити наступні можливі канали витоку конфіденційної інформації (рис. 1):

- несанкціоноване копіювання конфіденційної інформації на зовнішні носії та винесення її за межі контрольованої території підприємства. Прикладами таких носіїв є флоппі-диски, компакт-диски CD-ROM, Flash-носії та ін.;
- друк конфіденційної інформації та винесення роздрукованих документів за межі контрольованої території. Необхідно відзначити, що в даному випадку можуть використовуватися як локальні принтери, які

безпосередньо підключені до комп'ютера зловмисника, так і віддалені, взаємодія з якими здійснюється через мережу;

- несанкціонована передача конфіденційної інформації по мережі на зовнішні сервери, розташовані поза контрольованої території підприємства. Так, наприклад, зловмисник може передати конфіденційну інформацію на зовнішні поштові або файлові сервери мережі Інтернет, а потім завантажити її звідти, перебуваючи в будинку або в будь-якому іншому місці. Для передачі інформації порушник може використовувати протоколи SMTP, HTTP, FTP або будь-який інший протокол в залежності від налаштувань фільтрації вихідних пакетів даних, що застосовуються в АС. При цьому з метою маскування своїх дій порушник може попередньо зашифрувати інформацію яка відправляється або передати її під виглядом стандартних графічних або відео-файлів за допомогою методів стеганографії [1];
- розкрадання носіїв, які містять конфіденційну інформацію - жорстких дисків, магнітних стрічок, компакт-дисків CD-ROM і ін.

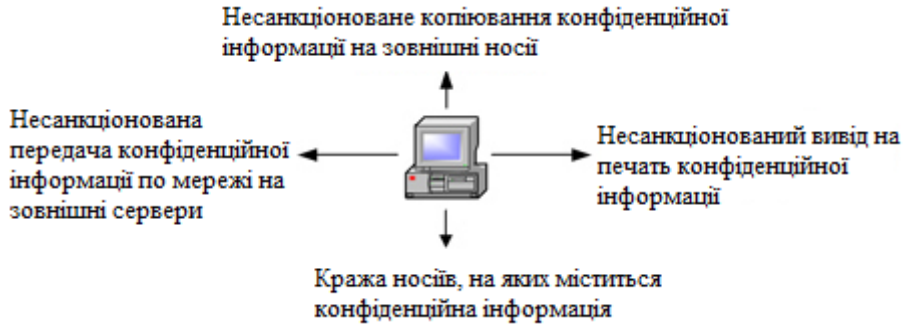


Рис. 1 Канали витоку конфіденційної інформації

Вважається, що в основі будь-якої системи захисту від атак, пов'язаних з витоком конфіденційної інформації, повинні лежати організаційні заходи забезпечення безпеки. В рамках цих заходів на підприємстві повинні бути розроблені і впроваджені організаційно-розпорядчі документи, що визначають список конфіденційних інформаційних ресурсів, можливі загрози, які з ними пов'язані, а також перелік тих заходів, які повинні бути реалізовані для протидії зазначеним загрозам. Прикладами таких організаційних документів можуть бути концепція і політика інформаційної безпеки, посадові інструкції співробітників компанії і ін. У доповненні до організаційних засобів захисту повинні застосовуватися і технічні рішення, призначені для блокування перерахованих вище каналів витоку конфіденційної інформації.

Література:

1. В.Г. Грибунин, И.Н. Оков, И.В. Туринцев, Цифровая стеганография, М: Солон-Пресс, 2002 г.

ОГЛЯД ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ БЕЗДРОТОВОЇ БЕЗПЕКИ WPA3.

Пономаренко Богдан Олегович *студент Державного Університету Телекомунікацій.*

Анотація:

З моменту впровадження стандарту IEEE 802.11 для бездротових локальних мереж (WLAN) у 1997 році, технології стрімко прогресували, щоб забезпечити зручний та стабільний бездротовий доступ для широкого спектру галузей та користувачів. З розповсюдженням різноманітних пристроїв, які використовують Wi-Fi доступ до мережі, бедротові атаки та захист від них стають все більш актуальною темою. В доповіді розглядається модель атаки, котра організовує та надає всебічний огляд можливих атак на новітні стандарти безпеки Wi-Fi. Основну увагу приділено технологіям, запропонованим в новій схемі захисту Wi-Fi Protected Access III (WPA3) та визначенню того, чи були подолані вразливості попереднього стандарту (WPA2).

Ключові слова: WPA3; WI-Fi; аналіз безпек

WPA3, випущена в кінці червня 2018 року, являється найновішою схемою безпеки, яка була розроблена для підсилення безпеки існуючих Wi-Fi мереж і вирішення проблем попередніх версій. WPA3 використовує метод SAE (Simultaneous Authentication of Equals) для аутентифікації клієнта. SAE вперше був використаний для бедротових mesh мереж (IEEE 802.11s) в 2008 році, проте згодом він виявився вразливим для пасивних та активних атак, зокрема “атак по словнику” від яких він повинен був захищати. Після перегляду (RFC7764), в 2015 році було показано, що покращений протокол забезпечуэ обціяний захист [1, с.260]. Це досягається за рахунок використання “рукопотискання стрекози” (dragonfly handshake), котре базується на дискретній криптографії на основі логарифмічних та еліптичних кривих. В результаті генерується PMK (Pairwaise Master Key), який далі використовується в стандартному 4-етапоному рукостисканню WPA2 [2, с.15].

Оскільки WPA3 являється розвитком WPA2 та лише доповнює її, огляд можливих вразливостей доцільно проводити на основі актуальних вразливостей WPA2. У випадку відсутності початкової переваги у зловмисника (альтернативний доступ до Ethernet мережі, наявність Wi-Fi ключа) можливо виділити 4 основні типи/напрямки атак проти WPA2 бездротової мережі: атака деаутентифікації (De-Authentication Attack), PMKID хеш-атака по словинку (PMKID Hash Dictionary Attack), атака на основі перехоплення рукостискання (Handshake Capture Dictionary Attack) та з використанням фальшивої точки доступу (Rogue AP Attack). Проведення KRACK-атаки (Key Reinstallation Attack), атаки злого двійника (Evil Twin), різних варіацій MIM (Man in the Middle) та Spoofing атак являються продовженням одного та/або декількох варіантів 4 основних типів [2, с.7].

Використання схеми безпеки WPA3 та впровадження dragonfly протоколу рукостискання націлене на протидію різним варіаціям хеш-атак по словнику, унеможливлює проведення DoS-атак на основі деаутентифікації та прямих маніпуляцій з ключем (як приклад, KRACK). Такий підхід запобігає та захищає від більшості вразливостей наявних в попередника, WPA2, проте не всіх. При цьому в стандарті WPA3 нічого не протиставляється фальшивим точкам доступу та подібним пристріям, які через клонування SSID, мак адреси, роботи

на сусідніх каналах все ще можуть використовуватись для проведення атак двійника, посредника та різноманітних варіацій фішингу. Для ускладнення проведення подібних операцій при побудові бездротової WPA3 мережі, ключову увагу необхідно приділя реалізації Ethernet та TCP/IP архітектурі таких як використання VPN-тунелів та класичних методів захисту в Metro Ethernet мережах (DHCP Snooping, ARP Watchdog, IP reverth-path verification, тощо).

Нещодавно була виявлена нова вразливість dragonfly протоколу через атаки по побічному каналу (так званий Dragonblood, ідентифікатор CVE-2019-9494). Для запобігання атаці по побічному каналу на основі синхронізації з технічного боку необхідно вікдлючити групи MODP 1, 2, 5, 22, 23, 24. Однак таке зменшення варіативності условних віток в кодуванні паролю в Dragonfly теоретично може призвести до реалізації атак на основі кешу (подібний принцип застосвується в автономних атаках по словнику в WPA2) [3 с.9].

Зважаючи на розглянуті атаки, WPA3 не складає враження відповідності сучасним стандартам безпеки. Дуже багато залишено для забезпечення сумістності з WPA2 та спрощення сертифікації під WPA3. Впровадження SAE (продемонстровано в [3]) лише ускладнює проведення атак по словнику, але не виключає їх, а лише зробить більш тривалими. Для обходу захисту в відкритих мережах зловмисник як і раніше зможе розгорнути свою точку доступу і перехоплювати будь-який трафік від користувачів, які підключились до неї.

Більш відкритий процес в проектуванні та істотніші зміни могли б допомогти усунути ці слабкі сторони при впровадженні нової редакції WPA3.

Перелік використаної літератури:

1. Lancrenon, J.; Škrobot, M. On the Provable Security of the Dragonfly protocol. In Proceedings of the International Information Security Conference, Trondheim, Norway, 19–21 September 2015; pp. 244–261.
2. Kohlios, C.P.; Hayajneh, T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3, 2018.
3. Vanhoef, M.; Ronen, E. Dragonblood: A Security Analysis of WPA3's SAE Handshake, 2019.

СОЦІАЛЬНА ІНЖЕНЕРІЯ В КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Галузін Ігор Сергійович

Найслабша ланка захисту будь-якої системи - самі користувачі. Соціальна інженерія намагається використовувати властиві людям слабкості, напр. квапливість, жадібність, альтруїзм чи страх перед офіційною установою, з метою отримання конфіденційної інформації і подальшого доступу в систему. Соціальна інженерія - це метод маніпуляції діями людини, що полягає у використанні слабкостей людського фактора в цілях незаконного отримання особистої інформації (облікових або банківських даних) або несанкціонованого доступу до комп'ютера жертви з метою встановлення на нього шкідливого ПЗ. Соціальна інженерія часто використовується як частина добре продуманої атаки на корпоративну середу.

Соціальну інженерію не варто недооцінювати. Навіть найбільш освічений в плані безпеки компанії можуть стати її жертвами, наприклад:

Березень 2011 року. Компанія RSA, зайнята забезпеченням безпеки, повідомила про переслідування своїх співробітників хакерами за допомогою фішингових листів, що дозволяють взяти управління над комп'ютерами. Таким чином хакери отримали доступ до мереж RSA і скомпрометували всю систему захисту компанії, яка використовує жетони SecureID для захисту клієнтів компанії. Атака коштувала компанії 66 мільйонів доларів і заміну призначених для користувача жетонів SecureID [1].

Фішингові повідомлення електронної пошти в корпоративному середовищі зазвичай знаменують собою таргетовану атаку, яка добре продумана і реалізована. На відміну від пересічних користувачів, співробітники компаній можуть бути проінструктовані належним чином про існуючі загрози інформаційної безпеки. За повідомленнями електронної пошти може бути встановлений той чи інший контроль з боку співробітників IT/ІБ підрозділів.

Проведення цільових фішингових кампаній вимагає від кіберзлочинців більше часу і грошей, ніж у випадку традиційних фішингових кампаній. Шахраї повинні отримати доступ або вкрасти списки діючих адресів електронної пошти для цільової організації або групи осіб, а потім створити правдоподібні листи, які з високою ймовірністю привернуть одержувачів і ті нададуть свої персональні дані. Однак в разі успіху фінансова віддача від цільового фішингу може бути набагато вище, тому інвестиції цілком окупаються.

Точковий фішинг став найпоширенішим типом таргетированной атаки з однієї простої причини: ця техніка по-справжньому працює, вводячи в оману навіть тих користувачів, які серйозно підходять до питань безпеки. Вона створює для хакерів опорний пункт для проникнення в корпоративну мережу. Реалізується декількома етапами:

Спочатку проводиться збір інформації з публічних джерел, з використанням спеціалізованих інструментів, запитів в пошукових системах, спеціалізованих сервісів, аналізу профілів компанії в соціальних мережах і на сайтах вакансій. Такого роду збір інформації можна співвіднести з методологією OSINT (Open Source Intelligence - розвідка на основі аналізу відкритих джерел інформації). Чим об'ємніше, точніше (як мінімум два-три джерела) і актуальніше інформація - тим вище успіх атаки.

Після розвідки та збору інформації зловмисники перевіряють отриману інформацію. Це може бути телефонний дзвінок, відправка повідомлення по електронній пошті - для того щоб підтвердити достовірність. Також перевіряються виявлені сервіси (піддомен mail.example.site) для формування фішингових форм входу.

З жертвою можуть вступити в листування, для з'ясування версії можливого програмного забезпечення, IP адреси, антивірусної програми - це все можна витягти з службових заголовків і тіла листа.

Далі формується сценарій атаки. Для формування фішингових атак зловмисники можуть зареєструвати підроблений домен.

Зловмисники можуть створити підроблену сторінку входу на:

- Корпоративний сайт;
- поштовий піддомен (або папку);
- корпоративний портал;
- CRM-систему;
- технічні послуги

Реалізація атаки. Фішингові поштові повідомлення, що розсилаються по великим списками адрес, розробляються з урахуванням методів соціальної інженерії. Наприклад, це може бути вміст, який вимагає виконання певної дії від одержувача, а також включення посилань на веб-сайти, які виглядають цілком правдоподібно (скажімо, шахрайські веб-сайти онлайнових банківських послуг). Однак в самих поштових повідомленнях цього типу дуже рідко використовуються будь-які персональні дані. У той же час завдяки цільовим фішинговим листам соціальна інженерія піднята на новий рівень. Звертаючись до одержувача по імені і відправляючи лист безпосередньо на його або її адресу, зловмисники неминуче збільшують ступінь довіри до шкідливого листа і фальшивим веб-сайтам, на які перенаправляється жертва.

Для атаки формується таргінг лист, що містить персоналізовану інформацію і посилання на фішингових сайтів. Розсилка може проводиться з підробленого сайту або використовуючи доступні (незакриті) smtp realy для підробки адреси відправника.

Основні вектори:

- помилка доставки поштового повідомлення;
- технічна помилка;
- повідомлення, що містить посилання на вкладення великого обсягу/невірного формату і т.д .;
- повідомлення від органів законодавчої/виконавчої влади;
- судові рішення.

Помилки відображення вмісту і посилання в листі зроблені для того, щоб змусити користувача покинути поштову програму (якщо він її використовує). Також, ці повідомлення можуть вести на відомий користувачеві, але скомпрометований ресурс - атаки такого класу мають назву watering hole.

Але левову частку фішингових повідомлень становлять шкідливі файли (користувач може не знати свій пароль), модифіковані документи, що містять макроси з тим чи іншим функціоналом.

Захист від соціальної інженерії передбачає, що крім стандартніх правил, в корпоративному середовищі необхідно керуватися ще наступними:

1. У політиці безпеки необхідно детально розписати загрозу соціальної інженерії і виставити ряд вимог, при виконанні яких загроза буде мінімізована.
2. Регулярно проводити інструктажі щодо нових технік соціальної інженерії і нагадувати про важливість дотримання цих правил.

Необхідність в сучасному антивірусному зазобі з налагодженою пісочницею. Згідно Cisco Annual Cybersecurity Report найбільшу кількість інфікованих файлів складають офісні документи та архіви [2, с. 16]. Тому

антивіруси повинні вміти ретельно аналізувати ці розширення. Але це не означає, що варто забувати про інші.

Також було відзначено велику кількість прикладів, коли шкідливий скрипт активувався після закриття документа. Ця техніка в більшості випадків прекрасно працювала тому, що документи не закривалися після того, як документ був відкритий і проаналізований в пісочниці. Так як пісочниця явно не закривала документ, вкладення здавалися їй безпечними і доставлялися відповідним одержувачам. Також пісочниця повинна вміти аналізувати файли всередині інших файлів (наприклад, документ word в PDF).

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 20 найгучніших кіберзлочинів XXI століття [Електронний ресурс]: © BIZUA.ORG – Электрон. дан. – м. Київ, Україна – 2015 – Режим доступа: World Wide Web. – URL: https://bizua.org/351/20-najguchnishix-kiberzlochiniv-xxi-stolittya

2. Отчет Cisco по информационной безопасности за 2018 год [Електронний ресурс]: Talos Security Intelligence and Research Group, Security Research and Operations, Security and Trust Organization. – Электрон. дан. – Cisco Systems, Inc. м. Сан-Хосе, Калифорния – 2018 – Режим доступа: World Wide Web. – URL: https://www.cisco.com/c/dam/global/ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf

РОЗРОБКА СИСТЕМИ МОДЕЛЮВАННЯ ЗАРАЖЕННЯ І КОНТРЗАХОДІВ БАЗОВО НЕВІДОМОЇ МЕРЕЖЕВОЇ АРХІТЕКТУРИ.

Гаркавенко Д.М.

АННОТАЦІЯ

Магістерська дисертація присвячена дослідженню проблеми прийняття рішень при зараженні комп'ютерної мережі.

Розглянуто основні теорико-ігрові підходи в задачах мережевої безпеки. Виявлено основні напрямки та методи.

Оцінені існуючі підходи моделювання поведінки порушника. Виявлено ключові особливості та недоліки існуючих моделей.

Використано теорико-ігрові підходи і мультиагентні системи для моделювання дій і стратегій порушника і захищаючого.

Створена система моделювання процесів зараження мережі і її протидії на основі ігор з неповною інформацією.

ТЕЗИ

Застосовувані теоретико-ігрові підходи до вирішення завдань інформаційної безпеки умовно можна розділити на 2 класи[4, 43]:

один клас (позначимо А) описує взаємодію «напад - захист», пророкуючи дії нападників і визначаючи відповідні дії захисту;

другий (В) дозволяє отримувати кількісні оцінки рівня захисту інформаційної системи шляхом передбачення дій нападників і захисту.

У класі А можна виділити два підкласу ігор - А1 і А2:

гри підкласу А1 дозволяють досліджувати взаємодію «напад - захист» в загальних випадках (гри зазвичай ведуться двома гравцями - «нападником» і «того, хто захищається», і у кожного з них є всього по два можливих дії: { «нападати», «не здійснювати будь дій»} і { «захищатися", "не здійснювати жодних дій»} відповідно);

в підкласі А2 розглядаються більш складні сценарії нападу і захисту, спеціалізовані під конкретні ситуаційні параметри (прикладом таких параметрів можуть бути властивості мережі, в якій здійснюється взаємодія).

Ігри підкласу А1 часто є статичними іграми з двома гравцями, або іграми з неповною інформацією.

Переваги ігор підкласу А2 в їх більшої реалістичності і кращому описі динаміки взаємодії «нападника» і «того, хто захищається», але отримання висновків про «правильному» поведінці учасників вимагає значних обсягів обчислень, а рішення в ряді випадків може не володіти достатньою точністю.

Підходи до оцінки рівня інформаційної безпеки використовують в якості вхідних даних передбачувані стратегії нападаючої і захищається сторін. Поєднання ідей таких підходів з відомими теоретико-ігровими методами призвело до появи класу В ігр, орієнтованих на отримання оцінок і аналіз рівня захищеності комп'ютерних систем.

Теоретико-ігрові методи знайшли широке застосування в задачах проектування систем виявлення вторгнень.

Нехай Ω - безліч спостережуваних об'єктів, кожному з яких зіставлено безліч відслідковуються параметрів Iω∈Ω.

Розглядається наступна взаємодія СВВ і атакуючого[1,240]. Кожну атака є послідовністю кроків. Кожен крок породжує певний вид активності, що виявляється СВВ. Після першої активності, яку СВВ розпізнала як підозрілу, здійснюється спроба передбачити подальші кроки передбачуваного зловмисника і розширюється безліч Iω∈Ω спостережуваних параметрів. Далі СВВ спостерігає розширений список параметрів протягом деякого періоду часу tm. Позначимо Jω∈Ω безліч додаткових параметрів спостереження. До виявлення підозрілої активності система виявлення вторгнень спостерігає базовий набір критичних параметрів.

$$S(t) = \sum_{\omega \in \Omega} \sum_{j \in J_{\omega}} s(\omega, j, t) = fkt$$

де f - середній ваговий коефіцієнт, що визначає ціну одного спостережуваного параметра, k - кількість спостережуваних пар «об'єкт - параметр», а S (t) - ціна додаткових ресурсів[4, 143].

Атакуючий формує свою стратегію на основі наступного безлічі дій:

{«Завершити атаку»; «Продовжити без паузи»; «Зробити паузу на деякий період часу»}.

У разі якщо вузлова СВВ виявляє атаку або ж зловмисник вирішує припинити напад, виграш для системи виявлення атаки буде α[3,89]. В іншому випадку його значенням буде -α. Атакуючий може належати одному з двох типів залежно від своїх цілей: проведення атаки на захищає систему або ж на саму СВВ. Перший тип атакуючих отримує виграш β в разі успішної атаки, інакше -β.

Z(t) - вартість паузи для атакуючого, яку, так само як і у випадку з СВВ, для простоти приймемо лінійно залежить від часу:

$$Z(t) = gt,$$

де g - ваговий коефіцієнт, який визначає вартість одиничного періоду паузи.

Відповідна першого типу атакуючих функція корисності СВВ має вигляд[4,47]:

$$U^1_{mon} = \begin{cases} \alpha - R(t_m), & 0 \le t_a < t_m, NA, \\ -\alpha - R(t_m), & 0 \le t_m < t_a. \end{cases}$$

СВВ та атакуючий здійснюють вибір на безлічі з чотирьох дій, зазначених раніше[2,59]. У таблиці 1 представлені результати одного раунду. Таблиці 2 і 3 показують стратегії гравці:

Таблиця 1. Результати першої ітерації гри

	a_1	a_2	a_3	a_4
b_1	0; 5000	0; 4950	0; 4500	0; 2000
b_2	2000; -5000	-2000; 4950	-2000; 4500	-2000; 2000
b_3	1800; -5000	1800; -5050	-2200; 4500	-2200; 2000
b_4	1500; -5000	1500; -5050	1500; -5500	-2500; 2000
b_5	2000; -5000	2060; -5060	2550; -5550	-2000; 1985
b_6	2000; -5000	3050; -6050	-2000; 4450	-2000; 1985

Таблиця 2. Стратегія атакуючого

b_1	b_2	b_3	b_4	b_5	b_6	очікувана корисність
0.6995816	0.02153313	0.0	0.0	0.2490239	0.02986128	0.0
0.6995493	0.0	0.0	0.0	0.2489484	0.05150225	0.0
0.6995799	0.02040104	0.0	0.0	0.2800189	0.0	0.0
0.6995493	0.0	0.0	0.0	0.3004506	0.0	0.0

Таблиця 3. Стратегія СВВ

a_1	a_2	a_3	a_4	очікувана корисність
0.5	0.0	0.0	0.5	1995.81672214
0.5	0.0	0.0	0.5	1995.49323986
0.5	0.0	0.0	0.5	1995.79971523
0.5	0.0	0.0	0.5	1995.49323986

Дії СВВ і атакуючого вибираються згідно рівноваги Неша. Одночасно з метою порівняння для кожного сценарію був підрахований відповідний обсяг ресурсів для традиційної реалізації СВВ.

1. Artificial Intelligence A Modern Approach by Stuart J. Russell and Peter Norvig
2. MULTIAGENT SYSTEMS Algorithmic, Game-Theoretic, and Logical Foundations by Yoav Shoham and Kevin Leyton-Brown
3. Fundamentals of Multiagent Systems with NetLogo Examples by José M Vidal
4. Network Security: A Decision and Game Theoretic Approach by Tansu Alpcan and Tamer Basar.

Тисячний Роман Олегович
Державний університет телекомунікацій
група УБДМ-51
Управління інформаційною безпекою
0932684307
romantysiachnyi@gmail.com

СУЧАСНІ ВИКЛИКИ І ЗАГРОЗИ В КІБЕРПРОСТОРІ: ФОРМУВАННЯ МЕХАНІЗМУ УКРАЇНСЬКОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Кіберзагрози, носять глобальний характер. Межі кіберпростору не визначаються державними кордонами, або іншими географічними бар'єрами. Географічні, кліматичні, часові характеристики, місцезнаходження, державна (коаліційна) належність, форма власності об'єктів тощо, не є стримуючими факторами для здійснення кібервпливу чи кібератак. Кіберзагрози можуть бути реалізовані будь-де та в будь-який час та за незначний проміжок часу нанести величезні збитки. Потенційно вразливими до кіберзагроз є життєво важливі сектори економіки (енергетика, транспорт), критично важливі об'єкти інфраструктури, об'єкти критичної інформаційної інфраструктури, національна телекомунікаційна мережа, національні електронні інформаційні ресурси, системи: банківсько-фінансова та охорони здоров'я, сфера оборон.

Правових і технічних заходів на національному та регіональному рівнях недостатньо для того, щоб подолати глобальні загрози кібербезпеки. Стандарт ITU та Європейського союзу ISO/IEC 27000 визначає загрозу (threat) як потенційну причину небажаного інциденту, що може призвести до збитків системі або/та організації [1]. Законодавство України [2] визначає кіберзагрози як наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. В Україні визнано [3], що у середньостроковій перспективі намагання реалізації іноземними державами, міжнародними злочинними угрупованнями кіберзагроз щодо автоматизованих систем державного та військового управління, об'єктів критичної інформаційної інфраструктури залишаються серед найбільш актуальних. Проблема оцінки стану кібербезпеки повинна передусім розглядатися в нерозривному зв'язку з оцінкою можливих чи завданих збитків соціальним або соціотехнічним системам відповідно до потенційних або/та реалізованих загроз.

Ряд системних та управлінських проблем слід розглянути окремо, як такі, що не забезпечують належний рівень (індекс) кібербезпеки:

- відсутність системності ведення кібердій, теорії застосування сил та засобів кібероборони, взаємодії різних відомств у сфері забезпечення кібероборони держави;
- відсутність в секторі оборони єдиного координуючого органу з питань забезпечення кібербезпеки та системи підготовки військового й цивільного персоналу;
- проблеми кадрового забезпечення відповідних структурних підрозділів та відтік за кордон кваліфікованих спеціалістів;
- низький рівень наукового потенціалу, майже повна відсутність наукових шкіл, критичні складнощі із методичним, науковим і технічним забезпеченням відтік за кордон кваліфікованих наукових кадрів.

Вирішення вище перерахованих проблем неможливе без гармонізації та унормування термінологічних систем сфер кібербезпеки та кібероборони.

На фоні не вирішення таких проблем, потенційні кіберзагрози можуть реалізуватися в успішні кібератаки на складні соціотехнічні системи держави, які призведуть до виникнення критичних ситуацій (у тому числі техногенних аварій та катастроф. Зокрема, це можуть бути: - порушення управління державою та її інституціями шляхом здійснення деструктивних впливів на соціум (населення та політиків і керівників різного рівня з метою усунення та дискредитація осіб, які приймають рішення, формування негативної громадської думки про дії влади, спонукання населення до деструктивних дій тощо); - використання глобальних інформаційних мереж терористичними та екстремістськими організаціями з метою організації терористичних актів, а також вербування нових бойовиків; - несанкціоноване втручання в комп'ютерні мережі та системи управління органів державного та військового управління, стратегічно важливих об'єктів критичної інфраструктури, національних підприємств, управління військами та зброєю з метою отримання доступу до службової, конфіденційної або комерційної інформації, її викрадення, спотворення чи знищення, або/та взяття таких систем під контроль чи виведення їх з ладу.

Список використаної літератури

1 .Рекомендації міжнародного союзу електрозв'язку. МСЕ-Т.Сер.Х.1208. Мережі передачі даних, взаємозв'язок відкритих мереж та безпека. Безпека кіберпростору – кібербезпека. 2014 р. ISO/IEC 27000. URL: https://www.itu.int/itut/recommendations/rec.aspx?rec=11950&lang=ru.

2. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19

3. Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 №92/2016. URL: https://zakon.rada.gov.ua/laws/show/92/2016

Коваль Т.Р.

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

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

Серед головних переваг інтернету речей:

1. Безпека, комфорт, ефективність

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

2. Краще прийняття рішень

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

3. Генерація доходів

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

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

1. Атаки на хмарні середовища

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

2. Проблеми з ботнетом

Мільйони нових підключених споживчих пристроїв створюють широку

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

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

3. Відсутність довіри

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

a) 96 відсотків підприємств і 90 відсотків споживачів вважають, що повинні існувати правила безпеки ІН
b) 54% споживачів володіють у середньому чотирма пристроями IoT, але лише 14% вважають, що вони знають про безпеку пристроїв IoT
c) 65 відсотків споживачів стурбовані тим, що хакер контролює їх пристрій IoT, а 60 відсотків стурбовані тим, що дані витікають

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

4. Розуміння IoT

У 2019 році справжня проблема полягає в тому, як підвищити здатність людей чіткіше зрозуміти зміни та їхні наслідки, а також зробити конкретні дії, щоб скористатися потенційним потенціалом.

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

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

Література:

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

УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ В КОРПОРАТИВІНЙ ІФНОРМАЦІЙНІЙ СИСТЕМІ

Коровайченко Ю.Ю.

Управління вразливістю - це процес виявлення вразливих місць в IT системі, задля їх частішого та ефективнішого виправлення. Вразливості, які потребують виправлення, повинні бути визначені як пріоритетні, виходячи з того, які з них створюють безпосередній ризик для мережі.

1) Що таке Vulnerability management?

Vulnerability management - це практика безпеки, спеціально розроблена для попереднього зменшення чи запобігання експлуатації вразливих IT-систем, наявних у системі чи організації.

Процес включає ідентифікацію, класифікацію, усунення та пом’якшення вразливостей у системі. Він є невід'ємною частиною комп'ютерної та мережевої безпеки і впроваджується разом з управлінням ризиками, а також іншими практиками безпеки.

2) Чому Vulnerability management є важливим?

Вразливості мережі - це прогалини в безпеці, якими зловмисники можуть скористуватись з метою пошкодження мережевих активів, викликати відмову в обслуговуванні або отримати доступ до закритої інформації. Зловмисники постійно шукають нові вразливості для експлуатації та використовують старі, які, можливо, ще не виправлені.

Створення системи управління вразливостями, яка регулярно перевіряє наявність потенційних вразливостей, є надзвичайно важливою для запобігання порушенням кібербезпеки. Без цієї системи та системи управління патчами старі прогалини в безпеці можуть залишатися в мережі протягом тривалого часу. Це надає зловмисникам більше можливостей використовувати вразливості для атак на IT систему.

3) Компоненти Vulnerability management

Vulnerability management складається з наступних компонентів:

• Визначення / відстеження активів (інвентаризація активів)

• Категоризація активів в групи

• Сканування активів на наявність відомих вразливостей

• Ранжування ризиків

• Управління виправленнями знайдених вразливостей

- Тестування патчів
- Застосування патчів

• Сканування після виправлення - підтверджує усунення вразливості.

4) Етапи Vulnerability management

Перший етап процесу управління вразливістю - виявлення активів. Вам потрібно знати, що розгорнуто у вашій мережі, та розподілити виявлені активи в групи. Ви дізнаєтесь про вразливості у вашій мережі через такі джерела, як тестування вашої IT системи на вразливості, звіт від постачальників, або центрів реагування на кіберзагрози, ваші журнали та ваш SIEM, звіти співробітників і, на жаль, в результаті реальних атак, які використовують ці вразливості.

Переконайтеся, що ви зберігаєте інформацію про свої виявленні вразливості якомога детальніше, з доступом лише тим співробітникам, які повинні про них знати.

Положення та стандарти дотримання, а також політика компанії також повинні враховуватися. Залежно від вашої компанії, галузі та юрисдикції, можуть існувати конкретні стандарти, яким має відповідати ваша звітність щодо управління вразливостями.

З часом ви неминуче виявите багато вразливих місць. Ефективний процес розстановки пріоритетів допоможе вам виявити свої вразливості, щоб ви могли

ефективніше реагувати на них. Є важливий і корисний спосіб класифікувати свої вразливості - за терміновістю. Очевидно, перш за все слід вирішити більш нагальні вразливості. Які можливі наслідки експлуатування певної вразливості? Скільки грошей потенційно втрачено? Чи можлива реальна шкода людям? Скільки ваших машин, приладів, додатків чи фізичних осіб наражаються на небезпеку? Чи витрати на захист активу менше, ніж вартість самого активу?

Наступна фаза - ваша відповідь на ризик. Ви можете класифікувати відповіді на ризики, відповідно до яких ви можете усунути, зменшити чи прийняти їх. Іноді доводиться приймати дуже важкі рішення. Актив, який би коштував дорожче, ніж втратити, може співвідноситись з ризиком, який ви вирішите прийняти. Або ви можете вирішити, що досить важливо, щоб працівники могли підключити власні пристрої до вашої мережі, приймаючи на себе великий ризик. Вразливості програмного забезпечення, що виправляються, є ризиком, який можна відшкодувати, але виправлення також може спричинити інші проблеми.

Саме тому Vulnerability management це дуже важливий та складний процес, який потребує дослідження та корегування під кожну IT систему, у яку впроваджується.

Список використаної літератури:

1) Foreman P. Vulnerability Management 1st Edition/ Park Foreman., 2010.
2) Foreman P. Vulnerability Management 2st Edition/ Park Foreman., 2019.

НЕСАНКЦІОНОВАНИЙ ДОСТУП ДО ІНФОРМАЦІЇ

Пахомов В.О., УБДМ – 61

Державний університет телекомунікацій

Оскільки програмне забезпечення та комп'ютерні бази даних є результатом висококваліфікованого інтелектуальної праці фахівців-професіоналів, а від надійної роботи комп'ютерних систем і прикладних програм залежить діяльність величезної кількості людей, які працюють в самих різних сферах в яких використовуються комп'ютерні технології, з самого початку входження комп'ютерної техніки в життя людської спільноти виникла необхідність захисту інформації від несанкціонованого її використання, небезпеки втрати або псування. Виникнення і глобальне поширення загальнодоступних комп'ютерних мереж поставило нові завдання перед розробниками засобів забезпечення захисту інформації та справило

визначальний вплив на всю сферу забезпечення інформаційної безпеки. Розглянемо докладніше основні питання, які відносяться до цієї галузі сучасної інформатики. [1]

Порушення безпечного функціонування комп'ютерної техніки прийнято називати ***інформаційними погрозами.*** Всі види інформаційних загроз, з якими стикається користувач сучасних обчислювальних пристроїв, можна розділити на дві основні групи:

- технологічні збої, тобто неможливість виконання будь-яких операцій та інші порушення працездатності використовуваних програмних і технічних засобів;
- навмисні шкідливі дії зловмисників, здатні перешкодити робочим процесам і (або) зруйнувати саме обчислювальний пристрій.

При інформаційні загрози першого типу виникає небезпека порушення фізичної і логічної цілісності зберігаються в оперативної і зовнішньої пам'яті структур даних через старіння або зносу її носіїв або через некоректне використання можливостей комп'ютера; можлива втрата даних та іншої важливої для користувача інформації через неправильне використання програмного забезпечення; руйнівного впливу різного роду помилок у програмних засобах, що не виявлених у процесі налагодження і випробувань програм, а також помилок, що залишилися в апаратних засобах після їх розробки, і т.п.

Основними способами захисту від інформаційних загроз першого типу є забезпечення структурної, тимчасової, інформаційної та функціональної надмірності комп'ютерних ресурсів, використання спеціальних програмних засобів, що попереджають неправильні дії користувача інформаційної системи, а також виявлення і своєчасне усунення помилок на етапах розробки програмно-апаратних засобів.

Другий тип інформаційних загроз є в даний час найбільш поширеним і менш вивченим. До таких загроз відносяться цілеспрямовані шкідливі дії інших людей (несанкціоноване копіювання інформації, порушення працездатності програмного і апаратного забезпечення, стороннє несанкціоноване використання ресурсів обчислювального пристрою з метою нанесення шкоди іншим користувачам комп'ютерної техніки, що перебуває у спільній комп'ютерної мережі, і т.д.).

Цей вид загроз безпеці використання обчислювальної техніки можна розділити на дві основні групи:

- шкідливі дії, які виконуються при постійному безпосередньої участі людини;
- шкідливі дії, які виконуються без безпосередньої участі людини спеціально розробленим для цих цілей програмним забезпеченням (вірусні програми, або програми - комп'ютерні віруси). [2]

Основні прийоми захисту від загроз такого роду однакові і полягають у забезпеченні заборони несанкціонованого доступу до ресурсів комп'ютера, а також до підключеним до нього пристроям; неможливість несанкціонованого

використання ресурсів комп'ютера після отримання до них доступу; своєчасне виявлення факту несанкціонованих дій і усунення їх причин та наслідків.

Основним способом заборони несанкціонованого доступу до ресурсів обчислювальних систем є підтвердження автентичності користувачів і розмежування їх прав на доступ до певних інформаційних ресурсів. Підтвердження автентичності користувача забезпечується виконанням процедури його ідентифікації, перевіркою автентичності особи та здійсненням контролю за всіма діями, обумовленими приписаними даному користувачеві повноваженнями доступу.

Ідентифікація користувача включає в себе ***реєстрацію*** в системі безпеки обчислювального пристрою унікального реєстраційного імені користувача ***(логіна)*** і відповідного цьому користувацькому імені - ***пароля.*** Встановлення автентичності користувача ***(аутентифікація)*** полягає в перевірці істинності його повноважень. Для особливо надійного впізнання при ідентифікації і аутентифікації користувача іноді використовуються спеціальні технічні засоби, що фіксують і розпізнають індивідуалізують людини фізичні та лінгвістичні характеристики (голос, відбитки пальців, структура зіниці, мовні особливості і т.д.). Однак такі методи вимагають значних витрат і тому використовуються рідко, так що основним і найбільш масовим засобом ідентифікації залишається парольний доступ. [3]

В даний час все більшої популярності набуває таке криптографічне засіб захисту інформації, як ***електронний цифровий підпис*** (ЕЦП). Вона вже стала досить часто використовуваним способом ідентифікації і аутентифікації користувача в банківській та інших сферах діяльності. Електронний цифровий підпис являє собою приєднане до якого-небудь тексту його криптографічне (зашифроване певним способом) перетворення, що дозволяє перевірити одержувачу тексту справжність його авторства і автентичність самого тексту.

Література:

1. Захист інформації - українське законодавство у сфері захисту інформації [Електронний ресурс]. – Режим доступу: http://library.detut.edu.ua/index.php/zahustinformacii.
2. Кузьменко Б.В., Чайковська О.А. Захист інформації. Навчальний посібник. Ч.1. (Організаційно-правові засоби забезпечення інформаційної безпеки) - К., 2009. – 83 с.
3. Богуш В.М., Довидьков О.А., Кривуца В. Г. Теоретичні основи захищених інформаційних технологій. Навч. посібник. – К.: ДУІКТ, 2010. – 454 с.

Тисячний Богдан Олегович студент групи УБДМ-51 Державного Університету Телекомунікацій

Сучасний етап розвитку української держави, як і багатьох держав світу, характеризується максимальною інформатизацією всіх сфер її життєдіяльності. В той же час перенесення багатьох процесів, зокрема й тих, що стосуються критичної інфраструктури, у т.з. кіберпростір, несе в собі разом з позитивними, також й негативні наслідки: уразливість цих процесів перед численними кіберзагрозами. Забезпечення безпеки у кіберпросторі є на сьогодні вкрай актуальним для нашої держави з огляду на те, що проти неї ведеться гібридна війна, одним з проявів якої є кібератаки на українські державні органи та установи, а також об'єкти критичної інфраструктури.

1. Неефективна нормативна база та система управління

1.1 Неефективна нормативна база та система управління.

1.2 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та серія нормативних документів про технічний захист інформації (НД ТЗІ) безнадійно застарілі.

1.3 Зобов'язання впровадження КСЗІ. Вона, окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність.

2. Неготовність реагувати на кіберінциденти.

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

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

2.3. Рівень обізнаності українців з питань кібербезпеки залишає бажати кращого. Державна програма для заповнення цієї прогалини в Україні наразі, на жаль, відсутня.

3. Низький рівень залучення професійної спільноти, відсутність трансформаційного підходу.

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

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

3.3. До того ж, через специфіку багатьох галузей (охорона здоров'я, енергетика, телекомунікації тощо) існує гостра потреба в окремих галузевих стандартах з кіберзахисту.

Посилання на джерела

1. https://zakon.rada.gov.ua/laws/show/2163-19

ТЕЛЕКОМУНІКАЦІЙНА І МЕРЕЖНА БЕЗПЕКА

Міщан Володимир Євгенович

Телекомунікації та мережі використовують різні механізми, пристрої, програмне забезпечення та протоколи, які є взаємопов'язаними і інтегрованими. Організація мереж є одним з найбільш складних питань в комп'ютерній області, що пов'язано в основному з великою кількістю застосовуваних концепцій і технологій. Адміністратор або інженер повинен знати, як налаштовувати мережеве програмне забезпечення, протоколи, сервіси, пристрої, враховуючи при цьому питання їх взаємодії. Він повинен встановлювати, налаштовувати і використовувати телекомунікаційне програмне забезпечення та обладнання, ефективно усувати неполадки. Спеціаліст з безпеки повинен не тільки розуміти ці питання, але і бути здатним проаналізувати їх на кілька рівнів глибше, щоб зрозуміти, де в мережі можуть виникнути уразливості. Це може бути вкрай складним завданням, що робить її більш цікавою

Телекомунікації - це електрична передача даних між системами з використанням аналогових, цифрових або бездротових видів передачі.

Еталонна модель взаємодії відкритих систем складається з семи рівнів:

7. Прикладний рівень працює в безпосередній близькості від користувача і забезпечує передачу файлів.

6. Представницький рівень отримує інформацію від протоколів прикладного рівня і перетворює її в формат, зрозумілий всім комп'ютерам, що використовують модель OSI.

5. Сеансовий рівень відповідає за створення з'єднань між двома додатками.

4. Транспортний рівень відповідає за взаємодію комп'ютерів.

3. Мережевий рівень відповідає за вставку в заголовок пакета інформації, необхідної для правильної адресації і маршрутизації цього пакета.

2. Канальний рівень - це рівень, на якому мережевий стек знає, який повинен застосовуватися формат кадру даних для правильної передачі.

1. Фізичний рівень перетворює біти в напругу для передачі.

TCP / IP - це набір протоколів, які керують переміщенням даних від одного пристрою до іншого.

IP - це протокол мережевого рівня, який надає послуги маршрутизації датаграмм.

Двома основними протоколами, які працюють на транспортному рівні, є TCP і UDP.

TCP - це надійний протокол з попереднім встановленням з'єднання.

UDP, з іншого боку, забезпечує кращу швидкість і не використовує попереднє встановлення з'єднань.

Типи передачі даних:

- Аналогова і цифрова
- Асинхронна і синхронна
- Односмугова і широкосмугова

Організація локальних обчислювальних мереж.

Топології мереж:

• Кільце
• Шина
• Зірка
• Повнозв'язна топологія

Для передачі даних використовуються три основні типи кабелів:

• Коаксіальний кабель складається з мідного центрального проводу, оточеного ізоляційним шаром і заземлюючим проводом.

• Вита пара складається з ізольованих мідних проводів, укладених в зовнішнє захисну оплетку.

• Оптоволоконні кабелі забезпечують передачу сигналів на великі відстані і з більш високою швидкістю, оскільки для передачі даних використовуються світлові хвилі.

Протоколи маршрутизації:

Динамічний протокол маршрутизації може знаходити маршрути і будувати таблицю маршрутизації.

Статичний протокол маршрутизації (static routing protocol) вимагає ручного налаштування таблиці маршрутизації адміністратором.

Протоколи **дистанційно векторної** маршрутизації приймають рішення про маршрути на основі відстані і вектора.

Протоколи маршрутизації **за станом каналу** будують більш точну таблицю маршрутизації, оскільки вони будують топологічну базу даних мережі.

Мережеві пристрої:

• Повторювачі
• Мости
• Маршрутизатори
• Комутатори

Міжмережеві екрани використовуються для обмеження доступу в одну мережу з іншої.

Фаєрволи:

• З фільтрацією пакетів.
• З контролем стану.
• Проксі.
• Проксі ядра.
• З динамічною фільтрацією пакетів.

Мережеві сервіси та Протоколи

Мережеві операційні системи

Служба доменних імен

DNS в Інтернет

NIS

Служби каталогів

Інтрамережі і екстрамережі

Інтрамережа (intranet - інтранет) - «приватна» мережа, в якій застосовуються інтернет-технології, такі як TCP / IP.

Екстрамережі (extranet - екстранет) поширюються за межі мережі компанії, дозволяючи двом або декільком компаніям спільно використовувати інформацію, створювати спільні ресурси.

Віддалений доступ включає в себе ряд технологій, які дозволяють віддаленим і домашнім користувачам підключатися до мережі для отримання доступу до мережевих ресурсів, які необхідні їм для виконання своїх завдань.

Список використаної літератури:

CISSP. Керівництво для підготовки до іспиту. П'ята редакція. Автор: Шона Харріс.

Білько Владислав Миколайович

Лавровський Ігор Миколайович

Баром Аліса Євгенівна

АТАКИ НА WEB-САЙТИ

Атаки на сайти — вчинення протиправних дій щодо веб-сайтів спрямованих на отримання конкурентних переваг шляхом злому, зараження шкідливими кодом, блокування доступу (з надалі вимогою викупу), крадіжку конфіденційних даних, виведення з ладу програмного забезпечення.

На першому етапі кібер-злочинець вивчає сайт на предмет вразливостей.

Вони, в свою чергу, бувають декількох типів:

Уразливості коду сайту. З’являються такі уразливості через помилки або недостатньої опрацюванні питання безпеки програмістами, що створюють CMS і розширення сайту. При наявності подібних вразливостей хакер може впровадити свій код в виконувані скрипти, запити до бази

даних (SQL-ін’єкції), поштового сервера сайту (email-ін’єкції), або в сторінку, яку користувач відкриває в своєму браузері, з метою крадіжки його особистих даних, включаючи паролі (міжсайтовий скриптинг).

Інтернет-сайти на популярних CMS зламують масово з метою зараження через типові уразливості. Що ж стосується DDoS-атак, то їх роблять на замовлення і тут є конкретні групи ризику. Наприклад, дуже часто атакують бізнес який залежить від інтернету і просто коштує грошей. Зловмисники починають атаку і пропонують власнику відкупитися. За статистикою найчастіше атакують:

– купонні сервіси;

– платіжні системи;

– Інформаційні агрегатори;

– Електронна комерція;

– Ігри та ігрові майданчики.

Веб-сторінки банків і електронних платіжних систем зламують з метою крадіжки грошей, сайти комерційних компаній ламають заради клієнтської бази і створення проблем конкуренту, або шантажу, вимагаючи гроші за відновлення нормальної роботи, сайти урядових органів і громадських організацій атакуються ідеологічними противниками.

Основним джерелом загрози для сайту є його власний код, написаний недбало, з помилками, без урахування строгих правил безпеки, а також використання застарілих, або викачаних з піратських сайтів модулів, розширень і плагінів.

Інша серйозна проблема – неправильне адміністрування. Надаючи користувачам надмірно широкі права, дозволяючи їм завантажувати на сайт файли без належної перевірки, адміністратор фактично відкриває ворота для всіляких вірусів, троянів, бекдорів та іншого шкідливого ПЗ.

Третє джерело небезпеки — погані паролі. Нарешті, ще одна, не пов’язана безпосередньо зі створенням і роботою сайту загроза — вміст як такий. Рушійною силою багатьох, в першу чергу DDoS-атак це помста. Від них не рятує найідеальніший код і надійне адміністрування — атака цілком і повністю йде ззовні. Зробити сайт стовідсотково стійким до будь-яких атак нереально. Можна лише ускладнити злочинцям досягнення їхніх цілей. Зрештою, атака на сайт вимагає часу і грошей, і якщо передбачувана вигода або збиток противника виявиться менше витрат на спробу злому — хакер переключиться на більш привабливу мету.

Принцип атаки переповнення буфера — програмні помилки, при яких пам’ять порушує свої ж кордону. Це, в свою чергу, змушує або завершити процес аварійно, або виконати довільний бінарний код, де використовується поточна обліковий запис. Якщо обліковий запис — адміністраторський, то дані дії дозволяють отримати повний доступ до системи.

Віруси, трояни, поштові черв'яки, сніфери – ці типи атак об'єднують різні сторонні програми. Призначення і принцип дії такої програми може бути надзвичайно різноманітним, тому немає сенсу докладно зупинятися на кожній з них. Всі ці програми об'єднує те, що їх головна мета — доступ і «зараження» системи.

Мережева розвідка – цей тип атаки сам по собі не передбачає будь-яких руйнівних дій. Розвідка має на увазі лише збір інформації зловмисником — сканування портів, запит DNS, перевірку захисту комп'ютера і перевірку системи. Зазвичай розвідка проводиться перед серйозною цілеспрямованої атакою.

Сніффінг пакетів: Принцип дії заснований на особливостях роботи мережевої карти. Пакети, отримані нею, пересилаються на обробку, де з ними взаємодіють спеціальні додатки. В результаті зловмисник отримує доступ не тільки до інформація про структуру обчислювальної системи, але і безпосередньо до переданої інформації — паролів, повідомлень та інших файлів.

Man-in-the-middle: Зловмисник перехоплює канал зв'язку між двома додатками, в результаті чого отримує доступ до всієї інформації, що йде через цей канал. Мета атаки — не тільки крадіжка, а й фальсифікація інформації. Прикладом такої атаки може служити використання подібної програми для шахрайства в онлайн-іграх: інформація про ігрову подію, що породжується клієнтською частиною, передається на сервер. На її шляху ставиться програма-перехоплювач, яка змінює інформацію за бажанням зловмисника і відправляє на сервер замість тієї інформації, яку відправила програма-клієнт гри

Ін'єкція також досить широкий тип атак, загальний принцип яких впровадження інформаційних систем зі сторонніми шматками програмного коду в хід передачі даних, де код фактично не заважає роботі додатка, але одночасно виконує необхідну зловмисникові дію.

Брутфорсом називається метод злому різних облікових записів, шляхом підбору логіна і пароля. Термін утворений від поєднання англійських слів brute force, що означають в перекладі «повний перебір». Ще брутфорс називають методом грубої сили. Його суть полягає в автоматизованому переборі всіх допустимих комбінацій пароля до облікового запису з метою виявлення правильного.

Цей різновид хакерської атаки ґрунтується на методі математики brute force. Рішення завдання знаходиться при переборі великої кількості символів, чисел, їх комбінацій. Кожен варіант перевіряється на вірність. З точки зору математики вирішити задачу таким способом можна завжди, але часові витрати на пошуки не у всіх випадках виправдовують мету, так як поле пошуку рішень величезне.

Брутфорс - один з найбільш популярних методів злому паролів облікових записів онлайн-банків, платіжних системах або на веб-сайтах.

Але з ростом довжини пароля цей метод стає незручним через тривалість витраченого часу на перебір всіх можливих варіантів. Таким методом можна перевіряти криптостійкість пароля.

Брутфорс ще називають методом вичерпування, так як рішення задачі полягає у вивченні всіх варіантів логічного ланцюжка, детальний аналіз кожної комбінації з метою знаходження істинно вірної. Класифікація та способи виконання брутфорс атаки.

Існує кілька видів «повного перебору»:

– Персональний злом. В цьому випадку брутфорс спрямований на отримання доступу до особистих даних користувача: акаунтів соціальних мереж, пошти, сайту. Під час спілкування через Інтернет, використовуючи схеми шахрайства, зловмисник намагається дізнатися логін, особисті дані та іншу інформацію, яка знадобиться йому для підбору пароля. Хакер прописує в програму злому адресу ресурсу, до якого потрібен доступ, логін, підключає словник і підбирає пароль. Якщо пароль користувача заснований на особистій інформації та складається з малої кількості символів, то спроба зловмисника може бути успішною навіть за короткий час;

– Брут-чек. Цей вид брутфорса означає полювання на паролі в великих кількостях. Тобто мета заволодіти даними не одного користувача, а отримати логіни і паролі від різних акаунтів на кількох веб-ресурсах. До хакерської програми підключається база логінів і паролів будь-яких поштових сервісів, а також проксі лист, щоб замаскувати вузол, не давши веб-сервісам пошти виявити атаку. При реєстрації на сайті, в соціальній мережі або в грі користувач заповнює поле з адресою своєї пошти, на який приходять дані для входу в відповідний аккаунт. В опціях брутфорса прописується список назв сайтів або інших ключових слів, за якими він буде шукати в поштових скриньках саме ці листи з логінами і паролями, виймати і копіювати інформацію в окремий файл. Так хакер отримує сотні паролів і може використовувати їх в будь-яких цілях;

– Віддалений злом системи комп'ютерного пристрою. Брутфорс в комбінації з іншими утилітами зламу застосовується для отримання доступу в систему віддаленого ПК з встановленим паролем. Злом такого виду полягає в пошуку IP-мереж для атаки. Адреси користувачів видобуваються через спеціальні програми або беруться з баз. Словники перебору і IP-адреси прописуються в налаштуваннях брутфорса. У разі успішного підбору пароля зберігається IP-адреса обчислювальної машини жертви, дані для входу, які далі використовуються зловмисником з метою повного управління ПК через утиліту Radmin з відображення робочого столу віддаленої машини на моніторі хакера.

DoS — атака, що має своєю метою змусити сервер не відповідати на запити. Такий тип атаки не має на увазі безпосередньо отримання деякої секретної інформації, але використовується для того, щоб паралізувати роботу цільових сервісів. Наприклад, деякі програми через помилки в своєму

коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не в змозі обробити всі вхідні пакети.

DDoS — підтип DoS атаки, що має ту ж мету що і DoS, але що проводяться не з одного комп'ютера, а з декількох комп'ютерів в мережі. В даних типах атак використовується або виникнення помилок, згенеровано відмова сервісу, або спрацьовування захисту, що викликає блокування роботи сервісу, а в результаті також і відмова в обслуговуванні. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об'єднуються, і кожен виробляє DoS атаку на систему жертви. Разом це називається DDoS-атака.

Класифікація DoS і DDoS атак:

– Насичені смуги пропускання – атака, пов'язана з великою кількістю безглуздих запитів до сайту, з метою його відмови через вичерпання системних ресурсів - процесора, пам'яті або каналів зв'язку;

– HTTP-флуд і PING-флуд – примітивна DoS атака, метою якої є насичення смуги пропускання і відмова сайту в обслуговування. Успіх атаки безпосередньо залежить від різниці розмірів ширини каналу сайту, що атакується і атакуючого сервера;

– SMURF-атака (ICMP-флуд) – одна з найнебезпечніших DDoS атак, коли атакуючий використовує трансляцію розсилку для перевірки працюючих вузлів в системі, відправляючи ping-запит. У ній по широкосповіщеним адресам атакуючий відправляє підроблений ICMP пакет. Потім адресу атакуючого змінюється на адресу жертви. Всі вузли надсилають їй відповідь на ping-запит. Тому ICMP-пакет, відправлений атакуючим через посилює мережу, що містить 200 вузлів, буде посилено в 200 разів;

– FRAGGLE-атака (UDP-флуд) – атака, аналогічна SMURF – атаці, де замість ICMP пакетів використовуються пакети UDP. Принцип дії цієї атаки простий: на атакуючий сервер відправляються echo-команди по широкосповіщеному запиту. Потім підміняється ip-адреса зловмисника на ip- адресу жертви, яка незабаром отримує безліч відповідей на них. Ця атака призводить до насичення смуги пропускання і повної відмови в обслуговуванні жертви. Якщо все ж таки служба echo відключена, то будуть згенеровані ICMP- повідомлення, що також призведе до насичення смуги;

– Атака пакетами SYN (SYN-флуд) – суть атаки полягає в наступному: два сервера встановлюють TCP з'єднання, установку якого виділяється невелика кількість ресурсів. Відправивши кілька помилкових запитів, можна витратити всі ресурси системи, відведені на встановлення з'єднання. Робиться це підміною істинного IP на неіснуючу IP адресу атакуючого сервера, при відправці SYN пакетів. Сервер – жертва буде створювати чергу з необроблених з'єднань, яка вичерпає його ресурси. Визначити джерело такої атаки вкрай складно, тому що істинні адреси

атакуючих серверів підміняються на неіснуючі.

У деяких випадках до фактичної DDoS-атаки призводить ненавмисні дії, наприклад, розміщення на популярному ресурсі посилання на сайт, розміщений на не дуже швидкому і продуктивному сервері. Великий наплив користувачів так само призводить до перевищення допустимого навантаження на сервер а, отже, до відмови в обслуговуванні.

Використовувати при створенні лише надійні, перевірені CMS, якщо сайт побудований на CMS. А якщо сайт розробляється вручну, з 0, без використання готових систем управління контентом, то доручати його написання команді досвідчених професіоналів. При використанні готових систем управління контентом регулярно їх оновлювати більшість, оновлень призначені якраз для усунення чергових виявлених уразливостей. Не можна використовувати старі, і вже тим більше неоновлювані CMS, вразливості в їх системах безпеки ніким не закриваються і добре відомі хакерам, які не забаряться ними скористатися. Те ж саме стосується будь-яких додатків і розширень. Безкоштовні додатки та розширювання слід завантажувати тільки з сайтів офіційних розробників і своєчасно оновлювати їх, платні версії — купувати ліцензійну версію, або відмовитися від їх використання. За умовно-безкоштовне скачування з піратського сайту в кінцевому рахунку доведеться заплатити набагато більше, коли знадобиться відновлювати як вміст, так і репутацію в очах пошукових систем, які ігнорують сайти, що містять нерелевантні посилання і поширюють заражені файли. Необхідно чітко розмежувати права різних категорій користувачів.

Ніхто не повинен мати більше можливостей, ніж необхідно. Паролі для адміністраторів і привілейованих груп користувачів повинні бути складними. Бажано використовувати різні програми і утиліти, що підвищують безпеку. Непогано також перевірити сайт спеціальними програмами пошуку вразливостей, або, якщо надійність важлива і фінанси дозволяють, доручити задачу професіоналам. Захист від DDoS-атак (в крайньому разі, низької та середньої потужності) здійснюється розміщенням сайту на серверах високої пропускної здатності, також використовується аналіз і фільтрування трафіку з блокуванням IP атакуючих машин. У разі ж потужних атак часто залишається лише перечекати, поки вона припиниться. Замовники DDoS-атак рідко мають у своєму розпорядженні власні ресурси для її проведення, і змушені платити хакерам-власникам ботнетів (мереж заражених комп'ютерів, з яких і ведеться атака). Відповідно, потужна атака коштує чималих грошей, і рідко триває довше декількох днів. А щоб знизити ймовірність DDoS-атак, не варто розміщувати контент, образливий для великих груп людей або впливових структур, здатних помститися. Нарешті, варто регулярно створювати резервні копії сайту, щоб в разі серйозних проблем швидко його відновити.

Перелік використаних джерел

1. anti-malware.ru //Комплексная и многофункциональная защита информационных ресурсов рабочих станций и серверов. [Електронний ресурс]. Режим доступу: World Wide Web. –URL: https://www.anti-malware.ru/threats/websites-attacks
2. Електронний журнал «Хакер» //Sqlmap: SQL-инъекции. [Електронний ресурс].Режим доступу: World Wide Web. – URL: https://xakep.ru/2011/12/06/57950
3. anti-malware //Брутфорс [Електронний ресурс]. –Режим доступу: https://www.anti-malware.ru/threats/brute-force
4. it-click // Виды хакерских атак на веб-ресурсы [Електронний ресурс]. –Режим доступу: World Wide Web. – URL: http://www.it- click.ru/articles/web-studio/hacking-web-site.aspx
5.OWASP //The free and open software security community [Електронний ресурс]. –Режим доступу: World Wide Web. – URL: http://www.owasp.org

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ WEB-ПОРТАЛУ

Лавровський І.М. БСДМ - 61

Магістерська робота присвячена технології забезпечення безпеки та виробленню рекомендацій щодо побудови системи захисту інформації веб-порталу.

Об’єкт дослідження: технологія забезпечення безпеки та система захисту інформації веб-порталу.

Мета роботи: розробити рекомендації підприємцям щодо побудови системи захисту інформації веб-порталу. Тим самим допомогти починаючим підприємцям захистити свій веб-портал та, як наслідок, бізнес. Для цього у роботі розглядаються шляхи забезпечення безпеки, їх види, принципи роботи.

Як результат у магістерській роботі досліджено шляхи забезпечення безпеки та розроблено рекомендації, щодо побудови системи захисту інформації веб-порталу на прикладі CMS WordPress. У роботі було виявлено основні проблеми та вразливості веб-порталу. Також було запропоновано методи вирішення цих проблем.

ВИВЧЕННЯ ОСНОВНИХ ВРАЗЛИВОСТЕЙ ВЕБ-ПОРТАЛУ НА ПРИКЛАДІ CMS WORDPRESS

Як одна з найпопулярніших у світі програм з відкритим кодом, WordPress є метою для постійних атак. Оскільки база користувачів продовжує зростати, і її позиції найпопулярнішої CMS у світі закріплюються, можна сказати напевне, що ця тенденція не змінюватиметься.

Виникнення значних вразливих місць в цьому році ще раз нагадує нам про необхідність постійної пильності та збереження сайтів оновленими.

Число компаній, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз.

Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію.

У відповідь на масові зломи систем безпеки був створений консорціум OWASP – Open Web Application Security Project, це відкритий проект забезпечення безпеки веб-додатків. Однак і зловмисники, і фахівці в області кібербезпеки продовжують знаходити вразливості в веб-додатках, які можуть привести до серйозних втрат з боку бізнесу.

Основною причиною більшості взломів в веб-додатках є написаний розробниками програмний код. Розробники можуть допускати помилки при написанні коду або не усвідомлювати всю важливість використання прийомів безпечного програмування – все це призводить до появи вразливостей в додатках.

ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ВЕБ-ПОРТАЛУ

Як тільки веб-додаток стає доступним в мережі, він робиться мішенню для кібератак. Незалежно від того, чи здійснюється атака цілеспрямовано зловмисниками, чи є результатом роботи автоматизованого шкідливого ПЗ, будь-який веб-додаток постійно перевіряється хакерами на стійкість. Відповідно, перш ніж починати використовувати веб-додаток, необхідно забезпечити його захист.

Безсумнівно, захист веб-інфраструктури потрібний для будь-якої компанії. Однак з безлічі категорій захисних рішень – Firewall, IPS/IDS, NGFW (Next Generation Firewall), WAF (Web-Application Firewall) тільки Web Application Firewall здатний забезпечити комплексний захист веб-додатків від відомих і невідомих загроз, а також забезпечити відповідність вимогам регуляторів. Ні класичний Firewall, ні IPS/IDS не зможуть забезпечити адекватного захисту веб-додатків.

Висновок: Матеріали роботи можуть бути використані при побудові системи захисту інформації. Дотримання всіх рекомендацій та використання шляхів забезпечення безпеки, запропонованих в даній роботі, забезпечить захищене функціонування веб-порталу, в компаніях та корпораціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Top 5 WordPress Vulnerabilities and How to Fix Them [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://www.esecurityplanet.com/open-source-security/top-5-wordpress-vulnerabilities-and-how-to-fix-them.html

2. A History of WordPress Security Exploits and What They Mean [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://premium.wpmudev.org/blog/wordpress-security-exploits/

3. Rolf Oppliger, Ph.D., SSL and TLS Theoryand Practice. Gümligen, Switzerland. – 2009. – С. 75–77.

4. WCSLC_2016_WP_Security_101 with Logan Kipp

Киричок Р. В.
аспірант кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій
м. Київ, Україна

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЯКОСТІ АНАЛІЗУ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

У зв’язку зі стрімким розвитком сучасних інформаційних технологій та їхнім інтегруванням в усі важливі сфери діяльності суспільства, виникає необхідність в надійному забезпеченні їхньої безпеки. А зважаючи на боротьбу спеціалістів інформаційної безпеки (ІБ) з кіберзловмисниками, що з кожним днем породжує тисячі нових кіберзагроз, все більш значиму роль відіграє моніторинг та аналіз захищеності інформаційних систем в процесі експлуатації.

Аналіз захищеності спрямований саме на виявлення уразливостей (на ранніх стадіях) з метою підвищення рівня захищеності цільової інформаційної системи (ІС) та даних, які оброблюються та зберігаються в ній. Це як гра на випередження, «хто перший виявить уразливість в інформаційній системі», якщо першим вразливість знайде зловмисник – в нього є можливість її використати та скомпрометувати систему, якщо ж спеціаліст з ІБ – є можливість закрити вразливість прийнявши певні контрміри. До основних підходів вирішення даного питання можна віднести як формальні методики (серед яких необхідно виділити методи імітаційного моделювання, що базуються на використанні дерев атак, мереж Петрі та графів атак) так і інструментальні засоби (які можна умовно поділити на два типи: засоби виявлення уразливостей, такі як ScanOVAL, Nessus Scanner, OpenVAS, Rapid7 Nexpose та засоби тестування на проникнення, тобто перевірки (валідації) та підтвердження конкретних вразливостей – Metasploit Framework, SQLmap, Core Impact).

Однак, вищезазначені підходи мають ті чи інші недоліки, так існує необхідність в ручному складанні формальних специфікацій, визначених конкретною моделлю; відсутня валідація даних, одержуваних від інтегрованих інструментальних засобів (звісно якщо їхнє використання взагалі передбачено

моделлю) або необхідність у висококваліфікованих спеціалістах для проведення ручної перевірки вразливостей цільової ІС, що в свою чергу також породжую ще один недолік, а саме довгу тривалість таких перевірок. Звісно ж необхідно згадати про засоби автоматизації (як от, наприклад, auto_pwn в Metasploit Framework), які частково пом'якшують дані недоліки, однак не вирішують цілком, оскільки виконується послідовний запуск експлойтів з урахуванням простих критеріїв, таких як сімейство операційної системи, сервіс та ранг експлойта, що знову ж таки займає чимало часу та призводить до ризику повного виведення з ладу цільової системи внаслідок використання некоректно підібраного експлойта.

Одним із перспективних направлень є дослідження можливості використання штучного інтелекту, зокрема машинного навчання та нейромережі.

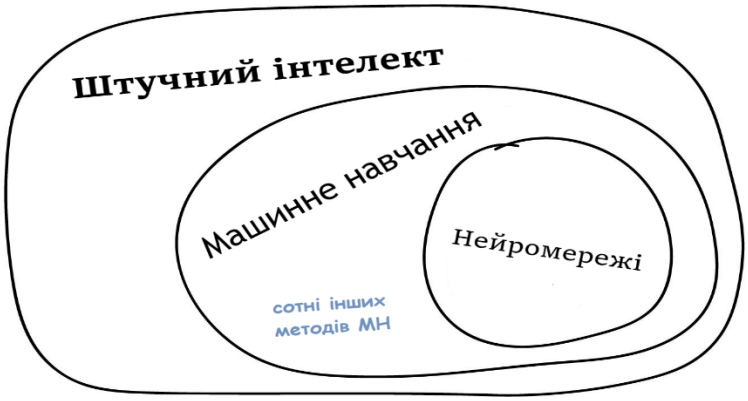


Рис.1 Структурна схема основних термінів штучного інтелекту

Таким чином, штучний інтелект (англ. Artificial intelligence, AI) – це наука та технологія створення інтелектуальних машин, в особливості інтелектуальних комп'ютерних програм, основною властивістю яких є виконання творчих функцій, що традиційно вважаються прерогативою людини.

Машинне навчання – один із розділів AI, що дозволяє робити висновки на підставі даних, не слідуючи жорстко заданим правилами. Тобто інтелектуальна машина може знайти закономірність у складних та багато-параметричних завданнях і як результат – є вірне прогнозування.

Нейромережі є одним із видів машинного навчання і будуються за допомогою штучних нейронів, які моделюють роботу людського мозку (нейронів), що вирішують певні завдання та мають здатність до самонавчання з урахуванням попереднього досвіду.

Загалом на сьогоднішній день існує велика кількість різноманітних алгоритмів машинного навчання, однак всі їх можна розділити за чотирма основними напрямками:

- класичне навчання – перш за все використовується в завданнях класифікації, кластеризації, регресії і т.п.;
- нейромережі і глибоке навчання – застосовуються здебільшого для розпізнавання або генерації зображень і відео, в складних алгоритмах управління або прийняття рішень, в машинному перекладі та інших подібних складних завданнях;

- навчання з підкріпленням – використовують у випадках, коли машині необхідно правильно виконати поставлені їй завдання у зовнішньому середовищі маючи безліч можливих варіантів дії;
- ансамблеві методи – поєднання кількох підходів.

При всіх можливостях та перевагах використання технологій штучного інтелекту для аналізу захищеності ІС в більшості випадках існує проблема недостатньої кількості якісних навчальних даних і саме за таких умов при розробці нового методу аналізу захищеності шляхом інтелектуального проникнення використовується навчання з підкріпленням. Що дозволить на основі взаємодії з досліджуваною ІС та спостереженні її реакції навчити розроблений засіб проникнення та в подальшому оцінювати фактичний стан захищеності системи без складання формальних специфікацій та без необхідності в ручній валідації усіх вразливостей.

Література:
1. Глибовець М.М. Системи штучного інтелекту / Глибовець М.М., Олецький О.В. // К.: КМ Академія. – 2002. – С. 366.

Стеблина Сергій Васильович
Держаний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

МІЖНАРОДНІ СТАНДАРТИ ПО КРИПТОГРАФІЧНИМ ПРОТОКОЛАМ ІДЕНТИФІКАЦІЇ/АВТЕНТИФІКАЦІЇ

Основним міжнародним стандартом по криптографічним протоколам аутентифікації є стандарт Міжнародної організації по стандартизації та Міжнародної електротехнічної комісії ISO / IEC 9798 - Information technology – Security techniques - Entity authentication mechanisms, що складається з п'яти частин :

ISO / IEC 9798-1 - «General Model»;
ISO / EEC 9798-2 - «Mechanisms using symmetric encipherment algorithms »;
ISO / EEC 9798-3 - «Entity authentication using a public-key algorithm »;
ISO / IEC 9798-4 - «Mechanisms using a cryptographic check function»;
ISO / IEC 9798-5 - «Mechanisms using zero knowledge techniques».

У цих протоколах претендент і перевіряючий мають симетричний секретний ключ або ключі парно-вибіркової зв'язку. Для їх отримання може використовуватися довірений сервер в режимі реального часу.

Стандартом ISO / IEC 9798-2 передбачені три способи аутентифікації (зірочками в таблицях позначені необов'язкові компоненти повідомлень):

1. Одностороння аутентифікація, заснована на мітці часу. Якщо у претендента і перевіряючого є системний годинник, немає необхідності надсилати запит. претендент відразу може направити повідомлення з включеною в нього міткою часу, а перевіряючий - звірити мітку з показаннями свого годинника.

2. Одностороння аутентифікація з використанням випадкових чисел. В якості запиту перевіряючий посилає випадкове число, сгенерированное з допомогою генератора псевдовипадкових чисел. Отримавши запит, претендент обчислює відповідь на нього - зашифровує з допомогою алгоритму симетричного шифрування отримане випадкове число і (якщо необхідно) ідентифікатор. перевіряючий розшифровує отриманий шифртекст і перевіряє структуру запиту. Якщо вона вірна, він приймає претендента.

3. Взаємна аутентифікація з використанням випадкових чисел. Відмінність цього протоколу від попереднього в тому, що тут кожен з учасників поочередале виконує ролі перевіряючого і претендента, т. е. вони перевіряють аутентічність один одного.

Протокол взаємної аутентифікації - це по суті два протоколи односторонньої аутентифікації, «упаковані» в три пересилання повідомлення. Подібного роду протоколи в силу їх симетричності називаються протоколами рукостискання. цей протокол допускає заміну шифру на хеш-функцію з ключем, як зазначено в стандарті ISO / IEC 9798-4. Для підвищення стійкості протоколу до переданим повідомленням можна додати мітки часу.

Протоколи «запит - відповідь» з використанням асиметричних криптосхем

Такі протоколи можна розділити на дві групи: протоколи з використанням ЕЦП і протоколи з використанням схем відкритого шіфрованія.В стандарті ISO / IEC9798-3 рекомендовані:

1) протоколи з використанням схем цифрового підпису:

В описах протоколів зустрічаються позначення certA сертифікатів відкритих ключів цифрового підпису відповідних учасників протоколу, тобто структури даних, містять їх ідентифікатори, відкриті ключі і іншу службову інформацію, завірену цифровим підписом засвідчувального центру. Детальніше метод сертифікації відкритих ключів буде розглянуто пізніше. Протоколи, подібні описаним вище, використовуються також в стандарті Міжнародного телекомунікаційного союзу ITU X.509. У ньому описані протоколи аутенті-ції, суміщені з протоколами обміну ключами.

2) протоколи з використанням схем відкритого шифрування.

Загрози безпеки ІКС можна поділити на мережеві атаки (інформація, яка надходить з віддаленого агента) і локальні атаки, які походять від шкідливих програм, вже встановлених на системі клієнта, наприклад, троянів, руткітів тощо. Часто оцінки безпеки автентифікації зосереджені переважно на мережевих атаках, припускають, що користувальницький термінал (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою. Проте нерідко зловмисник отримує повний доступ до ПК жертви через приховані процеси зв'язку, які залишилися від шкідливих програм, що використовують невиправлені діри в безпеці ліцензійного програмного забезпечення.

Типовими методами атак на протоколи аутентифікації:

1. Самозванство (impersonation) - один користувач намагається видати себе за іншого.
2. Повторна передача (replay attack) – повторна передача колишніх аутентифікаційних даних будь-яким користувачем.
3. Підміна боку аутентификационного обміну (Interleaving attack) - зловмисник в ході атаки має можливість модифікувати проходить через нього трафік.
4. Відображення передачі (reflection attack) - один з варіантів атаки підміни, коли в рамках даного Сенсу зловмисник пересилає назад перехоплену інформацію.
5. Вимушена затримка (forced delay) – зловмисник перехоплює деяку інформацію і передає її через деякий час.
6. Атака з вибіркою тексту (chosen-text attack) - зловмисник перехоплює трафік і намагається отримати інформацію про довготривалі ключах.

Література:

1. Василюк В.Я., Климчук СО. Інформаційна безпека держави : Курс лекцій. - К.: КНТ, Видавничий дім «Скіф», 2008. - 136с,
2. Баранов О.А. Інформаційне право України: Стан, проблеми, перспективи. -К.: Видавничий дім «СофтПрес», 2005. - 316с.
3. Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: «МК-Прес», 2005.-432с.

УДК 004.056.053

МЕТОДИКА УДОСКОНАЛЕННЯ АПАРАТНО ПРОГРАМНОГО КОМПЛЕКСУ РАДІОМОНІТОРИНГУ.

Лаптєв О.А.ктн,снс.
Половінкін І.М.квн,снс
Клюковський Д.В. аспірант

В даних тезах оглянути основні характеристики засобів радіомоніторингу, виявлено частотний діапазон середньостатистичних загроз несанкціонованого отримання інформації, розглянуто тенденції розвитку засобів негласного отримання інформації (ЗНОІ)

Ключові слова: радіомоніторинг, частотний діапазон, апаратно програмний комплекс.

Введення. Для ефективного вирішення завдань захисту інформації необхідний якісний аналіз загроз та аналіз можливих каналів витоку інформації. Цей процес пов'язаний зі збором всієї можливої інформації навколо носіїв і об'єктів захисту. Обсяг отриманої інформації про загрози обмежується, з одного боку, можливостями контрольної апаратури, з іншого - можливістю ефективно цю інформацію обробити. Стосовно до апаратури контролю радіоефіру -радіомоніторингу-ефективність одержуваної інформації визначається, перш за все, її якістю та повнотою відображення. Повнота відображення визначається, зокрема, діапазоном досліджуваних частот.

Аналіз засобів контролю радіоефіру (радіомоніторингу), представлених на сучасному ринку показує, що так званий середньостатистичний частотний діапазон загроз є 25-3000 МГц (діапазон в якому підвищена ймовірність використання ЗНОІ) В цьому діапазоні виготовляються ЗНОІ- зв'язку з дешевизною та простотою виготовлення. Однак у хід йдуть різні методи маскування: використання перескоків частоти передачі, розширення спектра сигналу до шуму подібного, над короткі виходи в ефір в найбільш безпечний час і, зокрема, вихід за частотні діапазони (25-3000 МГц), де вони не піддаються контролю з боку фахівців захисту інформації, тобто вони не потрапляють в робочий діапазон що переважає на ринку - пошукового обладнання.

Виходячи з огляду ЗНОІ - діапазон частот так званих середньостатистичних загроз засобів знімання інформації 25-3000 МГц, в якому працює більшість універсальних приладів пошуку ЗНОІ вимагає значного розширення. Проблема пошуку засобів негласного знімання інформації за межами серед нестатистичного діапазону є актуальною.

Проводячи аналіз пошукових засобів негласного отримання інформації ЗНОІ- закладок -закладка-закладний пристрій (ТЗІ)-потай встановлюваний технічний засіб, який створює загрозу для інформації [3], можливо зробити висновок: основні діапазони роботи цих засобів - НВЧ (30-300 МГц) плюс УВЧ (300-3000 МГц).Данні пошукових засобів приведені в табл.1.

Таблиця 1.

Частотний діапазон засобів радіомоніторингу

Засоби пошуку ЗНОІ	Основний діапазон пошуку	Наявність приладу, збільшеною частоті
Детектори поля		

NR-D	50-3500 МГц	
ST-110	50-2500 МГц	антенна-перетворювач до 7 ГГц
RAKSA 120	50-3200 МГц	
SEL SP-75 Black Hunter	100-3000 МГц	
Універсальні пошукові пристрої		
ST-033 "Пиранья"	30-2500 МГц	ST 03.SHF до 10 ГГц
ST-131 "Пиранья-2"	30-4100 МГц	ST 131.SHF до 18 ГГц
СРМ-700	200 Гц - 3 ГГц	ВМР-1200 до 12 ГГц
Скануючи приймачі		
AOR 8200	30-3000 МГц	
Скорпион-XL	30-2500 МГц	
Контур	30-2500 МГц	
Комплекси радіомоніторингу		
"Кассандра-М"	24-3000 МГц	СВЧ-конвертер до 18 ГГц
ОМЕГА	25-3000 МГц	ОМЕГА-К18 до 18 ГГц
OSC-5000	10 кГц - 3 ГГц	MDC-1200 до 21 ГГц
RS digital Mobile	50-2000 МГц	СВЧ-конвертер RS/DC до 12 ГГц

Це обумовлено тим що більшість доступних ЗНОІ використовують саме ці діапазони. Перш за все, через дешевизну та простоту створення передавачів, які легко створити на базі доступних модулів стандартних радіоканалів (табл. 2).

Таблиця 2.

Типові частотні діапазони резонаторів для гетеродинів ЗНОІ

292-294 МГц	378-391 МГц	857-868 МГц
302-326 МГц	402-434 МГц	914-916 МГц, 979-981 МГц

Однак за межами вищевказаного середньостатистичного діапазону загроз знаходяться, випромінювання цивільних і військових радіорелейних станцій (діапазони 3,6; 4, 7 ГГц і вище), випромінювання літакових РЛС, РЕМ управління повітряним рухом, метеорології, морські радари, засоби супутникового зв'язку, та, системи широкосмугового доступу Wi-Fi і WiMAX. Останні найцікавіші, оскільки дозволяють організувати канали витоку інформації, використовуючи як легальні мережі, так і передавачі на базі стандартних модулів широкосмугових систем. Тобто канали радіопередачі ЗНОІ виходять за традиційно аналізовані УВЧ та НВЧ. Це:

1. ЗНОІ мереж широкосмугового доступу.
2. Пристрої, створені на основі готових радіо модулів.
3. Спеціально розроблені пристрої на базі новітніх СВЧ радіоелементів.

Для нейтралізації цих загроз необхідно перш за все їх виявити. Для виявлення пристроїв першої групи загроз використовуються звичайні карти широкосмугового доступу зі спеціальним програмним забезпеченням, що дозволяє проаналізувати топологію мережі і відфільтрувати "чужі" сигнали. Прикладом такої програми може служити спеціалізоване ПО «DeltaX».

Для виявлення другої групи можна використовувати той факт, що для них міжнародними угодами визначено фіксовані діапазони частот. Так СВЧ діапазоні це 3,4-3,7 ГГц і 5,15-5,85 ГГц.

Виходячи з цих міркувань, визначаємо, що стандартну верхню межу діапазону контролю радіоефіру потрібно підняти як мінімум до 6 ГГц.

Цей висновок змусив переглянути методику створення апаратно програмних комплексів (АПК). Стало очевидно, що розроблені в даний час АПК типу "Кассандра-М" та ін., навіть до оснащені СВЧ конвертерами, перестали задовольняти сучасним вимогам.

Була розроблена нова методика побудови АПК яка передбачає уніфікацію елементів і створення радіо контрольних комплексів під необхідний діапазон підбором відповідного тюнера. Новий удосконалений тюнер з робочою частотою яка збільшена до 6 ГГц, за своїми основними характеристиками — чутливості та динамічному діапазону — не поступається класичним трьох гігагерцовим. Така методика дозволяє будувати АПК які задовольняють сучасним вимогам.

Висновки

1.Розглянуто основні характеристики засобів радіомоніторингу, визначений граничний діапазон середньостатистичних загроз, який складає 25-3000 МГц.

2. Визначено тенденції розвитку ЗНОІ та алгоритми передачі інформації (переважно — цифрові) яких дозволяють створювати стійкі, які не піддаються перешкод канали зв'язку на частотах до 6ГГц канали передачі інформації.

Література:

1.А.В.Кривцун Радиомониторинг: частотній диапазон. [Электронный ресурс] режим доступу: http://detektor.ru/files/publikaci/binder1_mini.pdf (1.06.2019)

2. Обзор технических средств, использующихся для получения конфиденциальной информации [Электронный ресурс] режим доступу:http://anb-rf.narod.ru/means.htm (04.06.2019)

3. Захист інформації. Технічний захист інформації .Терміни та визначення (ДСТУ 3396.2-97) .– [Дійсний від 01.01.1998]. – (Державний Стандарт України).

4. Распределение частот для аппаратуры радиоуправления [Электронный ресурс] режим доступу : http://www.aviaboy.com/content/view/24/21/(04.06.2019)

APPLICATION OF STEGANOGRAPHIC METHODS FOR PROTECTION OF CONFIDENTIAL DATA

Писаренко Павло Володимирович
Pavlo Pysarenko

The work contains information on steganographic methods, their scope and basic principles of work. There is also a description of the informal requirements for the qualitative use of such methods. Steganography is relevant to cybersecurity today, as this approach is used to protect, in particular, intellectual property. The need for secure transmission of sensitive data has been raised. The thesis can be useful for cybersecurity professionals.

Key words: digital steganography, intellectual property, protection, sensitive data, copyright.

Steganography is a science that studies ways to protect information by concealing the fact of sending it. It is usually used when sensitive and other data is being transmitted . It is advisable to consider digital steganography - the direction of steganography, which implies copying the contents of some digital file for its further insertion into another digital file, which in this case is called a container file [1, p.176].

First of all, it is used to protect copyrights when electronic files include "watermarks" and other marking objects. Such changes to files may result in distortions. In order for the process of applying steganographic methods and means to be successful, it is necessary that the changes made are invisible without the use of specially developed software or other means of their detection, because that is the essence of hiding the fact of sending any sort of infromation at all. The container file can be represented by a text file, an image, an audio file and so on.

The easiest way to use digital steganography is to use bitmap images (.bmp or .jpg extension) and change the least significant bits by converting them to bits of the message that is to be secretly sent. Such changes will not be noticeable to the naked eye.

An additional advantage of steganographic methods as such is the fact that changes can only be theoretically noticeable only the ones who have already been able to view the original file, which is not the case. It is worth noting that the stability of such a system (a "combined" container file) not only depends on the capabilities of the recipient of the file, the method of encoding information and its further insertion to the container, but also on the number of changes made and, by extension, the recorded information.

In general terms, the graph that shows how the difficulty of change detection is dependent on the amount of data embedded in the container file is shown in Figure 1 [1, p.177].

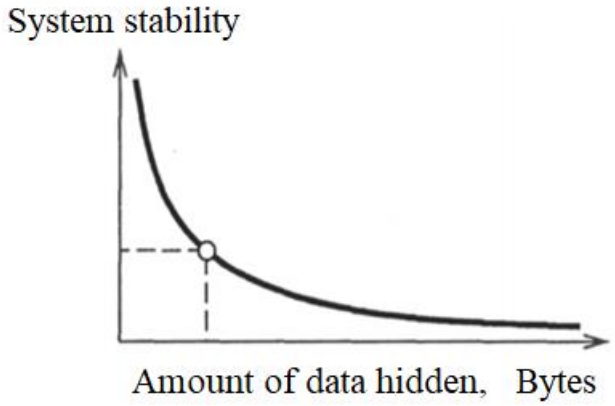


Figure 1 – Correlation between steganographic system stability and the amount of input data

The point characterizing the optimal conditions for each resulting file is noticable on the graph. It is neither possible to clearly quantify how much information is worth entering, nor the level of sustainability it guarantees. However, one can talk about the percentage of content of each file involved. Typically, professionals are looking for the ratio of the changed data to the total file size of 1:5.

The fairly simple pieces of software to work with such methods are ExifTool, ExifViewer, Steghide and others.

Conclusion

Hence, digital steganography is first and foremost used to protect copyrights and is also an effective method for safe transmission of sensitive information. The advantage of this direction over, for example, cryptography is that a third-party recipient will not be able to compare the received file with the original and will most likely consider it as an authentic one without trying to look for anything. Also, the quality of using steganography methods depends on the ratio of the volume of changes made to the volume of the entire resulting file.

Source:

1. A.Horpeniuk, A. Storozhenko — Дослідження та порівняльний аналіз стеганографічних методів для впровадження даних у цифрові файли, p. 176-177.

Злотін Іван Олегович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Призначення комплексної системи захисту інформації

Головна мета створення системи захисту інформації – забезпечення надійності ЗІ. Система ЗІ - це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого – самі організовують систему, здійснюючи захисні заходи.

Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами та пов'язаний з ними логічно і технологічно.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальні СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правова, організаційна, інженерно-технічна).

По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які забезпечують або можуть впливати на якість захисту. Наприклад, система охоплює якісь об'єктів захисту, а всі вони внесені до неї чи ні – це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися все, виходячи з цілей і завдань захисту заходу.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, в всіх місцях її збирання, зберігання, передачі і використання, весь час і при всіх режимах функціонування систем обробки інформації.

У той же час комплексність не усуває, а, навпаки, передбачає диференційований підхід до захисту інформації, залежно від складу її носіїв,

видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умов прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації полягає у:

– інтеграції локальних систем захисту;

– забезпеченні повноти всіх складових системи захисту;

– забезпеченні всеосяжність захисту інформації.

Виходячи з цього, можна сформулювати таке означення:

«Комплексна система захисту інформації – система, що повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї захищуваної інформації».

Використання рішень IBM для захисту платіжних систем

Щебланін Олександр Юрійович
Державний університет телекомунікацій
Інститут захисту інформації

Програмне рішення Safer Payments було розроблено компанією IBM для запобігання шахрайству у сфері платіжних систем.

IBM Safer Payments, інсталюється на сервері або окремо виділеному ресурсі та постійно моніторить ефективність впроваджених методів та обраних правил протидії шахрайству. Для простоти використання в інтерфейсі програми реалізовано функцію, яка при виявленні застарілості правила, змінює колір запису , що свідчить про необхідність втручання спеціаліста для аналізу та зміни правила. У той самий час штучний інтелект розроблює нові контрзаходи щодо шахрайства, які потім надаються для аналізу користувачу (адміністратору).

Зазвичай серверам продукту надають обчислювальні можливості для аналізу максимальної кількості транзакцій. Однак більшість цих ресурсів не потрібна для аналізу стандартної кількості потоків в секунду і замість простою їх можливості застосовуються для складних статистичних сценаріїв та алгоритмів штучного інтелекту для розробки методів протидії шахрайству. Найцікавішим є факт того, що продукт сертифікований PCI PA-DSS, що свідчить про офіційне підтвердження безпечності платіжного програмного забезпечення.

Система може обробляти до 4 000 транзакцій в секунду із можливою затримкою у 3,5 мілісекунди. Для розуміння апаратних вимог системи можна зазначити, що сервер з одним процесором Intel Xeon E3-1231V3 (4 ядра, частота 3,40 ГГц) може обробляти до 1000 транзакцій у секунду із затримкою в 10 мілісекунд [1].

Велику швидкість обробки інформації забезпечують ряд особливостей :

1) Продукт створений на мові програмування C++;
2) Застосовується SOA (Service-Oriented Architecture) архітектура, що впроваджує паралельне вирішення задач, тобто продукт розділений на кілька сервісів, що не чекають своєї черги у коді, а працюють одночасно;
3) Спеціально побудована база даних, яка базується на багатьох технологіях крім SQL та великої кількості оперативної пам'яті.

Установка на одну інстанцію займає кілька хвилин, при цьому не потрібно самостійно створювати базу даних та налаштовувати її, оскільки і налаштування, і база даних встановлюються автоматично. Легко інтегрується в організацію, наприклад інтеграція у компанію, що оброблює 7 біліонів фінансових транзакцій у рік зайняла всього 5 неділь [].

Завдяки використанню компонентів AJAX Java-script та MVC архітектури, не потрібно завантажувати додаткове програмне забезпечення для доступу до системи, потрібен лише будь-який веб-браузер. Тобто оператор може аналізувати події як з персонального комп'ютера, так і з смартфона. Отримати доступ до системи можна як завдяки внутрішнім методам авторизації, так і завдяки Active Directory.

Система складається з кластера інстанцій. IBM Safer Payments не потребує окремого центрального адміністративного центру, можна підключитися до будь-якої інстанції та провести налаштування всього кластеру. Кожна інстанція є копією іншої, оскільки відбувається постійний обмін інформацією про налаштування та функції через протокол SCI (Status Control Interface). Якщо одна інстанція була від'єднана для технічних робіт, то після підключення одразу ініціюється перевірка, чи були зміни в інших, якщо так, то ця частина додасть зміни і до себе. Завдяки цьому система є доволі відказостійкою (якщо перестане працювати одна частина, роботу системи почнуть продовжувати інші) і не потребує великих зусиль для налаштування кожного елемента, та створення додаткових елементів загального керування. Допускається використовувати будь-яку кількість інстанцій, в залежності від потреб. Специфічна структура інформації відносно платежів не займає велику кількість пам'яті, що дозволяє зберігати історію транзакцій не один рік.

Завдяки MCI (Message Command Interface) протоколу, система у режимі реального часу приймає і обробляє відповідні транзакції. Дані відносно платежів Приймаються у форматі XML, специфічна структура якого, не займає велику кількість пам'яті, що дозволяє зберігати історію транзакцій роками. Для завантаження у систему, наприклад для аналізу, інформації відносно процесів

транзакцій, які не потрапили через MCI, у форматах CSV, XML та інших, використовується BDI (Batch Data Interface).

Компанія IBM надає можливість безкоштовного користування продуктом на протязі 90 днів, після чого кожен місяць ліцензії коштує 17 700 доларів, а ліцензія на рік обійдеться у 412 000 доларів (станом на 03.10.2019), що є чудовою можливістю спочатку протестувати програму на протязі значного періоду часу, і лише у разі актуальності системи для компанії його придбати [2].

Література:

1. *IBM Safer Payments [Електронний ресурс] / - режим доступу: https://www.ibm.com/downloads/cas/9LOPLO0V*
2. *Technical background for IBM Safer Payments [Електронний ресурс] / - режим доступу: ontext.reverso.net/перевод/английский-русский/*

ТЕХНОЛОГІЯ ПРОВЕДЕННЯ МОНІТОРИНГУ ТА ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ WEB-САЙТІВ МЕРЕЖІ ІНТЕРНЕТ

Поляков В.О.

Підхід до безпеки WEB-сайтів застарів. Загроз занадто багато, і треба щось вибирати в основу ієрархії захисту. Інтернет уже давно не просто мережа html-сторінок. Це складні додатки, скрипти, транспортна мережа, телеконференції, електронна пошта та багато іншого Проведення робіт з тестування на проникнення і аудитів інформаційної безпеки - уразливості в Web-сайтів, як і раніше залишаються одним з найбільш поширених недоліків забезпечення захисту інформації.

Найбільш часто зустрічається проблема- це низька поінформованість співробітників у питаннях ІБ, слабка парольна політика чи повсюдне її недотримання, недоліки у процесах управління оновленнями ПЗ, використання небезпечних конфігурацій та неефективне міжмережеве розмежування доступу. Незважаючи на те, що уразливості Web-сайтів неодноразово описані в науковій та спеціалізованої літературі, досить рідко зустрічаються превентивні захисні механізми, які знижують ризики експлуатації різних вразливостей в них. Проблема захищеності Web-сайтів ускладнюється ще й тим, що при розробці Web- сайтів, що часто не враховуються питання, пов'язані з захищеністю цих систем від внутрішніх і зовнішніх загроз, або не достатньо уваги приділяється даному процесу. Це в свою чергу породжує ситуацію, в якій проблеми ІБ потрапляють у поле зору власника системи вже після завершення проекту. А усунути уразливість в уже створеному Web- сайті є більш витратною статтею бюджету, ніж при його розробці та впровадженні. Недооцінка серйозності ризику реалізації загроз ІБ з використанням Web-додатків, доступних з боку мережі Інтернет, можливо, є основним чинником поточного низького стану захищеності більшості з них.

Поширені уразливості Web-сайтів складається з дев'яти класів:

1. Аутентифікація (Authentication).

2. Авторизація (Authorization).
3. Атаки на клієнтів (Client-side Attacks).
4. Виконання коду (Command Execution).
5. Розголошення інформації (Information Disclosure).
6. Логічні недоліки (Logical Flaws).
7. Не безпечні конфігурації (Misconfiguration).
8. Недоліки протоколу (Protocol Abuse).

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

Сканери уразливості діляться на дві основні групи:

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

2. Друга група - сканери уразливості веб-додатків. На даний момент їх популярність зростає в силу того, що більшість комерційних організацій і банків використовують у своїй діяльності інтернет ресурси, захист яких стає важливим фактором.

Дані продукти мають всі можливості і засоби для ефективної установки і управління виправленнями вразливостей, які створені після аналізу та фільтрації результатів.

Література

1. https://tproger.ru/digest/website-inspection-services
2. Шива Парасрам, Алекс Замм, Теди Хериянто, Шакил Али, Дамиан Буду, Джерард Йохансен, Ли Аллен Тестування на проникнення и безпеку. – Питер. -2016. – 448с.

СТРУКТУРА ІНФОРАЦІЙНОЇ МЕРЕЖІ НА ОСНОВІ ІЄРАРХІЧНОЇ ГІПЕРМЕРЕЖІ

Собчук В.В.
кандидат фізико-математичних наук, доцент
Державний університет телекомунікацій
м. Київ, Україна
Гогонянц С.Ю.

кандидат військових наук, старший науковий співробітник
Національний університет оборони України імені Івана Черняховського,
м. Київ, Україна

Реалізація функціональної стійкості досягається застосуванням в складній технічній системі різних уже існуючих видів надмірності (структурної, часової, інформаційної, функціональної та ін.) шляхом перерозподілу ресурсів з метою парирування наслідків позаштатних ситуацій. Разом з тим, існуючі роботи в галузі забезпечення функціональної стійкості складних технічних систем не дають змоги виробити єдині підходи та започаткувати теоретичні основи забезпечення функціональної стійкості для інформаційної мережі. Проблема полягає у відсутності підходу та відповідних моделей щодо опису структури сучасної інформаційної мережі, параметрів її елементів та зв'язків, а також відсутністю можливості врахувати руйнуючі впливи різного характеру.

Здатність інформаційної мережі протистояти руйнівним діям і продовжувати виконувати певний обсяг функцій, можливо з погіршенням якості, є їх властивістю, яку називають функціональною стійкістю [1-3].

Ієрархічна гіпермережа – це впорядкована множина графів, сусідні елементи якої утворюють гіпермережу:

$$HS = \left(PS, WS_1, WS_2, \ \ldots, WS_h\right).$$

Іншими словами, якщо взяти гіпермережу $Sp\left(X, R_{p-1}, R_p\right)$, утворену WS_{p-1} і WS_p, то WS_{p-1} – первинна мережа S_p, WS_p – вторинна, R_{p-1} – множина ребер WS_{p-1}, R_p – множина ребер WS_p.

Можна говорити про гіпермережі *p*-го рівня, де WS_{p-1} – первинна мережа, якщо $p > 1$, PS – первинна мережа, якщо $p = 1$.

Сформулюємо поняття видалення *p*-го рівня. Внутрішнє (зовнішнє) видалення *p*-го рівня – це видалення вершини гіпермережі рівня *p*, при якому видаляються інцидентні ребра, строго слабо інцидентні ребра, а також сама вершина і гілки гіпермережі *p*-го рівня.

Очевидно, що видалення *p*-го рівня вплине на всі гіпермережі, рівень яких вище *p*. Таким чином, якщо розглянути графи WS_{p-1}, WS_p і WS_{p+1}, то видалення будь-якого ребра *r* з WS_p, спричинене будь-яким видом видалення вершини з гіпермережі S_p, призведе до видалення всіх ребер WS_{p+1}, інцидентних ребру *r* в гіпермережі S_{p+1}. Якщо параметри ієрархічної гіпермережі залежать від часу, то вона називається нестаціонарною.

Види видалення елементів. Для того, щоб проводити всебічний аналіз функціональної стійкості та оцінювати вплив руйнівних факторів на інформаційну мережу, потрібно також описати поняття видалення елементів гіпермережевих моделей:

1) видалення ребер: ребро *r* буде видалено, якщо з графа *WS* буде видалено ребро *r*;

2) видалення гілок: гілка *v* буде видалена, якщо вона буде видалена з графа первинної мережі *PS*, а з графа вторинної мережі будуть видалені всі інцидентні цій гілці ребра.

Для гіпермережі розрізняють три способи видалення вершин:

1. Вершина *x* буде внутрішньо видалена, якщо будуть видалені всі інцидентні їй ребра, тобто в графі *WS* вершина x виявиться ізольованою.

2. Вершина *x* буде зовні видалена, якщо будуть видалені всі слабо інцидентні (але не інцидентні) їй ребра. На графі *WS* це відповідає видаленню деякої підмножини ребер, а на гіперграфі *FS* – слабкому видаленню підмножини ребер.

3. Вершина *x* буде видалена, якщо будуть видалені всі інцідентні їй гілки і вона сама.

Дослідження процесу функціонування сучасних інформаційних мереж надали можливість розробити математичну модель інформаційної мережі на основі нестаціонарної гіпермережі. Тому дана модель враховує усі необхідні основні з точки зору функціональної стійкості параметри мережі, їх властивості та відношення, які здійснюють значний вплив на синтез оптимальної структури мережі.

Відмінність гіпермереж від інших структурних моделей полягає в тому, що в створені структури гіпермережі бере участь більше двох твірних множин, що дозволяє врахувати вплив можливих позаштатних ситуацій, які обумовлені внутрішніми і зовнішніми чинниками. Таким чином, забезпечення ІІМ властивості функціональної стійкості стикається з новою теоретичною проблемою, що вимагає для її рішення розробки адекватного математичного апарату синтезу системи.

Перспективними шляхами подальших досліджень у зазначеному напрямку може бути широке коло питань щодо розробки нових та удосконалення існуючих методик підвищення рівня функціональної стійкості інформаційних мереж, які мають автономно функціонувати в умовах впливу зовнішніх та внутрішніх дестабілізуючих факторів.

1. Построение функционально устойчивых распределенных информационных систем: монография / О.В. Барабаш. К.: НАОУ, 2004. 226 с.

2. Саланда І.П., Барабаш О.В., Мусієнко А.П., Лукова-Чуйко Н.В. Математична модель структури розгалуженої інформаційної мережі 5 покоління (5G) на основі випадкових графів. *Наукове періодичне видання «Системи управління, навігації та зв'язку».* Полтава: ПНТУ, 2017. Вип. 6 (46). С. 118 – 121.

3. Musienko A.P., Barabash O.V., Lukova-Chuiko N.V., Salanda I.P. Diagnostic model of wireless sensor network based on the random test of checks. *Science and Education a New Dimension. Natural and Technical Sciences*, 2018. VI (18), Issue 158, Budapest, Hungary, P. 25 – 28.

ВПРОВАДЖЕННЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ НА БАЗІ MPLS

Мицик Максим Владиславович

Анотація

В 90-х роках 20 століття MPLS або Multi-Protocol Label Switching стали новими ефективними методами IP роутингу. У той час, коли традиційні методи маршрутизації втрачали ефективність, MPLS пропонував користувачам більш інноваційні варіанти відправки пакетів на IP-адреси. На відміну від інших служб що могли бути встановлені, MPLS найбільш точно описувалась в технічному плані. Ця технологія найчастіше використовувалась суб'єктами які прагнули забезпечити повноцінну інженерію трафіку. MPLS набула популярності як технологія, що використовувалась для покращення підключення до Ethernet. Оскільки масштабованість та надійність стають все більшими проблемами для підприємств, MPLS запропонував користувачам спосіб розставити пріоритетні зв’язки в межах послуги. Сьогодні будь-якій організації, яка прагне підвищити в себе ефективність та масштабованість мережі, було б розумно розглянути можливість використання MPLS. Протягом останніх кількох років існувала думка, що MPLS застарів і має бути заміненим більш ефективними з певних міркувань технологіями, такими як SD-WAN . Однак варто стверджувати, що це далеко не так .Наразі варто розглянути що таке MPLS, як ця технологія вирішує проблеми безпеки мереж і чому вона буде актуальною ще досить довгий термін.

Стислий опис технології

У більшості мереж кожен маршрутизатор визначає як маршрут буде проходити. На кожному маршрутизаторі забезпечено пошук IP-адреси, щоб знайти, куди надалі надсилати дані. MPLS використовує комутацію міток і знаходить кінцевий маршрутизатор для встановлення маршруту прямо до кінцевого місця. Потім маршрутизатори читають цю мітку, щоб передати пакети прямо до місця призначення. Як результат, маршрутизаторам по всій мережі не потрібно проводити пошук IP-адреси, оскільки вся інформація вже є.

Поглиблений огляд MPLS

У традиційній IT-мережі кожен раз, коли маршрутизатор отримує IP-пакет, йому надається IP-адреса призначення. Так повідомляється маршрутизатору, де кінцеве призначення пакету. Хоча це здається досить розумним на перший погляд, це не сприяє ефективності. Причина в тому, що маршрутизатор не має інформації про те, як пакет повинен подорожувати до місця призначення. Іншими словами, традиційна маршрутизація IP надає обмежену кількість інформації про маршрут, який повинен пройти пакет.

Рішення цієї проблеми за допомогою MPLS полягає в тому щоб зробити перший маршрутизатор, який перехоплює пакет, таким, який визначає його майбутній маршрут. При першому маршруті для встановлення контакту кожному пакету надається мітка, яку маршрутизатори можуть читати далі по ланцюгу. Головне що пакети передаються на рівні комутації, а не на рівні маршрутизаторів. Це призводить до зменшення навантаження на обладнання.

MPLS знаходиться між другим та третім мережевими рівнями. Рівень 2 використовується для протоколів типу Ethernet що використовуються для транспортування пакетів, а рівень 3 охоплює фактичну маршрутизацію пакетних даних. MPLS використовує взаємозв'язок цих рівнів для прискорення процесу передачі.

Зазвичай мережа MPLS підключена до хмарної служби, яка підключається до кожного вузла наявної мережі. По суті, MPLS виступає як VPN. Технологія може використовуватись як для мереж PPTP VPN так і для віртуальних приватних мереж 2 та 3 мережевих рівнів. Тоді як для підключення PPP потрібні маршрутизатори з обох сторін мережі, MPLS не потребує додаткового обладнання.

MPLS діє по принципу закладки. Коли маршрутизатор використовує MPLS, його таблиця маршрутизації розбивається на кожен розділ із зазначенням унікального номеру. У технічному плані маршрутизатор міток (LER) забезпечує кожен пакет ярликом, який використовується для ідентифікації класу переадресації еквівалентності (FEC). LER також несе відповідальність за видалення цієї мітки в точці виходу з мережі та заміну її на звичайну IP-адресу.

Щоразу, коли LER отримує пакет без мітки, то повинен присвоювати йому мітку MPLS. Після того, як пакет був названий він потім надсилається на наступний маршрутизатор LSR в ланцюжку. Як тільки LSR отримує пакет, він сканує мітку MPLS у заголовку і робить одну з двох речей; він змінює мітку MPLS і передає її далі, або якщо пакет готовий покинути мережу MPLS, то LSR видаляє мітку MPLS взагалі. Після завершення останнього вузла зчитується інформація про маршрутизацію, щоб відправити її до кінцевого пункту призначення.

Після того, як мітка присвоєна пакету, вона надсилається до наступного пункту вниз по Label-Switched Path (LSP). LSP - це заздалегідь визначений шлях, по якому проходять пакети. Кожен маршрутизатор у мережі повинен мати чіткий доступ до LSP, щоб ефективно пересилати пакети до наступного пункту призначення. Коли LSR перехоплює пакет, він перевіряє мітку, перш ніж надсилати її вниз по LSP до наступного пункту призначення.

Основна перевага MPLS полягає в тому, що після з'єднання маршрутизатор не повинен переповнювати інформацію про пакет перед тим, як надіслати його на наступний пристрій, він може просто використовувати заголовок. Він надає маршрутизаторам всю необхідну інформацію, щоб визначити, куди потрібно

переслати або перенаправити пакет .Кінцевим результатом є більш швидка передача пакетів.

Пристрої по всій мережі зчитують мітку MPLS для переданих пакетів, щоб визначити кінцеве місце, до якого вона надсилається .На відміну від цього, IP протоколи надсилають пакети даних, але дозволяють окремим пакетам визначати свій власний шлях. Замість того, щоб подорожувати фізичним шляхом, таким як IP-трафік, MPLS використовує віртуальні шляхи для отримання пакетів до їх кінцевого пункту призначення.

Ролі / позиції маршрутизаторів MPLS

Перемикач / маршрутизатор міток

Перемикач міток / маршрутизатор (LSR) - це маршрутизатор, який здійснює передачу пакетів за допомогою мітки MPLS. Це маршрутизатор, який створює мітки пакетів до кінця їхнього шляху. Як правило, LSR розташовані посередині мережі MPLS. Після того, як пакет отриманий маршрутизатор визначає наступне місце розташування LSP і додає мітку кореляції з цим. Він видаляє стару мітку і замінює її новою.

Маркер маршрутизаторів

Маршрутизатор міток (LER) - це маршрутизатор, розташований на кінці мережі MPLS, який виступає в якості точки входу або виходу. LER розміщують мітки на вхідних пакетах, перш ніж надсилати їх до домену MPLS. Якщо пакет надходить до виходу, LER видаляє мітку і пересилає пакет, використовуючи протокол IP.

Маршрутизатор провайдер

У середовищі VPN, що працює над MPLS, маршрутизатори, які функціонують як точки входу та виходу для VPN, називаються маршрутизаторами PER .Ті маршрутизатори, які несуть відповідальність за передачу пакетів , називаються маршрутизаторами-провайдерами.

Протокол розподілу міток

Протокол розподілу міток (LDP) використовується для розподілу міток між LER та LSR. LSR регулярно взаємодіють між собою, щоб обмінюватися мітками та інформацією про маршрутизацію між собою, щоб допомогти розвинути своє розуміння мережі та полегшити передачу пакетів.

Клієнтська межа

Клієнтська межа (CE) - це пристрій на кінці замовника, з яким комутуються маршрутизатор-провайдер .Клієнтська межа приймає комунікації зі сторони клієнтів і транспортує їх безпосередньо до постачальника. Маршрутизатор CE також підключається до мережі клієнтів. CE знаходиться в епіцентрі обміну пакетами зі своїми клієнтами.

Що таке MPLS VPN і як він використовується

У багатьох випадках існує інформація про MPLS, на яку посилається в контексті VPN. Причина полягає в тому, що MPLS має можливість підтримувати послуги VPN. VPN-адреси MPLS надходять у формі PPP, "рівень 2" (MPLS) VPN (також його називають "Віртуальна приватна послуга локальної мережі" або VPLS) і 3- й рівень VPN MPLS. PPP - це з'єднання "точка-точка", що працює на рівні 2 в моделі OSI за допомогою використання LDP. Ця послуга використовує віртуальні орендовані лінії (VLL) для з'єднання двох різних сайтів разом.

MPLS рівень 2 VPN (VPLS) - це VPN другого рівня який з'єднує одну точку з мультиточкою за допомогою Ethernet. Організації використовують VPLS для з'єднання географічно окремих мереж локальної мережі разом. Цей шар використовує сигнальну технологію Cisco на основі LDP. Ретрансляцію кадрів і Ethernet можна транспортувати через MPLS 2 рівня.

MPLS Layer 3 VPN - це тип послуги MPLS, що мають на увазі більшість людей, коли вони посилаються на VPN MPLS. У цій службі адміністратори створюють віртуальну технологію маршрутизації та переадресації на своїх PER. Віртуальна маршрутизація та переадресація означають, що в одному маршрутизаторі одночасно може працювати кілька сегментів таблиці маршрутизації.

MPLS VPN та хмарні служби

Одне з найпопулярніших застосувань MPLS VPN - це хмарні сервіси. Поєднання хмарних служб із CPL MPLS створює віртуальну приватну хмару. Ця приватна хмара захищена та відокремлена від загальнодоступного Інтернету. Однією з головних причин організацій прийняття VPN MPLS для хмарних сервісів є те, що вони можуть контролювати пріоритет трафіку.

Таким чином, хмарні сервіси, керовані MPLS VPN, є більш надійними. Наприклад, якщо один додаток або з'єднання забирає занадто багато ресурсів, його можна просто депріоритизувати, щоб зберегти ресурси для більш важливих процесів. Це забезпечує підприємствам набагато більш високий рівень контролю та диференціації, ніж це доступно в публічному Інтернеті. Також перевага в тому, що підприємство може швидко підвищувати масштаб. Підвищити масштаб VPN MPLS можна набагато простіше, ніж традиційні послуги оператора.

Чому доцільно використовувати MPLS?

Масштабованість

Багато організацій вирішують використовувати MPLS через його масштабованість. MPLS не потребує додаткового фізичного обладнання для роботи, а це означає, що при підвищенні масштабу вам не потрібно купувати дороге обладнання. Для великих організацій це може заощадити багато грошей у довгостроковій перспективі та мінімізувати ускладнення, які виникають із

налаштуванням нового обладнання кожного разу, коли мережа збільшується в розмірах.

Гнучкість

Ще одна причина, чому компанії вирішили розгорнути MPLS, - це через її гнучкість. Можливість перенаправляти трафік за найбільш ефективним маршрутом та мінімізувати перебої дуже корисно. Традиційна IP-маршрутизація може дозволяти пакетам вибирати власне місце призначення, але це не забезпечує швидкість, яку робить швидка передача пакетів MPLS.MPLS також є гнучким, оскільки ваш постачальник послуг може надавати 2 та 3 рівень VPN в одному місці.

Підвищення продуктивності та безпеки

Відбувається підвищення продуктивності через переключення міток .Зміна маршруту передачі пакетів на рівні комутації означає, що пристрої вниз по ланцюгу можуть передавати пакети більш ефективно. Як вже було сказано вище, це призводить до зменшення використання обладнання. Це особливо вигідно у великих організаціях, які проводять безліч різних пакетних передач.

MPLS вибирає маршрут через який проходить трафік , а значить, він може уникнути перевантажених маршрутів на користь оптимальних шляхів. Це велика перевага, оскільки означає, що не повинно виникати коллізій що негативно впливає на продуктивність організації.

Гнучка маршрутизація робить процес перенаправлення трафіку неймовірно швидким. Це полегшує роботу окремих пакетів і підвищує продуктивність мережі в цілому. Голосові послуги та відеопрограми - це дві сфери, де якість обслуговування надзвичайно важлива для запобігання зайвих затримок.

Які недоліки MPLS?

Незважаючи на те, що вже не доведеться турбуватися про налаштування обладнання, організація берете на себе нове питання щодо управління своїми відносинами зі своїм провайдером. Ваш постачальник мережі несе відповідальність за надання вам хмари MPLS, і тому вам доведеться працювати з постачальником, щоб переконатися, що ваш трафік MPLS правильно та безпечно спрямований. Це означає, що вам доведеться надати частковий контроль над вашою мережею. Це суттєвий недолік, оскільки технологія використовується для роботи як правило з конфіденційною інформацією.

Проблема вирішується шифруванням всього трафіку, переданого між двома маршрутизаторами. В мережах даного типу це є можливим.

MPLS проти SD-WAN

Незважаючи на те, що MPLS все ще широко використовується, багато хто очікує, що в майбутньому SD-WAN (визначена програмним забезпеченням мережа) буде лідером.SD- WAN застосовується до стандартних підключень

WAN для підключення пристроїв на великій відстані. Як правило, їх використовують великі корпорації або провайдери центрів обробки даних .Він найбільш відомий тим, що допомагає підтримувати хмарні сервіси.

Однією з найбільших переваг SD-WAN над MPLS є більш висока продуктивність. SD-WAN використовує комбінацію MPLS, широкосмугового зв'язку та LTE, щоб залишатися на зв'язку.По суті, це створює гібридну мережу, яка може перемикатися між залежно від швидкості передачі пакетів і продуктивності мережі в режимі реального часу.На практиці це призводить до кращої доставки пакетів.

Зважаючи на це MPLS не відстає з точки зору своєї надійності. Це ефективний метод доставки пакетів що забезпечує високу якість обслуговування. Проблема полягає в тому, що MPLS працює в спільній мережі, що часто призводить до конкуренції за пропускну здатність. Це може бути значною причиною затримок у порівнянні з SD-WAN.

MPLS все ще актуальний

Якщо організація серйозно ставиться до того, щоб зробити свої маршрути пакетів більш ефективними та підвищити продуктивність власної мережі, то MPLS - це те, що компанія обов'язково повинна врахувати. Більші організації, яким постійно доводиться підвищувати свою технічну інфраструктуру , виграють від MPLS, оскільки це зменшить потребу в придбанні нового обладнання. Це допоможе значно зменшити накладні витрати.

Незважаючи на те, що це пов'язано з ускладненням роботи з мережевим провайдером, переваг більше ніж втрат. MPLS має своїх прихильників та опонентів, але його переваги зрозумілі. Він має можливість підтримувати масштабованість та надійність обслуговування таким чином як традиційні IP-маршрутизаційні з'єднання не можуть.

Зростання використання сервісів Ethernet та Wide Area Network говорить про те, що MPLS настільки ж популярний як раніше. Незважаючи на це все ж більшість користувачів надають перевагу технології Ethernet, ніж будь-яка іншій альтернативі. Поки Ethernet залишається основним вибором типу з'єднання, MPLS буде перебувати на задньому плані.

Використані джерела :

1. Захватов М. Побудова віртуальних приватних мереж (VPN) на базі технології MPLS. — М.: Риверсайд Тауерз, 2004.

2. Вишняков А. Сигналізація VPLS: LDP чи BGP? // mpls-exp, 2005.

3. Юшков Т. Організація VPN на базі MPLS (https://www.opennet.ru/docs/RUS/mpls/mplsvpn.html)

4. Дадалі О. MPLS зробить маршрутизатори швидкими (https://compress.ru/article.aspx?id=10621)

РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ "РОЗУМНИЙ БУДИНОК"

Авєрін І.Ю. студент БСДМ-61

Розумний будинок - автоматична система управління будівлею. Під «розумним будинком» слід розуміти систему, яка допомагає людині забезпечити повний контроль і моніторинг всіх інженерних систем будівлі. В якості основних засобів для з'єднання використовується типове Ethernet або Wi-Fi з'єднання. При цьому зловмисник може отримати доступ до основної мережі та виконувати роль другої довіреної особи для відправлення всіх команд на життєво важливі системи будинку. Тому для таких систем доцільно зробити аналіз основних ризиків, які можна очікувати при використанні системи «Розумний будинок».

Система «Розумний будинок» - це повна автоматизація управління пристроями, девайсами у всіх приміщеннях будинку, квартири, офісів. Під системою «Розумний будинок» розуміється система, яка забезпечує безпеку та ресурсозбереження всіх користувачів системи. Управління накою системою можливо як з приміщення, так і дистанціно з телефоеів. Така система повинна вміти розпізнавати конкретні систуації, які відбувються у приміщенні та відповідним чином на них реагувати. Така система може складатися з різних підсистем, які в свою чергу можут впливати одна на іншу. Система «Розумний будинок» дозволяє у будь-який час проводити автоматизоване управління в ручний режим.

Для нормальної роботи такої системи не може бути ідеальною. Тому необхідно визначити недоліки, які пов’язані з забезпеченням інформаційної безпеки та використовують дану систему. Загрози інформаційної безпеки «Розумний дім» є порушенням конфеденційності,цілосності та доступності інформації. Основними загрозами системі «Розумний дім» є:

1. Атака хакеров;
2. Перехоплення інформації;
3 . Віруси в системі;
4. Доступ зловмисника, у зв’язку отримання прав доступу.
5. Виток інформації по каналам.

Існує також багато інших загро, які можуть впливати на працездатність системи. До таких загро можна віднести: підключення системи «Розумний дім» до Інтернету, що підвищує в свою чергу ймовірність атаки хакерів. Особливу увагу необхідно приділяти аутентифікації та ідентифікації, для запобігання доступу несанкціонованого користувача до сховища даних. Неефективний захист трафіку, підвищує рівень ймовірності перехоплення інформацій по каналам зв’язку. Для того, щоб виключити можливість виконання зловмисником ролі додаткового довіреної особи, захистити канали передачі даних і звузити
кордони неконтрольованої зони системи «розумний дім», при цьому враховуючи специфіку використовуваних пристроїв, необхідно створити надійний і довірений канал між керуючим центром автоматизованої системи і

пристроями автоматизації. Для цього передбачається розробка спеціального програмно-апаратного модуля, який дозволить прибрати основні недоліки в захисті розумного будинку і значно обмежити зловмисника в можливих негативних діях, як на окремі компоненти системи, так і на весь «Розумний будинок» в цілому.

Також можна для додаткового забезпечення захисту системи розумного дому, можна використовувати багатофакторну автентифікацію: можна додати додатковий фактор аутентифікації крім застарілої технології захисту паролем. В якості додаткового фактору захисту може бути обраний одноразовий код, що приходить в SMS–повідомленні, або один з варіантів біометричної аутентифікації: сканування відбитку пальця або сітківки ока. Таке рішення дозволить захистити важливі дані навіть якщо зловмисник зможе дізнатися ім'я користувача і пароль.

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. Найбільш поширені функції системи «Розумний будинок» [Електронний ресурс] // Режим доступу: http://megapredmet.ru/1-76622.html .

АНАЛІЗ МЕТОДІВ БЕЗПЕЧНОГО ОБМІНУ ЕЛЕКТРОННОЮ ПОШТОЮ

Грибіняк Владислав Іванович

Не є відкриттям те, що мережа Інтернет стала основою комунікацій у повсякденній діяльності. Важливим елементом сучасного життя є електронна пошта, яка стала невід'ємною частиною сьогодення у більшості людей.

Електрона пошта - це системи транспортування повідомлень, так званий поштовий зв'язок з доставки поштових повідомлень, що здійснюється електронними методами за допомогою комп 'ютерів. Потрібно усвідомлювати, що безпека електронних листів залежить не тільки від складного та унікального пароля до облікового запису.

Використання електронної пошти призводить до обробки інформації в системі. Відповідно до законодавства обробка інформації в системі - це виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Системи електронної пошти є прикладним програмним забезпеченням і їх створення та функціонування регламентується стандартом МККТТ Х.400.

Щоб мати справу з електронною поштою, використовується спеціальний клієнт для доступу до поштового сервера. У свою чергу, вони можуть обмінюватися інформацією один з одним, використовуючи при цьому абсолютно різні протоколи.

Найбільш часто використовуються протоколи електронної пошти в мережі Інтернеті - POP3 IMAP і SMTP. Кожен з них має певну функцію і спосіб роботи. Дослідження досвіду проектування, виготовлення, випробувань і експлуатації автоматизованих систем говорять про те, що інформація в процесі введення, зберігання, обробки й передачі зазнає різним випадковим впливам.

Для вирішення питань захисту в Інтернеті як для великих підприємств, організацій, так і для представників малого бізнесу є Cisco Umbrella. Це хмарний сервер, що було створено з

метою захисту мереж, який дозволяє не тільки захищати комп'ютери від вже існуючих загроз, а й попередити нові потенціальні загрози.

За рахунок того, що все більше користувачів підключаються до Інтернету напряму, Umbrella – найшвидший та найпростіший спосіб звбезпечити безпеку всіх користувачів за лічені секунди серед усіх існуючих на даний момент сервісів. Оскільки це хмарове рішення, не потрібно встановлювати ніяке обладнання та вручну обновляти програмне забезпечення. Можна також швидко ініціалізувати всі пристрої всередині мережі, включаючи персональні пристрої співробітників. А підтримка декількох видів підписок на хмаровий сервіс Cisco Umbrella значно розширює список цільової аудиторії користувачів та дає можливість використовувати цей елемент захисту як для невеликих компаній, так і для спеціалістів по розширеним функціям безпеки.

Впровадження захищенного Інтернет шлюзу на основі хмарного продукту Cisco Umbrella є рішенням, яке допоможе зменшити негативний вплив та забезпечити більш надійне та достовірне емейл-листування поза корпоративною мережею.

Література:

1. Таненбаум Э. С. Компьютерные сети / Эндрю С. Таненбаум. – СПб: Издательский дом «Питер», 2012. – 955 с.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 19.04.2014 р. // Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286.

3. CISCO UMBRELLA FAQ // https://www.cisco.com URL: https://www.cisco.com/c/dam/global/ru_ru/about/brochures/assets/pdfs/cisco_umbrella_faq.pdf (дата звернення: 03.04.2018).

4. Cisco Umbrella // learn-umbrella.cisco.com URL: https://learn-umbrella.cisco.com/datasheets/cisco-umbrella-at-a-glance (дата звернення: 05.04.2018).

Стукальський Сергій Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Біометричні системи автентифікації в автоматизованих системах

Різні Біометричні системи автентифікації інгтегруються в автоматизовані системи різних класів задля забезпечння цілісності ІС, а також розмежування доступу до будь якого виду інформації. Біометричні системи автентифікації широко використовуються в сучасному інформаційному просторі, тому дана тема є надактуальною для розгляду та вивчення, обумовлені сучасними розробками у сфері біометричних технологій та систем захисту інформації

Основною метою є підвищення ефективності захисту інформації при експлуатації АС з використанням біометричних систем автентифікації, визначення недоліків та переваг систем біометричної автентифікації в АС

Основною задачею забезпечення безпеки інформаційних комп'ютерних систем є обмеження кола осіб, що мають доступ до критичної інформації.

Аутентифікація користувачів комп'ютерних систем задача, рішення якої дозволяє організувати процес управління правами доступу, а також вирішити ряд інших питань, що мають прикладне значення .

Аутентифікація - перевірка приналежності суб'єкту доступу пред'явленого їм ідентифікатора.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

Термін "біометрія" означає вимірювання будь-яких фізіологічних або поведінкових параметрів індивідуума. Дані, отримані в процесі вимірювання, порівнюються з тими, що були введені раніше, - комп'ютер намагається "впізнати" людину, так, наприклад, як ми розпізнаємо один одного.

Звісно при інтегруванні будь-якої з біометричних систем в АС потрібно керуватися діючими нормативно-правовими документами та стандартами у сфері ІБ.

Основними функціями нормативної бази є регулювання взаємовідносин між суб'єктами інформаційної безпеки, визначення їх прав, обов'язків та відповідальності. Також невід’ємною складовою є встановлення порядку застосування різних сил і засобів забезпечення інформаційної безпеки.

Основними завданнями автоматизованих біометричних систем є:

- реєстрація біометричних параметрів (характеристик) особи за допомогою сенсорних пристроїв ;

- формування вибірки біометричних даних ;

- формування ознак ідентифікації ;

- порівняння біометричних даних особи з еталонними персоніфікованими даними - аналіз ;

- прийняття рішення про відповідність порівнювальних біометричних параметрів особи

вимогам (персоніфікованому еталону) ;

- формування рішення про надання доступу (досягнення ідентифікації), або повторення

процедури ідентифікації, або відмова у доступі.

Список використаних джерел:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
2. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
3. R. Adhami, P. Meenen. Fingerprinting for security // IEEE Potentials, vol. 20, no. 3, pp. 33-38, Aug.-Sept. 2001.
4. Гирман М.Г. Использование автоматизирован- ных дактилоскопических идентификационных систем в раскрытии и расследовании преступлений

ТЕХННОЛОГІЇ ТА МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ШИРОКОСМУГОВОГО ЗВ'ЯЗКУ WI-FI

Шумейко Андрій Олександрович

В даному дипломному проекті велася розробка технології захисту інформації бездротових мереж, яка може застосовуватися для підвищення захисту комп'ютера користувача, корпоративних мереж, малих офісів.

В ході виконання дипломного проекту було проведено аналіз технології інформації захисту інформації бездротових мереж, аналіз програмних продуктів дозволяють підвищити захист бездротових мереж від загроз.

В результаті виконання проекту придбаний досвід налаштування програмних продуктів, що дозволяють максимально захистити бездротову мережу від найпоширеніших загроз.

МОДЕЛЬ СТУПЕНЮ ЗАХИЩЕНОСТІ ПІДПРИЄМСТВА В ЗАЛЕЖНОСТІ ВІД ЧАСТОТИ ПРОВЕДЕННЯ АУДИТІВ ОРІЄНТОВАННИХ НА ЗАПОБІГАННЯ КІБЕРАТАК

Галахов Є.М.,

старший викладач кафедри вищої математики, Державний університет телекомунікацій м. Київ, Україна

Дослідницька увага орієнтована на вивчення системи кібербезпеки підприємства у контексті аналізу ризик-менеджменту підприємства з детермінацією його послідовних етапів. Разом з тим, існуючі роботи у напрямку забезпечення кібербезпеки підприємства недостатньо розкривають

проблемне питання ефективного інтервального аналізу проведення аудитів орієнтованого на превентивність кібератак. У цьому контексті запропоновано модель визначення рекомендованої частоти для процесу управління кібер-ризиками на підприємстві, визначено основні принципи, ключові питання, підходи щодо ефективної реалізації даної моделі в сучасних умовах діяльності підприємства. Математична модель базується на розкладі кусково-неперервної аналітичної апроксимуючої функції в ряд Фур'є, що дає можливість перейти системі аудиту кібер-загроз підприємства від дискретного до неперервного автоматизованого процесу аудиту.

Кібербезпека підприємства – це сукупність заходів щодо захисту локальної та хмарної інфраструктури бізнесу, а також перевірка сторонніх постачальників та забезпечення зростаючої кількості кінцевих точок, підключених до системи підприємства через Інтернет речей [1].

Потреба в надійній кібербезпеці підприємства зростає прямо пропорційно технічним інноваціям, які дозволяють бізнесу рости та бути більш мобільними та різноманітними щодо місцеположення [2].

Зі зростанням загрози та вартості кіберзлочинності зростає і потреба у тактичних діях та комплексній стратегії кібербезпеки [3]. Щоденні кіберзагрози в мережі Інтернет створюють все більш нові кібер-ризики підприємства, які обумовлюються більшою складністю, повнотою і трансформаційним впливом на діяльність підприємства.

Сучасний підхід ризик-менеджменту підприємства складається з наступних послідовних етапів: передбачення кількості можливих кібератак, проведення їх статистично-аналітичної оцінки кібератак, вчасної ідентифікації, розробки плану дій та превентивних заходів щодо усунення ідентичних кібератак, реалізації системи контролю та внесення модернізованих підходів аудиту кібератак на підприємстві [4].

Основою вищезазначеного підходу ризик-менеджменту може виступати запропонована математична модель зв'язку між рівнем кібер-ризику та частотою аудиту, що дає можливість забезпечити ефективну автоматизацію процесів кібер-безпеки підприємства.

У цьому контексті модель спирається на визначення часу між оцінками має вирішальне значення для загального рівня ризику, т. б. чим довший часовий період між оцінками ризику, тим вищий рівень ризику. На практиці підприємства використовують різні інтервальні підходи оцінки кібер-ризиків

Розглянемо більш деталізовано сутність зазначеної математичної моделі.

Дослідницький інтерес даної моделі полягає у визначенні рекомендованої частоти для процесу управління кібер-ризиками на підприємстві.

Модель орієнтується на наступні ключові базиси дослідження:

1. Ретроспективний статистичний аналіз часових рядів ідентифікації кібер-ризику:
   1.1. Визначених часових проміжків аудиту та апроксимування статистичних зрізів аналітичними функціями (рис. 1, 2).
   1.2. Графічна візуалізація проведеного реалізованого статистичного аналізу часових рядів ідентифікації кібер-ризику (рис. 2).

2. Аналіз існуючої стратегії кібер-ризиків підприємства на основі вище проведеного ретроспективного статистичного аналізу часових рядів ідентифікації кібер-ризику з виокремленням: слабких сторін існуючої стратегії, можливих кіберзагроз, ідентифікації потенційних сильних сторін і знаходження можливостей подальшої модернізації.
3. Розробка прогнозно-аналітичної моделі проведення аудитів.
4. Внесення модернізованих підходів у існуючу систему аудиту підприємства.

На рис. 1 зображено 4 часових періоди проведення аудиту в рамках запропонованої моделі. Впровадження послідовних аудиторських заходів забезпечує мінімізацію кібер-загроз у кожному часовому періоді, що ілюструє рис. 1.

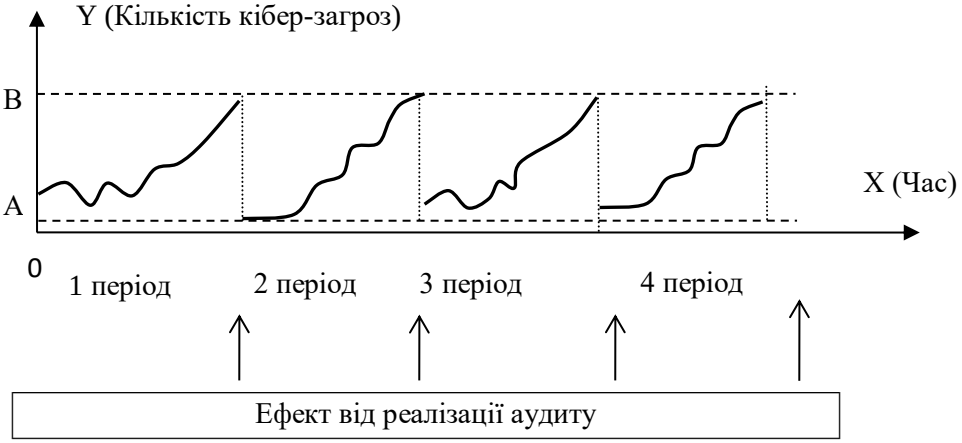


Рис.1. Залежність кількості кібер-загроз від частоти проведення аудиту за 4 часових проміжка.

Згідно п.1.1. вищезазначених ключових базисів дослідження моделі, проведена апроксимація статистичних зрізів аналітичними функціями (Рис.2).

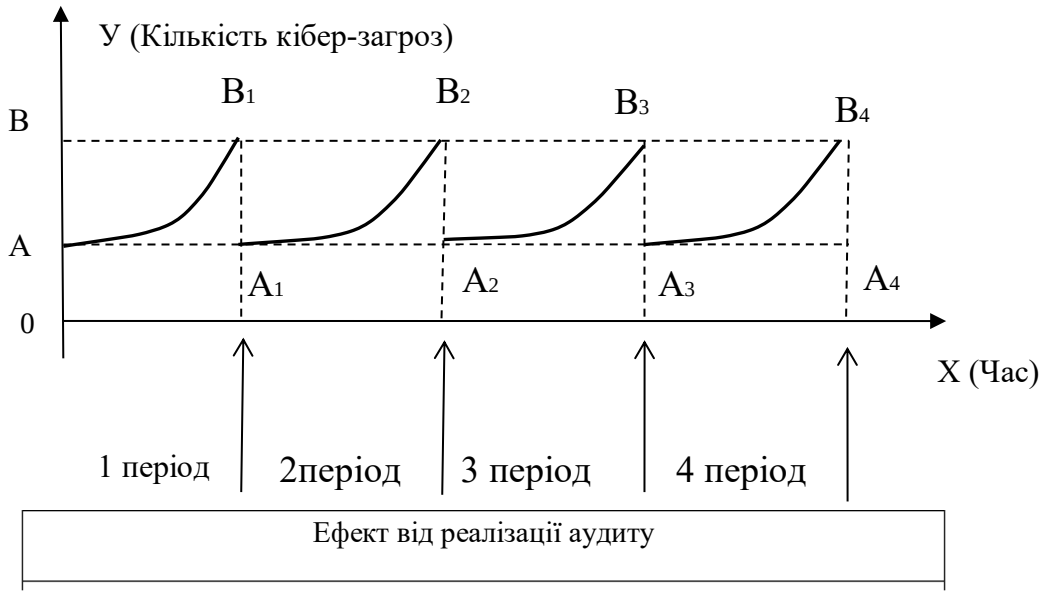


Рис.2. Апроксимація статистичних зрізів аналітичними функціями

Математична модель базується на розкладі кусково-неперервної аналітичної апроксимуючої функції (рис.2) в ряд Фур'є, що дає можливість перейти системі аудиту кібер-загроз підприємства від дискретного до неперервного автоматизованого процесу аудиту.

Таким чином, постійний неперервний моніторинг та аудит кібер-загроз підприємства надає керівництву ключову інформацію у режимі реального часу щодо ефективності кібербезпеки підприємства, дозволяючи не тільки краще розуміти проблеми під час їх виникнення, але і передбачати їх виникнення, що покращує здатність керувати ризиками та можливостями.

1. Построение функционально устойчивых распределенных информационных систем: монография / О.В. Барабаш. К.: НАОУ, 2004. 226 с.
2. M. Lange, F. Kuhr and R. Möller, "Using a Deep Understanding of Network Activities for Network Vulnerability Assessment," in Proceedings of the 1st International Workshop on AI for Privacy and Security, 2016.
3. Котенко И. В., Саенко И. Б., Коцыняк М. А., Лаута О. С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей, Тр. СПИИРАН, 2017, выпуск 55, 160–184.
4. Авсентьев О. С., Дровникова И. Г., Застрожнов И. И., Попов А. Д., Рогозин Е. А. Методика управления защитой информационного ресурса системы электронного документооборота, Тр. СПИИРАН, 2018, выпуск 57, 188–210.

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМІ ЕЛЕКТРОННИХ ПЛАТЕЖІВ КОМЕРЦІЙНОГО БАНКУ УКРАЇНИ

Балабаєв В.С., БСДМ-61

Фінансові дані – один із найпопулярніших об'єктів атак кіберзлочинців в інформаційному просторі. Найбільш вигідні дані, використання яких спрямовані на отримання грошового прибутку, знаходяться у розпорядженні фінансових організацій. Саме через це банківські установи завжди знаходяться під загрозою кібернетичних атак на всіх рівнях своєї IT-інфраструктури у будь-якій точці світу.

Сучасні хакери мають у своєму розпорядженні безпрецедентно широкий набір інструментів і здатні застосовувати цей арсенал з максимальною ефективністю. Лавиноподібне зростання обсягів онлайн-трафіку і кількості мобільних кінцевих пристроїв грає на руку атакуючим. Хакери користуються розширеним робочим простором, а також свободою вибору мішені і засобів її поразки.

З кожним роком в Україні збільшується кількість кібератак, пов'язаних з отриманням фінансових даних і подальшим використанням їх у власних цілях кіберзлочинців. При цьому близько половини українських банків і платіжних систем (48%) вважає за краще боротися з наслідками кібератак, а не інвестувати кошти у засоби для покращення рівня захисту даних і рахунків своїх клієнтів.

У сучасних умовах однією з актуальних практичних задач є оцінка ефективності заходів щодо захисту інформації в інформаційних комп'ютерних системах. Дослідження цієї задачі дасть можливість розробникам і власникам інформаційних комп'ютерних систем отримувати обґрунтовану оцінку техніко-економічної

доцільності різних заходів та способів захисту інформації і формувати раціональний комплекс заходів для забезпечення інформаційної безпеки, економно витрачаючи виділені на ці цілі ресурси. Сьогодні не викликає сумнівів необхідність вкладень в забезпечення інформаційної безпеки сучасного бізнесу. Основне питання сучасного бізнесу - як оцінити необхідний рівень вкладень в інформаційну безпеку для забезпечення максимальної ефективності інвестицій в дану сферу. Для вирішення цього питання існує тільки один спосіб - застосовувати системи / комплекси аналізу ризиків, що дозволяють оцінити існуючі в системі ризики і вибрати оптимальний з точки зору ефективності варіант захисту (по співвідношенню існуючих в системі ризиків / витрат на інформаційну безпеку).

Впровадження в банківську діяльність системи управління операційним ризиком покликане зменшити втрати банку від недбалості персоналу, нестабільної роботи інформаційної системи та зовнішнього впливу, що сприяє банківській установі досягнути поставленої стратегічної мети з мінімальними фінансовими, ресурсними та інформаційними втратами.

У сучасних умовах фінансовим компаніям необхідно використовувати комплекс програмних і апаратних засобів, які б дозволили забезпечити високий рівень захищеності інфраструктури із збереженням достатньої ефективності бізнес-процесів.

1. Для протистояння атакам ефективними є методи соціальної інженерії – це регулярне навчання всіх співробітників компанії безпечній роботі в інтернет-мережі та інформування їх про існуючі види загроз;
2. Всі торгові точки, на яких може використовуватися пластикова карта будь-якого банку, є потенційними уразливими об’єктами до тих пір, поки їх POS-термінали не захищені спеціалізованим програмним забезпеченням;
3. Користування послугами сторонніх компаній, які спеціалізуються на захисті данних від DDoS-атак, підключившись до хмарних сервісів організації;
4. Сайтам, яким найбільше загрожують кібератаки, слід уважніше ставитися до рівня своєї безпеки. Необхідно посилити захищеність від підбору ідентифікаторів або паролів користувачів. Слід зазначити, що найнебезпечніші сайти написані на мові PHP, так як 76% з них містять критичні уразливості. Менш уразливими виявилися веб-ресурси на Java (70%) і ASP.NET (55%) (згідно даних компанії Positive Technologies);
5. Адміністратори корпоративної мережі організації повинні контролювати, якими додатками користуються співробітники і які сайти вони відвідують. У них повинні бути дійсні сертифікати SSL.

Інформаційна безпека та захист інформації банку повинні бути на високому рівні, для того щоб відбивати будь-які хакерські атаки і спроби будь-яких вторгнень з боку кіберзлочинців, у тому числі з боку співробітників самої організації. Для того щоб мінімізувати фінансові ризики, а в подальшому й репутаційні ризики, службам безпеки банків необхідно захистити не тільки бази даних і робочі станції персоналу, а також і комп'ютерні мережі, термінали працівників фронт-офісу та банкомати небезпечних кодів і дій кіберзлочинців.

Література

1. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD).К: НБУ., 2010. – 67 с.

2. Невойт Я.В. Методи дослідження джерел загроз інформаційній безпеці //Матеріали роботи семінару при вченій раді НАН України «Технічні засоби захисту України" (Київ, 16-19 листопада 2015 р).– Київ. – 2015. – С.18.

ЗАХИСТ АВТОРСЬКОГО ПРАВА В МЕРЕЖІ ІНТЕРНЕТ

Мужанова Т.М.

У роботі розглянуто основні положення Директиви Європейського парламенту щодо авторського права на єдиному цифровому ринку (2019 р.), у якій регулюються питання взаємовідносин авторів та дистриб'юторів їхніх творів в Інтернеті, умов оприлюднення онлайн творів з некомерційною метою, об'єктів культурної спадщини. Наведено також зауваження до положень Директиви з боку фахівців з авторського права.

Проблема захисту авторських прав у мережі Інтернет залишається гострою упродовж останніх років. Так, Інтернет-компанії не мають стимулів підписувати справедливі ліцензійні угоди з власниками авторських прав, оскільки вони не вважаються відповідальними за вміст, який завантажують їх користувачі; Інтернет-майданчики зобов'язані видаляти вміст, що порушує авторське право, лише на вимогу власника прав; можливості притягнення Інтернет-компаній до відповідальності є обмеженими.

На рівні Європейського Союзу, починаючи з 2016 року, тривала робота над удосконалення регулювання питань захисту авторських прав в Інтернеті. У березні 2019 року Європейський парламент ввів у дію новий документ - Директиву щодо авторського права на єдиному цифровому ринку [1], яка є завершенням кількарічних законодавчих зусиль. Держави-члени ЄС мають два роки для впровадження оновлених правил щодо захисту авторського права онлайн.

Нагадаємо, що авторське право (англ. - Copyright)- це форма правового захисту прав інтелектуальної власності авторів оригінальних творів, включаючи літературні, драматичні, музичні, художні, архітектурні та інші інтелектуальні твори. Також до об'єктів авторського права відносять програмне забезпечення.

Законодавство про авторські права, зокрема і Закон України про авторське та суміжні права, дають право оригінальним авторам чи художникам володіти виключним правом їх копіювання й поширення, в тому числі і в мережі Інтернет. Водночас механізми захисту копірайту в Інтернеті є недосконалими.

Директива Європарламенту щодо авторського права на єдиному цифровому ринку також спрямована на те, щоб багаторічні права та обов'язки авторського права діяли в Інтернеті.

Це законодавство найбільше вплине на Інтернет-гіганти YouTube, Facebook та Google News, оскільки має на меті заставити зазначених суб'єктів ділитися своїми прибутками з авторами, чиї твори вони оприлюднюють. Так, власники прав, зокрема музиканти, виконавці, автори сценаріїв, а також видавці новин, отримують право вести переговори щодо винагороди за використання своїх творів, коли вони розміщуються онлайн, і укладати угоди про передання

прав та ліцензійні угоди. Внаслідок цього Інтернет-платформи нестимуть безпосередню відповідальність за вміст, завантажений на їхні сайти.

Водночас, відповідно до Директиви, такі правила стосуються не всіх Інтернет-гравців, зокрема завантаження творів в онлайн-енциклопедії некомерційним способом, наприклад Вікіпедію, або платформи програмного забезпечення з відкритим кодом, такі як GitHub, виключено із сфери дії цієї директиви і регулюватимуться відповідно до «м'якших» вимог.

Крім того, документ дає право авторам і виконавцям вимагати додаткову винагороду від розповсюджувача, який користується їхніми правами, коли початково узгоджена винагорода непропорційно низька порівняно з прибутками, які отримує дистриб'ютор.

Директива має забезпечити сприяння передовим дослідженням через спрощення механізмів вільного використання матеріалів, захищених авторським правом, обміну текстами та даними, тим самим усуваючи значний конкурентний недолік, з яким зараз стикаються європейські дослідники. Директива також передбачає, що обмеження авторських прав не поширюватимуться на вміст, який використовується для викладання чи ілюстрації.

Нарешті, документ дозволяє безкоштовно використовувати матеріали, захищені авторським правом, для збереження культурної спадщини. Таким чином бібліотеки зможуть переводити в цифровий формат твори, які є культурним, історичним, науковим надбанням.

Однак, фахівці неоднозначно оцінюють положення Директиви щодо авторського права на єдиному цифровому ринку, відзначаючи крім позитивних моментів низку зауважень. Зокрема, на їх думку, зазначений нормативний документ не враховує 20-річної практики застосування американського законодавства щодо копірайту (Digital Millennium Copyright Act, 1998 р.), положень аналогічних законів інших країн, широку судову практику, огляди, публікації з аналізу ефективності або недоліків існуючих підходів нормативно-правового регулювання питань авторського права. Відповідно, результатом введення в дію Директиви може стати певна дисгармонізація законодавства держав-членів ЄС [2].

Для вітчизняної практики захисту авторських прав в Інтернеті доцільно було б запозичити положення щодо забезпечення збалансованих взаємовідносин авторів та розповсджувачів їх творчих доробків, оцифрування й вільного використання творів, що використовуються поза комерційним обігом, надання загального доступу онлайн до об'єктів наукової та культурної спадщини.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
URL: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0231_EN.pdf?redirect (дата звернення: 24.10.2019)
2. Капіца Ю.М. Директива 2019/790/ЄС про авторське право в єдиному цифровому ринку та питання адаптації законодавства України // Інформація і право. - № 3(30). – 2019. с. 65-77.
URL: http://ippi.org.ua/sites/default/files/10_14.pdf (дата звернення: 24.10.2019)