ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ЗАХИСТУ ЖИТТЄВОГО ЦИКЛУ ПРОДУКЦІЇ ВІД АТАК SUPPLY CHAIN»

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Гашніков Д.М.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
“___”_____ 2023 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Гашнікову Данилу Миколайовичу
(прізвище, ім’я, по батькові)

1. Тема бакалаврської роботи:
«Розробка рекомендацій по захисту життєвого циклу продукції від атак Supply Chain».

керівник бакалаврської роботи Гайдур Галина Іванівна, д.т.н., проф.
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24 » лютого 2023 року № 26.

2. Строк подання студентом бакалаврської роботи 28.05.2023 р.

3. Вихідні дані до бакалаврської роботи
аналіз потенційних загроз;
визначення рівня ризику для кожної ідентифікованої загрози;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність проблеми атак на ланцюг постачання.
2. Зміст процесу реагування атаку на ланцюг постачання.
3. Методи та засоби захисту від атак на ланцюг постачання.
4. Рекомендації щодо захисту від атак на ланцюг постачання

5. Перелік графічного матеріалу
1. Тема бакалаврської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу змісту процесу реагування на атаку на ланцюг постачання

4. Результати аналізу методів та засобів захисту від атак на ланцюг постачання

5. Призначення та можливості рішення проблем з ланцюгом постачання

6. Рекомендації щодо захисту від атак на ланцюг постачання

7. Висновки за результатами роботи.

6. Дата видачі завдання 15.02.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів бакалаврської роботи	Строк виконання етапів бакалаврської роботи	Примітка
1.	Визначення актуальності проблеми захисту життєвого циклу продукції від атак Supply Chain.	23.02.2023 р.	Вик.
2.	Аналіз наукової та технічної літератури з питань теми бакалаврської роботи.	8.02.2023 р.	Вик.
3.	Аналіз методів та засобів для захисту життєвого циклу продукції від атак Supply Chain.	19.03.2023 р.	Вик.
4.	Розроблення рекомендацій щодо застосування методів та засобів захисту життєвого циклу продукції від атак Supply Chain.	10.04.2023 р.	Вик.
5.	Оформлення результатів дослідження.	24.04.2023 р.	Вик.
6.	Підготовка доповіді до захисту.	28.05.2023 р.	Вик.

Студент Гашніков Д.М.

(підпис) прізвище та ініціали

Керівник бакалаврської роботи Гайдур Г.І.

(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА

на бакалаврську роботу

студента ***Гашнікова Данила Миколайвича***

на тему: «Розробка рекомендацій по захисту життєвого циклу продукції від атак у ланцюжку постачання. Supply Chain»

Актуальність: Атаки на ланцюги постачання становлять значну загрозу для організацій, націлені на постачальників на всіх рівнях. Ці атаки можуть призвести до втрати даних, порушення конфіденційності, витрат на відновлення, втрати довіри клієнтів та репутаційної шкоди. Рекомендації щодо захисту включають перевірку постачальників, дотримання стандартів безпеки, впровадження криптографічного захисту даних, моніторинг вразливостей та підвищення обізнаності персоналу. Захист життєвого циклу продукту має вирішальне значення для стратегії безпеки організації.

Позитивні сторони:

1. На основі проведеного аналізу в роботі було встановлено зміст процесу реагування на атаки в supply chain та визначено як їх розслідувати.
2. Було досліджено методи та засоби створення захисної моделі від атак на ланцюг постачання.
3. Розроблення рекомендацій щодо застосування методів та засобів в моделі захисту від атак на ланцюг постачання
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою бакалаврської роботи.

Недоліки:

1. У бакалаврській роботі бажано було б провести аналіз можливих умов функціонування запропонованих мною наборів рішень які могли б доповнити існуючу модель політики безпеки.
2. Бажано було б провести оцінку ефективності запропонованих методів на реальних показниках.

Висновок: Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Гашніков Д. М.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую

Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Гашніков Д. М. до захисту бакалаврської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Розробка рекомендацій по захисту життєвого циклу продукції від атак у ланцюжку постачання. Supply Chain».
Бакалаврська робота і рецензія додаються.
Директор інституту Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Гашніков Д. М. за період навчання в інституті
(прізвище та ініціали студента)

ННІЗІ з 2019 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) Берестяна Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент ***Гашніков Д.М.*** обрав тему роботи, метою якої було дослідження методів та засобів для захисту від атак на Supply Chain та розроблення рекомендацій щодо застосування цього під час реальної атаки. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання бакалаврської роботи Гашніков Д. М. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану бакалаврську роботу студента Гашнікова Данила Миколайовича на оцінку **«добре»** та присвоїти йому кваліфікацію: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник бакалаврської роботи Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2022 року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студент Гашніков Д. М.
(прізвище та ініціали)
допускається до захисту даної бакалаврської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____” _____ 2022 року

РЕФЕРАТ

Ця робота на 64 сторінках містить 6 ілюстрацій, 6 таблиць та 22 джерела згідно переліку посилань.

Об'єктом дослідження - захист життєвого циклу продукції від атак Supply Chain.

Предметом дослідження — методи та засоби для захисту життєвого циклу продукції від атак Supply Chain.

Мета роботи - Розробити рекомендації щодо застосування методів та засобів для захисту життєвого циклу продукції від атак Supply Chain.

Методи дослідження - опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

В роботі приведено основні відомості про supply chain, загрози та кіберзлочини.

Проаналізовано різні види загроз.

Досліджено методи та засоби створення захисної моделі від атак на ланцюг постачання

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування методів та засобів захисної моделі від атак на ланцюг постачання

АТАКА НА ЛАНЦЮГ ПОСТАЧАННЯ, ЗАГРОЗИ, МЕТОДИ ЗАХИСТУ, КІБЕРБЕЗПЕКА, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ НА ЛАНЦЮГ ПОСТАЧАННЯ, ПОЛІТИКА БЕЗПЕКИ, ОСОБЛИВОСТІ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface.

CVV – Card Verification Value.

DDoS – Distributed Denial-of-service attack.

DGA – Domain Generation Algorithms.

DNS – Domain Name System.

DoS – Denial-of-service attack.

EDR – Endpoint Detection and Response.

FTP – File Transfer Protocol.

Ip-адрес – Internet Protocol address.

IT-директор – Information Technology директор.

MITM – Man In The Middle.

PDF – Portable Document Format.

PCI DSS – Payment Card Industry Data Security Standard.

PC – персональний комп’ютер.

SMB – Server Message Block.

SSN – Social Security number.

TSP – Time Stamp Protocol.

USB – Universal Serial Bus.

VGA – Video Graphics Array.

ВСТУП

Несанкціонований доступ до системи може призвести до завантаження шкідливого програмного забезпечення на продукт і подальшого розповсюдження зараженої програми серед користувачів. Це може вивести їхні комп'ютери з ладу та призвести до вимагання значного викупу. Через велику кількість даних користувачів і складність захисту від таких атак цей метод стає все більш поширеним. На практиці спостерігається, що сучасним системам важко створити надійний захист від атак на ланцюги поставок, які з часом стають дедалі складнішими.

Актуальність роботи полягає в недостатності сучасних політик безпеки для ефективного захисту інформаційних систем підприємств від атак на ланцюги поставок. Ці атаки мають потенціал заразити значну частину користувачів за короткий проміжок часу, оскільки вони можуть відбуватися на будь-якому етапі процесу розробки та формування, впливаючи на всю інформаційну систему. Вирішення цієї проблеми сприятиме розробці більш надійної системи захисту.

Об'єктом дослідження є захист життєвого циклу продукції від атак Supply Chain.

Предметом дослідження методи та засоби для захисту життєвого циклу продукції від атак Supply Chain.

Мета роботи - полягає в розробці рекомендацій щодо застосування методів та засобів для захисту життєвого циклу продукції від атак Supply Chain.

Для цього були поставлені такі завдання:

1) аналіз успішно реалізованих атак та можливих вразливих місць в ланцюгу постачання;

2) створення переліку загроз у кожному етапі ланцюга постачання; визначення найефективніших методів захисту;

3) вдосконалення існуючих методів захисту та оцінка ефективності створеної моделі захисту від атаки на ланцюг постачання для інформаційної системи компанії.

Завдання бакалаврської роботи:

Дослідити існуючі загрози протягом життєвого циклу ланцюга поставок та сформулювати рекомендації щодо вдосконалення політики безпеки;

Проаналізувати відомі атаки на ланцюги поставок та зробити висновки, які будуть покладені в основу розробки рекомендацій щодо політики безпеки;

Посилити заходи безпеки компаній, які працюють з конфіденційною інформацією.

Методи дослідження - Дослідження охоплювало комплексне вивчення відповідної літератури, аналіз експлуатаційної документації та міжнародних стандартів, порівняння отриманих результатів та проведення експерименту.

Практичне значення одержаних результатів: Пропозиції щодо розслідування атаки на ланцюг постачання з метою забезпечення кібербезпеки корпоративних інформаційних систем.

1 РОЗГЛЯНЕМО ПРИНЦИП ДІЇ ТА НАЙБІЛЬШІ ВИПАДКИ УСПІШНОЇ РЕАЛІЗАЦІЇ АТАКИ НА ЛАНЦЮГ ПОСТАЧАННЯ

Ланцюг поставок охоплює кілька етапів і залучає численні сторони, починаючи з постачання сировини і закінчуючи кінцевим споживачем, який отримує готову продукцію **[1].**

Різноманітні атаки на ланцюги поставок використовують довіру між учасниками, роблячи їх вразливими до кіберзагроз. Ці атаки можуть призвести до значних втрат конфіденційної інформації, включаючи персональні та комерційні дані. Щоб запобігти таким атакам, вкрай важливо запровадити заходи безпеки на всіх етапах ланцюга постачання та реалізувати стратегії захисту від кіберзагроз

1.1. Використання принципу дії та випадків успішного використання атаки на ланцюг постачання

Ланцюг постачання - це багатогранна процедура, що охоплює контракти на поставку та кінцеву доставку товарів споживачам. Зловмисники можуть використовувати цей ланцюг у різний спосіб, зокрема, встановлюючи підроблені чіпи та використовуючи скомпрометований код у програмному забезпеченні. Особливо небезпечним є те, що атака може статися на будь-якому етапі ланцюга постачання, що потенційно може завдати значної шкоди організації. Тому дуже важливо ретельно перевіряти кожну ланку ланцюга постачання та вживати заходів для захисту від потенційних атак [1].

Отже, для виявлення комп'ютера, зараженого зловмисним кодом, можна проаналізувати ланцюг поставок системи. (див. рис. 1.1).

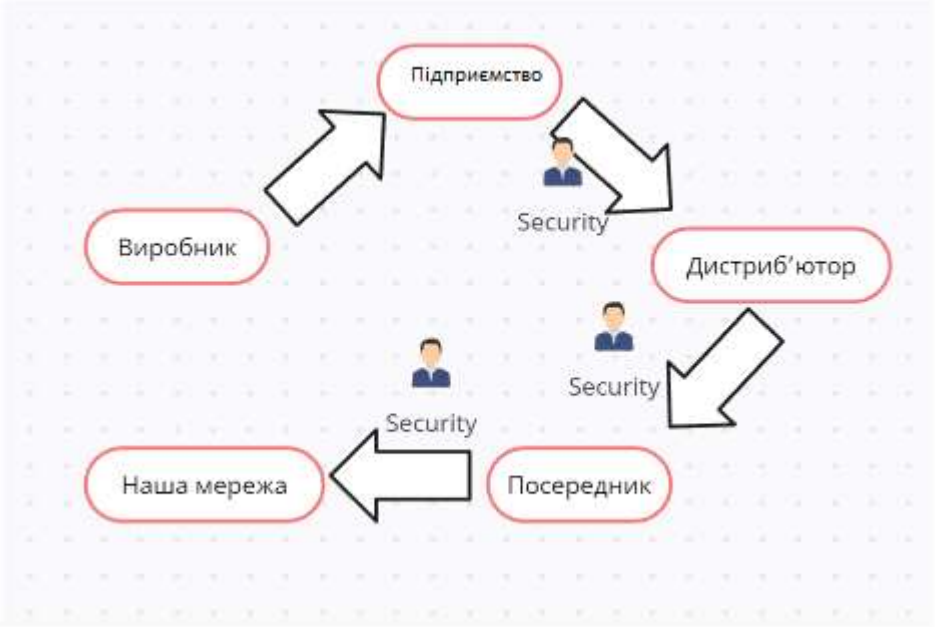

Рис. 1.1. Схема ланцюга поставок

Отже, початкові атаки відбулися у 2013 році, і кожна наступна була більш хитрою. Злочинці поступово розвивалися, ускладнюючи свої дії і роблячи їх більш непрозорими. На початкових етапах їхні цілі полягали в отриманні грошей, але з часом вони змінили свої пріоритети і почали націлюватися на великі компанії.

1.2. Реалізація атаки на ланцюг постачання

Ланцюг поставок - це комплексний процес, який охоплює залучення постачальників сировини і до кінцевого продажу готових товарів або послуг. У сучасному контексті цей процес став більш складним через включення фізичних активів, а також цифрових активів, таких як інформація та послуги.

У сучасному цифровому ландшафті організації різних секторів значною мірою покладаються на Інтернет та програмні інструменти для здійснення таких важливих операцій, як закупівлі, платіжні транзакції, обмін інформацією з партнерами та залучення клієнтів. Збої в цих процесах можуть мати серйозні наслідки, особливо для традиційного бізнесу. Такі компанії, як Advisen Ltd., чиї продукти в основному існують у цифровій сфері, вразливі до збитків, якщо їхні постачальники інформації або цифрова інфраструктура страждають від операційних збоїв. Зловмисні атаки, спрямовані на веб-сайти та мережі, становлять

значну загрозу, яка постійно зростає. Ці атаки спрямовані на встановлення несанкціонованого зв'язку з кіберзлочинцями, які прагнуть використати цінну інформацію та завдати шкоди. Наслідки таких атак можуть бути навіть більш згубними, ніж вплив на транспортну інфраструктуру.

У цифровій сфері компанії стикаються зі значними загрозами, пов'язаними з проблемами програмного та апаратного забезпечення. Одним з найпоширеніших сценаріїв є комп'ютерний збій, що призводить до перебоїв у роботі компанії. Показовим є інцидент, пов'язаний з активістською групою Anonymous, яка, як повідомляється, націлилася на компанію GoDaddy, відомого веб-хостера. Через низку внутрішніх мережевих подій, які вплинули на таблиці даних маршрутизаторів, у вересні 2012 року GoDaddy пережив відключення, яке тривало шість годин. Незважаючи на те, що компанія є найбільшим провайдером безпечного хостингу веб-сайтів з більш ніж 53 мільйонами зареєстрованих доменних імен, цей інцидент висвітлив вразливість, з якою стикаються компанії у підтримці безперебійного надання цифрових послуг.

Для посилення захисту від кібератак компанії застосовують низку технологій і практик. До них відносяться впровадження захищених мереж, використання надійних паролів, шифрування даних, антивірусний захист та інші відповідні методи. Однак важливо зазначити, що кіберзлочинці постійно вдосконалюють свою тактику зламу мереж і систем. Отже, компанії повинні постійно оновлювати та посилювати свої заходи мережевої безпеки, щоб випереджати потенційні загрози.

Крім того, компанії можуть регулярно створювати резервні копії даних і матеріалів, щоб зменшити ризик втрати або пошкодження даних у разі кібератаки або інших непередбачуваних ситуацій. Це гарантує, що критичні ресурси можуть бути легко відновлені. Крім того, щоб підвищити стійкість ланцюга постачання, компанії можуть вивчити та визначити альтернативних постачальників для забезпечення надійного та безпечного постачання. Дуже важливо стратегічно планувати та координувати різні етапи ланцюга постачання, мінімізуючи потенційний вплив на операційну діяльність у разі виникнення проблем з певним постачальником. Диверсифікуючи та зміцнюючи ланцюг постачання, компанії

можуть краще управляти ризиками та підтримувати безперервність операційної діяльності.

Отже, компанії повинні бути готовими до вирішення безлічі проблем, пов'язаних з безпекою та стійкістю ланцюгів поставок. Це вимагає постійного оновлення та вдосконалення технологій безпеки, ретельного планування та ефективної координації різних етапів ланцюга поставок. Крім того, активний пошук альтернативних постачальників сприяє створенню стійкого ланцюга постачання, здатного протистояти збоям. Постійно адаптуючи та посилюючи ці заходи, компанії можуть підвищити свою здатність підтримувати безпечну та стійку екосистему ланцюга поставок.

Кібератаки дійсно можуть мати негативний вплив на репутацію компанії. Ось кілька прикладів, які це ілюструють:

DigiNotar, голландська компанія, відповідальна за видачу цифрових сертифікатів, що використовуються в онлайн-транзакціях, зазнала порушень безпеки, які призвели до видачі шахрайських сертифікатів. Цей інцидент суттєво вплинув на репутацію компанії та підірвав довіру до послуг центру сертифікації.

Велика американська система метрополітену: Відома американська система метро стала жертвою масштабної кібератаки. Атака, ймовірно, спричинила перебої в роботі, потенційно поставивши під загрозу безпеку пасажирів і завдавши шкоди репутації транспортного відомства.

Американська електростанція: В іншому випадку американська електростанція зіткнулася з серйозними перебоями в роботі, коли комп'ютерний вірус націлився на систему управління турбінами. Вірус проник в мережу, коли технік ненавмисно підключив заражений USB-пристрій. Інцидент призвів до відключення електростанції на три тижні, підкресливши далекосяжні наслідки кібератаки на об'єкти критичної інфраструктури.

Ці приклади демонструють, як кібератаки можуть завдати репутаційної шкоди компаніям і організаціям, підкреслюючи важливість надійних заходів кібербезпеки для захисту від таких ризиків.

Один з помітних інцидентів, який виділяється як надзвичайно руйнівний акт комп'ютерного саботажу, стався, коли вірус стер дані приблизно на 75% корпоративних комп'ютерів, що належать нафтовому гіганту Saudi Aramco. Цей інцидент вважається однією з найбільш руйнівних кібератак на сьогоднішній день [2].

Важливо зазначити, що кібератаки, як правило, спрямовані на конкретні організації або групи організацій. Однак їхній вплив може виходити за межі окремих організацій і мати потенціал завдати шкоди цілому бізнес-сектору або навіть цілій країні. Такі атаки можуть вивести з ладу критично важливу інфраструктуру, скомпрометувати конфіденційну інформацію та завдати значної фінансової та операційної шкоди. Далекосяжні наслідки кібератак підкреслюють важливість надійних заходів кібербезпеки та пильності для захисту від цих загроз.

1.3. Аналіз відомих атак на ланцюг постачання

У 2013 році відбулася значна атака на ланцюг поставок, спрямована проти гіганта роздрібної торгівлі Target. Цей інцидент став одним з перших відомих випадків компрометації ланцюга поставок. Зловмисникам вдалося проникнути в системи Target, що призвело до несанкціонованого доступу до даних клієнтів. Спочатку повідомлялося, що було викрадено 40 мільйонів номерів кредитних карток, але пізніше з'ясувалося, що персональні дані, включаючи 70 мільйонів імен, адрес електронної пошти та номерів телефонів, також були скомпрометовані.

Наслідки атаки були серйозними для Target, як у фінансовому плані, так і з точки зору репутації. Компанія зазнала збитків на сотні мільйонів доларів, не враховуючи потенційних судових позовів від постраждалих клієнтів. Цей резонансний інцидент висвітлив вразливі місця в ланцюгу поставок і підкреслив потребу в надійних заходах безпеки для захисту від атак на ланцюги поставок, захисту даних клієнтів і пом'якшення потенційного впливу на бізнес.

На жаль, статистика свідчить, що рівень безпеки платежів дуже низький. Приблизно половина всіх витоків даних у роздрібних компаніях пов'язана з платіжними даними. Для порівняння, банки, які володіють платіжними даними,

стикаються з меншою кількістю таких порушень - 29%, тоді як процесингові компанії стикаються з 31% таких інцидентів. Основною причиною такої тривожної ситуації є недотримання торговельними підприємствами вимог Стандарту безпеки даних індустрії платіжних карток (PCI DSS) та незахищене зберігання ними інформації про клієнтів. Недотримання протоколів безпеки призводить до вразливості платіжних даних у роздрібній торгівлі.

У відповідь на інцидент з витоком даних компанія Target вжила заходів, щоб зменшити ймовірність крадіжки та захистити постраждалих клієнтів. Вони запропонували безкоштовну послугу протягом одного року для відстеження всіх транзакцій, яка мала на меті запобігти несанкціонованому використанню облікових записів. Зазвичай, у випадках крадіжки даних кредитних карток така послуга може не знадобитися, оскільки картки можна перевипустити, щоб запобігти шахрайським діям. Однак експерт з безпеки Брайан Кребс висловив серйозну стурбованість серйозністю і тривожним характером витоку даних в Target. За його оцінкою, ситуація створює значні ризики та потенційну шкоду для постраждалих осіб.

Target зазнав значної кібератаки, коли хакери викрали інформацію про кредитні картки та персональні дані понад 110 мільйонів користувачів. Витік даних також включав номери соціального страхування користувачів, зареєстрованих у дисконтній програмі Target. Викрадена інформація становить серйозний ризик, оскільки може бути використана зловмисниками для крадіжки особистих даних та шахрайських дій, таких як отримання кредитів під чужими іменами. Wall Street Journal повідомив, що в результаті цього інциденту було скомпрометовано понад 1 мільйон записів. На жаль, Target була не єдиною компанією, яка постраждала, оскільки Neiman Marcus і кілька інших компаній також стали жертвами подібних атак. Широке розповсюдження цих порушень викликає значне занепокоєння щодо злочинного використання даних користувачів. Як повідомляє Bloomberg, Волтер Лоеб, президент консалтингової компанії Loeb Associates, підкреслив, що це вплинуло не лише на Target і Neiman Marcus, але й на багато інших компаній [3].

З'явилися додаткові подробиці щодо часу та способу витоку даних Target. Слідчі встановили, що атака відбулася в період з 15 по 28 листопада, що збіглося зі святом Дня подяки та напередодні "чорної п'ятниці", головного дня шопінгу. У цей період група з 15 зловмисників успішно впровадила шкідливе програмне забезпечення в окремі касові апарати в магазинах Target, щоб викрасти конфіденційні дані карток. Було помічено, що зловмисники використовували цей часовий проміжок для тестування функціональності та ефективності свого шкідливого програмного забезпечення в точках продажу. Ці висновки проливають світло на конкретні часові рамки і тактику, застосовані зловмисниками під час витоку даних Target.

Слідчі надали додаткові подробиці про витік даних Target, показавши, що зловмисники успішно впровадили шкідливе програмне забезпечення в касові апарати магазинів Target в період з 15 по 28 листопада. Згодом, наприкінці місяця, зловмисники розширили сферу дії шкідливого програмного забезпечення на більшість магазинів Target і розпочали збір даних про транзакції клієнтів з платіжних карток у режимі реального часу. В результаті цього злому було скомпрометовано близько 40 мільйонів рахунків дебетових і кредитних карток. Однак пізніше Target переглянула цю оцінку, включивши до неї ще 30 мільйонів клієнтів, в результаті чого загальна кількість постраждалих осіб досягла 70 мільйонів. Викрадена інформація виходила за межі даних платіжних карток і включала особисті дані, такі як повні імена, адреси, адреси електронної пошти та номери телефонів. Загалом витік інформації торкнувся близько 110 мільйонів клієнтів Target, що свідчить про масштабний характер інциденту та обсяг інформації, яка була скомпрометована.

У березні 2014 року директор з інформаційних технологій (CIO) Target подав у відставку, а в травні того ж року пішов у відставку і генеральний директор. За останніми даними, збитки компанії в результаті злому склали 162 мільйони доларів США. Під час атаки зловмисники використовували з'єднання FTP (протокол передачі файлів) для передачі викраденої інформації про картки в різні місця в Росії. Джерела, пов'язані з розслідуванням, припускають, що значна частина викрадених

фінансових даних була згодом передана в кілька "віддалених" пунктів призначення. Ці події підкреслюють значний вплив і складність злому, а також ступінь розпорошеності викраденої інформації та її потенційного використання.

Значна кількість скомпрометованих комп'ютерів, що постраждали від Target-атаки, були розташовані в США та інших країнах. Викрадені дані зберігалися і були доступні кіберзлочинцям, які переважно базувалися у Східній Європі та Росії. У випадку з Target, викрадена інформація з їхньої мережі була знайдена на зламаних комп'ютерних серверах, розташованих в Майамі, і ще на одному віддаленому сервері в Бразилії. Наразі Сполучені Штати ведуть переговори з бразильською владою про взаємну правову допомогу з метою отримання доступу до конкретних даних, що зберігаються на сервері, розташованому в Бразилії. Повідомляється, що значна частина викрадених фінансових даних була розповсюджена в декількох інших "віддалених" місцях, що посилює складність порушення і проблеми, пов'язані з відстеженням і пом'якшенням його наслідків [4].

У вересні 2018 року авіакомпанія British Airways та Ticketmaster були об'єктами атак. British Airways зазнала компрометації зловмисниками, які отримали доступ до більше ніж 380 000 транзакцій з банківськими картами її клієнтів. Зловмисникам вдалося отримати не тільки основну інформацію про банківські картки користувачів, а й коди перевірки дійсності карток (CVV), які авіакомпанія не зберігає. Цей інцидент виявився катастрофічним для компанії, яка зазнала фінансових втрат і пошкодження репутації. Крім того, виникла серйозна загроза безпеці клієнтів і корпоративної інформації, що може мати значні наслідки. Аналогічні атаки також відбулися на інших веб-сайтах, включаючи Ticketmaster, які можуть призвести до витоку важливої конфіденційної інформації в руки зловмисників. Внаслідок цього порушується політика безпеки, і діяльність компаній може бути тимчасово призупинена до впровадження всіх необхідних заходів безпеки.

Отже, атаки мають значні наслідки для окремих осіб, персоналу та організації, а їх вирішення не є ані швидким, ані постійним. Досвід цієї авіакомпанії не є унікальним, оскільки повідомлялося і про інші випадки успішних атак на ланцюги

поставок. За кілька місяців до цього сайт з продажу квитків Ticketmaster зіткнувся з подібним порушенням, яке вплинуло на 5% його користувачів. У цьому випадку зловмисники маніпулювали кодом зовнішнього постачальника послуг, щоб отримати несанкціонований доступ до фінансової інформації клієнтів [5].

CCleaner, програма для очищення реєстру Windows, розроблена Piriform, невеликою британською компанією, яку придбала AVAST, стала критичною ланкою в серії атак на відомі організації. Під час Kaspersky Security Analyst Summit представники AVAST поділилися цією реальною історією. CCleaner, будучи відомим і широко використовуваним продуктом з більш ніж 2 мільярдами завантажень, став привабливим вибором для зловмисників для розповсюдження шпигунського ПЗ.

Зловмисникам вдалося проникнути в середовище компіляції Piriform, скомпрометувавши сервер збірки програм. Цей несанкціонований доступ дозволив їм впровадити шкідливе програмне забезпечення в легальний вихідний код, який використовується для компіляції програм. За допомогою модифікацій, внесених до бібліотеки компілятора, зловмисники успішно включили справжній цифровий підпис Piriform у заражене програмне забезпечення. В результаті компанія несвідомо поширювала скомпрометовані версії CCleaner 5.33.6162 та CCleaner Cloud 1.7.0.3191.

Атака розгорталася в три етапи. Спочатку шкідливе програмне забезпечення було впроваджено в CCleaner, широко використовувану програму з базою користувачів, що перевищує 100 мільйонів. Заражену версію CCleaner завантажили приблизно 2,27 мільйона разів, що призвело до виявлення близько 1,65 мільйона спроб підключення до серверів зловмисників. Згодом зловмисники обрали цілі з пулу комп'ютерів, які відповідали певним критеріям, включаючи осіб, потенційно пов'язаних з великими IT-компаніями та постачальниками. На наступному етапі зловмисники зосередилися на чотирьох особливо привабливих цілях і встановили на їхні комп'ютери чорний хід, використовуючи модифіковану версію шкідливого програмного забезпечення ShadowPad [6].

Під час бета-тестування своєї нової технології виявлення експлойтів компанія Cisco Talos зробила важливе відкриття. Вони помітили, що система безпеки запускала попередження у відповідь на інсталяційний файл CCleaner v5.33, який завантажувався з легітимних серверів. Подальший аналіз показав, що завантажений файл містив шкідливе корисне навантаження, включаючи алгоритм генерації доменів (DGA) і функції управління і контролю (C2), незважаючи на те, що він був підписаний дійсним цифровим підписом Piriform. Це відкриття стало приводом для розслідування атаки CCleaner, яка протягом місяця вже вразила понад 2 мільйони комп'ютерів користувачів. Крім того, другий зразок інсталятора, пов'язаний з цією загрозою, також мав дійсний цифровий сертифікат, але час його підписання відрізнявся від початкової збірки на 15 хвилин. Така розбіжність потенційно вказує на серйозну проблему в процесі розробки або підписання, що вимагає відкликання сертифіката. Будь-яке майбутнє створення сертифікатів повинно відповідати суворим стандартам безпеки, щоб зменшити ризик компрометації зловмисниками. Повний масштаб цієї проблеми та шляхи її вирішення можуть бути визначені лише в результаті ретельного розслідування.

Існує ймовірність того, що зовнішня або внутрішня організація зламала середовище розробки або збірки CCleaner і впровадила шкідливий код у збірку, підписану цифровим підписом. Це може бути зловмисник, який отримав несанкціонований доступ, або інсайдер, який має привілеї на модифікацію коду. Хоча попередні версії CCleaner залишаються доступними для завантаження, версія, що містить шкідливий код, була видалена і більше не доступна для завантаження. Необхідно провести додаткове розслідування, щоб з'ясувати масштаби проблеми та вжити відповідних заходів для її вирішення [7].

Шкідлива програма, вбудована в CCleaner, використовує тактику затримки, щоб обійти автоматизовані системи аналізу та сканування. Для цього вона перехоплює поточний системний час, встановлює 601-секундну затримку у виконанні, а потім перевіряє поточний час. Якщо заздалегідь визначена умова не виконується, шкідлива програма припиняє своє виконання, дозволяючи бінарному файлу CCleaner нормально функціонувати. Крім того, у випадках, коли програма не

може виконати IcmpCreateFile, вона використовує функцію Sleep для реалізації затримки.

Після затримки шкідливе програмне забезпечення переходить до перевірки привілеїв, призначених користувачеві, який запускає систему. Якщо користувач, який виконує шкідливий процес, не володіє правами адміністратора, шкідливе програмне забезпечення припиняє своє виконання.

Якщо користувач, який запускає шкідливу програму, має адміністративні привілеї на скомпрометованій системі, процес активує привілей SeDebugPrivilege. Після цього шкідлива програма отримує значення "InstallID", що зберігається в певному розділі реєстру.

Після виконання вищезазначених дій шкідливе програмне забезпечення ініціює профілювання системи та збирає відповідну системну інформацію, яка згодом передається на командно-контрольний сервер (C2). Після збору системна інформація шифрується і кодується за допомогою модифікованої версії Base64. Нарешті, шкідливе програмне забезпечення встановлює канал зв'язку з сервером C2 для отримання подальших інструкцій та обміну даними.

Під час аналізу цього шкідливого програмного забезпечення Talos виявив програмну помилку у шкідливому коді, пов'язану з функціоналом C2. Після того, як шкідливе програмне забезпечення ідентифікує сервер C2 для зв'язку, воно починає передавати закодовані дані, що містять інформацію про профіль системи. Крім того, шкідливе програмне забезпечення зберігає IP-адресу сервера C2 у визначеному місці реєстру. Крім того, він записує значення поточного системного часу для довідки.

У ситуаціях, коли основний керуючий сервер зараженої програми не відповідає на HTTP POST-запити, шкідливе програмне забезпечення використовує алгоритм генерації доменів (Domain Generation Algorithm, DGA). Цей алгоритм використовує поточні значення року та місяця для генерації залежних від часу доменів. Шкідливе програмне забезпечення шукає в DNS кожен домен, згенерований за допомогою алгоритму DGA. Якщо пошук в DNS не призводить до отримання IP-адреси, процес повторюється. Програма виконує DNS-запит для

активного домену DGA і очікує від сервера імен повернення двох IP-адрес. Шляхом побітових операцій над отриманими значеннями IP-адрес програма обчислює резервний сервер керування. Це дозволяє визначити фактичну адресу резервного сервера управління (C2), який буде використовуватися для подальших операцій управління. Cisco Talos зазначає, що домени DGA не були зареєстровані, що може мати серйозні наслідки, оскільки значна кількість систем може бути інфікована. Згідно зі звітами CCleaner за листопад 2016 року, кількість завантажень програми перевищила 2 мільярди по всьому світу, а кількість нових користувачів постійно зростає на 5 мільйонів щотижня.

Рис. 1.2. Споживча демографія CCleaner[5]

Якщо хоча б частина цих систем буде скомпрометована, зловмисник зможе використовувати їх у різних цілях. Вкрай важливо відновити або перезавантажити вразливі системи до 15 серпня 2017 року. Крім того, користувачам настійно рекомендується оновити всі екземпляри CCleaner до останньої доступної версії, щоб мінімізувати ризик зараження.

Користувачам вкрай важливо негайно оновити своє програмне забезпечення, включаючи CCleaner, до останньої доступної версії, щоб зменшити ризик потенційного зараження. Телеметричні дослідження показали, що багато систем генерують DNS-запити, спрямовані на домени DGA, пов'язані з цією атакою. Ці домени ніколи не були зареєстровані, а це означає, що системи, які намагаються вирішити їх за IP-адресою, ймовірно, заражені шкідливим програмним

забезпеченням. Зловмисники експлуатують довіру користувачів до постачальників програмного забезпечення та їхніх серверів, що дозволяє їм поширювати шкідливе програмне забезпечення серед організацій та приватних осіб по всьому світу. Слід зазначити, що активність доменів DGA, пов'язаних з цією загрозою, зросла в серпні та вересні, що свідчить про значний рівень цілеспрямованої активності [8].

Цей сценарій ілюструє, як зловмисники можуть використовувати довірчі відносини між постачальниками програмного забезпечення та їхніми користувачами для розповсюдження шкідливого програмного забезпечення. Користуючись довірою користувачів до файлів і серверів, шахраї можуть поширювати шкідливі оновлення та отримувати несанкціонований доступ до систем інших користувачів. У багатьох випадках процес перевірки даних, отриманих від постачальників програмного забезпечення, не такий суворий, як для інших джерел. Використання цієї вразливості дозволяє шахраям непомітно поширювати шкідливе програмне забезпечення, використовуючи довіру до постачальників програмного забезпечення.

Вірус Petya.A (Diskoder.C) здійснив значну кібератаку в Україні, націлену на різні організації, такі як банки, енергетичні компанії, державні ресурси, мережі, засоби масової інформації та інші відомі підприємства. Атака, що характеризується значними масштабами, призвела до порушення роботи комп'ютерних систем та операцій. Варто зазначити, що атака CCleaner, яка сталася раніше, має багато спільного з цією масштабною атакою і спочатку залишалася непоміченою протягом тривалого періоду часу.

ISSP Labs виявила вірусну розсилку на одному з веб-сайтів та знайшла зразок вірусу Crystal Finance Millennium. Цей конкретний скрипт є завантажувачем і його основним завданням є завантаження та запуск шкідливого файлу. У скрипті також міститься критична інформація, включаючи адресу, з якої буде завантажений шкідливий файл. Ця адреса зберігається у вигляді тексту в масиві. Серед зразків вірусу, що були виявлені вірусною розсилкою, один мав адресу завантаження, яка вказувала на 23-cfm.com.ua - веб-сайт, пов'язаний з програмним пакетом бухгалтерського обліку Crystal Finance Millennium.

Подальші дослідження, проведені Microsoft, встановили зв'язок між вірусом Crystal Finance Millennium і програмою M.E.Doc, яка сприяла поширенню вірусу Petya.A. Метою цього вірусу було шифрування головного завантажувального запису інфікованого комп'ютера, що в кінцевому підсумку призводило до потенційної втрати даних на всьому жорсткому диску. На відміну від типових програм-вимагачів, які вимагають викуп, цей вірус становив більшу небезпеку, оскільки був спрямований на знищення файлів, що робило його особливо небезпечним для користувачів [9].

Компанія Cisco Talos провела розслідування щодо розповсюдження шкідливої програми, яка використовує вразливості мережі. Цей вірус має різні назви, зокрема Petrwrap, GoldenEye та Nyetya. Він використовує такі технології, як Eternal Blue, Eternal Romance, WMI та PsExec для переміщення мережею. На відміну від WannaCry, Nyetya не має компоненту сканування зовнішніх систем. На думку експертів Cisco Talos, зараження пов'язане з програмою оновлення MeDoc, яка використовується для українського пакету податкової звітності. Однак точне джерело вектора поки що не встановлено. Важливо зазначити, що на відміну від WannaCry, Nyetya не містить компоненту зовнішнього сканування.

Точний вектор джерела шкідливого програмного забезпечення все ще досліджується компанією Cisco Talos. Наразі немає жодних доказів, які б вказували на використання електронної пошти або документів Office як способу доставки цього шкідливого програмного забезпечення. Однак експерти вважають, що зараження пов'язане з системами оновлення програмного забезпечення MeDoc, українського пакету податкової звітності. Cisco Talos активно проводить розслідування з цього приводу.

Враховуючи характер атаки Nyetya, Cisco Talos твердо переконана, що наміром зловмисника було спричинити руйнування, а не отримати фінансову вигоду. Ми рекомендуємо користувачам і організаціям не платити викуп, оскільки отримати ключ розшифровки неможливо. Зловмисник використовував поштову скриньку на posteo.de, яка була закрита. Це означає, що зловмисник не міг отримати платежі від жертв або надати ключі розшифровки після отримання викупу. Крім

того, шкідливе програмне забезпечення не використовувало метод прямого підключення до командного сервера для віддаленого розблокування [10].

Атака була полегшена здатністю шкідливого програмного забезпечення сканувати мережу на наявність вразливих машин і згодом експлуатувати їхні системи. Процес сканування включав використання API NetServerEnum і націлювався на відкритий TCP-порт 139. Nyetya використовував різні механізми для саморозповсюдження після зараження пристрою, зокрема:

EternalBlue: Це той самий експлойт, що використовувався вірусом-здирником WannaCry.

EternalRomance: Експлойт SMBv1, який не був розкритий групою "ShadowBrokers".

PsExec: Легальний інструмент адміністрування Windows.

WMI (Windows Management Instrumentation): Легітимний компонент Windows.

Ці механізми використовувалися шкідливим програмним забезпеченням для поширення та зараження інших пристроїв у мережі. Їхньою метою було полегшити встановлення та виконання файлу perfc.dat на інших пристроях, тим самим уможливлюючи поширення шкідливого програмного забезпечення.

The malware utilized the EternalBlue and EternalRomance exploits to target systems that did not have the MS17-010 security update installed. The specific exploit launched against a victim's system depended on the operating system being used. Here are the operating systems associated with each exploit:

EternalBlue:

Windows Server 2008 R2;

Windows Server 2008;

Windows 7.

EternalRomance:

Windows XP;

Windows Server 2003;

Windows Vista.

Експлойти EternalBlue та EternalRomance здатні розгортати модифіковану версію DoublePulsar, яка діє як постійний бекдор у просторі ядра скомпрометованої системи. Розробник вніс незначні зміни в оригінальну версію DoublePulsar, щоб уникнути мережевого виявлення і використовувати інструменти сканування DoublePulsar з відкритим вихідним кодом, знайдені в Інтернеті. Ці модифікації передбачали зміну лише кількох байтів коду, що дозволило шкідливому програмному забезпеченню уникнути виявлення та розширити свої можливості.

Атакер внес зміни в коди команд, що містяться в таблиці 1.1, а також змінив відповіді, занесені до таблиці 1.2.

Таблиця 1.1

Змінені коди команд.

Original Command	Code Nyetya Command Code	Purpose
0x23	0xF0	PING
0x77	0xF1	KILL
0xC8	0xF2	EXEC

Таблиця 1.2

Змінені коди відповідей.

Original Response	Code Nyetya Response Code	Purpose
0x10	0x11	OK
0x20	0x21	CMD_INVALID
0x30	0x31	ALLOCATION_FAILURE

Зловмисник, який стоїть за Nyetya, змінив спосіб зберігання коду у відповіді DoublePulsar в SMB-пакеті. Перемістивши код в зареєстроване поле, яке зазвичай містить значення 0x0000 замість поля MultiplexID, що використовувалося в попередній версії, модифікований DoublePulsar стає складніше виявити.

Для зараження мережевих пристроїв зловмисник використовує такі інструменти, як PsExec або WMI, щоб встановити шкідливе програмне

забезпечення. Після того, як система скомпрометована, Nyetya шифрує файли на хості за допомогою 2048-бітного RSA-шифрування і очищає журнали подій, щоб приховати свою діяльність.

Nyetya також намагається отримати адміністративні привілеї для поточного користувача, щоб змінити завантажувальний сектор диска PhysicalDrive0. Якщо ця спроба виявляється невдалою, шкідлива програма стирає перші десять секторів диска. При перезавантаженні системи зміни, внесені в завантажувальний сектор або стирання перших десяти секторів, викличуть сповіщення або попередження (див. рис. 1.3).

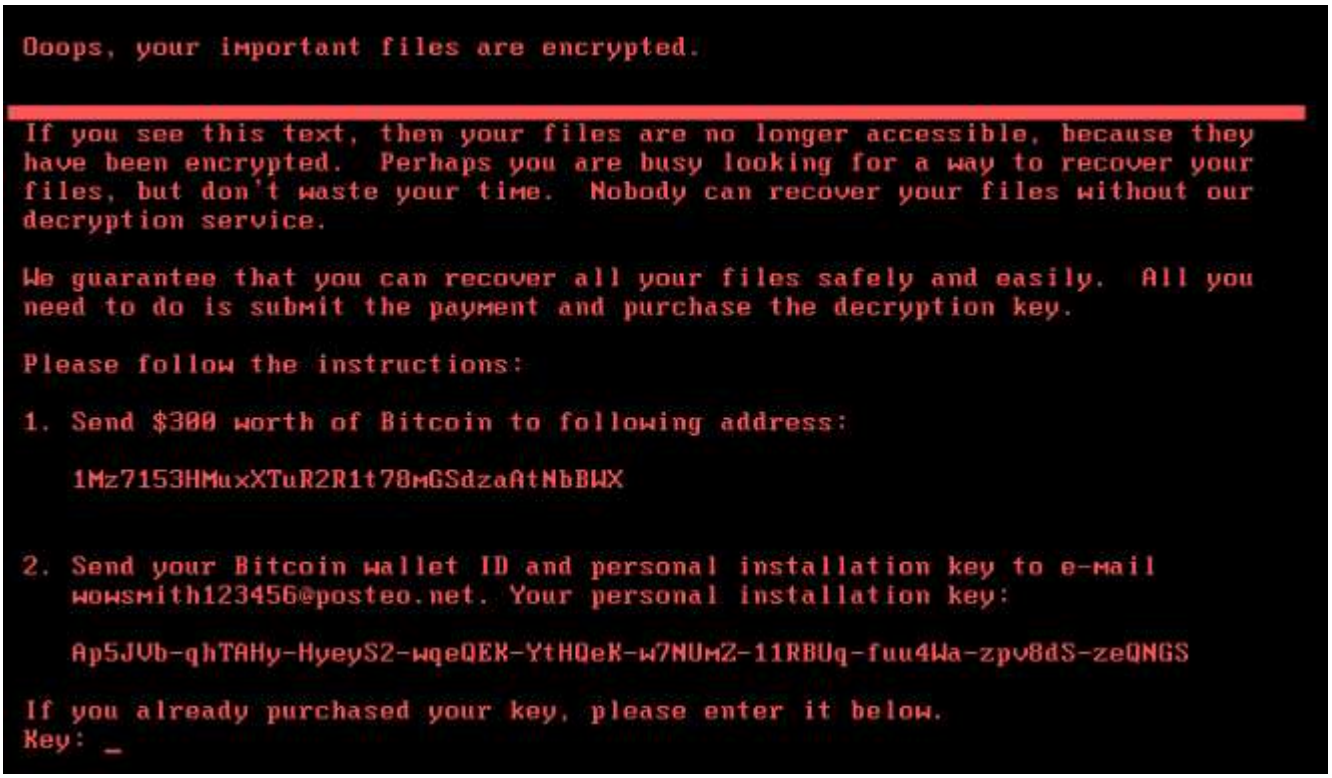

Рис. 1.3. Знімок екрану системи, скомпрометованої Nyetya

Незалежно від того, чи вдасться Nyetya успішно перезаписати завантажувальний сектор, вона наполегливо виконуватиме запрограмовану функцію перезавантаження системи через годину після зараження за допомогою завдань. Фахівці Cisco Talos стверджують, що метою Nyetya не є насамперед фінансова вигода за рахунок шифрування файлів, оскільки творці не ставили в пріоритет генерацію ключів або зберігання ключових компонентів для

розшифровки. Натомість, Nyetya була спеціально розроблена для деструктивних операцій, які можуть бути зумовлені політичними або економічними мотивами. Цікаво, що ці атаки, з відмінними характеристиками і результатами, можна віднести до цих двох мотиваційних груп [11].

Атака Nyetya привернула значну увагу ЗМІ та широко обговорювалася людьми з обмеженими знаннями в галузі ІТ. На відміну від неї, атака CCleaner залишалася непоміченою протягом тривалого періоду часу. З роками атака Nyetya стає все більш небезпечною, здатною завдати значної шкоди та створити проблеми в національному масштабі. Вірус швидко поширюється в локальних мережах, що призводить до значної кількості інфікованих комп'ютерів і значних наслідків. Останній варіант вірусу Nyetya має схожість з WannaCry, демонструючи спільні характеристики у своїх виконуваних файлах, що вказує на потенційне спільне авторство.

Атака Nyetya використовує протокол зв'язку, який зазвичай використовується в локальних мережах, що дозволяє швидко заразити компанії, які мають значну базу користувачів, що користуються однією мережею. Користувачі, які не використовують цей протокол зв'язку, з меншою ймовірністю стануть мішенню атаки. Аналогічно, компанії, які не під'єднані до тієї ж локальної мережі, що й інфіковані, мають меншу вразливість до зараження.

У разі атаки всі постраждалі організації стикаються з потенційною втратою важливої інформації, що зберігається в їхніх комп'ютерних системах. Серйозність загрози зростає, коли інфекція вражає не лише окремі робочі станції, але й сервери компанії. У таких випадках існує значний ризик втрати даних, оскільки серверні середовища часто зберігають копії важливих даних. Втрата даних на серверах є найбільш критичним сценарієм, і єдиним способом відновлення даних може бути використання резервних копій. Якщо резервні копії недоступні, розшифровка вірусу може зайняти багато часу. Однак банки мають найнижчий ризик втрати даних, оскільки більшість з них регулярно створюють резервні копії своїх даних. В результаті вони можуть втратити лише кілька хвилин або годин інформації завдяки

наявності резервних копій. З іншого боку, організації, які нехтують створенням резервних копій, часто стикаються з ускладненнями, як підкреслив Сич [12].

Антон Геращенко, народний депутат і радник глави МВС, заявив на своїй сторінці у Facebook, що кібератака, яка мала на меті дестабілізувати українську економіку та суспільні настрої, готувалася щонайменше місяць. Вірус поширювався через електронні листи, які надсилалися адресатам російською та українською мовами. Дата запуску вірусу була запланована на 27 червня об 11:00.

Атака була спрямована на різні сектори, включаючи банківські відділення, засоби масової інформації, зв'язок, транспорт, телекомунікації та енергетичні об'єкти. Від вірусу постраждали такі компанії, як "Укртелеком", "Київ- та Дніпроенерго", "Укрзалізниця", аеропорт "Бориспіль" та Кабінет Міністрів. Вірус шифрує дані на жорстких дисках і вимагає викуп у кілька сотень доларів.

Висновки до розділу 1

У першому розділі представлено огляд атак на ланцюги поставок, включаючи їх здійснення та зростаючу актуальність цієї проблеми. Такі атаки можуть мати серйозні наслідки для будь-якої галузі, роблячи кожну компанію вразливою до ризику стати жертвою. Дивно, але середній бізнес, який часто вважає, що має імунітет до атак на ланцюги поставок, часто стає першою мішенню для компрометації більших організацій.

У наступній частині ми заглиблюємося у найвідоміші атаки, висвітлюючи конкретні деталі реалізації в ланцюгу поставок. Ці атаки є складними, здатними проникати в різні сегменти і включають в себе кілька етапів. Дуже важливо виявити вразливі місця та розробити стратегічний план захисту, щоб ефективно протистояти таким атакам.

Проведення успішної атаки на ланцюг поставок є дуже складним завданням, що вимагає значних ресурсів і часу для виявлення вразливостей і створення шкідливого коду. Кваліфіковані програмісти з досвідом обходу захисних систем компанії є незамінними, а також необхідні значні фінансові інвестиції. Однак, якщо зловмисникам це вдається, вони можуть отримати несанкціонований доступ до

особистої інформації клієнтів, завдати шкоди обладнанню, видалити важливі дані і навіть викрасти значні суми грошей.

2 МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ ЗАХИСНОЇ МОДЕЛІ ВІД АТАК НА ЛАНЦЮГ ПОСТАЧАННЯ.

У 2017 році було виявлено дві значні атаки на ланцюги постачання: WilySupply та атака зловмисників, які використовували оновлення програмного забезпечення для розповсюдження шкідливого програмного забезпечення. Ці атаки призвели до широкого розповсюдження програм-вимагачів у всьому світі. Компрометація українського програмного забезпечення для податкового обліку стала джерелом зараження вірусу-здирника Petya. Крім того, того ж року було інфіковано безкоштовну утиліту CCleaner. На початку 2018 року було виявлено та зупинено спалах вірусу Dofoil. Усі ці атаки використовували довіру користувачів до механізмів оновлення програмного забезпечення для розповсюдження шкідливого програмного забезпечення.

Згадані випадки є лише кількома прикладами з-поміж численних випадків атак на ланцюги поставок, що сталися у 2017 та 2018 роках. Частота таких атак неухильно зростає з кожним роком (див. рис. 2.1).

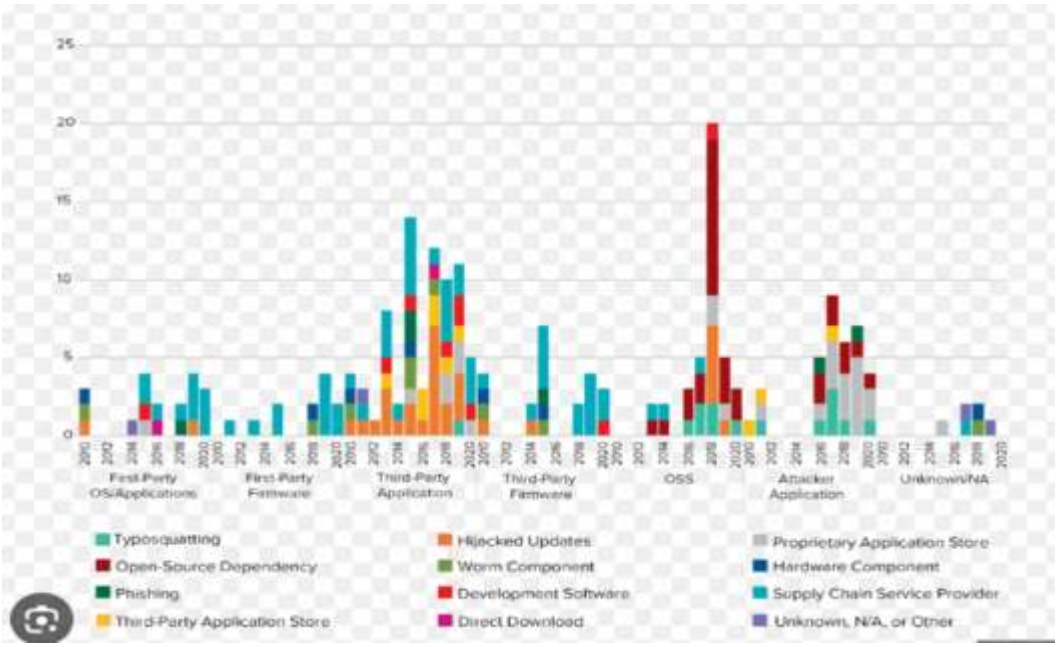

Рис. 2.1. Тенденції атак в ланцюжку поставок програмного забезпечення (джерело: презентація RSA Conference 2018 «Вектор несподіваних атак: засобу оновлення програмного забезпечення») [13]

Атаки на ланцюги поставок стають все більш поширеними завдяки підвищенню рівня безпеки сучасних платформ, таких як Windows 10, та зменшенню ефективності традиційних векторів атак, таких як експлойти в браузерах. Зловмисники постійно шукають найслабші місця в системах, враховуючи, що розробка або отримання експлойтів "нульового дня" є дорогим і складним завданням. Як наслідок, вони вдаються до більш доступних альтернатив, таких як компрометація ланцюжка постачання програмного забезпечення. Ці атаки використовують вразливості в практиках кодування, протоколах та серверній інфраструктурі постачальників програмного забезпечення.

Експлуатація ланцюжків постачання пропонує зловмисникам кілька переваг, зокрема можливість націлитися на велику кількість потенційних жертв і отримати значні прибутки. Це перетворилося на загальногалузеву проблему, яка потребує уваги та співпраці різних зацікавлених сторін, включаючи розробників програмного забезпечення, постачальників та системних адміністраторів. Співпраця між цими сторонами має важливе значення для забезпечення захисту від атак, їх швидкого виявлення та розробки ефективних рішень для протидії їм.

2.1. Схема захисту від атаки на ланцюг постачання

Успішна атака на ланцюг поставок залежить від наявності численних вразливостей у системі безпеки підприємства, які можуть бути використані зловмисниками для проникнення. Навіть невеликі пропущені деталі можуть стати початковим етапом для майбутньої атаки на ланцюг поставок. Ці атаки мають чітко виражені характеристики:

Компанії, які постраждали від атаки на ланцюги поставок, часто виявляють втрату персональних даних та конфіденційної інформації через тривалий час після початку атаки. Таким чином, чим довше триває атака, тим більше даних клієнтів стає скомпрометованими;

Зловмисники користуються довірою користувачів до продукту, яким вони раніше користувалися, та репутацією компанії, відомої своєю турботою про клієнтів та випуском оновлень продуктів;

Інфікування може відбуватися в ланцюжку поставок компанії-постачальника, коли заражений продукт потрапляє на початкову ланку ланцюжка поставок компанії, яка користується їхніми послугами;

Атаку можна порівняти зі сценарієм бомби уповільненої дії. На певному етапі в ланцюжок поставок впроваджується інфікований компонент, наприклад, виконуваний файл або спеціалізований програмний інструмент. Згодом, коли користувачі завантажують програму, вона починає діяти за сценарієм зловмисників і може швидко відкрити доступ або вивести з ладу мільйони комп'ютерів користувачів;

Процес атаки може розпочатися на будь-якому етапі створення та розвитку компанії. Ефективні операції передбачають використання розвідувальних даних, отриманих шляхом спостереження за співробітниками, моніторингу стратегічних приміщень, перевірки обладнання та вивчення способу роботи компанії.

Для розробки моделі захисту ми можемо взяти уявну компанію, яка має багато елементів у своєму ланцюжку постачання, що можуть бути використані зловмисниками для проведення ефективної атаки. Розглянемо сценарій компанії, яка самостійно виготовляє все необхідне обладнання та програмне забезпечення, не залучаючи фахівців та не співпрацюючи з іншими компаніями. Однак слід зазначити, що такий сценарій є нереальним, дуже дорогим і не може гарантувати повного захисту від можливих атак на ланцюг постачання.

На схемі рис. 2.2 зображено процес створення та розвитку компанії, підкреслюючи вразливості, які можуть виникнути при використанні послуг різних постачальників. Початковий етап схеми передбачає створення або облаштування приміщень з нетехнічним обладнанням таким чином, щоб мінімізувати ризик витоку інформації технічними каналами.

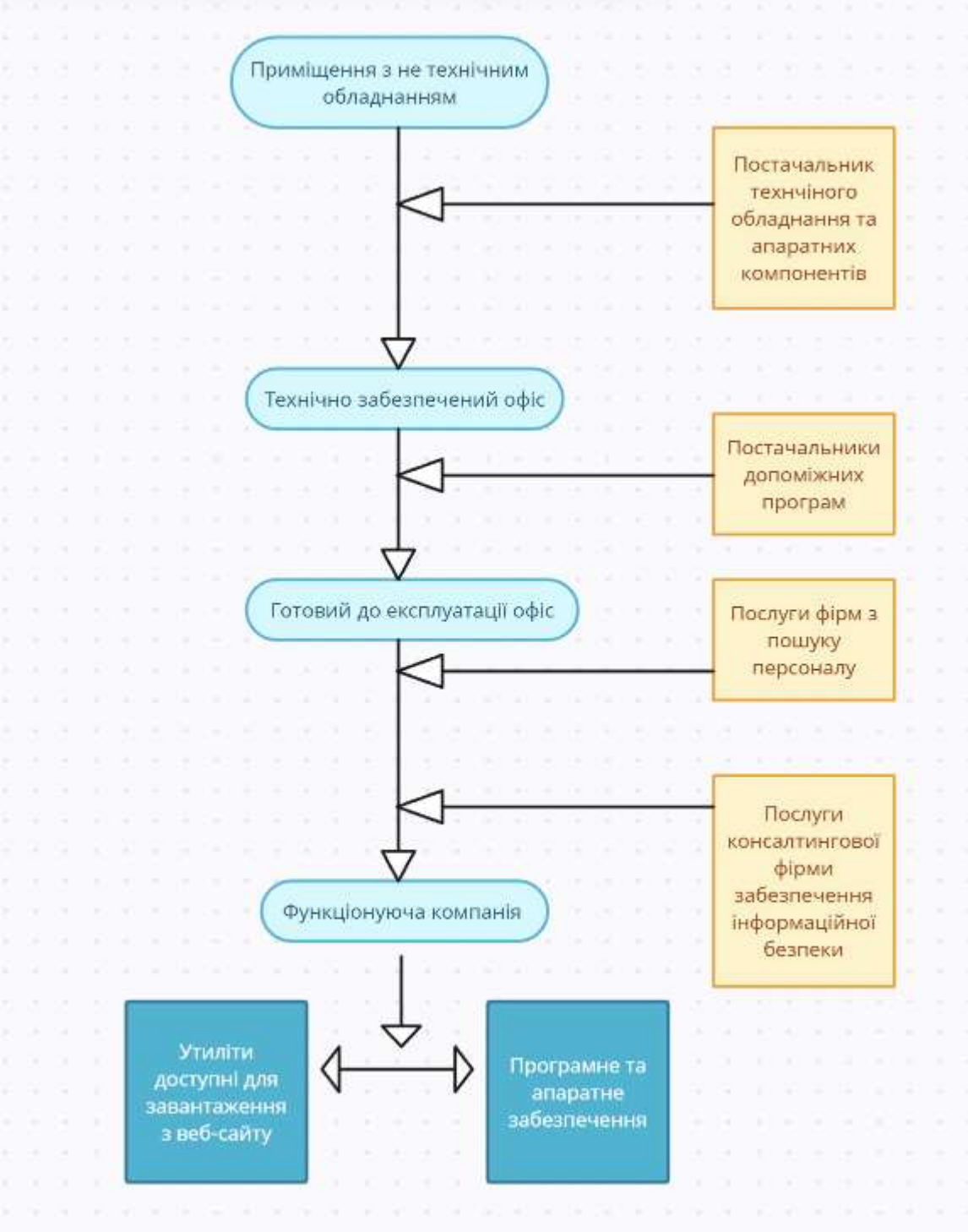

Рис. 2.2. Процес створення та функціонування абстрактної компанії

Для того, щоб компанія працювала ефективно та безпечно, вона повинна обладнати свій офіс відповідним апаратним та програмним забезпеченням. Цього можна досягти шляхом залучення постачальників, які надають технічне

обладнання, апаратні компоненти та програмні рішення. Цей аспект ланцюжка поставок має вирішальне значення, і його не можна залишати поза увагою.

Навіть якщо офіс технічно оснащений, йому може бракувати програмного забезпечення, необхідного для безпечної та продуктивної роботи, ефективної комунікації між співробітниками та сприятливого робочого середовища. Керівництву компанії необхідно прийняти рішення щодо необхідного набору програм для кожного відділу та організації в цілому. Цей вибір має на меті забезпечити безпеку та ефективність працівників у виконанні їхніх посадових обов'язків.

На наступному етапі компанія може розглянути два варіанти задоволення своїх кадрових потреб. По-перше, вона може співпрацювати з рекрутинговими компаніями, які пропонують послуги з підбору кандидатів і збирають необхідну інформацію про потенційних працівників, зменшуючи таким чином ризики для компанії. Крім того, компанія може створити власний внутрішній відділ, який займатиметься процесом підбору персоналу, укомплектований профільними фахівцями. Однак створення власного відділу може бути дорогим і складним процесом. Компанії з обмеженим бюджетом часто починають з партнерства з рекрутинговими фірмами, а згодом, у міру розширення бізнесу, розглядають можливість створення власного спеціалізованого відділу.

Коли йдеться про послуги з інформаційної безпеки, зазвичай рекомендується створювати власний відділ. Це гарантує, що програмні продукти будуть захищені, а політики безпеки будуть адаптовані до конкретних потреб і обставин компанії.

Після того, як компанія створила власний відділ, вона може приступити до виробництва програмного та апаратного забезпечення, яке може бути доступним для придбання через онлайн-сервіси або спеціалізовані магазини. Щоб краще зрозуміти, які вразливості можуть виникнути і на якому етапі вони з'являються, звернімося до рисунку 2.3. На діаграмі стрілками різних кольорів позначені потенційні вектори атак, класифіковані залежно від типу постачальника та об'єкта атаки.

Однак важливо зазначити, що на цьому етапі також можуть з'явитися вразливості, які створюють ризики для ланцюга постачання. Щоб зменшити ці ризики, компанія проводить ретельний аналіз потенційних загроз і втрат на кожному етапі. На основі цього аналізу приймаються рішення щодо нейтралізації або мінімізації цих загроз, забезпечуючи проактивні заходи для захисту цілісності та безпеки ланцюга постачання [14] .

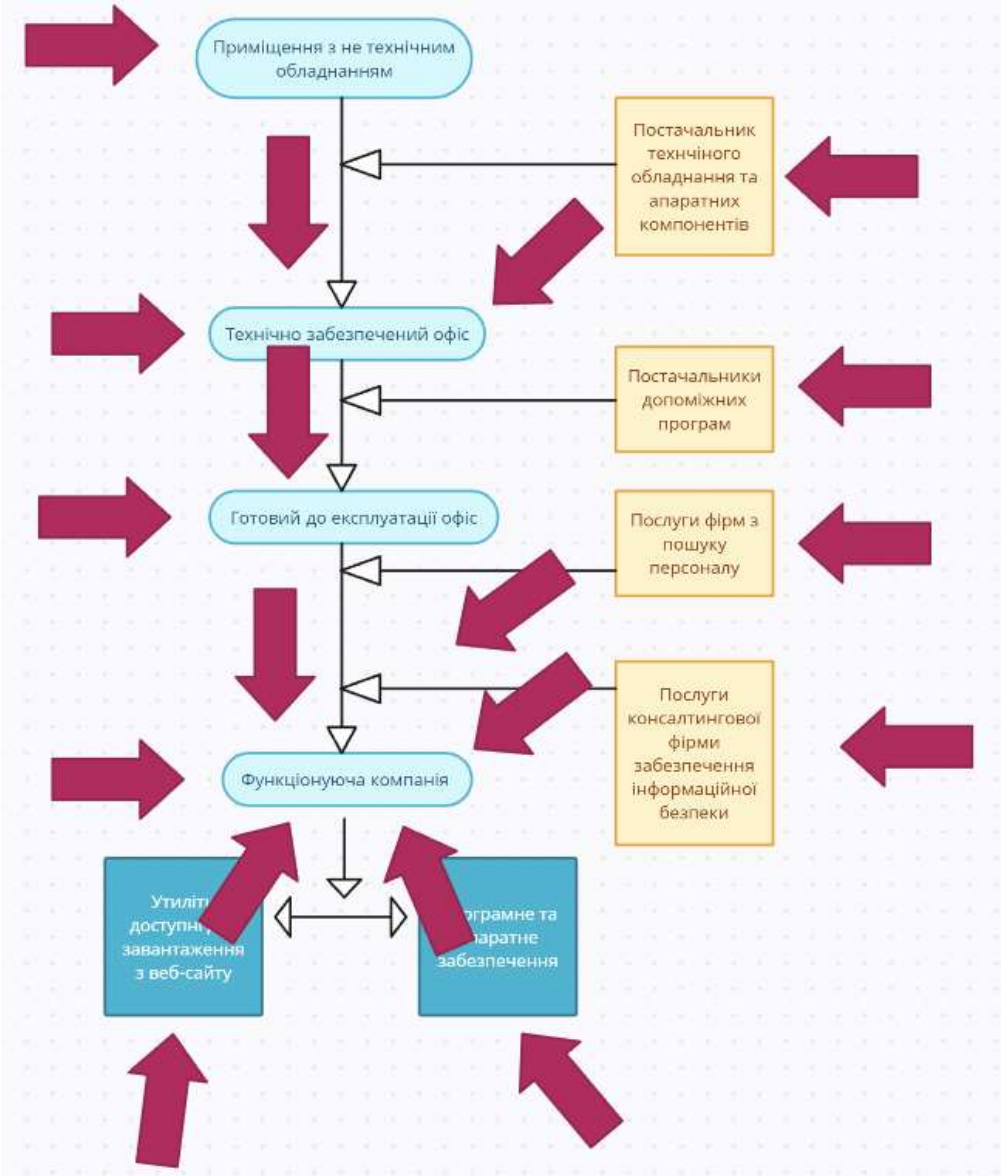

Рис. 2.3. Можливі вразливі місця в процесі розвитку і становлення компанії

2.2. Створення методів захисту від атаки на ланцюг постачання на кожному етапі

Перший тип атак передбачає спроби зловмисників проникнути в приміщення на етапі нетехнічного налаштування обладнання. Рівень ризику на цьому етапі залежить від репутації компанії та ринкового попиту. Маловідомі або новостворені компанії зазвичай стикаються з меншим ризиком, тоді як відомі компанії, що розвиваються, особливо ті, що відкривають філії, є більш вразливими. На цьому етапі можна виділити наступні загрози:

Проникнення підслуховувального пристрою під час облаштування офісу, що може бути здійснено вантажником або несанкціонованою особою, яка отримала доступ до приміщення;

Встановлення Wi-Fi мікрокамери для прихованого спостереження.

Несанкціоноване фотографування облаштованого приміщення та розміщення його в соціальних мережах;

Навмисне розміщення в приміщенні сторонніх предметів або захаращення, що підвищує ймовірність успішної реалізації першої та другої загроз;

Встановлення підслуховуючого пристрою в телефон співробітника.

У разі успішної реалізації цих загроз можуть виникнути наступні наслідки:

Втрата інформації про місцезнаходження сховища конфіденційних даних, планів компанії та інших важливих даних, які можуть бути використані зловмисниками для організації ефективної атаки;

Внесення зайвих предметів під час облаштування приміщення, які потенційно можуть перешкоджати виявленню встановлених камер або підслуховуючих пристроїв. Використання мінімалістичного підходу до дизайну офісу допомагає помічати будь-які нові доповнення та зберігати контроль над навколишнім середовищем [15] .

Важливо зазначити, що одна загроза може призвести до іншої, що підкреслює необхідність прийняття комплексних рішень на кожному етапі, незважаючи на потенційно вищі витрати. Такі заходи необхідні для запобігання значних втрат важливої інформації в майбутньому.

Рішення:

Залучити фахівця для проведення ретельної перевірки та пошуку підслуховуючих пристроїв, камер і жучків в офісних приміщеннях та на пристроях;

Впровадити комплексну систему безпеки, включаючи встановлення металодетекторів на вході до офісу, для виявлення та контролю за переміщенням осіб та предметів, що входять до приміщення;

Обмежити доступ на територію офісу уповноваженим працівникам компанії, забезпечивши пропуск лише затвердженого персоналу;

Впровадити спеціальні заходи для гостей, такі як:

Надання одноразових наклейок для закриття камер смартфонів;

Перевірка речей на наявність пристроїв для зчитування інформації;

Інформування гостей про правила поведінки в офісі та покарання за їх недотримання.

5. Запровадити процедури моніторингу для виявлення та ідентифікації будь-яких нових предметів, що з'являються в офісі;

6. Підкресліть важливість дотримання співробітниками протоколів і правил безпеки на цьому етапі.

Другий етап передбачає співпрацю з постачальником технічного обладнання привносить свій набір вразливостей і загроз для безпеки компанії. Для усунення ризиків, пов'язаних з технічним обладнанням, можна впровадити наступні рішення:

Провести ретельне дослідження та належну перевірку репутації та практик безпеки постачальника технічного обладнання перед встановленням партнерства. Обирайте постачальників, які мають добру репутацію у сфері безпеки та надійності;

Впроваджуйте суворий процес перевірки для вибору програмного забезпечення та додатків, щоб переконатися, що вони походять з надійних та авторитетних джерел. Регулярно оновлюйте та виправляйте програмне забезпечення для усунення будь-яких відомих вразливостей;

Застосовуйте суворі заходи контролю доступу, включаючи використання багатофакторної автентифікації, щоб запобігти несанкціонованому доступу до

системи. Регулярно переглядати та оновлювати привілеї доступу користувачів на основі принципу найменших привілеїв;

Впроваджувати заходи шифрування для захисту конфіденційних даних як у стані спокою, так і під час передачі. Це включає шифрування даних на пристроях зберігання та використання захищених протоколів зв'язку для передачі даних;

Використовуйте системи виявлення та запобігання вторгненням для моніторингу та виявлення будь-яких несанкціонованих спроб отримати доступ до системи або порушити її роботу. Регулярно перевіряйте системні журнали та мережевий трафік на наявність підозрілих дій;

Роз'яснюйте працівникам важливість дотримання належної гігієни кібербезпеки, наприклад, уникати підозрілих веб-сайтів і посилань, використовувати надійні та унікальні паролі, а також бути обережними щодо спроб фішингу;

Проводьте регулярні аудити та оцінки безпеки для виявлення вразливостей і прогалин у захисті системи. Негайно усувати будь-які виявлені слабкі місця.

Впроваджуючи ці заходи, компанія може мінімізувати ризики, пов'язані з постачальниками технічного обладнання, та забезпечити безпеку і цілісність своїх систем і даних.

Згадані вами загрози, пов'язані з апаратними атаками, дійсно можуть становити значний ризик для безпеки конфіденційної інформації компанії. Щоб протистояти цим загрозам, розгляньте можливість впровадження наступних рішень:

Впровадьте заходи фізичної безпеки, такі як обмеження доступу до комп'ютерних систем та забезпечення фізичного доступу до конфіденційних зон лише уповноваженому персоналу.

Регулярно перевіряйте та відстежуйте комп'ютерне обладнання на наявність ознак несанкціонованого втручання або підозрілих пристроїв, підключених до нього. Проводьте регулярні перевірки комп'ютерних периферійних пристроїв, у тому числі клавіатур, для виявлення будь-якого несанкціонованого обладнання.

Інформуйте працівників про ризики, пов'язані з апаратними атаками, та розвивайте культуру пильності. Заохочуйте їх повідомляти про будь-які незвичні або підозрілі пристрої чи поведінку, яку вони спостерігають на робочому місці.

Впроваджуйте заходи безпеки для захисту від апаратних атак, наприклад, використовуйте пломби на корпусах комп'ютерів, що перешкоджають несанкціонованому доступу, та безпечні механізми завантаження для виявлення будь-яких несанкціонованих модифікацій системи [16] .

Використовувати рішення для захисту кінцевих точок, які включають функції безпеки на апаратному рівні, такі як захищені процесори або модулі довірених платформ (TPM), які можуть допомогти захистити від несанкціонованого доступу до конфіденційних даних.

Регулярно оновлюйте та виправляйте комп'ютерні системи та програмне забезпечення, щоб усунути будь-які відомі вразливості та забезпечити застосування останніх оновлень безпеки.

Впроваджуйте надійні заходи автентифікації, такі як багатофакторна автентифікація, щоб запобігти несанкціонованому доступу, навіть якщо паролі або натискання клавіш перехоплені.

Розглянути можливість використання технологій, які шифрують дані на апаратному рівні, таких як самошифрувальні диски (SED), для захисту даних у стані спокою від несанкціонованого доступу.

Проводити регулярний аудит безпеки та тестування на проникнення для виявлення та усунення будь-яких вразливостей в апаратному забезпеченні та загальній безпеці системи.

Впроваджуючи ці заходи, компанія може посилити свій захист від апаратних атак і захистити свою конфіденційну інформацію від компрометації. Важливо регулярно оцінювати та оновлювати заходи безпеки, щоб адаптуватися до нових загроз у цьому мінливому середовищі.

Дійсно, виявлення апаратних шпигунських програм має вирішальне значення для забезпечення безпеки даних. Ось кілька методів, які можна застосувати для виявлення таких загроз:

Попередня перевірка пристроїв: Залучайте спеціалістів для перевірки пристроїв перед їх поставкою на наявність можливих апаратних шпигунських програм або шкідливих компонентів. Це може допомогти виявити та зменшити ризики, пов'язані із зараженими пристроями. Також важливо переконатися в надійності та благонадійності постачальників, щоб звести до мінімуму шанси отримати скомпрометоване обладнання;

Паспорт постачальника та перевірка надійності: Створіть паспорт постачальника, що включає детальну інформацію про постачальника, в тому числі про його репутацію та методи забезпечення безпеки. Проводьте ретельні перевірки надійності потенційних постачальників, щоб переконатися в їхній надійності та зменшити ризик отримання заражених пристроїв;

Відділ спостереження та безпеки: Встановіть камери спостереження в критичних зонах і створіть спеціальний відділ безпеки, відповідальний за моніторинг і відстеження підозрілої поведінки співробітників і відвідувачів. Це допоможе виявити будь-яке несанкціоноване втручання в апаратні пристрої та визначити потенційні загрози;

Контрольоване робоче середовище: Впровадьте суворий контроль над робочими місцями співробітників, щоб переконатися, що на їхніх робочих столах немає жодних зайвих предметів. Регулярні перевірки допоможуть виявити будь-яке несанкціоноване обладнання або підозрілі пристрої, які могли бути принесені на робоче місце;

Захищене приміщення для зберігання: Створіть спеціальне захищене приміщення для зберігання серверів, паперових документів, що містять секретні дані, та комп'ютерів, якими користуються керівники відділів. Доступ до цього приміщення має бути обмежений лише для уповноваженого персоналу, а також мають бути впроваджені такі заходи безпеки, як відеоспостереження та контроль доступу;

Поінформованість та навчання працівників: Проінформуйте працівників про ризики апаратного шпигунського програмного забезпечення та важливість

підтримки безпеки даних. Проведіть тренінги з виявлення підозрілих пристроїв або дій та інформування про них відповідного персоналу служби безпеки.

Впроваджуючи ці заходи, компанія може підвищити свою здатність виявляти та зменшувати загрози, спричинені апаратними шпигунськими програмами, тим самим захищаючи свої дані та підтримуючи безпечне робоче середовище. Також слід проводити регулярні оцінки та аудити безпеки для виявлення та усунення будь-яких нових ризиків або вразливостей.

Третій тип загроз становлять постачальники допоміжних програм. Завантаження корпоративної електронної пошти та інших інструментів на комп'ютер може створити вразливість системи. Крім того, існує ймовірність, що антивірусні та оптимізаційні програми для операційної системи можуть містити шкідливе програмне забезпечення.

Загрози:

Всі види шкідливих шпигунських програм;

Програмний кейлоггер;

Оновлення інформації, яка вже заражена;

Спам, фішинг та інші можливі атаки на корпоративну пошту.

Можливі наслідки:

Отримання доступу до корпоративної пошти, крадіжка інформації та віддавання розпоряджень під маскою керівника;

Перехід за невідомими посиланнями може призвести до завантаження вірусу;

Отримання даних співробітників і клієнтів, крадіжка їхніх грошей і шантаж для досягнення певних цілей;

Крадіжка інтелектуальної власності компанії;

Нищівний удар по репутації компанії [17] .

Рішення:

Оцінити ризики, пов'язані з потенційною втратою даних;

Розподілити комп'ютери на основі конкретних даних, з якими вони працюють;

Розробити індивідуальні антивірусні плани дій для кожного комп'ютера, враховуючи типи інформації, що зберігається, потенційні шляхи зараження та ризики, пов'язані зі шкідливими програмами;

Зберігати конфіденційні дані та інтелектуальну власність на ізольованих комп'ютерах, не підключених до зовнішніх мереж;

Встановіть правила користування електронною поштою, обмежте доступ до ризикованих веб-сайтів та забороніть використання електронної пошти в особистих цілях;

Запровадьте обмеження доступу для працівників за допомогою надійної політики безпеки, гарантуючи, що вони мають доступ лише до тих ресурсів, які необхідні для виконання їхніх посадових обов'язків;

Постійно аналізуйте аномалії мережевого трафіку.

Цей етап є особливо важливим, оскільки він надає доступ до широкого спектру інформації, втрата якої може зашкодити існуванню компанії.

Четвертий крок – крадіжка даних через рекрутингові фірми є поширеним методом, який зловмисники використовують для атак на компанії. Такі фірми, як правило, мають великі бази даних, що містять велику кількість інформації про потенційних працівників, включаючи такі конфіденційні дані, як інформація про кредитні картки, сімейний стан, історію працевлаштування та судимості. Щоб зменшити ризики, пов'язані з крадіжкою даних, важливо проявляти обережність при відборі кандидатів на роботу та проводити ретельне навчання співробітників з питань безпеки даних, враховуючи, що соціальна інженерія та людські помилки є поширеними факторами, що сприяють цьому.

загрози:

Несанкціонований доступ до бази даних працівників;

Несанкціонований доступ до бази даних клієнтів.

Рішення:

Використовувати сучасні антивірусні програми з розширеними можливостями виявлення та боротьби з новими шкідливими програмами;

Впроваджувати програми моніторингу мережевої та комп'ютерної активності

для аналізу поведінки системи, дій користувачів та виявлення незвичної або підозрілої активності з генеруванням повідомлень про загрози;

Впровадити суворий контроль над даними постачальників;

Впровадити політику паролів, що включає в себе 16-символьні паролі для адміністраторів та 8-символьні паролі для користувачів;

Обов'язкове використання спеціальних символів та паролів, що не повторюються;

Максимальний термін дії пароля - 90 днів;

Вимоги до складності паролів;

Здійснювати контроль за місцем фізичного зберігання даних компанії;

Вести список системних адміністраторів у постачальників, які мають доступ до систем з даними компанії, із зазначенням їх кількості та імен;

Використовувати шифрування для конфіденційних даних та даних під час передачі;

Регулярно перевіряти та виправляти програмне забезпечення, надане постачальниками, встановлене на комп'ютерах компанії, для забезпечення безпеки та актуальності;

Тестуйте нові програми, оновлення та антивірусне програмне забезпечення на окремій віртуальній машині для перевірки працездатності та виявлення потенційних проблем перед встановленням на всі комп'ютери компанії;

Встановити політику та процедури перегляду політики доступу до системи постачальника для діючих та колишніх співробітників, включаючи зміну або анулювання облікових записів та паролів, забезпечення обізнаності співробітників та проведення регулярних перевірок;

Перегляньте політику постачальника щодо безпеки портативних пристроїв та ноутбуків;

Ознайомтеся з процедурами безпеки бездротового зв'язку та можливостями моніторингу постачальника;

Регулярно створюйте резервні копії всіх важливих даних;

Періодично перевіряйте та оновлюйте брандмауери та антивірусне програмне забезпечення постачальників для забезпечення ефективності;

Регулярно переглядайте права доступу до "критично важливих" файлів;

Розробити письмовий та протестований план аварійного відновлення, а також процедури повідомлення про потенційні ризики;

Перед укладанням контракту з постачальником створіть паспорт постачальника, що містить наступну інформацію:

Назва компанії;

Дати початку та закінчення співпраці (підписаний договір);

Відділи, які співпрацюють з постачальником;

Інформація про компанію, якою керує постачальник і до якої має доступ;

Список постачальників, з якими співпрацює постачальник;

Перелік компаній, з якими постачальник працював або працює в даний час;

Інформація про методи захисту інформації, які застосовує постачальник;

Згода на проведення аудиту постачальника фахівцями компанії-користувача;

Проведення оцінки ризиків для виявлення потенційних загроз для компанії та розробка індивідуальних сценаріїв інформаційної безпеки для кожного комп'ютера з акцентом на виявлення вразливостей, можливих атак та використання методів антивірусного захисту;

Забезпечення належного знищення та видалення інформації для запобігання несанкціонованому доступу;

Встановити процедури обробки інцидентів для ефективного реагування на інциденти безпеки;

Використовувати віртуальні приватні мережі (VPN) для підвищення конфіденційності та цілісності даних під час передачі через відкриті канали зв'язку. VPN створюють зашифровані з'єднання між комп'ютерами, зменшуючи ризики зловживань та злому;

Проводити регулярні аудиторські перевірки компаній-постачальників для оцінки їхніх заходів безпеки;

Регулярно оновлювати паролі для посилення безпеки;

Посилити відділ інформаційної безпеки компанії для постійного вдосконалення та захисту веб-серверів від потенційних загроз у ланцюгу постачання. Розгляньте наступні варіанти:

Захист від завантаження на веб-сайти інфікованих програм, що спричиняють атаки з вимогою викупу та вимагання викупу;

Запобігайте атакам на адміністраторів веб-сайтів шляхом перехоплення паролів, створення масок сайтів і запуску DoS або DDoS-атак, використовуючи вразливості програмного забезпечення;

Будьте пильними щодо потенційних загроз від існуючих шпигунських програм у компанії, оскільки зловмисники можуть знати оптимальний час атаки та використовувати заражене програмне забезпечення;

Протидіяти загрозам, пов'язаним зі створенням апаратного та програмного забезпечення, в тому числі запобігати несанкціонованому копіюванню та розповсюдженню серед роздрібних продавців.

Загроза:

Неякісне виготовлення продукції, що призводить до втрати репутації компанії.

Рішення:

Проведення аудиту виробничих процесів для забезпечення дотримання стандартів якості.

Здійснювати ретельні перевірки перед випуском продукції на ринок [18] .

2.3. Оцінка ризиків, пов'язаних з певною загрозою

Ступінь небезпеки загрози можна розрахувати, розглядаючи п'ять аспектів оцінки:

1. Важливість інформації: Оцінка важливості інформації, що знаходиться під загрозою. Якщо є кілька варіантів, визначте пріоритетність цінності, пов'язаної з найбільш важливою інформацією, як зазначено в Таблиці 2.1.

2. Кількість заходів для виявлення та запобігання: Оцінка кількості доступних заходів для виявлення та запобігання атакам;

3. Складність шляху атаки: Оцінка складності шляху, яким повинен пройти зловмисник, щоб отримати цільову інформацію;

4. Ризик фальшивих облікових записів співробітників: Розгляд потенційного ризику для компанії, якщо зловмисник використовує фальшивий обліковий запис співробітника;

5. Кількість працівників з доступом та їхні ризики: визначення кількості працівників з доступом до відповідного комп'ютера та оцінка потенційного ризику, пов'язаного з їхньою участю в атаках.

Включивши ці п'ять аспектів у формулу, можна розрахувати комплексну оцінку небезпеки загрози.

Таблиця 2.1

Цінність інформації, яку втратимо в результаті успішної атаки

Інформація	Показник цінності
Не зашифровані персональні дані	5
Зашифровані персональні дані	4
Не зашифровані дані, що є інтелектуальною власністю компанії	5
Зашифровані дані, що є інтелектуальною власністю компанії	4
Паролі входу в комп’ютер	3
Паролі входу в базу даних, папку з секретною інформацією і т.д.	5
Паролі входу в корпоративну пошту	4
Інформація, потрібна зловмиснику для побудови стратегії атаки	1
Інформація про постачальників	2

Для посилення захисту від атак можна досягти меншої ймовірності, визначивши повний набір можливих дій для виявлення та зупинки атаки, наприклад, 20 дій. Додавши до цього числа 1, ми отримаємо показник, який можна

використовувати у формулі. Такий підхід дозволяє створити більш міцний і надійний механізм захисту від атак.

У таблиці 2.2 показано відносну складність шляху атаки, необхідного для отримання бажаної інформації. Рівень складності досягнення цілі безпосередньо впливає на ймовірність реалізації загрози. Наприклад, якщо вірус проникає в систему, він повинен виконати певні дії, такі як підбір пароля або пошук потрібного каталогу. Чим більша кількість цих дій, тим вища ймовірність виявлення аномальної поведінки на комп'ютері-мішені. Отже, з'являється більше часу для виявлення та зупинки атаки.

Таблиця 2.2

Складність шляху атаки для отримання інформації.

Шлях атаки	Відносна складність
Перейти в даному комп’ютері в певну директорію	4
Перейти в даному комп’ютері в певну директорію з паролем	3
Перейти з даного комп’ютера на інший	4
Перейти в базу даних	2
Потрапити в комп’ютер, сейф, т.д.	5
Потрапити на сервер	2
Потрапити у комп’ютер директора	1
Потрапити у комп’ютер керівника відділу захисту інформації	1

Оцінка ризику, пов'язаного з працівником, має вирішальне значення через те, що люди помиляються і можуть вчиняти навмисні або ненавмисні дії, які можуть призвести до комп'ютерних злочинів. Помічено, що до 80% таких злочинів пов'язані з внутрішніми порушеннями, вчиненими працівниками, як навмисно, так і ненавмисно, в тому числі тими, хто звільнився.

Для оцінки ризику, пов'язаного з працівником, можна використовувати таблицю 2.3. Кожен пункт таблиці слід оцінити, щоб визначити, наскільки він має відношення до особи, яка оцінюється [19] .

Таблиця 2.3

Тест, що складається для кожного співробітника.

Факти	Так(1) / Ні(0)
Наявність сім’ї 1	1
Працював в компанії конкурента	1
Невідомі причини звільнення з попереднього місця роботи	1
Наявність судимості	0
Наявність залежностей (ігроман, наркоман)	0
Наявність психічних захворювань	0
Наявність кредитів, боргів	0
Наявність високої посади	1

Для оцінки ризику, пов'язаного з працівником, можна створити таблицю, в якій кожному пункту присвоюється 1 бал за відповідь "так". Спочатку кожен пункт починається зі значення 1. Після заповнення таблиці шляхом підсумовування всіх балів отримують загальну оцінку ризику для співробітника.

Щоб розрахувати ймовірність зради співробітника, який заповнив таблицю, розділіть загальну кількість балів на кількість фактів плюс 1. Наприклад, якщо в таблиці 4 пункти, розрахунок буде (4 + 1) / 9 ≈ 0,55.

Щоб врахувати кількість працівників, які мають доступ до комп'ютера, де може бути реалізована загроза, визначимо "k" як кількість таких працівників.

Використовуючи цю інформацію, ми можемо вивести наступну формулу. Якщо k = 1, то маємо скорочену формулу:

$$R = \Sigma A_{3i=1} + (P(h) * 100\%) \; 5 \; (2.1)$$

де, A_1 – цінність інформації;

q – кількість дій;

max – максимальна кількість дій для захисту інформації існує, для виявлення та зупинення атаки;

A_2 – показник кількості дій, потрібних для виявлення та зупинення атаки;

$A_2 = q \ mod(max+1)$

A_3 – складність шляху атаки;

h – подія, коли співробітник активував загрозу;

$P(h)$ – ймовірність зради компанії співробітником;

Якщо $k > 1$, то :

$h1$ – подія, коли співробітник 1 активував загрозу;

$h2$ – подія, коли співробітник 2 активував загрозу;

$h3$ – подія, коли співробітник 3 активував загрозу;

І т.д., в залежності від кількості співробітників, які мали доступ до комп'ютера, де може бути реалізована загроза.

$P(h1)$ – ймовірність події h1, аналогічно $P(h2)$, $P(h3)$ і т.д..

$P(\overline{h1}) = 1 - P(h1)$ – ймовірність не здійснення події $h1$, аналогічно $P(\overline{h2})$, $P(\overline{h3})$ і т.д.. Тоді потрібно знайти ймовірність події h, коли хтось один атакує.

$$h=\overline{h1}\cdot h2\cdot\overline{h3}+h1\cdot\overline{h2}\cdot h3+\overline{h1}\cdot\overline{h2}\cdot\overline{h3}\ 52$$

Застосовуючи теореми додавання і множення, ймовірність настання події h можна обчислити за формулою:

$$P(h) = P(\overline{h1}) \cdot P(h2) \cdot P(\overline{h3}) + P(\overline{h1}) \cdot P(h2) \cdot P(h3) + P(h1) \cdot P(\overline{h2}) \cdot P(\overline{h3})$$

Підставивши цю формулу в (2.1), коли доступ до комп'ютера має більше одного співробітника, ми можемо розрахувати ймовірність загрози.

Наприклад, маючи такі вхідні дані:

Зловмисник отримав віддалений доступ до комп'ютера, до якого мають доступ троє співробітників, один з яких є членом сім'ї.

Другий працівник працював у компанії-конкурента.

Третій працівник - член сім'ї, який займає високу посаду.

Тепер ми можемо застосувати формулу для розрахунку ймовірності.

$$A_1 = 4,\ q = 7,\ max = 20,\ A_3 = 3$$

$$P(h1) = (1+1)/9 = 0.22 \qquad P(\overline{h1}) = 1 - 0.22 = 0.88$$

$$P(h2) = (1+1)/9 = 0.22 \qquad P(\overline{h2}) = 1 - 0.22 = 0.88$$

$$P(h3) = (1+2)/9 = 0.33 \qquad P(\overline{h3}) = 1 - 0.33 = 0$$

$$R = A\,1 + q_{mod}(max+1) + A\,3 + (P(\overline{h1}) \cdot P(\overline{h2}) \cdot P(h3) + P(\overline{h1}) \cdot P(h2) \cdot P(\overline{h3}) + P(h1) \cdot P(\overline{h2}) \cdot P(\overline{h3})) * 100\%$$

$$R = (4 + 7 mod 21 + 3) + (0.88 \cdot 0.88 \cdot 0.33 + 0.88 \cdot 0.22 \cdot 0.77 + 0.22 \cdot 0.88 \cdot 0.77) * 100\%5 = (21 + (0.25 + 0.15 + 0.15) * 100\%) = \mathbf{76/5 = 15.2}$$

Щоб визначити ступінь успішності впровадження, необхідно оцінити загрозу, використовуючи як мінімальний, так і максимальний сценарії даних. Модель спеціально розроблена для захисту інформації підприємства від атак на ланцюги поставок і узгоджується з існуючою політикою безпеки. Тому запропоновані рішення спрямовані на адаптацію політики безпеки для протидії атакам на ланцюги поставок. Однак, оскільки ці атаки використовують вразливості, впровадження цих рішень підвищує загальну ефективність будь-якої політики безпеки за рахунок усунення та пом'якшення потенційних слабких місць [20].

2.4 Особливості щодо впровадження захисної моделі

Модель складається з чотирьох основних елементів: створення паспорта постачальника, проведення перевірок співробітників компанії, формування

позитивної корпоративної культури та розробка антивірусного плану дій. Ці заходи мають вирішальне значення, оскільки минулий досвід показав, що довіра до постачальників становить ризик для компанії. Якщо постачальник нехтує безпекою власної організації, це може призвести до втрати репутації, втрати партнерів та фінансових наслідків для всіх учасників. Тому вкрай важливо проактивно запобігати атакам на постачальників. У разі атаки постачальник повинен нести відповідальність за свої дії, а компанія повинна розробити комплексний план дій для запобігання виникненню подібних проблем у майбутньому.

Другий аспект передбачає ретельну перевірку потенційних працівників. Внутрішні порушення, скоєні працівниками, становлять до 80% усіх комп'ютерних злочинів. Оскільки люди можуть мати різні мотиви, важливо вивчити конкретні фактори, що впливають на їхнє минуле. Наприклад, якщо людина має діагноз, який може призвести до втрати самоконтролю або бажання помститися через звільнення, вона становить потенційну загрозу для компанії.

Третій аспект передбачає пріоритетність психологічного благополуччя працівників. Робота в умовах високого тиску під суворим наглядом може призвести до відрази до роботи та зниження продуктивності. Щоб сприяти згуртованості колективу та зменшенню стресу, компанії можуть використовувати методи командоутворення, такі як заохочення, надання відпусток та запровадження гнучких графіків роботи, які передбачають нетрадиційний робочий час.

Четвертий аспект передбачає розробку та налаштування індивідуальних сценаріїв антивірусного захисту для кожного типу інформації, що зберігається в системі. Такий підхід допомагає зменшити потенційні вразливості, які можуть виникнути, якщо покладатися лише на стандартні налаштування безпеки. Пристосовуючи антивірусний захист до конкретних категорій даних, компанія може підвищити загальний рівень безпеки [21] .

Щоб ефективно впровадити цю модель у компанії, необхідно зробити кілька кроків:

1. Провести комплексну оцінку всіх ділянок комп'ютерної системи для виявлення потенційних загроз.

2. Оцінити ймовірність успішної реалізації кожної виявленої загрози за формулою (2.1).

3. Впровадити рекомендовані рішення для мінімізації виявлених загроз.

4. Після модифікації системи переоцінити загрози з початкового списку та ранжувати їх у порядку спадання за ймовірністю реалізації.

5. Підтримувати пильний моніторинг загроз, які становлять найвищий рівень ризику для системи, оскільки їх ймовірність виникнення не може бути повністю усунена [22] .

Висновки до розділу 2

Схема атаки на ланцюг поставок була ретельно вивчена, і на кожному етапі були виявлені слабкі місця. Щоб створити надійну модель захисту, ми оцінили кожен етап атаки, визначили ключові ризики та розробили низку заходів для виявлення, зупинки та пом'якшення наслідків атаки на її початкових етапах. Вивчивши найбільш небезпечні атаки, було виділено п'ять ключових ознак атак на ланцюги поставок. Використовуючи ці знання, було створено формулу для оцінки рівня загрози, яку становить конкретна атака. Ця формула може бути універсально застосована для оцінки всіх загроз і стратегічного впровадження запропонованих підходів до захисту.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВІД АТАК НА ЛАНЦЮГ ПОСТАЧАННЯ

Подивимось вже створену політику безпеки, проаналізуємо скільки запропонованих рішень можна втілити для її покращення та оцінимо їх ефективність.

Політика інформаційної безпеки розроблена відповідно до:

– закону України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 № 80/94-ВР;

– постанови Кабінету Міністрів України від 27.11.98 № 1893 “Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію”;

– постанови Кабінету Міністрів України від 29.03.2006 № 373 “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах”;

– державних стандартів України в галузі технічного захисту інформації

3.1. Розгляд існуючої політики безпеки

Розглянемо вже існуючу політику безпеки у таблиці 3.1.

Таблиця 3.1

Політика безпеки.

№	Положення політики інформаційної безпеки
1.	Встановлення замків на вхідних дверях для забезпечення надійного закриття приміщень у неробочий час є ефективним заходом фізичної безпеки, який допомагає запобігти несанкціонованому доступу.
2.	Оснащення приміщень охоронною та пожежною сигналізацією підвищує загальний рівень безпеки.

Продовження таблиці 3.1

3.	Забезпечення відповідності розміщення обладнання вимогам безпеки, санітарії та пожежної безпеки має вирішальне значення для підтримання безпечного та нешкідливого робочого середовища.
4.	Зберігання запасних ключів від серверної кімнати в опечатаному пеналі в сейфі керівника РПО забезпечує додатковий рівень фізичної безпеки та обмежує доступ до неї лише уповноваженому персоналу.
5.	Підключення корпоративної мережі до Інтернету через брандмауер є критично важливим заходом безпеки, який допомагає контролювати та моніторити вхідний та вихідний мережевий трафік.
6.	Застосування фільтрів брандмауера для регулювання мережевого трафіку підвищує безпеку, блокуючи спроби несанкціонованого доступу та відфільтровуючи потенційно шкідливий вміст.
7.	Адміністрування брандмауера локально або віддалено з фіксованої адреси адміністратора допомагає забезпечити безпечне управління брандмауером.
8.	Закриття невикористовуваних служб і протоколів у конфігурації брандмауера та регулярне оновлення його програмного захисту є ефективними заходами для мінімізації потенційних векторів атак
9.	Надання користувачам доступу до Інтернету тільки через брандмауер допомагає забезпечити дотримання політик безпеки, а також дозволяє здійснювати моніторинг і фільтрацію інтернет-трафіку.
10.	Ведення детальних системних журналів усіх сеансів роботи брандмауера та обмеження доступу до них обмеженою кількістю авторизованих співробітників допомагає ефективно відстежувати та розслідувати інциденти безпеки.

Продовження таблиці 3.1

11.	Ведення "стоп-листів" інтернет-ресурсів із сумнівним вмістом і дозвіл на завантаження лише дозволених програм через брандмауер є ефективними заходами контролю та обмеження доступу до потенційно шкідливого або несанкціонованого контенту.
12.	Встановлення всіх рекомендованих патчів для операційних систем і серверного програмного забезпечення допомагає захиститися від відомих вразливостей і зміцнює загальну систему безпеки.
13.	Встановлення всіх рекомендованих патчів для операційних систем і серверного програмного забезпечення допомагає захиститися від відомих вразливостей і зміцнює загальну систему безпеки.
14.	Обмеження доступу до Інтернету лише через брандмауер компанії допомагає впроваджувати політику безпеки та забезпечує контрольований і відстежуваний шлюз для підключення до Інтернету.
15.	Впровадження механізму перевірки на наявність вірусів і троянських коней для кожного завантаженого файлу допомагає запобігти впровадженню шкідливого програмного забезпечення в мережу і системи.
16.	Заборона користувачам встановлювати та використовувати зовнішні поштові сервери без спеціального дозволу допомагає підтримувати контроль над інфраструктурою електронної пошти та мінімізувати потенційні ризики безпеки.
17.	Забезпечення того, щоб електронні документи, які містять службову інформацію, не надсилалися електронною поштою відкритими каналами в незашифрованому вигляді, підвищує конфіденційність даних і захист від несанкціонованого доступу.

Продовження таблиці 3.1

18.	Примусове використання авторизованих поштових програм, визначених адміністратором мережі, допомагає підтримувати стандарти безпеки та забезпечує сумісність із заходами безпеки, впровадженими в мережі.
19.	Обмеження використання електронної пошти компанії авторизованими співробітниками та заборона відвідувачам або тимчасовим працівникам користуватися нею допомагає захистити конфіденційну інформацію та зберегти контроль над каналами зв'язку.
20.	Налаштування поштових серверів на відхилення листів, які не адресовані на домен компанії, допомагає запобігти спаму та несанкціонованому спілкуванню електронною поштою.
21.	Покладання відповідальності за нагляд за виконанням заходів інформаційної безпеки при роботі в Інтернеті та використанні електронної пошти на мережевого адміністратора забезпечує належне управління та контроль за практиками безпеки в цих сферах.
22.	Наявність антивірусного контролю на всіх робочих станціях з автоматичним періодичним оновленням антивірусних баз забезпечує безперервний захист від відомих загроз шкідливого програмного забезпечення.
23.	Обмеження використання спільних дискових ресурсів на робочих станціях винятковими випадками знижує ризик несанкціонованого доступу або випадкового витоку конфіденційних даних.
24.	Дозвіл на використання знімних носіїв інформації та USB-портів на робочих станціях лише у виняткових випадках допомагає запобігти впровадженню шкідливого програмного забезпечення або несанкціонованій передачі даних.

Продовження таблиці 3.1

25.	Обмеження використання персональних комп'ютерів і мережевих ресурсів компанії службовими обов'язками допомагає мінімізувати можливість зловживань або несанкціонованого доступу до конфіденційної інформації.
26.	Зберігання робочих матеріалів і документів в електронному вигляді у визначеному каталозі файлового сервера полегшує централізоване управління, резервне копіювання та контроль доступу, підвищуючи безпеку та доступність даних.
27.	Блокування робочої станції при короткочасному відлученні з робочого місця запобігає несанкціонованому доступу до робочої станції та захищає конфіденційні дані.
28.	Вимкнення робочої станції, коли ви залишаєте робоче місце на тривалий час, знижує ризик несанкціонованого доступу, економить енергію та допомагає підтримувати цілісність системи.
29.	Заборона використання чужих даних доступу для входу в комп'ютерну мережу компанії забезпечує підзвітність і запобігає несанкціонованому доступу.
30.	Не залишати підключену та розблоковану робочу станцію без нагляду зменшує ризик несанкціонованого доступу або втручання в роботу робочої станції та її дані.
31.	Заборона відключення встановленого антивірусного програмного забезпечення та зміни його налаштувань забезпечує безперервний захист від шкідливого програмного забезпечення та підтримує цілісність заходів безпеки.
32.	Заборона завантаження програмного забезпечення з Інтернету допомагає мінімізувати ризик потрапляння потенційно шкідливого або несанкціонованого програмного забезпечення в мережу та на робочі станції.

33.	Заборона ділитися правами доступу до комп'ютера з іншими особами забезпечує підзвітність і запобігає несанкціонованому доступу або зловживанню обліковими записами користувачів.
34.	Заборона самостійного внесення змін до апаратної чи програмної конфігурації робочих станцій допомагає підтримувати цілісність, сумісність та безпеку системи.
35.	Заборона користувачам встановлювати програмне забезпечення на робочі станції допомагає підтримувати контроль над цілісністю, ліцензуванням та безпекою програмного забезпечення.
36.	Визнання того, що паролі користувачів є приватною інформацією, призначеною для ідентифікації, підкреслює важливість збереження та захисту цієї конфіденційної інформації.
37.	Зберігання паролів адміністратора та серверних паролів у запечатаних конвертах у сейфі, причому кожен пароль в окремому конверті, додає додатковий рівень безпеки та контролю над привілейованим доступом.
38.	Впровадження механізму, коли операційні системи серверів і робочих станцій блокують доступ до мережі після певної кількості помилок при введенні пароля, підвищує безпеку і допомагає запобігти несанкціонованому доступу.
39.	Видалення імені користувача з інформаційної системи підприємства при звільненні працівника на підставі обхідного листа забезпечує оперативне відкликання прав доступу після припинення трудових відносин.
40.	Блокування імені користувача в інформаційній системі підприємства на час відпустки співробітника на підставі заяви керівника структурного підрозділу допомагає зберегти безпеку даних і запобігти несанкціонованому доступу під час відсутності співробітника.

Продовження таблиці 3.1

41.	Захист активного мережевого обладнання (маршрутизаторів, комутаторів) унікальними паролями запобігає несанкціонованому переналаштуванню та забезпечує цілісність і безпеку мережевої інфраструктури.
42.	Заборона адміністраторам різних інформаційних систем використовувати адміністративний пароль для неадміністративних завдань і виділення окремого пароля з правами користувача підвищує безпеку і знижує ризик зловживань або випадкових змін.
43.	Налаштування операційних систем робочих станцій на активацію захищених паролем заставок під час пауз у роботі, з максимальним часом активації 15 хвилин, допомагає захистити конфіденційну інформацію та запобігти несанкціонованому доступу за відсутності користувача.
44.	Налаштування серверних операційних систем таким чином, щоб обмежити доступ до парольної інформації, обмеживши його адміністратором і керівником служби інформаційної безпеки, допомагає захистити конфіденційні облікові дані і знизити ризик несанкціонованого доступу до паролів користувачів.
45.	Налаштування операційних систем робочих станцій в комп'ютерній мережі підприємства на заборону перегляду введеної парольної інформації підвищує конфіденційність паролів і посилює захист від потенційного несанкціонованого доступу.
46.	Впровадження політики закінчення терміну дії паролів, наприклад, заміна паролів кожні 90 днів на нові, які раніше не використовувалися, сприяє регулярному оновленню паролів і знижує ризик компрометації облікових даних через їх тривале використання.

Продовження таблиці 3.1

47.	Роздруківка конфігураційних файлів при створенні копій - це захід, що вживається для забезпечення резервного копіювання даних у випадках, коли створення електронних копій є неможливим. Зберігання резервних копій до тих пір, поки вони не втратять актуальність, забезпечує доступність попередніх конфігурацій у разі потреби.
48.	Створення резервних копій на знімних носіях, таких як машинні носії, після початкової конфігурації або змін у серверних операційних системах, серверному програмному забезпеченні та мережевому обладнанні допомагає захистити від втрати даних і полегшує відновлення системи в разі збоїв або помилок.

3.2. Створення набору рішень, які покращать ефективність роботи політики безпеки, та які відповідають політиці безпеки

Ось кілька пропонованих рішень для підвищення ефективності політики безпеки:

1. Залучити професійного фахівця для виявлення потенційних підслуховуючих пристроїв, жучків, камер у приміщенні та на телефонах;
2. Встановити металодетектори на вході до офісу для ідентифікації предметів та впровадити систему контролю доступу для працівників та відвідувачів;
3. Обмежити доступ до приміщень компанії незареєстрованим користувачам. Впровадити спеціальні заходи для осіб, які класифікуються як гості;
4. Заклеїти одноразовими наклейками камери смартфонів;
5. Проводити перевірку особистих речей на наявність пристроїв для зчитування інформації;
6. Інформувати співробітників про правила поведінки в офісі та можливі наслідки їх порушення;
7. Контролювати та регулярно перевіряти офіс на наявність нових предметів;
8. Проводити перевірку обладнання перед встановленням в офісі;

9. Створити паспорт постачальника для забезпечення контролю якості та безпеки його продукції;

10. Встановіть камери спостереження та створіть відділ безпеки для контролю за діяльністю співробітників;

11. Впровадити контроль на робочих місцях, забезпечити відсутність зайвих предметів на столах працівників;

12. Розподілити комп'ютери за типами даних та розробити спеціальні антивірусні сценарії для кожного комп'ютера;

13. Для зберігання інтелектуальної власності компанії використовувати окремий комп'ютер, відключений від інтернету та інших пристроїв. Запровадити обмеження доступу для співробітників;

14. Проводити пошук файлів та оцінювати ризик, який кожен співробітник становить для компанії;

15. Регулярно проводити курси з інформаційної безпеки для співробітників, акцентуючи увагу на критично важливих протоколах безпеки;

16. Організовувати заходи, спрямовані на створення позитивної атмосфери та сприяння комфортному робочому середовищу для всіх співробітників;

17. Періодично нагадувати співробітникам про правила компанії, включаючи такі аспекти, як чистота робочих поверхонь, заборона фотографування в офісі та пильність щодо незвичних предметів;

18. Сприяти та підтримувати чистоту робочих поверхонь;

19. Заборонити фотографувати в офіс;.

20. Заохочувати пильність до наявності незвичних предметів в офісі;

21. Використовувати програмне забезпечення, яке відстежує мережеву та системну активність, виявляючи та повідомляючи про ненормальну поведінку;

22. Впровадити засоби контролю для управління даними про постачальників;

23. Скласти вичерпний список системних адміністраторів, відповідальних за управління системами, пов'язаними з постачальниками, що містять дані компанії, із зазначенням їхніх імен та контактних даних;

24. Регулярно перевіряти та встановлювати патчі до програмного забезпечення постачальників, встановленого на комп'ютерах компанії, для оперативного усунення потенційних вразливостей та проблем;

25. Тестувати нові програми та оновлення на окремій віртуальній машині, перш ніж інтегрувати їх у систему компанії;

26. Ознайомтеся з політикою управління доступом до систем постачальника, включаючи процедури зміни або анулювання імен користувачів та паролів як для працюючих, так і для тих, хто вже вийшов на пенсію. Переконайтеся, що всі співробітники розуміють і дотримуються цієї політики;

27. Оцініть політику постачальника щодо безпеки портативних пристроїв та ноутбуків;

28. Перевірте процедури безпеки бездротової мережі та можливості моніторингу постачальника;

29. Переконайтеся, що постачальники оновлюють брандмауери та антивірусне програмне забезпечення до найновіших версій в рамках регулярних аудитів. 30. Регулярно переглядайте права доступу до критично важливих файлів;

31. Розробити та протестувати письмовий план аварійного відновлення та створити систему оповіщення про потенційні ризики;

32. Впровадити надійну політику використання паролів;

33. Проводити оцінку ризиків для компанії в разі виникнення загрози та розробляти індивідуальні сценарії безпеки для кожного комп'ютера з урахуванням рівня ризику та потенційних атак, використовуючи антивірусні методи захисту інформації;

34. Налагодження процесів реагування на інциденти;

35. Проводити регулярні аудиторські візити до компаній постачальників;

36. Постійно вдосконалювати та модернізувати відділ інформаційної безпеки компанії;

37. Ретельно тестувати продукти перед їх випуском.

3.3. Оцінка ефективності запропонованих методів

Якщо припустити, що політика безпеки має 48 однаково важливих пунктів і претендує на 100% ефективність, то при наявності 37 альтернативних рішень, що відхиляються від політики, приблизне збільшення ефективності політики безпеки становитиме близько 77,08%. Оцінка загроз дозволяє більш точно оцінити ефективність рішення і зменшити ймовірність того, що кожен пункт буде під загрозою. Слід зазначити, що цей розрахунок слугує доказом ефективності моделі за умови, що жодна політика безпеки не може гарантувати 100% захисту.

Висновки до розділу 3

Запропонована модель була впроваджена з метою підвищення ефективності політики безпеки для пом'якшення наслідків атак на ланцюги поставок. Це було досягнуто шляхом впровадження додаткових заходів безпеки, які зменшили ймовірність успішної атаки. Хоча досягнення абсолютної надійності системи недосяжне, можна підвищити її стійкість, тим самим зменшивши вразливість до атак на ланцюги поставок. Загалом, використання цієї моделі виявляється корисним для захисту від таких атак у ланцюгу поставок.

ВИСНОВКИ

У бакалаврській роботі детально досліджено концепцію ланцюга постачання та пов'язані з нею атаки. Надання детального уявлення про основні схеми атак, їх операційні характеристики, методи захисту від атак, а також пролила світло на нові загрози та стратегії зловмисників.

Основні результати дослідження включають:

- Виявлення основних вразливостей, присутніх в політиці безпеки.
- Виявлення основних системних загроз, які зловмисники можуть використовувати для здійснення атак.
- Розробка ефективних методів захисту для мінімізації виявлених загроз.
- Проведення ретельної оцінки загроз.
- Ідентифікація та розмежування основних етапів атаки на ланцюг постачання.

Було проаналізовано реальні випадки атак на ланцюги постачання та висвітлено вразливість постачальників у цій системі. Було виявлено, що постачальники часто не знають про те, що вони є потенційними векторами атак. Для зменшення ризику атак на постачальників були розроблені різні заходи, включаючи створення паспорта постачальника та регулярні аудити. Здійснюючи контроль над постачальниками, стає можливим запобігти атакам на ланцюги поставок на початковому етапі, оскільки постачальники не завжди застосовують усі доступні заходи безпеки для захисту конфіденційної інформації.

Враховуючи, що 80% атак пов'язані з людським фактором, в дипломній роботі визнано важливість оцінки персоналу на предмет ризику крадіжки інформації або компрометації системи як частини захисних заходів. Кожна особа в організації може мати мотиви, які можуть призвести до підривних дій, включаючи шантаж співробітників, хабарництво, незадоволеність роботою або інші фактори, які потенційно можуть призвести до зради. Тому проведення оцінки ризиків для визначення потенційної загрози, яку становлять співробітники, набуває

вирішального значення, оскільки вони мають доступ до секретної інформації або можливість інфікувати критичні системи. Крім того, важливим і часто недооціненим фактором посилення загальної безпеки є розвиток командної роботи серед співробітників.

Для оптимального захисту від конкретної загрози, спрямованої на конкретний комп'ютер, важливо розробити антивірусний сценарій, який враховує типи даних, що зазвичай обробляються на комп'ютері, і потенційні загрози, які можуть виникнути. Такий підхід допомагає уникнути потенційних вразливостей системи, які можуть виникнути в результаті використання всіх доступних функцій для загального захисту. Використовуючи спеціально розроблений сценарій для даного комп'ютера, можна досягти більш ефективного захисту, забезпечуючи цілеспрямований і індивідуальний механізм захисту.

Під час дослідження атак на ланцюги поставок ретельно було вивчено та визначено потенційні вразливі місця в ланцюгу поставок. Систематично визначено загрози, які можуть виникнути на кожному етапі ланцюга, і розроблено високоефективні методи захисту для зменшення цих ризиків. Крім того, вдосконалено існуючі механізми захисту та розроблено власну формулу для точної оцінки рівня загрози від конкретних атак. Використовуючи ці результати, побудовано та оцінено комплексну модель захисту від атак на ланцюги поставок. Також надано практичні рекомендації щодо впровадження цієї моделі для підвищення загальної інформаційної безпеки в інформаційній системі компанії.

Результати дослідження демонструють ефективність моделі захисту та вдосконалень, внесених до існуючої політики безпеки. В цілому, дослідження успішно підвищило рівень захисту інформації в інформаційній системі підприємства, тим самим забезпечивши вищий ступінь безпеки критично важливих активів і даних.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Blackmer M. Attacking the Weakest Link in the Supply Chain URL: https://blogs.cisco.com/security/attacking-the-weakest-link-in-the-supply-chain?dtid=osscdc000283. (дата звернення: 19.07.2019)

2. Panda Security. Supply chain attack: риски для предприятий от атак на цепочку URL:https://www.cloudav.ru/mediacenter/news/business-risks-supply-chain-attacks/.(дата звернення: 12.08.2019)

3. ЛУГАНОВСЬКА Є. GDPR в Україні: стратегічний план чи необдумане рішення? URL:https://delo.ua/business/gdpr-v-ukrajini-strategichnij-plan-chi-neobduman-348025/ . (дата звернення: 19.04.2019)

4. Pankov N. Не станьте звеном в атаке через цепочку поставок URL:https://www.kaspersky.ru/blog/ccleaner-supply-chain/20045/ . (дата звернення: 10.02.2020)

5. CCleanup: A Vast Number of Machines at Risk URL:https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html . (дата звернення: 21.07.2019)

6. Нова хвиля кібератак в Україні може поширитись через сайт розробника ПЗ для бухобліку - експерти Детальніше читайте на УНІАН: URL: https://www.unian.ua/science/2095776-nova-hvilya-kiberatak-v-ukrajini-moje-poshiritis-cherez-sayt-rozrobnika-pz-dlya-buhobliku-. (дата звернення: 19.04.2019)

7. New Ransomware Variant "Nyetya" Compromises Systems Worldwide URL: https://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html. (дата звернення:28.09.2017)

8. Точно в цель - атака на Target URL: https://www.infowatch.ru/analytics/leaks_monitoring/5196.(дата звернення:01.01.2019)

9. Target Hackers Broke in Via HVAC Company URL:https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/..(дата звернення: 01.02.2014)

10. Експерти з кібербезпеки зазначають, що на розшифровування вірусу можуть піти тижні. URL: https://tsn.ua/ukrayina/u-antivirusnoyi-kompaniyi-rozpovili-hto-mozhe-stoyati-za-hakerskoyu-atakoyu-petya-a-i-chim-ce-zagrozhuye-952457.html. (дата звернення: 10.04.2017)
11. В Україні зафіксували наймасштабнішу кібератаку в історії URL: https://tsn.ua/ukrayina/robota-ukrayinskih-komp-yuternih-merezh-bude-povnistyu-vidnovlena-za-kilka-dniv-geraschenko-952460.html. (дата звернення: 16.02.2017)
12. Patrick Moorhead. That Time Of Year Again: Cisco Systems Releases Its Annual Cybersecurity Report URL:https://www.forbes.com/sites/patrickmoorhead/2018/03/05/that-time-of-year-again-cisco-systems-releases-its-annual-cybersecurity-report/#3e35b42518ec. (дата звернення: 16.02. 2018)
13. Information security breaches survey 2013: technical report URL: https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report. (дата звернення: 18.04.2019)
14. Managing Cyber Supply Chain Risks URL: http://www.advisenltd.com/wp-content/uploads/2013_OBPI_SupplyChainCyberRM_Whitepaper.pdf. (дата звернення: 10.03.2020)
15. Cyber-security risks in the supply chain URL: https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf. (дата звернення: 15.04.2019)
16. ROB WAUGH. The terrifying rise of cyber crime: Your computer is currently being targeted by criminal gangs looking to harvest your personal details and steal your money URL https://www.dailymail.co.uk/home/moslive/article-2260221/Cyber-crime-Your-currently-targeted-criminal-gangs-looking-steal-money.html. (дата звернення: 16.19.2020)
17. Supply Chain Risk – the “Cyber Attack” https://www.isg-one.com/industries/consumer-goods/articles/supply-chain-risk-the-cyber-attack. (дата звернення: 16.19.2020)

18. Elia Florio. Attack inception: Compromised supply chain within a supply chain poses new risks URL: https://www.microsoft.com/security/blog/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/.(дата звернення: 26.07.2018)
19. ISO/IEC 28001:2007, Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance.
20. Про захист інформації в інформаційно-телекомунікаційних системах URL: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. (дата звернення: 26.07.2022)
21. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію URL: https://zakon.rada.gov.ua/laws/show/1893-98-%D0%BF. (дата звернення: 26.07.2022)
22. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF. 23. ISO/IEC 27001:2013, Information technology Security Techniques - Information security management systems — Requirements. (дата звернення: 26.07.2021)