МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2021 р.

На правах рукопису
УДК 004.492.3

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Програмні засоби захисту локальної мережі банківської установи

Виконавець: Д.О. Козаченко
Керівник: д.т.н., доцент кафедри БІТ О.В. Заріцький
Нормоконтролер: д.т.н., доцент кафедри БІТ О.В. Заріцький

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 2021 р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Козаченка Дмитра Олексійовича

1. Тема: *Програмні засоби захисту локальної мережі банківської установи* затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати існуючі програмні та апаратні засоби захисту локальної мережі; на основі аналізу виділити вхідні і вихідні параметри, завдяки яким можливо провести порівняння існуючих засобів захисту, виявлення їх переваг і недоліків; розробити комплекс програмних засобів захисту локальної мережі.
4. Зміст пояснювальної записки: аналіз існуючих засобів захисту локальної мережі; розробка системи програмних засобів захисту локальної мережі; впровадження розробленої системи програмних засобів захисту локальної мережі на прикладі типової банківської установи.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	21.04.2021	*Виконано*
2.	Аналіз літературних джерел	22.04.2021 – 29.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	30.04.2021	*Виконано*
4.	Збір інформації	01.05.2021 – 10.05.2021	*Виконано*
5.	Написання розділу дипломного проекту щодо ролі банків в економіці країни та аналіз загроз для їх діяльності	11.05.2021 – 16.05.2021	*Виконано*
6.	Написання розділу дипломного проекту щодо структури та захисту локальної мережі банківської установи	17.05.2021 – 22.05.2021	*Виконано*
7.	Написання розділу дипломного проекту щодо впровадження комплексу додаткових програмних засобів захисту локальної мережі	23.05.2021 – 28.05.2021	*Виконано*
8.	Перевірка на антиплагіат	03.06.2021	*Виконано*
9.	Оформлення і друк пояснювальної записки	05.06.2021	*Виконано*
10.	Оформлення презентації	06.06.2021 – 08.06.2021	*Виконано*
11.	Отримання рецензій від рецензента	09.06.2021	*Виконано*

Здобувач вищої освіти Д.О. Козаченко

Керівник дипломної роботи О.В. Заріцький

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатки і має 64 сторінкок основного тексту, 6 рисунків, 1 таблиця, 8 сторінок додатків. Список використаних джерел містить 33 найменування і займає 4 сторінки. Загальний обсяг роботи 72 сторінок.

Метою роботи є підвищення рівня захищеності локальної мережі банківської установи. Метою дослідження: порівняння, оцінка, аналіз, підвищення.

В дипломній роботі були розглянуті сучасні кіберзагрози для банківської сфери, проаналізована типова схема атаки на локальну мережу, визначення слабких місць в захисті локальної мережі, реалізованою за допомогою основних програмних та апаратних засобів захисту та впровадження додаткових програмних засобів захисту для підвищення рівня захищеності локальної мережі.

Практична цінність роботи полягає в проведенні аналізу загроз для локальної мережі банківської установи та визначення рівня захищеності системи, реалізованому виключно за допомогою програмних та апаратних засобів захисту, необхідних згідно вимог Національно банку України. Було аргументовано недостатній рівень захищеності локальної мережі, без впровадження додаткових програмних засобів захисту та запропоновано програмні рішення для підвищення рівня її захищеності.

Розглянуті програмні засоби можуть бути успішно реалізовані на практиці для підвищення рівня захищеності локальної мережі банківської установи.

Ключові слова: локальна мережа, захист локальної мережі, програмні засоби захисту, інформаційна безпека, банківська установа.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

LAN – Local Area Network – локальна комп'ютерна мережа
WAN – Wide Area Network – глобальна комп'ютерна мережа
VLAN – віртуальна локальна комп’ютерна мережа
VPN – Virtual Private Network – віртуальна приватна мережа
ПК – персональний комп’ютер
ОС – операційна система
ЕОМ – електронна обчислювальна машина
ІОМ – інформаційно-обчислювальна мережа
URL – уніфікований локатор ресурсів (адреса ресурсу)
HTTP – протокол передачі гіпертексту та інших типів даних
OSI – базова еталонна модель взаємодії відкритих систем
НБУ – Національний банк України
ІБ – інформаційна безпека
IDS – Intrusion Detection System – система виявлення вторгнень
IPS – Intrusion Prevention System – система запобігання вторгненням
SIEM – Security information and event management – система моніторингу та управління інформаційною безпекою
UEBA – User and Entity Behavior Analytics – система поведінкового аналізу
IRP – Incident Response Platform – система автоматизації реагування на інциденти інформаційної безпеки
DLP – Data Loss Prevention – системи запобігання витоків даних

ВСТУП

Актуальність. За останні роки в новинах регулярно з'являються повідомлення про нові масштабні пограбуваннях банків. Назви злочинних угрупування, які проводять кібератаки, зазвичай відомі не лише кожному фахівцю в сфері кібербезпеки, але й пересічним людям. До найвідоміших угрупувань відносять Cobalt, Carbanak, Lazarus, оскільки на їх рахунку ряд багатомільйонних крадіжок.

В ЗМІ постійно з'являються новини про нові успішно проведені кібератаки на всесвітньо відомі банки. Так, до найвідоміших кіберзлочинних угрупованнь минулого десятиріччя можна віднести угруповання Cobalt, яке відоме своїми атаками на фінансові організації СНД, Східної Європи і Південно-Східної Азії. У 2017 році були зафіксовані атаки в країнах Західної Європи, Північній та Південній частині Америки. Цілями Cobalt є фінансові організацій, серед яких відомі банки, фондові біржі, інвестиційні фонди та інші організації кредитно-фінансового профілю. Проникнувши у мережу банку, ціллю зловмисників став доступ до системи управління банкоматами. Схема викрадення грошей реалізовувалася без фізичного втручання в роботу пристрою. Хакери віддалено відправляли команди на видачу готівки, а їх співучасники забирали з банкомату всі наявні в ньому банкноти. [1]

Хакери організації Carbanak були причетні до серії атак 2014-2015 роках. Зловмисники експлуатували виключно недоліки захищеності корпоративних мереж, завдяки чому їм вдавалося отриманий доступ до будь-яких систем. За підрахунками експертів загальна сума вкрадених коштів перевищує мільярд доларів.

Головною метою злончиців є захоплення контролю над корпоративною мережею банку. Отримавши повний доступ до всір ресурсів організації, хакери отримують в свої руки повний контроль над міжбанківськими переказами коштів, інтернет-банкінгом, системами управління терміналами та банкоматами.

Окрім безпосередньо фінансової складової, банківські установи зберігають конфіденційні дані стосовно клієнтів банку та його співробітників, інофрмацію, що становить банківську та комерційну таємницю. При наявності знань та необхідних технічних засобів, зловмисники отримують вагому винагороду, а потрапляють в руки правохоронних органів лише одиниці з них.

Захоплення контролю над корпоративною мережею банку починається з атаки на найбільш незахищені її компоненти. Переважно банківська корпоративна мережа складається з багатьох локальних мереж - філіалів та офісів організації. Працівники банку здатні отримувати доступ до інформаційних ресурсів при віддаленій роботі. Необхідною умовою для забезпечення захищеності інформаційних ресурсів банку є відповідальний підхід до захисту кожної її локальної мережі. Методи та засоби захист комплексним підходом, що включають в себе організаційні вимоги, програмні та апаратні засоби захисту.

Банківські установи приділяють багато уваги захисту своїх інформаційних ресурсів, однак, як показує практика, хакерам постійно вдається подолати багаторівневі засоби захисту локальних мереж. Відповідно до проведених компанією Positive Technologies досліджень, для проникнення у корпоративну мережу банку, злочинцям необхідно в середньому п'ять днів, а отримати повний контроль над інфраструктурою банку вони зможуть за додаткові два дні. [2]

Метою дипломного проекту є підвищення рівня захищеності локальної мережі банківської установи.

Досягнення мети потребує розв’язання наступних задач:

- аналіз існуючих загроз для локальної мережі;
- визначення загроз, що залишаються після реалізації мінімального комплексу обов’язкових програмних та апаратних засобів захисту локальної мережі;
- розробка та впровадження комплексу додаткових програмних засобів захисту.

Об’єкт – процес захисту локальної мережі банківської установи.

Предмет – програмні засоби захисту локальної мережі.

Практична цінність дипломної роботи полягає у тому, що запропоновані програмні засоби захисту можуть використовуватися на практиці при побудові комплексного захисту локальних мережах банківських установ. Методичні рекомендації, запропоновані в даній роботі, можуть бути корисними для працівників інформаційної безпеки банку при прийнятті рішення щодо вибору ефективних програмних засобів для підвищення рівня захищеності вже створених локальних мереж мереж.

РОЗДІЛ 1. РОЛЬ БАНКІВ В ЕКОНОМІЦІ КРАЇНИ ТА АНАЛІЗ ЗАГРОЗ ДЛЯ ЇХ ДІЯЛЬНОСТІ

1.1 Світові збитки від проведених кібератак

"Цифровий світ змінив майже всі аспекти нашого життя, включаючи ризик та злочинність, завдяки чому злочин є більш ефективним, менш ризикованим, вигіднішим і ніколи не був простішим у виконанні" , - Стів Гробман, головний технологічний директор McAfee. [3]

За даними проведених спільних досліджень компанією McAfee, одним з лідерів на ринку програмних рішень з кібербезпеки для бізнесу та споживачів, та Центром стратегічних та міжнародних досліджень (CSIS)- некомерційної організації з досліджень політики, яка займається наданням стратегічної інформації та політичних рішень, спостерігається стрімке збільшення впливу кібератак на світову економіку. Станом на 2018 рік кіберзлочинність коштувала компаніям близько 600 млрд доларів на рік. При проведених аналогічних дослідженнях у 2014 році глобальні збитки склали близько 445 млрд доларів, а в 2012- 110 мільярдів доларів. Однак за останніми підрахунками експертів, у 2020 році збитки сягнули 1 відсоток від всесвітнього ВВП- трильйон долларів США (рис1.1). [4]

Наразі банківська сфера залишаються улюбленою ціллю кіберзлочинців. За даними досліджень, хакери з Росії, Північної Кореї та Ірану переважно займаються зламали фінансових установ по всьому світу.

Рис. 1.1 Діаграма світових збитків від кіберзлочинів

Стрімкий технологічний розвиток, інформатизація діяльності бізнесу, багатомільйонні доходи та відносно низький ризик затримання сприяють активному розвитку кіберзлочинності. Незважаючи на те, що окремих осіб вдається викрити, їх місце швидко займають інші. Складається ситуація, при якій зловмисник володіючи мінімальними знаннями в мережевій архітектурі та структурі баз даних здатен провести кібератаку та викрасти мільйони доларів, проникнувши в мережу банку. На спеціалізованих інтернет форумах будь-який бажаючий може знайти та придбати програмне забезпечення для проведення атаки, отримати докладні інструкції щодо його використання, знайти посібників серед співробітників організації та заручитися підтримкою злочинних співтовариств.

Злочинці швидко адаптуються до середовища та постійно вдосконалюють техніки атак. Вони невпинно досліджують вразливості захисту підприємств та встигають експлуатувати їх набагато швидше, ніж служби безпеки знайдуть дефекти в захисті та встановлять відповідні оновлення.

1.2 Роль банку в економіці країни

Роль банку в економіці країни

Розвиток ефективних ринкових відносин неможливо створити без функціонуючого банківського сектору. Саме завдяки банкам реалізуються зв'язки між всіма складовими частинами господарського механізму економіки країни. Комерційні банки є центрами фінансової системи, що зосереджують фінансові ресурси вкладників і відкривають можливості доступу до джерел позичених ресурсів позичальникам, тим самим сприяючи розвитку реального сектора економіки.

За даними Міністерства фінансів України, станом на 1 травня 2021 року загальна кількість діючих комерційних банків в Україні становить 73, серед яких 33 банки з іноземним капіталом 33, з яких 23 зі 100% іноземним капіталом. [5]

Головним завданням сьогодення є встановлення стабільної економічної ситуації в Україні. Успішність виконання цього завдання залежить від розвитку банківської системи та кожного банку зокрема. Спираючись на досвід країн із розвиненою ринковою економікою, можна констатувати, що лише функціонування адекватної ринковим умовам банківської системи є одним із головних важелів створення ефективної, глобалізованої економіки країни.

Банківська таємниця як вид інформації

Під час відкриття банківського рахунку з метою отримання заробітної плати або користувацького кредиту, клієнт підписує з банком згоду на отримання та обробку своїх персональних даних відповідно до Закону України "О захисті персональних даних".

Відповідно до статті 21 Закону України "Про інформацію", інформацією є будь-які відомості та дані, які зберігаються на матеріальних носіях або відображені в електронному вигляді. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. [6]

Національний банк України створює та контролює нормативно-правові акти з питань зберігання, обробки, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів у статті 60 Закону України "Про банки і банківську діяльність". [7]

Відповідно до даного закону, до банківської таємниці відносять інформацію про банки та клієнтів, а саме:

1. відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
2. операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди;
3. фінансово-економічний стан клієнтів;
4. інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності;
5. відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
6. інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;
7. коди, що використовуються банками для захисту інформації;
8. інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності.

Втрата документів, які є банківською таємницею, може призвести до значних репутаційних та фінансових втрат, а в окремих випадках- до повної втрати банком ліцензії на роботу. Клієнти банку, відповідно до статті 200 Цивільного кодексу України, мають право вимагати усунення порушень їх права на захист конфіденційної інформації та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями. [8]

1.3 Опис сучасних загроз

Аналіз типової схеми атаки та визначення способів несанкціонованого доступу до локальної мережі

Вибір цілі зловмисника багато в чому обумовлений його технічною підготовкою, наявними інструментами і знаннями про внутрішні процеси банку, які мають злочинці. Кожна з атак має свої особливості, зокрема дії злочинців розрізняються на етапі виведення грошових коштів, але присутні і спільні риси.

Етап розвідки та підготовки досить тривалий і трудомісткий. Зловмиснику необхідно зібрати якомога більше інформації про банк, яка допоможе подолати системи захисту, і провести попередню організаційну роботу, з огляду на специфіку банку. Оскільки сканування зовнішніх ресурсів може бути виявлено системами захисту, для того, щоб не розкрити себе на початковому етапі, злочинці вдаються до пасивних методів отримання інформації, наприклад для виявлення доменних імен і адрес, що належать банку.

Зловмисники додатково використовують інформацію про складові частини локальної мережі банку, її топологію та IP адреси, яку недобросовісні співробітники банків готові за грошову винагороду надати злочинцям.

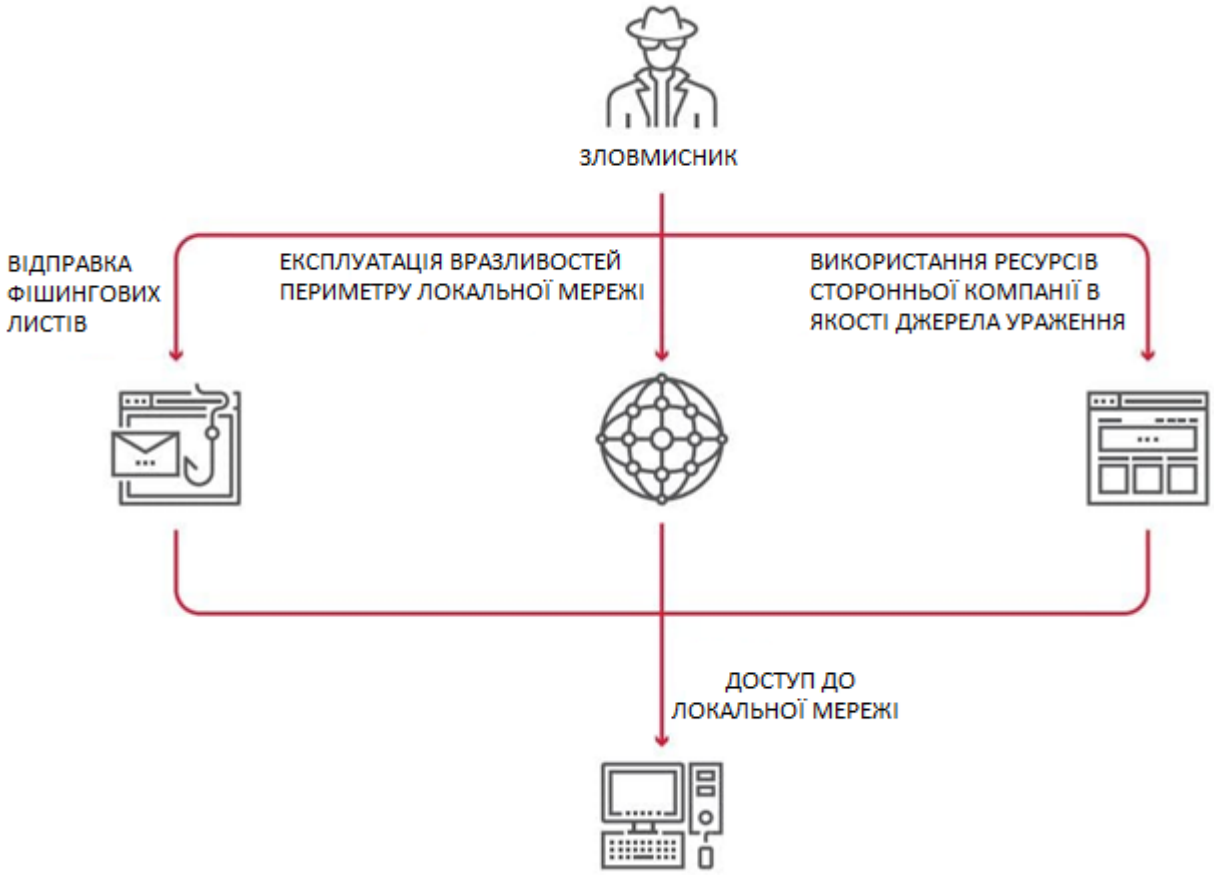

Рис. 1.2 Методи проникнення у локальну мережу

Популярні техніки проведення атак

Після проведення зловмисниками дослідження структури та захисту локальної мережі, вони переходять в наступ. На сьогоднішній день банки приділяють достатньо уваги для захисту свого зовнішнього периметру, впроваджуючи декілька рівнів програмних та апаратних засобів захисту. Однак для проведення атаки, зловмиснику не потрібно “йти в лоб” на систему. Аналізуючи успішно проведені атаки, експерти виділяють декілька напрямків атаки на систему, що наразі активно практикуються зловмисниками. До найпоширеніших відносять пошук уразливостей нульового дня та фішинг-розсилку уражених шкідливим програмним забезпеченням листів на корпоративну пошту співробітників компанії.

Уразливості нульового дня

На етапі підготовки до атаки на певну компанію, зловмисники активно аналізують доступні методи ураження системи зловмисними програмами. Виявлені ними слабкі місця в захисті, які наразі не усунені розробниками або підрозділами забезпечення безпеки організації називають уразливістю нульового дня. Найчастіше зловмисники використовують власні розроблені експлойти, які використовують вразливості в програмному забезпеченні.

Уразливістю нульового дня є раніше невідомий дефект в безпеці, яку зловмисник успішно експлуатує для проведення атаки. Подібні уразливості оцінюються як критичні і потребують негайного вживання заходів щодо їх усунення.

Спочатку такі уразливості нікому не відомі. Розробники програмного забезпечення, антивірусні компанії, системні адміністратори не підозрюють про їх існування. Про небезпеку стає відомо до того, як виробник випускає оновлення з виправленням дефекту. Мережа, на пристроях якої встановлена програма, чи недолік у мережевій безпеці знаходяться в зоні ризику, а користувачі не мають можливості захиститися.

Атака на уразливість нульового дня означає що зловмисники знали про наявність дефекту достатньо довго, оскільки їм вистачило часу для написання шкідливого програмного коду та його успішну експлуатацію.

Найвідомішою шкідливою програмою, що використовує цю уразливість є мережевий черв'як-вимагач WannaCry який використовував експлойт EternalBlue в уразливості Server Message Block на операційних системах сімейства Windows.

При потраплянні на комп'ютер, WannaCry встановлює бекдор для подальших зловмисних дій. Даний черв'як був виявлений в середині травня 2017 року.

Атаки нульового дня на сьогоднішній день є одними з найскладніших типів загроз, оскільки зловмисники здатні використати врзливості до моменту їх виправлення розробниками, відповідно дані типи атак мають найбільш руйнівні наслідки.

Фішинг

Фішинг наразі є одним з найдавніших способів отримання конфіденційної інформації. Дана атака проводиться з використанням електронної пошти. Метою зловмисників переважно є крадіжка конфіденційної інформації, наприклад облікових даних користувача. Однак досить часто кіберзлодії обманом підштовхують жертву до завантаження на її пристрій файлу чи програмного додатку, в якому знаходиться шкідливе ПЗ, наприклад віруси, черви, троянські програми.

Стандартний спосіб фішингу будується наступним чином. Жертва отримує електронний лист або текстове повідомлення, відправник якого видає себе за певну особу або організацію. Коли одержувач відкриває електронний лист, то він виявляє текст, що вимагає від жертви перейти на певний веб-сайт або завантажити файл.

Наразі найбільш поширеним і ефективним методом проникнення в інфраструктуру банку є саме фішингове розсилання електронних листів на адресу співробітників банку. Повідомлення можуть надходити як на робочі адреси, так і на особисті. Такий метод використовується, наприклад, угрупованням Cobalt, також його застосовували Lazarus, Metel, GCMAN.

Даний метод активно використовується на етапі проникнення в систему банку. На Рис.1.3 зображено лист, який у 2017 розі використовувало злочинне угрупованням Cobalt для проведення атаки на банки.

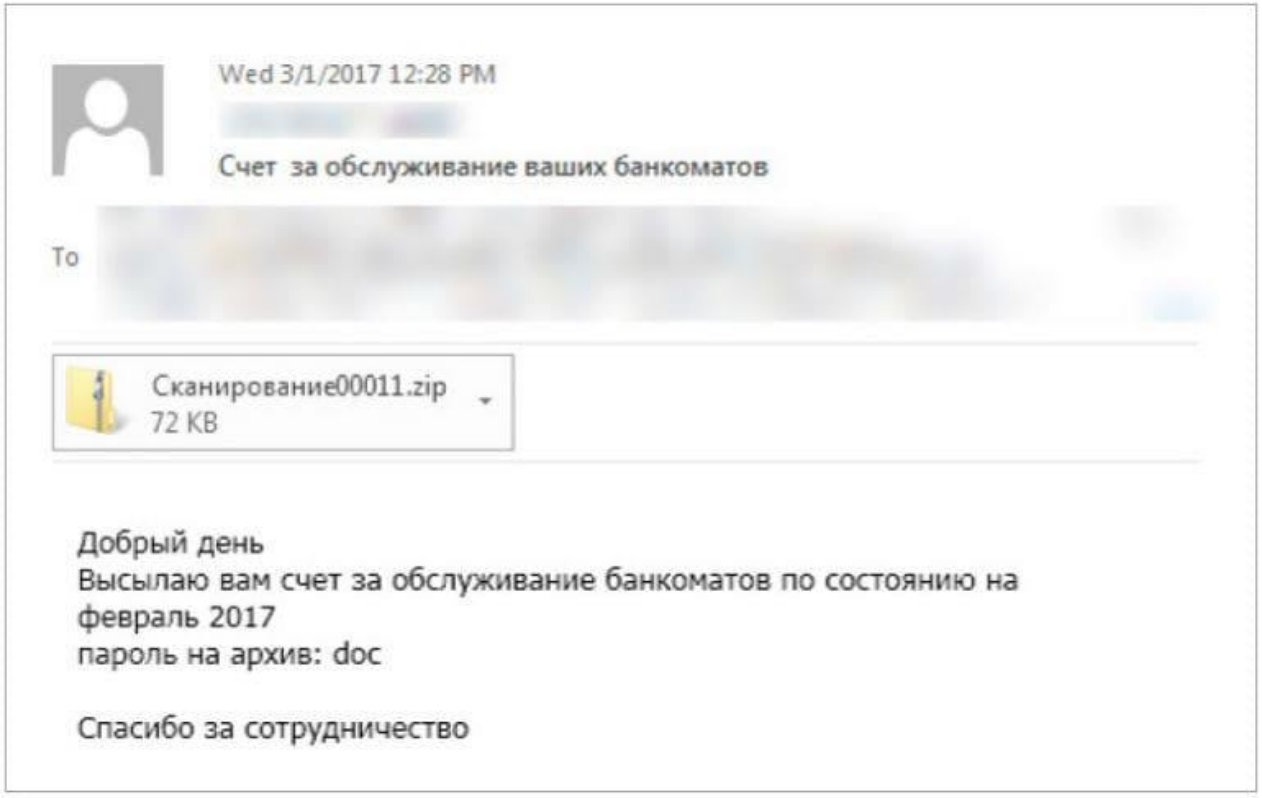

Рис.1.3 Приклад фішингового листа

У сфері атак на корпоративні системи фішингу передує ретельний збір і аналіз інформації про об'єкт та суб'єктів атаки, горизонтальні зв'язки, можливі зони відповідальності та повноваження. Це необхідно для розробки сценарію з додаванням унікальних деталей, що дозволяють знизити пильність одержувачів листа.

В даний час зростає частка цільових фішинг-атак, організованих за допомогою розповсюдження електронних листів, де можна визначити конкретну організацію або групу осіб. Цільові користувачі отримують фішингові повідомлення, які змушують людину вводити конфіденційну особисту інформацію. Окрім запитів на введення облікових даних, цільові фішингові електронні листи також можуть містити шкідливий код. Так, наприклад, при натисканні певної клавіші можна завантажувати програми для відстеження всього, що жертва вводить з клавіатури.

Засоби проведення атак

Після визначення необхідного методу атаки, зловмисник переходить до пошуку або написання шкідливого програмного забезпечення, необхідного для проведення цільової атаки.

Шкідлива програма - комп'ютерна програма або код, призначений для реалізації загроз інформації, що зберігається в комп'ютерній системі, або для прихованого нецільового використання ресурсів системи, або іншого впливу, що перешкоджає нормальному функціонуванню комп'ютерної системи. До шкідливого програмного забезпечення відносяться мережеві черв'яки, класичні файлові віруси, троянські програми, хакерські утиліти та інші програми, що завдають шкоди комп'ютеру, на якому вони запускаються на виконання, або іншим комп'ютерам в мережі.

Незалежно від типу, шкідливі програми здатні завдавати значної шкоди, реалізуючи будь-які загрози інформації - порушення цілісності, конфіденційності, доступності.

До найпоширеніших видів шкідливого ПЗ відносять:

1. віруси;
2. хробаки;
3. троянські програми;
4. шпигунське програмне забезпечення;
5. шифрувальники.

Хакери активно працюють над створенням шкідливих програм, які не виявляються антивірусними сканерами. Відсутність детектування досягається за рахунок застосування хакерами таких технологій, як обфускація, шифрування програмного коду тощо.

Віруси

Комп’ютерним вірусом є невеликі програми, що здатні самостійно проникнути в комп'ютер і додавати зловмисний код. Результатом зараження

вірусом може бути збій роботи системи за рахунок порушення структури розміщення даних або навіть повне руйнування компонентів операційної системи.

Віруси діють виключно програмним шляхом. Вони потрапляють на комп’ютер тільки разом з зараженими файлами та програмними додатками, додаючи в структуру програми зловмисний код з метою управління при виконанні зараженого файлу.

Вірус активується та починає діяти самостійно після завантаження файлу на пристрій. Під час запуску зараженого файлу деякі види вірусів закріпляються в оперативній пам’яті комп’ютера, тобто стають постійними резидентами та можуть заражати інші файли та програми, що завантажуються на ПК. Характерною особливістю вірусів є те, що вони активуються відразу після завантаження на комп’ютер та переважно спрямовані на спричинення серйозних пошкоджень системі, наприклад шифрування жорсткого диску, тощо.

На відміну від хробаків, віруси не використовують мережевих сервісів для проникнення на інші комп'ютери. Копія вірусу потрапляє на віддалені комп'ютери тільки в тому випадку, якщо заражений об'єкт з яких-небудь не залежних від функціонала вірусу причин виявляється активізованим на іншому комп'ютері, наприклад:

- при зараженні доступних дисків вірус проник у файли, розташовані на мережевому ресурсі;

- вірус скопіював себе на знімний носій або заразив файли на ньому;

- користувач відіслав електронний лист із ураженим вкладенням.

На сьогоднішній день фахівцями встановлено, що загальна чисельність досліджених комп’ютерних вірусів перевищує 50 тисяч.

Хробаки

Хробаки - шкідливі програми, які є більш небезпечними, ніж віруси та троянські програми. Вони здатні до стрімкого розповсюдження між всіма комп’ютерами у локальній мережі використовуючи електронну пошту та інші інформаційні канали. Під час потрапляння на комп’ютер, хробаки отримують

доступ до мережевих адрес інших комп’ютерів у системі, сканують адресні книги поштових клієнтів та розсилають за знайденими адресами свої копії.

Основною метою є:

1. проникнення на віддалені комп'ютери;
2. запуску своєї копії на віддаленому комп'ютері;
3. подальшого поширення на інші комп'ютери в мережі.

Для свого поширення мережеві хробаки використовують різноманітні комп'ютерні і мобільні мережі: електронну пошту, системи обміну миттєвими повідомленнями, файлообмінні, LAN, мережі обміну даними між мобільними пристроями, тощо.

Деякі хробаки володіють властивостями інших різновидів шкідливого програмного забезпечення. Наприклад, деякі програми даного типу містять троянські функції або здатні заражати виконувані файли на локальному диску, тобто мають властивість троянської програми або комп'ютерного вірусу.

Троянські програми

Трояни, на відміну від вірусів, не заражають інші програми. Троянські програми також не проникають в комп'ютер самостійно - зловмисники маскують їх під виглядом корисного ПЗ, яке встановлює сам користувач. Трояни наносять ще більшої шкоди, оскільки крім видалення системних і особистих файлів здатні збирати конфіденційну інформацію і її передачу зловмисникові.

Окремі категорії троянських програм завдають шкоди віддаленим комп'ютерам і мережам, не порушуючи працездатність зараженого комп'ютера

Даний тип шкідливого програмного забезпечення виконує в уражених комп’ютерах несанкціоновані дії від особи користувача. До розповсюджених шкідливих дій можна віднести:

1. знищення частково або повністю інформації на носіях інформації;
2. крадіжка конфіденційної інформації;
3. призводить до некоректної роботи системи.

Збитки, заподіяні троянськими програмами, можуть багатократно перевищувати втрати від інших типів шкідливого ПЗ.

Шпигунське програмне забезпечення

Шпигунські програми використовується для збору конфіденційної інформації про певний користувача шляхом тотального сканування системних і робочих папок його комп'ютера. Програми-шпигуни функціонують на ПК непомітно, не надаючи видимої навантаження на операційну систему. Крім отримання особистих даних шпигунські програми застосовуються для віддаленого контролю чужого комп'ютера.

Головною метою шпигунського програмного забезпечення є:

1. реєстрація дій користувача на ПК;
2. збір інформації про зміст жорсткого диску;
3. збір інформації про встановлене на комп’ютері програмне забезпечення та його налаштування;
4. збір інформації про параметри модему та іншого мережевого обладнання, його конфігурації, спосіб підключення, тощо.

Деякі програми мають можливість вбудовуватися у встановлений на комп’ютері браузер та перенаправляти трафік.

Шифрувальники

У 2016 програми-шифрувальники визнали основною загрозою інформаційної безпеки року. Наразі шифрувальщики мають покращений код, більш складні алгоритми шифрування, отже стали більш небезпечними ніж раніше. Потрапляючи в систему, вони зашифровують усі файли користувача і вимагають сплатити кошти за дешифрування інформації.

Оскільки програми класифікуються як шкідливий код, до них застосовуються ті самі загальні критерії класифікації, що й до інших зразків

небезпечного коду. Програми можна розділити за методом розповсюдження: шляхом фішингу або спаму, завантаження заражених файлів, використання служб обміну файлами тощо. Після перетворення файлів користувача кодер вірусу зазвичай залишає інструкцію: у вигляді фону робочого столу, як текстовий документ на робочому столі або в будь-яких зашифрованих файлах.

У 2017 році ряд українських державних установ та банків зазнали кібератаки з використанням мережевого хробака-шифрувальника під назвою "Petya". За підрахунками експертів, від дій вірусу постраждала майже третина банків України.

1.4 Постановка задачі дослідження

Банківський сектор України потребує особливої уваги до системи захисту корпоративної мережі. Неправомірний доступ до банківської таємниці та фінансам організації може нанести незворотній вплив на діяльність банку в майбутньому.

Для створення ефективної системи захисту локальної мережі банківської установи, в першу чергу необхідно проаналізувати кібератаки, що були проведені на банківський сектор та визначити актуальні кіберзагрози для локальної мережі банківської установи.

Необхідно ознайомитись із структурою локальної мережі та основними її компонентами, проаналізувати нормативно-правову базу, яку використовують про побудові локальної мережі банківської установи та необхідні вимоги Національного банку України щодо впровадження комплексу обов’язкових програмних, апаратних та організаційних підходів до захисту локальної мережі. Необхідно проаналізувати основні компоненти локальної мережі, визначити шляхи їх ураження та оцінити рівень захищеності системи за допомогою мінімального необхідного комплексу засобів захисту. Результатом проведених

досліджень має стати визначення основних недоліків у комплексі засобів захисту, що реалізовані відповідно до комплексу мінімальних вимог НБУ.

Заключним етапом роботи буде аналіз ринку сучасних програмних засобів захисту локальної мережі, визначення комплексу необхідних програмних засобів для підвищення рівня безпеки захисту локальної мережі банківської установи та впровадження обраних засобів захисту до існуючої локальної мережі. Після реалізації комплексу додаткових програмних засобів захисту необхідно провести порівняння рівня захищеності локальної мережі до та після їх впровадження, та за результатами проведеної оцінки зробити висновок щодо доцільності використання обраного комплексу програмних засобів захисту локальної мережі.

Висновки до першого розділу

Всесвітні економічні збитки від хакерських атак у 2020 році склали понад один відсоток всього світового ВВП, що на п’ятдесят відсотків більше ніж у 2018. Ввиду стрімкого зростання рівня кіберзлочинності та постійного вдосконалення існуючого шкідливого програмного забезпечення, яке наразі здатне безперешкодно обходити наявні засоби захисту мережі, організаціям різного напрямку бізнесу необхідно постійно переглядати політику інформаційної безпеки своєї організації.

Для проведення атаки на фінансовий сектор бізнесу, хакерам необхідні значні технічні та фінансові ресурси. Відповідно до статистики успішно проведених атак, проти працівників кіберпезпеки банку виступають зловмисники з не менш високим рівнем підготовки, на рахунку яких десятки успішно проведених атак на всесвітньо відомі банки. Відповідно протидіяти їх загрозам надзвичайно складно та дорого.

Розвинена банківська система країни прискорює розвиток бізнесу та призводить до швидкого покращення рівня життя населення загалом.

Забезпечення безперебійної роботи банківського сектору є не лише вимогою правління організації, а й національним інтересом країни.

Фінансові втрати та витік конфіденційної інформації клієнтів банку може призвести до найсуворіших наслідків для організації- репутаційним та фінансовим втратам, та зниженню довіри населення до банківського сектору країни загалом.

Однак, не зважаючи на високу фінансову спроможність банків до впровадження актуальних програмних та технічних засобів захисту корпоративної мережі, випадки успішних нападів на банки все частішають.

РОЗДІЛ 2. СТРУКТУРА ТА ЗАХИСТ ЛОКАЛЬНОЇ МЕРЕЖІ БАНКІВСЬКОЇ УСТАНОВИ

2.1 Локальна мережа банку

Корпоративна мережа банку

Корпоративна мережа на сьогоднішній день є невід'ємною частиною сучасних компаній. Основною метою корпоративної мережі є створення ефективної внутрішньої та зовнішньої роботи компанії. За допомогою таких мереж можна безпечно та швидко передавати інформацію всередині організації.

Фактично, корпоративна мережа складається з сукупності взаємопов'язаних локальних мереж під впливом глобальної мережі. Користувачами цієї мережі є виключно працівниками відповідної організації. До корпоративної мережі можуть входити офіси, філіали, підрозділи та інші структури компанії, розміщені в межах одного міста, країни або навіть об'єднувати офіси, розташовані на різних континентах (Рис. 2.1.).

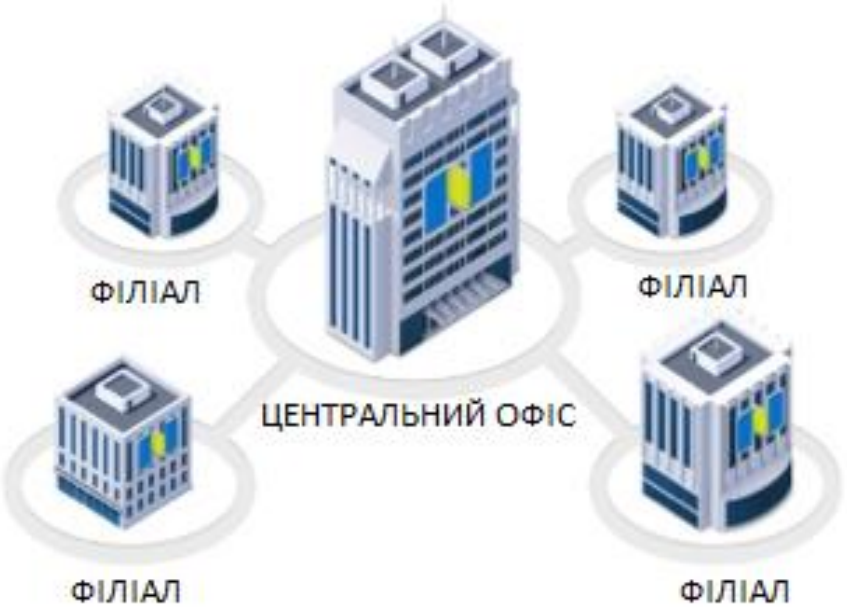

Рис. 2.1. Схема корпоративної мережі банку

Локальні корпоративні мережі організації пов'язані між собою через транспортну мережу, якою найчастіше виступає мережа Інтернет. Основний

обмін даними здійснюється в локальних мережах. Транспортна мережа призначена для об’єднання офісів організації між собою. Трафік у каналах передачі даних зменшується за допомогою побудови ієрархічної структури мережі.

Канал передачі даних містить магістральну транспортну мережу в ролі лінії зв'язку для обміну даними між відділами, кінцеве обладнання для прийому та передачі даних, комутаційне обладнання на шляху передачі даних. Вибір каналу зв'язку є важливим завданням під час організації єдиної корпоративної мережі. До основних способів реалізації зв'язку відносять власний фізичний канал зв'язку та VPN з'єднання.

Фізичний канал зв'язку реалізується методом прокладання між відділами організації фізичного кабелю. Даний метод прийнятний лише для об’єднання філіалів в межах кількох будівель. До переваг цього методу відносять безпеку передачі даних, адже потоки інформації не передаються через мережу Інтернет.

Інший варіант організації мережі використовує вже існуючу глобальну мережу. Однак для забезпечення безпечного з'єднання між філіалами та віддаленими користувачами, організації створюють захищені канали зв'язку-VPN.

Наразі технологія VPN є основною при побудові глобальної корпоративної мережі, філіали якої охоплюють великі території. Технологія віртуальних приватних мереж забезпечує безпечну передачу даних всередині корпоративної мережі за допомогою шифрування трафіку. Дана технологія також дозволяє безпечно підключатися до мережі компанії віддаленим працівникам та отримувати доступ до всіх її компонентів.

Локальна мережа банку

Локальною комп’ютерною мережею називають комп’ютерну мережу, що складається з сукупності комп’ютерів та мережних пристроїв, які з’єднані між собою. На відміну від глобальної комп’ютерної мережі, шо об’єднує окремі

комп’ютери та комп’ютерні мережі, розташовані в різних країнах або навіть континентах, пристрої в локальній мережі розташовані на відносно невеликій відстані один від одного, в межах одного приміщення чи будівлі підприємства.

Поєднання комп’ютерів між собою є необхідним кроком у компаніях та організаціях різного профілю та масштабу, оскільки даний підхід надає значні переваги при роботі з інформацією та периферійними пристроями.

До основних переваг об’єднання комп’ютерів у локальну мережу можна віднести:

1. розподіл даних вирішує проблему зберігання однакової інформації на всіх комп’ютерах в мережі, оскільки дані зберігаються на сервері та можуть бути доступні для будь-якого ПК, підключеного до мережі;
2. розподіл ресурсів надає користувачам мережі спільний доступ до периферійних пристроїв- принтерів, факсів, тощо;
3. розподіл програм дозволяє отримати усім користувачам мережі доступ до централізовано встановлених програм за умови, що необхідна мережева версія цих програм;
4. електронна пошта надає можливість всім користувачам мережі швидко передавати та приймати повідомлення.

До основних складових локальної мережі входять:

1. комп’ютери;
2. периферійні пристрої;
3. комунікаційне обладнання;
4. операційні системи;
5. мережеві додатки.

Комп'ютери

Основою будь-якої локальної мережі є комп’ютери, які підключаються до мережі за допомогою мережевої карти- периферійного пристрою, щ надає можливість з’єднати комп’ютери з іншими пристроями в мережі. Всі комп'ютери в локальних мережах поділяються на два класи: робочі станції та сервери.

Робочі станції

Робочою станцією називають комп’ютер, який знаходиться в сладі локальної мережі. На робочих станціях працівники виконують свої службові обов’язки- працюють з базами даних, документами, звітами, проводять розрахунки, обслуговують клієнтів банку.

Працівники мають доступ до персональних робочих станцій локальної мережі банку, отже захист цих пристроїв від навмисних або енавмисних неправомірних дій та контроль за наданих їм повноважень є одним з головних кроків при побудові системи безпеки локальної мережі.

Сервери

Сервером називають спеціальний комп’ютер, який призначено для прийому, зберігання та передачі інформації певного типу. Він виконує функції обслугоування мережі та надання власних ресурсів вузлам мережі- робочим станціям. Доступ до серверу здійснюється з клієнтських пристроїв, яким надано відповідні привілеї.

Залежно від функцій, що виконує сервер в корпоративній мережі, на ньому зберігаються різні типи даних. До основних різновидів серверів відносять:

1. Веб сервер - зберігає графічний та текстовий матеріал, з якого створено сайт організації;
2. Поштовий сервер –зберігає корпоративну електронну пошту від локальних користувачів, які знаходиться в одному домені, та віддалених - тобто тих, що знаходиться в іншому домені;
3. Сервер локальної мережі –виконує функції управління локальною мережею, відповідає за зв’язок всередині мережі, зберігання спільних файлів та забезпечує доступ до спільного дискового простору;
4. VPN-сервер - зебезпечує роботу віртуальної приватної мережі та дозволяє віддаленим користувачам безпечно приєднуватися до локальної мережі;

5. Сервери додатків - виконують прикладні частини клієнт-серверних додатків, а також зберігають дані, доступні клієнтам.

Комунікаційне обладнання

Комутатори - основні структурні елементи будь-якої мережі. Вони з'єднують багато пристроїв (комп'ютери, бездротові точки доступу, принтери та сервери) між собою у локальній мережі. Завдяки комутатору підключені пристрої можуть обмінюватися інформацією та підтримувати зв’язок між собою.

Маршрутизатори - здійснюють передачу даних між комп’ютерними мережами та керують трафіком в глобальній мережі. Пакет даних пересилається між маршрутизаторами через мережу Інтернет доки він не досягне кінцевого пункту призначення. Маршрутизатор виконує підключення до двох або більше ліній зв’язку з різних мереж.

2.2 Вимоги Національного банку України до захисту локальної мережі

Специфіка роботи банківської установи пов’язана з безпосереднім зберіганням та обробкою значного об’єму персональної інформації працівників та клієнтів банку, інформації що становить банківську та комерційну таємницю. Відповідно до проектування та захисту локальної мережі банку приділяється особлива увага.

Обов’язкові мінімальні вимоги до організації заходів із забезпечення інформаційної безпеки та кіберзахисту, принципи управління інформаційною безпекою та вимоги до інформаційних систем банку описані в постанові Національного банку України 28.09.2017 № 95 “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України”. [9]

Забезпечення безпеки локальної мережі відбувається за допомогою впровадження комплексу програмних та апаратних засобів захисту. Відповідно до вимог НБУ, обов’язковими засобами захисту є:

1. Антивіруси;
2. Міжмережеві екрани;
3. Системи виявлення та запобігання вторгненням;
4. Системи контролю та управління обліковими записами;
5. Системи запобігання витоків даних;
6. Засоби перевідки пошти та захисту від спаму;
7. Засоби захисту від DoS/DDoS-атак;

Даний комплекс програмних та апаратних засобів є мінімальним необхідним для впровадження в кожній банківській установі, та небанківських установах, що є учасниками інформаційних систем Національного банку.

Організації різного профілю діяльності, включаючи банківську сферу, активно практикують доповнення комплексу основних засобів захисту додатковими програмними засобами, серед яких:

1. Засоби захисту від експлойтів;
2. Сканери вразливостей;
3. Засоби управління портативними пристроями.

Антивіруси

Антивірусний захист є основою інформаційної безпеки та наразі є єдиним ефективним засобом боротьби зі шкідливим програмним забезпеченням, що забезпечує комплексний захист від загроз.

До антивірусного програмного забезпечення відносять спеціалізоване програмне забезпечення, що надає можливість виявляти, нейтралізувати та видаляти комп'ютерні віруси. Програми виявляють і блокують загрози у режимі реального часу.

Найважливіший метод виявлення загроз базується на основі підписів. Підписом загрози у даному випадку є унікальні цифрові ідентифікатори файлів, які є спеціальним набором байтів і отримуються на основі вмісту файлу, що перевіряється. Він може використовуватися для ідентифікації конкретного файлу чи програми.

Антивірусна програма перевіряє файли, що зберігаються в системі та завантажуються з Інтернету та порівнює результати дослідження з підписами, зареєстрованими в базі антивірусних програм. Якщо підпис збігається з раніше зареєстрованим вірусом, файл вважається зловмисним.

Антивірус додатково може містити наступні компоненти:

1. Знешкодження вірусів, хробаків, троянський програм, шпіонських програм;
2. Мережевий екран;
3. Захист користувача у веб-просторі, унеможливлюючи отримання доступу до потенційно небезпечних ресурсів, що розповсюджують шкідливе програмне забезпечення, фішинг та шахрайські сайти;
4. Захист електронної пошти від фішинг атак методом сканування вкладень у листи;
5. Забезпечують цілісність даних;
6. Запобігають небезпечним операціям програм.

Для забезпечення максимального захисту системи необхідно купувати ліцензовані антивірусні продукти, розроблені для бізнесу. Серед лідерів на ринку можна віиділити пропозиції від компаній Eset, McAfee та Norton.

Антивірусний захист встановлюється на всі складові інформаційної системи, які відповідають за обробку, збереження та транспортування файлів. До таких об'єктів відносять:

1. сервери;
2. робочі станції;
3. персональні комп'ютери мобільних працівників;
4. мобільні телефони працівників організації

Міжмережеві екрани

Міжмережеві екрани використовують для контролю вхідного та вихідного мережевого трафіку в середині локальної мережі та при виході в Інтернет. Він виступає фільтром, що контролює потік інформації між локальним комп’ютером та Інтернетом, є бар’єром безпеки між комп’ютером та іншим інформаційним простором;

Метою контролю є фільтрування і блокування небажаного трафіку та розподілення його на легітимний та потенційно небезпечний. Він перевіряє адреси джерела та призначення кожного інформаційного пакета, який передається та отримується на комп'ютер.

Мережеві фаєрволи розміщуються на шлюзах в Інтернет та на відокремлених сегментах локальної мережі. Фаєрвол може бути встановлений у форматі програми на робочу станцію локальної або може бути у програмно-апаратному вигляді. Додатково міжмережеві екрани можуть виступати в якості сервера VPN або DHCP.

Системи виявлення та запобігання вторгненям

Системи виявлення та запобігання вторгненням є ключовим елементом захисту корпоративних мереж. Вони аналізують мережевий трафік, виявляють ознаки неавторизованого доступу до локальної мережі та запобігають проведенню подальшої атаки. Для протидії загрозі, система виявлення та запобігання вторгненням здатна змінити налаштування фаерволу та заблокувати доступ до даних. Про можливі порушення мережевої безпеки та загрозу атаки система інформує фахівців з кібербезпеки банку.

Система може забезпечувати захист конкретних вузлів локальної мережі або цілого її сегменту. Основний принцип роботи полягає у виявленні та блокуванні атак та корпоративну мережу на основі аналізу пакетів даних, що циркулюють в цій мережі та виявленні аномалій мережевого трафіку. Система

дозволяє ефективно виявляти та блокувати атаки з боку зовнішніх та внутрішніх порушників.

Системи контролю та управління обліковими записами

Системи контролю та управління обліковими записами є головною вимогою при побудові розподіленої інформаційної мережі, де кожному користувачу надано привілеї відповідно до його посадових повноважень. Вона здійснює централізоване управління обліковими записами користувачів та адміністраторів.

Кожному працівнику установи необхідно виділити окремий обліковий запис користувача та надати права доступу до ресурсів системи відповідно до його повноважень. Обліковий запис складається верифікується за допомогою імені користувача та паролю. Кожен користувач відноситься до певної групи користувачів.

Системи запобігання витоків даних

Засоби запобігання витоків даних використовуються для захисту від несанкціонованої передачі конфіденційної інформації. Такі системи забороняють копіювати інформацію на змінний зовнішній накопичувач або відправляти файли за допомогою пошти.

До основних способів аналізу інформації відносять фільтрацію контенту (перевірка змістового наповнення документу з використанням заздалегіть підготовлених фраз) та контекстну фільтрацію (перевірка контексту, в якому передається інформація).

Антиспам

Антиспам- програмний модуль, що встановлюється на поштовий сервер з метою сканування вхідних повідомлень на наявність загроз та блокування листів, що викликають підозру. До основних загроз, що можуть передаватися поштою

відносять фішинг листи, які уражені зловмисним кодом та посилання на веб-сайти зловмисників.

Для фільтрації вхідних повідомлень, антиспам система виконує оцінку повідомлень відповідно до “чорних” та “білих” списків, ключових слів та адресним спискам. Якщо користувач оцінює повідомлення як спам, система надалі не буде пропускати повідомлення від даного відправника та автоматично помічатиме їх як спам.

Засоби захисту від D/DoS-атак

Захист від атак на відмову реалізовується для запобігання хакерським атакам на веб-сервер. До основної небезпеки від D/DoS-атак выдносять можливий витік конфіденційної інформації про співробітників або клієнтів банку та припинення функціонування об’єкта атаки.

Захист від даного типу атак реалізовується впровадженням додаткового бар’єру на зовнішньому кордоні локальної мережі з використанням спеціального ПЗ.

Засоби захисту від експлойтів

За допомогою наявних експлойтів в програмному забезпеченні, яке встановлене на робочій станції працівника, зловмисник може непомітно отримати доступ до комп'ютера користувача.

Модуль захисту від експлойтів стежить за поведінкою процесів, що виконує системне та програмне забезпечення, наприклад веб-браузери, поштові клієнти, компоненти Microsoft Offive та інші додатки. Виконання даними додатками підозрілих дій може свідчити про наявність експлойту. При виявленні підозрілого процесу, модуль зупиняє виконання програми та реєструє дані про наявну загрозу.

Сканери вразливостей

Сканери вразливостей дозволяють проводити сканування локальної мережі з метою діагностики комп'ютерів та програмних додатків з метою виявлення наявних в них уразливостей. Під час сканування програма виявляє наявні хости в мережі, проводить сканування всіх відкритих портів, проводить сканування додатків та операційної системи, та визначає рівень загрози для них. За проведеним скануванням программа створює звіт, завдяки якому працівник, відповідальний за забезпечення безпеки локальної мережі, моє усунути наявні загрози.

Засоби управління портативними пристроями

До засобів управління портативними пристроями входять програмні додатки для мобільних пристроїв, які надають змогу надійно захистити телефон користувача при роботі з корпоративними даними.

Як правило дані програмні засоби складаються з клієнтського програмного забезпечення та контрольного центру. Це надає змогу шифрувати конфіденційну інформацію на мобільному пристрої, а за необхідности надає змогу дистанційно видалити інформацію, наприклад у разі втрати пристрою. Додатково програмні засоби управління портативними пристроями додатково мають функції антивірусного захисту.

2.3 Аналіз способів несанкціонованого доступу до локальної обчислювальної мережі

Види загроз інформаційній безпеці

Для оцінки інформаційної безпеки та вразливих місць інформаційної системи розглянемо можливі способи несанкціонованого доступу до інформаційних ресурсів.

Під несанкціонованим доступом до інформації мають на увазі такий доступ, що порушує правила використання інформаційних ресурсів комп'ютерної системи, встановлені для її користувачів.

Обчислювальні системи є територіально розподілені комп'ютерні мережі, які поєднують за допомогою каналів зв'язку різні комп'ютери і локальні мережі. Вразливість таких систем істотно перевищує вразливість автономних комп'ютерів. Відповідно існує чимало способів атак на комп'ютерні мережі.

Усі можливі способи несанкціонованого доступу до інформації в комп'ютерних системах, що захищаються, можна класифікувати за такими ознаками: [10]

За принципом несанкціонованого доступу: фізичний несанкціонований доступ, логічний несанкціонований доступ.

1. Фізичний несанкціонований доступ - подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів.
2. Логічний несанкціонований доступ - логічне подолання системи захисту ресурсів активної комп'ютерної мережі.

За розташуванням джерела несанкціонованого доступу:

1. несанкціонований доступ, джерело якого розташоване у локальній мережі,
2. несанкціонований доступ, джерело якого розташоване поза локальною мережею.

За безпосереднім місцем розташування кінцевого об'єкта атаки:

1. на інформацію, що зберігається на зовнішніх запам'ятовуючих пристроях,
2. на інформацію, передану по лініях зв'язку,
3. атаки на інформацію, оброблювану в основній пам'яті комп'ютера.

Визначення загроз для локальної мережі

Локальна мережа міцно захищена від зовнішнього вторгнення апаратними міжмережевими екранами (Рис.2.2.). Банки приділяють достатньо багато уваги захисту свого мережевого периметра, тому організувати атаку на сервери або

веб-додатки не тільки складно, але й ризиковано, оскільки велика ймовірність виявити себе.

Розподіл мережі на сегменти є обов'язковою вимогою при побудуванні локальної мережі банківської установи. Обмеження доступу між сегментами мережі відбувається на фізичному та логічному рівні з використанням міжмережевих екранів.

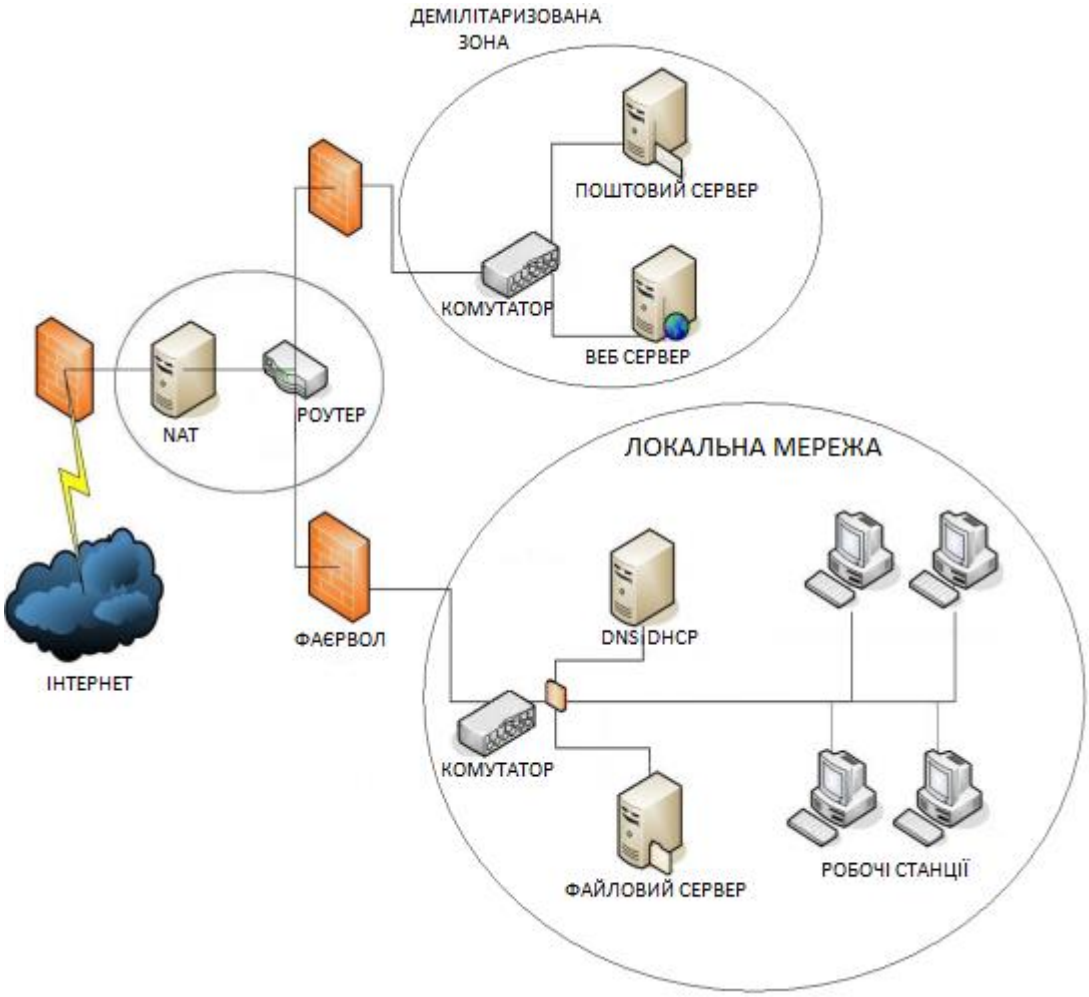

Рис. 2.2. Топологія локальної мережі

Обмін інформацією між філіалами та центральним офісом організоване з використанням безпечного VPN з'єднання. За розмежування мережі банку від публічної мережі та безпеку внутрішнього периметру відповідає апаратний засіб

захисту- міжмережевий екран, який є обов’язковою вимогою при проектуванні локальної мережі банківської установи.

На даний момент дієвим методом захоплення контролю над локальною мережею банку є інфікування однієї з її складових частин шкідливим програмним забезпеченням.

Найбільш вразливими до хакерської атаки є робочі станції працівників компанії.

Загрози для локальної мережі, які здатні спричинити робочі станції

Ураження робочих станції в локальній мережі- один з основних шляхів хакерської атаки на локальну мережу організації. Порушення безпеки внутрішнього периметру мережі може бути завдана працівником навмисно або без злочинного умислу, в результаті неосвіченості.

До ненавмисного ураження робочої станції можна віднести спам лист, який працівник отримав на корпоративну пошту. Як правило даним методом хакери користуються найчастіше, оскільки їм не потрібно ретельно досліджувати зовнішній периметр локальної мережі. Створивши переконливий змістовний лист, переважно з надзвичайно важливою робочою інформацією та додавши в нього вкладення з додаванням шкідливого програмного забезпечення, зловмиснику необхідно лише дочекатися поки співробітник відкриє вкладення та запустить в локальну мережу вірус або мережевого хробака. Іншим варіантом ураження мережі є підключення змінного носія інформації, на якому перебуває шкідливе програмне забезпечення до робочої станції.

Однак завжди існує можливість навмисного ураження недобросовісним співробітником мережі за допомогою шкідливого ПЗ, яке може бути встановлене з використанням змінного носія інформації.

Загрози для локальної мережі, які здатні спричинити співробітники використовуючи свою персональну техніку

Захист ноутбуків, домашніх персональних комп'ютерів та мобільних телефонів є надзвичайно важливим кроком. Непоодинокі випадки, коли керівник певного департаменту організації відлітає у відрядження на конференцію в інше місто або країну. Підключившись до мережі WI-FI в готелі, працівник уразив свій ноутбук чи телефон вірусом. Повернувшись в офіс та підключившись до локальної мережі компанії, працівник без злих намірів сам того не підозрюючи інфікував організацію небезпечним хакерським ПЗ.

Загрози для локальної мережі, які здатні спричинити сервери організації

Відокремлення серверів у окремий сегмент та їх захист окремим апаратним фаєрволом є обов'язковою вимогою при проектуванні локальної мережі банківської установи.

На всі сервери обов'язково встановлюється антивірусний захист, а для поштового серверу додатковим засобом захисту є антиспам фільтр.

Ураження серверу шкідливим програмним забезпеченням з боку внутрішнього периметру мережі, тобто робочих станцій працівників, може призвести до ураження всієї корпоративної мережі організації, оскільки інформація що зберігається на серверах переважно використовується всіма філіалами організації.

2.4 Визначення недоліків захисту локальної мережі

Система забезпечення безпеки локальної мережі є комплексом програмних та апаратних засобів захисту. До її складу входять багато компонентів: міжмережеві екрани, які розділяють локальну мережі від глобальної та захищають окремі сегменти мережі (сегмент робочих станцій працівників та сегмент серверів), антивірусні програмні засоби, що встановлені на кожному комп'ютері (серверах всіх типів та робочих станціях), системи виявлення та запобігання вторгненням та інші системи. Кожна з систем відіграє відповідну важливу роль у комплесному захисті мережі.

Після проведення Національним банком України у 2017 році аналізу методів ураження систем комерційних банків вірусом “Petya”, головними причинами, що призвели до пошкодження інформаційної та комп’ютерної мережі банків, було віднесено формальне ставлення до організації системи управління інформаційною безпекою, та формальне виконання вимог Національного банку в цій сфері. [11]

У 2019 році компанією Positive Technologies були проведення дослідження захищеності локальних мереж ряду установ фінансового сектору бізнесу. Відповідно до отриманих результатів, зловмисникам необхідно в середньому п’ять днів для захоплення повного контролю над локальною мережею. До того ж в ряді установ на багатьох засобах захисту мережевого периметру були помічені сліди попередніх атак. Це свідчить про те, що локальна мережа банку була скоспроментована злочинцем, однак виявити факт вторгнення не вдалося. [12]

Мінімально необхідні програмні та апаратні засоби захисту нажаль не гарантують стовідсотковий захист локальної мережі. Антивірусні програмні засоби не здатні виявити ряд сучасних шкідливих програмних засобів. Під час аналізу файлів на наявність шкідливого ПЗ, антивіруси переважно звіряються зі своїми базами сигнатур для порівняння необхідного файлу з наявними в базах записами. Шкідливе програмне забезпечення, створене для цільової атаки на банк створене з особливою прискіпливістю, відповідно розпізнати його як вірус система в деяких випадках не здатна.

Антиспам системи, встановлені на поштових серверах також не гарантують повний захист від поштових загроз. Система може не розпізнати файл заражений вірусом, або не перевірити посилання в поштовому лисні, перейшовши на яке працівник зможе натрапити на підробний сайт.

Вагомою загрозою для локальної мережі є можливість атак на вразливості нульового дня. Зловмисники невпинно шукають можливі дефекти в офісних програмних засобах. Підготуватися до такого типу атаки надхвичайно складно.

Єдиним засобом захисту в такому випадку є своєчасно виявити вторгнення в систему, а зробити це без спеціалізованих засобів захисту надзвичайно складно.

Кожен з компонентів захисту спрямований на виконання певних завдань, однак централізовано збирати, обробляти та зберігати інформацію з усіх систем в даному випадку неможливо. Системному адміністратору необхідно одночасно контролювати більше десятка різноманітних захисних систем, розміщених лише на одній робочій станції працівника. В окремих сегментах локальної мережі кількість робочих станцій та апаратних засобів захисту може варіюватись від одиниць до сотень машин, відповідно своєчасно виявити загрозу та вжити заходів щодо її нейтралізації буде фізично неможливо.

Кількість цільових атак на банківську сферу невпинно зростає. Хакери постійно удосконалюють засоби і методи проникнення у локальну мережу, отже фахівцям необхідно реагувати на інциденти інформаційної безпеки дуже швидко та прицільно. Необхідно постійно проводити оцінку роботи системи та оперативно виявляти відхилення в ній. Для автоматизації даного процесу та покращення результатів оцінки, в провідних компаніях активно впроваджуються системи поведінкового аналізу.

Виявити атаку при використанні мінімального необхідного комплексу програмних та апаратних засобі захисту системи досить складно. Однак після виявлення факту порушення безпеки локальної мережі, оперативно протидіяти загрозі без впровадження додаткових програмних засобів захисту надзвичайно складно. Відсутність системи автоматизації реагування на інциденти інформаційної безпеки призводить до занадто довгої реакції аналітика безпеки банку, адже він повинен відповідно до регламенту реагування на порушення захищеності локальної мережі зібрати велику кількість допоміжної інформації про атакований вузол мережі, ідентифікатор серверу, зв'язатись з керівництвом та отримати додаткову інформацію та інструкції. Без впровадження системи автоматизації реагування на інциденти інформаційної безпеки, на рутинну роботу буде витрачено надзвичайно багато часу, а при сценарії хакерської атаки на інформаційний сервер банку, кожна хвилина яку зловмисник провів у

корпоративній мережі може коштувати установі багатомільйонних фінансових збитків, втрати або оприлюднення конфіденційної інформації стосовно клієнтів банку та завдати значної репутаційної шкоди.

Підсумовуючи, наявна система захисту має ряд недоліків:

1. Шкідливе програмне забезпечення, яке не вдалося виявити антивірусу;
2. Вразливості нульового дня;
3. Неправомірні дії користувачів;
4. Відсутність загального контролю над всією системою;
5. Низька швидкість реагування на інциденти інформаційної безпеки;
6. “Людський фактор” при ліквідуванні інцидентів інформаційної безпеки;

Нажаль, згідно з проведеним у 2017 році компанією VMware дослідженням, лише 25% банків та страхових компаній на території СНД використовують цифрові інновації разом з відповідними засобами кібербезпеки, а 44% з опитаних організацій обмежується лише загальними засобами захисту інфраструктури. [13]

Висновки до другого розділу

Корпоративна мережа банківської установи переважно має складну структуру, яка поєднує в собі від одного офісу до десятків, а в деяких випадких сотні офісів та філіалів.

Безпека корпоративної мережі банку на пряму залежить від безпеки кожної її локальної мережі. Отримавши доступ до локальної мережі філіалу організації, зловмисник зможе поширити шкідливе програмне забезпечення, наприклад хробаків, які за декілька днів зможуть повністю захопити корпоративну мережу та надати зловмиснику контроль над всіма ресурсами організації.

Зовнішній периметр локальної мережі міцно захищений за допомогою апаратних засобів захисту, до яких відносяться міжмережевий екран, що відокремлює локальну мережу від глобальної незахищеної мережі Інтернет, та

система виявлення та запобігання вторгненням, яка реєструє та блокує всі несанкціоновані підключення з глобальної мережі до локальної.

Під час аналізу захищеності системи за допомогою мінімально необхідного рівня програмних та апаратних засобів захисту, було визначено ряд питань, що залишаються невирішеними. До основних недоліків системи можна віднести відсутність своєчасного виявлення факту вторгнення до локальної мережі, оскільки антивірусні та антиспам системи не гарантують стовідсотковий захист від шкідливого ПЗ.

Системи захисту мережі розподілені по всьому периметру, відсутність єдиної системи збору інформації може призвести до того, що факт компроментації системи може бути розпізнан занадто пізно, або не виявлений зовсім.

Без впровадження додаткових засобів аналізу поведінки користувачів або компонентів системи, розпізнати загрози на ранніх стадіях їх прояву спеціалістам навряд чи вдасться.

РОЗДІЛ 3: ВПРОВАДЖЕННЯ КОМПЛЕКСУ ДОДАТКОВИХ ПРОГРАМНИХ ЗАСОБІВ ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Система моніторингу та управління інформаційною безпекою SIEM

Загальні відомості

Існують два принципово різні за реалізацією підходи для забезпечення безпеки локальної мережі - превентивний та детективний.

Превентивний підхід спрямований на недопущення порушення стану інформаційної безпеки активу, тобто ймовірні загрози присікаються в момент їх виявлення. Яскравим прикладом превентивного підходу є блокування антивірусом інфікованого файлу або відхилення мережевим екраном спроби несанкціонованого підключення до локальної мережі ззовні.

Іншим підходом є детективний підхід. Метою даного підходу є збір інформації про певні події або дії для подальшого оцінення їх легітимності. Зібрані дані про події відправляються фахівцям з інформаційної безпеки для тподальшого прийняття рішення.

До захисту периметра локальної мережі наразі приділяється надзвичайно багато уваги. Фінансові установи впроваджують різноманітні програмні та апаратні засоби для захисту як від зовнішніх порушників, так і від внутрішніх.

В другому розділі були описані основні засоби захисту локальної мережі, впровадження яких вимагає Національний банк України. До них відносять наступні компоненти:

1. Антивірусні програмні засоби;
2. Захист та сегментування мережі за допомогою міжмережевих екранів;
3. Системи виявлення та запобігання вторгненням;

4. Системи контролю та управління обліковими записами;
5. Системи запобігання витоків даних;
6. Програмний захист поштових серверів за допомогою антиспам систем;
7. Засоби захисту від експлойтів;
8. Сканери вразливостей локальної мережі.

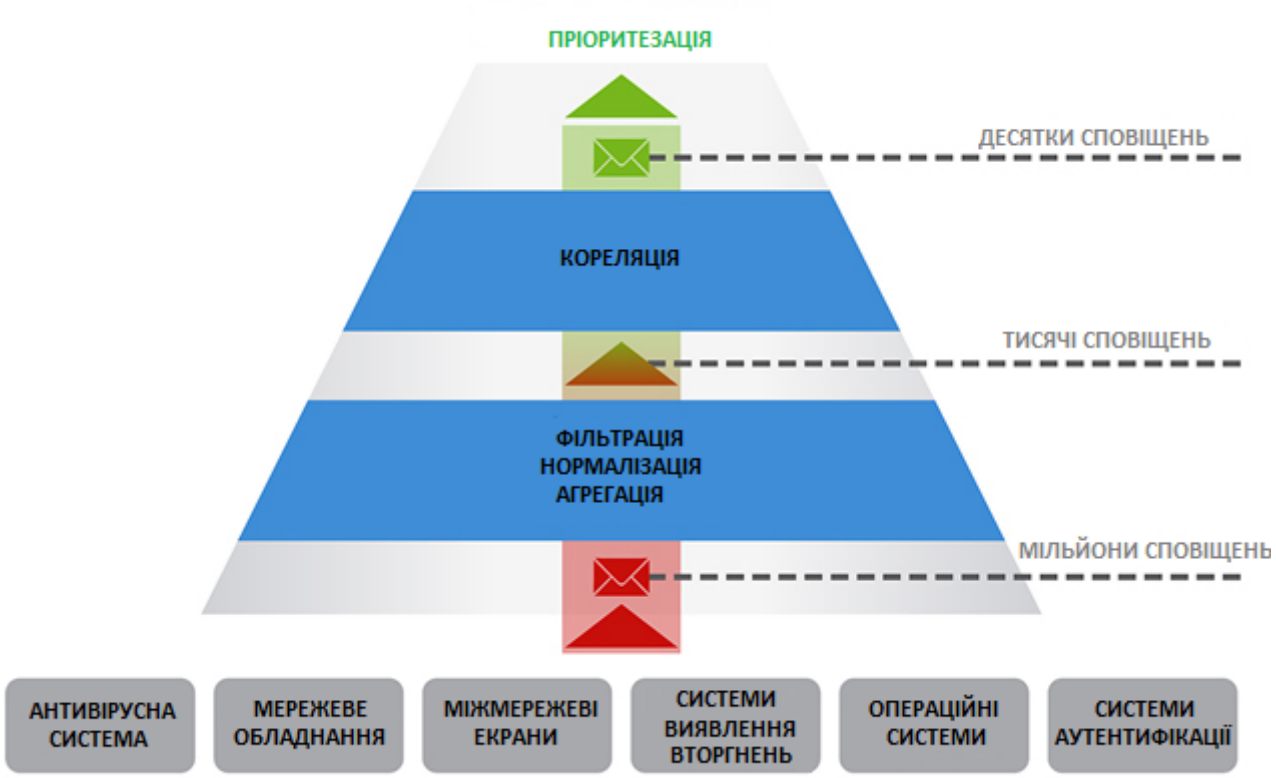

Рис. 3.1. Структура системи SIEM

Контролювати кожен з перелічених засобів та оцінювати захищеність локальної мережі у режимі реального часу без впровадження додаткових програмних засобів систематизації даних - не легке завдання для спеціалістів з інформаційної безпеки банку, адже на контроль десятків мережевих вузлів, сотень робочих станцій та серверів різного призначення за допомогою різних програм для моніторингу необхідно надзвичайно великий штат співробітників,

але всерівно їх робота не зможе бути цілком скоординованою а реакція на інциденти інформаційної безпеки не зможе бути своєчасною та повною.

Своєчасне виявлення відхилень в роботі елементів локальної мережі є запорукою оперативного усунення інформаційного інциденту та недопущення подібних інцидентів в майбутньому.

З метою одночасного отримання та об'єднання інформації з усіх компонентів локальної мережі в одному ресурсі була створена система моніторингу та управління інформаційною безпекою- SIEM.

Система SIEM виконує збір, обробку та аналіз інформації з усіх мережевих пристроїв, програмних засобів захисту мережі та апаратних пристроїв безпеки. На базі обровленої інформації створюються звіти, які наглядно демонструють аналітикам з інформаційної безпеки банку інформацію про актуальний стан локальної мережі (Рис. 3.1.).

Принцип роботи та основні функції

Першочерговим завданням системи моніторингу та управління інформаційною безпекою є збір інформації від усіх компонентів локальної мережі. Деякі компоненти здатні передавати дані до SIEM-системи самостійно, вказати їм мережеву адресу серверу збору даних SIEM, однак до частини засобів захисту система звертається самостійно. Зібравши всю інформацію від джерела, SIEM-система обробляє та перетворює її в зрозумілий для спеціалістів форамат, використовуючи наглядну статистику роботи в даний момент часу. Даний процес називається нормалізацією інформації.

Наступним кроком система SIEM виконує таксономію- класифікує попередньо нормалізовані повідомлення в залежності від їх змісту. Система надає інформацію про безліч подій, які мають привернути увагу працівників забезпечення безпеки банку. До таких подій відносять надання інформації щодо аутентифікація користувача на робочій станції або спрацьовування

антивірусного захисту на певному компоненті компоненті комп'ютеної мережі, тощо.

Отримана інформація стосовно функціонування компонентів мережі перетворюється у структуровану послідовність подій з вказанням змісту та часу настання. Дана форма відображення інформації надає можливість зрозуміти порядок натсння події і як вони можуть бути пов'язані між собою.

Головною перевагою SIEM-системи є механізм кореляції даних. Кореляцією називають співвідношення подій, які відповідають певним умовам-правилам кореляції.

До яскравих прикладів правила кореляції можна віднести ситуацію, коли на декількох робочих станціях в межах однієї локальної мережі протягом короткого проміжку часу спрацювало антивірусне попередження. Дана подія може свідчити про вірусну атаку на компанію.

Результатом спрацьовування правил кореляції в SIEM-системі є формування інциденту інформаційної безпеки. Фахівець додатково має можливість швидко знайти інформацію щодо подібних інцидентів в минулому, адже система зберігає дані протягом тривалого проміжку часу. Аналіз додаткової інформації та подробиць попередніх інцидентів надасть повну картину щодо склавшоїся ситуації.

SIEM система здатна виконувати багато функцій, серед яких:

1. Контроль аутентифікації користувачів та адміністраторів в системі;
2. Виявлення компрометації облікових записів користувачів;
3. Виявлення випадків ураження системи шкідливим програмним забезпеченням;
4. Контроль вхідного та вихідного трафіку;
5. Виявлення неправомірного доступу до інформації;
6. Виявлення несанкціонованих зовнішніх з'єднань до локальної мережі;
7. Контроль та порівняння відповідності політиці безпеки адміністративних дій у внутрішніх системах;
8. Контроль та фіксування змін у системі;

9. Фіксування атак на веб-додатки завдяки контролю журналів веб-сервера, логів програм та їх наслідків;
10. Виявлення спроб компрометації веб-додатків за допомогою аналізу попередніх звітів та поточного стану системи.

До основних завдань системи відносять:

1. Отримання інформації з різноманітних засобів захисту;
2. Нормалізація отриманих даних;
3. Кореляція класифікованих подій;
4. Створення інциденту, надання інструментів для проведення розслідування;
5. Зберігання інформації про події та інциденти протягом тривалого часу (від 6 місяців);
6. Швидкий пошук по даними, що зберігаються в SIEM.

Функціонал SIEM-системи може бути розширено додатковими компонентами, серед яких можливість управління ризиками та уразливими, побудова звітів та діаграм, тощо.

Система зручно налаштовується під кожну локальну мережу та спроектовану систему безпеки. Якісно сформовані правила кореляції дозволяють представляти інформацію в звітах за зниженням пріоритету- від найбільш критичних загроз системі до менш значущих.

Реалізація SIEM системи

Зрозуміло, при впровадженні та налагодженню SIEM-систем існують очевидні труднощі як організаційного, так і технічного характеру: крім покупки самої SIEM-системи доведеться ще налаштувати всі джерела даних на відправку даних в SIEM, створювати правила кореляції, усувати причини хибнопозитивних спрацьовувань, підтримувати SIEM- систему в актуальному стані, оперативно розслідувати інциденти інформаційної безпеки, згенеровані SIEM.

З лідерів світового ринку SIEM можна виділити наступних виробників програмного забезпечення: HP ArcSight, IBM QRadar, Tibco Loglogic, McAfee NitroSecurity.

3.2 Система поведінкового аналізу UEBA

Загальні відомості

Щорічно невпинно зростає кількість цільових атак на банківські установи. Хакери удосконалюють свої навички та планують все більш продумані та витончені методи проникнення до локальних мереж. Наразі шкідливе програмне забезпечення здатне маскуватися в системі та успішно долати всі наявні прогрмні та апаратні засоби захисту локальної мережі. До того ж зловмисником може виявитися співробітник банку, який володіє певною інформацією стосовно архутектури та систем захисту банківської системи.

Навіть якщо засоби захисту мережі не виявляють загроз, не потрібно вважати що система знаходиться в безпеці. Отже перед спеціалістами із захисту інформації в банківській установі постає майже нездійсненне завдання- відбити хакерську атаку за умови що немає жодного сповіщення щодо наявності загрози.

Однак, вявлення замаскованих атак на локальну мережу за умови відсутності явних сигналів загрози здатна виявити система поведінкового аналізу.

UEBA – іноваційний програмний комплекс, який зарекомендував себе з найкращого боку. Дані системи використовують принципово новий підхід в боротьбі з сучасними загрозами, завдяки чому привернули до себе увагу в провідних компаніях по всьому світу та отримали найвищі оцінки серед експертів.

Системи поведінкового аналізу створили принципово новий клас систем, які дозволяють за допомогою алгоритмів статистичного аналізу та машинного навчання створювати моделі поведінки користувачів та в режимі реального часу визначати відхилення від цих моделей.

Принцип роботи та основні функції

Системи UEBA здатні ідентифікувати широкий спектр загроз, джерелами яких можуть виступати не лише користувачі, а й об'єкти IT-інфраструктури.

Для проведення ефективної роботи, система UEBA отримує та аналізує інформацію з журналів серверів, програмних та апаратних систем безпеки, компонентів мережі, систем аутентифікації, проводить аналіз поштових повідомленнь та інших джерел.

Отриману інформацію про користувачів, система поведінкового аналізу збагачує інформацією про мережеве оточення, наявні хости, програмні додатки, аналізуючи мережевий трафік.

Широкий спектр оброблюваних джерел дозволяє системі будувати профілі не лише користувачів, а й всього мережевого оточення.

Система поведінкового аналізу може вирішити декілька основних завдань:

1. Статистична та розширена використанням методів машинного навчання аналітика даних з різних джерел;

2. Ідентифікація атак та порушень безпеки, більшість з яких не можливо визначити класичними засобами захисту локальної мережі;

3. Пріоритизація подій, отриманих з системи моніторингу та управління інформаційною безпекою SIEM, для оперативного реагування на загрозу інформаційній безпеці;

4. Ефективна реакція на події за рахунок надання розширеної інформації стосовно інциденту (інформація про залучені в аномальну активність об'єкти, тощо).

Відповідно до масиву зібраних даних, система поведінкового аналізу створює модель нормальної поведінки користувача та його взаємодії з корпоративними системами. Модель поведінки створюється за допомогою простих статистичних алгоритмів та алгоритмів машинного навчання. Присутня можливість створення моделі поведінки одночасно цілих груп користувачів та аналіз відхилення від загальної моделі кожної з них.

Якщо дії користувача відрізняються від моделі його звичайної поведінки, система визначає це як аномальну активність та створює в режимі реального часу попередження адміністратору безпеки.

На основі зібраних даних про аномальну активність користувачів, системи UEBA здатні виставляти оцінки ризику кожному користувачеві за допомогою використання ретроспективної статисти

3.3 Система автоматизації реагування на інциденти інформаційної безпеки IRP

Загальні відомості

На сьогоднішній день кількість інцидентів інформаційної безпеки у великих компаніях досить велика, а часу на реагування у спеціалістів відділу забезпечення інформаційної безпеки дуже мало. Кожна хвалина, що йде на усунення загрози може коштувати банку значних збитків. Не кожна компанія спроможна найняти великий штат фахівців, тому гостро постає питання автоматизації реагування на інформаційні інциденти.

Уявімо ситуацію, коли система моніторингу та управління інформаційною безпекою показує на те, що відбувається атака на локальну мережу. Зловмисники можуть отримати доступ до банківської таємниці або викрасти гроші з рахунків клієнтів. Аналітик із забезпечення безпеки, відповідно до протоколу реагування на інцидент має зібрати та проаналізувати велику кількість допоміжної інформації: який сегмент мережі був атакований, які дії наразі проводить зловмисник в мережі та багато інших операцій. За результатами оцінки становища необхідно сповістити керівника відділу та отримати додаткові інструкції. Аналітик має якомога швидше ізолювати атакований сегмент мережі від загальної мережі та заблокувати скомпрометований обліковий запис.

На виконання вищеперелічених дій буде витрачено занадто багато часу, хоча сучасні програмні рішення здатні автоматично виконати всі рутинні операції та звести роботу аналітика до мінімуму.

Саме таким рішенням є система автоматизації реагування на інциденти інформаційної безпеки. Дана система виконує ряд рутинних операцій по збору додаткової інформації, здійсненню невідкладних дій щодо стримання зловмисника та усунення загрози, відновити атаковану систему та зібрати і структурувати дані про інцидент для подальшого розслідування. IRP система здатна автоматизувати дії фахівця з забезпечення інформаційної безпеки, які він виконує вручну при реагуванні на інциденти інформаційної безпеки.

Принцип роботи та основні функції

IRP-система виконує завдання з реагування на інциденти інформаційної безпеки, що складаються з декількох процесів, пов'язаних між собою. До них відносять наступні етапи:

1. Підготовка;
2. Детектування;
3. Аналіз;
4. Локалізація;
5. Усунення;

6. Відновлення;
7. Пост-інцидентні дії.

1. Підготовка. Етап підготовки є першочерговим та одним з ключових. На даному етапі IRP платформу необхідно налаштувати для ефективного застосування. До неї підключаються інформаційні системи і засоби захисту локальної мережі, з якими система буде взаємодіяти під час реагування на інциденти. Підключаються системи, які надають інформацію про інцидент, а саме відомості про скомпроментований обліковий запис користувача, його посаду, структурний підрозділ організації та надані йому повноваження. Дана інформація необхідна для розуміння того, до яких даних зловмисник може отримати доступ. Система також збирає інформацію стосовно пристрою, тип його операційної системи, наявне програмне забезпечення, тощо.

Крім цього, до IRP платформи підключаються засоби захисту, які під час реагування на інцидент будуть виконувати функції стримування зловмисника та усунення загроз. Серед них засоби захисту кінцевих точок, міжмережеві екрани, тощо.

На етапі підготовки налаштовуються сценарії реагування на інфораційний інцидент, відповідно до яких система автоматизації реагування на інциденти інформаційної безпеки буде виконувати заздалегідь задані їй дії.

2. Детектування. На етапі детектування строрюються списки типів можливих інцидентів інформаційної безпеки та формується перелік їх ознак. Дані ознаки умовно розділяються на прекурсори та індикатори інцидентів інформаційної безпеки. Прекурсором називають ознаку того, що інцидент може статися в майбутньому, а індикатором є ознака того, що інцидент вже стався або відбувається прямо зараз.

До яскравих прикладів прекурсорів інциденту належать такі події, як зафіксоване системою інтернет-сканування відкритих портів або виявлення уразливості в якийсь інформаційній системі. До індикаторів інциденту інформаційної безпеки входять поява сповіщень про можливу атаку від засобів захисту локальної мережі- антивірусів, брендмауерів, тощо.

Для максимально ефективної роботи системи автоматизації реагування на інциденти інформаційної безпеки на йьому етапі її необхідно інтегруавти з SIEM-системою. Саме така комбінація програмних засобів здатна забезпечити швидку та ефективну передачу прекурсорів та індикаторів від інформаційної системи і засобів захисту локальної мережі через систему SIEM безпосередньо в IRP систему. Це дозволить системі оперативно виявляти інциденти і вживати відповідних заходів для реагування на них.

3. Аналіз. Під час аналізу інциденту основну роботу виконує аналітик, адже саме людині необхідно прийняти остаточне рішення про те, чи вважати інцидент інформаційної безпеки реальною загрозою, або дане спрацювання системи безпеки є хибним.

Саме на етані аналізу система IRP надає аналітику контекстну інформацію стосовно інциденту для прийняття ним остаточного рішення. Прикладом такого інциденті може бути повідомлення від антивірусної системи про виявлення загрози на робочій станції. Скориставшись даними IRP системи аналітик виявляє аналогічну мережеву активність на декількох інших мережевих пристроях компанії, що може означати одночасте массове ураження системи. Аналітик присвоїть даному інциденту стсатус “критичний” та приступить до усунення загрози. На даному етані IRP система автоматизує заходи з ескалації інциденту та запротоколює всі дії, виконані в рамках реагування на даний інцидент для подальшого аналізу.

4. Локалізація. На етапі локалізації інциденту інформаційної безпеки головним завданням проведених заходів має бути мінімізація потенційних збитків від даної загрози та надання додаткового часу фахівцям для прийняття рішення щодо етапів усунення загрози.

Локалізувати інцидент можливо за допомогою декількох заходів. Присутня можливість ізолювати уражений хост від локальної мережі, повністю вимкнувши уражений пристрій або деактивувавши частину сервісів і функцій на ньому. Іншим варіантом локалізації може бути аетивація більш суворих заборонних правид на мережевому екрані.

Спеціалісту з забезпечення безпеки необхідно проаналізувати ситуацію та прийняти рішення щодо локалізації загрози. Необхідно визначити яку функцію виконує уражений актив та яку шкоду може завдати інцидент інформаційної безпеки. Відключення критично важливого для функціонування банку сервера може привести до більш вагомих негативних наслідків для компанії, ніж перезавантаження окремого некритичного сервісу на ньому. IRP система здатна проаналізувати створені ситуацію та надати для аналітика рекомендації стосовно його подальших дій.

На етапі підготовки IRP системи необхідно створити сценарії для її регування на інциденти конкретного типу. Наприклад у разі виявлення вірусного ураження всередині одного сегмента мережі не потрібно ізолювати пристрої в іншому сегменті.

Система здатна проаналізувати і надати звіт з подробиць атаки. Вона збирає інформацію про те в якому порядку були діяли зловмисники, за допомогою яких методів та яка саме ситема була атакована першою.

5. Усунення. На етапі усунення інциденту працівниками проводяться видалення загроз з локальної мережі та запобігання повторним атаки. З локалізованих систем видаляється шкідливе програмне забезпечення, встановлюються оновлення на системи, де були експлуатованих вразливостей в їх захисті, проводиться перенаслаштування програмних та апаратних засобів захисту.

Ретельне усунення вразливостей в захисті мережі є критично необхідним завданям, оскільки хакери здатні повторно проводити атаки на ті ж самі вразливості в системах, що були ними зламані раніше.

Система IRP збирає дані про оновлену конфігурацію системи та порівнює її з результатами, що були задані для системи захисту до проведення атаки. При впровадженні системи реагування на інциденти суттєво зростає швидкість усунення загроз для інформаційної безпеки.

6. Відновлення. На етапі відновлення фахівці перевіряють надійність та якість вжитих заходів захисту та повертають систему якнайшвидше в нормальну

роботу. Система IRP здатна допомогти фахівцям повторно перевірити на надійність раніше скомпроментровані злочинцями об'єкти локальної мережі.

7. Пост-інцидентні дії. Після усунення загрози для подальшої роботи мережі, експерти приступають до аналізу причин інциденту для мінімізації вірогідності проведення повторної атаки даного типу в майбутньому.

Проводиться оцінка діям IRP системи з метою можливого проведення коригувань та аналізується швидкість та якість роботи фахівців із забезпечення захисту інформації.

IRP система зберігає докладну інформацію про інциденти що відбулися в минулому та вжиті заходи реагування на загрозу та створює змістовні аналітичні звіти за результатами відбиття хакерської атаки.

До основних переваг системи відносять:

1. Зручну інтеграцію з системами захисту, як приклад системою SIEM;
2. Зручна інтеграція з інфраструктурою організації;
3. Автоматизоване реагування на інциденти інформаційної безпеки;
4. Адаптивність роботи;
5. Зручна візуалізація роботи та звітність

Результати впровадження системи автоматизації реагування на інциденти інформаційної безпеки (за даними розробників): [33]

- до 90% - зниження ймовірності поширення шкідливого ПЗ в межах локальної мережі при налаштованому автоматичному реагуванні на інциденти;
- до 90% - зниження ризику людського фактора і помилок персоналу, залученого в реагування на інформаційні інциденти;
- до 70% - вивільнення часу у персонала, залученого в реагування на інциденти інформаційної безпеки, перехід від рутинних операцій для більш експертних завдань.

3.4 Оцінка захищеності локальної мережі після впровадження додаткових програмних засобів захисту

Система моніторингу та управління інформаційною безпекою

Впровадження SIEM системи наразі є необхідністю для організацій, що мають розгалуджену корпоративну мережу. Гарантувати захищеність локальної мережі, не отримуючи єдиної чіткої картини щодо процесів які в ній відбуваються, наразі надзвичайно складно, а в деяких ситуаціях- неможливо.

Система моніторингу та управління інформаційною безпекою здатна швидко отримати та обробити великий поток даних від різних джерел, а також надати змістовний звіт щодо актуального стану локальної мережі. SIEM врази прискорює процес обробки та аналізу інцидентів інфораційної безпеки, оскільки аналітику не потрібно підключатися до кожного засобу захисту мережі- вся інформація надається в єдиному зручному інтерфейсі у консолідованому вигляді.

SIEM система відіграє ключову роль у протидії загрозам інформаційної безпеки, адже допомагає контролювати цілий ряд ключових завдань: виконує збір та аналіз іноформації з мережевих пристроїв, пристроїв безпеки та програмних додатків, включаючи антивірусне програмне забезпечення, систем запобігання вторгненням та брандмауерів.

Впровадження системи моніторингу та управління інформаційною безпекою позитивно позначиться на швидкості виявлення інцидентів інформаційної безпеки та своєчасного реагування на них.

Система поведінкового аналізу

Система поведінкового аналізу є надзвичайно потужним аналітичним інструментом, робота якої тісно пов'язана з SIEM-системою, адже для створення та контролю моделі поведінки UEBA системі необхідно постійно отримувати та обробляти великі об'єми даних, зібраних з різних джерел.

Наразі захист периметра та кінцевих станцій не гарантує достатній захист локальної мережі, оскільки як показує практика, зловмисники спроможні обійти такий захист не компроментуючи себе. UEBA-система відстежує активність, що викликають підозру, починаючи з ранньої стадії стадії ураження локальної мережі і закінчуючи кінцевими станціями та серверами.

Крім зовнішніх атак на локальну мережу, загрози можуть надходити від співробітників компанії. До таких загроз відносять виток даних, експлуатацію вразливостей в корпоративних системах для підвищення привілеїв, тощо. В цьому випадку система поведінкового аналізу здатна визначити аномальну активність в поведінці певного користувача та сповістити адміністраторів безпеки банку про несанкціоновану взаємодію користувача з корпоративними системами.

До того ж система UEBA здатна проводити моніторинг прав доступу співробітників до ресурсів мережі. Вона збирає інформацію про користувачів та їх привілеї та оцінює до яких корпоративних систем користувачі здійснюють доступ. За результатами аналізу певним користувачам можна знизити привілеї доступу до цільових систем, якщо вони не використовують повний список привілеїв у доступі до певних систем корпоративної мережі. Результатом зниження привілеїв є зниження ризики внутрішніх загроз локальної мережі.

Наразі інтерес до систем поведінкового аналізу збільшується з кожним роком. Вони можуть бути представлені окремими програмними засобами та у вигляді розширень до систем SIEM. До лідерів на ринку входять Microsoft Advanced Threat Analytics, HPE ArcSight, IBM QRadar.

Система реагування на інциденти кібербезпеки

У випадку атаки на локальну мережу банку, система реагування на інциденти кібербезпеки буде реагувати ключову роль у швидкості протидії злочинцям. Для банківської установи швидкість відбиття атаки відіграє ключову

роль, оскільки кожна зайва витрачена хвилина на ліквідацію загрози буде коштувати компанії не лише репутації, але й значних фінансових втрат.

Системи IRP дозволяє автоматизувати процеси та засобами реагування на інциденти інформаційної безпеки та проводити контрзаходи для протидії загрозам інформаційної безпеки згідно із заздалегідь заданими сценаріями реагування.

Сценаріями реагування є набір автоматизованих завдань з детектування загроз та аномалій в інфраструктурі, негайне реагування та стримування загроз в режимі реального часу. Сценарії реагування діють на підставі правил і типів інцидентів, виконуючи ті чи інші дії в залежності від даних, що надходять з засобів захисту або інформаційних систем. Платформи IRP допомагають проводити структуроване і журнальованою реагування на інциденти інформаційної безпеки на підставі правил і політик.

Система здатна на підставі аналізу атаки та її протидії створити звіт, який надалі може застосовуватися для редагуваття сценаріїв роботи.

Завдяки впровадженню система автоматизації реагування на інциденти інформаційної безпеки працівники департаменту інформаційної безпеки банку зможуть істотно заощадити зусилля на виконання рутинних завдань при протидії інцидентам інформаційної безпеки, що значно підвищить швидкість реагування та мінімізує втрати у разі проникнення зловмисників у локальну мережу.

Результат впровадження заходів

До основних складових локальної мережі можна віднести зовнішній периметр, внутрішній периметр, робочі станції, файлові сервери, поштові сервери. Захист кожного ж компонентів було посилено системою SIEM, яка збирає та обробляє інформацію з апаратних та програмних засобів захисту, характерних для даної системи.

Порівняння захищеності системи до та після впровадження додаткових заходів наведено в таблиці 3.2.

Вимоги	Захищеність системи за допомогою мінімально необхідних систем захисту	Захищеність системи після впровадження додаткових програмних засобів захисту
Захист зовнішнього периметра	Міжмережевий екран, система IDS, система IPS	Доповнено системами SIEM, UEBA, IRP
Захист внутрішнього периметра	Міжмережевий екран	Доповнено системами SIEM, UEBA, IRP
Захист робочих станцій	Антивірус, Антиспам	Доповнено системами SIEM, UEBA, IRP
Захист файлових серверів	Міжмережевий екран, Антивірус	Доповнено системами SIEM, UEBA, IRP
Захист поштових серверів	Міжмережевий екран, Антивірус, Антиспам	Доповнено системами SIEM; UEBA; IRP
Виявлення прихованих загроз	Не реалізовано	Реалізовано системами SIEM; UEBA
Єдина система збору даних від компонентів локальної мережі	Не реалізовано	Реалізовано системою SIEM
Єдиний контроль та фіксування змін в системі	Не реалізовано	Реалізовано системами SIEM, UEBA
Єдиний звіт щодо актуального стану захищеності системи	Не реалізовано	Реалізовано системою SIEM
Автоматизована локалізація та протидія загрозам	Не реалізовано	Реалізовано системою IRP

Таблиця 3.2. Порівняння захищеності системи до та після впровадження додаткових програмних засобів захисту

- не реалізовано
- частково реалізовано
-реалізовано в повній мірі

На основі отриманих даних, система поведінкового аналізу створює модель роботи системи. У випадку проведення дій, що не є характерними для звичайної роботи системи, система UEBA миттєво виявить факт компроментації мережі. Відповідно до попередньо налаштоварих протоколів безпеки, система IRP проведе локалізацю та ліквідацію загрози.

До впровадження систем SIEM та UEBA виявити факт наявності зловмисника або шкідливого ПЗ в системі, якщо антивірус не виявив загрозу було майже неможливо.

Єдиний контроль, фіксування змін та єдиний звіт щодо актуального стану системи став можливим після впровадження додаткового комплексу прорамних засобів захисті.

Результатом впровадження заходів є створення досконалої системи захисту локальної мережі з використанням найсучасніших рішень щодо аудиту всіх компонентів локальної мережі, попередженню та своєчасному виявленню несанкціонованого доступу до інформаційної системи банку, а в разі виникнення інфораційного інфиденту, система автоматично дасть відсіч порушнику.

Захист локальної мережі має бути комплексним підходом, із залученням найсучасніших рішень програмного та апаратного забезпечення та створенням актуальної політики інформаційної безпеки організації.

Висновки до третього розділу

Впровадження системи моніторингу та управління інформаційною безпекою є обов'язковим заходом при створенні комплексного програмно-апаратного захисту мережі. Адмініструвати кожну систему окремо надзвичайно складно, а в деяких випадках- неможливо. SIEM система дозволяє отримувати інформацію про стан компонентів локальної мережі в режимі реального часу, фіксувати та зберігати звіти з точними оцінками захищеності системи.

Система поведінкового аналізу може існувати як у вигляді окреммого програмного засобу, так і у формі розширення до системи SIEM. Аналіз системи комплексно та виокремлення сегментів мережі, де зафіксована не типова аномальна активність- неперевершена особливість сучасних систем, побудованих з використанням штучного інтелекту та машинного навчання.

Система автоматизації реагування на інциденти інформаційної безпеки значно спрощує експертам із забезпечення інформаційної базпеки банку реагувати на наявні інциденти, адже працівнику необхідно лише визначити, чи несе дана аномалія в системі загрозу для локальної мережі.

Впровадження даних заходів значно посилить заходи із забезпечення безпеки локальної мережі банківської установи та надасть можливість виявляти загрози та атаки на ранніх етапах, коли злочинець ще не встиг подолати зовнішній периметр локальної мережі.

ВИСНОВКИ

Дипломний проект було присвячено аналізу захищеності локальної мережі банківської установи та впровадженню додаткових програмних засобів захисту.

Під час виконання роботи було:

- розглянуто актуальні кіберзагрози для банківської сфери та визначино основні загрози для локальної мережі банківської установи;
- досліджено локальну мережу, захищену за допомогою засобів, регламентованих Національним банком України, та визначено наявні недоліки в її захисті;
- запропоновано додаткові програмні засоби захисту локальної мережі та оцінено їх позитивний вплив на підвищення рівня захищеність системи після їх впровадження.

Відповідно до проведених досліджень, лише четверта частина банків використовує іноваційні засоби кібербезпеки, а майже половина з опитаних фінансових організацій обмежується загальними засобами захисту своєї мережевої інфраструктури.

Нажаль, ця статистика підтверджується чисельними атаками на банківський сектор, що призводить до значних фінансових та репутаційних втрат, а в окремих випадках – до повного припинення існування банківської установи.

Формальне ставлення до вимог “Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України” Національного банку України та обмеження виключно основними програмними та апаратними засобами захисту є неприпустимим в умовах активно зростаючого рівня кіберзагроз банківському сектору.

Під час аналізу захищеності локальної мережі, що реалізована виключно за допомогою програмних та апаратних засобів захисту, що входять до переліку мінімально необхідних засобів захисту локальної мережі відповідно до постнови Національним банком України було визначено ряд недоліків в її захисті:

1. антивірус не здатен гарантувати повний захист системи від шкідливого ПЗ;
2. вразливості нульового дня не можливо виявити за допомогою програмних або апаратних засобів захисту;
3. неправомірні дії співробітників;
4. відсутність єдиного контролю над всією системою;
5. низька швидкість реагування на інциденти інформаційної безпеки;
6. можливість не повного ліквідуванні інцидентів інформаційної безпеки;

Було аргументовано доцільність впровадження у локальну мережу банківської установи додаткових програмних засобів захисту та контролю, а саме:

- системи моніторингу та управління інформаційною безпекою SIEM;

- системи поведінкового аналізу UEBA;

- системи автоматизації реагування на інциденти інформаційної безпеки IRP.

Комплексне впровадження даних засобів захисту надасть можливість контролювати в режимі реального часу функціонування всіх елементів локальній мережі організації, збирати та аналізувати дані стосовно всіх програмних та апаратних складових мережі, аналізувати поведінку систем та працівників організації та в разі виявлення відхилень від встановлених шаблонів їх поведінки оперативно сповістити департамент інформаційної безпеки банку про можливу кібератаку на локальну мережу.

При підтвердженні працівниками факту існування загрози для конфіденційності, доступності та цілісності інформації в локальній мережі, система автоматизації реагування на інциденти інформаційної безпеки миттєво

виконає визначені на випадок відповідного інциденту директиви та зробить все необхідне для ліквідації загрози та мінімізації втрат компанії. Це значно прискорить шкидкість реагування на інформаційний інфидент та виключить некоректні дії працівників, пов'язані з “людським фактором”.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вектори хакерських атак на банки - [Електронний ресурс] - Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/
2. Тестування на проникнення в організаціях кредитно-фінансового сектора - [Електронний ресурс] - Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/
3. New Global Cybersecurity Report Reveals Cybercrime Takes Almost $600 Billion Toll on Global Economy від 21.02.2018 [Електронний ресурс] - Режим доступу: https://www.mcafee.com/enterprise/ko-kr/about/newsroom/press-releases/press-release.html?news_id=51f0b839-200c-4c4e-8f35-d45dff11afb0
4. The Economic Impact of Cybercrime— No Slowing Down [Електронний ресурс] - Режим доступу: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
5. Кількість банків в Україні (2008-2021) [Електронний ресурс] - Режим доступу: https://index.minfin.com.ua/ua/banks/stat/count/
6. ст. 21 Закону України "Про інформацію" [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
7. ст. 60 Закону України "Про банки і банківську діяльність" [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/2121-14#Text
8. ст. 200 Цивільного кодексу України [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/435-15#Text
9. Постанова 28.09.2017 № 95 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
10. Аналіз актуальних способів та методів несанкціонованого доступу в сучасних інформаційно-комунікаційних системах та мережах [Електронний

ресурс] - Режим доступу: http://www.rusnauka.com/35_OINBG_2010/Informatica/76311.doc.htm

11. Як банкам захиститися від кібератак від 07.07.2017 [Електронний ресурс] - Режим доступу: http://finpost.com.ua/news/4021
12. Тестування на проникнення в організацію кредитно-фінансового сектора [Електронний ресурс] - Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/
13. Поединок з майбутнім. Як банк захищається від кіберугроз нового покоління [Електронний ресурс] - Режим доступу: https://www.forbes.ru/finansy-i-investicii/357609-poedinok-s-budushchim-kak-bankam-zashchititsya-ot-kiberugroz-novogo
14. Роль банківської системи в розвитку фінансового ринку україни [Електронний ресурс] - Режим доступу: https://essuir.sumdu.edu.ua/bitstream-download/123456789/53895/6/Bashlai_corporation.pdf1.pdf;jsessionid=A966DD7240B3A9B29926E7A10B33AC2A
15. Банківська система та її роль у ринковій інфраструктурі. Реферат [Електронний ресурс] - Режим доступу: https://osvita.ua/vnz/reports/bank/19682/
16. Системи виявлення та запобігання вторгнень [Електронний ресурс] - Режим доступу: http://itland.com.ua/solutions/network-security/intrusion-detection-prevention-systems/
17. Захист комп’ютерних мереж [Електронний ресурс] - Режим доступу: https://magistrweb.wordpress.com/home-2/protection/
18. Захист мереж банків від зовнішніх загроз [Електронний ресурс] - Режим доступу: https://www.osp.ru/winitpro/2009/09/10690275
19. Структура комп'ютерної мережі [Електронний ресурс] - Режим доступу: https://stud.com.ua/54447/informatika/struktura_kompyuternoyi_merezhi
20. Об'єднання локальних мереж офісів [Електронний ресурс] - Режим доступу: http://www.murava.ru/solutions/vpn/

21. Банки посилять власну інформаційну безпеку та співпрацю з протидії кіберзагрозам [Електронний ресурс] - Режим доступу: https://bank.gov.ua/ua/archive-news/all/51479152-banki-posilyat-vlasnu-informatsiynu-bezpeku-ta-spivpratsyu-z-protidiyi-kiberzagrozam
22. Програмні засоби захисту інформації [Електронний ресурс] - Режим доступу: https://mosgensovet.ru/office-programs/programmnye-sredstva-zashchity-informacii-primery-programmnye/
23. Що таке система SIEM? 16.10.2019 [Електронний ресурс] - Режим доступу: https://softlist.com.ua/articles/chto-takoe-siem-sistema/
24. SIEM-системи [Електронний ресурс] - Режим доступу: https://www.anti-malware.ru/security/siem
25. SIEM – Security Information and Event Management [Електронний ресурс] - Режим доступу: https://amica.ua/ru/siem-security-information-and-event-management/
26. Порівняння siem-систем [Електронний ресурс] - Режим доступу: https://searchinform.ru/products/siem/sravnenie-siem-sistem/
27. Огляд ринку систем поведінкового аналізу - User and Entity Behavioral Analytics (UBA / UEBA) [Електронний ресурс] - Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba
28. UEBA, або поведінкова аналітика. Базова функція всіх систем безпеки майбутнього [Електронний ресурс] - Режим доступу: http://itsec.ru/articles2/Inf_security/ueba--ili-povedencheskaya-analitika-bazovaya-funktsiya-vseh-sistem-bezopasnosti-buduschego
29. Аналіз поведінкі користувачів: модний тренд чи панацея? [Електронний ресурс] - Режим доступу: https://uk.conservationdatasystems.com/2970-analysis-of-user-behavior-a-fashion-trend-or-a-panac.html
30. Платформа реагування на інциденти IRP [Електронний ресурс] - Режим доступу: https://rvision.pro/blog-posts/irp-1/

31. R-Vision Incident Response Platform [Електронний ресурс] - Режим доступу: https://mte-cyber.by/services-and-solutions/platform-irp/

Теоретичні основи побудова та функціонування систем управління інцидентами інформаційної безпеки [Електронний ресурс] - Режим доступу: http://jrnl.nau.edu.ua/index.php/ZI/article/view/2073

33. Security Vision Incident Response Platform [Електронний ресурс] - Режим доступу: https://www.securityvision.ru/products/irp/