УДК 004.056.2

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ПІДПРИЄМСТВА В УМОВАХ ПАНДЕМІЇ

Малькевич Р., Ящук В.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто актуальні проблеми забезпечення безпеки інформації підприємства в умовах пандемії, проаналізовано основні тенденції процесу збору, оброблення, перетворення та зберігання конфіденційної інформації. Наведено опис сучасних концепцій віддаленого доступу та Bring your Own Device, та найслабших ланок у ланцюзі безпеки. Запропоновано у межах програми управління інформаційною безпекою проведення моніторингу безпеки, який захищає від порушень даних, зменшуючи витрати на аудит та сприяючи дотриманню внутрішніх і зовнішніх стандартів безпеки та конфіденційності.

Ключові слова: *інформаційна безпека, конфіденційна інформація, моніторинг безпеки, ландшафт кіберзагроз.*

The current problems of information security of the enterprise in a pandemic are considered, the main trends in the process of collecting, processing, converting and storing confidential information are analyzed. Describes modern concepts of remote access and Bring your Own Device, and the weakest links in the security chain. It is proposed within the information security management program to conduct security monitoring, which protects against data breaches, reducing audit costs and promoting compliance with internal and external standards of security and confidentiality.

Key words*: information security, confidential information, security monitoring, cyber threat landscape.*

Сьогодні сучасні підприємства створюють, об'єднують і зберігають великі обсяги інформації про своїх клієнтів, включаючи поведінкову аналітику, дані про використання, особисту інформацію, дані про кредитні картки та платежі, інформацію про медичне обслуговування та багато іншого. Збільшення обсягів збору корпоративних даних за останнє десятиліття разом із зростанням загрози кібератак і злому даних призвело до значних змін у сфері управління інформаційною безпекою для IT-організацій.

Управління інформаційною безпекою описує набір політик і процедурних засобів контролю, які впроваджують в IT та бізнесі для захисту своїх інформаційних активів від загроз та вразливостей. Відповідальність за інформаційну безпеку може бути покладена на начальника відділу безпеки, головного технічного директора або менеджера з IT-операцій, до команди якого входять IT-оператори та аналітики безпеки. Більшість організацій розробляють офіційний документований процес для управління InfoSec, який називають системою управління інформаційною безпекою або СУІБ.

У випадку, коли підприємство не збирає ідентифікаційну або особисту інформацію від клієнтів, виникає питанням, чи потрібно приймати процеси управління інформаційною безпекою для захисту даних. Всі організації володіють інформацією, яку вони не хотіли б поширювати або оприлюднювати. Незалежно від того, чи зберігаються ці дані в цифровому чи фізичному форматі. Управління інформаційною безпекою має вирішальне значення для захисту даних від несанкціонованого доступу або крадіжки.

Інформаційна безпека на організаційному рівні зосереджена навколо тріади ЦРУ: конфіденційність, цілісність та доступність. Для забезпечення конфіденційності, цілісності та доступності захищеної інформації введені засоби контролю інформаційної безпеки. Фахівці InfoSec та команди SecOps повинні розуміти кожен нещодавно впроваджений контроль з точки зору того, як він сприяє тріаді CIA для захищеного класу даних [1,2].

Збереження конфіденційності інформації означає забезпечення того, що лише уповноважені особи можуть отримати доступ до даних або змінити їх. Щоб дані вважалися захищеними, IT-організація повинна переконатися, що вони належним чином зберігаються і не можуть бути змінені чи видалені без відповідних дозволів. Процеси і процедури, які забезпечують доступність важливої інформації авторизованим користувачам у разі потреби.

Для деяких підприємств управління інформаційною безпекою є більш ніж вимогою захисту конфіденційних внутрішніх документів та інформації про клієнтів. Залежно від галузі управління інформаційною безпекою існують юридичні вимоги для захисту конфіденційної інформації, яка надходить від клієнтів.

Підприємства, які збирають персоналізовані медичні записи або записи про медичне обслуговування, зобов'язані дотримуватися вказівок щодо конфіденційності та безпеки даних щодо перенесення та підзвітність медичного страхування. Організації, які обробляють платежі кредитними картками, несуть відповідальність за відповідність стандарту безпеки даних індустрії платіжних карток. Організації, які збирають персоналізовану інформацію від клієнтів, підпадають під загальний регламент про захист даних і можуть отримати тисячі або мільйони доларів штрафу за їх недотримання.

У період пандемії число віддалених працівників зростає в геометричній прогресії. Аналізуючи ландшафт кіберзагроз, виникає питання впливу домашніх пристроїв користувачів на загальну безпеку. В такій ситуації актуальними є два сценарія, таких як віддалений доступ і Bring your Own Device (BYOD). За даними Gallup [4], 43% зайнятих американців вже працюють віддалено, а це означає, що вони використовують свою власну інфраструктуру для доступу до ресурсів компаній. Посилює цю проблему зростання числа компаній, які дозволяють концепцію BYOD на робочому місці. Хоча існують способи безпечного впровадження BYOD, але біль-

шість збоїв в сценарії BYOD зазвичай відбувається через погане планування і мережну архітектуру, які призводять до небезпечної реалізації.

Спільного між усіма технологіями, згаданими вище є те, що керувати ними, потрібен користувач, і він як і раніше є головною метою для атаки. Люди - найслабша ланка в ланцюзі безпеки. З цієї причини старі загрози, такі як фішингові електронні листи, продовжують рости в обсязі, оскільки вони зачіпають психологічні аспекти користувача, спонукаючи його клікнути що-небудь, наприклад, додаток файлу або шкідливе посилання. Зазвичай, коли користувач виконує одну з цих дій, його пристрій заражається шкідливим ПЗ або до нього віддалено отримує доступ хакер.

Головним напрямом у процесі забезпечення інформаційної безпеки підприємства являється дотримання у таємниці комерційної інформації, що дозволяє підприємству успішно залишатися конкурентоспроможним на ринку товарів та послуг. Наслідком недотримання цих вимог стають проблеми у ділових справах; зриви переговорів з конкурентами, втрата вигідних контрактів; невиконання договірних зобов'язань тощо.

Для розв'язання проблем інформаційної безпеки підприємства необхідно створити підрозділ інформаційної безпеки, який входить до складу служби економічної безпеки підприємства. Цей підрозділ повинен підпорядковуватись вищому керівництву.

Отже, ефективний моніторинг безпеки та реагування є важливими аспектами програми управління інформаційною безпекою. Платформа хмарної аналітики дозволяє IT-організаціям легко збирати найновіші дані про загрози, налаштовувати сповіщення про загрози в реальному часі та автоматизувати реагування на інциденти у гібридних середовищах із розрізненими даними. Також моніторинг безпеки захищає від порушень даних, одночасно зменшуючи витрати на аудит і сприяючи дотриманню внутрішніх і зовнішніх стандартів безпеки та конфіденційності.

Література

1. Управління інформаційною безпекою [Електронний ресурс] – Режим доступу: https://studfile.net/preview/9650065/.

2. Система управління інформаційною безпекою як ключовий чинник успішності організації [Електронний ресурс] – Режим доступу: https://ua.ikmj.com/isms/.

3. Управління інформаційною безпекою підприємства для утримання конкурентних позицій на ринку [Електронний ресурс] – Режим доступу: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.

4. Система Управління інформаційною безпекою [Електронний ресурс] – Режим доступу: https://core.ac.uk/download/pdf/48401951.pdf.