МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Систем інформаційного та кібернетичного захисту

До захисту
Завідувачкафедри СІКЗ
к.т.н., доцен
Шуклін Г.В.
“____”_____2022р.

ДИПЛОМНА РОБОТА
Зі спеціальності: 125 Кібербезпека
на тему:

УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ ТА МАЛИХ КОМЕРЦІЙНИХ ПІДПРИЄМСТВ

Студент групи СЗД-41 Саричев Валерій Олегович _____
(підпис)

Керівник к.т.н., доцент Шуклін Герман Вікторович _____
(підпис)

Нормконтроль ст. викл. Гребенніков Асаді Болдгоягович _____
(підпис)

Київ – 2022

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра Систем інформаційного та кібернетичного захисту

Освітньо-кваліфікаційний рівень – магістр
Спеціальність – 125 Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н., доцент
_____Шуклін Г.В.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ
Студенту: САРИЧЕВУ ВАЛЕРІЮ ОЛЕГОВИЧУ

1.Тема роботи: "Управління інцидентами кібербезпеки та малих комерційних підприємств" затверджена наказом вищого навчального закладу від «16» лютого 2022 р. № 22.

2.Термін подання студентом закінченої дипломної роботи

3.Вихідні дані до роботи: Проаналізувати процес управління інцидентами, а також, дізнатися про групи реагування на інциденти. Виявити потенційні інциденти безпеки шляхом моніторингу та звітування про них. Оцінити виявлені інциденти для визначення відповідних наступних кроків для зменшення ризику. Відреагувати на інцидент, обмеживши його, дослідивши та розв'язавши його, а також, дізнатися та задокументувати основні висновки кожного інциденту.

4.**Зміст пояснювальної записки(перелік питань, які потрібно розробити):**

1. Підготування до інциденту кібербезпеки на підприємстві.
2. Виявлення та ідентифікація потенційні інциденти кібербезпеки.
3. Спілкування під час інциденту кібербезпеки.

5.**Дата видачі завдання**" " _____2022р.

КАЛЕНДАРНИЙ ПЛАН

№	Процедура	Термін виконання	
1	Підготовка Розділу 1	-	До 04.04
2	Підготовка Розділу 2	З 04.04	До 25.04
3	Підготовка Розділу 3	З 25.04	До 06.05
4	Висновки + Презентація	З 06.05	До 13.05
5	Перевірка роботи на плагіат + Предзахист	З 16.05	До 01.06
6	Захист роботи	З 02.06	До 21.06
7	Випуск	30.06	

Студент Саричев В.О.

Керівник роботи Шуклін Г.В.

Реферат

Дипломна робота присвячена дослідженню методу управління інцидентами кібербезпеки на малих підприємствах. Робота складається зі вступу, трьох розділів, що містять 4 мадюнки, 11 таблиць, висновки та списки використаних джерел, що містять 16 найменувань. Загальний обсяг роботи становить 85 сторінок.

Об'єктом дослідження є метод управління інцидентами малих та комерційних підприємств.

Метою роботи полягає в тому, щоб захищати малі та комерційні підприємства від кіберзагроз, фішинг, зловмисне програмне забезпечення. Дослідити організаційні вимоги до організації управління інцидентами кібербезпеки на малих та комерційних піприємств. Задля цього в роботі використовується більше всього до організації управління інцидентами кібербезпеки на малих та комерційних підприємств.

В результаті роботи розглянули на досвіді країн у використанні підходу для того щоб створити результативної системи управління кібербезпеки.

КЛЮЧОВІ СЛОВА: Управління кібербезпеки, інцидент кібербезпеки, управління інцидентами кібербезпеки на малих та комерційних підприємств.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT – це скорочення від Advanced Persistent Threat. Це набір прихованих і безперервних процесів комп'ютерного злому. У випадку APT зловмисник використовує кілька етапів для проникнення в мережу, щоб уникнути виявлення та отримати цінну інформацію протягом тривалого періоду.

Артефакт – є об'єктом цифрового археологічного інтересу.

Актив – Будь-який ресурс або можливості. Активи Постачальника послуг включають все, що може сприяти наданні Послуг. Активи можуть бути одного з таких типів: управління, організація, процес, знання, люди, інформація, програми, інфраструктура та фінансовий капітал.

Резервне копіювання – Процедури резервного копіювання використовуються для копіювання файлів на другий носій, такий як диск, стрічка або хмара. Файли резервної копії слід зберігати поза межами сайту. Резервне копіювання зазвичай автоматизується за допомогою команд операційної системи або допоміжних програм резервного копіювання. Більшість програм резервного копіювання стискають дані так, що для резервних копій потрібно менше носіїв.

Ботнет – Набір комп'ютерів (часто десятки тисяч), якими керує одна або кілька осіб (так звані бот-майстри) за допомогою зловмисного програмного забезпечення. Ботнети можна використовувати для розсилки спаму, для початку DDoS-атаки, для поширення шкідливих програм тощо.

DDoS — це скорочення від Distributed Denial of Service. У разі DDoS бот-майстер дає команду комп'ютерам ботнету отримати доступ до визначеного веб-сайту. Сервер цього веб-сайту буде перевантажений і перестане функціонувати належним чином.

DMZ — це скорочення від демілітаризованої зони і відноситься до фізичної або логічної підмережі (зони), яка відокремлює внутрішню локальну мережу від інших ненадійних мереж, таких як Інтернет. Мета DMZ — додати додатковий рівень безпеки. Назва походить від військового терміну «демілітаризована зона», що є територією між національними державами, де військові операції заборонені.

IDS — це скорочення від Intrusion Detection System, що є автоматизованою системою, метою якої є виявлення злому або несанкціонованого доступу до комп’ютерної системи чи мережі.

IPS – скорочення від адреси Інтернет-протоколу. Це цифрова мітка, присвоєна кожному пристрою, що бере участь у комп’ютерній мережі. IP-адреси використовуються як для ідентифікації, так і для визначення місцезнаходження пристрою.

Мережа – Телекомунікаційна мережа, яка дозволяє комп’ютерам або іншим пристроям обмінюватися даними. Найвідомішою комп’ютерною мережею є Інтернет.

Патч — це невелика частина програмного забезпечення, яку часто розробляють виробники певного програмного забезпечення для оновлення, виправлення (помилків чи вразливостей) або покращення цього програмного забезпечення. Це дозволяє змінювати програмне забезпечення, не перевстановлюючи його з нуля.

PGP — це скорочення від Pretty Good Privacy, що є комп’ютерною програмою для шифрування та дешифрування даних, яка забезпечує криптографічну конфіденційність та аутентифікацію для передачі даних.

RAM – скорочення від оперативної пам’яті. Оперативна пам'ять є найпоширенішим типом сховища даних в комп'ютерах та інших пристроях, таких як принтери.

Руткіт — Колекція комп’ютерного програмного забезпечення, часто шкідливого, розробленого з подвійною метою: (1) забезпечити доступ до комп’ютера або областей його програмного забезпечення, які інакше не були б дозволені, і в той же час (2) маскування його існування або наявність іншого програмного забезпечення.

Snort — це безкоштовна система запобігання вторгненню в мережу з відкритим кодом і система виявлення вторгнень в мережу.

VPN – це скорочення від віртуальної приватної мережі. Це група комп’ютерів, об’єднаних разом через загальнодоступну мережу, наприклад Інтернет.

ВСТУП

Актуальність теми: Управління інцидентами кібербезпеки не є лінійним процесом; Це цикл, який складається з підготовки, виявлення, стримування інцидентів, пом’якшення наслідків та відновлення. Останній етап складається з витягу уроків з інциденту, щоб покращити процес і підготуватися до майбутніх інцидентів. Під час цього циклу комунікація як з внутрішніми, так і з зовнішніми зацікавленими сторонами має вирішальне значення.

Мета та завдання дослідження: Мета полягає у тому щоб захистити підприємства від кібератак, фішинг , зловмисне програмне забезпечення , програмне забезпечення -вимагач або розширену постійну загрозу, а також вдосконалити процес управління інцидентами на підприємствах.

Щоб досягнути такої мети потрібно зробити такі завдання:

- Наявність плану реагування на інциденти може значно попередити кіберінциденти та обмежити шкоду, якщо вони все-таки трапляються.
- Зробити методику для забезпечення захисту, управлінням інциденту кібербезпеки на підприємстві

Об’єктом дослідження є управління інцидентами кібербезпеки. Предмет дослідження – організація управління інцидентами кібербезпеки на підприємстві.

Методи дослідження. Для вирішення завдання в цій роботі використовувалася структура системного аналізу та терорії кібербезпеки, а також використовувалось теорія управління інцидентами кібербезпеки.

Розділ 1 ПІДГОТУВАННЯ ДО ІНЦИДЕНТУ КІБЕРБЕЗПЕКИ НА ПІДПРИЄМСТВІ

В даному розділі буде проаналізовано підготування до інциденту кібербезпеки на підприємстві. Для цього необхідно розкрити основні характеристики забезпечення кібербезпеки, роль управління інцидентами кібербезпеки, а також проаналізувати основні вимоги стандартів цієї сфери.

1.1 План реагування на інциденти кібербезпеки

Зіткнувшись із інцидентом кібербезпеки, організація повинна бути в змозі швидко і належним чином реагувати. Ось чому важливо вирішити, як ви будете поводитися з певними ситуаціями заздалегідь, а не коли ви зіткнетеся з ними вперше під час інциденту. Складіть план (на папері, а не тільки в голові), щоб обмежити шкоду, скоротити витрати та час відновлення та спілкуватися як із внутрішніми, так і зовнішніми зацікавленими сторонами.

Що таке план реагування на інциденти кібербезпеки ?

План реагування на інциденти з кібербезпеки – це документ, який дає спеціалістам з IT та кібербезпеки інструкції щодо того, як реагувати на серйозні інциденти безпеки, такі як злом даних, витік даних, атака програмного забезпечення-вимагача або втрата конфіденційної інформації. За даними Національного інституту стандартів і технологій (NIST), найбільш ефективні плани реагування на інциденти мають чотири етапи: підготовка; виявлення та аналіз; стримування, ліквідація та відновлення; та діяльність після інциденту.

Огляд плану реагування на інциденти з кібербезпеки

План реагування на кіберінциденти не є статичним документом. Важливо інтегрувати його у свої бізнес-процеси, а також регулярно переглядати та оновлювати, щороку та як частину перевірки після інциденту.

Процедури реагування на інциденти з кібербезпеки

Спираючись на свій план реагування на інциденти кібербезпеки, ви можете визначити ряд стандартних операційних процедур для поширених інцидентів, які можуть статися у вашій організації. Така процедура повинна крок за

кроком пояснювати, як можна вирішити конкретну проблему. Ці посібники швидкого реагування на ймовірні сценарії мають бути легко доступними.

Чому кожній компанії потрібен план реагування на інциденти з кібербезпеки?

Минулого року атаки програм-вимагачів привернули увагу, оскільки постраждали організації всіх галузей. Незалежно від того, чи є ви невеликою компанією чи такою великою, як Colonial Pipeline чи T-Mobile , справа не в тому, «чи» ви стикаєтесь із інцидентом із кібербезпекою, а «коли». І ніхто, хто зберігає чи обробляє конфіденційні дані, не є занадто малими чи надто безпечними, щоб потрапити в нього.

Відсутність детального CSIRP зашкодить вам кількома способами, коли ви зазнаєте зламу: по-перше, ваша команда безпеки та команда керівництва намагатимуться зрозуміти та відповісти. Без розробленого плану вони будуть схильні робити дорогі помилки.

Залежно від типу розкритої інформації та розміру порушення, ви можете бути зобов’язані вжити певних заходів і повідомити не лише постраждалих, а й державні установи чи інші організації. Відсутність CSIRP створить багато можливостей для вас, щоб пропустити кроки та піддати себе додатковим штрафам або судовим позовам.

По-друге, якщо ваш бізнес зазнає значних порушень, вам доведеться пройти зовнішнє розслідування або аудит. Відсутність записаних доказів CSIRP буде сигналом для аудиторів, що ви не сприймаєте всерйоз ймовірність порушення даних.

Більше того, деякі правила щодо конфіденційності даних, як-от Каліфорнійський закон про захист прав споживачів (CCPA), вимагають плану реагування на інциденти . Отже, якщо у вас немає CSIRP, ви порушите CCPA .

Деякі галузеві системи безпеки також вимагають від організацій наявність CSIRP. Наприклад, якби ви проходили сертифікацію за стандартом ISO 27001 і не мали CSIRP, ви б не пройшли аудит. Додаток A стандарту ISO 27001 містить конкретні вимоги до плану реагування на інциденти інформаційної безпеки. Отже, якщо ви не можете надати своєму аудитору

причину, чому вашому бізнесу не потрібен CISPR, ви повинні мати його, щоб отримати сертифікат ISO 27001.

Зрештою, незалежно від розміру вашого бізнесу, у якій б галузі ви не працювали та де б ви не знаходилися з точки зору зростання, вам потрібно мати план реагування на кіберінциденти, щоб забезпечити безпеку вашого бізнесу та допомогти вашому бізнесу ефективно відновитися після інциденту з безпекою.

Дослідження вартості кіберзлочинності Інституту Понемон показало, що типова організація зазнає в середньому 130 інцидентів на рік і витрачає 11,7 мільйонів доларів на рік на захист. Ефективний процес реагування може значно зменшити ці витрати.

Плани реагування на інциденти також важливі для захисту ваших даних. Захист активів даних у процесі реагування на інциденти включає безпечне резервне копіювання, використання журналів і попереджень безпеки для виявлення зловмисної діяльності, належне керування ідентифікацією та доступом, щоб уникнути внутрішніх загроз, а також велику увагу до керування виправленнями.

Нарешті, планування реагування на інциденти захищає репутацію вашої компанії. IDC виявила , що 80% споживачів перенесли б свій бізнес в інше місце, якщо б безпосередньо постраждали від порушення даних. Якщо порушення безпеки не буде усунено швидко та належним чином, компанія ризикує втратити бізнес. Довіра інвесторів та акціонерів може різко знизитися після оприлюдненого порушення даних.

План реагування на інциденти (IRP) допомагає підготуватися до інцидентів безпеки та, в ідеалі, запобігти їх. Відповіді, які диктують IRP, також можуть мати деякі менш очевидні позитивні наслідки для вашої організації, зокрема:

- Захист даних — Захист даних і системи є основою IRP. Захист досягається шляхом захисту резервних копій, забезпечення достатньої ідентифікації та керування доступом, а також своєчасного усунення вразливостей. Ці заходи підкріплюються швидким реагуванням на сповіщення та ретельним аналізом журналів і даних про події.
- Зміцнює репутацію — Ефективне реагування на інциденти показує відданість бренду безпеці та конфіденційності. Атаки, що призводять до втрати даних, можуть викликати у клієнтів сумніви в компетентності організації, що призведе до відмови від бренду. Так само акціонери та

інвестори можуть відмовитися від бізнесу, який зазнав порушення. IRP може запобігти або мінімізувати ці втрати.

- Зменшує витрати — порушення коштують дорого через нормативні штрафи, компенсацію клієнтам або просто витрати на розслідування та відновлення систем. Згідно з дослідженням IBM у 2019 році , середня вартість порушення становить майже 4 мільйони доларів. IRP можуть допомогти знизити ризик порушення та обмежити шкоду, завдану атаками, мінімізуючи ваші витрати.

Як зробити план реагування на інцидент успішним?

Які ключові міркування для реагування на інцидент?

План реагування на інцидент повинен включати такі елементи, щоб бути ефективним:

- Підтримка вищого керівництва — підтримка керівництва дозволить вам залучити найбільш кваліфікованих членів для вашої групи реагування та створити процеси та потоки інформації, які допоможуть вам ефективно керувати інцидентом.
- Послідовне тестування — план реагування на інцидент не коштує багато, якщо він тільки на папері: його потрібно перевірити. Проведення запланованого (а ще краще, незапланованого) навчання безпеки, виконання плану та визначення слабких місць значно підтвердить, що команда готова до реального інциденту.
- Баланс між деталізації та гнучкості — план повинен містити конкретні кроки, які можна діяти, щоб команда могла швидко виконати, коли трапиться інцидент. У той же час створення жорстких процесів призводить до ускладнень і нездатності впоратися з несподіваними сценаріями. Створіть детальний план, але забезпечте гнучкість для підтримки широкого кола інцидентів. Часте оновлення плану також може допомогти з гнучкістю — перегляд плану кожні шість місяців може допомогти вам врахувати нові типи проблем безпеки та атак, які впливають на вашу галузь.
- З’ясуйте канали зв’язку — у плані має бути чітко вказано, з ким повинна спілкуватися група інциденту, через які канали зв’язку та яку інформацію слід передати. Це важлива частина процесу реагування, яку іноді не помічають. Наприклад, повинні існувати чіткі вказівки щодо того, який рівень деталізації слід повідомити керівництву IT, вищому керівництву, постраждалим відділам, постраждалим клієнтам і пресі.
- Знайомтеся зі своїми зацікавленими сторонами — хто є ключовими ролями в організації, які повинні піклуватися про інцидент безпеки та

бути залученим до нього? Вони можуть змінюватися залежно від типу інциденту та цільових організаційних ресурсів. Зацікавлені сторони можуть включати керівників відділів, вище керівництво, партнерів, клієнтів та юридичних осіб.

- Зберігайте план простим — до планів реагування слід також застосовувати добре відомий принцип управління «Нехай буде просто, дурно» (KISS). Складний план, навіть якщо він дуже добре продуманий, навряд чи буде точно виконуватися в реальному часі. Зведіть деталі, кроки та процедури до абсолютного мінімуму, щоб команда могла обробити та застосувати їх до інциденту, коли вони потрапляють у «туман війни» .

Які ключові ролі в плані реагування на інцидент?

План реагування на інциденти не є повним без команди, яка може його виконати — Групи реагування на інциденти з комп'ютерної безпеки (CSIRT). Група реагування на інциденти — це група людей — або IT-спеціалісти, які мають певну підготовку з питань безпеки, або штатний персонал із безпеки у великих організаціях, — які збирають, аналізують та діють на основі інформації про інцидент.

Вони є центром інциденту і відповідають за спілкування з іншими зацікавленими сторонами в організації та зовнішніми сторонами, такими як юрисконсульт, преса, правоохоронні органи, постраждалі клієнти тощо.

Який зв'язок між планом реагування на інцидент і планом аварійного відновлення?

План реагування на інцидент повинен доповнюватися планом аварійного відновлення. Останній визначає, як організація керує катастрофічними подіями, такими як стихійне лихо або випадкова втрата даних. У той час як план реагування на інциденти зосереджується на ідентифікації події безпеки та доведенні її до закриття, аварійне відновлення має на меті повернути системи в режимі онлайн відповідно до цілі часу відновлення (RTO).

Нові ризики кібербезпеки, викликані COVID-19

Тепер, коли новий коронавірус змусив більшість організацій перейти на модель роботи лише віддалено, важливо, щоб ваш персонал із IT-безпеки був напоготові та розумів нові ризики, з якими стикається ваша організація. Шкідливі кіберзлочинці можуть скористатися стурбованістю громадськості навколо нового коронавірусу, проводячи фішингові атаки та кампанії дезінформації.

Фішингові атаки часто використовують комбінацію електронної пошти та фіктивних веб-сайтів, щоб обманом змусити жертв розкрити конфіденційну інформацію. Дезінформаційні кампанії можуть поширювати розбрат, маніпулювати публічною розмовою, впливати на розробку політики або руйнувати ринки

Поради щодо кібербезпеки щодо COVID-19

Протягом цього часу ваша команда з IT-безпеки повинна нагадати співробітникам про вжиття запобіжних заходів, повторити ключові поняття, висвітлені під час навчання з безпеки, переконатися, що всі системи моніторингу працюють правильно, і бути готовими до оперативного реагування на будь-які інциденти безпеки.

Агентство з кібербезпеки та безпеки інфраструктури (CISA), ключовий радник країни з питань ризиків, опублікувало нещодавні рекомендації щодо управління ризиками для COVID-19 . CISA рекомендував організаціям перевірити безпеку систем інформаційних технологій, виконавши такі кроки:

- Захищені системи, які забезпечують віддалений доступ.
    - Переконайтеся , що віртуальна приватна мережа та інші системи віддаленого доступу повністю виправлені.
    - Покращте моніторинг системи, щоб отримувати раннє виявлення та сповіщення про ненормальну активність
    - Впровадити багатофакторну аутентифікацію
    - Переконайтеся, що всі машини мають належним чином налаштовані брандмауери, а також встановлене програмне забезпечення для захисту від шкідливих програм і вторгнень.
- Перевірте потужність рішень віддаленого доступу або збільште потужність
- Переконайтеся , що плани безперервності діяльності або плани безперервності бізнесу оновлені
- Підвищити обізнаність про механізми підтримки інформаційних технологій, які працюють віддалено
- Оновіть плани реагування на інциденти, щоб врахувати зміни персоналу в розподіленому середовищі.

Як пишеться план реагування на інциденти кібербезпеки?

Національний інститут стандартів і технологій (NIST) передбачає чотири етапи плану реагування на інцидент: підготовка; виявлення та аналіз; стримування, ліквідація та відновлення; та діяльність після інциденту. Важливо визнати, що підготовчі заходи та заходи після інциденту однаково важливі. Фактично, NIST підкреслює обидва види діяльності в їх плані.

Ключ до ефективного плану реагування на інциденти кібербезпеки (CSIRP) полягає в тому, щоб його було створено задовго до того, як станеться порушення. Планування, яке ви робите до того, як станеться інцидент із безпекою, допоможе вам реагувати на інцидент якомога швидше та ефективно.

1. Підготовка

По-перше, у вашому плані має бути детально описано, хто входить до групи реагування на інцидент, а також їхню контактну інформацію та їхню роль, а також коли необхідно зв'язатися з членами команди. Кожен член цієї команди, від генерального директора до членів IT-команди, повинен розуміти своє місце в команді та що їм потрібно робити в разі порушення. Їм також потрібно запам'ятати деталі вашого CSIRP, щоб у разі виникнення інциденту безпеки вони могли швидко реагувати.

Офіційний посібник NIST з обробки інцидентів з комп'ютерної безпеки дає вам вичерпне уявлення про всі речі, які вам потрібно визначити, перш ніж інцидент станеться. Ви можете бути здивовані, наскільки детальним є список, але коли відбувається інцидент з безпекою, ваша команда повинна мати можливість працювати якомога швидше, і необхідність приймати багато рішень щодо того, як впоратися з порушенням, сповільнить їх. вниз. Вам також потрібно переконатися, що ви працюєте продуктивно, і запобігти вибору, який допоможе хакерам продовжувати експлуатувати та проникати у ваші системи. Попереднє визначення всієї цієї інформації, поряд з регулярним тестуванням вашого CSIRP і проведенням тренувань з вашою командою, дасть вам найкращі шанси швидко та без додаткових проблем припинити атаку.

Попередження інцидентів є другою частиною підготовчого етапу. Сподіваємося, це не новина для вас, оскільки ви вже розробили політику інформаційної безпеки для захисту конфіденційної інформації, яка довіряється вашому бізнесу. Однак NIST все ще надає деякі рекомендації щодо уникнення інцидентів , як-от регулярна оцінка ризиків , безпека хоста, запобігання шкідливому програмному забезпеченню тощо.

Вся інформація у вашому CSIRP повинна зберігатися в одному місці, доступному для всіх членів групи реагування на інциденти, і її слід регулярно

оновлювати в міру додавання та вилучення співробітників до групи реагування, а також у міру змін у вашому бізнесі.

2. Виявлення та аналіз

Фаза виявлення та аналізу у вашому CSIRP запускається, коли щойно стався інцидент, і вашій організації потрібно визначити, як на нього реагувати.

Інциденти безпеки можуть виникати з багатьох різних джерел, і створити план реагування на будь-який тип інцидентів безпеки непрактично чи навіть можливо. NIST надає список деяких найбільш поширених методів атаки , які ви можете використовувати як відправну точку, коли визначатимете, які кроки потрібно вжити в разі події безпеки. Ви також повинні розглянути, які вразливі місця має ваша компанія і наскільки ймовірна атака на одну з цих вразливостей, і включити їх у своє планування.

Інциденти безпеки можна виявити кількома різними способами. Ознаками інциденту є або попередні (виявлені до події), або індикатори (виявлені під час або після нападу). Наприклад, ви можете помітити велику кількість невдалих спроб входу і визначити, що хакер намагається вгадати робоче ім’я користувача та пароль, щоб проникнути у вашу мережу (попередник інциденту безпеки). Або, можливо, ваше антивірусне програмне забезпечення сповіщає вас, коли один із ваших співробітників натискає посилання на зловмисне програмне забезпечення і воно заразить його комп’ютер (індикатор того, що подія безпеки вже триває). В ідеалі ви могли б виявити кожну атаку до того, як вона станеться, але це не завжди можливо. Завчасне планування відповіді – це найкраща річ.

Після того, як ви визначите, що стався інцидент, NIST виклав кілька способів, якими ви можете проаналізувати та підтвердити інцидент , щоб переконатися, що ви запускаєте правильну реакцію на інцидент. Ваш CSIRP має дати вказівки щодо документування інциденту, незалежно від великого чи маленького, та визначення пріоритету реагування на інцидент. Наприклад, використовуючи два наведені вище приклади, ваша відповідь на когось, хто намагається ввійти в мережу, буде відрізнятися від зараженого комп’ютера, і якщо обидва події відбувалися б одночасно, вам потрібно було б надати пріоритет одному над іншим.

Останнім кроком на цьому етапі є повідомлення. Залежно від того, яка інформація була порушена, вам також може знадобитися сповістити певні сторони , такі як правоохоронні органи, FTC, ваші клієнти, уражені підприємства та інші. Вам потрібно працювати з юридичною командою та командою з дотримання вимог, щоб переконатися, що ви розумієте, кого потрібно сповістити, і мати план сповіщення. Якщо ви не приділите час, щоб включити це в свій CSIRP, ви ризикуєте порушити закони штату, федеральні

чи міжнародні закони та створити додаткові проблеми для вашого бізнесу. CCPA і GDPR обидва вимагають звітування про порушення, тому вам і вашій команді з дотримання вимог доведеться допомагати один одному. Наявність відкритого каналу зв'язку з вашою командою з відповідності є неоціненним у багатьох відношеннях, особливо коли ви маєте справу з інцидентом.

3. Стримування, викорінення та відновлення

Цей етап є серцем вашого CSIRP. Усе, що ви робите у відповідь на атаку, буде зосереджуватися на стримуванні інциденту, ліквідації загрози та відновленні після атаки.

Як тільки команда визначить інцидент з безпекою, найближчою метою є стримати інцидент і запобігти подальшому пошкодженню. Це передбачає:

- Короткочасне стримування — це може бути так само просто, як ізоляція сегмента мережі, що піддається атаці, або зняття зламаних виробничих серверів, які перенаправляють трафік на резервні сервери.
- Довгострокове стримування — застосування тимчасових виправлень до уражених систем, щоб дозволити їх використовувати у виробництві, під час перебудови чистих систем, підготовки до введення їх в режим онлайн на стадії відновлення.

NSIT надав список критеріїв , які ви повинні враховувати при прийнятті рішення щодо стратегії стримування:

- Потенційне пошкодження та крадіжка ресурсів
- Необхідність збереження доказів
- Доступність послуг (наприклад, підключення до мережі, послуги, що надаються зовнішнім сторонам)
- Час і ресурси, необхідні для реалізації стратегії
- Ефективність стратегії (наприклад, часткове стримування, повне стримування)
- Тривалість рішення (наприклад, екстренний обхідний шлях, який потрібно видалити за чотири години, тимчасовий обхідний шлях, який потрібно видалити за два тижні, постійне рішення).

Поки ви працюєте на цьому етапі, ви також повинні зібрати якомога більше доказів про атаку та зберегти їх для внутрішнього та зовнішнього використання. Ви також можете попрацювати над ідентифікацією атакуючого хоста, якщо це буде розумно, але це може зайняти багато часу і навіть неможливо в деяких сценаріях. Ваша увага завжди повинна бути максимально стримана.

Видалення включатиме різні кроки залежно від типу інциденту, з яким ви стикаєтесь, але, по суті, ви усунете все, що вам потрібно, щоб зупинити атаку,

чи це означає видалення зловмисного програмного забезпечення, відключення зламаних облікових записів , закриття вразливостей у вашій мережі тощо. .
FTC надає деякі кроки, які ви можете зробити, щоб захистити свої операції та ліквідувати загрозу безпеці ваших даних, включаючи консультації з групою криміналістів даних, захист будь-яких фізичних зон, пов'язаних із порушенням, виправлення інформації, яка була неправильно розміщена на вашому веб-сайті, спілкування з людей, які виявили порушення, тощо. Коли ви намагаєтеся заблокувати свою безпеку під час або після злому даних, ви не хочете його крити. Це найбільша перевага задокументованого CSIRP: ви матимете охоплення всіх ваших баз і матимете набагато менше шансів залишити вразливість відкритою під час порушення.
Після того, як ви усунули порушення, можна приступати до етапу відновлення. Це включає внесення змін та оновлень до вашого плану безпеки, усунення вразливості, яка спричинила інцидент безпеки, і проведення будь-якого навчання щодо процесів або процедур, які співробітники повинні знати, щоб запобігти повторенню подібної події, якщо це було частиною проблеми.
Ліквідація та відновлення може зайняти дні, тижні або місяці залежно від розміру порушення. NIST виступає за поетапний підхід , коли на ранніх етапах якомога швидше підвищують вашу загальну безпеку, а пізні фази зосереджуються на довгострокових змінах та поточній роботі, щоб забезпечити безпеку вашої організації.

4. Діяльність після інциденту

Після того, як інцидент було зупинено, оновлення системи безпеки було зроблено, а ваша організація повернулася до нормального стану, вашій організації має знадобитися деякий час, щоб розібратися в інциденті.

- Поміркуйте про те, що трапилося, і поговоріть про те, як ви можете виявити подібні випадки в майбутньому і зупинити їх швидше.
- Оцініть тяжкість і пошкодження. Може бути важко усвідомити серйозність інциденту та розмір збитків, які він завдав. Загалом, вам потрібно буде з'ясувати причину інциденту. У випадках, коли був успішний зовнішній зловмисник або зловмисний інсайдер, вважайте подію більш серйозною і відповідайте відповідним чином.
- Перегляньте свій CSIRP і запитайте себе та свою команду, чи було щось, що зробило б план більш ефективним.
- Почніть процес сповіщення. Злом даних — це інцидент безпеки, під час якого конфіденційні, захищені або конфіденційні дані копіюються, передаються, переглядаються, викрадаються або використовуються окремою неавторизованою особою. Закони про конфіденційність, такі як GDPR та SB1386 Каліфорнії, вимагають публічного сповіщення у

разі такого порушення даних. Повідомте постраждалих сторін, щоб вони могли захистити себе від крадіжки особистих даних або інших наслідків розкриття конфіденційних особистих або фінансових даних.

NIST також надав детальний список запитань, показників та рекомендацій щодо відновлення після інциденту , який допоможе вашій команді ефективно відновлюватися після інциденту безпеки та вчитися на цьому, а не просто рухатися далі. твоя робота.

Як часто ви повинні переглядати свою процедуру реагування на інциденти?

Вам слід переглядати план реагування на інциденти безпеки щонайменше щороку, щоб переконатися, що заходи безпеки вашого бізнесу працюють належним чином і відповідають найкращим практикам галузі та темпам змін технологій. Однак ваша процедура реагування на інцидент має розвиватися, коли відбуваються зміни, зокрема:

- Дотримання нових застосовних правил, таких як Загальний регламент захисту даних (GDPR)
- Зміни штатів щодо конфіденційності даних та кібербезпеки
- Прийняття нових технологій
- Зміни в структурі внутрішніх команд, які займаються питаннями безпеки
- Нові типи загроз, такі як криза громадського здоров’я, змушують організації рухатися до розподіленої робочої сили
- Збій даних у компанії

Переглядаючи політику та процедури своєї організації, важливо поставити такі запитання:

- Чи важко виконувати процедури?
- Чи почали ви використовувати нові технології чи процеси, які ще не вписані у ваші процедури реагування?
- Чи потребує належного впровадження політики та процедур більше навчання працівників?

1.2 ЗМІСТ ПЛАНУ РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ

Як визначити, задокументувати та класифікувати життєво важливі елементи, вразливості та потенційні загрози вашої організації

Визначте бізнес і ресурси, які необхідно захистити:

- Визначте, які з ваших основних видів діяльності дозволяють вашій організації існувати, досягати її корпоративних цілей і отримувати дохід: виробляти товари, продавати товари, доставляти товари тощо.
- Для кожного з цих видів діяльності визначте, які системи ІКТ (бази даних, програми, системи керування) та мережеві з'єднання їх підтримують
- Визначте також, де розташовані ці системи ІКТ: на ваших власних серверах чи в хмарі?
- Визначаючи ці активи, не забувайте про потоки інформації до третіх сторін (постачальників, клієнтів тощо) або потоки промислової системи контролю.

Визначте свої коштовності в короні

Визначте зараз, які активи, дані, процеси або мережеві з’єднання настільки важливі для вашої організації, що, якщо ви втратите (контроль) над ними, у вас великі проблеми або ви навіть втратите бізнес

Призначте пріоритети бізнесу для відновлення

Цей акт визначення пріоритетів визначить порядок, у якому системи будуть відновлені. У більшості випадків базова мережа потребує найвищого пріоритету, оскільки це не тільки шлях, яким системні адміністратори досягають ваших активів, але й шлях, яким кіберзлочинці атакують ваші системи. Поки зловмисники можуть користуватися вашими мережевими з’єднаннями, вони можуть скасувати будь-яку іншу діяльність із відновлення. Якщо активи мають однаково високий пріоритет, можна розглянути можливість паралельного відновлення.

Задокументуйте, як працюють ваші системи, і зберігайте цю документацію актуальні

Переконайтеся, що спосіб роботи ваших систем задокументований і що це інформація оновлюється та доступна в системах документації групи реагування на інциденти. Абсолютно необхідними документами є:

Схема мережі, що відображає архітектуру мережі з внутрішньою сегментацією мережі та різними шлюзами до зовнішніх мереж, DMZ, VPN, діапазонами IP-

адрес. Ця схема також повинна включати різні пристрої безпеки, які можуть містити реєстраційну інформацію про діяльність мережі (брандмауери, (зворотні) проксі-сервери, системи виявлення вторгнень, системи керування подіями інцидентів безпеки). Для великих компаній зі складними мережами також необхідно мати версію архітектури мережі високого рівня, щоб ви могли швидко отримати уявлення про мережу в разі надзвичайної ситуації.

Інвентаризація обладнання та послуг. Цей інвентар міститиме життєво важливі активи у вашому середовищі, усі різні сервери та мережеві компоненти, які використовуються для надання різних корпоративних послуг. Оскільки деякі з цих (фізичних) серверів можуть обслуговувати кілька бізнес-функцій, важливо знати, які служби на якому сервері працюють.

Списки облікових записів і доступу. Завжди важливо знати, хто має право на доступ, використання та/або керування вашою мережею та різними системами в ній. Це дозволить вам виявити будь-які дивні або зловживані облікові записи під час інциденту.

ЗНАЙТЕ, ЩО ЗАХИЩАЄТЕ

Визначте свої активи та потенційні загрози

Коли потрапить інцидент, першими питаннями, які виникнуть, є: які активи знаходяться під загрозою, а які з цих активів є життєво важливими для вашої діяльності? Вам доведеться вирішити, які активи потребують вашої уваги в першу чергу, щоб залишатися в бізнесі та мінімізувати шкоду вашому бізнесу.

Ось чому дуже важливо визначити, задокументувати та класифікувати «життєво важливі» вашої організації: активи, від яких залежить ваша організація для здійснення своєї основної діяльності. Це допоможе вам визначити, де застосовувати які захисні заходи, і прийняти швидкі та виправдані рішення під час процесу управління інцидентом.

Наступний список дає вам уявлення про те, якими можуть бути ці «життєві елементи»: управління, організація, процеси, знання (наприклад, інтелектуальна власність була вкрадена), люди, інформація (наприклад, набори даних були вкрадені або змінені), програми (наприклад, веб-сайт). не працює або зіпсовано, інфраструктура (наприклад, система та/або мережеві з’єднання не працюють), фінансовий капітал (наприклад, банківські рахунки).

Також непогано визначити вразливі місця та потенційні загрози.

Ключові ролі в групі реагування на інциденти

Щоб виконати план реагування на інциденти, вам потрібна команда реагування на інциденти . У великій організації ці ролі можуть виконувати штатні співробітники або цілі команди; у менших організаціях їх можуть заповнити співробітники з іншими штатними посадами, які також беруть участь у процесі реагування на інциденти.

Основні ролі в команді:

- Менеджери з реагування на інциденти — мають принаймні двох співробітників, відповідальних за затвердження плану реагування на інциденти та координацію діяльності у разі виникнення інциденту.
- Аналітики безпеки — переглядають сповіщення, визначають можливі інциденти та проводять первинне розслідування, щоб зрозуміти масштаб атаки.
- Дослідники загроз — відповідальні за надання контекстної інформації про загрозу, використання інформації з Інтернету, каналів розвідки загроз, даних із засобів безпеки тощо.
- Інші зацікавлені сторони — до них можуть входити вище керівництво або члени правління, відділ кадрів, PR та старший персонал із безпеки, наприклад Головне управління інформаційної безпеки (CISO).
- Треті сторони — наприклад, юристи, сторонні служби безпеки або правоохоронні органи.

Рекомендації NIST щодо організації групи реагування на інциденти з комп’ютерною безпекою (CSIRT)

Посібник з обробки інцидентів NIST Computer Security містить детальні вказівки щодо того, як створити можливості реагування на інциденти в організації. Він охоплює декілька моделей для груп реагування на інциденти , як вибрати найкращу модель та найкращі методи роботи з командою.

Моделі груп реагування на інциденти

NIST пропонує три моделі для груп реагування на інциденти:

- **Центральний — централізований** орган, який займається реагуванням на інциденти для всієї організації.
- **Розподілене** — кілька груп реагування на інциденти, кожна з яких відповідає за фізичне розташування (наприклад, філію), відділ або частину IT-інфраструктури
- **Координована** — центральна група реагування на інциденти, яка працює разом із розподіленими групами реагування на інциденти, не маючи на них повноважень. Центральна команда слугує центром знань

і пропонує допомогу у складних, критичних або загальноорганізаційних інцидентах.

У кожній із цих моделей персонал може бути співробітником, частково або повністю переданим на аутсорсинг. Співробітники також можуть працювати повний або неповний робочий день.

Вибір моделі команди

NIST пропонує кілька міркувань для вибору моделі реагування на інцидент:

- **Чи потрібно реагувати на інцидент 24/7?** Чи повинні бути на місці співробітники, які реагують на інцидент, чи достатньо зв'язку по телефону? Доступність у режимі реального часу та присутність на місці найкращі, оскільки вони дозволяють негайно реагувати на інцидент, що може запобігти пошкодженню.
- **Персонал повинен працювати на неповний чи повний робочий день?** Співробітників, які працюють на неповний робочий день, можна використовувати для створення віртуальної групи реагування на інциденти, як-от волонтерський відділ реагування на надзвичайні ситуації. Коли трапляється інцидент, IT-довідкова служба може бути першою точкою контакту. Вони можуть провести первинне розслідування, швидко викликати членів групи реагування на інцидент, і будь-який доступний може відреагувати на інцидент.
- **Чи мають персонал бути експертами з безпеки?** Який рівень знань необхідний? Реагування на інциденти вимагає широких знань про IT-системи, протоколи зв'язку, методи атаки, а також середовище, системи та процедури організації. Аутсорсингові команди, як правило, мають більш потужний досвід у сфері безпеки, але співробітники краще розуміють IT-середовище, нормальну поведінку чи шкідливу поведінку, а також те, які системи є критичними тощо.
- **Скільки коштуватиме група реагування на інцидент** ? Оскільки працівники, які реагують на інциденти, потребують спеціального досвіду та часто вимагають бути на місці 24/7, вони можуть становити значну інвестицію. Постачальники керованих послуг безпеки (MSSP) також можуть бути дорогими, а також є додаткові витрати на інструменти безпеки, фізичні засоби та безпечні методи зв'язку.

Як організувати реагування на інциденти

Посібник NIST з реагування на інциденти містить декілька вказівок щодо організації та роботи підрозділу реагування на інциденти.

Як створити офіційну ‘‘можливість’’ реагування на інцидент?

Навіть якщо ваша організація невелика, поставтеся серйозно до реагування на інциденти та створіть офіційний орган реагування на інциденти. Якщо неможливо створити штатну групу реагування на інциденти, створіть віртуальну команду з персоналом, який працює неповний робочий день, і надайте цій команді повні повноваження та відповідальність. Це значно покращить вашу здатність реагувати на кібератаку.

Створення політики реагування на інциденти

Це попередній план реагування на інцидент, який викладає організаційні рамки реагування на інциденти. Він визначає, що вважається інцидентом безпеки, хто відповідає за реагування на інцидент, ролі та відповідальність, вимоги до документації та звітності.

Визначення плану реагування на інцидент

Згідно з методологією NIST, план реагування на інцидент — це не просто перелік кроків, які необхідно виконати, коли інцидент трапиться. Це дорожня карта для програми реагування на інциденти організації, включаючи короткострокові та довгострокові цілі, показники для вимірювання успіху, навчання та вимоги до роботи для ролей реагування на інциденти.

Розробка процедури реагування на інцидент

Нижче наведено детальні дії, які групи реагування на інцидент використовуватимуть для реагування на інцидент. Вони повинні ґрунтуватися на політиці та плані реагування на інциденти та охоплювати всі чотири фази життєвого циклу реагування на інцидент: підготовку, виявлення та аналіз, стримування, ліквідацію та відновлення та діяльність після інциденту.

Життєвий цикл реагування на інциденти NIST

NIST визначає чотириетапний процес реагування на інцидент, проілюстрований на схемі нижче. Процес NIST підкреслює, що реакція на інцидент не є лінійною діяльністю, яка починається з виявлення інциденту і закінчується ліквідацією та відновленням. Швидше, реагування на інциденти — це циклічна діяльність, де постійно навчаються та вдосконалюються, щоб дізнатися, як краще захистити організацію. Після кожного інциденту докладають значних зусиль для документування та розслідування того, що сталося під час інциденту, для повернення на попередні етапи та для кращої підготовки, виявлення та аналізу майбутніх інцидентів.

Існує також петля зворотного зв'язку від етапу стримування та ліквідації до виявлення та аналізу — багато частин атаки не повністю зрозумілі на етапі виявлення і розкриваються лише тоді, коли на місце події «виходять особи реагування». Ці уроки можуть допомогти команді більш повно виявляти й аналізувати атаки наступного разу.

1.3 ПРИЗНАЧЕННЯ ОБОВ'ЯЗКІВ ТА СТВОРЕННЯ КОМАНДИ РЕАГУВАННЯ НА ІНЦЕНДИ З КІБЕРБЕЗПЕКИ

ПРИЗНАЧЕННЯ ОБОВ'ЯЗКІВ ТА РОЛЬ ЛЮДЯМ С ПРАВИЛЬНІ НАВИЧКИ

Важливо, щоб ролі та відповідальність у разі інцидентів кібербезпеки були задокументовані у вашому плані реагування на інциденти кібербезпеки. Складаючи опис цих ролей та обов'язків, ви повинні поставити собі такі запитання:

1. Хто є внутрішнім контактним пунктом щодо інцидентів кібербезпеки? І як з ним/нею можна зв'язатися?
2. Які існують різні завдання реагування на інцидент? І хто за що відповідає?
3. Хто керує інцидентом з ділової/технічної сторони? Це має бути хтось у вашій компанії з повноваженнями приймати рішення, який стежитиме за інцидентом від початку до кінця.

4. Хто буде підтримувати зв’язок із вищим керівництвом?
5. Хто може залучити зовнішнього партнера з реагування на інциденти?
6. Хто може подати скаргу до правоохоронних органів/повідомити контролюючі органи?
7. Хто має право спілкуватися з пресою та сторонніми особами?

Ви зрозумієте, що для того, щоб адекватно подолати інцидент кібербезпеки, потрібні різні навички, щоб брати на себе різні обов’язки та необхідні ролі в ефективному реагуванні на інцидент.

	ОБОВ'ЯЗКИ	РОЛЬ
Управління інцидентами	Управління інцидентом кібербезпеки з моменту його виявлення до закриття.	Менеджер з реагування на інциденти кібербезпеки
Можливість прийняття ділових рішень	Оцінка впливу на бізнес і дії відповідно до нього. Залучення правильних ресурсів. Прийняття рішень про те, як діяти, напр. вирішувати, чи можна вимкнути підключення до Інтернету зламаної системи та коли це найбільш підходящий час. Вирішити, коли почати очищення. Прийняття рішення щодо подання скарги.	Менеджмент
Можливості управління мережею	Технічне ноу-хау в мережі організації (брандмауер, проксі, IPS, маршрутизатори, комутатори,...). Аналіз, блокування або обмеження потоку даних у вашій мережі та з неї. IT-операції, інформаційна безпека та безперервність бізнесу.	Персонал технічної підтримки ІКТ
Можливості адміністратора робочої станції та сервера (права адміністратора)	Аналіз і керування скомпрометованими робочими станціями та серверами.	Персонал технічної підтримки ІКТ
Юридична порада	Оцінка договірних та судових наслідків інциденту. Гарантія того, що заходи з реагування на інциденти залишаються в межах законодавчих, нормативних і політичних кордонів організації. Подання скарги.	Юридичний відділ/ Юрист компанії
Навички комунікації	Відповідне спілкування з усіма відповідними групами зацікавлених сторін. Негайно відповідаючи клієнтам, акціонерам, прес-питання.	Відділ комунікацій або зв'язків з громадськістю
Криміналістичні навички	Збір та аналіз доказів належним чином, тобто для того, щоб докази були прийнятними в суді.	Персонал технічної підтримки ІКТ
Фізична безпека	Розгляд аспектів інциденту, які пов’язані з • фізичним доступом до приміщення • фізичний захист кіберінфраструктури.	Офіцер безпеки
Кризовий менеджмент	Кризовий менеджмент	Кризовий менеджмент

ГРУПА РЕАГУВАННЯ НА КІБЕРІНЦИДІЇ

В ідеальному світі кожна організація має групу реагування на інциденти, яка скликається щоразу, коли виникає інцидент. Звичайно, розмір компанії

визначає розмір і структуру групи реагування на інциденти. Менші компанії, які не мають ресурсів для справжньої команди, можуть призначити особу першого реагування – в ідеалі – когось із можливостями прийняття ділових рішень – зі свого персоналу. У разі інциденту з кібербезпекою він/вона повинен звернутися до зовнішньої допомоги, але залишиться особою, яка в кінцевому рахунку відповідає за реагування на інцидент в організації.
Склад цієї групи реагування на інцидент буде визначатися різними навичками, які необхідні для обробки інциденту (див. також: таблицю на сторінці 11). Для невеликих компаній, деякі з цих навичок, можливо, доведеться отримати поза організацією, щоб отримати першу допомогу.

МІНІМАЛЬНА ГРУПА РЕАГУВАННЯ НА ІНЦЕНДІ ПОВИННА ВХОДИТИ НАСТУПНІ РОЛІ

1. МЕНЕДЖЕР РЕАГУВАННЯ НА ІНЦИДЕНТИ

Особа, яка буде керувати інцидентом найближчим часом

як це доводиться до їхньої уваги, поки воно не буде локалізовано та виправлено. Він/вона буде підтримувати зв’язок у розслідуванні показників, з керівництвом і, можливо, з іншим внутрішнім персоналом і зовнішніми ресурсами для вирішення інциденту. Ця особа повинна знати про бізнес-діяльність вашої організації, тому що вона першою прийматиме бізнес-рішення.

2. ПЕРСОНАЛ ТЕХНІЧНОЇ ПІДТРИМКИ ІКТ

Ця особа повинна добре знати вашу інфраструктуру ІКТ, оскільки вона відповідатиме за дослідження індикаторів, підтвердження інциденту та розробку технічних рішень для управління інцидентом.

РОЗМІР ТА ПРИРОДА ОРГАНІЗАЦІЇ ВИЗНАЧАЮТЬ ЧИ ПОТРІБНО БІЛЬШЕ РОЛЕЙ

Невеликі організації часто мають гнучкість, щоб швидко залучити корпоративне керівництво, щоб впоратися з інцидентом. Це не стосується великих організацій, яким, можливо, доведеться обробляти кілька інцидентів в більш автономному режимі, і в цьому випадку керівники компанії будуть задіяні в реагуванні на інциденти лише тоді, коли станеться дуже серйозний інцидент.

Більші організації. Чим більша ваша організація, тим більш диференційованим повинен бути склад вашої групи реагування на інциденти. Для більших організацій, на додаток до групи реагування на інциденти, може бути створена група з кризового управління, що складається з представників корпоративного управління, щоб взяти на себе відповідальність за стратегічні та пов'язані з бізнесом рішення та комунікації, коли стикаються з серйозними інцидентами. Це дозволить менеджеру з реагування на інцидент більше зосередитися на технічних питаннях інциденту.

ДЕЯКІ ОРГАНІЗАЦІЇ ПОВИННІ ПРИЗНАЧИТИ ДАНІ ОФІЦЕРА З ЗАХИСТУ АБО КОНТАКТНИЙ ПУНКТ

Загальний регламент про захист даних (GDPR) зобов'язує певні організації призначати спеціаліста із захисту даних або «DPO». Точніше ті організації, які займаються обробкою персональних даних і які потребують регулярного та систематичного спостереження за великими зацікавленими особами, або обвинувачені у широкомасштабній обробці спеціальних категорій даних, наприклад, даних охорони здоров'я або кримінальних судимостей або правопорушення.

Директива про мережеву та інформаційну безпеку (NIS) вимагає від операторів основних послуг (OES) і постачальників цифрових послуг (DSP) призначати контактну точку для безпеки мереж та інформаційних систем, щоб забезпечити безперебійну комунікацію з компетентними органами у разі інцидентів.

1.4 ЗВЕРНЕННЯ ДО ЗОВНІШНІХ ЕКСПЕРТІВ; ЕКСПЕРТИ З РЕАГУВАННЯ НА КІБЕРІНЦИДІЇ

Незалежно від того, чи є ваша організація МСП чи велика організація, розвивати та підтримувати весь необхідний досвід та навички для реагування на інциденти в домашніх умовах коштує дорого. Особливо це стосується навичок реагування на інциденти з кібербезпеки в судово-медичних та юридичних консультаціях. Тому майте на увазі, що може бути більш рентабельним звернутися до зовнішніх партнерів з реагування на інциденти з кібербезпеки, щоб закрити прогалину в базі навичок вашої організації.

- Професійні спеціалісти з реагування на інциденти, які знають можливі загрози та сценарії, можуть скоротити час на діагностику інциденту.

- Використовуйте обґрунтований з точки зору криміналістики підхід, щоб будь-які докази були забезпечені та задокументовані відповідно до юридично чинного ланцюга опіки. Ці докази потім можуть бути представлені в суді, якщо це необхідно.
- Вони мають досвід роботи в правильному порядку та мають інструменти для відновлення слідів із RAM-пам'яті, віртуальних машин, жорстких дисків та мереж.
- Ці експерти допоможуть вам визначити причини інциденту та запропонують поради щодо стримування, ліквідації та ліквідації інциденту.

КОЛИ ЗВ'ЯЗАТИСЯ З ЕКСПЕРТОМ?
А. НА ФАЗІ ПІДГОТОВКИ
Б. КОЛИ ІНЦИДЕНТ КІБЕРБЕЗПЕКИ ВІДБУВАЄТЬСЯ

Ви можете або укласти контракт і залишити партнера з реагування на інциденти кібербезпеки на етапі підготовки, або дочекатися фактичного інциденту кібербезпеки. Майте на увазі, що укладення такого договору вимагає часу та зусиль. Тому, якщо ви впевнені, що вам знадобиться стороння допомога, краще не чекати. Таким чином ви виграєте дорогоцінний час на початку інциденту з кібербезпекою. Кілька спеціалізованих консалтингових фірм з надання послуг з реагування на інциденти та юридичних офісів пропонують підписки, які зберігають свої можливості реагування на інциденти для абонента. Крім того, більшість із них включають навчальні заняття з вашою командою реагування на інциденти, щоб полегшити співпрацю між ними, коли трапиться інцидент.

ДЕЯКІ ОРГАНИ МОЖУТЬ ДОПОМОГТИ ІЗ РОЗСЛІДЖЕННЯМ

Інші сторони, як-от галузеві регулятори, Національний орган із захисту даних, Центр кібербезпеки Бельгії (CCB), відділ Cert.be та правоохоронні органи (поліція та магістрати), можуть мати значення, коли ви стикаєтесь з кібербезпекою. інцидент безпеки кримінального характеру або у разі порушення персональних даних. Деякі законодавчі акти навіть зобов’язують вас інформувати ці сторони, коли ви виявили інцидент конкретного характеру.

Ці сторони часто можуть допомогти інформацією про загрозу та практичними вказівками на основі попередніх інцидентів, з якими вони впоралися. Але майте на увазі, що метою правоохоронних органів є виявлення та зловживання зловмисника. Це не їхнє завдання — відновити роботу вашого бізнесу. Також можливо, що найефективніший спосіб зловити зловмисника не обов'язково буде таким самим, як найшвидший спосіб повернутися до звичайного режиму.

Крім того, більшість цих розслідувань охоплюються професійною таємницею, що ускладнює отримання інформації про їх результати. Однак вони можуть розкрити інформацію, яка допоможе вам ідентифікувати зловмисника та його спосіб роботи, що може прискорити аналіз вашого інциденту кібербезпеки.

Поліція може попросити вашу організацію не вимикати вашу систему відразу. Якщо ви це зробите, зловмисник помітить і відступить, що часто робить неможливим простежити їх потім. Однак для вашої організації найшвидший спосіб повернутися до бізнесу може бути негайно закритий і почати з чистого аркуша.

1.5 ПІДГОТОВКА ОРГАНІЗАЦІЇ ДО ЛІКУВАННЯ ІНЦИДЕНТУ КІБЕРБЕЗПЕКИ

МЕРЕЖА ЕКСПЕРТІВ – СПИСОК КОНТАКТІВ

Звернення за допомогою до потрібних професіоналів у потрібний час має вирішальне значення під час інциденту, оскільки це може допомогти обмежити фізичну та репутаційну шкоду вашій компанії. Список контактів, який містить усіх цих людей або організацій, допоможе вам у цьому процесі. Цей список містить імена, ролі, контактні та резервні дані різних членів групи з реагування на кіберінциденти, зовнішніх сторін, які є уповноваженими, правоохоронних органів тощо.

Контактна інформація, яка записується, має включати номери стаціонарних та мобільних телефонів, ділові адреси електронної пошти (включаючи публічні ключі шифрування для конфіденційності та цілісності зв'язку) та фізичні адреси традиційної пошти та посилок. Переконайтеся, що у вас також є альтернативні варіанти контакту (додаткові адреси електронної пошти, номери факсів), оскільки можливо, що група реагування на інцидент не зможе використовувати внутрішню мережу під час інциденту.

Ця контактна інформація має бути доступна в центральному автономному місці, як-от фізична підшивка або автономний комп'ютер. Поряд із «сирою» контактною інформацією ця екстрена інформація також повинна включати процедури ескалації. Ця інформація має бути легкодоступною та зберігатися у надзвичайному фізичному захищеності. Один із методів захисту та забезпечення доступності цієї інформації полягає в шифруванні її на спеціальному портативному комп'ютері безпеки, розміщеному в захищеному сховищі, і обмеження доступу до сховища уповноваженим особам, таким як керівник групи реагування на інциденти та керівник інформаційної служби. - tion Officer (CIO) або Chief Technology Officer (CTO).

ПОСАДА	МІСЦЕ РОБОТИ	РОЛЬ	КОНТАКТНІ ДАНІ
Менеджер з реагування на інциденти	В будинку/ в офісі	Управління реагуванням на кіберінциденти	Адреса Телефон E-mail Вихідні та резервні Контактна інформація
Юрист	В будинку/ в офісі	Експерт з права	
Судова експертиза	В офісі	Судмедексперт	
Поліція	Правоохоронна діяльність	Правоохоронна діяльність	

АППАРАТНО ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ІНЦИДЕНТУ КІБЕРБЕЗПЕКИ

Щоб підвищити зрілість та ефективність групи реагування на інциденти, необхідно створити відповідні інструменти. Важливо, щоб група реагування на інциденти мала в розпорядженні автономні системи та інструменти, які дозволяють їм обробляти інцидент, навіть якщо корпоративна мережа була скомпрометована. Це означає, що коли системи або мережі вашої організації більше не доступні, система реагування на інциденти все ще є. У цих системах мають бути доступні процедури інцидентів та списки контактів.

Інструменти реагування на інциденти мають життєво важливе значення для того, щоб організації могли швидко виявляти кібератаки, експлойти, зловмисне програмне забезпечення та інші внутрішні та зовнішні загрози безпеці та впоратися з ними.

Зазвичай ці інструменти працюють разом із традиційними рішеннями безпеки, такими як антивірус і брандмауери , щоб аналізувати, сповіщати, а іноді й допомагати зупинити атаки. Для цього інструменти збирають інформацію з

системних журналів, кінцевих точок, систем автентифікації або ідентифікації та інших областей, де вони оцінюють системи на наявність підозрілих дій та інших аномалій, які вказують на компроміс або порушення безпеки.

Інструменти допомагають автоматично та швидко контролювати, виявляти та вирішувати широкий спектр проблем безпеки, таким чином оптимізуючи процеси та усуваючи необхідність виконувати більшість повторюваних завдань вручну. Більшість сучасних інструментів можуть надавати різноманітні можливості, включаючи автоматичне виявлення та блокування загроз і, в той же час, попередження відповідних груп безпеки для подальшого розслідування проблеми.

Групи безпеки можуть використовувати інструменти в різних областях залежно від потреб організації. Це може бути моніторинг інфраструктури, кінцевих точок, мереж, активів, користувачів та інших компонентів.

Вибір найкращого інструменту є проблемою для багатьох організацій. Щоб допомогти вам знайти правильне рішення, нижче наведено список інструментів реагування на інциденти для виявлення, запобігання та реагування на різні загрози безпеці та атаки, спрямовані на ваші системи ІКТ.

1. **ManageEngine**

ManageEngine EventLog Analyzer — це інструмент SIEM, який зосереджується на аналізі різних журналів і витягує з них різну інформацію про продуктивність та безпеку. Інструмент, який в ідеалі є сервером журналів, має аналітичні функції, які можуть виявляти та повідомляти про незвичайні тенденції в журналах, наприклад, які є результатом несанкціонованого доступу до IT-систем та активів організації. Цільові області включають ключові послуги та програми, такі як веб-сервери, DHCP-сервери, бази даних, черги друку, служби електронної пошти тощо. Також аналізатор ManageEngine, який працює в системах Windows і Linux, корисний для підтвердження відповідності стандартам захисту даних. такі як PCI, HIPPA, DSS, ISO 27001 тощо.

2. **IBM Qradar**

IBM QRadar SIEM — це чудовий інструмент виявлення, який дає змогу групам безпеки зрозуміти загрози та визначити пріоритети відповідей. Qradar бере дані активів, користувачів, мережі, хмари та кінцевої точки, а потім співвідносить їх із інформацією про загрози та вразливості. Після цього він

застосовує розширену аналітику для виявлення та відстеження загроз, коли вони проникають і поширюються крізь системи. Рішення створює інтелектуальне уявлення про виявлені проблеми безпеки. Це показує основну причину проблем із безпекою разом із областью дії, що дозволяє командам безпеки реагувати, усувати загрози та швидко зупиняти поширення та вплив. Як правило, IBM QRadar — це повне аналітичне рішення з різноманітними функціями, включаючи опцію моделювання ризиків, що дозволяє командам безпеки моделювати потенційні атаки.

IBM QRadar підходить для середнього та великого бізнесу і може бути розгорнутий як програмне забезпечення, апаратне забезпечення або віртуальний пристрій у локальному, хмарному або SaaS середовищі.

Інші функції включають

- Відмінна фільтрація для отримання бажаних результатів
- Розширена здатність полювання на загрози
- Аналіз Netflow
- Можливість швидкого аналізу масових даних
- Відтворіть очищені або втрачені злочини
- виявити приховані потоки
- Аналітика поведінки користувачів.

3. **SolarWinds**

SolarWinds має широкі можливості керування журналами та звітами, а також реагування на інциденти в реальному часі. Він може аналізувати та виявляти експлойти та загрози в таких областях, як журнали подій Windows, отже, дозволяє командам контролювати та вирішувати системи проти загроз.

Security Event Manager має прості у використанні інструменти візуалізації, які дозволяють користувачам легко ідентифікувати підозрілі дії або аномалії. Він також має детальну та просту у використанні панель інструментів на додаток до чудової підтримки з боку розробників. Аналізуючи події та журнали для виявлення загроз локальної мережі, SolarWinds також має автоматичну відповідь на загрози на додаток до моніторингу USB-накопичувача. Його менеджер журналів і подій має розширені можливості фільтрації та пересилання журналів, а також параметри консолі подій і керування вузлами.

Основні особливості включають

- Високий криміналістичний аналіз
- Швидке виявлення підозрілої діяльності та загроз
- Постійний моніторинг безпеки
- Визначення часу події
- Підтримує відповідність нормам DSS, HIPAA, SOX, PCI, STIG, DISA та іншим нормам.

Рішення SolarWinds підходить для малого та великого бізнесу. Він має як локальні, так і хмарні варіанти розгортання та працює на Windows та Linux.

4. **LogRhythm**

LogRhythm , який доступний як хмарний сервіс або локальний пристрій, має широкий спектр чудових функцій, які варіюються від кореляції журналів до штучного інтелекту та аналізу поведінки. Платформа пропонує платформу аналізу безпеки, яка використовує штучний інтелект для аналізу журналів і трафіку в системах Windows і Linux. Він має гнучке зберігання даних і є хорошим рішенням для фрагментованих робочих процесів на додаток до забезпечення сегментованого виявлення загроз навіть у системах, де немає структурованих даних, централізованої видимості чи автоматизації. Підходить для малих і середніх організацій, він дає змогу переглядати вікна чи інші журнали та легко звужуватись до діяльності мережі.

5. **Rapid7 InsightIDR**

Rapid7 InsightIDR — це потужне рішення безпеки для виявлення інцидентів і реагування, видимості кінцевої точки, моніторингу аутентифікації, серед багатьох інших можливостей. Хмарний інструмент SIEM має функції пошуку, збору та аналізу даних і може виявляти широкий спектр загроз, включаючи вкрадені облікові дані, фішинг і зловмисне програмне забезпечення. Це дає йому можливість швидко виявляти й сповіщати про підозрілі дії, несанкціонований доступ як внутрішніх, так і зовнішніх користувачів.

1.6 ПІДГОТОВКА СТРАТЕГІЇ З КОМУНІКАЦІЇ

Комунікація є життєво важливим компонентом кожного кроку в реагуванні на інциденти кібербезпеки. Ви хочете контролювати потік зв’язку, щоб забезпечити передачу потрібної інформації в потрібний момент від правильних відправників потрібним одержувачам. Це справедливо як для внутрішнього спілкування, так і для спілкування із зовнішнім світом.

Рекомендуємо координувати всі зовнішні комунікації з представниками юридичної служби та відділу зв'язків з громадськістю.

СПІЛКУВАННЯ ІЗ КИМ?

Тип інциденту та його (потенційний) вплив визначать тип необхідного зв'язку. Наприклад, випадок внутрішнього шахрайства або спроба внутрішнього злому, швидше за все, не вимагають зв'язку зі ЗМІ для розкриття інциденту. З іншого боку, коли персональні дані клієнтів організації витікають, було б гарною ідеєю зв'язатися принаймні з цими клієнтами та Національним органом із захисту даних та підготувати заяву для преси. Крім того, всі комунікації повинні знаходити правильний баланс між прозорістю та захистом. У більшості випадків внутрішня комунікація буде більш прозорою, ніж зовнішня комунікація. Однак навіть для внутрішнього спілкування слід дотримуватися принципу «необхідно знати».

ВИЗНАЧЕННЯ ВНУТРІШНІХ ТА ЗОВНІШНІХ ЗАКОНЕЧНИХ СТОРІН

Під час заходів з реагування на інциденти існуватиме постійна потреба в інформації від багатьох різних зацікавлених сторін. Кожному з них знадобиться різний тип інформації. Складіть власний список потенційних зацікавлених сторін і переконайтеся, що доступна правильна контактна інформація. Зауважте, що організація повинна мати цю контактну інформацію, але не завжди їй потрібно спілкуватися з усіма сторонами.

ХТО? ВНУТРІШНЬО ЗАЦІКАВЛЕНІ СТОРОНИ	ЩО? ТИП ІНФОРМАЦІЇ, ЯКОЇ ПОТРУБУЄ ЗАЦІКАВЛЕНА СТОРОНА
Керівництво	Що впливає? Яка відповідь? Який очікуваний результат і коли робота повернеться в норму?
Бізнес менеджери потраплені під вплив	Коли буде відновлено нормальну роботу?
Співробітники	Що повинен робити працівник? Як довго, як очікується, триватиме така ситуація?

ХТО? ВНУТРІШНЬО ЗАЦІКАВЛЕНІ СТОРОНИ	ЩО? ТИП ІНФОРМАЦІЇ, ЯКОЇ ПОТРУБУЄ ЗАЦІКАВЛЕНА СТОРОНА
Національний орган із захисту даних	Чи було порушення даних? Яких суб'єктів даних це стосується? У деяких випадках існує юридичне зобов'язання зв'язатися з Національним органом із захисту даних (телеком і GDPR).
CCB (Cert.be відділ)	Технічні деталі виявлених доказів
Поліція	Ви бажаєте подати скаргу? Якщо подія спричинила значний вплив і є підозра у злочинному намірі, ви можете повідомити про інцидент до правоохоронних органів. Їм знадобиться юридична та технічна інформація.
Галузеві регулятори	Що за інцидент? Який статус інциденту? У деяких випадках існує юридичний обов'язок зв'язуватися з певними органами влади або галузевим регулятором

Під час заходів з реагування на інциденти існуватиме постійна потреба в інформації від багатьох різних зацікавлених сторін. Кожному з них знадобиться різний тип інформації. Складіть власний список потенційних зацікавлених сторін і переконайтеся, що доступна правильна контактна інформація. Зауважте, що організація повинна мати цю контактну інформацію, але не завжди їй потрібно спілкуватися з усіма сторонами.

Організації повинні пам'ятати, що після того, як сторона буде проінформована, вона запитатиме періодичні оновлення, пов'язані з інцидентом, про який йде мова. Зазвичай немає «одноразового» спілкування, і в розкладі комунікацій слід враховувати ці періодичні оновлення.

ХТО? ВНУТРІШНЬО ЗАЦІКАВЛЕНІ СТОРОНИ	ЩО? ТИП ІНФОРМАЦІЇ, ЯКОЇ ПОТРУБУЄ ЗАЦІКАВЛЕНА СТОРОНА
ЗМІ	Заява про інцидент та його наслідки. Для високопоставлених компаній та/або інцидентів можуть бути залучені ЗМІ. Увага ЗМІ до інциденту з безпекою рідко є бажаною, але іноді може бути неминучою. Увага засобів масової інформації може дозволити вашій організації зайняти активну позицію в повідомленні про інцидент, таким чином показавши вашу відданість і здатність впоратися з інцидентом. У плані комунікації має бути чітко визначено осіб, уповноважених спілкуватися з представниками ЗМІ (як правило, відділи зв'язків з громадськістю або юридичні відділи).
Клієнти	Чи може на них вплинути інцидент кібербезпеки? Їхні (особисті) дані були втрачені чи вкрадені? Чи потенційно вони є основною метою атаки? У деяких випадках існує юридичне зобов'язання зв'язатися з галузевим регулятором
Постачальники	Чи може на них вплинути інцидент кібербезпеки? Чи потенційно вони є основною метою атаки?
Інша (партнерська) група реагування на кібербезпеку	Зв'язок з іншими групами реагування на інциденти може надати технічну допомогу, пропонуючи таким чином швидше вирішення (наприклад, вони, можливо, бачили/обробляли цей тип інциденту раніше). Цей тип зв'язку, як правило, включає технічні деталі виявлених доказів.
інтернет провайдер	Зв'язок з вашим постачальником послуг Інтернету може надати технічну допомогу, пропонуючи таким чином швидше вирішення (наприклад, вони, можливо, бачили/обробляли цей тип інциденту раніше). Цей тип зв'язку, як правило, включає технічні деталі виявлених доказів.

ВПЛИВ ІНЦИДЕНТУ ВИЗНАЧАЄ ЦІЛІ КОМУНІКАЦІЇ

Щоб знати, що і кому повідомити, організація повинна оцінити (потенційний) вплив інциденту кібербезпеки: напр. чи це стосується лише внутрішніх чи зовнішніх зацікавлених сторін? Чи є витік даних? Залежно від цього впливу ваше повідомлення про інциденти кібербезпеки матиме різні цілі, наприклад:

1. **КОМУНІКАЦІЯ, ЩО МАЄ РОЗРІШЕННЯ ТА ЛІКУВАННЯ ІНЦИДЕНТУ**

   Спілкування з іншими внутрішніми командами або сторонніми групами реагування на інциденти

2. **КОМУНІКАЦІЯ НА ВІДПОВІДНОСТІ**

   Повідомлення про інцидент постраждалим клієнтам, зв’язок з галузевими регуляторами

3. **КОМУНІКАЦІЯ, ЯКЕ МАЄ ОБМЕЖЕННЯ РЕПУТАЦІЙНОЇ ШКОДИ**

   Спілкування з клієнтами, партнерами та ЗМІ, а також із внутрішнім персоналом.

НАЯВНІСТЬ ДОСТУПНОСТІ ДО ДЕЯКИХ КАНАЛІВ ЗВ'ЯЗКУ

Інцидент може вплинути на існуючі канали зв’язку (наприклад, зламати системи електронної пошти). Як організація, мають бути доступні альтернативні безпечні канали зв’язку. Доступно кілька методів комунікації, і організація має вибрати метод, найбільш підходящий для конкретного інциденту.

Найкращою практикою, яку використовують багато організацій, є використання номера мосту конференції, який можна налаштувати миттєво. Групу реагування на інцидент та всі зацікавлені сторони слід поінформувати про номери доступу, але не про контрольний номер, необхідний для організації конференції. Зазвичай це робить кризовий менеджер, який відповідає за керування, контроль та організацію кризових викликів.

МОЖЛИВІ МЕТОДИ КОМУНІКАЦІЇ

• Електронна пошта (бажано з використанням PGP для конфіденційності та цілісності зв'язку)

• Веб-сайт (інтранет для співробітників, загальнодоступний веб-сайт,...)

• Телефонні дзвінки

• Особисто (наприклад, щоденні інструктажі)

• Папір (наприклад, розмістити оголошення на дошках оголошень і дверях,

роздати повідомлення на всіх входах)

1.7 КІБЕР СТРАХУВАННЯ

Деякі страховики пропонують індивідуальні страхові поліси, яким завжди передує аналіз ризиків, характерних для даної організації. Цей аналіз дозволяє організації визначити, чи потрібна їй страхування кібербезпеки та в якій мірі. Аналіз ризиків також буде використовуватися страховиком для визначення необхідного покриття. Фактори, які враховуються:

- бізнес-експозиція: високі технології з ексклюзивним виробничим процесом та поглибленими дослідженнями та розробками
- тип торговельної мережі: електронна комерція
- кількість і тип даних (критичні чи ні), наявність правової бази.

Компенсація виплачується понад перевищення, узгоджене зі страхувальником. Страхові суми на випадок та/або страховий рік завжди визначаються відповідно до потреб компанії та можливостей страхової компанії.

Чому кіберстрахування?

Додана вартість кіберстрахування збільшується, якщо ви залежите від цифрових систем та інформації в цих системах для ваших бізнес-операцій. Іншими причинами для оформлення кіберстрахування можуть бути те, що клієнти або постачальники вашої компанії просять про це, оскільки ви ризикуєте збільшувати. Наприклад, завдяки продуктам чи послугам, які ви продаєте, або тому, що у вас є певні знання (інтелектуальна власність, наприклад дизайн).Ризики, які ви хочете застрахувати, — це ризики, які мають значний вплив, але трапляються нечасто. У фізичному світі вогонь або крадіжка будуть включені. Пожежа або крадіжка, як правило, нечасті. Але коли це відбувається, шкода може бути великою, а витрати зазвичай швидко збільшуються. Тому завжди думайте, чи можете і хочете ви самі нести ризик, чи ні. Якщо ви не можете або не хочете нести відповідальність, кіберстрахування може мати додаткову цінність для вашої компанії.

Які запитання я повинен задати про кіберстрахування?

Щоб допомогти вам визначити, оформляти кіберстрахування чи ні, ось кілька конкретних запитань:

1. Наскільки ваша компанія піддається цифровому ризику? Щоб відповісти на це запитання, ви можете скористатися інформацією від вашої галузевої асоціації, банку чи радника.
2. Які можливі наслідки та витрати кіберінциденту і чи можете чи хочете ви самі їх нести?
3. Перевірте, чи забезпечують ваші поточні страхові поліси, наприклад, страхування відповідальності , будівлі , товарів або інвентарю , на випадок цифрового інциденту. Зверніть особливу увагу на перекриття між страховими полісами. Додаткову інформацію про це можна знайти в умовах вашого полісу у страхової компанії, страхового брокера або консультанта.
4. Не думайте, що ваші існуючі страхові поліси також автоматично покривають збитки, спричинені кіберінцидентами. Додаткову інформацію про це можна знайти в умовах вашого полісу у страхової компанії, страхового брокера або консультанта.
5. Ринок кіберстрахування розвивається. У результаті поліси кіберстрахування не є ідентичними і можуть відрізнятися для кожного модуля, покриття та премії.
6. Премії та покриття мають обмеження. Які обмеження існують для покриття? Чи існують граничні суми, часові інтервали чи обидва? Чи відповідають вони вашому профілю ризику?
7. Скільки коштує страхування і чи пропорційна премія до покриття та ризиків, які ви несете у своїй компанії?

Що покриває кіберстрахування?

Наслідки кіберінциденту можуть мати різні форми. Як уже згадувалося, важливо визначити, що ви хочете застрахувати і який ризик ви можете і хочетенести. Витрати на інцидент можуть швидко
збільшуватися. Кіберстрахування може покривати:

- Прямі витрати на кіберінцидент: включаючи ремонт або заміну апаратного та програмного забезпечення, відновлення даних, отримання інформації та відновлення адміністрування. Прямі витрати включають найм спеціалістів для ремонту та втрату (виробничих) годин чи обороту.
- Непрямі витрати: включаючи шкоду репутації, штрафи від регуляторів (наприклад, штрафи GDPR), компенсації потерпілим.
- Втрата даних, відновлення та відтворення

- Припинення діяльності/втрата доходу через порушення
- Втрата перерахованих коштів
- Комп'ютерне шахрайство
- Кібер-вимагання

Страховики також можуть запропонувати послуги, пов’язані з кіберінцидентами, такі як:

- Обізнаність, знання та навички для підприємця або персоналу. Наприклад, пропонуючи підтримку в онлайн-навчанні.
- Підтримка при інцидентах: наприклад, цілодобовий центр екстреної допомоги та технічна підтримка.
- Юридична підтримка: наприклад, у разі порушення даних відповідно до GDPR.
- Криміналістичні служби: з'ясування, хто стоїть за нападом.

Важлива примітка. Страхування від помилок і упущень не є кіберстрахуванням і не може замінити належне кіберстрахування, навіть якщо поліс E&O містить технологічну помилку.

Якщо хакери викривають або викрадають особисту інформацію, таку як номери соціального страхування, номер водійського посвідчення (у деяких штатах), адресу та інформацію про банківський рахунок, поліс страхування кібер-відповідальності оплачує:

- Витрати на повідомлення: ці витрати є значними, оскільки компанія несе тягар як виявлення потенційних жертв, що вимагає внутрішнього розслідування, так і надання сповіщень, які розумно розраховані для фактичного повідомлення.
- Моніторинг кредиту. Фактично, ваш поліс кіберстрахування оплачує страхові поліси жертв. Регулятори зазвичай диктують вид кредитного моніторингу, який необхідно забезпечити, і можна впевнено ставити, що вони не будуть задоволені найдешевшим доступним захистом.
- Відшкодування цивільно-правових збитків: більшість із цих позовів про відповідальність є груповими позовами, із як мінімум сотнями тисяч доларів відшкодування збитків, навіть для дуже маленької компанії.
- Комп’ютерна криміналістична експертиза: це покриває витрати на найм консультантів із комп’ютерної криміналістичної експертизи, які працюють під керівництвом ваших адвокатів, щоб визначити, чи відбулося порушення даних, локалізувати й запобігти подальшому пошкодженню, а також з’ясувати причину та масштаби порушення.
- Репутаційна шкода: порушення даних можуть мати серйозні наслідки для PR для будь-якого бізнесу. Бажана політика допоможе вам впоратися з потенційними наслідками, покриваючи збитки, спричинені відразою до бренду через кіберінцидент протягом певного часу після

порушення. Це також може допомогти пом’якшити потенційні витрати, оплачуючи експертів з управління PR.

Постачальники кіберстрахування також зобов’язані захищати страхувальників від пов’язаних адміністративних дій або судових позовів про відповідальність. Наприклад, кіберстрахування пропонує покриття відповідальності за конфіденційність. Це покриття важливе для більшості компаній, особливо тих, які зберігають конфіденційну інформацію про клієнтів і співробітників у своїх мережах. Порушення, які розкривають таку інформацію, не тільки ставлять під загрозу постраждалих, але й можуть поставити ваш бізнес до судових позовів від жертв таких кіберінцидентів. Крім того, він забезпечить покриття у випадках, коли ви, ймовірно, порушили закони про конфіденційність.

Крім того, більшість політик також надають ресурси, які допомагають страхувальникам розробити економічно ефективний і надійний протокол безпеки та шифрування даних. Щоб ще більше мінімізувати ризик відповідальності .

Щоб отримати право на страхування, деякі страховики спочатку хочуть знати, чи вжили ви заходів безпеки. Іноді страховики просять вас виконати сканування ризиків для вашої компанії. Також можливо, що страховик вимагає певних налаштувань, наприклад наявність антивірусного сканера або брандмауера. Те, чи вимагаються ці вимоги, залежить від страховика та буде частиною умов полісу.

Що не покривається?

Як і більшість покриттів, існують певні винятки, які кіберполітика зазвичай не поширюється.

Політика не відповідатиме, якщо на вас пред’являть позов за будь-які потенційні вразливості ваших систем до того, як станеться порушення.

Зокрема, поліси кіберстрахування, як правило, не відшкодовують вам майбутні прибутки, втрачені через кібератаку або злом даних.

Якщо ви боїтеся втрат через крадіжку вашої інтелектуальної власності, вам доведеться звернути увагу на спеціально розроблений поліс страхування інтелектуальної власності. Крім того, звинувачення в тому, що патенти власника поліса порушують патенти третьої сторони, також не будуть охоплюватися.

Якщо агент іноземної держави спричиняє порушення, у покритті може бути відмовлено відповідно до актів виключення війни.

Крім того, вартість покращення ваших систем безпеки та технологій після атаки не буде включена в більшість політик (обов'язково прочитайте наші посібники про те, як реагувати на кібератаки та як відновлюватися після кібератаки).

Вирішуючи питання про те, чи будете ви захищені від загроз, пов'язаних із кіберпрограмою, дуже важливо зрозуміти концепцію «тихого кібер». Багато традиційних страхових полісів, зокрема страхування загальної відповідальності (CGL), не були розроблені з урахуванням кіберризиків. Це означає, що вони не мають точної мови, неявно включаючи чи виключаючи кібервикриття. Однак на практиці це означає, що політика CGL зазвичай не покриває кібер-відповідальність, а якщо і покриває, то покриття буде в кращому випадку мінімальним.

Також важливо зазначити, що атаки соціальної інженерії можна вважати окремим випадком. Соціальна інженерія відноситься до атак, які покладаються на психологічні маніпуляції для отримання доступу до конфіденційної інформації або коштів. Жертви, які виконують інструкції з шахрайських листів або дзвінків, не вважаються зломом комп'ютерної системи. Тому до кіберстрахування необхідно додати спеціальний поліс соціальної інженерії.

Навіщо це Вам потрібно?

Не дивно, що кіберстрахування з'явилося на страховій сцені нещодавно в результаті того, що інші традиційні поліси страхування бізнесу просто не були створені для покриття видів ризиків , які найчастіше пов'язані з кіберстрахуванням.

Тому багато експертів зі страхування стверджують, що поліси кіберстрахування все ще знаходяться в зародковому стані, і потрібно багато попрацювати, коли справа доходить до стандартизації покриття та забезпечення того, щоб страхові компанії могли задовольнити потреби сучасного бізнесу. Мало того, освіта важлива для того, щоб підприємства розуміли загрозу кібератак і серйозність цих типів загроз.

У недавньому звіті страховиків Hiscox стверджується, що сім з 10 компаній не мають якісної стратегії кібербезпеки.

Однак, безсумнівно, що простір кіберстрахування буде продовжувати швидко розвиватися, а пропозиції, безсумнівно, будуть розширюватися та адаптуватися. Крім того, як і у випадку з більшістю інших видів страхових пропозицій, поліси кіберстрахування розвиваються в напрямку більш галузевих рішень і стають менш загальними.

Висновки до першого розділу: Заходи кібербезпеки призначені для захисту людей, власності, систем, мереж, даних та пов’язаних ресурсів від загроз. Ці заходи включають запобігання, виявлення, реагування на інциденти кібербезпеки та відновлення після них. Активи ідентифікуються, а загрози, вразливі місця та ризики оцінюються до розробки та впровадження заходів кібербезпеки. Дослідження безпеки можуть допомогти в розробці нових і вдосконаленні існуючих заходів кібербезпеки. Заходи кібербезпеки часто не враховують людей, які їх використовують. Люди можуть як сприяти, так і перешкоджати зусиллям з кібербезпеки. З цієї причини необхідно створити ефективні заходи та системи кібербезпеки з урахуванням тих, хто їх використовуватиме.

Розділ 2 ВИЯВЛЕННЯ ТА ІДЕНТІФІКАЦІЯ ПОТЕНЦІЙНИХ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ

2.1 КАТЕГОРІЇ ІНЦИДЕНТІВ

ВИЗНАЧЕННЯ ІНЦИДЕНТУ КІБЕРБЕЗПЕКИ ТА ПОВ’ЯЗАНІ З НИМ ТЕРМІНИ

Для початку доцільно визначити «інцидент кібербезпеки» та пов’язані з ним терміни у вашій організації. Це зробить комунікацію про інцидент набагато ефективнішою. Ви можете знайти натхнення для цих визначень у попередньому розділі цього посібника в розділі «Основні принципи та ключові визначення». Наприклад, ви повинні вирішити, коли подія кібербезпеки стане інцидентом кібербезпеки для вашої організації. Іншими словами, які види подій кібербезпеки можуть мати негативний вплив на діяльність вашої організації?

ВИЗНАЧЕННЯ МОЖЛИВИХ КАТЕГОРІЙ ІНЦЕНТІВ КІБЕРБЕЗПЕКИ

Щоб мати можливість виявляти та ідентифікувати інциденти кібербезпеки, ви повинні мати принаймні уявлення про те, що ви шукаєте. Тому мати список категорій інцидентів кібербезпеки, які найбільше можуть вразити вашу організацію, не є розкішшю. Крім того, коли ви виявляєте кіберподію, часто важко зрозуміти, наскільки серйозними будуть наслідки з самого початку. Однак це не змінює того факту, що вам потрібно продовжити. Категорії

інцидентів дозволяють визначити пріоритети кіберподій і приймати відповідні рішення. Цей розділ пропонує типологію низки інцидентів кібербезпеки. Мета полягає не в тому, щоб надати «остатковий» огляд усіх типів інцидентів, а просто дати вам уявлення про найбільш поширені типи інцидентів. Інциденти можуть належати до кількох категорій.

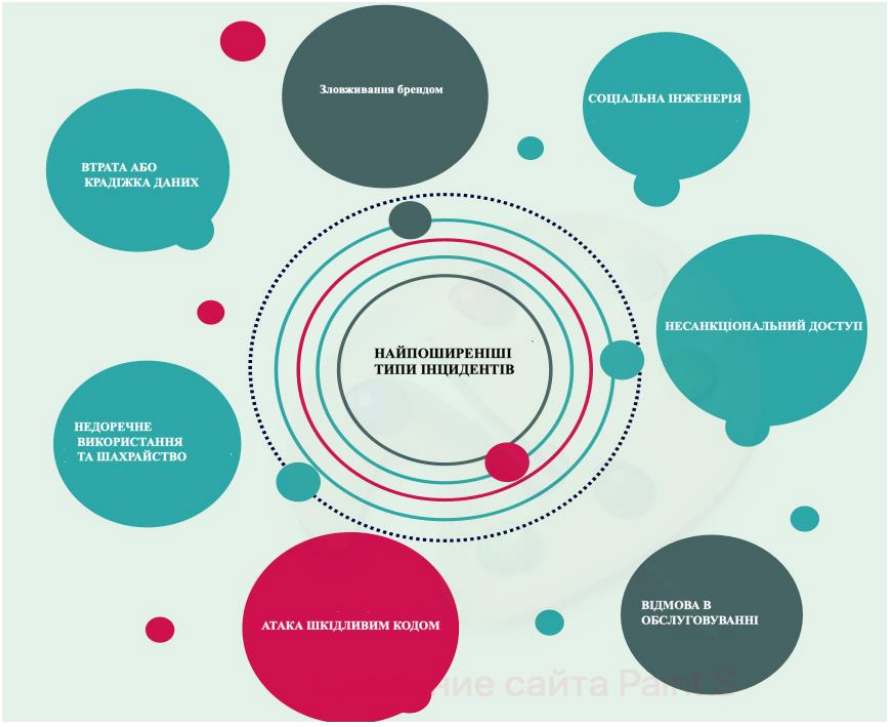
Класифікування інцидентів інформаційної безпеки, потрапивших до зловмисника

Однією з найбільших помилок традиційної інформаційної безпеки є припущення, що ви знаєте, яким шляхом зловмисник піде через вашу мережу. Наприклад, зловмисники рідко проникають через ваші вхідні двері або в цьому контексті брандмауер вашого шлюзу. Але кожна атака, як правило, працює за певною схемою, або тим, що Lockheed Martin назвала «ланцюжком кібер-вбивства». «Ланцюжок кібер-знищення» — це послідовність етапів, необхідних зловмиснику для успішного проникнення в мережу та вилучення з неї даних. Кожен етап демонструє конкретну мету на шляху нападника. Розробка плану моніторингу та реагування на основі моделі ланцюга кібер-вбивства є ефективним методом, оскільки він фокусується на тому, як відбуваються фактичні атаки.

USB-флешка ЧИ USB-шпигун?

У 2013 році Росія приймала зустріч лідерів G20. Наприкінці цього заходу всі учасники, серед них і Герман Ван Ромпей, отримали нагороди

подарунковий пакет, що містить USB-накопичувач і пристрій для зарядки мобільного телефону. Хоча Кремль завжди заперечував це, повідомлялося, що обидва пристрої можуть таємно завантажувати інформацію, таку як електронна пошта, текстові повідомлення та телефонні дзвінки з ноутбуків і телефонів.



CRYPTOLOCKER ТАКОЖ МОЖЕ ШИФРОВАТИ ВАШУ РЕЗЕРВНУ КОПІЮ

Компанія отримує електронний лист із вкладеним рахунком-фактурою, схожим на рахунок-фактуру від своїх постачальників. Бухгалтер компанії натискає вкладення, і через кілька секунд на його екрані з'являється повідомлення: «Вся ваша інформація зашифрована! Якщо ви хочете, щоб ключ розблокував шифрування, ви повинні заплатити мені 1000 біткойнів». Компанія не хоче платити кіберзлочинцям. Зрештою, немає ніякої гарантії, що вони дійсно повернуть втрачені дані після отримання викупу. Щоб відновити свої дані, компанія вирішує відновити їх із резервної копії. Коли компанія хоче це зробити, співробітники помічають, що оскільки резервна копія була підключена до системи, вона також була зашифрована...

У разі інциденту безпеки головною метою є відновлення нормального рівня зведення до мінімуму функціонування систем або послуг щодо їх якості та доступності

втрат якомога більше.

Процес можливого відновлення цього рівня нормальної активності разом із діями

пом’якшення можливих наслідків інциденту, а також процес отримання та аналізуючи докази, складають комплекс дій, які необхідно здійснити в
подія інциденту безпеки.
Для ідентифікації інциденту безпеки, визначення його масштабу та систем, на які він вплинув, можуть бути докази
збираються різними способами, що визначаються характером і типом інциденту. Одна з основних
Методи — це аналіз журналів та інших джерел інформації для виявлення аномалій. Такий
джерела включають:

- Антивірусні консолі.
- Виявлення вторгнень і вторгнення

Системи профілактики (IDS/IPS).

- Інформація та події безпеки

Попередження керування (SIEM).

- Перевірка журналів аудиту для виявлення спроб

при несанкціонованому доступі.

- Журнали з'єднань, заблокованих брандмауерами.
- Журнали з'єднань, здійснені корпоративними

довірені особи.

- Журнали інструментів запобігання втраті даних (DLP).
- Блокування облікових записів користувачів або інше

аномалії, повідомлені в CAU або які
передбачають такі ризики, як втрата USB-пристроїв або
ноутбуки.

- Раптове та надмірне використання пам’яті або

простір на диску сервера.

- Аномалії дорожнього руху, такі як споживання

пік у незвичайний час.

- Дампи мережі, наприклад, через порт

дзеркальне відображення, що може дозволити підтвердження
про підозрюваний інцидент.
Виявлення цих типів аномалій дозволяє ідентифікувати можливий інцидент безпеки,
разом з його природою та масштабами. Якщо будь-який із цих записів містить аномалії, докладніше
необхідно провести аналіз, щоб визначити, чи дійсно інцидент стався.
Такий аналіз може здійснюватися, наприклад, шляхом виявлення шкідливого мережевого трафіку,

визначення ураженої інфраструктури, адреси хоста та призначення, використовувані значення портів,
TTL, протоколи тощо.
Ці дії допоможуть визначити, чи дійсно був інцидент безпеки та його характер.
На системному рівні способи з’ясувати, чи мав інцидент наслідки, включають:

- Незвичайний або особливо привілейований користувач
рахунки.
- Приховані файли або файли, які здаються підозрілими
через їх розмір, назву файлу чи розташування,
можливо, що вказує на витік даних або журналів
з боку шкідливого програмного забезпечення.
- Файли з незвичайними дозволами, із SUID
або GUID, з незвичайними шляхами, файлами-сиротами,
що вказує на можливість якогось роду
вторгнення або руткіт.
- Підозрілі записи в реєстрі, переважно в
випадок систем Windows із шкідливими програмами
інфекції, це один з основних шляхів
шкідливе програмне забезпечення гарантує його стійкість у
інфікована система.
- Незвичайні процеси та послуги, не тільки
служби прослуховування, але ті з
підключення до портів або хостів, які є
дивні, незвичайні або які з’являються на
чорні списки серверів командування та керування
використовується ботнетами.
- Надмірне завантаження диска або пам’яті, що
може бути спровоковано інцидентом безпеки
із шкідливим програмним забезпеченням, відмовою в обслуговуванні або
вторгнення.
- Сеанси на пристрої, відкритому іншими
пристроїв, аномалії таблиці ARP, незвич
спільні папки, підвищена кількість
аномальні активні TCP-з'єднання, які
може свідчити про атаку відмови в обслуговуванні.
- У випадку обладнання користувача або мобільного
пристроїв, наведене нижче може вказувати на деякі
тип системної інфекції, серед іншого:
аномальний спільний доступ до програм,
спливаючі вікна навігатора, повільно

підключення, перезавантаження або програми, які
закрити без попередження.

- Заплановані завдання або незвичайна діяльність у журналі
файли, що може свідчити про ненормальний
функції системи або спроби вторгнення
дана послуга через, наприклад, грубу
сила.
- Сповіщення корпоративної антивірусної платформи,

або інші інструменти, які зазвичай використовуються для ідентифікації

руткіти, щоб виконати перевірку цілісності

файли, сигнатури двійкових файлів тощо. Встановлення

такі інструменти на можливо заражених системах ad

hoc не рекомендується, оскільки доступ

дати можуть бути змінені, а докази втрачені.

На додаток до цих заходів для виявлення інцидентів безпеки в уражених пристроях, це не можна виключати

що інцидент можна ідентифікувати за допомогою зовнішнього джерела даних, звіту CERT або звіту

від іншого органу або від користувача, який не є для організації, тощо.

2.2 МЕТОДИ ВИЗНАЧЕННЯ ІНЦИДЕНТА

ПЕРСОНАЛ ОРГАНІЗАЦІЇ МАЄ ПОТЕНЦІАЛ

Люди часто вважаються найслабшою ланкою, коли йдеться про кібербезпеку. Однак вони також мають найбільший потенціал, щоб допомогти організації виявляти та ідентифікувати інциденти кібербезпеки. Переконайтеся, що кожен член вашої організації знає про ризики кібербезпеки та про роль, яку вони можуть зіграти у їх виявленні. Перетворіть їх у свій людський брандмауер! Кожен член вашої організації повинен знати, як повідомити про щось

ненормальне на своєму комп’ютері чи мобільному пристрої. Переконайтеся, що контактні дані для цього легко доступні та що з цією особою легко зв’язатися.

Щоб організувати звітування про інциденти персоналом (та іншими партнерами), зробіть доступним наступне:

• Номер телефону для повідомлення про надзвичайні ситуації

• Адреса електронної пошти для неформального повідомлення про інцидент

• Веб-форма для офіційного звіту про інциденти

ТЕХНОЛОГІЯ ТА ЗАХИСТ КІНЦІВНИХ ТОЧОК

Технологія

Технологія є одним з основних факторів, коли мова йде про виявлення, розслідування, ліквідацію та відновлення інцидентів. Коли інцидент стався, тимчасове розгортання технології все ще можливе, але ваше розслідування часто обмежується поточними подіями. Застосування правильної технології на етапі підготовки дозволить вам отримати вичерпну картину поточних і минулих подій. Це дає вашій організації кращі шанси відстежити інцидент до його коріння.

Чому безпека кінцевої точки важлива

Платформа захисту кінцевих точок є важливою частиною кібербезпеки підприємства з кількох причин. Перш за все, у сучасному діловому світі дані є найціннішим активом компанії, і втрата цих даних або доступу до них може поставити весь бізнес під загрозу неплатоспроможності. Підприємствам довелося боротися не тільки зі зростанням кількості кінцевих точок, але й зі зростанням кількості типів кінцевих точок. Ці фактори самі по собі ускладнюють безпеку кінцевих точок підприємства, але до них посилюється віддалена робота та політика BYOD, що робить безпеку периметра все більш недостатньою та створює вразливості. Ландшафт загроз також стає складнішим: хакери завжди придумують нові способи отримати доступ,

викрасти інформацію або маніпулювати співробітниками, щоб вони розповсюджували конфіденційну інформацію

Захист кінцевої точки

Кінцева точка – це пристрій, який під'єднано до мережі вашої організації, наприклад, ноутбуки, смартфони тощо. Кожен із цих пристроїв є потенційною точкою входу для кіберзлочинців. Тому важливо, щоб усі ці пристрої були належним чином захищені.

Як працює захист кінцевої точки

Безпека кінцевої точки — це практика захисту даних і робочих процесів, пов'язаних з окремими пристроями, які підключаються до вашої мережі. Платформи захисту кінцевих точок (EPP) працюють шляхом перевірки файлів, коли вони потрапляють в мережу. Сучасні EPP використовують потужність хмари для зберігання постійно зростаючої бази даних про загрози, звільняючи кінцеві точки від роздуття, пов'язаного із локальним зберіганням усієї цієї інформації та обслуговуванням, необхідним для оновлення цих баз даних. Доступ до цих даних у хмарі також забезпечує більшу швидкість і масштабованість.

EPP надає системним адміністраторам централізовану консоль, яка встановлюється на мережевий шлюз або сервер і дозволяє фахівцям з кібербезпеки віддалено контролювати безпеку кожного пристрою. Клієнтське програмне забезпечення потім призначається кожній кінцевій точці — воно може поставлятися як SaaS і керуватися віддалено, або його можна встановити безпосередньо на пристрої. Після налаштування кінцевої точки клієнтське програмне забезпечення може надсилати оновлення на кінцеві точки, коли це необхідно, автентифікувати спроби входу з кожного пристрою та адмініструвати корпоративні політики з одного місця. EPP захищають кінцеві точки за допомогою контролю програм, який блокує використання небезпечних або неавторизованих програм, а також за допомогою шифрування, яке допомагає запобігти втраті даних.

Коли EPP налаштовано, він може швидко виявляти зловмисне програмне забезпечення та інші загрози. Деякі рішення також включають компонент виявлення та відповіді кінцевої точки (EDR). Можливості EDR дозволяють виявляти більш розширені загрози, такі як поліморфні атаки, безфайлові шкідливі програми та атаки нульового дня. Використовуючи

безперервний моніторинг, рішення EDR може запропонувати кращу видимість і різноманітні варіанти реагування.
Рішення EPP доступні в локальних або хмарних моделях. Хоча хмарні продукти є більш масштабованими і можуть легше інтегруватися з вашою поточною архітектурою, певні нормативні правила/правила відповідності можуть вимагати локальної безпеки.

Що вважається кінцевою точкою?

Кінцеві точки можуть варіюватися від більш поширених пристроїв, таких як:

- Таблетки
- Мобільні пристрої
- Розумні годинники
- Принтери
- Сервери
- Банкомати
- Медичні прилади

Якщо пристрій підключено до мережі, він вважається кінцевою точкою. Зі зростанням популярності BYOD (принесіть свій власний пристрій) та IoT (Інтернет речей), кількість окремих пристроїв, підключених до мережі організації, може швидко досягти десятків (і сотень) тисяч.

Оскільки кінцеві точки (особливо мобільні та віддалені пристрої) є улюбленою мішенню зловмисників, вони є точками входу для загроз і шкідливих програм. Мобільні кінцеві пристрої стали набагато більше, ніж просто пристрої Android та iPhone — згадайте новітні носимі годинники, розумні пристрої, цифрові помічники з голосовим керуванням та інші розумні пристрої з підтримкою IoT. Тепер ми маємо підключені до мережі датчики в наших автомобілях, літаках, лікарнях і навіть на бурових установках нафтових платформ. Оскільки різні типи кінцевих точок еволюціонували та розширювалися, рішення безпеки, які їх захищають, також повинні були адаптуватися.

Компоненти безпеки кінцевої точки

Як правило, програмне забезпечення безпеки кінцевої точки включає такі ключові компоненти:

- Класифікація машинного навчання для виявлення загроз нульового дня майже в реальному часі

- Розширений захист від шкідливих програм і вірусів для захисту, виявлення та виправлення зловмисного програмного забезпечення на кількох кінцевих пристроях та операційних системах
- Проактивна веб-безпека для безпечного перегляду в Інтернеті
- Класифікація даних і запобігання втраті даних для запобігання втрати та ексфільтрації даних
- Вбудований брандмауер для блокування ворожих мережевих атак
- Шлюз електронної пошти для блокування спроб фішингу та соціальної інженерії, спрямованих на ваших співробітників
- Криміналістична експертиза загроз, що дозволяє адміністраторам швидко ізолювати інфекції
- Захист від внутрішніх загроз для захисту від ненавмисних і зловмисних дій
- Централізована платформа керування кінцевими точками для покращення видимості та спрощення операцій
- Шифрування кінцевої точки, електронної пошти та диска для запобігання ексфільтрації даних

Платформи захисту кінцевих точок проти традиційних антивірусів

Платформи захисту кінцевих точок (EPP) і традиційні антивірусні рішення відрізняються в деяких ключових аспектах.

- **Безпека кінцевої точки проти безпеки мережі:** антивірусні програми розроблені для захисту однієї кінцевої точки, забезпечуючи видимість лише цієї кінцевої точки, у багатьох випадках лише з цієї кінцевої точки. Проте програмне забезпечення безпеки кінцевих точок розглядає мережу підприємства в цілому і може запропонувати видимість усіх підключених кінцевих точок з одного місця.

- **Адміністрування:** застарілі антивірусні рішення покладалися на те, що користувач вручну оновлює бази даних або дозволить оновлення у заздалегідь встановлений час. EPP пропонують взаємопов’язану безпеку, яка перекладає обов’язки адміністрування на корпоративну команду IT або кібербезпеки.

- **Захист:** традиційні антивірусні рішення використовували виявлення вірусів на основі сигнатур. Це означало, що якщо ваш бізнес був Patient Zero, або якщо ваші користувачі нещодавно не оновлювали антивірусну програму, ви все ще можете бути в зоні ризику. Використовуючи хмару, сучасні рішення EPP автоматично оновлюються. А за допомогою таких

технологій, як поведінковий аналіз, на основі підозрілої поведінки можна виявити раніше невідомі загрози.

Захист безпеки кінцевих точок підприємства	**Захист безпеки кінцевих точок споживача**
Захист безпеки кінцевих точок споживача	Потрібний для керування лише невеликою кількістю однокористувацьких кінцевих точок
Краще керувати різноманітними колекціями кінцевих точок	Потрібний для керування лише невеликою кількістю однокористувацьких кінцевих точок
Програмне забезпечення центрального центру управління	управління Кінцеві точки індивідуально налаштовані та налаштовані
Можливості віддаленого адміністрування	Рідко вимагає віддаленого керування
Віддалено налаштовує захист кінцевої точки на пристроях	Налаштовує захист кінцевої точки безпосередньо на пристрої
Розгортає виправлення на всіх відповідних кінцевих точках	Користувач вмикає автоматичне оновлення для кожного пристрою
Потрібні модифіковані дозволи	Використовує адміністративні дозволи
Можливість контролювати пристрої, активність та поведінку співробітників	Діяльність і поведінка обмежені лише одним користувачем

ІНСТРУМЕНТ ДЕТЕКЦІЇ

Кожен засіб виявлення (наприклад, IDS) має конкретну мету і може здійснювати моніторинг з іншої точки зору: на основі мережі або хоста. Враховуючи різноманітність різних загроз, інструменти повинні використовуватися та бути налаштовані на правильні вхідні дані.

З точки зору мережі

Хорошим початком було б впровадження системи запобігання вторгненню, такої як датчик мережі Snort IDS, на висхідній лінії Інтернету. Крім того,

багато організацій не знають, що вони вже мають багато інформації, яку можна використати для виявлення інциденту. Це може бути у формі:

- журнали доступу до серверів і пристроїв;
- операційні журнали з систем (наприклад, створення процесу); • журнали політики брандмауера.

Ці дані можна використовувати для створення правил і тенденцій, які допомагають виявляти неочікуваний або недійсний трафік (наприклад, трафік на незвичайні веб-сайти, спроби входу неіснуючих користувачів тощо).

Які варіанти зловмисного програмного забезпечення є доступними?

Існує багато способів, якими адміністратори мережі можуть вирішити ці проблеми зловмисного програмного забезпечення, деякі з яких включають:

- Встановлення **антивірусів та антивірусних** рішень для боротьби із загрозами
- Створення **технологічної обізнаності** серед користувачів мережі, щоб запобігти витоку даних та крадіжці – навмисно чи ні
- Впровадження та **виконання політики , забезпечення фізичної безпеки** апаратних пристроїв
- Регулярне **оновлення та виправлення** операційної системи та прикладного програмного забезпечення

Але якщо ви вжили всіх цих заходів захисту, це ще не означатиме, що ваша робота виконана. Вам потрібно постійно контролювати свою мережу, а також стратегію захисту, яка її захищає. Вам потрібно буде стежити за ознаками зовнішніх загроз і лазівок, які можуть відкритися. У разі неминучої загрози вам потрібно розробити ефективну стратегію захисту на основі аналізу в реальному часі даних про поведінку, зібраних з вашої мережі.

Що таке інструмент SEM?

Щоб зрозуміти інструмент, ми повинні переконатися, що ми розуміємо, що таке керування подіями безпеки, для початку.
Управління подіями безпеки — це сфера безпеки комп’ютерів і мережі, яка обробляє процес збору, моніторингу та звітування про події безпеки в програмному забезпеченні, системі або мережах.
Таким чином, інструмент SEM – це програма, яка відстежує дані системних подій (зазвичай зберігаються в журналах подій), витягує з них інформацію,

співвідносить або перетворює її в корисні поради та представляє її кому б то не було. Він робить це за допомогою бажаного способу доставки сповіщень або сповіщень, а також з наміром вжити подальших дій для усунення підозрілих чи шкідливих проблем, про які повідомляється.
Джерелом зареєстрованих даних можуть бути пристрої безпеки, такі як брандмауери, проксі-сервери, системи виявлення вторгнень (програмне забезпечення IDS , NIDS , HIDS тощо), а також комутатори або маршрутизатори.

SIM проти SEM проти SIEM

У цей момент ми подумали, що має сенс пролити світло на ці три тісно пов’язані терміни:

- **SIM (управління інформацією про безпеку):** це програма, яка автоматизує збір даних журналу подій з різних пристроїв безпеки та адміністрування, знайдених у мережі. Це продукт безпеки, який в основному використовується для довготривалого зберігання даних, які потім можуть бути використані для створення спеціальних звітів.
- **SEM (управління подіями безпеки):** коли справа доходить до цих систем безпеки, все відбувається в режимі реального часу, оскільки воно відстежує події, стандартизує введення даних, оновлює інформаційні панелі та надсилає сповіщення чи сповіщення.
- **SIEM (інформація про безпеку та управління подіями):** ці системи безпеки надають послуги як SIM-карт, так і SEM – вони роблять все: від збору даних до криміналістичного аналізу та звітності.

Слід зазначити, що SEM і SEIM використовуються як взаємозамінні, і обидва можуть бути у формі програмних рішень, апаратних пристроїв або послуг SaaS.

Переваги використання інструменту SEM для виявлення та аналізу шкідливих програм

Однією з ключових переваг використання інструменту SEM є те, що він є оптимальним рішенням головоломки «витрати проти досвіду». Ось пояснення:

Малі підприємства не можуть дозволити собі витрачати багато на свою IT-інфраструктуру, не кажучи вже про команду конкурентоспроможних

технічних гуру на своїй зарплаті. І все ж, 43% малого та середнього бізнесу є мішенню, коли справа доходить до злому та злому даних.

Усе це означає, що **SEM стає оптимальним рішенням, оскільки надає послуги команди експертів із мережевої безпеки за частковою ціною, необхідною для того, щоб вони були на борту постійно** . Тому що, як тільки він налаштований правильно, він стає цілодобовою системою захисту, яка ретельно перевіряє кожну зареєстровану подію-тригер і чекає відповідного сповіщення або відповіді.

Озброївшись інструментом SEM, ви зможете подбати про:

- **Безпека** – відстеження та обробка шкідливих програм
- **Дотримання вимог** – аудит і звітність стають легкими
- **Усунення несправностей** – тестування та підтримка мережі та пристроїв легше за допомогою журналів
- **Криміналістичний аналіз** – зареєстровані дані можуть дати вирішальні докази та зрозуміти, що сталося
- **Керування** журналами – отримання та зберігання даних журналів відбувається автоматично

Функції, які створюють хороший інструмент для керування подіями безпеки

Шукаючи гідний інструмент SEM, ви можете переконатися, що вони включені у ваш вибір:

- **Реєстрація подій –** ...очевидно!
- **Інтелект** – він повинен бути достатньо розумним, щоб інтерпретувати зареєстровані події. Він повинен мати можливість, принаймні, виявляти основні підозрілі дії прямо з коробки з шаблонами та конфігураціями варіантів використання за замовчуванням.
- **Гнучкість** – можливість як структурованого, так і неструктурованого пошуку в журналах і даних.
- **Відповідність** – мати можливість надавати сповіщення правильного типу, у потрібний час, з потрібних причин чи підозр, а також правильному користувачеві чи адміністратору.
- **Безмежні межі** – еластична здатність відповідати всім запитам користувачів, використовуючи будь-які та всі доступні дані для створення чітких, стислих, точних і зрозумілих звітів.

- **Сумісність** – можливість інтеграції з якомога більшою кількістю апаратних і програмних рішень для легкої безперебійної інтеграції в широку мережу.
- **Хмарні можливості** – це епоха хмарних обчислень, і ця технологія продовжує широко використовуватися; це робить критичним, щоб ваше нове рішення SEM також було сумісним.

З точки зору господаря

Антивірусних рішень недостатньо, щоб відбити розширені атаки на кінцеві точки. Багато зловмисних програм сьогодні є поліморфними (вони змінюються залежно від поведінки хоста), що ускладнює їх виявлення на основі статичних сигнатур класичних антивірусів. Розширені засоби захисту кінцевих точок досліджують підозрілу поведінку і, таким чином, можуть бути більш ефективними в багатьох випадках.

Однак це не означає, що антивірусні рішення не слід розгортати. Навпаки, антивірус необхідний для захисту більшості загальновизнаних загроз.

Застереження: Щоб уникнути шкідливого коду, оновлюйте своє програмне забезпечення, антивірусні сканери тощо! Регулярно оновлюйте програмне забезпечення або встановлюйте виправлення, коли вони доступні.

Не використовуйте непідтримувані версії програмного забезпечення, такі як Windows XP і Windows 2003. Непідтримуване означає, що програмне забезпечення більше не оновлюється, і ваш комп’ютер більше не захищений від нових, відомих шкідливих програм.

2.3 ЗАВДАННЯ РЕАЛЬНОГО ІНЦИДЕНТУ: СТРИМУВАННЯ, ВИДАЛЕННЯ ТА ВІДНОВЛЕННЯ

СТВОРЕННЯ ІНЦИДЕНТУ З КІБЕРБЕЗПЕКИ

КОМАНДА ВІДПОВІДАННЯ

Коли виявляється фактичний інцидент, дуже важливо швидко оцінити ризики, щоб вжити правильних заходів. Менеджера з інцидентів кібербезпеки слід негайно повідомити та скликати нараду групи реагування на інциденти кібербезпеки, якщо така є у вашій організації. Менеджер з інцидентів із

кібербезпеки та його/її команда звітуватимуть перед генеральним директором, який повинен буде підтвердити свої рішення.

СИТУАЦІЙЕ ОБІЗНАННЯ

Після виявлення інциденту важливо зібрати всю доступну інформацію про дії в період інциденту. Центральний збір та архівування інформації про безпеку (наприклад, системних журналів, журналів політики брандмауера) надає аналітику легкий доступ до цієї інформації. Важливими факторами, які слід враховувати, є цілісність інформації та індексація.

Може знадобитися судово-медичне розслідування, щоб зібрати всі артефакти та вивчити масштаб і глибину нападу. Інструменти для створення та аналізу повних образів диска, а також отримання (віддалених) дампів пам'яті підозрілої машини та блокувальники запису корисні для виконання цього аналізу.

Щоб виявити масштаб інциденту, артефакти або індикатори, зібрані в рамках первинного розслідування, можуть згодом використовуватися для пошуку подальших вторгнень у великому масштабі на всіх керованих пристроях. Наявність центральної точки управління, яка може запитувати їх, може прискорити цей процес. Ви також повинні перевірити, чи не були втрачені/викрадені дані.

ВИЗНАЧЕННЯ РИЗИКІВ НАДАННЯ ПЕРСОНАЛЬНИХ ДАНИХ

Ключовим елементом у боротьбі з порушенням персональних даних є визначення рівня ризику такого порушення. Наскільки серйозним є порушення та можливі наслідки для особи, чиї дані було порушено? Відповідь на це питання є важливим фактором у визначенні кроків, які необхідно зробити. Кожен рівень ризику (без ризику, ризик, високий ризик) вимагає різного підходу, особливо в контексті зобов'язання щодо повідомлення. Таким чином, точна та послідовна оцінка ризику є ключем до ефективної боротьби з порушенням персональних даних. Це гарантує, що вжито правильних дій для дотримання законодавчих положень.

Оцінка порушення персональних даних у повному обсязі дає змогу сформулювати адекватний і реалістичний рівень ризику та вжити правильних подальших заходів. Для того, щоб мати можливість оцінити ризики для прав і свобод особи, необхідно враховувати ряд елементів. Основні елементи описані нижче:

Характер та конфіденційність персональних даних	Конфіденційні дані Чим чутливіші персональні дані, тим вище ризик завдати шкоди постраждалим особам. Публічність даних На додаток до чутливості даних, що витікають, важливий також рівень публічності, який уже надано цим даним. Необхідно перевірити, чи персональні дані особи вже були (загальнодоступними). Пов'язані персональні дані Порушення даних, пов'язаних із даними про стан здоров'я, документами, що посвідчують особу, або фінансовими даними, такими як дані кредитної картки, можуть завдати шкоди самостійно, але в поєднанні з загальнодоступною інформацією також можуть бути скоєні серйозні злочини, такі як крадіжка особистих даних. З цієї причини пов'язані персональні дані становлять більший ризик, ніж ізольована категорія персональних даних.
Кількість особистих даних та кількість постраждалих осіб	Цей елемент розглядає кількість інформації, на яку вплинуло порушення, і загальну кількість осіб, чиї дані постраждали. Чим більше даних і осіб постраждало, тим вищі ризики.
Легкість ідентифікації осіб	Цей елемент зосереджується на тому, наскільки легко стороні, яка має доступ до витоку даних, ідентифікувати особу (можливо, після порівняння з додатковою доступною інформацією). Ризик залежить від того, чи можна ідентифікувати осіб безпосередньо без будь-яких інших персональних даних, чи потрібна додаткова інформація з інших категорій даних для ідентифікації осіб.

Серйозність наслідків	Потенційна шкода, заподіяна особам, і серйозність шкоди повинні бути визначені. Порушення даних можуть бути надзвичайно шкідливими, завдаючи фізичної шкоди, психологічного стресу, приниження або шкоди репутації у таких випадках як шахрайство з ідентифікацією. Якщо витік стосується особистих даних уразливих осіб (наприклад, пацієнтів, дітей), можна віднести більший ризик пошкодження.
існуючі заходи пом'якшення	Заходи пом’якшення, які вже були вжиті під час порушення даних, повинні бути враховані в загальній оцінці ризику; запитуючи, чи і як ці заходи захищають постраждалих осіб.

Реєстр порушень даних

Відповідно до принципу відповідальності, всі міркування та висновки, що випливають з оцінки ризику, повинні бути задокументовані в реєстрі порушень даних. Цей реєстр повинен містити принаймні такі елементи:

Дата і час порушення даних	Точна дата та час, коли організації стало відомо про порушення персональних даних. Ця інформація важлива для дотримання 72-годинного терміну для повідомлення від органу захисту даних та будь-яких суб’єктів даних.
Хронологія та опис порушення даних	Опис подій, пов’язаних із порушенням персональних даних: коли було повідомлено про порушення, коли (ймовірно) сталося порушення, огляд уражених систем та інші описи.
Контактна особа	Важливо мати центральну контактну особу, яка інформована про обставини порушення персональних даних і з якою можна зв’язатися у разі подальших запитань. Зазвичай особа, яка повідомила про витік, є спеціалістом із захисту даних або керівником ураженого відділу.
Залучені сторонні сторони	Містить інформацію про природу та роль організації (контролер, обробник, спільний контролер) та зовнішні сторони, які можуть постраждати, і тому їх потрібно поінформувати.
Оцінка ризику – мотивація та висновок	Детальний аналіз ризику та загальна оцінка ризику на основі елементів визначення рівня ризику (див. розділ вище).
Існуючі засоби контролю та виправні дії	Перелік існуючих технічних та організаційних заходів, а також заходів, які будуть вжиті для зменшення існуючих ризиків для постраждалих осіб.
Сповіщення	Зведення повідомлень, які були зроблені та кому (органу із захисту даних, постраждалим особам, третім сторонам).

2.4 МІСТИТЬ ІНЦИДЕНТ КІБЕРБЕЗПЕКИ

ШВИДКО ВІДНОВИТИ ЧИ ЗБИРАТИ ДОКАЗИ?

Стримка інциденту з кібербезпекою полягає в тому, щоб обмежити шкоду та зупинити зловмисника. Ви повинні знайти спосіб обмежити ризик для вашої організації, водночас підтримуючи її роботу. Вам потрібно запобігти подальшому поширенню інциденту на інші системи, пристрої та мережі як у вашій організації, так і за її межами.

На початку цього етапу вашій організації доведеться прийняти важливе стратегічне рішення: негайно відключити системи, щоб якомога швидше відновитися? Або знайдіть час, щоб зібрати докази проти кіберзлочинця, який проник у систему?

Можливо, вам доведеться знайти баланс між цими двома варіантами.

Яке рішення прийме ваша організація, залежатиме від сфери застосування,

масштаб і вплив інциденту. Наступні критерії можуть допомогти вам оцінити:

- Що могло б статися, якби інцидент не було ліквідовано?
- Чи завдає атака чи прорив негайної серйозної шкоди?
- Чи є (потенційні) пошкодження та/або крадіжка активів?
- Чи потрібно зберігати докази? І якщо так, то які джерела доказів має придбати організація? Де будуть зберігатися докази? Як довго слід зберігати докази?
- Чи потрібно уникати сповіщення хакера?

- Вам потрібно забезпечити доступність служби чи можна перевести систему в автономний режим? (наприклад, послуги, що надаються зовнішнім сторонам)

У деяких випадках повернутися (безпосередньо) до звичайної роботи буде взагалі неможливо. Коли це станеться, метою стримування має бути докласти максимум зусиль, щоб повернутися до звичайної функціональності, тобто зробити систему придатною для використання, зберігаючи доступ для законних користувачів, одночасно блокуючи зловмисника.

Під час інциденту виникне величезний тиск, щоб діяти швидко. Але щоб уникнути непотрібних помилок, дуже важливо зробити крок назад і подумати, перш ніж діяти!

РОЗСЛІДЧЕННЯ: ЗБІР ДОКАЗІВ

Якщо ви хочете вирішувати проблему в її корені та виявити винного для притягнення до відповідальності, вам потрібно буде зберегти докази. Щоб зібрати докази, необхідно провести судово-медичне розслідування, перш ніж ліквідувати інцидент. Якщо у вас немає необхідного внутрішнього досвіду для проведення судової експертизи самостійно, зверніться до зовнішніх експертів, які мають відповідні інструменти для збору доказів юридично дійсним способом.

Майте на увазі, що навіть якщо у вашій організації є дуже компетентна команда ІКТ, вам все одно може знадобитися зовнішня допомога у разі складного інциденту з кібербезпекою. Це не означає, що ваші спеціалісти з ІКТ зазнали невдачі; навпаки, це означає, що вони швидко визначили, що інцидент настільки складний, що вимагає додаткової експертизи.

Для боротьби з DDOS-атакою ПОТРІБНИЙ ДОСВІД

DDoS-атака — це цілеспрямована атака, спрямована на збій вашої системи. Таким чином, він може мати дуже значний вплив на доступність вашої системи. Ці атаки дуже складні, і від них важко позбутися. Більшість

організацій не зможуть самостійно розв’язати DDoS-атаку, і їм доведеться звернутися до зовнішніх експертів.

Для того, щоб докази були прийнятними в суді, вони повинні бути зібрані згідно з процедурами, які відповідають усім чинним законам і нормам. Вам слід уникати компрометуючих доказів. Отже, запам’ятайте наступне:

НЕ ВИМИКАЙ СВІЙ СЕРВЕР

• Якщо ви вимикаєте сервер, ви очищаєте пам'ять на сервері. Це означає, що ви не зможете виконувати криміналістичну експертизу пам’яті, тому що вам не залишиться нічого аналізувати.

• Ви можете знищити важливі докази, оскільки оперативна пам'ять часто містить багато слідів шкідливого програмного забезпечення. Перш ніж вимкнути сервер, його потрібно скинути на USB-накопичувач.

НЕ ВІДРІЗАЙ СЕРВЕР ВІД ІНТЕРНЕТУ

• Ви можете знищити важливі докази. Негайне завершення роботи робить неможливим визначити ступінь скомпрометації вашої інфраструктури, оскільки сервер, який був вимкнений та відключений від Інтернету, більше не спілкується зі своїм сервером управління та управління в Інтернеті або з іншими зараженими робочими станціями/ серверів у вашій мережі.

• Можливо, ви попереджаєте кіберзлочинця про те, що ви на нього/неї, і на даному етапі це не дуже гарна ідея.

НЕ ВІДНОВЛЮЙТЕ ВАШУ СИСТЕМУ З РЕЗЕРВНОЇ КОПІЇ, КОЛИ ВИ НЕ ВПЕВНЕНІ, ЩО САМА РЕЗЕРВНА КОПІЯ НЕ ЗАРАЖЕНА

Ваша резервна копія може бути заражена: АТП можуть заразити вашу мережу протягом тривалого періоду, не помічаючи. Це робить ймовірним ризик зараження резервної копії. Встановлення зараженої резервної копії може відтворити зараження.

НЕ ВСТАВЛЯЙТЕ ПЕРЕВСТАНОВЛЕННЯ НА ОДИН СЕРВЕР БЕЗ СУДОВОЇ КОПІЇ

НАЙПОШИРЕНІШІ ТИПИ ІНЦИДЕНТІВ

На цьому етапі корисно мати список категорій інцидентів, які найбільше вразять вашу організацію (див. також: сторінка 20, Визначення можливих категорій інцидентів кібербезпеки). Цей список має містити типи інцидентів, які найімовірніше вразять вашу організацію, та основні інструкції щодо вирішення таких інцидентів.

ВИКОРІНЕННЯ ТА ОЧИЩЕННЯ

Після завершення розслідування можна приступати до ліквідації. На цьому етапі ви повинні видалити всі компоненти, пов’язані з інцидентом, усі артефакти, залишені зловмисником (зловмисний код, дані тощо), і закрити кожну діру чи вразливість, які спочатку використовувалися хакером для вторгнення.

Не починайте прибирання, поки не отримаєте повну картину інциденту! Це означає, що слід почати з визначення його першопричини. Це непросте завдання. Крім того, ви повинні переконатися, що ви принаймні переглянули всі машини з однаковою уразливістю, оскільки вони також можуть бути заражені. Щоразу, коли приймається рішення почати ліквідацію інциденту, важливо бути швидким, синхронізованим і ретельним, щоб дати вашому супротивнику якомога менше шансів (в ідеалі — жодного) для відповіді.

Викорінення може приймати різні форми. Він часто включає в себе такі дії, як:

• Запуск сканера вірусів або шпигунських програм для видалення шкідливих файлів і служб

• Оновлення підписів

• Видалення шкідливих програм

• Відключення зламаних облікових записів користувачів

• Зміна паролів зламаних облікових записів користувачів

• Виявлення та пом'якшення всіх уразливостей, які були використані

• Виявлення прогалин безпеки та їх усунення

• Інформування працівників про загрозу та надання їм інструкцій щодо того, чого слід уникати

в майбутньому

• Інформування зовнішніх зацікавлених сторін, таких як ЗМІ та ваші клієнти

Також важливо інформувати вище керівництво про результати ліквідації та очищення, а також про ситуацію в мережі.

Антивірусне рішення може виявляти окремі файли, поміщати їх на карантин або видаляти з систем. Це рішення повинно приймати конкретні визначення вірусів, які ви надаєте.

Фішингові електронні листи можна стримувати на поштовому шлюзі шляхом блокування на основі відправника, передачі пошти або частини вмісту.

Індикатори IP і домену можна заблокувати на основі мережевого трафіку, додавши їх у списки доступу, політики брандмауера або політики проксі. Тому важливо мати необхідний потенціал для випадкового впровадження цих змін.

ВІДНОВЛЕННЯ

Коли ми говоримо про відновлення, ми маємо на увазі відновлення системи (систем) для повернення до нормальної роботи та (якщо можливо) усунення вразливостей для запобігання подібним інцидентам. Існує кілька способів відновлення після інциденту кібербезпеки. Усі вони по-різному впливають на час відновлення, обмеження вартості або втрату даних:

	ЧАС ВІДНОВЛЕННЯ	ВАРТІСТЬ	ВТРАТА ДАНИХ	ЗАУВАЖЕННЯ
Очистіть шкідливі артефакти та замініть скомпрометовані файли чистими версіями	Швидко	Економічно ефективним		Ви можете залишити невідкриті артефакти
Відновлення з резервної копії	Середній	Економічно ефективним		Це можливо, лише якщо у вас є надійна резервна копія. У деяких випадках важко визначити мітку часу початкового інциденту, або інцидент міг тривати протягом тривалого часу, без резервної копії періоду до інциденту.
Перебудуйте систему(и) або середовище з нуля	Повільно, не ефективно за часом	Дуже дорого	Імовірність втрати даних	Однак це єдиний спосіб бути впевненим на 100% у позбавленні від злочинця.

Тип відновлення буде залежати не тільки від часу та фінансових можливостей, які ви маєте в своєму розпорядженні. Це також залежатиме від шкоди, яку інцидент завдав вашій інфраструктурі. Наприклад, у вас може не бути неінфікованої резервної копії, оскільки навіть найстаріша резервна копія була зроблена після того, як зловмисник увійшов у вашу систему. Тому важливо перевірити резервну копію на наявність вірусів, руткітів і бекдорів, перш ніж відновлювати її. Якщо не вдається знайти належну резервну копію, систему необхідно перевстановити з нуля (включаючи операційну систему!). Після відновлення системи вам необхідно усунути вразливі місця, які дозволили зловмиснику отримати доступ до вашої системи.

Це включатиме такі дії, як: встановлення патчів як на рівні операційної системи, так і на рівні програми, зміна паролів, зміна облікових записів,

посилення безпеки периметра мережі, напр. зміна брандмауера, списків контролю доступу прикордонного маршрутизатора тощо та блокування служб.

Ви також повинні враховувати, що після успішної атаки на ресурс є ймовірність, що він буде атакований знову, або інші ресурси у вашій організації можуть бути атаковані подібним чином. Тому вам слід розглянути можливість покращення свого захисту, наприклад, застосувавши більш високий рівень системного журналу або моніторингу мережі.

Нарешті, перед тим, як система буде знову ввімкнена, її слід перевіряти як на безпеку, так і на бізнес-функції. З точки зору безпеки, вашу систему можна перевірити, відсканувавши її за допомогою інструмента, який перевіряє наявність уразливостей. Щоб підтвердити бізнес-функції, відповідальна особа повинна перевірити, чи всі функції, необхідні для бізнесу, працюють належним чином.

Не забувайте: якщо у вас немає необхідного досвіду у вашій організації, зверніться до зовнішніх експертів. І не забудьте перевірити, чи покриває цю вартість ваша кіберстраховка.

Висновок до другого розділу: Інциденти з безпекою та даними стають все більш частими. Жоден окремий продукт чи метод не може гарантувати, що кіберзахист вашого бізнесу витримає. Тому дуже важливо заздалегідь продумати та вирішити, як ви будете керувати своєю реакцією на кіберзлом.

Розділ 3 СПІЛКУВАННЯ ПІД ЧАС ІНЦИДЕНТУ КІБЕРБЕЗПЕКИ

Коли відбувається фактичний інцидент кібербезпеки, група реагування на інциденти кібербезпеки повинна негайно скласти конкретний план комунікації для конкретного інциденту. Складіть цей план спілкування на основі загальної підготовки, яку ви вже зробили на етапі підготовки (див. також сторінку 16: Підготуйте свою комунікаційну стратегію). В основному вам потрібно буде відповісти на наведені нижче запитання, і пам’ятайте, що ми рекомендуємо координувати всі зовнішні комунікації як з юридичними, так і зі зв’язків з громадськістю. Подумайте, перш ніж спілкуватися!

ІНСТРУМЕНТИ

Якщо ви добре підготовлені, ваша команда реагування на інциденти кібербезпеки вже матиме в своєму розпорядженні ряд інструментів. Під час підготовчого етапу ваша організація склала список усіх потенційних зацікавлених сторін, з якими можна зв’язатися (внутрішні, зовнішні та офіційні зацікавлені сторони) та їхні контактні дані (конкретна особа та її/її). резервне копіювання).

3.1 ПЛАН КОМУНІКАЦІЇ НА ІНЦИДЕНТ

З КИМ СПІЛКУВАТИСЯ І ЯК СПІЛКУВАТИСЯ

ДО КОЖНОЇ КАТЕГОРІЇ ЗАЦІКАВЛЕНИХ СТОРІН

Першим кроком у вашому плані комунікації для конкретного інциденту є визначення того, з ким ви будете спілкуватися. Для цього вам потрібно визначити, на яких потенційних зацікавлених сторін може (несприятливо) вплинути інцидент кібербезпеки, з яким ви зіткнулися, і чи зобов’язані ви за законом сповістити певні організації, такі як Національний орган із захисту даних або галузевий регулятор.

• Внутрішні зацікавлені сторони: топ-менеджмент, керівники, які впливають, співробітники

• Зовнішні зацікавлені сторони: ЗМІ, клієнти, постачальники, інші партнери тощо.

• Офіційні зацікавлені сторони: Національний орган із захисту даних, галузевий регулятор, CCB (Cert.be відділ), Національний кризовий центр, міліція

Коли ви визначаєте, що і з ким ви будете спілкуватися, гарне основне правило — спілкуватися лише на основі потреби знати. Будуть зацікавлені сторони, з якими ви хочете спілкуватися, щоб стримати інцидент кібербезпеки, і будуть зацікавлені сторони, з якими вам доведеться спілкуватися, або тому, що вони тиснуть на вас за інформацією (наприклад, ЗМІ), або тому, що ви юридично зобов’язані сповістити їх (наприклад, Національний орган із захисту даних, галузеві регулятори, осіб, чиї дані були зламані).

3.2 ОСОБИСТІ ДАНІ

Якщо персональні дані були втрачені або викрадені (злом даних), доцільно повідомити про це Національний орган із захисту даних. У деяких випадках ви будете зобов’язані це зробити за законом. Наприклад: • Постачальники загальнодоступних послуг електронного зв'язку (провайдери телекомунікацій)

мають юридичний обов’язок повідомляти про порушення персональних даних до Національних даних

Органу захисту та особам, чиї дані були зламані.

• Відповідно до GDPR існує юридичне зобов’язання повідомляти про будь-яке порушення персональних даних, яке може спричинити ризик для осіб, чиї дані були зламані, як Національному органу із захисту даних (протягом 72 годин), так і особам, чиї особисті дані

дані були скомпрометовані.

ЗОБОВ'ЯЗАНА ЗВІТНІСТЬ: ДИРЕКТИВА НІШ

OES та DSP зобов’язані повідомляти про всі інциденти з далекосяжними наслідками CCB (CERT.be dept), Національний кризовий центр та їхні галузеві органи через захищену платформу звітності. CCB діє як національна CSIRT. Чи є наслідки інциденту суттєвими чи ні, необхідно оцінювати з огляду на доступність, конфіденційність, цілісність або достовірність інформаційних систем, тобто інформаційних систем OES/DSP.

• Доступність означає можливість доступу користувачів до послуг OES/DSP. Наприклад, DDoS-атака може паралізувати мережу OES і поставити під загрозу доступність послуги.

• Прикладом інциденту конфіденційності є, наприклад, «людина в середині атаки», під час якої перехоплюються дані між користувачами та OES/DSP. Такий інцидент також може призвести до зобов'язання повідомити орган із захисту даних (див. стор. 29).

• Порушення цілісності відбувається, коли дані з OES/DSP знищуються під час збою системи.

• Інцидент щодо автентичності відбувається, наприклад, коли постачальник доменних імен більше не може з упевненістю гарантувати автентичність доменних імен.

Можливо, рівні впливу та/або порогові значення на сектор чи підсектор визначаються Королівським указом, але цього ще не було.

Майте на увазі, що за порушення зобов'язання щодо звітності можуть бути накладені суворі адміністративні та кримінальні стягнення.

КОЛИ СПІЛКУВАТИСЯ?

Після того, як ви визначите, з ким ви будете спілкуватися і що ви їм скажете, вам потрібно вирішити, коли ви будете з ними зв'язуватися. Час має бути заснований на цілях комунікації

Важливий час:

• Деяким зацікавленим сторонам знадобиться інформація якомога швидше, оскільки вони можуть допомогти містять інцидент кібербезпеки (наприклад, топ-менеджмент вашої організації, е- працівники);

• Необхідно зв'язатися з іншими зацікавленими сторонами (наприклад, Національним органом із захисту даних) у визначений законом термін; і, нарешті,

• Інші (наприклад, ЗМІ) можуть зв'язатися з вами, і в такому випадку ви повинні отримати відповіді готовий.

Майте на увазі, що, щоб не попередити зловмисника про те, що ви на нього/неї, може знадобитися розпочати фазу без комунікації з моменту виявлення інциденту до моменту, коли ви отримаєте повну картину інциденту та план дій. Якщо зловмисник попереджений, він, ймовірно, відступить і зітре всі свої сліди або, що ще гірше, завдасть остаточної шкоди, наприклад, вкраде останні коштовності вашої організації або встановить бэкдори. Щоб уникнути витоку на цьому етапі відсутності зв'язку, ви можете вести список людей, які знають про інцидент кібербезпеки. Так буде легше виявити, хто несе відповідальність, коли здається, що інформація була витоком. До будь-кого, хто розповсюджує інформацію, можна застосувати юридичні заходи.

Про інцидент NIS необхідно повідомити негайно. Немає необхідності чекати, поки буде доступна вся відповідна інформація. Якщо зрозуміло, що про інцидент необхідно повідомити, і, отже, якщо дотримано хоча б один критерій, це потрібно зробити якомога швидше.

ЗВІТНІСТЬ ДО ОРГАНІВ

Звітування перед владою є дуже специфічною частиною спілкування. Це важливо з різних причин:

• Як уже згадувалося вище, у деяких випадках існує законодавча вимога щодо звітування витік даних або інші інциденти безпеки.

• Певні органи влади можуть вам допомогти. Інцидент кібербезпеки, з яким ви зіткнулися, може не бути поодиноким випадком. Органи влади можуть мати інформацію, яка може допомогти вам швидше розв'язати інцидент.

• Якщо ви хочете подати скаргу на злочинця, який стоїть за інцидентом кібербезпеки, необхідно звернутися до правоохоронних органів. В принципі це буде поліція.

• Крім того, звітування перед владою є необхідним кроком, який дозволяє їм винаходити- виявлення та вимірювання кіберзлочинності в країні. Поглиблені знання та розуміння цього явища та його поширеності допоможе покращити загальний ландшафт безпеки, напр. шляхом формування превентивних та контрзаходів.

Добровільна звітність до ССВ (відділ CERT.be)

Організації завжди повинні серйозно розглядати можливість повідомлення про інциденти кібербезпеки федеральній групі реагування на надзвичайні ситуації в кібернетичних ситуаціях, ССВ (CERT.be dept). Щоб запобігти атакам на інші комп'ютерні системи, ССВ (CERT.be dept) особливо цікавиться тим, що вони називають «індикаторами компромісу» (IOC). Це артефакти, помічені в мережі або операційній системі, що вказує на те, що дуже ймовірно було вторгнення. Звітування до ССВ (CERT.be dept) є життєво важливим для того, щоб визначити, чи є інцидент ізольованим, і зробити можливим відстежувати тенденції загроз у Бельгії. ССВ (CERT.be dept) зможе надати деяку інформацію та поради щодо інциденту, які можуть допомогти потерпілому вжити ефективних контрзаходів. Крім того, інформація, яку надає ваша організація, може допомогти запобігти атакам на інші комп'ютерні системи.

НЕОБХІДНО ПОЗВІТИТИ ТАКУ ІНФОРМАЦІЮ
1. Ваші контактні дані
2. Тип інциденту
3. Дата події
4. Інцидент триває?
5. Як ви помітили цей випадок?
6. Який вплив інциденту?
7. Ви вже вжили заходів чи заходів? Якщо так, то які?
8. Чи є у вас журнали чи інші корисні дані?
9. Кого ви вже повідомили?
10. Чого ви очікуєте від свого звіту?

Обов'язкове звітування про інциденти з НІС

Звіти необхідно подавати через платформу звітності NIS. Платформа доступна через Інтернет через безпечне з’єднання та унікальний ідентифікаційний ключ для кожного AED та DDV (логін/ім’я користувача та пароль). Якщо платформа недоступна, про інцидент необхідно повідомити через веб-сайт ССВ. Платформа гарантує, що звіт досягне ЦКБ, Національного кризового центру та секторального уряду.

Нижче наведено відповідний секторальний уряд для кожного сектора.

Сектор	Галузевий уряд
Енергія	Міністр, відповідальний за енергетику
Транспорт	Міністр, відповідальний за транспорт або морську мобільність
Охорона здоров'я	Міністр, відповідальний за охорону здоров'я
Питна вода	Національний комітет з безпеки постачання та розподілу питної води
Цифрові інфраструктури	Міністр, відповідальний за економіку
Фінанси	НБУ (фінансові установи

Звіт містить всю наявну інформацію, яка дає змогу відповідним особам визначити характер, причини, наслідки та наслідки інциденту:

• назва та контактні дані постачальника та наданої послуги;

• дата і час, коли стався інцидент;

• тривалість інциденту;

• протяжність географічної території, яка постраждала від інциденту, та її транскордонний простір природа, якщо є;

• кількість постраждалих користувачів;

• відомості про характер інциденту;

• масштаби наслідків інциденту, зокрема соціально-економічних діяльності;

• важливість систем або залученої інформації;

• наслідки інциденту для міжнародних організацій

• вжиті дії;

• опис поточної ситуації.

Початкове повідомлення, яке має бути зроблено якомога швидше, є одним із етапів процедури повідомлення. Всього процедура може включати три етапи:

• Початковий звіт має бути складений негайно, навіть якщо OES або DSP ще не мають усієї необхідної інформації. Метою цього початкового звіту є висвітлення інциденту та його можливих наслідків для ССВ, секторального уряду або його секторального CSIRT та NCCN.

• Додаткові сповіщення слід надсилати регулярно або відразу ж, як тільки OES або DSP отримає нову інформацію. Метою цих додаткових звітів є інформування ССВ, секторального уряду або його секторального CSIRT та NCCN про стан інциденту. Потім OES або DSP створює новий звіт на платформі, вказуючи лише нові дані та контрольний номер початкового звіту.

• Можливий остаточний звіт (на запит одного з вищезгаданих органів), що містить всю інформацію, надіслану до ССВ, державного сектору або його галузевої CSIRT та NCCN. Мета цього підсумкового звіту – надати огляд інциденту та зробити висновки з нього.

OES або DSP повинні інформувати ССВ та урядовий сектор або, якщо це доречно, галузевий CSIRT про розвиток інциденту та вжиті заходи з усунення.

Подання скарги до правоохоронних органів

Після виявлення інциденту кібербезпеки правоохоронні органи мають бути повідомлені якомога швидше, враховуючи нестабільність слідів та дій, які необхідно вжити (інтернет-ідентифікація тощо). Щоб судове переслідування було успішним, ланцюг тримання під вартою має бути збережений у законодавчий спосіб, що вимагає збереження доказів негайно після виявлення інциденту.

Для кваліфікації правопорушення та встановлення особи підозрюваного органам юстиції необхідно володіти наявною інформацією щодо події. Інформація, яку слід повідомити поліції у випадку шахрайства в Інтернеті ("традиційний" злочин, вчинений за допомогою електронних засобів), може не збігатися з інформацією, яка потрібна поліції у випадку ІКТ-злочинів (злом, саботаж, шпигунство). У ході розслідування слідчі запитують, збиратимуть та розшукують додаткову інформацію. Надзвичайно важливо, щоб ваші служби надавали допомогу та внесок, про які запитують правоохоронні органи, щоб допомогти просунути розслідування.

I. Поліція

Якщо ваша організація постраждала від інциденту і як така стала жертвою правопорушення, ви можете подати скаргу. За замовчуванням ви повинні звернутися до місцевої поліцейської дільниці або поліцейської дільниці на ваш вибір. У більш складних випадках місцева поліція отримає підтримку від Регіональних підрозділів по боротьбі з комп'ютерними злочинами (RCCU), які спеціалізуються на боротьбі з ІКТ-злочинами (злом, саботаж, шпигунство) та/або Федерального відділу комп'ютерної злочинності (FCCU). Якщо справа стосується критичної інфраструктури або сектора з особливими правилами, може застосовуватися спеціальна процедура.

II. Слідчий суддя

Також можна подати скаргу безпосередньо до магістрату (слідчого судді). Це має бути винятковим заходом. Крім того, вашій організації, ймовірно, доведеться авансувати витрати на розслідування, оскільки магістрат проводить його за вашим конкретним запитом.

ПОВІДОМЛЕННЯ ПРО ПОШИРЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ ОРГАН ЗАХИСТУ ДАНИХ

Про певні порушення персональних даних необхідно повідомляти Національний орган із захисту даних. Нагадаємо, під персональними даними ми маємо на увазі всі дані, що стосуються фізичної особи, яка є або може бути ідентифікована прямо чи опосередковано. Таким чином, число, наприклад IP-адреса, у багатьох випадках також розглядатиметься як персональні дані.

Зобов'язання щодо сповіщення стосується порушень, які становлять ризик для прав і свобод суб'єктів даних. Прикладом цього є втрата конфіденційності зв'язку, внаслідок чого дані рахунків-фактур, адреси тощо тимчасово стають

видимими для третіх сторін. В принципі, період повідомлення становить 72 години після виявлення порушення даних.

Коли ваша організація повідомить Національний орган із захисту даних, останній зможе оцінити вплив порушення даних у співпраці з особою, відповідальною за обробку порушених даних, і може дати рекомендації щодо правил обробки даних та необхідності захисту це Крім того, особа (особи), відповідальна за обробку даних, повинна буде переглянути спосіб організації та безпеки обробки даних зараз і в майбутньому. Організації з конкретних секторів, наприклад постачальники фінансових послуг або електронні комунікаційні мережі, повинні пам’ятати, що вони вже зобов’язані повідомляти Національний орган із захисту даних про будь-який інцидент, пов’язаний із порушенням персональних даних.

ПОВІДОМЛЕННЯ ФІЗИЧНИМ ОСОБИМ, ЧИМИ ПЕРСОНАЛЬНІ ДАНІ

СКОМПРОМІЗОВАНО

У певних випадках необхідно повідомити осіб, чиї дані причетні до порушення даних. Особа, відповідальна за обробку даних, повинна сповістити осіб, причетних до порушення даних, за допомогою засобів зв'язку, що гарантує, що інформація буде отримана якомога швидше. Якщо неможливо ідентифікувати жертв порушення, обробник даних може повідомити їх через публічні засоби масової інформації, в той же час переслідуючи особистість осіб, щоб повідомити їх на особистий основі.

Повідомлення для залучених осіб має бути чітким і легким для розуміння. Національний орган із захисту даних рекомендує надати як мінімум таку інформацію:

• Ім'я особи, відповідальної за обробку даних;

• Контактна інформація для отримання додаткової інформації;

• Короткий опис інциденту, під час якого відбулося порушення даних;

• (Ймовірна) дата інциденту;

• Тип і характер залучених персональних даних;

• Можливі наслідки порушення для причетних осіб;

• Обставини, за яких відбулося порушення даних;

• Заходи, вжиті обробником даних для запобігання злому даних;

• Заходи, які відповідальна особа рекомендує вжити залученим особам

обмежити можливі збитки.

3.3 ДОСЛІДЖЕННЯ ТА ЗАКЛЮЧЕННЯ ІНЦИДЕНТІВ: ДІЗНАТИСЯ ВІД КОЖНОГО ІНЦИДЕНТУ!

Усі інциденти кібербезпеки, як і будь-які інші інциденти, мають бути належним чином закриті. Крім того, дуже важливо витягувати уроки з кожного інциденту, щоб оцінити майбутні покращення.

ОЦІНЮВАННЯ УРОКІВ ТА МАЙБУТНІ ДІЇ: ОРГАНІЗУЙТЕ ОГЛЯД ПІСЛЯ ІНЦИДЕНТУ

Огляд після інциденту є дуже корисним документом, оскільки він показує фактичні дані та реальні наслідки. Це може допомогти вашій організації оцінити ваш план реагування на кіберінциденти та бюджет.

ЯК МАЄ ВИГЛЯДАТИ ОГЛЯД ІНСЦЕНДІВ?

Огляд після інциденту та можливі уроки повинні бути частиною обробки всіх інцидентів кібербезпеки.

Контрольний список питань, які можуть допомогти в оцінці:

• Чи дотримувалися план та процедури управління інцидентами кібербезпеки? Чи були вони адекватними? Повинен

план адаптувати за певними моментами?

• Чи була інформація доступна вчасно? Якщо ні, то чи можна було б отримати його раніше і як?

• Чи були якісь кроки або дії, які ви вжили, які могли б загальмувати відновлення?

• Чи можна покращити обмін інформацією з іншими організаціями?

• Які коригувальні дії можуть запобігти подібним інцидентам у майбутньому?

• Чи існують прекурсори або індикатори, які слід відстежувати, щоб легше виявляти подібні інциденти в країні

майбутнє?

• Які додаткові інструменти чи ресурси необхідні для виявлення, аналізу та пом'якшення майбутніх інцидентів кібербезпеки?

• Чи мала група реагування з кібербезпеки належні організаційні повноваження для реагування на інцидент?

Чи варто найняти більше людей чи призначити консалтингову фірму, юриста, на випадок майбутнього інциденту з кібербезпекою?

ВІДСТЕЖЕННЯ ТА ЗВІТНІСТЬ ІНЦЕНДІВ

Важливо задокументувати кожен інцидент і вжиті вами дії, а також зберігати всю цю документацію разом. Подібні інциденти можуть повторюватися і потребувати тих самих процедур обробки, або невеликий інцидент може виявитися частиною більшого інциденту, який ви дізнаєтеся пізніше. Крім того, необхідно також повідомити про інцидент відповідним зацікавленим сторонам, як внутрішнім, так і зовнішнім. Використовуйте результати перевірки після інциденту, щоб визначити, до яких зацікавлених сторін слід звернутися. Внутрішнє керівництво організації має завжди розглядатися як відповідна зацікавлена сторона і, таким чином, отримувати документований звіт про те, що сталося, які дії були вжиті, де все пішло добре/неправильно тощо.

ОБ'ЄКТИВНЕ ВІДСТЕЖЕННЯ

Усі інциденти кібербезпеки та їх вирішення мають бути задокументовані.

Звітність: про всі інциденти кібербезпеки та їх вирішення необхідно повідомляти вищому керівництву та, якщо ця функція існує у вашій організації, спеціалісту з інформаційної безпеки.

ЧОМУ?

Відстеження: Подібні інциденти можуть виникати і вимагати використання тих самих процедур, або менший інцидент може бути частиною більшого інциденту, виявленого пізніше.

Звітність: Про будь-які інциденти з кібербезпеки необхідно інформувати вищого керівництва та/або осіб у вашій організації, відповідальних за аналіз ризиків у вашій організації (наприклад, комітет з операційних ризиків або еквівалент).

ЯК МАЄ ВИГЛЯДАТИ ЦЕЙ ДОКУМЕНТ ВІДТЕЖЕННЯ ТА ЗВІТНОСТІ?

Документований звіт має бути складений для всіх інцидентів кібербезпеки та зберігатися разом із іншими звітами про інциденти кібербезпеки. Ви можете скласти цей звіт на основі висновків огляду після інциденту.

Про всі серйозні інциденти безпеки слід негайно повідомляти вищому керівництву. Принаймні раз на рік про всі інциденти кібербезпеки необхідно повідомляти та пояснювати вищому керівництву та людям у вашій організації, які аналізують ризики вашої організації.

Висновок до третього розділу: Ефективно сплановані канали зв’язку можуть допомогти зменшити операційні, репутаційні та юридичні ризики, пов’язані з кібер-подіями, і навіть можуть мати вирішальне значення для пом’якшення збитків. Чітка і всеосяжна реакція, яку проводить заздалегідь узгоджена команда, зменшує хаос, який часто виникає після атаки або порушення. Крім того, зовнішні та медіа комунікації можуть бути ефективними лише в тому випадку, якщо внутрішні співробітники усвідомлюють свої обов’язки, коли справа доходить до передачі інформації.

ВИСНОВКИ

Отже, сьогодні ми бачимо як інтернет змінює спосіб ведення бізнесу: кількість даних, які ми передаємо через Інтернет, і наша залежність від їх доступності постійно збільшуються. Зрозуміло, що зв’язок зі світом не тільки приносить великі можливості, але й створює нові ризики. Кіберзлочинність — це великий бізнес, і навіть найменша зловмисна атака може серйозно зашкодити репутації організації, продуктивності, системі ІКТ тощо.

Жодна організація не повинна думати, що вона захищена від кіберзлочинності. Кіберзлочинці націлені не лише на великі організації. Навпаки, невелика організація може бути більш цікавою жертвою через інформацію, яку вона обробляє, або навіть через партнерів, з якими вона працює.

Звертаю увагу на важливість усвідомлення того, що в той чи інший день ваша організація може стати об’єктом кібератаки. І коли це станеться, потрібно бути готовим! Хороший план реагування на інциденти кібербезпеки може змінити інцидент кібербезпеки від кризи кібербезпеки. Швидкість, з якою організація здатна розпізнати, проаналізувати і реагувати на інцидент, вплине на завдану шкоду та вартість відновлення.

Такий план реагування на інциденти кібербезпеки не повинен обмежуватися лише технологіями! Процеси, люди та інші організаційні аспекти також є важливими елементами, які слід враховувати. Багато організацій можуть не мати необхідного внутрішнього досвіду та навичок, щоб адекватно реагувати на інциденти кібербезпеки. Коли вони стикаються з інцидентом, їм може знадобитися звернутися до експертів для локалізації інциденту та/або для проведення судово-медичного розслідування. Це не означає, що вони самі нічого не можуть зробити. Навпаки, є багато речей, які можна і потрібно зробити до того, як станеться реальний інцидент.

Складання плану реагування на інциденти кібербезпеки організації є важливим першим кроком в управлінні інцидентами кібербезпеки. Також дуже важливо, щоб вище керівництво підтвердило цей план і брало участь у кожному етапі циклу управління інцидентами кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. НВ БІЗНЄС (Грудень 20, 2021) Дійте так, ніби вас уже зламали. Захист бізнесу від кіберзагроз — експерт з кібербезпеки, (онлайн джерело), за посиланням: https://biz.nv.ua/ukr/bizinterview/kiberbezpeka-dlya-biznesu-v-ukrajini-poradi-eksperta-50202511.html

2. Нехай В.А (Лютий 24, 2017) ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ (онлайн стаття), за посиланням: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf

3. О. В. Криворучко (Листопад 27, 2020) КІБЕРГІГІЄНА. КІБЕРБЕЗПЕКА. БЕЗПЕКА ДЕРЖАВИ (онлайн стаття), за посиланням: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

4. Віннікова І.І., Марчук С.В. (Червень 07, 2019) КІБЕР-РИЗИКИ ЯК ОДИН ІЗ ВИДІВ СУЧАСНИХ РИЗИКІВ У ДІЯЛЬНОСТІ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ТА УПРАВЛІННЯ НИМИ (онлайн стаття), за посиланням: https://chmnu.edu.ua/wp-content/uploads/2019/07/Vinnikova-I.I.-Marchuk-S.V..pdf

5. Телесфера (Вересень 25,2020) Кібербезпека: як захистити підприємство в епоху Індустрії Х.0 (онлайн джерело), за посиланням: http://www.telesphera.net/blog/kiberbezpeka-indystrii-x-0.html

6. Лисенко І.А. (Серпень 29, 2018) Основи управління кібербезпекою (онлайн джерело), за посиланням: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8431/1/Osn_ypr_kiber.pdf

7.Василішин С. (2021) УДОСКОНАЛЕННЯ ВАЖЕЛІВ УПРАВЛІННЯ ДІДЖИТАЛІЗАЦІЙНИМИ РИЗИКАМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ФОРМУВАННЯ КІБЕРБЕЗПЕКИ ОБЛІКОВОЇ СИСТЕМИ (онлайн стаття), за посиланнм: http://dspace.wunu.edu.ua/bitstream/316497/42062/1/%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D1%96%D1%88%D0%B8%D0%BD.pdf

8.Гулак Г.М. (2020) МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ. АСПЕКТИ КІБЕРБЕЗПЕКИ (онлайн стаття), за посиланням: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf

9. НКЦК (2021) Нормативно-правовий та організаційний аспекти забезпечення міжнародної кібербезпеки (онлайн стаття), за посиланням: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/28072021/Bulltn_NCK_2.pdf

10.Довгань О. (2018) КІБЕРБЕЗПЕКА ВІНФОРМАЦІЙНОМУСУСПІЛЬСТВІ (онлайн стаття), за посиланням: http://ippi.org.ua/sites/default/files/bezpeka_2018-6.pdf

11.Підгайна Є. (Липень 20, 2018) Галузі майбутнього: що відбувається в світі Cybersecurity (онлайн джерело), за посиланням: https://mind.ua/publications/20186697-galuzi-majbutnogo-shcho-vidbuvaetsya-v-sviti-cybersecurity

12.PWC (2018) Посилення цифрового середовища проти кібер-загроз (онлайн стаття), за посиланням: https://www.pwc.com/ua/uk/survey/2018/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks-ukr.pdf

13. The Ultimate Cybersecurity Checklist for Small Businesses
https://optimalidm.com/resources/blog/small-business-cyber-security-checklist/

14. MORE THAN HALF OF SMALL BUSINESSES CLOSE AFTER A CYBER ATTACK
https://www.businessaustralia.com/resources/news/more-than-half-of-small-businesses-close-after-a-cyber-attack

15.Susan Morrow (Травень 27, 2021) A Beginners Guide to Cybersecurity – for Small Businesses
https://vpnoverview.com/internet-safety/business/beginners-guide-cybersecurity-businesses/

16. Cybersecurity planning for any small business
https://www.wellsfargo.com/biz/wells-fargo-works/planning-operations/security-fraud-protection/cybersecurity-management-plan-and-your-business/

17.НАСБУ (Березень 26, 2021)
https://academy.ssu.gov.ua/uploads/p_57_53218641.pdf

18. Раєцький А. Кібербезпека бізнесу
https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/