МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

“ОРГАНІЗАЦІЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ АНАЛІЗУ ІНЦИДЕНТІВ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Андрій Тюленінов

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Андрій ТЮЛЕНІНОВ

Керівник:
д.е.н., професор Світлана ЛЕГОМІНОВА

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Тюленінову Андрію Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Організація кібербезпеки підприємства на основі аналізу інцидентів"

керівник кваліфікаційної роботи Світлана ЛЕГОМІНОВА, д.е.н., професор
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, інциденти, нормативні документи, стандарти, міжнародні стандарти.*

4. Перелік питань, які потрібно розробити:

1. Проаналізувати проблематику виявлення інцидентів інформаційної безпеки, їх критерії, види, способи та методи реагування на інциденти.
2. Розглянути вплив інцидентів на організацію та важливість ведення статистичного спостереження інцидентів інформаційної безпеки.
3. Розробити рекомендації керівництву підприємства для підвищення ефективності захисту інформаційної безпеки підприємства.
4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	виконано
2.	Збір та аналіз літератури.	15.10.2023	виконано
3.	Аналіз інцидентів інформаційної безпеки підприємства.	25.10.2023	виконано
4.	Причини виникнення інцидентів	11.11.2023	виконано
5.	Рекомендації керівництву підприємства, для підвищення ефективності захисту інформаційної безпеки.	15.11.2023	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	22.11.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ДЕК.	18.01.2024	виконано

Здобувач вищої освіти _____ Андрій ТЮЛЕНІНОВ
(підпис)

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня магістра

Направляється здобувач Тюленінов А.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Організація кібербезпеки підприємства на основі аналізу інцидентів"
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ТЮЛЕНІНОВ Андрій** у кваліфікаційній роботі дослідив сучасний стан організаційних заходів кібербезпеки для підприємства на основі аналізу інцидентів, визначив основні проблеми та розробив пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності діяльності захисту інформаційних систем підприємства. **ТЮЛЕНІНОВ Андрій** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **ТЮЛЕНІНОВА Андрія** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Тюленінов А.С. допускається до захисту роботи в екзаменаційної комісії**.**

Завідувач кафедри
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Тюленінова Андрія Сергійовича
на тему "**ОРГАНІЗАЦІЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ АНАЛІЗУ ІНЦИДЕНТІВ**"

Актуальність Існуючі моделі забезпечення кібербезпеки підприємства передбачають постійний аналіз кібератак з позиції дослідника реалізації кібератак, з позиції атакуючого та моделей, що враховують більш широкий спектр аналітичних підходів. Адаптивні системи безпеки потребують удосконалення організаційних та функціональних аспектів кіберзахисту до, під час та після проведення кібератак. Пошук організаційної моделі кіберзахисту, визначення складових та формулювання основних функцій є предметом постійної уваги. Тому управління інцидентами безпеки та організація роботи команди реагування на кіберінциденти є актуальною в сучасних умовах та підтверджує своєчасність наукових досліджень.

Позитивні сторони

1. Автором детально проаналізувана проблематика виявлення інцидентів інформаційної безпеки, їх критерії, види, способи та методи реагування на інциденти.
2. Розглянуто вплив інцидентів на підприємство та важливість ведення статистичного спостереження інцидентів інформаційної безпеки.
3. Розроблено рекомендації керівництву підприємства для підвищення ефективності захисту інформаційної безпеки підприємства.

Недоліки

1. Робота суттєво виграла б, якщо б була досконало проаналізована сучасна технологія компанії, яка надає послуги по вивченню наслідків інцидентів, або проаналізовані певні форензік інструменти, які застосовуються провідними компаніями на ринку кібербезпеки.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку "**відмінно"**, а здобувач ТЮЛЕНІНОВ Андрій - присвоєння кваліфікації магістр кібербезпеки за спеціалізацією "Управління інформаційною безпекою".

Рецензент: завідувач кафедри
Інформаційної та кібернетичної
безпеки, Галина ГАЙДУР
д.т.н, професор

_____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 93 стор., 14 рис., 2 табл., 19 джерел.

Метою роботи є розробка рекомендацій для підвищення ефективності захисту інформаційної безпеки за рахунок аналізу інцидентів інформаційної безпеки та покращення організаційних заходів групи реагування підприємства на виявлені інциденти.

Об'єкт дослідження - процес управління інцидентами інформаційної безпеки підприємства.

Предмет дослідження - організаційні заходи спрямовані на зменшення ймовірності виникнення інцидентів інформаційної безпеки підприємства.

Методи дослідження. Статистичне спостереження та експеримент, розрахунково – аналітичний, метод критичних сценаріїв.

Короткий зміст роботи. Розглянуто систему реагування на інциденти інформаційної безпеки підприємства, проведено аналіз методів виявлення подій інформаційної безпеки підприємства.

У кваліфікаційній роботі другого вищого рівня вищої освіти магістр розглянуто підходи до визначення подій інформаційної безпеки підприємства з використанням систем виявлення інцидентів інформаційної безпеки та розроблено рекомендації керівництву підприємства щодо підвищення рівня інформаційної безпеки за рахунок виявлених інцидентів інформаційної безпеки.

Галузь застосування. Практична цінність роботи полягає в тому, що запропоновані в роботі рішення можуть бути використані при розробці, впровадженні, експлуатації чи модифікації системи інформаційної безпеки підприємства, нормативних документів та безпеки підприємства в цілому.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА, КОМЕРЦІЙНА ТАЄМНИЦЯ ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПОДІЯ, ІНЦИДЕН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗБИТКИ.

ABSTRACT

The text part of the qualification work for the master's degree: 93 pages, 14 figures, 2 tables, 19 sources.

The purpose of the work is to develop recommendations for increasing the effectiveness of information security protection by analyzing information security incidents and improving the organizational measures of the company's response group to identified incidents.

The object of the study is the process of managing information security incidents of the enterprise.

The subject of the study is organizational measures aimed at reducing the probability of occurrence of information security incidents of the enterprise.

Research methods. Statistical observation and experiment, calculation - analytical, method of critical scenarios.

Brief content of the work. The response system to information security incidents of the enterprise was considered, and the methods of detecting information security events of the enterprise were analyzed.

In the master's qualification work of the second higher level of higher education, approaches to the identification of information security events of the enterprise using information security incident detection systems were considered and recommendations were developed for the management of the enterprise to increase the level of information security at the expense of detected information security incidents.

Field of application. The practical value of the work is that the solutions proposed in the work can be used in the development, implementation, operation or modification of the information security system of the enterprise, regulatory documents and security of the enterprise as a whole.

KEYWORDS: INFORMATION SECURITY, BUSINESS SECRET, INFORMATION SECURITY MANAGEMENT SYSTEM, EVENT, INFORMATION SECURITY INCIDENT, DAMAGES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КТ	-	комерційна таємниця
ІБ	-	інформаційна безпека
ІС	-	інформаційна система
СУІБ	-	система управління інформаційною безпекою
ISO	-	міжнародна організація зі стандартизації (англ. International Organization for Standardization)
IEE	-	міжнародна електротехнічна комісія (The International Electrotechnical Commission)
SIEM	-	система управління інформацією та подіями (Security information and event management)
DLP	-	система попередження витоку конфіденційної інформації (Data Leak Prevention)
ІТ	-	інформаційні технології
ГРІІБ	-	група реагування на інциденти інформаційної безпеки
ОС	-	операційна система
ПК	-	персональний комп’ютер
ПЗ	-	програмне забезпечення

ВСТУП

Безпека конфіденційної інформації полягає у поєднанні систем, процесів і засобів внутрішнього контролю для забезпечення цілісності та конфіденційності даних і робочих процесів в підприємства.

Термін “кібербезпека” стосується технологій і процесів, призначених для захисту комп’ютерних систем, програмного забезпечення, мереж і даних користувачів від несанкціонованого доступу та загроз, які поширюються через Інтернет з боку кіберзлочинців, терористичних груп і хакерів.Кібербезпека - це захист пристроїв і мережі від несанкціонованого доступу або модифікації. Інтернет є не тільки головним джерелом інформації, а й засобом, за допомогою якого люди ведуть бізнес [1].

Сьогодні Інтернет використовується для реклами та продажу товарів, спілкування з клієнтами та продавцями та проведення фінансових операцій.

У цьому контексті хакери та кіберзлочинці використовують Інтернет як інструмент для розповсюдження шкідливих програм і здійснення кібератак.

Метою кібербезпеки є захист комп’ютерів, мереж і програм від таких кібератак.Більшість цих цифрових атак спрямовані на доступ, зміну або видалення конфіденційної інформації. Вимагати від жертви гроші, або порушити нормальну бізнес-операцію.

Проблематика дослідження полягає у тому, що для визначення та підвищення рівня інформаційної безпеки підприємства та захисту інформації, необхідно налаштувати величезну кількість засобів та створити способи визначення інцидентів, реагуваня на події інформаційної безпеки, зокрема проведений аналіз і практичний досвід показують, що в якості основи при забезпеченні безпеки інформації необхідно використовувати міжнародні та вітчизняні нормативні документи. При цьому інформація розглядається як ресурс виявлення подій, які в результаті визначені як інцидент інформаційної безпеки.

Інформаційна безпека має вирішальне значення для всіх підприємств, щоб захистити свою інформацію і вести свій бізнес. Інформаційна безпека визначається як захист інформації і системи, і обладнання, яке використовує, зберігає і передає цю інформацію. Інформаційна безпека виконує чотири важливих для підприємства аспекти: захищає здатність підприємства функціонувати, забезпечує безпечну роботу додатків, реалізованих в IT-системах підприємства, захищає дані, які підприємство збирає та використовує, і, нарешті, захищає технологічні активи, які використовуються на підприємстві. Є також проблеми і ризики, пов'язані з впровадженням інформаційної безпеки на підприємстві. В свою чергу зневага питаннями покращення методів та засобів інформаційної безпеки та захисту інформації може призвести до повного банкрутства. Тому аналіз інцидентів інформаційної безпеки є визначальним при спробах оптимізації системи реагуваня на інциденти та управління ними, що підтверджує актуальність обраної теми кваліфікаційної роботи.

Метою роботи є розробка рекомендацій для підвищення ефективності захисту інформаційної безпеки за рахунок аналізу інцидентів інформаційної безпеки та покращення організаційних заходів групи реагування підприємства на виявлені інциденти.

Об’єкт дослідження - процес управління інцидентами інформаційної безпеки підприємства.

Предмет дослідження - організаційні заходи спрямовані на зменшення ймовірності виникнення інцидентів інформаційної безпеки підприємства.

Методи дослідження. Статистичне спостереження та експеримент, розрахунково – аналітичний, метод критичних сценаріїв.

Практичне значення одержаних результатів: Рівень інформаційної безпеки підприємства напряму впливає на економічну безпеку підприємства. Рекомендації щодо підвищення рівня інформаційної безпеки можуть використовуватися керівниками підприємства для підвищення його конкурентоспроможності, рентабельності, інвестиційної привабливості.

Тому організація та покращення системи управління інформаційної безпеки з урахуванням статистичних даних про інциденти інформаційної безпеки та реагуванню на виявлені інциденти, є, безумовно, актуальною науковою задачею.

За результатами кваліфікаційної роботи проведена апробація на Всеукраїнській науковій конференції “Актуальні проблеми кібербезпеки”, яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

РОЗДІЛ 1.
АНАЛІЗ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Інформаційна безпека - це процес захисту інтелектуальної власності підприємства. Бізнес будується на інформації – на секретах компанії. Цими секретами можуть бути секретні інгредієнти, методи виробництва, цінові угоди з постачальниками або списки клієнтів. Всі ці бізнес-секрети сприяють прибутковості компанії. Всі вони повинні бути надійно захищені. Всі беруть участь у збереженні інформації і в якійсь мірі несуть за неї відповідальність. Однако витік може нашкодити.

Немає простих відповідей на питання безпеки. На жаль, люди занадто часто переконані, що все, що їм потрібно зробити для захисту своїх інформаційних систем, - це встановити брандмауер, поліпшити метод автентифікації або прописати політику безпеки. Але, кожен з них може допомогти підвищити безпеку,однако, жоден з них не панацеєю вирішення проблематики захисту.

Залежність від комп'ютеризованих інформаційних систем є невід'ємною частиною діяльності підприємства. Проблеми, які пов'язані з інформацією, повинні розумітися і управлятися так само, як і будь-який інший бізнес-процес. Керівництво має визначати важливість розробки політики, дотримання стандартів і процедур для захисту інформації і розподілу ресурсів для досягнення мети. Діапазон загроз, з якими може зіткнутися підприємство, сильно варіюється від спалахів вимагачів до прихованих цільових атак і випадкових зломів даних. Але це не означає, що підприємства не можуть бути готові до всіх викликів. Ключ до набуття впевненості в вашому підході до безпеки - це розуміння загроз, з якими стикається ваш бізнес, і правильне поєднання технологій і автоматизації, людей і навичок, політики і процесів.

Кожне підприємство матиме програму безпеки, оскільки вона допомагає зосередитися на особливостях ІБ. Це допоможе вам визначити і дотримуватися правил, які впливають на управління вашими даними. Програма дозволяє

правильно здійснювати комунікації з клієнтами та відвідувачами, виконувати як юридичні, так і договірні зобов'язання. Процес життєвого циклу гарантує, що безпека постійно адаптується до підприємства в постійно мінливому IT-середовищі, в якому ми живемо. Це правильно, тому що захист безпеки даних - це те ж саме, що захист вашого найважливішого активу [2].

1.1. Сутність та критерії визначення інциденту

На сьогоднішній день існує велика кількість визначень поняття інцидент, які можна націлити та адаптувати до потреб конкретного випадку та вимог компанії. Однак існує загальне визнане поняття інциденту.

Згідно міжнародного документу з інформаційної безпеки ISO/IEC 27000:2018 інцидентом інформаційної безпеки є єдиний або ряд небажаних або несподіваних подій інформаційної безпеки, які мають значну ймовірність погіршення ділових операцій та загрози інформаційній безпеці [3].

Інцидент може визначатись як будь-яка подія: велика чи маленька, хороша чи погана, передбачувана або непередбачувана всі ці події можна охарактеризувати як інцидент. Однозначно, це небажана подія або серія небажаних подій інформаційної безпеки, які мають велику ймовірність компрометації бізнес-операцій та можуть загрожувати інформаційній безпеці підприємства та є інцидентом інформаційної безпеки.

Відповідно до Закону України “Про основні засади забезпечення кібербезпеки України”, який визначає термін “Інцидент кібербезпеки”, як подію або сукупність несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема, пов’язаних з людським фактором) або події що мають ознаки можливої (потенційної) кібератаки, які:

- становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами,

- створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами),
- ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

В свою чергу, подія інформаційної безпеки – це ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути суттєвою для політики безпеки.

Подія ІБ може ідентифікуватися автоматизованими засобами або шляхом надходження повідомлення від користувачів інформаційних активів (ресурсів). Ідентифіковані події ІБ мають фіксуватися. Членам групи реагування на інциденти ІБ повинно бути надано безпосередній доступ до всіх фактичних свідчень про події ІБ. Не всі події є інцидентами ІБ, однак окремі події можуть бути ознаками початку інциденту. Всі ідентифіковані події ІБ потребують негайного оцінювання з метою визначення, чи є подія інцидентом, або фіктивним сигналом тривоги. Первинне оцінювання здійснюється персоналом підприємства, який відповідає за технічне супроводження інформаційної інфраструктури. Кінцеве визначення інциденту здійснюється групою реагування на інциденти ІБ або кваліфікованим спеціалістом.

Недосконалий контроль інформаційної безпеки можна характеризувати наступним чином: елементи управління можуть бути перевантажені або підірвані (наприклад, компетентними хакерами, шахраями або шкідливими програмами), збоями в роботі (збоями аутентифікації), працюють частково або погано (виявлення повільної аномалії), більше або менш повно відсутні (повністю не реалізована і не повністю функціонує система ідентифікації та аналізу ризиків). Отже, інциденти інформаційної безпеки можуть статися навіть на підприємствах, які мають свій відділ інформаційної безпеки.

Управління інцидентами ефективно, якщо включає в себе розслідувальні та коригувальні заходи контролю, які призначені для визнання і реагування на події

та інциденти, зведення до мінімуму несприятливих наслідків, збору судових доказів (коли це може бути застосовано) і належно вдосконалювати SIEM (Security information and event management).

Управління інцидентами ІБ впроваджується з метою забезпечення:

- своєчасного виявлення та ефективної обробки подій ІБ;
- правильного оцінювання ідентифікованих інцидентів ІБ та реагування на них найбільш доцільним та результативним способом;
- мінімізації впливу інцидентів ІБ на підприємство та бізнес-процеси, у тому числі запобігання нанесення шкоди діловій репутації та іміджу підприємства;
- швидкого здобуття досвіду з відбувшихся інцидентів ІБ (формування архівів, що має сприяти підвищенню шансів запобігання виникненню інцидентів у майбутньому, поліпшенню впровадження та використання захисних заходів ІБ.

Для ефективного управління інцидентами ІБ необхідно здійснювати:

- планування та підготовку системи управління інцидентами ІБ;
- використання системного підходу;
- аналіз функціонування системи;
- внесення удосконалень в процеси управління інцидентами ІБ.

Віднесення події до інциденту є важливою частиною управління ІБ підприємства. Заради цього керівництвом або відповідними підрозділами підприємства визначаються критерії віднесення до інциденту:

- причини виникнення події;
- чи може подія зашкодити діяльності інших (більш критичних) інформаційних систем;
- розмір потенційних наслідків події, враховуючи зв’язки між інформаційними системами та прикладними програмами (ефект доміно);
- чи впливає подія на клієнтів або працівників підприємства, що є користувачами ІС;
- категорія інформації, скомпрометованої внаслідок події.

У випадку підтвердження виявлення інциденту, група реагування на інциденти ІБ проводить класифікацію інциденту у співпраці з бізнес-власником ІС згідно з наступними критеріями класифікації:

За наслідками інциденти інформаційної безпеки класифікуються за наступними критеріями (рівнями критичності):

- Критичний: скомпрометовано/пошкоджено критичні інформаційні системи підприємства, у результаті чого вплив на діяльність підприємства може бути руйнівним;
- Високий: скомпрометовано/пошкоджено важливі та/або некритичні інформаційні системи підприємства; виявлено порушення політики ІБ; було припинено критичні або важливі бізнес-процеси підприємства;
- Середній: компрометацію/пошкодження не виявлено, але існують ознаки спроб компрометації/пошкодження/негативного впливу; зафіксовані порушення вимог з інформаційної безпеки користувачами ІС;
- Низький: було виявлено ознаки порушень вимог нормативно-правових актів з інформаційної безпеки підприємства.

Окремі інциденти мають бути віднесені до відповідних категорій значущості, наприклад ті, що мають “суттєві”, “важливі” або “незначні” наслідки.

На рівні мережі визначаються події безпеки:

- вдалі та невдалі спроби доступу до мережевих пристроїв;
- невдалі спроби (блокування брандмауером) доступу до мережевих служб;
- вдалі та невдалі спроби створення, зміни та видалення груп та облікових записів (в тому числі зміни паролів доступу);
- вдалі та невдалі спроби зміни налаштувань пристрою;
- увімкнення та вимкнення пристрою;
- деактивація заходів безпеки ІС.

З метою впровадження та належного функціонування процесу управління інцидентами ІБ на підприємстві створюється група реагування на інциденти ІБ.

Група реагування на інциденти інформаційної безпеки (ГРІІБ), - це група кваліфікованих та надійних працівників підприємства, яка виконує, координує й підтримує реагування на порушення інформаційної безпеки, що охоплюють інформаційні системи в межах визначеної зони відповідальності. Група може доповнюватися зовнішніми експертами та фахівцями певного відділу підприємства, які можуть допомогти при інциденті.

ГРІІБ створюється для забезпечення підприємства відповідним персоналом для оцінки, реагування на інциденти інформаційної безпеки та отримання досвіду з них, а також необхідної координації, менеджменту, зворотного зв'язку і процесу передачі інформації. Члени ГРІІБ беруть участь у зниженні фізичної, матеріальної та фінансової шкоди, а також шкоди для репутації підприємства, пов'язаної з інцидентами інформаційної безпеки. Кількість і склад даного персоналу повинні відповідати масштабу й цілям діяльності підприємства. ГРІІБ може представляти собою окремо створену команду або колектив залучених працівників з різних відділів підприємства (наприклад, IT, бухгалтерія, відділи кадрів, маркетингу). Керівник ГРІІБ повинен мати окрему лінію для оповіщення керівництва, ізольовану від інших бізнес-процесів. Обов'язки ГРІІБ можна розділити на дві основні групи:

- дії в актуально реальному часі, безпосередньо пов'язані з головним завданням - реагуванням на порушення;
- превентивні профілактичні дії, які відіграють допоміжну роль і здійснюються не в реальному часу.

Перша група включає оцінку входу інформації (класифікація порушень) і роботу над інформацією разом з іншими групами, постачальниками послуг Internet та іншими комунікаційними представниками (координація та реагування), а також допомога локальним користувачам у відновленні роботи після порушення (вирішення певних проблем). Класифікація порушень включає в себе:

- оцінка доповідей: вхідна інформація ранжується за ступенем важливості, співвідноситься з триваючими подіями і виявляються тенденції;
- верифікація: виявляється порушення і його масштаби.
- категорування інформації: інформація, що відноситься до порушення (реєстраційні журнали, контактна інформація) категоризується відповідно до політики розкриття інформації;
- координація: у відповідності з політикою розкриття відомостей про порушення повідомляються інші сторони.

У превентивні профілактичні дії входять:

- ознайомлення з інформацією;
- навчання і підготовка кадрів;
- оцінка продуктів;
- оцінка захищеності підприємства;
- консультаційні послуги.

До ознайомлення з інформацією відноситься підтримка архіву відомих уразливих місць, способів вирішення минулих проблем чи організація адресної розсилки з рекомендаційними цілями; надання засобів безпеки (наприклад, кошти для проведення аудиту);

Навчання і підготовка кадрів дозволяє максимально знизити ймовірність появи ненавмисних помилок у поводженні з інформацією. Необхідно пам'ятати, що ніякі заходи організаційного та технічного характеру не компенсують можливий витік інформації з боку співробітників підприємства і те, що інформаційна безпека - це комплекс заходів.

В даний час існує велика кількість різних методів підвищення обізнаності співробітників в області ІБ. Найбільша ж ефективність, досягається при комплексному комбінуванні та використанні різних елементів. Деякими методами такого навчання є:

1. Скрінсейвер;
2. Фільми, мультфільми, ролики, (ситуативні кейси);

3. Новини по ІБ;

4. Офісні приналежності.

Одним із прикладів оцінки саме практичних, а не теоретичних знань співробітників, є використання соціальної інженерії, коли імітуються ситуації, в яких дії неграмотного користувача можуть призвести до порушення ІБ.

Оцінка безпеки продуктів програмного забезпечення (ПЗ) в широкому сенсі є властивістю даного ПЗ функціонувати без прояву різних негативних наслідків для конкретної комп'ютерної системи. Під рівнем безпеки ПЗ розуміється ймовірність того, що при певних умовах в процесі його експлуатації буде отриманий функціонально придатний результат. Причини, що призводять до функціонально непридатного результату можуть бути різними: збої комп'ютерних систем, помилки програмістів і операторів, дефекти в ПЗ. При цьому дефекти прийнято розглядати двох типів: навмисні і ненавмисні. Перші є, як правило, результатом злочинних дій, другі помилкових дій людини.

Масштаб деструктивності загроз безпеки для програмних комплексів комп'ютерних систем як з боку зовнішніх, так і з боку внутрішніх джерел загроз постійно зростає. Це пояснюється стрімким розвитком засобів інформаційних технологій, глобальних інформаційних систем, необхідністю розробки для них складного програмного забезпечення із застосуванням сучасних засобів автоматизації процесу проєктування програм. Крім того, це пояснюється значним або навіть різким підвищенням останнім часом активності діяльності хакерів їх обєднань, які атакують комп'ютерні системи, кримінальних груп комп'ютерних зломщиків, різних спеціальних підрозділів і служб, які здійснюють свою діяльність в області створення засобів впливу на критично вразливі об'єкти інформаційних структур.

Оцінка захищеності підприємства спрямована на глибоку оцінку того чи іншого аспекту інформаційної безпеки, або на комплексний аналіз всієї СУІБ в цілому. В першу чергу, захищеність - стан інформації, при якому виключається можливість випадкового або навмисного впливу штучного або природного характеру, яке може завдати неприйнятного збитку суб'єктам інформаційних

відносин. Проблема оцінки ефективності заходів вважається актуальною й сьогодні. У більшості випадків це пов'язано зі складністю оцінки якості застосовуваних інструментів, а також з їх високою вартістю. Одним із способів аналітичної оцінки захищеності є проведення експертної оцінки системи захисту підприємства. Така перевірка може проводитися як співробітниками компанії, так і незалежними експертами.За допомогою експертної оцінки можна перевіряти не тільки програмне забезпечення робочих станцій, а й нормативну документацію.

Сучасні технології передбачають використання сканерів вразливостей, які залишаються ефективним засобом контролю захищеності різних інформаційних систем і корисні при побудові захисту в корпоративній мережі підприємства, а також при роботі на робочих станціях. Перманентні оновлення актуальних сканерів дозволяють ефективно використовувати їх можливості для виявлення існуючих вразливостей, що позитивно позначається на загальній захищеності інформаційної системи.

Консультаційні послуги спеціалізуються на незалежних консультаціях щодо оптимізації використання IT та ресурсів підприємства. Для ефективного вирішення складних IT завдань, оптимальної побудови інформаційної системи підприємству потрібні знання, досвід, професіоналізм. Правильна методологія при побудові системи захисту інформації, знання найсучасніших і ефективних технологій, величезний практичний досвід – це шлях до побудови ефективного управління. Найважливішим аспектом також є комплексне поєднання всіх методів забезпечення інформаційної безпеки: правового, організаційного, інженерно-технічного і програмно-апаратного захисту інформації.

Перелік консультаційних послуг з питань інформаційної безпеки, що надаються аутсорсинговими компаніями:

- проведення обстеження об'єкта, що застосовуються в ділових процедурах і інформаційних системах (як об'єкта захисту), аналіз її структури, функцій і особливостей, використовуваних технологій автоматизованої обробки і передачі інформації, аналіз виконуваних бізнес-процесів, аналіз нормативної та технічної документації.

- виявлення значущих загроз, основних шляхів їх реалізації; виявлення та ранжування за ступенем небезпеки існуючих вразливостей технологічного та організаційного плану в інформаційній системі.
- розробка політики безпеки.
- складання неформальній моделі порушника.
- оцінка системи управління інформаційною безпекою на відповідність вимогам міжнародних, державних стандартів, розробка рекомендацій.
- розробка пропозицій і рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів забезпечення інформаційної безпеки.
- розробка необхідних організаційних та нормативних документів, поставка, установка, настройка і технічний супровід програмно-апаратних засобів захисту інформації, в тому числі криптографічних.
- передпроєктне обстеження і аналітичні роботи в області документаційного забезпечення, діловодства та документообігу.
- підготовка проєктів нормативно-правових актів у сфері електронного документообігу, що встановлюють випадки і порядок використання електронних документів, електронного цифрового підпису, порядок здійснення електронного документообігу.
- організація ліцензування та отримання дозвільних документів на здійснення діяльності в галузі технічного та криптографічного захисту інформації, надання послуг, що засвідчуються електронним цифровим підписом.
- організація і проведення навчальних заходів: семінари, тренінги.

Для здійснення консультаційних послуг замовник надає співробітникам аутсорсингової компанії доступ на об'єкти, к інформаційним системам, до нормативних і інших документів і відомостей, що стосуються предмету консультування. Результат заходів з надання консультаційних послуг - звіт, що містить аналіз поточного стану та рекомендації щодо підвищення рівня інформаційної безпеки.

1.2. Типи та види інцидентів інформаційної безпеки

Необмежені можливості в галузі обміну інформацією, створюють надзвичайні вразливості щодо шкідливого кібернетичного впливу та різних видів загроз як на інформаційний простір, так і на свідомість людей . На перший план почали виходити проблеми кібербезпеки, тобто кіберпростору від загрозливого втручання, інцидентів у роботу інформаційно- телекомунікаційних мереж.

Інциденти, які завдають шкоди конфіденційності, цілісності та доступності комп'ютерних даних та систем.

Прикладами таких інцидентів є:

- Несанкціонований доступ, втручання в роботу або компрометація інформаційних систем, ресурсів чи інформаційної інфраструктури підприємства (рис.1.1).

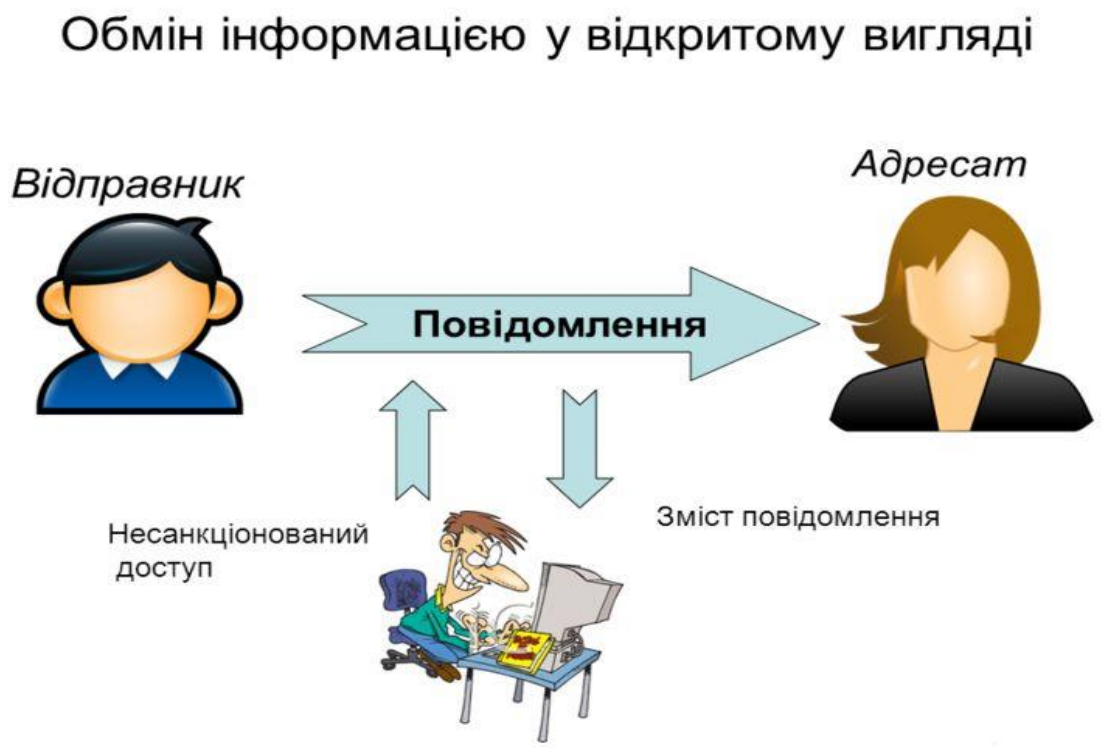

Рис. 1.1. Несанкціонований доступ

- Вірусни, атаки, шпигунське та інше зловмисне шкідливе програмне забезпечення (рис.1.2).

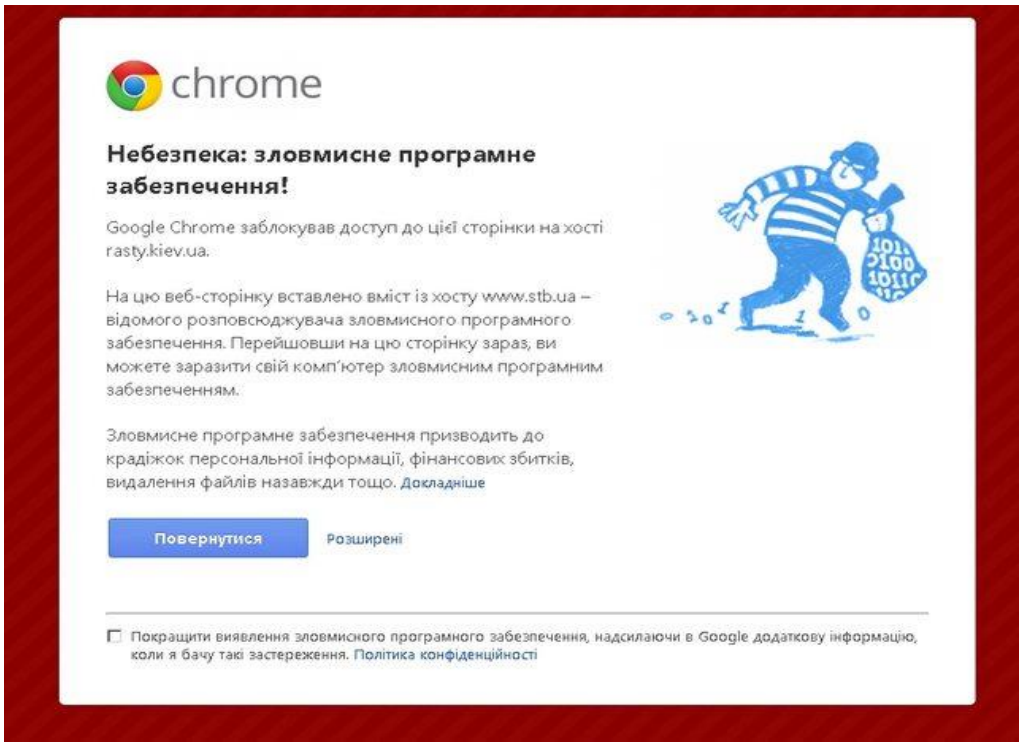

Рис. 1.2. Приклад спроб зараження ПК зловмисним ПЗ

- Компрометація криптографічних ключів (рис.1.3)

Рис. 1.3. Токени для автентифікації

- Компрометація автентифікаційних даних користувачів ІС (рис.1.4).

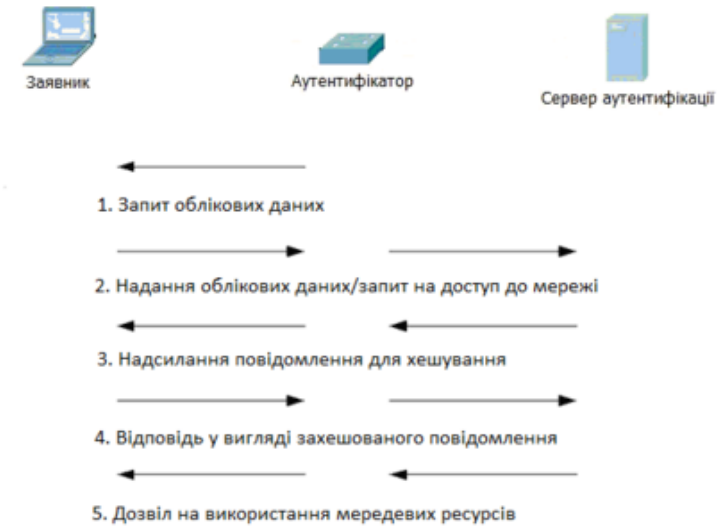

Рис. 1.4 Схема автентифікації

- Мережеві атаки на інформаційні системи, ресурси підприємства, в тому числі спрямовані на відмову в обслуговуванні, спроби підбору паролів, сканування, перехоплення мережевого трафіку (рис.1.5).

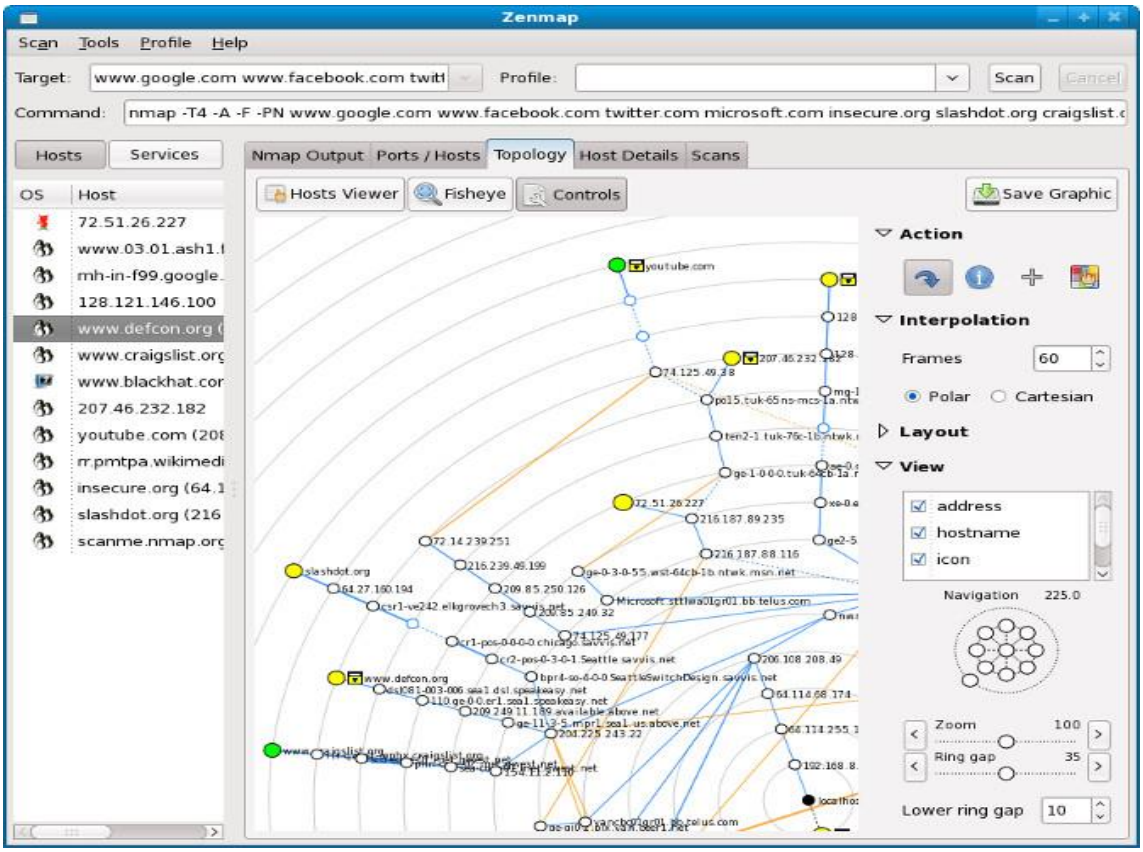

Рис. 1.5. Сканування мережі

- Витік інформації з обмеженим доступом каналами передачі даних в електронному вигляді (рис.1.6).

Рис. 1.6 Приклад передачі даних

- Вимкнення або перешкоджання роботі засобів забезпечення безпеки: антивірусних програм, міжмережевих екранів (рис.1.7).

Рис. 1.7 Антивірусні програми

- Вразливості інформаційних систем, ресурсів підприємства (рис.1.8).

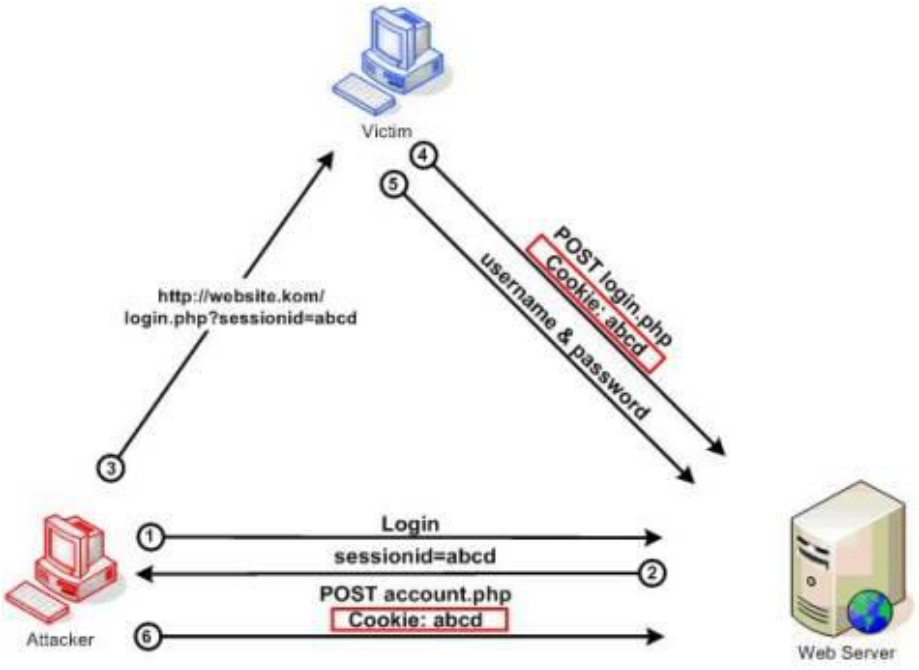

Рис. 1.8 Приклад вразливості веб-ресурсу

- Несанкціоноване використання підключень віддаленого доступу до мережі підприємства (рис.1.9).

Рис. 1.9 Приклад розповсюдження файлів через віддалений доступ

- Порушення правил використання інформаційних систем та мережі підприємства. В тому числі відсутність, несанкціонована модифікація, або неналежне ведення журналів реєстрації подій безпеки та протоколів роботи інформаційних систем підприємства.

Розрізняють внутрішні і зовнішні інциденти. Під внутрішнім інцидентом розуміють подію, джерелом якої є порушник, безпосередньо пов’язаний з пошкодженою інформаційною системою. Під зовнішнім інцидентом розуміють подію, джерелом якого є порушник, безпосередньо не пов’язаний з інформаційною системою. До такого типу належать вище вказані події: вірусні атаки на програмне та технічне забезпечення ІКС, атаки типу “відмова в обслуговуванні”, перехоплення мережевого трафіку, сканування порталу корпоративної мережі, неправомірний доступ до конфіденційної інформації, шахрайство в системах електронного документообігу. Найпоширеніші такі види атак:

- Відмова в обслуговуванні (Denial of Service – DoS) – атака з метою недоступності ресурсів ІКС для авторизованих користувачів. Створюється провокування надмірного навантаження на ОС, додатки або технічні засоби мережі. До найпоширеніших DoS-атак належать Flood, ICMP flood, Identification flood та Tribe Flood.
- Розподілена DDoS-атака (Distributed Denial of Service) – скоординована DoS-атака відразу з багатьох комп’ютерів. До найпоширеніших DDoS-атак належать TCP flood, UDP flood, Smurf та ICMP flood.
- Сніфер пакетів (Sniffer) – програма, яка використовує інтерфейсну карту мережі, що працює в нерозбірливому (promiscuous mode) режимі прийому і дозволяє перехоплювати всі пакети мережі.
- IP-спуфінг (spoof – обман) – вид хакерської атаки, що передбачає використання зловмисником чужої IP-адреси, при маскуванні під санкціонованого користувача.
- Віруси (Virus) – шкідливий програмий фрагмент, здатний до впровадження в інформаційну систему у змістовній частині переданого користувачем файла в інші файли комп’ютера, зокрема у файли системних і прикладних програм та на електронну пошту.
- Мережеві хробаки (Worm) – злоякісні програми, здатні до

автономного створення своїх копій і розповсюдження в комп’ютерній мережі без участі в цьому процесі користувачів. Хробак збирає інформацію про вузли мережі, їх адреси та інші дані, які цікавлять зловмисника.

- Трояни (троянські коні, Trojan horse) – різновид шкідливих програм, які маскуються під корисні додатки, але наносять шкоду інформаційній системі: знищують або спотворюють інформацію на диску, копіюють паролі, спотворюють імена файлів.
- Логічні бомби (Logic bombs) – спеціально сконструйовані коди, які за певною ознакою спричиняють деструктивну роботу програми, що виконується, зокрема, повне припинення її виконання.
- Спам (Spam) – вид атаки засобами електронної пошти. Велика кількість листів, яка надсилається зловмисником на адресу електронної пошти, унеможливлює роботу поштових скриньок, а іноді і поштових серверів.
- Ін’єкції (Exploit tools) – вид атаки шляхом впровадження шкідливих команд або даних в працюючу систему з метою впливу на її роботу так, щоб отримати доступ до комп’ютера чи даних, або дестабілізувати роботу системи загалом. Прикладом такого виду атаки є SQL-ін’єкції, які зловмисники використовують для зміни параметрів запитів до бази даних (сховища).
- Бекдор (back door) – злоякісна програма, яка забезпечує зловмиснику доступ до конфіденційної інформації, розміщеної на віддаленому комп’ютері. Завдяки бекдору зловмисник може витягнути з інфікованої LAN назву та ЄДРПОУ компанії, пароль проксі-сервера, ім’я поштового сервера, паролі та email-адреси клієнтів.

Ефективність боротьби з новими видами інцидентів у сфері кібербезпеки залежить від залучення належних інвестицій та тісної співпраці всіх підрозділів підприємства.

Інциденти можуть траплятися різними способами, тому неможливо розробити покроковий алгоритм щодо протидії при кожному інциденті. Підприємства повинні бути готові вирішувати будь-який інцидент, але слід прорахувати основні типи інцидентів, які заслуговують на увагу різних стратегій

реагування. Класифікація інцидентів передбачає перерахування основних способів атак:

Зовнішні, знімні носії: атака виконана зі знімного носія або периферійного пристрою, наприклад, шкідливий код поширюється на систему із зараженого флеш-накопичувача USB.

Видалення: атака, яка використовує методи грубої сили для компрометування, знищення або знищення систем, мережі або служби.

Веб: атака, виконана з веб-сайту або веб-додатку, наприклад, крос-сайт атака сценаріїв використовується для викрадення облікових даних або перенаправлення на сайт, який використовує вразливість браузера та встановлює зловмисне програмне забезпечення.

- Електронна пошта: атака, виконана через повідомлення електронної пошти або вкладення: використання коду, що маскується, як доданий документ або посилання на шкідливий веб-сайт у змісті повідомлення електронної пошти.
- Засмічення: напад із заміною чогось корисного з чим-небудь зловмисним наприклад, спуфінг, людина в середині атаки, шахрайські бездротові точки доступу та ін'єкції SQL.
- Неправильне використання: будь-який інцидент, спричинений порушенням прийнятного використання в підприємства політики авторизованого користувача, за винятком зазначених вище категорій; Наприклад, користувач встановлює програмне забезпечення для обміну файлами, що призводить до втрати конфіденційних даних або користувач виконує незаконну діяльність в системі.
- Втрата або викрадення обладнання: втрата або крадіжка обчислювального пристрою або носія, що використовується в підприємства: ноутбук, смартфон або токен автентифікації.

Однією з найбільших помилок у традиційній інформаційній безпеці є те, що зловмисники знають, яким шляхом вони потраплять у мережу. Наприклад, зловмисники рідко проходять через вхідні двері або, брандмауер та шлюзи. Це серія кроків, необхідних зловмиснику для успішного проникнення в мережу і

вилучення даних з мережі. Кожен етап являє собою певну мету на шляху зловмисника. Розробка планів моніторингу та реагування на основі моделі ланцюжка кібератак є ефективним способом зосередитися на фактичній атаці.

1.3. Засоби виявлення інцидентів

1.3.1. Security information and event management

Очікується, що ринок глобальної інформації про безпеку та управління подіями зростатиме значними темпами протягом прогнозованого періоду, між 2022 і 2030 роками.

Згідно з нашим останнім дослідженням, глобальний ринок інформації про безпеку та управління подіями виглядає багатообіцяючим у найближчі 5 років. Станом на 2022 рік глобальний ринок інформації про безпеку та управління подіями оцінювався в 4942,27 млн. доларів США, і очікується, що він досягне 8338,99 млн доларів США в 2028 році з CAGR 9,11% протягом прогнозованих років. Вплив від короткострокового SIEM є опорним сектором економіки, і навіть у періоди економічного спаду витрати все одно відбуватимуться. Малі компанії та компанії, що розвиваються, можуть бути під загрозою, але дохід від продажів і залучення капіталу забезпечують буферний простір для подолання труднощів.

Компанії SIEM будуть більш розпорошеними, ніж раніше, що сприятиме розвитку нульової довіри. Процеси безпеки та стратегії для віддаленої роботи стануть частиною постійного плану на майбутнє, і навчання найкращим практикам безпеки для працівників SIEM буде особливо важливим. COVID-19 матиме непередбачуваний довгостроковий вплив на індустрію мережевої безпеки. SIEM має вжити заходів для подолання цієї епідемії та виживання.

Зростання занепокоєння щодо IT-безпеки. IT-безпека стала надзвичайно важливою проблемою для всіх пыдприэмств, незалежно від їх галузі та розміру. Клієнти вимагають системи управління безпекою, яка добре інтегрована з IT-

інфраструктурою компанії та забезпечує ефективну роботу за доступною ціною. SIEM пропонує журнал, і управління подіями за доступною ціною та з уніфікованим рішенням для спрощення складності керування кількома рішеннями безпеки з високою продуктивністю. Це спонукало до постійного розвитку ринку інформації про безпеку та управління подіями.

Збільшення проблем безпеки та конфіденційності. Аудіо- та відеосеанси SIEM пропонують можливості шифрування у початковому стані; однак користувач, який використовує відеоконференцію, має перевірити підтримку шифрування. Зростання занепокоєння щодо безпеки та конфіденційності негативно впливає на SIEM з точки зору підтримки шифрування та високого рівня безпеки. Складність рішень SIEM — це складна технологія, яка включає мобільні пристрої, хмару та сторонні дані про загрози на додаток до традиційних джерел, таких як кінцеві точки, брандмауери, системні журнали та служби каталогів. Хоча ці доповнення пропонують кращу аналітику даних, вони вимагають постійного налаштування та обслуговування. Очікується, що серед різних типів продуктів у 2027 році найбільшу частку ринку займе сегмент керування журналами та подіями. Огляд додатків. Найбільшим сегментом ринку за додатками є сегмент банківських, фінансових послуг і страхування (BFSI) із часткою ринку 44,86% у 2021 році. Цей звіт охоплює проміжок часу дослідження з 2018 по 2028 рік і представляє глибокий і всебічний аналіз глобального ринку інформації про безпеку та управління подіями, із систематичним описом статус-кво та тенденцій усього ринку, уважний аналіз конкурентного середовища основних гравців і детальна розробка сегментованих ринків за типом, застосуванням і регіоном.

Основним з інцидентів безпеки є незвичайний трафік через несанкціонований порт, несанкціонований доступ до певного місця або інші дії, які порушують прийнятний стандарт підприємства. Щоб мінімізувати ризик, важливо мати процес, що дозволяє швидко ідентифікувати ці інциденти, розслідувати і виконувати аналіз першопричин, а також реалізовувати кроки щодо виправлення ситуації до того, як збиток від витоку даних стане більш масштабним. Ризик може бути зменшений, якщо діяти швидко. Можливість

виявлення інцидентів і реагування на них лежить в основі багатьох правил забезпечення безпеки.

Управління інформацією про безпеку та подіями (SIEM) — це підхід до керування безпекою, який об’єднує функції керування інформацією про безпеку (SIM) і керування подіями безпеки (SEM) в одну систему керування безпекою. Абревіатура SIEM вимовляється як "сім" із беззвучною літерою е .

Основними принципами кожної системи SIEM є агрегування відповідних даних із багатьох джерел, виявлення відхилень від норми та вжиття відповідних заходів. Наприклад, коли виявляється потенційна проблема, система SIEM може реєструвати додаткову інформацію, генерувати сповіщення та вказувати іншим елементам керування безпекою зупинити виконання дії.

Відповідність стандарту безпеки даних індустрії платіжних карток спочатку спонукала до впровадження SIEM у великих підприємствах, але занепокоєння щодо прогресивних постійних загроз спонукало менші організації звернути увагу на переваги інструментів SIEM. Можливість розглядати всі пов’язані з безпекою дані з єдиної точки зору полегшує організаціям будь-якого розміру виявлення незвичайних моделей.

На самому базовому рівні система SIEM може базуватися на правилах або використовувати механізм статистичної кореляції для встановлення зв’язків між записами журналу подій. Розширені системи SIEM розвинулися, щоб включити аналітику поведінки користувачів і об’єктів, а також оркестрування безпеки, автоматизацію та реагування (SOAR).

Системи SIEM працюють шляхом розгортання кількох агентів збору в ієрархічній манері для збору пов’язаних із безпекою подій від пристроїв кінцевих користувачів, серверів і мережевого обладнання, а також спеціалізованого обладнання безпеки, такого як брандмауери , антивірусні програми або системи запобігання вторгненням (IPS). Колектори пересилають події на централізовану консоль керування, де аналітики безпеки відсіюють шум, з’єднуючи точки та визначаючи пріоритетність інцидентів безпеки [4].

У деяких системах попередня обробка може відбуватися на граничних колекторах, лише певні події передаються до централізованого вузла керування. Таким чином можна зменшити обсяг інформації, що передається та зберігається. Незважаючи на те, що прогрес у машинному навчанні допомагає системам точніше позначати аномалії, аналітики все одно повинні надавати зворотний зв’язок, постійно навчаючи систему про середовище.

Як працює SIEM?

Інструменти SIEM збирають дані про події та журнали, створені хост-системами по всій інфраструктурі компанії, і об’єднують ці дані на централізованій платформі. Хост-системи включають програми, пристрої безпеки, антивірусні фільтри та брандмауери. Інструменти SIEM ідентифікують і сортують дані за такими категоріями, як успішні та невдалі входи, активність зловмисного програмного забезпечення та інша ймовірна шкідлива діяльність.

Програмне забезпечення SIEM генерує сповіщення безпеки, коли виявляє потенційні проблеми безпеки. Використовуючи набір попередньо визначених правил, організації можуть встановити ці сповіщення як низький або високий пріоритет.

Наприклад, обліковий запис користувача, який генерує 25 невдалих спроб входу протягом 25 хвилин, може бути позначений як підозрілий, але йому все одно буде встановлено нижчий пріоритет, оскільки спроби входу були зроблені користувачем, який забув свою інформацію для входу.

Однак обліковий запис користувача, який генерує 130 невдалих спроб входу протягом п’яти хвилин, буде позначено як подія з високим пріоритетом, оскільки, швидше за все, це атака грубої сили .

SIEM спрощує для підприємств керування безпекою, фільтруючи величезні обсяги даних безпеки та визначаючи пріоритетність сповіщень безпеки, які генерує програмне забезпечення.

Програмне забезпечення SIEM дозволяє організаціям виявляти інциденти, які інакше могли б залишитися непоміченими. Програмне забезпечення аналізує записи журналу, щоб виявити ознаки зловмисної діяльності. Крім того, оскільки

система збирає події з різних джерел у мережі, вона може відтворити хронологію атаки, дозволяючи організації визначити характер атаки та її вплив на бізнес.

Система SIEM також може допомогти організації виконати вимоги відповідності шляхом автоматичного створення звітів, які містять усі зареєстровані події безпеки серед цих джерел. Без програмного забезпечення SIEM компанії довелося б збирати дані журналів і складати звіти вручну.

Система SIEM також покращує керування інцидентами , допомагаючи групі безпеки компанії розкривати маршрут атаки в мережі, визначати джерела, які були скомпрометовані, і надавати автоматизовані інструменти для запобігання атакам, що відбуваються.

Переваги SIEM

Переваги SIEM включають наступне:

Це значно скорочує час, необхідний для виявлення загроз, мінімізуючи шкоду від цих загроз.

SIEM пропонує цілісне уявлення про середовище інформаційної безпеки організації, полегшуючи збір і аналіз інформації про безпеку для забезпечення безпеки систем. Усі дані організації надходять у централізоване сховище, де вони зберігаються та легко доступні.

Компанії можуть використовувати SIEM для різноманітних випадків використання даних або журналів, включаючи програми безпеки, звіти про аудит і відповідність, службу підтримки та усунення несправностей мережі.

SIEM підтримує великі обсяги даних, тому організації можуть продовжувати масштабувати та додавати більше даних.

SIEM забезпечує виявлення загроз і сповіщення безпеки.

Він може виконувати детальний криміналістичний аналіз у разі серйозних порушень безпеки.

Обмеження SIEM

Незважаючи на свої переваги, SIEM також має такі обмеження:

Впровадження SIEM може зайняти багато часу, оскільки для забезпечення успішної інтеграції з засобами безпеки організації та багатьма хостами в її

інфраструктурі потрібна підтримка. Зазвичай для встановлення SIEM потрібно 90 днів або більше, перш ніж він почне працювати.

Це дорого. Початкові інвестиції в SIEM можуть обчислюватися сотнями тисяч доларів. Супутні витрати можуть збільшуватися, включаючи витрати на персонал для керування та моніторингу впровадження SIEM, щорічну підтримку та програмне забезпечення або агентів для збору даних.

Аналіз, налаштування та інтеграція звітів вимагають таланту експертів. Ось чому деякими системами SIEM керують безпосередньо в центрі безпеки , централізованому підрозділі, укомплектованому командою інформаційної безпеки, яка займається питаннями безпеки організації.

Інструменти SIEM зазвичай залежать від правил для аналізу всіх записаних даних. Проблема полягає в тому, що мережа компанії може генерувати тисячі сповіщень на день. Важко визначити потенційні атаки через кількість нерелевантних журналів.

Неправильно налаштований інструмент SIEM може пропустити важливі події безпеки, що зменшить ефективність керування інформаційними ризиками .

Функції та можливості SIEM

Важливі характеристики, які слід враховувати при оцінці продуктів SIEM, включають наступне:

Агрегація даних. Дані збираються та контролюються з програм, мереж, серверів і баз даних.

Кореляція. Як правило, кореляція є частиною SEM в інструменті SIEM. Це означає, що інструмент знаходить подібні атрибути між різними подіями.

Приладові панелі. Дані збираються та агрегуються з програм, баз даних, мереж і серверів і відображаються на діаграмах, щоб допомогти знайти закономірності та уникнути пропуску критичних подій.

Оповіщення. У разі виявлення інциденту безпеки інструменти SIEM можуть повідомити користувачів.

автоматизація. Деяке програмне забезпечення SIEM також може містити автоматизовані функції, наприклад автоматичний аналіз інцидентів безпеки та автоматичні відповіді на інциденти .

Користувачам також слід поставити такі запитання щодо можливостей продукту SIEM:

Інтеграція з іншими елементами керування. Чи може система надавати команди іншим засобам безпеки підприємства для запобігання або припинення поточних атак?

Штучний інтелект (ШІ). Чи може система підвищити власну точність за допомогою машинного та глибокого навчання ?

Канали розвідки про загрози. Чи може система підтримувати канали розвідки про загрози за вибором організації, чи вона зобов’язана використовувати певний канал?

Розширена звітність про відповідність. Чи містить система вбудовані звіти для загальних потреб у відповідності та надає організації можливість налаштовувати або створювати нові звіти щодо відповідності?

Криміналістичні можливості. Чи може система отримувати додаткову інформацію про події безпеки, записуючи заголовки та вміст цікавих пакетів?

Інструменти та програмне забезпечення SIEM

На ринку існує велика різноманітність інструментів SIEM, але нижче наведено лише приклади:

Сплунк. Splunk — це локальна система SIEM, яка підтримує моніторинг безпеки та пропонує постійний моніторинг безпеки, розширене виявлення загроз, розслідування інцидентів і реагування на інциденти.

IBM QRadar. Платформа IBM QRadar SIEM забезпечує моніторинг безпеки IT-інфраструктур. Він включає збір даних журналу, виявлення загроз і кореляцію подій.

LogRhythm. LogRhythm — це система SIEM для невеликих організацій. Він об’єднує керування журналами, мережевий моніторинг і моніторинг кінцевих точок, а також криміналістику й аналітику безпеки.

Exabeam. Портфоліо SIEM від Exabeam Inc. пропонує озеро даних, розширену аналітику та засіб пошуку загроз .

NetWitness. Платформа RSA NetWitness — це інструмент виявлення загроз і реагування на них, який включає збір, пересилання, зберігання та аналіз даних.

Datadog Cloud SIEM. Datadog Cloud SIEM від Datadog Security — це хмарна мережа та система керування. Інструмент включає як моніторинг безпеки в реальному часі, так і керування журналами.

Журнал 360. Інструмент Log360 SIEM пропонує аналіз загроз, керування інцидентами та функції SOAR. Збір журналів, аналіз, кореляція, попередження та архівування доступні в режимі реального часу.

Менеджер подій безпеки SolarWinds. Інструмент SolarWinds Security Event Manager SIEM автоматично виявляє загрози, відстежує політику безпеки та захищає мережі. Інструмент пропонує такі функції, як моніторинг цілісності, звітування про відповідність і централізований збір журналів.

Як вибрати правильний продукт SIEM

Ключ до вибору правильного інструменту SIEM залежить від ряду факторів, включаючи бюджет організації та стан безпеки. Однак компаніям слід шукати інструменти SIEM, які пропонують такі можливості:

звітність про відповідність;

реагування на інциденти та криміналістика;

моніторинг доступу до бази даних і серверів;

виявлення внутрішніх і зовнішніх загроз;

моніторинг загроз у реальному часі, кореляція та аналіз у різноманітних програмах і системах;

система виявлення вторгнень, IPS, брандмауер, журнал подій, а також інші прикладні та системні інтеграції;

розвідка загроз; і

моніторинг активності користувачів.

Найкращі практики впровадження SIEM

Під час впровадження SIEM дотримуйтесь цих передових практик:

Ставте зрозумілі цілі. Інструмент SIEM слід вибирати та впроваджувати на основі цілей безпеки, відповідності та потенційних загроз організації.

Застосуйте правила кореляції даних. Правила кореляції даних повинні бути реалізовані в усіх системах, мережах і хмарних розгортаннях, щоб дані з помилками можна було легше знайти.

Визначте вимоги відповідності. Це допомагає переконатися, що вибране програмне забезпечення SIEM налаштовано на перевірку та звітування щодо правильних стандартів відповідності.

Список цифрових активів. Перелік усіх цифрових даних, що зберігаються в IT-інфраструктурі, допомагає керувати даними журналу та відстежувати мережеву активність. Записуйте плани реагування на інциденти та робочі процеси. Це допомагає командам швидко реагувати на інциденти безпеки.

Призначити адміністратора SIEM. Адміністратор SIEM забезпечує належне обслуговування реалізації SIEM.

Історія SIEM

Технологія SIEM, яка існує з середини 2000-х років, спочатку розвинулась із керування журналами, що є колективними процесами та політиками, які використовуються для адміністрування створення, передачі, аналізу, зберігання, архівування та утилізації великих обсягів даних журналу, створених в інформаційному система.

Постачальники створили SIEM, об’єднавши SEM, який аналізує дані журналів і подій у режимі реального часу, забезпечуючи моніторинг загроз, кореляцію подій і реагування на інциденти, із SIM, який збирає, аналізує та звітує про дані журналів.

SIEM тепер є більш комплексним і вдосконаленим інструментом. Було представлено нові інструменти для зниження ризиків в організації, наприклад використання машинного навчання та ШІ, щоб допомогти системам точно позначати аномалії. Згодом продукти SIEM із цими розширеними функціями почали називати SIEM наступного покоління .

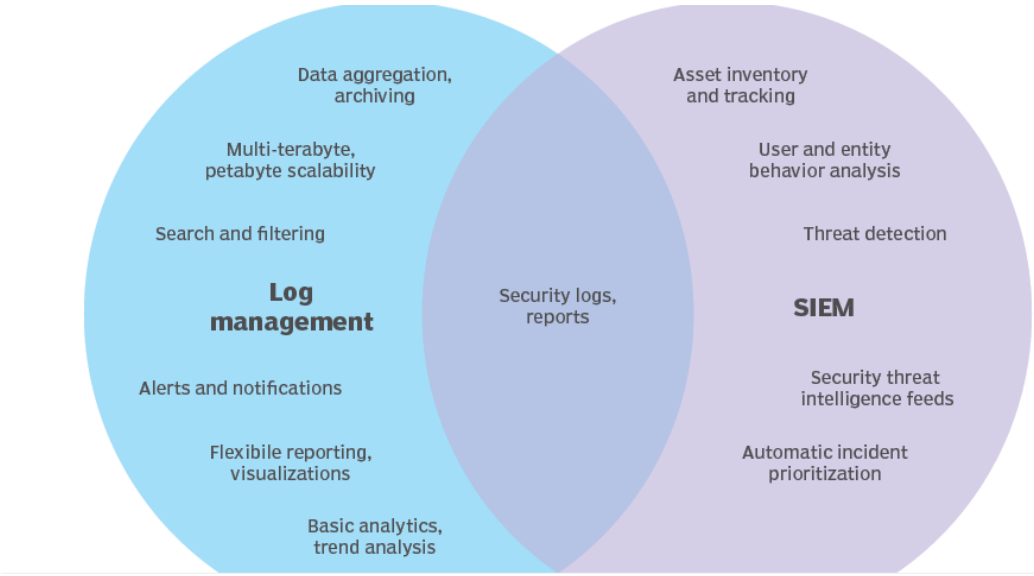

Рис.1.10. Від керування журналами до майбутнього майбутнього SIEM

Майбутнє SIEM

Майбутні тенденції SIEM включають наступне:

Покращена оркестровка. Наразі SIEM надає компаніям лише базову автоматизацію робочого процесу. Однак, оскільки ці організації продовжують розвиватися, SIEM має запропонувати додаткові можливості. Наприклад, за допомогою штучного інтелекту та машинного навчання інструменти SIEM повинні пропонувати швидшу оркестровку, щоб забезпечити однаковий рівень захисту для різних відділів компанії. Крім того, протоколи безпеки та виконання цих протоколів будуть швидшими, ефективнішими та ефективнішими.

Краща співпраця з інструментами керованого виявлення та реагування (MDR). Оскільки загрози злому та несанкціонованого доступу продовжують зростати, важливо, щоб організації застосовували дворівневий підхід для виявлення та аналізу загроз безпеці. IT-команда компанії може впровадити SIEM власними силами, а керований постачальник послуг може впровадити інструмент MDR.

Покращене керування хмарою та моніторинг. Постачальники SIEM вдосконалять можливості керування хмарою та моніторингу своїх інструментів, щоб краще задовольнити потреби безпеки організацій, які використовують хмару.

SIEM і SOAR стануть одним інструментом. Шукайте традиційні продукти SIEM, щоб скористатися перевагами SOAR; однак постачальники SOAR, швидше за все, відреагують розширенням можливостей своїх продуктів.

Згідно з нещодавньою статтею Forbes , майбутнє SIEM може включати такі п’ять можливих результатів:

1. Моделі ціноутворення на основі використання для SIEM стануть поширеними.

2. Інструменти аналізу будуть побудовані на універсальних платформах даних SIEM.

3. Організації співпрацюватимуть, щоб забезпечити більше інтеграцій.

4. Вартість SIEM знизиться, що зробить SIEM доступнішим для невеликих груп безпеки.

5. Стартапи вирішуватимуть більше багатогранних проблем управління безпекою.

SIEM є однією з найбільш ефективних аналітичних систем безпеки. Важливим є той факт, що рішення підтримує роботу з продуктами від різних провідних виробників і проводить збір, аналіз і кореляцію даних через широкий спектр систем, включаючи мережеві рішення, засоби безпеки, сервери, хости, операційні системи і додатки [5].

1.3.2. Запобігання витоків інформації (Data loss prevention software)

Запобігання втраті даних (DLP) — це набір інструментів і процесів, які використовуються для запобігання втраті конфіденційних даних, їх неналежному використанню чи доступу неавторизованих користувачів.

Програмне забезпечення DLP класифікує регульовані, конфіденційні та критично важливі для бізнесу дані та виявляє порушення політик, визначених організаціями або в рамках попередньо визначеного пакету політик, як правило, керуючись нормативними вимогами, такими як HIPAA, PCI-DSS або GDPR.

Після виявлення цих порушень DLP примусово виправляє їх за допомогою сповіщень, шифрування та інших захисних дій, щоб запобігти випадковому чи зловмисному обміну даними кінцевими користувачами, що може створити організаційні ризики.

Програмне забезпечення й інструменти запобігання втраті даних відстежують і контролюють дії кінцевих точок, фільтрують потоки даних у корпоративних мережах і відстежують дані в хмарі, щоб захистити дані в стані спокою, у русі та під час використання. DLP також надає звіти для відповідності вимогам дотримання вимог і аудиту, а також визначає слабкі місця та аномалії для судової експертизи та реагування на інциденти .

3 основні варіанти використання DLP

Запобігання втраті даних вирішує три основні цілі, які є загальними проблемними точками для багатьох організацій: захист особистої інформації / відповідність вимогам, захист інтелектуальної власності (IP) і видимість даних.

Захист особистої інформації/відповідність : якщо підприємство збирає та зберігає ідентифікаційну інформацію (PII), захищену інформацію про здоров'я (PHI) або інформацію про платіжні картки (PCI), це має регулюватись дією нормативних актів, які вимагають від вас захисту конфіденційних даних ваших клієнтів. DLP може ідентифікувати, класифікувати та позначати конфіденційні дані та відстежувати дії та події, пов'язані з цими даними. Крім того, можливості звітування надають деталі, необхідні для аудиту відповідності.

Захист інтелектуальної власності : якщо підприємство має важливу інтелектуальну власність і комерційну або державну таємницю, яка може поставити під загрозу фінансовий стан вашої організації та імідж бренду у разі втрати чи викрадення, рішення DLP, такі як Digital Guardian, які використовують контекстну класифікацію, можуть класифікувати інтелектуальну власність як у структурованій, так і в неструктурованій формах. Завдяки політикам і засобам керування можна захистити ці дані від небажаного викрадання.

Видимість даних: якщо підприємство прагне отримати додаткову видимість руху даних, комплексне корпоративне рішення DLP може допомогти переглядати

та відстежувати свої дані в кінцевих точках, мережах і хмарі. Це забезпечить бачення того, як окремі користувачі підприємства взаємодіють з даними.

Хоча це три основні випадки використання, DLP може усунути низку інших проблемних моментів, включаючи внутрішні загрози, безпеку даних Office 365, аналіз поведінки користувачів і об'єктів, а також розширені загрози.

7 тенденцій, що стимулюють впровадження DLP

У магічному квадранті Gartner для Enterprise DLP показує, що розмір ринку в 2020 році склав 2,64 мільярда доларів США. Ринок DLP не новий, але він еволюціонував, включаючи керовані служби, хмарне сховище та функціональність, а також розширений захист від загроз, серед іншого. Усе це в поєднанні з тенденцією до зростання гігантських витоків даних призвело до масового зростання впровадження DLP як засобу захисту конфіденційних даних.

Дев'ять тенденцій, які сприяють більш широкому впровадженню DLP:

Зростання ролі CISO: компаній розширили відділи інформаційної безпеки (CISO), які часто підпорядковуються генеральному директору. Керівники зацікавлені у боротьби з витоком даних. DLP забезпечує бізнес- та надає CISO необхідні можливості для звітування, щоб надавати регулярні оновлення генеральному директору.

Розвиваються мандати щодо відповідності: Глобальні правила захисту даних постійно змінюються, і ваша організація має бути адаптованою та підготовленою. Протягом останніх кількох років законодавці в ЄС і штаті Нью-Йорк, відповідно, прийняли GDPR і NYDFS Cybersecurity Регламент, обидва з яких посилили вимоги до захисту даних. Рішення DLP дозволяють підприємствам гнучко розвиватися відповідно до змін глобальних норм.

Сучасні технічні можливості дозволяють для захисту даних: збільшити використання хмари, складних мереж постачання, над якими ви більше не маєте повного контролю, ускладнили захист ваших даних. Видимість подій і контексту подій, які оточують ваші дані, перш ніж вони покинуть вашу організацію, важлива для запобігання потраплянню ваших конфіденційних даних у чужі руки.

Витоки даних є частими та масштабними: вороги з національних держав, кіберзлочинці та зловмисні інсайдери націлюються на ваші конфіденційні дані з різних мотивів, таких як корпоративне шпигунство, особиста фінансова вигода та політична вигода. DLP може захистити від усіх видів зловмисників, зловмисних чи ні. Лише за останні пару років відбулися тисячі витоків даних і значно більше інцидентів з безпекою. Мільярди записів було втрачено через гігантські витоки даних, такі як: неправильна конфігурація бази даних, яка призвела до витоку майже 200 мільйонів записів виборців у США в 2015 році , витік даних Equifax , який ставав все більшим, і злом Yahoo , який вплинув на 3 мільярди користувачів. Це лише деякі з багатьох заголовків, які підкреслюють необхідність захисту даних вашої організації.

Викрадені дані підприємства коштують більше: викрадені дані часто продаються в Dark Web, де окремі особи та групи можуть придбати та використовувати їх для власної вигоди. Оскільки певні типи даних продаються за кілька тисяч доларів, існує явний фінансовий стимул для крадіжки даних, зокрема фінансової інформації, як-от кредитної картки чи банківської інформації [6].

1.3.3 Sanblast безпека мережі

Sanblast network – засіб захисту від загроз нульового дня дозволяє виявляти невідоме шкідливе ПО і забезпечує повний захист мережевого периметра від самих сучасних атак, що гарантує доставку безпечного контенту користувачам.

Загрози нульового дня та вдосконалені постійні загрози використовують елемент несподіванки, щоб обійти традиційну безпеку, що робить ці загрози складними для захисту та дуже популярними серед хакерів. Традиційна пісочниця була розроблена, щоб допомогти з цими типами загроз, але кіберзлочинці розвинули свої методи, створивши шкідливе програмне забезпечення, яке може уникнути виявлення багатьма рішеннями пісочниці. Як наслідок, багато підприємств виявляють, що вживають реактивних заходів для протидії інфекції, а не запобігають їй.

Щоб просунутися вперед, підприємствам потрібна багатогранна стратегія запобігання, яка поєднує в собі проактивний захист, який усуває загрози до того, як вони досягнуть користувачів, і найсучасніше виявлення експлойтів на рівні ЦП, щоб виявляти навіть найбільш замасковані загрози.

Безпека мережі SandBlast

Для корпоративних мереж, яким загрожує цілеспрямована атака, наприклад фішинг і Advanced Persistent Threats, Check Point SandBlast забезпечує найкращий у галузі захист мережі навіть від найскладніших шкідливих програм і загроз нулевого дня. Використовуючи технології ізольованого програмного середовища Threat Emulation і Threat Extraction, SandBlast Network запобігає проникненню невідомих зловмисних програм і атак нулевого дня до користувачів. На відміну від традиційних рішень, які використовують методи ухилення, створюють неприйнятні затримки або пропускають потенційні загрози під час оцінювання файлів, Check Point SandBlast запобігає проникненню у мережу більшої кількості зловмисних програм, зберігаючи при цьому швидкий темп сучасного бізнесу.

SandBlast агент

Веб-браузери та кінцеві точки швидко стали прибутковими векторами атак для хакерів. Check Point SandBlast Agent розширює найкращий у галузі захист нульового дня, щоб запобігти розширеним атакам як на кінцеві точки, так і на веб-браузери. Технологія Anti-Bot ідентифікує та блокує командні та контрольні дії, спрямовані на підключені до мережі пристрої. У той же час криміналістика SandBlast Agent забезпечує автоматичний аналіз інцидентів, розкриваючи повний масштаб атаки та вплив на бізнес. SandBlast Agent надає користувачам захист у режимі реального часу від зловмисного програмного забезпечення у файлах, завантажених з Інтернету, а його технологія Zero Phishing™ захищає облікові дані від атак із використанням відомих і невідомих фішингових сайтів або спричинених повторним використанням корпоративних паролів для неділових служб.

SandBlast Cloud – безпека електронної пошти Office 365

Хмарні інструменти електронної пошти, такі як Microsoft Office 365™, дозволяють компаніям ефективно спілкуватися та співпрацювати. Але це часто пов’язано з відмовою від контролю безпеки ваших критично важливих активів. Отже, як підприємства можуть забезпечити баланс між використанням переваг розгортання хмарної інфраструктури електронної пошти та збереженням надійного захисту від сучасних шкідливих програм? Check Point SandBlast™ Cloud — це ненав’язливе рішення, яке надає користувачам Office 365 найкращий у своєму класі проактивний захист від відомих загроз, невідомого зловмисного програмного забезпечення та атак “нульового дня”. Завдяки численним рівням захисту SandBlast Cloud постійно надає безпечний вміст кінцевим користувачам без затримок.

Пакети пристроїв і програмного забезпечення SandBlast

Спеціалізовані пристрої SandBlast і пакет програмного забезпечення захищають підприємства як від відомих, так і від невідомих загроз, використовуючи провідні в галузі можливості безпеки, включаючи емуляцію загроз (ізольоване програмне середовище), вилучення загроз, антибот, антивірусю

Емуляція загроз (пісочниця)

Для запобігання сучасних складних атак потрібні інновації. Як частина рішення Check Point SandBlast Zero-Day Protection механізм емуляції загроз виявляє зловмисне програмне забезпечення на етапі використання, навіть до того, як хакери зможуть застосувати методи ухилення, намагаючись обійти пісочницю. Файли швидко поміщаються в карантин і перевіряються у віртуальній пісочниці, щоб виявити зловмисну поведінку до того, як вони потраплять у вашу мережу. Це інноваційне рішення поєднує перевірку на рівні ЦП і пісочницю на рівні ОС, щоб запобігти зараженню від найнебезпечніших експлойтів, а також атак нульового дня та цілеспрямованих атак.

Вилучення загроз

Швидка доставка безпечного вмісту має вирішальне значення для підтримки діяльності бізнесу. У рамках рішення Check Point SandBlast Zero-Day Protection функція Threat Extraction негайно надає користувачам безпечну версію

потенційно шкідливого вмісту. Вміст, який можна використовувати, включаючи активний вміст і різні форми вбудованих об’єктів, витягується з реконструйованого файлу для усунення потенційних загроз. Доступ до оригінальної підозрілої версії заблоковано, доки її не буде повністю проаналізовано SandBlast Zero-Day Protection. Користувачі мають миттєвий доступ до вмісту та можуть бути впевнені, що вони захищені від найсучасніших зловмисних програм і загроз нульового дня [7].

1.4. Способи та методи реагування на інциденти

Реагування на інцидент — це процес боротьби з витоком даних або кібератакою, включаючи те, як підприємство намагається контролювати наслідки такого інциденту. Мета полягає в тому, щоб ефективно керувати інцидентами, щоб мінімізувати шкоду системам і даним, скоротити час і вартість відновлення, а також контролювати шкоду репутації бренду.

Має бути розроблений чіткий план реагування на інциденти. У цьому плані має бути зазначено, що є інцидентом безпеки, і описано простий процес, яким команди можуть слідувати, коли трапиться інцидент.

Підприємство має призначити команду, співробітника або керівника, відповідального за управління загальною ініціативою реагування на інциденти та виконання плану. У більшій організації ця команда називається Групою реагування на інциденти комп’ютерної безпеки (CSIRT).

Інцидентна діяльність, яка не контролюється належним чином, може перерости у більшу проблему, що зрештою призведе до витоку даних, високих витрат або збою системи. Швидко реагуючи на інциденти, організації можуть мінімізувати втрати, пом’якшити використані вразливості, відновити служби та процеси, а також знизити ризик майбутніх інцидентів.

Реагування на інциденти дозволяє організаціям робити наступне:

Підготовка до відомого і невідомого;

Швидке виявлення інцидента.

Найкращі методи блокування вторгнень до того, як вони завдадуть шкоди

Реагування на інциденти має вирішальне значення для бізнесу, оскільки діяльність більшості організацій залежить від критично важливих обчислювальних систем і зберігає конфіденційну інформацію. Інциденти безпеки можуть мати короткострокові та довготермінові наслідки, які вплинуть на успіх усього підприємства. Це може включати простої та збої в роботі, регулятивні штрафи, судові витрати та витрати на відновлення даних.

Окрім цих прямих впливів, нездатність ефективно реагувати на інциденти негативно впливає на ефективність діяльності підприємства.

Підприємство не може повністю усунути інциденти, реагування на інциденти може допомогти мінімізувати їх виникнення. Підприємства повинні зосередитися на підготовці до впливу інциденту безпеки. Зловмисники завжди будуть поруч, але будь-яке підприємство може підготуватися до атаки за допомогою функціонально ефективного підходу до реагування на інциденти.

План реагування на інциденти

План реагування на інцидент — це документ, у якому детально описано процеси безпеки, які мають виконуватися у разі інциденту, і осіб, відповідальних за реагування на інцидент.

План реагування на інцидент зазвичай містить такі деталі:

1. Методи та стратегії реагування на інциденти
2. Масштабне реагування на інциденти
3. Поетапні дії реагування на інцидент
4. Ролі та відповідальність за виконання заходів реагування на інциденти
5. Канали зв’язку між групою реагування на інциденти та рештою організації
6. Метрики для оцінки ефективності реагування на інцидент

План продовжує надавати підтримку форензік-аналізу, передбачає формування документації для подання аудиторам, архіви інцидентів, які дозволяють краще реагувати на подібні інциденти в майбутньому.

Дії реагування на інцидент

Стандартний план реагування на інциденти, який може запровадити організація, включає такі кроки:

Крок 1: Раннє виявлення

Відбувається подія безпеки, і система її виявляє. Як правило, платформа управління інформацією та подіями безпеки (SIEM) сповіщає групу реагування на інциденти.

Крок 2: Аналіз

Аналітики переглядають сповіщення, визначають індикатори компрометації (IoC) і використовують їх для визначення загрози. Вони часто проводять додаткові тести, переглядають пов’язані сповіщення та виключають помилкові спрацьовування, щоб отримати повну картину підозрілих подій.

Крок 3: визначення пріоритетів

Аналітики повинні розуміти вплив інцидентів безпеки на ділову діяльність організації та цінні активи. Пріоритезація інцидентів допомагає команді зрозуміти, на яких подіях безпеки зосередитися, і як найкраще керувати ресурсами на наступних етапах.

Крок 4: Сповіщення

По-перше, служба реагування на інциденти повідомляє відповідних людей в організації. У разі підтвердженого порушення організації зазвичай повідомляють зовнішні сторони, такі як клієнти, ділові партнери, регуляторні органи, правоохоронні органи або громадськість. Рішення про сповіщення зовнішніх сторін зазвичай залишається за вищим керівництвом.

Крок 5: Стримування та криміналістика

Служби реагування на інциденти вживають заходів, щоб зупинити інцидент і запобігти повторному зараженню навколишнього середовища. Вони також збирають судово-медичні докази, необхідні для подальшого розслідування або майбутніх судових розглядів.

Крок 6: Відновлення

Служби реагування на інциденти видаляють зловмисне програмне забезпечення з уражених систем, потім перебудовують, відновлюють із резервної копії та виправляють ці системи для відновлення нормальної роботи.

Крок 7: Огляд інциденту

Щоб запобігти повторенню інциденту та покращити реагування в майбутньому, співробітники служби безпеки переглядають кроки, які привели до виявлення останнього інциденту. Вони визначають аспекти успішного реагування на інциденти, можливості для вдосконалення систем (таких як інструменти, процеси та навчання персоналу) і рекомендують способи усунення виявлених вразливостей.

Механізми реагування на інциденти

Деякі великі організації зі значним досвідом безпеки розробили рамки реагування на інциденти, щоб допомогти організаціям створити стандартизовані плани реагування. Національний інститут стандартів і технологій (NIST) та Інститут системного адміністрування, аудиту, мереж і безпеки (SANS) розробили добре відомі системи реагування на інциденти.

Система реагування на інциденти SANS

SANS – це приватна організація, яка проводить розслідування та інформує громадськість щодо питань безпеки. Структура SANS поділяє процес реагування на інцидент на шість етапів:

Підготовка

Ідентифікація

Стримування

Ерадикація

Відновлення

Вивчені уроки

SANS також містить контрольний список реагування на інциденти для кожного кроку та два шаблони із системними командами, які допомагають організаціям виконувати конкретні завдання реагування на інциденти. Ці шаблони доступні для систем Windows і UNIX.

Система реагування на інциденти NIST

NIST – це урядова агенція США, яка розробляє стандарти для галузі технологій і безпеки. У рамках своєї роботи з кібербезпеки вони розробили комплексну структуру реагування на інциденти. Він містить детальну інформацію про створення плану реагування на інциденти, створення групи реагування на інциденти, створення плану зв'язку та сценарії навчання.

Структура зводить шість етапів реагування на інциденти, які використовує структура SANS, до чотирьох:

Підготовка

Виявлення та аналіз

Стримування, викорінення та відновлення

Діяльність після інциденту [8]

Рис. 1.11. Цикл реагування на інцидент

Підготовка - методології реагування на інциденти підкреслюють підготовку - не тільки створення здатності реагувати на інциденти, щоб організація була готова реагувати на інциденти, а й запобігати інцидентам, забезпечуючи достатню безпеку систем, мереж та програм.

Менеджер комунікацій та обладнання при інциденті:

- Контактна інформація для членів команди та інших осіб в межах підприємства та поза нею (основні та резервні контакти), інформація може містити номери телефонів, адреси електронної пошти, загальнодоступні ключі шифрування (відповідно до програмного забезпечення для шифрування, та інструкції для підтвердження ідентичності контакту;
- Механізми звітування про випадки, такі як номери телефонів, адреси електронної пошти, онлайнові форми та безпечні системи обміну миттєвими повідомленнями, які користувачі можуть використовувати для повідомлення про можливі випадки; щонайменше один механізм повинен дозволити людям повідомляти про інциденти анонімно;
- Система для відстеження інформації про інцидент, статус;
- Смартфони, якими повинні використовувати члени команди для позачасової підтримки та комунікації на місці, шифрувальне програмне забезпечення, яке буде використовуватися для спілкування між членами команди, всередині підприємства та з третіми сторонами;
- Головна кімната для центрального зв'язку та координації; якщо постійна головна кімната не є необхідною або практичною, команда повинна створити процедуру закупівлі тимчасової кімнати, коли це буде необхідно;
- Безпечне сховище для забезпечення доказів та інших чутливих матеріалів.

Обладнання та програмне забезпечення для аналізу аварій:.

- Цифрові судово-медичні робочі станції та пристрої резервного копіювання для створення дискових зображень, збереження файлів журналів та збереження іншого відповідного інциденту;
- Ноутбуки для таких видів діяльності, як аналіз даних, написання звітів;
- Запасні робочі станції, сервери та мережеве обладнання або віртуалізовані еквіваленти, які можуть бути використані для багатьох цілей,

наприклад, відновлення резервних копій та спробування зловмисного програмного забезпечення;

- Портативний принтер для друку копій файлів журналів та інших доказів із систем, що не входять в мережу;
- Скупчення пакетів та аналізатори протоколів для захоплення та аналізу мережевого трафіку;
- Цифрове криміналістичне програмне забезпечення для аналізу зображень диска;
- Змінні носії з надійними версіями програм, які будуть використовуватися для збору доказів від систем;
- Аксесуари зі збору доказів, у тому числі твердозамкнені ноутбуки, цифрові камери, аудіореєстратори, сумки для зберігання доказів та мітки, а також докази, щоб зберегти докази можливих юридичних дій.

Ресурси аналізу інцидентів:

- Списки портів, включаючи звичайно використовувані порти;
- Документація для операційних систем, програм, протоколів, виявлення вторгнень та антивірусів;
- Мережеві діаграми та списки критичних активів, таких як сервери баз даних;
- Поточні базові рівні очікуваної мережі, системи і додатки діяльності;
- Криптографічні хеші критичних файлів для швидкого аналізу, підтвердження та знищення інцидентів.

Програмне забезпечення для пом'якшення наслідків події:

- Доступ до зображень чистої ОС та додатків для відновлення та відновлення цілей;
- Доступ до копій мережевих пристроїв та систем;

Група з реагування на інциденти створює комплект для використання, який є портативним та містить матеріали, які можуть знадобитися під час розслідування. Комплект повинен бути готовим до роботи завжди. Комплект

містять багато однакових елементів, перелічених у маркованих списках вище. є Кожен комплект включає в себе ноутбук, завантажений відповідним програмним забезпеченням (наприклад, sniffers пакетів, цифрова криміналістика). Інші важливі матеріали включають пристрої резервного копіювання, засоби масової інформації та основне мережеве обладнання та кабелі. Оскільки мета створення набору полягає в тому, щоб полегшити швидку реакцію, команда повинна уникати запозичення предметів.

Кожен виконавець повинен мати доступ щонайменше до двох обчислювальних пристроїв (наприклад, ноутбуків). Один комплект, повинен використовуватися для виконання перевірки пакетів, аналізу шкідливих програм та всіх інших дій, які можуть загрожувати забрудненню ноутбука, який їх виконує. Цей ноутбук повинен бути очищений, і все програмне забезпечення перевстановлюється, перш ніж його буде використано для іншого інциденту. Оскільки цей ноутбук є з спеціальним призначенням, він, імовірно, буде використовувати програмне забезпечення, відмінне від стандартних інструментів та конфігурацій підприємства, і, коли це можливо, виконавцям випадків слід дозволити вказувати основні технічні вимоги до цих спеціальних ноутбуків-розслідувачів. Кожен співробітник повинен також мати стандартний ноутбук, смартфон або інший обчислювальний пристрій для написання звітів, читання електронної пошти, і виконувати інші обов'язки, не пов'язані з аналізом практичних інцидентів. Вправи, що включають імітаційні інциденти, також можуть бути дуже корисними для підготовки персоналу для обробки інцидентів.

Виявлення та аналіз - інциденти можуть траплятися незліченними способами. Для підприємства найбільш складною частиною процесу реагування на інциденти є визначення та оцінка інцидентів, тип, обсяг та масштаб проблеми.

Існують технічні рішення, які можуть зробити виявлення легше, але кращим засобом є створення команди висококваліфікованих і досвідчених співробітників, які можуть ефективно аналізувати показники та вживати відповідні заходи.

Група з реагування на інцидент має швидко працювати над аналізом та перевіркою кожного інциденту за попередньо визначеним процесом та

документування кожного кроку. Коли команда вважає, що інцидент стався, команда повинна швидко виконати початковий аналіз, щоб визначити масштаб інциденту, наприклад, які мережі, системи чи програми зачеплені, хто чи що винен у винекненні інциденту; і як відбувається інцидент.

Викорінення стримування і відновлення. Більшість інцидентів потребують стримування, тому це важливий момент на початку кожного процесу. Зберігання забезпечує час для розробки спеціальної стратегії відновлення. Необхідною частиною стримування є прийняття рішень (наприклад, вимкнення системи, відключення його від мережі, відключення певних функцій). Такі рішення набагато простіше зробити, якщо існують заздалегідь визначені стратегії та процедури для утримання інциденту. Підприємства повинні визначати прийнятні ризики при розгляді інцидентів та відповідно розробляти стратегії.

Стратегії утримання залежать від типу інциденту:

- стратегія затримання інфекції від шкідливих програм дуже відрізняється від стратегії мережевої атаки DDoS.
- скомпрометований вузол може запустити шкідливий процес, який періодично впливає на інший хост. Коли обробник інцидентів намагається утримувати інцидент, відключивши з сеансу скомпрометований вузол, наступні пінги не зможуть виконати роботу.

  У результаті несправності, шкідливий процес може перезаписати або шифрувати всі дані на жорсткому диску хоста. Оброблювачі не повинні припускати, що тільки тому, що хост був відключений від мережі, подальше пошкодження хоста припинено.

Збір доказів з обчислювальних ресурсів представляє проблеми.

1. Бажано отримати докази від системи, як тільки виникає підозра, що інцидент може статися.

2. Багато інцидентів призводить до динамічного ланцюга подій; перший знімок системи може зробити більше користі у визначенні проблеми та її джерела, ніж у більшості інших дій, які можуть бути застосовані на цьому етапі.

3. Користувачам та системним адміністраторам слід ознайомитись із кроками, які вони повинні вжити для збереження доказів.

Діяльність після події - одну з найважливіших частин реакції на інциденти також найчастіше пропущеною є навчання та вдосконалення. Кожна група з реагування повинна розвиватися, щоб протистояти новим загрозам. Проведення "уроків" зустрічі з усіма зацікавленими сторонами після великого інциденту та, можливо, періодично після менших інцидентів, як це дозволяють ресурси, може бути надзвичайно корисним для покращення заходів безпеки та самого процесу обробки інцидентів.

Створення ефективного і адаптивного плану реагування на інциденти має вирішальне значення не тільки для виживання в нашому сучасному кіберпросторі, але також для контролю витрат на IT-безпеку і забезпечення захисту інтелектуальної власності та даних клієнтів від їх поширення та нанесення серйозного збитку бренду і довіри клієнтів підприємства. Забезпечуючи ефективні методи виявлення і чіткий процес оповіщення потрібного персоналу, чітко визначаючи ролі і обов'язки кожного члена групи реагування на інциденти, постійно тестуючи та впроваджуючи нові рішення для підтримки захисту в актуальному стані, приділяючи особливу увагу метрикам, які дійсно мають значення, і впровадженню програмного забезпечення для автоматизації, яке може допомогти аналітикам і інженерам зосередитися на відповідних загрозах, які потрібно створити, щоб план реагування на інциденти відповідав вимогам підприємства.

В основному виділяють два методи реагування на інцидент:

- Активний, в який входить прямий вплив на інцидент, його компоненти та затронуті ресурси.
- Пасивний, аналіз інциденту, його поведінки за допомогою допоміжних підсистем та засобів, які ніяк не впливають на інцидент.

В залежності від вибору методу реагування буду відрізнятись способи реагування, так при активному методі реагування способи будуть такі:

- Блокування мережевих з’єднань

- Блокування користувачів
- Побітове копіювання робочих станцій, серверів, мережевих пристроїв
- Вилучення носіїв пам’яті та жорстких дисків.
- Від’єднання від мережі підприємства.

При пасивному методі способи реагування доцільно використовувати на єтапі збору інформації про інцидент або коли відомо, що інцидент уже відбувся і шкода від нього є мінімальною, способи будуть такі:

- Отримання інформації від підсистем захисту інформації (SIEM, DLP, Sandblast, антивірус)
- Отримання журналів подій з мережевих пристроїв та затронутих систем
- Опитування постраждалих осіб або можливо винуватих в інциденті
- Консультація з профільними спеціалістами затронутих систем

Насправді список активних та пасивних способів реагування є невичерпним і залежить від кожного типу інцидента, ресурсів та можливостей підприємства.

Група реагування на інциденти

Групи реагування на інциденти — це групи IT-фахівців, які готуються до кібератак і реагують на них. До обов’язків групи реагування на інциденти входить розробка проактивного плану реагування на інциденти, тестування та усунення вразливостей системи, дотримання найкращих практик безпеки та надання підтримки для всіх дій з обробки інцидентів.

Члени групи реагування на інциденти зазвичай мають різні навички, досвід і ролі, тож вони можуть підготуватися до низки інцидентів безпеки.

Конкретний набір навичок груп реагування на інциденти організацій може відрізнятися, оскільки компанії мають різні персональні профілі ризиків і бізнес-процеси. Загалом, основними функціями членів групи реагування на інциденти є:

Керівництво — координує загальний напрямок і стратегію реагування, звільняючи решту команди на зосередженні мінімізації збитків, швидкому відновленні та ефективній роботі.

Розслідування — координація зусиль для визначення першопричини інциденту, що допомагає усунути поточні загрози та запобігти майбутнім. Для цього важливо зібрати якомога більше відповідної інформації.

Комунікації — керуйте відповідними внутрішніми та зовнішніми комунікаціями, необхідними для реагування на інциденти. Може знадобитися спілкування між командами та відділами всередині організації або із зовнішніми зацікавленими сторонами.

Документація — запис дій і дій з реагування на інциденти.

Юридичне представництво — захистіть організацію, забезпечивши відповідність діяльності з реагування на інциденти законам і нормам.

Структура для використання інструментів реагування на інциденти

Окрім звернення за адміністративною підтримкою та дотримання задокументованого плану реагування на інциденти, інструменти реагування на інциденти є ключовими для підготовки до інцидентів безпеки та реагування на них. Інструменти кібербезпеки слід впроваджувати задовго до того, як станеться інцидент, оскільки вони можуть надавати важливу інформацію, яку можна використовувати для виявлення, розслідування та реагування на інциденти.

Більшість організацій уже мають загальні засоби контролю безпеки для підтримки можливостей реагування на інциденти, зокрема щодо реєстрації та попередження. Однак існують спеціальні інструменти, які можуть направляти команду через робочий процес реагування на інциденти та надавати всі деталі, необхідні для прийняття обґрунтованого рішення.

Деякі організації дотримуються циклу спостерігати, орієнтуватися, вирішувати, діяти (OODA), щоб надати вказівки щодо того, які інструменти потрібні та коли. Цей військовий підхід до реагування на інцидент передбачає чотириетапний підхід до загроз:

Оцініть видимість мережевого трафіку, операційної системи та програм — установіть базову лінію для середовища організації та надайте інформацію в реальному часі про те, що сталося до, під час і після інциденту безпеки.

Збирайте контекстну інформацію - збирайте детальну контекстну інформацію та розвідку про існуючі загрози та поточні атаки.

Збирайте інформацію в режимі реального часу та криміналістичну інформацію – збирайте інформацію про активні загрози, що виникають на даний момент, і аномальну поведінку (а також виконуйте реактивне дослідження після події), щоб допомогти командам безпеки приймати обґрунтовані рішення про те, як реагувати.

Усунути загрозу – вжити заходів для усунення загрози, мінімізувати ризик і вплив на бізнес і повернутися до нормальної роботи.

Цикл OODA може керувати використанням інструментів реагування на інциденти протягом усього процесу реагування на інциденти.

Категорії засобів реагування на інциденти

Існує кілька типів інструментів, корисних для реагування на інциденти:

Оркестровка безпеки, автоматизація та реагування (SOAR)

SOAR відноситься до платформ, які пропонують інструменти для збору даних безпеки з різних джерел. Рішення SOAR може поєднувати машинне навчання та людський вхід для аналізу даних, отримання розуміння та визначення пріоритетів відповідних процедур реагування на інциденти.

Програмне забезпечення SOAR зазвичай включає три можливості:

Управління загрозами та вразливістю

Реагування на інцидент

Автоматизація операцій безпеки

Організації використовують SOAR для збору та аналізу даних, пов’язаних із загрозами, із різноманітних джерел, що забезпечує автоматичне реагування на загрози.

Аналітика поведінки користувачів і суб’єктів (UEBA)

Рішення UEBA використовують великі набори даних і машинне навчання для встановлення базових показників для типових моделей поведінки, що дозволяє їм ідентифікувати нетипову поведінку в мережі, яка може вказувати на загрози. Акцент на підозрілій поведінці дозволяє UEBA виявляти загрози, які

можуть оминути традиційні інструменти безпеки та антивірусні засоби, включно з атаками, не заснованими на зловмисному програмному забезпеченні.

УЄБА використовує поведінкові моделі для оцінки рівнів загрози, надаючи оцінки ризику, щоб керувати процесом реагування.

Інформація про безпеку та керування подіями (SIEM)

SIEM — це підхід до управління безпекою, який забезпечує уніфіковану систему для поєднання функцій керування інформацією та подіями. Рішення SIEM розгортають кілька агентів збору даних для ієрархічного збору даних про події із серверів, пристроїв кінцевих користувачів та мережевої інфраструктури. Центральна консоль керування об’єднує дані, дозволяючи аналітикам безпеки фільтрувати шум і визначати пріоритети реальних інцидентів безпеки.

Виявлення кінцевої точки та відповідь (EDR)

Системи EDR збирають і аналізують дані безпеки кінцевих точок, щоб захистити мережу від вразливих пристроїв і робочих станцій користувачів. EDR спрямований на виявлення порушень безпеки в режимі реального часу, що забезпечує швидке реагування. Цей підхід допомагає ідентифікувати нові та прогресивні загрози, які традиційні засоби безпеки можуть не використовувати. Конкретні можливості кожного рішення EDR можуть значно відрізнятися.

Розширене виявлення та реагування (XDR)

Рішення XDR — це інструменти SaaS для виявлення загроз безпеці та впровадження процедур реагування на інциденти. Інструменти XDR об’єднують кілька можливостей безпеки в уніфіковане рішення для операцій безпеки, що робить складні можливості реагування на інциденти більш доступними та доступними.

Перевагою XDR є консолідація кількох продуктів безпеки, що базуються на можливостях EDR. Він може підвищити продуктивність операцій безпеки завдяки вдосконаленому виявленню та реагування, а також централізованій видимості та контролю в корпоративному середовищі. Інструменти XDR приймають і дистилюють кілька телеметричних потоків і аналізують вектори загроз і тактику.

Вони допомагають прискорити реагування, керуючи процесами виявлення та розслідування.

Дізнайтеся більше в нашому докладному посібнику з інструментів реагування на інциденти

Служби реагування на інциденти

Реагування на інциденти є найефективнішим, якщо їх швидко здійснюють досвідчені служби реагування. Організаціям часто не вистачає ресурсів для підтримки повноцінної групи реагування на інциденти, яка працює 24 години на добу. Одним із варіантів є робота із зовнішньою організацією, яка надає професійні послуги реагування на інциденти.

Взаємодія з цими організаціями дає такі переваги:

Доступність — чим швидше команда реагування на інциденти приступить до роботи, тим менша вартість і менший вплив атаки на організацію. Інциденти кібербезпеки можуть статися в будь-який час, і може бути важко зв’язатися з членами групи реагування на інциденти в неробочий час. Професійні постачальники послуг з реагування на інциденти мають кілька команд персоналу, щоб забезпечити краще покриття та більшу доступність.

Досвід — неправильне поводження з інцидентами безпеки може збільшити витрати та завдати шкоди організації. Наприклад, атака програм-вимагачів може дестабілізувати заражену систему, що означає, що зашифровані дані можуть не відновитися після перезавантаження. Професійні спеціалісти з реагування на інциденти мають досвід, необхідний для ефективного й точного вирішення таких інцидентів безпеки.

Спеціалізований досвід — реагування на інциденти часто потребує досвіду в таких сферах, як криміналістичний аналіз і зворотне проектування зловмисного програмного забезпечення. Хоча більшості компаній не потрібно володіти цими навичками, спеціальна група реагування на інциденти має доступ до експертів, необхідних для належного вирішення інцидентів кібербезпеки.

Управління всім процесом реагування на інциденти — зовнішні постачальники реагування на інциденти повинні підтримувати всі потреби

організації у реагуванні на інциденти. Це включає підготовку до реагування на інциденти, керування виявленими вторгненнями та пом’якшення майбутніх атак.

Висновки до першого розділу

Аналіз інцидентів ІБ дозволяє визначити інцидент, своєчасно зреагувати на подію та підібрати ефективні дії і засоби для стримування, локалізації інциденту та його наслідків. Класифікація типів та видів інцидентів на підприємстві дає змлгу з’ясувати маштаби інциденту та ризики. Коректні підсистеми захисту (SIEM, DLP), дозволяють своєчасно виявити інцидент, зменшити його вплив на підприємство або навіть попередити його. Способи та методи реагування на інциденти зменшать час, який потрібен ГРІІБ на прийняття рішень.

РОЗДІЛ 2.
ПРИЧИНИ ВИНИКНЕННЯ ІНЦИДЕНТІВ

Оскільки компанії більше, покладаються на IT-системи, стає все більш важливим усвідомлювати ризики інформаційної безпеки і те, що ви можете зробити для захисту своєї підприємства.

Існує п’ять основних причин виникнення інцидентів [10]:

1. Зловмисні або випадкові дії з боку внутрішнього персоналу. У 60% всіх організацій які зіткнулися з порушеннями безпеки половина з них була здійснена діями внутрішнього персоналу. Наприклад, співробітниками, випадково залишили конфіденційну інформацію в поїзді, або в деяких випадках, зловмисно пропускаючи інформацію.

2. Віруси. Найбільш поширений приклад зовнішніх атак - комп'ютерні віруси. Вони прикріплюються до невинного повідомлення електронної пошти або програмами на заражених USB-пристроях. Після відкриття вони можуть переписати ключові частини системи, щоб навмисно пошкодити здатність компанії продовжувати працювати, або надати зовнішній доступ до конфіденційної інформації.

3. Фішинг. Фішинг - досить поширений вид шахрайства. Саме тут електронні листи відправляються від осіб, що не працюють в компанії, прикидаючись, що вони отримані з законного джерела, і запитують конфіденційну інформацію (наприклад, особисті дані клієнта). Вони також можуть містити веб-посилання, яке вказує співробітнику точну копію загального веб-сайту (наприклад, інтернет-банку, який вони використовують). Як тільки вони вводять дані свого логіна, вони фактично передають цю інформацію зовнішній особі, яка потім може отримати доступ до облікового запису.

4. Взлом. Хакерство - це коли окремі користувачі використовують спеціалізоване письмове програмне забезпечення для атаки на системи компанії,

часто намагаючись переписати доступ до системи, щоб дозволити їм читати і отримувати конфіденційні дані.

5. Атака на комп'ютерну мережу. Це атака на систему підприємства, яка не дозволяє системі працювати до тих пір, поки атака не буде зупинена (зазвичай після виплати «викупу»). Оскільки підприємства більше, ніж будь-коли, покладаються на свої IT-системи, вкрай важливо забезпечити наявність засобів управління для управління і зниже

Більшість мереж створюються, обслуговуються і використовуються людьми, і ці люди схильні до помилок та ряду обмежень (наприклад, бюджети, пріоритети виробництва). Компанії повинні виходити з того, що навіть якщо вони встановлюють самі передові технологічні рішення і отримують певні сертифікати безпеки, їх заходи безпеки можуть зазнати невдачі, і стороння людина може отримати доступ до свого середовища.

2.1. Вплив інциденту на діяльність та результат підприємства

Кожен бізнес, незалежно від його розміру, є потенційною метою кібератаки. Успішна кібератака може завдати серйозної шкоди бізнесу. Це може вплинути на прибуток, а також на положення бізнесу і довіру споживачів. Наслідки злому безпеки в цілому можна розділити на три категорії: фінансові, репутаційні та юридичні [9].

Економічна (фінансова) вартість кібератаки часто призводять до суттєвих фінансових втрат, що виникають в результаті:

- крадіжки корпоративної інформації;
- крадіжки фінансової інформації (наприклад, банківські реквізити або реквізити платіжної картки)
- крадіжки грошей;

- порушення торгівлі (наприклад, неможливість проводити транзакції онлайн);
- втрати бізнесу або контракту.

Підприємства, які постраждали від кібер-порушення, також зазвичай несуть витрати, пов'язані з ремонтом вразливих систем, мереж і вимушені простої.

Фахівці вивчають, як підприємство, піддалася атаці, порівнюється з іншою подібною компанією, яка не постраждала від кібер-вторгнення. Існує проблема в тому, що вони не можуть бути повністю впевнені, що підприємство порівняння насправді теж не піддалася атаці. Однак в тій мірі, в якій фінансова картина впливає не на саму атаку, а на її розкриття, методологія працює. Наприклад, вплив на оцінку фондового ринку, пов'язано з розкриттям критичної інформації підприємства. З огляду на це застереження, результати припускають істотні, але не катастрофічні ефекти від розкритих кібер-порушень. Середня втрата ринкової капіталізації після атаки становить близько 1 відсотка, причому великі втрати пов'язані з використанням особистої фінансової інформації і менші втрати. В середньому взлом особистої фінансової інформації призводить до втрати ринкової вартості в розмірі трохи менше 1,5 мільярда доларів. Повторні атаки викликають диспропорційні ефекти. Також вважається, що фірми з наглядом за ризиками в раді директорів знижують ризик винекнення витоку інформації та зменшують наслідки після вдалої атаки. У дослідженні також оцінюється вплив атаки на фактори, що виходять за рамки фондового ринку. Визначається зниження зростання продажів більш ніж на 3 відсотки в середньому і більш ніж на 5 відсотків для підприємств роздрібної торгівлі. Виявляється, що фірми скорочують інвестиції, збільшують борг і відчувають зниження свого кредитного рейтингу.

Одним з нових підходів захисту підприємства від витрат на кібератаки є кіберстрахування, яке виплачується підприємства після атаки.

Кіберстрахування призначене для виконання ряду завдань:

- воно надає організаціям інформацію і досвід після порушення;
- допомагає отримати дохід і сплатити судові витрати, пов'язані з інцидентом;

- допомагає підприємствам мінімізувати порушення роботи IT-фахівців;
- покривають вартість штрафів, стягнутих державними / приватними організаціями, або витрати на розслідування, пов'язані з цими штрафами.

Важливо розуміти, що не всі поліси кіберстрахування забезпечують таке покриття. Існують також політики, які обмежують те, що входить в покриття, скільки виплачується і коли починається страхування. Кіберстрахування є важливою і цінною гарантією, але не слід припускати, що всі штрафи будуть оплачені.

Кіберстрахування важливо для всіх підпрриємств, незалежно від їх розміру, галузі або нормативних зобов'язань. Кожне підприємство стикається з цим ризиком навмисного нападу або випадкового порушення. Також немає підприємств, які мають надійну кібербезпеку. В результаті всі підприємства повинні очікувати порушення. Коли всі інші засоби захисту не працюють, кіберстрахування забезпечує стабільність, безпеку та душевний спокій, захищає постраждалі фірми. Цей підхід накладає відповідальність на страховиків, щоб оцінити ризики і стати центром передової практики, якої повинні дотримуватися застраховані фірми. Однак існують серйозні питання про те, чи успішно страхові компанії, що виходять на цей ринок, виконують необхідні завдання. У міру розвитку кіберзагроз міцний ринок кіберстрахування може не тільки пом'якшити фінансові наслідки для підприємтва, але і мінімізувати частоту успішних спроб злому, що також допоможе захистити споживачів.

Репутаційний збиток. Довіра є важливим елементом відносин з клієнтами. Кібератаки можуть зашкодити репутації бізнесу і підірвати довіру ваших клієнтів до вас. Це, в свою чергу, може привести до:

- втрата клієнтів;
- втрата продажів;
- зменшення прибутку.

Наслідки нанесення шкоди репутації можуть вплинути на постачальників або вплинути на ваші стосунки з партнерами, інвесторами та іншими третіми сторонами, якими підприємство наділена.

Підвищення репутаційних ризиків - ймовірність відхилення від запланованих показників діяльності підприємства через здійснення активно-пасивних операцій, їх організацію, стан корпоративного управління та вплив факторів зовнішнього середовища, наслідки якої можуть бути негативними, нульовими або позитивним. Це впливає на спроможність підприємства встановлювати нові відносини з контрагентами, надавати нові послуги або підтримувати відносини, що склалися. Ризик репутації може привести підприємство (або його керівників) до фінансових втрат або зменшення клієнтської бази. Цей ризик має місце на всіх рівнях підприємства, і тому підприємства повинні відповідально ставитися до своїх відносин із клієнтами та суспільством. Система управління ризиком репутації підприємства складається з регламентних документів — політик, положень, процедур, процесів тощо, які затверджуються відповідно до обраної форми корпоративного управління з урахуванням розміру банку та складності його операцій.

Система управління ризиком репутації охоплює:

- політику й положення щодо управління ризиком репутації, які мають бути розглянуті та затверджені відповідно до обраної підприємством форми корпоративного управління. Політика і положення повинні періодично переглядатися, та охоплювати стандарти роботи з клієнтами та іншими зовнішніми сторонами, роботи з інформацією та наймання персоналу з відповідною позитивною репутацією;
- інформаційну систему управління (форми звітності, схема документообігу тощо) для спостережної ради, правління або профільних колегіальних органів підприємства, щодо моніторингу вразливості всіх видів діяльності підприємства до;

- процес контролю за репутацією клієнтів підприємства для уникнення контактів із клієнтами з незадовільною репутацією, що (контакти) можуть негативно вплинути на репутацію самого підприємства.

Крім того, для адекватного управління ризиком репутації підприємство може проводити регулярний моніторинг повідомлень засобів масової інформації про підприємство, пов’язані з ним структури та клієнтів з метою вжиття відповідних заходів, спрямованих на підтримання та відновлення позитивної репутації підприємства та його іміджу.

Правові наслідки кібератак. Закони про захист даних і конфіденційність вимагають, щоб керування безпекою охоплювало всі особисті дані - будь то співробітників або клієнтів. Якщо ці дані випадково або навмисно скомпрометовані, і не можна застосувати відповідні заходи безпеки, підприємство може зіткнутися з штрафами і регулятивними санкціями. Щоб повністю зрозуміти ризики, які представляє кібербезпека, необхідно зрозуміти закони і штрафи, які застосовуються.

В Україні до кіберзлочинів відносять порушення авторського права і суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення; ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних предметів, незаконне збирання з метою використання відомостей, що становлять комерційну або банківську таємницю.

Згідно закону України «Про основні засади забезпечення кібербезпеки України» № 2469-VIII від 21.06.2018р. зі змінами від 22.08.2022, правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, укази Президента

України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України. Якщо міжнародним договором України, згоду на обов’язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

Конкретні закони, застосовні до бізнесу, залежать від типу бізнесу і типу даних, з якими воно працює.

Підприємства не зобов'язані підтримувати будь-які конкретні типи засобів захисту від кібербезпеки, але вони несуть відповідальність, якщо ці засоби захисту виявляються недостатніми.

Підприємства мать дотримуватись міжнародним законам і галузевим стандартам.

Загальний стан речей про захист даних (GDPR)

Звіт правил призначений для захисту особистої інформації усіх громадян в Європейському Союзі. Оскільки багато компаній працюють з європейськими фірмами і клієнтами, дані підприємства повинні відповідати GDPR. На відміну від більшості законів про кібербезпеки, цей зобов'язує використовувати шифрування.

- Стандарти безпеки даних індустрії платіжних карт (PCI DDS)

Будь-яка організація, яка приймає платіжні картки - кредитні та дебетові картки і т.д. підпадає під дію цього закону, розробленого галузю платіжних карток. Підприємства повинні відповідати 12 вимогам, пов'язаним із захистом інформації про платіжну картку. Порушення PCI DDS обкладає підприємства мінімальними штрафами в розмірі 5000 доларів США в місяць і максимальними штрафами 100 000 доларів США на місяць.

Для покращення відповідності нормативним документам підприємства потрібно виконати декілька кроків:

- першим кроком є розуміння конкретних законів про кібербезпеку, які застосовуються до підприємства;
- другий крок - зрозуміти, які саме рівні безпеки і захисту можуть знадобитися в цих законах і як вони визначають порушення закону.

Таким чином, не існує єдиної стратегії для досягнення 100-відсоткової відповідності. Проте, існують передові методи, яким можуть слідувати всі підприємства, щоб запобігти інцидентам, які призводять до штрафів і зборів:

- інвентаризація IT обладнання та програмного забезпечення. Розуміння всього обсягу IT-інфраструктури гарантує, що вразливості і ризики не будуть приховані від очей;
- Виконати аналіз прогалин. Визначення відстані між реальними та необхідними рівнями захисту показує, що і де потрібно найбільше для роботи;
- Провести оцінку ризику. Включає в себе розуміння найбільш поширених і непрямих типів загроз, а потім оцінку того, наскільки добре поточні заходи безпеки захищають від них.
- Розробити і задокументувати план безпеки. Кібербезпека вимагає більше, ніж просто технологію. План безпеки описує політики, протоколи та пріоритети для кожного можливого типу атаки. Якщо і коли відбувається інцидент, план повинен точно визначити, які дії повинні зробити різні департаменти і окремі особи.
- Впровадити нові заходи безпеки. Робота в рамках закону часто вимагає оновлення технічних і логістичних оновлень до кібербезпеки;
- Аудит контролю безпеки. Тестування і оцінка того, наскільки ефективно працюють різні засоби захисту, дозволяє організаціям виконувати оновлення до цього, а атаки виявляють слабкість;
- Виконання рекомендацій аудиту. Знання слабких місць марна справа, якщо підприємства не хочуть вкладати час і ресурси, необхідні для поліпшення кібербезпеки.

2.1.1. Оцінка інцидентів інформаційної безпеки

Швидкий розвиток інформаційних технологій обумовлює необхідність приділяти належну увагу забезпеченню інформаційної безпеки, відповідності її стану швидким змінам в технологіях, що забезпечує зменшення ймовірності настання ризиків, пов’язаних з інформаційними загрозами. Найбільшу увагу при формуванні систем інформаційної безпеки на вітчизняних підприємствах, приділяють, як правило, виконанню вимог нормативно-методичної бази в сфері захисту інформації, визначаючи ці вимоги як першооснову становлення системи інформаційної безпеки, що, однак, само по собі ще не створює гарантій достатнього рівня захисту. Організація може виділяти значні ресурси для забезпечення стійкості і стабільності функціонування корпоративних інформаційних систем, що однак не гарантує досягнення навіть мінімального рівня безпеки інформації. Суть проблеми полягає в тому, що при проектуванні та побудові системи захисту інформації основна увага має бути приділена не мінімізації впливів з певного переліку типових загроз, складеному відповідно до деякого уявного середовища функціонування підприємства, а виявленню та мінімізації інформаційних ризиків, пов’язаних з практичною діяльністю конкретної підприємства. Саме формування реального профілю ризиків, пов’язаних з процесами діяльності підприємства, зменшення цих ризиків або їх нейтралізація при збереженні постійного контролю ризикової ситуації становить суть провідних сучасних концепцій створення систем захисту інформації. На жаль, сама сутність методології ризиків обумовлює певні труднощі у своєму практичному застосуванні, бо вимагає обчислення високоточних оцінок інформаційних ризиків, оперування з ними й передбачає необхідність певної індивідуалізації, винятковості отриманих в рамках цього підходу рішень.

Зважаючи на те, що оцінка інцидентів на якісному рівні не дозволяє однозначно порівняти витрати на забезпечення інформаційної безпеки і отриманої від них віддачі (у вигляді зниження сумарного ризику), зосередимося на більш

точному кількісному підході. Зазначимо, що в цьому разі процедура побудови систем захисту інформації на базі методології інформаційних ризиків із застосування настанов основних стандартів. По-перше, це необхідність параметризації інцидентів. Загальновживане математичне співвідношення, за яким обчислюються ризик, обумовлений можливою реалізацією інцидента (Т), має вигляд:

$$I_T = P_T q = P_t P_V q$$

де $P_T -$ ймовірність реалізації загрози Т, $q -$ збитки, що виникають за умов реалізації інциденту Т, $P_t -$ ймовірність виникнення (активації) інциденту Т, $P_V -$ ймовірність вдалого використання зловмисником уразливостей інформаційної системи, що призводить до реалізації інциденту Т. Тобто обчислення ризику потребує знання двох або трьох параметрів ризику інцидента Т, які звичайно визначаються експертним шляхом, що може суттєво погіршити якість оцінок інцидентів, а відтак – абсолютно непрогнозовано вплинути на кінцеві результати менеджменту інцидентів ІБ [13].

2.2. Організація статистичного спостереження інцидентів інформаційної безпеки

Встановлено, що частота всіх кібер-інцидентів зростає. Норма тривалості інцидентів п'ять годин, всередньому 45 інцидентів на місяць. Аналіз рівня інцидентів для різних векторів атаки дає більш детальне уявлення кіберзахисту на підприємстві. 85% фахівців з кібербезпеки пояснюють збільшення кількості кібератак використанням генеративного ШІ поганими акторами (CFO). Близько 46% респондентів вважають, що інтеграція генеративного ШІ в бізнес-операції збільшить вразливість до кібератак (CFO). Занепокоєння з приводу штучного інтелекту в кібербезпеці включають можливість посилення проблем із конфіденційністю (39%), невиявлених фішингових атак (37%) і загального

збільшення обсягу та швидкості атак (33%) (CFO). 85% фахівців з кібербезпеки пов’язують зростання кількості кібератак зловмисниками, які використовують генеративний штучний інтелект (CFO

Однією з головних вимог відповідності нормативним документам для підприємств є документування інцидентів безпеки. Далі будуть детально описані кроки, які організаціям потрібно використовувати, якщо вони документують інциденти безпеки (таблиця. 2.1).

- Крок 1: Контактна інформація. Звіт про інцидент безпеки повинен містити певну інформацію для відповідності вимогам. Найкраще зробити форму, яка буде містити певну інформацію в різних розділах. Перший розділ, який потрібно зробити, це контактна інформація. Інформація повинна включати:
  - ім'я та посада особи, яка звітує інформацію;
  - робочий та мобільний номер телефону;
  - ПІБ співробітника служби безпеки підприємства;
  - адреса електронної пошти.
- Крок 2: Опис інциденту безпеки. Звіт про інцидент безпеки повинен мати розділ, призначений для опису інциденту безпеки. У цьому розділі небхідно бути локонічними, але включати якомога більше подробиць про інцидент безпеки. Це не тільки буде добре виглядати для аудиторів, але і послужить хорошою документацією по часто виникаючих проблемах безпеки, з якими стикається організація.
- Крок 3: Вплив або потенційний вплив. Документуйте будь-який вплив, який цей інцидент безпеки міг нвнести підприємства. Необхідно уявити це, як текстове поле довільної форми для заповнення, прапорці поруч з зумовленими типами впливу або підхід, в якому використовуються обидва. Якщо обов’язково використовувати зумовлені типи впливу, вони повинні включати наступне:
  - втрата даних / компрометація даних;
  - затронуті системи;
  - фінансовий збиток;
  - порушення к/ц/д;

- порушення нормативно-правових документів підприємства;
- інше.

- Крок 4: Чутливість інформації. Можна класифікувати рівень чутливості інформації, пов'язаної з порушенням безпеки. Для кожного вибору співробітник з безпеки захоче включити приклад інформації, яка відповідає кожному з різних рівнів чутливості. Потрібно використати такі рівні:

- тільки для внутрішнього користування;
- обмежена або конфіденційна (порушення політики конфіденційності)
- невідома

Після визначення рівнів чутливості встановіть прапорець для різних рівнів. Також включіть область текстового поля для короткого опису інформації, яка була взломана.

- Крок 5: Повідомлення. Увімкніть розділ, в якому описано, хто ще був повідомлений про інцидент безпеки. Не забудьте вказати ім'я та посаду людини в підприємства.

- Крок 6: Подробиці інциденту. Цей розділ представляє собою короткий огляд вищенаведеного розділу. Це повинні бути короткі відповіді на заздалегідь поставлені запитання про інцидент безпеки. Питання про подію повинні включати:

- дату і час початку виявлення інциденту безпеки;
- фізичне розташування ураженої системи або інформації;
- кількість порушених фізичних місць;
- кількість систем, пошкоджених інцидентом безпеки;
- кількість користувачів, на яких вплинув інцидент безпеки;
- будь-яка інша додаткова важлива інформація про інцидент безпеки.

- Крок 7: Пом'якшення. Цей розділ повинен містити відомості про те, які дії вчинила організація для пом'якшення інциденту безпеки. Відповідь має бути короткою, але включати всю відповідну інформацію.

- Крок 8: Підпис співробітника служби безпеки. Звіт про інцидент безпеки повинен включати підпис співробітника служби безпеки, який займався створенням звіту про інцидент та підписи всіх членів групи реагування.
- Крок 9: Журнал інцидентів безпеки. Крім звіту про інцидент безпеки, співробітникам служби безпеки також доручено створення і ведення журналу інцидентів безпеки. Журнал інцидентів безпеки - це короткий документ, який розповість вам більшу частину того, що ви хочете дізнатися з першого погляду. Деякі елементи, які ви хочете включити в свій журнал інцидентів безпеки, - це час, дата і хто виявив інцидент безпеки, разом з коротким описом того, що було інцидентом безпеки.

Якщо журнал інцидентів безпеки відрізняється від звіту про інциденти безпеки, використовується шкала відповідності. Журнал повинен містити елемент, який оцінює серйозність інциденту безпеки від 1 до 5, де 1 - найменш серйозний, а 5 - найбільш серйозний.

- Крок 10: Утримання. Для забезпечення відповідності підприємства повинні зберігати всі звіти і журнали інцидентів безпеки протягом шести років. Цей шестирічний період починається під час останнього запису [15]. Нижче наведено приклад формування звіту інцидента інформаційної безпеки (табл.2.1).

Таблиця. 2.1

Звіт інциденту інформаційної безпеки

№	
Місце винекнення інциденту	м. Київ, ФОП "Кряк", вул. Січових стрільців 23
Початок винекнення інциденту	15.12.21 р.
Дата виявлення інциденту	16.12.21 р.
Дата звітності	23.12.21 р.
Дата закриття інциденту	23.12.21 р.
Ким виявлено	Адміністратор управління інцидентами інформаційної безпеки
Відповідальний за оброку інциденту	Малина О.М. - головний інженер.
Вид інциденту	Витік інформації з обмеженим доступом
Тип інциденту	ВитікКТ

Затронуті системи	Електронна пошта
Порушено К/Ц/Д	Конфіденційність
Збитки	Невиявлено
Порушено	Нормативні документи підприємства
Винуватець	Жолудь Є.О. - секретар
Опис інциденту	
Було виявлено 16.12.21р. пересилання з робочої скриньки Жолудь Є.О на зовнішню скриньку kjdfghdfkj@gmailk.row файл "Договір.doc" що містить дані клієнтів та гриф "Комерційна таємниця".	
Вжиті заходи	
Проведено службове розлідування, файли з обох робочих скриньок видалено, Жолудь Є.О отримала догану.	
Дії щодо неповторення в майбутньому	
Проведення додаткового тестування співробітників підприємства	
Відповідальний за обробку звіту	
Голова групи реагування	
Члени групи реагування	
Члени групи реагування	
Члени групи реагування	
Члени групи реагування	
Члени групи реагування	
Члени групи реагування	

Для контролю виконання інцидентів, спрощеного перегляду інформації, щодо інцидентів та створення статистики інцидентів інформаційної безпеки потрібно створювати журнал інцидентів інформаційної безпеки який буде спиратись на звіти інцидетів (табл. 2.2).

Таблиця 2.2

Журнал інцидентів інформаційної безпеки

Місце винекнення інциденту	Дата виявлення інциденту	Дата звітності	Дата закриття інциденту	Вид інциденту	Порушено К/Ц/Д	Опис інциденту
м. Київ, ФОП "Кряк", вул. Січових стрільців 23	16.12.18 р.	23.12.18 р.	23.12.18 р.	Витік інформації з обмеженим доступом	Конфіденційність	Було виявлено 16.12.18 р. пересилання з робочої скриньки Жолудь Є.О на зовнішню скриньку kjdfghdfkj@gmailk.row файл "Договір.doc" що містить дані клієнтів та гриф "Комерційна таємниця".
м. Київ, ФОП "Кряк", вул. Січових стрільців 23	16.12.18 р.	23.12.18 р.	23.12.18 р.	Витік інформації з обмеженим доступом	Конфіденційність	Було виявлено 16.12.18 р. пересилання з робочої скриньки Жолудь Є.О на зовнішню скриньку kjdfghdfkj@gmailk.row файл "Договір.doc" що містить дані клієнтів та гриф "Комерційна таємниця".
м. Київ, ФОП "Кряк", вул. Січових стрільців 23	16.12.18 р.	23.12.18 р.	23.12.18 р.	Витік інформації з обмеженим доступом	Конфіденційність	Було виявлено 16.12.18 р. пересилання з робочої скриньки Жолудь Є.О на зовнішню скриньку kjdfghdfkj@gmailk.row файл "Договір.doc" що містить дані клієнтів та гриф "Комерційна таємниця".
м. Київ, ФОП "Кряк", вул. Січових стрільців 23	16.12.18 р.	23.12.18 р.	23.12.18 р.	Витік інформації з обмеженим доступом	Конфіденційність	Було виявлено 16.12.18 р. пересилання з робочої скриньки Жолудь Є.О на зовнішню скриньку kjdfghdfkj@gmailk.row файл "Договір.doc" що містить дані клієнтів та гриф "Комерційна таємниця".
м. Київ, ФОП "Кряк", вул. Січових стрільців 23	16.12.18 р.	23.12.18 р.	23.12.18 р.	Витік інформації з обмеженим доступом	Конфіденційність	Було виявлено 16.12.18 р. пересилання з робочої скриньки Жолудь Є.О на зовнішню скриньку kjdfghdfkj@gmailk.row файл "Договір.doc" що містить дані клієнтів та гриф "Комерційна таємниця".

Статистичні дані інцидентів інформаційної безпеки підприємства допомогають зрозуміти яку шкоду може нанести інцидент, які засоби захисту краще використовувати з огляду на повторюваність інцидентів. Також статистика сприяє створенню рекомендацій по оптимізації процесів реагування на іциденти, покращення методик виявлення інцидентів та підвищенню рівня інформаційної безпеки підприємства.

Нижче буде наведено ряд статистичних даних, які використовувались в практиці фінансового підприємства для аналізу вжитих заходів по запобіганню інцидентів інформаційної безпеки. Для створення діаграм використовувались дані з 2021року по 2022 рік (рис. 2.3), дані за 2023 рік (рис.2.4).

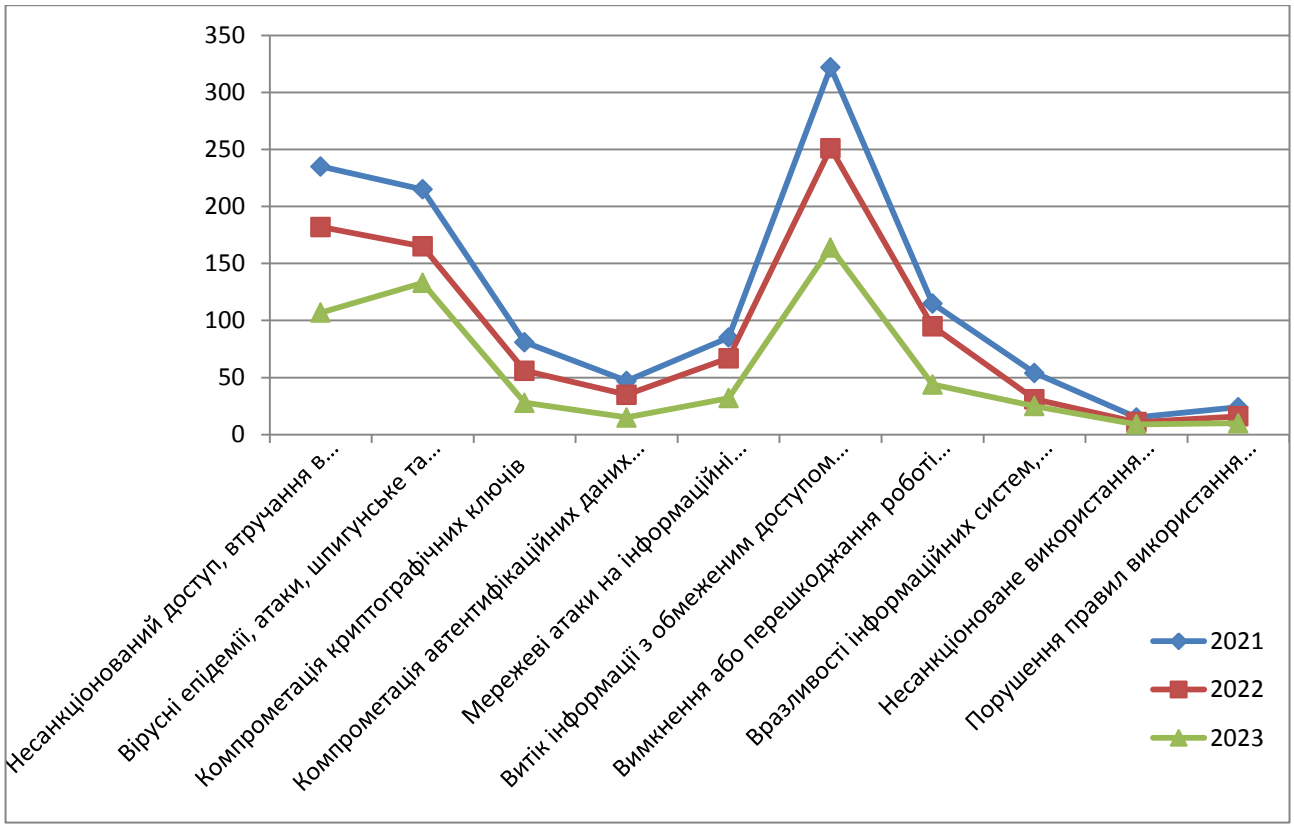

Рис. 2.1. Динаміка інцидентів

В період з 2021 року по 2023 рік на підприємстві було проведено ряд заходів щодо підвищення рівня інформаційної безпеки. В 2021 та 2023 році було введено SIEM та DLP, що знизило загальну кількість інцидентів, але не суттєво. В кінці 2022 року та на початку 2023 була створена ГРІІБ та План дій групи реагування підприємства на виявлені інциденти, що спричинило своєчасне реагування на інциденти, якісний аналіз інцидентів ІБ та документування даних, втому числі статистичних, що в свою чергу дало змогу возначити основні причини інцидентів. Визначення причин та прийняття заходів по відповідно причинам сприяло значному зниженню кількості інцидентів ІБ в 2023 році.

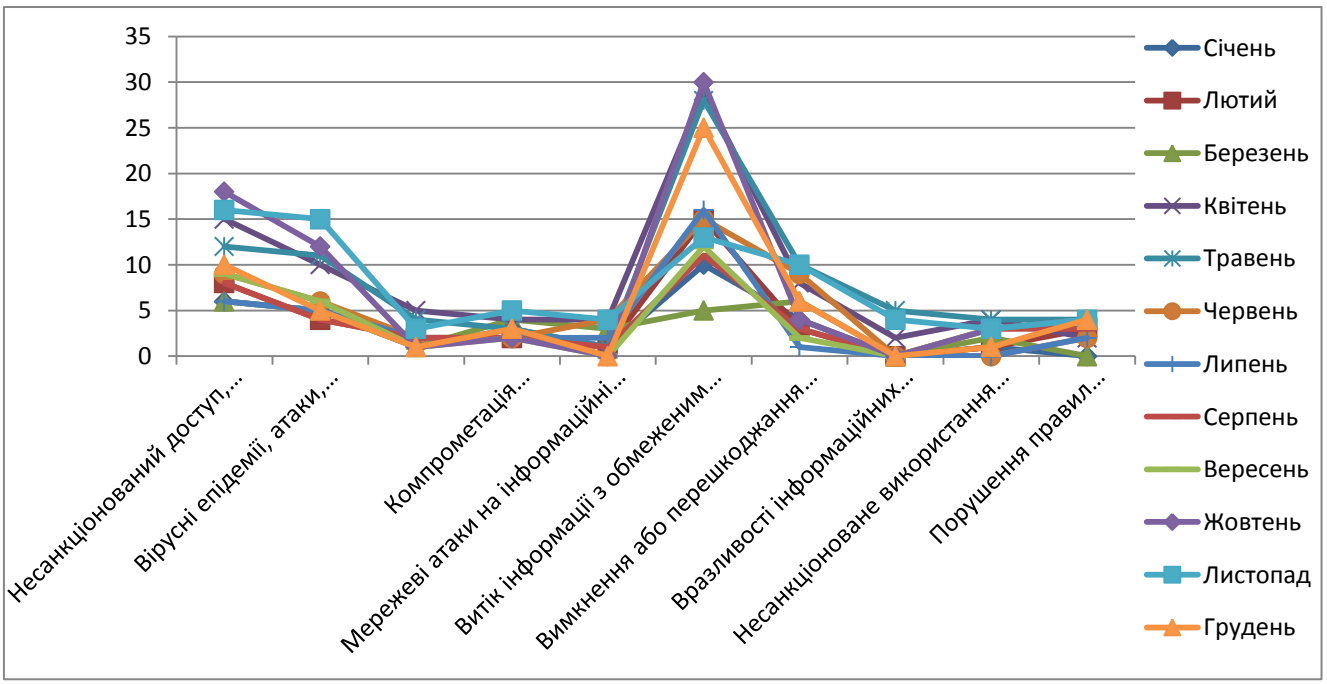

Рис. 2.1. Річна статистика інцидентів ІБ

Статистичні дані в розрізі одного року допомогають з'ясувати причини виникнення певних виді інцидентів в залежності від сезону року, подій які відбулися на підприємстві в цілому або суспільстві та державі. На Рис. 2.4 виділяється підвищення кількості інцидентів два рази на рік: весна (квітень, травень) та осінь (жовтень, листопад). Подальший аналіз адміністраторами управління інцидентами інформаційної безпеки вказаного явища виявив, що причиною такої активності є найм нових співробітників. Не кваліфіковані молоді співробітники та погано ознайомлені з політикою ІБ підприємства спричиняють підвищенню порушень. Результатом було створення додаткового дистанційного навчання співробітників нормативних документів ІБ підприємства з подальшим проходженням тестів.

Висновки до другого розділу

Розлянуто вплив інцидентів інформаційної безпеки на підприємство та можливість їх оцінки. Описані вимоги до документування даних про інциденти, створення звіту про інцидент та ведення журналу. Наведено приклад з практичного досвіду використання звітів про інциденти інформаційної безпеки

при створенні статистичних даних для визначення причин зміни кількості інцидентів.

Документування та аналіз впливу інцидента, його оцінка сприятиме коректній класифікації подій ІБ для визначення ресурсів підприємства, які можуть бути втраченими або знищеними, що даст змогу зменшити нанесеня збитків підприємству в майбутньому. Документування та зберігання даних щодо виявлених інцидентів, їх характеристик допоможе краще використовувати ресурси підприємства для захисту інформації та проводити цілеспрямовані заходи зі зниження кількості та масштабності інцидентів певного типу.

РОЗДІЛ 3.
РЕКОМЕНДАЦІЇ КЕРІВНИЦТВУ ПІДПРИЄМСТВА ЩОДО ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Рекомендації щодо проведення аналізу інцидентів та їх класифікації

Складання діагностичних матриць служить для візуалізації результатів аналізу подій, що відбуваються в інформаційній системі. Матриця формується з рядків потенційних ознак інциденту та стовпців – типів інцидентів. Дається оцінка події за шкалою пріоритетів "високий", "середній", "низький". Діагностична матриця покликана документувати хід логічних висновків експертів в процесі прийняття рішення і, поряд з іншими документами, служить свідченням розслідування інциденту.

При аналізі інцидентів ІБ працівникам підприємства рекомендовано виконати наступне:

- своєчасно ідентифікувати невдалі та успішні порушення безпеки і інциденти безпеки;
- допомогти у виявленні подій безпеки, таким чином запобігти інцидентам безпеки шляхом використання індикаторів.

Управління інцидентами інформаційної безпеки повинно включати наступні дії заради коректності обробки даних щодо інцидету та повного аналізу події ІБ.

Повідомлення про події інформаційної безпеки. Ці повідомлення повинні якомога швидше відправлятися за належними управлінськими каналами та містити якомога більше даних про подію ІБ.

Повідомлення про недоліки захисту. Необхідно зобов'язати всіх співробітників, підрядчиків і користувачів із сторонніх організацій, що використовують інформаційні системи та сервіси, відмічати і повідомляти про всі

спостережувані або передбачувані недоліки захисту систем або сервісів. Одним з результатів такого підходу є визначення причин винекнення інцидентів ІБ.

Відповідальність і процедури. Повинна бути встановлена відповідальність керівництва та визначені процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки, вразі необхідності при аналізі інцидентів додаткових матеріалів, визначення винуватих осіб або виявлення вході аналізу наявність інших порушень інформаційної безпеки підприємства, які можуть вплинути на бізнес-процеси.

Навчання на інцидентах інформаційної безпеки. Повинні бути реалізовані механізми, що дозволяють виміряти та відстежувати типи, об'єми і вартість інцидентів інформаційної безпеки, заради використання оцінки інцидентів використовуючи дані з попередніх інцидентів того ж типу.

Збір доказів. Аналіз подій, які в результаті інциденту інформаційної безпеки передбачається зробити щодо особи або підприємства, включають в себе, окрім інших, і правові, то необхідно зібрати, зберегти та надати докази, щоб виконати правила доказу, встановлені у відповідному правоохоронному органі (органах).

При аналізі інцидентів інформаційної безпеки виконується ряд дій в залежності від виду інциденту, однак існує загальний план аналізу, а саме:

- Визначення основних ознак інциденту
- Визначення основних джерел повідомлення про події
- Визначення мінімального обсягу інформації про події ІБ
- Визначення дій по локалізації або стримуванню інцидента
- Визначення дій по усуненню та відновленню

Визначення основних ознак інциденту допомогає визначити до якого виду інцидентів відноситься подія ІБ. Дотаких ознак відноситься масовість підії, періодичність, на які системи підприємства впливає подія, які дані були задіяні, місце винекнення інциденту.

Визначення основних джерел повідомлення про події сприяє визначенню місця винекнення інциденту і його маштабу. Джерелами повідомлення можуть

виступати підсистеми управління інцидентами (SIEM), підсистеми запобігання витоку інформації (DLP), співробітники підприємства, адміністраторів систем, клієнтів, бізнес партнерів або третіх осіб, під час службових розслідувань або перевірок.

Визначення мінімального обсягу інформації про події ІБ такого як дати винекнення інциденту, тип інформації що підлягає аналізу (сервер, ПК, мобільний пристрій або інше), яка інформація була скопрометована, відповідальні особи дозволить з'ясувати вплив інциденту, необхідний об'єм роботи при локалізації та стримуванню.

Визначення дій по локалізації або стримуванню інцидента таких як: блокування скопрометованих даних, доступу до мережі, облікових записів, вилучення ПК, носіїв інформації, надання журналів подій з зкомпрометованих систем або інших систем в яких можуть бути наявні докази, блокування можливого джерела загрози, побітове крпіювання ПК, серверів, інформування третіх осіб – це все допоможе своечасно зменшити маштаби та можливі збитки підприємству.

Визначення дій по усуненню та відновленню таких як: зміна скопрометованих даних, відновлення даних або інформаційних систем з резервної копії, здійснення повного або часткового розблокування доступів, зняття запобіжних заходів, інформування користувачів або надання їм конкретних інструкцій, після усунення наслідків інциденту та усунення причин інциденту відновлюється операційний процес заблокованих систем або осіб, інформування третіх сторін, якщо вони мають відношення до інциденту якщо наслідки інциденту можуть привести до збитків, сприяє швидкому поверненню працездатності підприємства або його окремих частин.

Аналіз подій ІБ є основною частиною реагування на інциденти інформаційної безпеки і від неї залежить чи завтра підприємство продовжить свою діяльність.

3.2. Рекомендації щодо Плану дій групи реагування підприємства на виявлені інциденти.

Реагування на інциденти- це мистецтво очищення і відновлення при виявленні порушення кібербезпеки. Також ці порушення, які називаються - інцидентами IT, інцидентами ІБ або комп'ютерними інцидентами, але, як би ви їх не називали, вам потрібен план і команда, призначена для управління інцидентом і мінімізації збитку і витрат на відновлення.

Деякі підприємства називають цю команду групою реагування на інциденти комп'ютерної безпеки (CSIRT) - існують і інші варіанти цієї абревіатури, такі як група реагування на інциденти безпеки (SIRT) або група реагування на комп'ютерні інциденти (CIRT), або група реагування на інцидети інформаційної безпеки (ГРІІБ). Місія цієї команди одна і та ж, незалежно від того, як ви її називаєте, - прийняти встановлений компанією план дій при реагування на інцидентиінформаційної безпеки [16].

План дій ГРІІБ підприємства на виявлені інциденти, має містити методичні вказівки та рекомендації щодо реагування на інциденти пов’язані з визначеним переліком типів інцидентів. План реагування має описувати загальні етапи та підходи при реагуванні на визначений інцидент. В залежності від обставин інциденту необхідно виконувати ті чи інші дії в межах кожного з пунктів, дотримуючись при цьому загальної послідовності.

Реагування на інциденти інформаційної безпеки, пов’язані з порушенням ІБ складається з наступних етапів:

- Виявлення події інформаційної безпеки.
- Визначення чи відноситься подія до інциденту сфери інформаційної безпеки.
- Попередній аналіз інциденту.
- Реєстрація інциденту.
- Визначення пріоритету та повідомлення щодо порушення.

- Локалізація та стримування. Збір даних.
- Усунення.
- Закриття інциденту.
- Визначення можливості вдосконалення процесів які призвели до інциденту.

Виявлення події інформаційної безпеки може мати невичерпний перелік, наприклад:

- Масова розсилка спам повідомлень з поштових скриньок підприємства;
- Виявлення вірусів в критичних або важливих інформаційних системах підприємства;
- Виявлено порушення вимог нормативних документів з питань інформаційної безпеки які призвели до порушення конфіденційності, цілісності, доступності;

Основними джерелами повідомлень про події виступають підсистеми управління інцидентами, підсистеми запобігання витоку інформації, від співробітників підприємства, клієнтів. Визначення чи відноситься подія до інциденту сфери інформаційної безпеки лягає на адміністратора управління інцидентами інформаційної безпеки, який за зовнішніми ознаками аналізує отриману інформацію про подію інформаційної безпеки та визначає чи є дана подія інцидентом.

Попередній аналіз інциденту. Після прийняття рішення адміністратор управління інцидентами збирає мінімальний обсяг інформації, який буде використовуватись при подальшому розслідуванні:

- Дата та місце виникнення інциденту
- Що саме було порушено з питань ІБ.
- Пов’язані події.
- Яким чином відбулося порушення ІБ
- Затронуті системи та ресурси підприємства.
- Ким та за яких обставин було порушено вимоги ІБ

Реєстрація інциденту. Після прийняття рішення щодо належності події ІБ до інциденту адміністратор управління інцидентами робить запис у відповідному журналі, при цьому заповнюються поля звіту: місце виникнення; дата виявлення; дата та час початку; відповідальні за обробку; запланована дата звітності; ким виявлено(роль); ким виявлено (ПІБ), вид інциденту; клас критичності; затронуті ресурси; затронуті системи; порушено К/Ц/Д, Опис інцидент.. В залежності від обставин інциденту до його розслідування можуть бути залучені представник служби охорони, адміністратор ЗІ, адміністратори інформаційних ресурсів, керівник підрозділу, в якому стався інцидент та інші.

Визначення пріоритету та повідомлення щодо порушення. За результатами отриманих даних приймається рішення стосовно критичності інциденту, заповнюються поле звіту «клас критичності» та повідомляються особи які причетні до реагування на даний інцидент. В залежності від критичності та обставин інциденту до його розслідування можуть бути залучені представник різних підрозділів. У випадку встановлення критичних порушень функціонування систем, правил ІБ і т.д. Головою групи реагування може ініціюватись службове розслідування, яке має проводитись згідно вимог підприємства.

Мінімальний перелік питань, які необхідно встановити в ході розслідування:

- Хронологія виникнення та розвитку інциденту
- Збитки
- Дату та час усунення інциденту
- Що було порушено
- Винних осіб та ступінь їх вини
- Причини
- Пропозиції щодо впливу на порушника та запобігання подібних інцидентів в майбутньому

Локалізація та стримування. Збір даних. У випадку порушення цілісності системи, автентифікаційних даних адміністратори зтронутих ресурсів повинні вжити заходи щодо локалізації та усунення інциденту таких як:

- Блокування облікового запису користувача, від імені якого здійснювалося порушення правил ІБ.
- Блокування доступу користувача до відправки електронної пошти;
- Блокування доступу до мережі інтернет;
- Вилучення ПК, носіїв інформації;
- Обмеження мережевої взаємодії окремих елементів чи сегментів мережі;
- Інформування третіх сторін, якщо вони мають відношення до інциденту, або зазначений інцидент може завдати їм збитків.

При здійсненні заходів, направлених на локалізацію та стримування інциденту варто звернути увагу на збереження журналів, протоколів, архівних копій та інших матеріалів, що можуть знадобитися для подальшого розслідування інциденту.

Усунення. Після усунення наслідків інциденту та усунення причин інциденту відновлюється операційний процес заблокованих систем або осіб. Інформування третіх сторін, якщо вони мають відношення до інциденту якщо наслідки інциденту можуть привести до збитків.

Закриття інциденту. На підставі отриманих в ході обробки інциденту інформаційної безпеки матеріалів Адміністратор управління інцидентами вносить всі необхідні дані в журнал реєстрації інцидентів. Заповнює поля звіту: причини виникнення (тип); причини виникнення (вид); що порушено; винуватець (роль); винуватець ПІБ; втрати/завдані збитки; дата закриття; тривалість інциденту, заходи по запобіганню .За необхідністю доповнюються всі інші поля звіту)

Визначення можливості вдосконалення процесів які призвели до інциденту. Після закриття інциденту проводиться аналіз інциденту: його причин, наслідків та можливих змін щодо недопущення подібного типу інцидентів або мінімізації їх кількості, або негативного впливу. До аналізу та його результатів

можуть долучатися окрім групи реагування на інциденти та адміністраторів управління інцидентами інші пов’язані або зацікавлені особи.

На підставі отриманих в ході обробки інциденту інформаційної безпеки матеріалів:

- керівництво підприємства приймає рішення щодо необхідності вжиття дисциплінарних заходів до порушників інформаційної безпеки;
- керівник групи реагування на інциденти приймає рішення щодо розробки та вжиття заходів направлених на недопущення подібного типу інцидентів або мінімізації їх кількості або негативного впливу (в тому числі внесення змін до нормативних документів, конфігурацій систем, порядку дій)
- керівник групи реагування на інциденти приймає рішення щодо внесення відповідних змін чи доповнень в процедуру реагування
- керівник групи реагування на інциденти приймає рішення щодо необхідності інформування інших підрозділів про інцидент та його причини.

Архітектура типової СУІБ має включати такі основні компоненти [17, 18, 19]: інтеграційну платформу; апаратно-програмні засоби моніторингу і аудиту; апаратно-програмні засоби захисту інформації; сховище інформації про інциденти ІБ; аналітичні інструменти і засоби генерації звітів; засоби управління та користувацькі інтерфейси. Інтеграційна платформа є ядром системи, вона покликана забезпечувати чітку і оперативну координацію та взаємодію осіб, що відповідають за реакцію на події, пов'язані з інцидентами ІБ. Апаратно-програмні засоби моніторингу і аудиту – засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування ІКС організації. Вони складають підсистему збору інформації про інциденти ІБ. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту. Апаратно-програмні засоби захисту в контексті СУІБ – засоби, які забезпечують локалізацію інцидентів або зниження збитку. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від

інцидентів ІБ. Також, в організації повинна бути розроблена та впроваджена система сповіщення про інциденти. Узагальненою метою забезпечення ІБ організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів ІБ. Основною задачею процесу УІІБ є усунення інцидентів в гранично стислі терміни. У ході процесу управління інцидентами ІБ проводиться виявлення, реєстрація, класифікація і початкова підтримка запитів, а також пошук рішення, його застосування, контроль, інформування і підготовка звітності. Оскільки, як ми вже визначили, інцидентом, в першу чергу, є певна недозволена подія, то вона має бути кимось заборонена. Отже, існує необхідність розробки та затвердження документів, що чітко описують всі дії, які можна виконувати в ІКС і які виконувати заборонено. Однією з кращих СУІІБ серед присутніх на вітчизняному ринку є програмний продукт для обробки подій – netForensics nFX Open Security Platform [17], зображений на рис. 3.1.

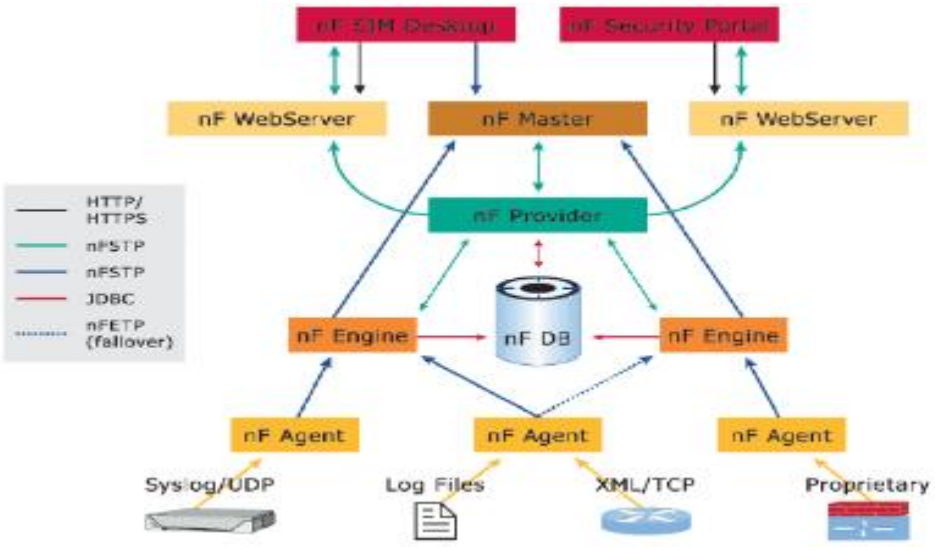

Рис. 3.1. СУІІБ netForensics

Висновки до третього розділу

Коректний та якісний аналіз і класифікація подій в результаті дозволить створити План дій групи реагування підприємства на виявлені інциденти, який максимально зменшить час реагування на інциденти ІБ, що в свою чергу

підвищить рівень інформаційної безпеки. Запропоновано рекомендації щодо аналізу інцидентів та їх класифікації. Сформульовані рекомендації по покращенню Плану дій групи реагування підприємства на виявлені інциденти.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальну науково-прикладну задачу, сутність якої полягає в обґрунтовані теоретико-методичних засад щодо організації захисту інформації підприємства на основі аналізу інцидентів.

Розв’язавши поставлені дослідницькі завдання, в результаті наукового пошуку вдалося дійти таких висновків:

Аналіз інцидентів ІБ дозволяє визначити інцидент, своєчасно зреагувати на подію та підібрати ефективні дії і засоби для стримування, локалізації інциденту та його наслідків. Класифікація типів та видів інцидентів на підприємстві дає змогу з’ясувати масштаби інциденту та ризики. Коректні підсистеми захисту (SIEM, DLP), дозволяють своєчасно виявити інцидент, зменшити його вплив на підприємство або навіть попередити його. Способи та методи реагування на інциденти зменшать час, який потрібен ГРІІБ на прийняття рішень.

Розглянуто вплив інцидентів інформаційної безпеки на підприємство та можливість їх оцінки. Описані вимоги до документування даних про інциденти, створення звіту про інцидент та ведення журналу. Наведено приклад з практичного досвіду використання звітів про інциденти інформаційної безпеки при створенні статистичних даних для визначення причин зміни кількості інцидентів.

Документування та аналіз впливу інцидента, його оцінка сприятиме коректній класифікації подій ІБ для визначення ресурсів підприємства, які можуть бути втраченими або знищеними, що надасть змогу зменшити нанесення збитків підприємству у майбутньому. Документування та зберігання даних щодо виявлених інцидентів, їх характеристик допоможе краще використовувати ресурси підприємства для захисту інформації та проводити цілеспрямовані заходи зі зниження кількості та масштабності інцидентів певного типу.

Результатом роботи є розробка рекомендацій щодо підвищення рівня інформаційної безпеки підприємства.

У процесі виконання роботи отримані наступні результати:

1. Проведений аналітичний огляд класифікацій і характеристик інцидентів інформаційної безпеки
2. Досліджені основні джерела виявлення інцидентів.
3. Розлянуті характеристики впливу інцидентів на підприємство.
4. Визначені вимоги щодо створення статистики подій інформаційної безпеки.
5. Запропоновані рекомендації щодо підвищення рівня інформаційної безпеки підприємства.

Отже, підготовка, виявлення і проведення дій відносно подій інформаційної безпеки, оформлення їх результатів пов’язані з виконанням низки обов’язкових процедур, необхідних для забезпечення безперервності бізнес-процесів. При недотриманні запропонованих рекомендацій виникає серйозна небезпека підвищення кількості інцидентів інформаційної безпеки. Контроль за виконанням цих вимог покладається на керівництво підприємства та відповідальних за інформаційну безпеку підрозділів.

Запропоновані рекомендації дозволять підвищити рівень інформаційної безпеки на підприємстві, при цьому можуть використовуватися керівниками та службою інформаційної безпеки підприємства під час створення ГРІБ та нормативних-документів таких як План дій групи реагування підприємства на виявлені інциденти.

Коректний та якісний аналіз і класифікація подій в результаті дозволить створити План дій групи реагування підприємства на виявлені інциденти, який максимально зменшить час реагування на інциденти ІБ, що в свою чергу підвищить рівень інформаційної безпеки. Запропоновано рекомендації щодо аналізу інцидентів та їх класифікації. Сформульовані рекомендації по покращенню Плану дій групи реагування підприємства на виявлені інциденти.

СПИСОК ПОСИЛАНЬ

1. Company COMODO. What is Cybersecurity? URL: https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php
2. Donald L. Pipkin Information Security: Protecting the Global Enterprise 1st Edition / Donald L. Pipkin. Publisher: Prentice Hall; 400p.
3. Information technology — Security techniques — Information security management systems — Overview and vocabulary: ISO/IEC 27000:2018(en). URL: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27000:ed-5:v1:en
4. Security information and event management (SIEM). URL: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM
5. Jeff Goldman. IBM QRadar vs Splunk: Top SIEM Solutions Compared URL: https://www.esecurityplanet.com/network-security/ibm-qradar-splunk-siem-solutions-compared.html
6. What is Data Loss Prevention (DLP)? Definition, Types & Tips. URL: https://www.digitalguardian.com/blog/what-data-loss-prevention-dlp-definition-data-loss-prevention
7. SandBlast Zero-Day Protection. URL: https://www.checkpointsecurity.co.za/sandblast/
8. Incident Response. Process. Frameworks and tools. URL: https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools
9. Олег Иванов. Что такое SIEM-системы и для чего они нужны? URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases
10. What is a Data Loss Prevention (DLP URL: https://www.infoblox.com/glossary/what-is-a-data-loss-prevention-dlp/
11. Introducing Check Point SandBlast Zero-Day Protection. URL: https://blog.checkpoint.com/2015/09/02/introducing-check-point-sandblast-zero-day-protection/

12. Andrew Davidson. What are the top five causes of information security breaches? URL: https://johnstoncarmichael.com/insights/what-are-the-top-five-causes-of-information-security-breaches
13. Cyber security for business. URL: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business
14. Олександр Архипов, Андрій Скиба. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Zi_2013_15_4_15.pdf
15. How to Document Security Incidents for Compliance in 10 Steps URL: https://resources.infosecinstitute.com/how-to-document-security-incidents-for-compliance-in-10-steps/#gref
16. Jeff Petters. What is Incident Response? A 6-Step Plan URL: https://www.varonis.com/blog/incident-response-plan/
17. Звіт "Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ" (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.И3-06. Київ: НАН України 2019. 149 с.
18. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки: Навчальний посібник. Одеса : ОНАЗ ім. О.С. Попова, 2009. 208 с.
19. Пількевич І.А., Котков В.І., Лобанчикова Н.М., Сугоняк І.І. Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій. *Восточноевропейский журнал передовых технологий.* 2012. № 2 (56). С. 18–21.