Гарань Д.С., ст. гр. УФЕБ – 22 МЗ
Левченко А.О., кандидат економічних наук, професор
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

ОСНОВНІ ВИДИ ЗАГРОЗ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному суспільстві інформація стає найважливішим стратегічним ресурсом і головною продуктивною силою, що гарантує подальший розвиток суспільства. Тому інформація, як і інші традиційно існуючі ресурси, потребує особливого захисту. Крім терміну "захист інформації", широко використовується термін "інформаційна безпека". Захист інформації описує процес створення необхідних умов для забезпечення необхідної безпеки інформації, тоді як інформаційна безпека відображає стан, в якому ця безпека забезпечена.

Питання інформаційної безпеки досліджували О. Дзьобань, О. Довгань, І.Доронін, В. Гур'єв, Г. Ємельянов, В.Лопатін та ін.

Загрози, що виникають у сфері забезпечення інформаційної безпеки умовно можна поділити на два типи: природні та штучні. До природних належать природні явища, які цілком не залежить від людини, до них належать природні катаклізми, урагани, повені, пожежі тощо. Штучні ж загрози безпосередньо залежать від участі людини і, в свою чергу, можуть бути ненавмисними або навмисними. Прикладом ненавмисних загроз інформаційної безпеки може бути встановлене програмне забезпечення, що не входять до числа необхідного для роботи але зрештою порушує роботу системи, що може призвести до втрати інформації. Навмисні загрози, на відміну попередніх, створюються спеціально [2]. До навмисних загроз належать інформаційні атаки зловмисників як ззовні, так і зсередини компанії, що спрямовані на завдання репутаційної шкоди, втрату цінної інформації, втрати коштів, порушення комерційної таємниці та втрату інтелектуальної власності організації.

Порушення інформаційної безпеки може виникнути як внаслідок цілеспрямованих дій зловмисників, так і через недосвідченість працівників. Користувач повинен мати поінформованість та розуміння сутності щодо питань інформаційної безпеки та шкідливого програмного забезпечення, щоб уникнути нанесення шкоди не тільки підприємству, а і самому собі. Інциденти, такі як втрата або витік інформації, можуть бути результатом умисних дій працівників, які мають намір отримання грошової винагороди в обмін на цінні дані своєї організації.

Основними джерелами загроз є індивідуальні зловмисники («хакери»), кіберзлочинні групи та державні кіберпідрозділи, які використовують різноманітні кіберзасоби, згадані вище. Для проникнення через захист і отримання доступу до інформації вони використовують слабкі місця та помилки в програмному забезпеченні та веб-додатках, застосовують конфігураційні помилки мережевих екранів та налаштування прав доступу, здійснюють прослуховування каналів зв'язку та використовують клавіатурні шпигуни [1].

Оцінка загроз інформаційної безпеки повинна бути комплексною, оскільки методи оцінки відрізняються у кожному конкретному випадку. Наприклад, для запобігання втраті даних через несправність обладнання слід використовувати якісне обладнання, проводити регулярне технічне обслуговування та встановлювати стабілізатори напруги. Також важливо встановлювати та регулярно оновлювати програмне забезпечення, приділяючи особливу увагу захисному програмному забезпеченню, бази якого повинні оновлюватися щоденно.

Навчання співробітників компанії основним поняттям інформаційної безпеки та принципам роботи різних шкідливих програм допоможе уникнути випадкових витоків даних, виключити випадкове встановлення потенційно небезпечного програмного забезпечення на комп'ютер. Також як запобіжний засіб від втрати інформації слід робити

резервні копії. Для того, щоб стежити за діяльністю співробітників на робочих місцях та мати можливість виявити зловмисника, слід використовувати DLP-системи.

Здійснювати забезпечення інформаційної безпеки можна за допомогою спеціалізованих програм, що розроблені з використанням сучасних технологій. До таких програм належать: захист від DDoS; контроль привілейованих користувачів (PUM); захист від небажаного контенту (антивірус, антиспам, веб-фільтри, антишпигуни); аналіз вихідного коду; мережеві екрани та системи виявлення вторгнень (IPS); керування обліковими даними (IDM); захист веб-додатків (WAF); антифрод; захист від таргетованих атак; управління подіями безпеки (SIEM); системи виявлення аномальної поведінки користувачів (UEBA); захист АСУ ТП; захист від витоків даних (DLP); шифрування; захист мобільних пристроїв; резервне копіювання; системи відмовостійкості [3].

До основних видів загроз інформаційній безпеці відносяться:

1. Внутрішні збої чи відмова інформаційної системи.
2. Відмова підтримуючої інфраструктури.
3. До основних загроз у підтримуючій інфраструктурі відносяться:
4. Збій у роботі, пов'язаний з навмисним або випадковим виходом з ладу електричних систем, систем зв'язку, водопостачання, теплопостачання та кондиціювання.
5. Обвал, руйнування чи пошкодження будівель та споруд.
6. Невиконання обслуговуючим персоналом своїх посадових обов'язків, зумовлене страйками, збоями у роботі транспортних служб, аваріями, природними катаклізмами, терористичними актами тощо.
7. Загрози цілісності поділяють на загрози статичної та динамічної цілісності, а також загрози цілісності службової інформації та змістовних даних.

Службовою інформацією на підприємстві є паролі для доступу, маршрути передачі даних у локальній мережі та інша подібна інформація. Дуже часто протиправні дії та хакерські атаки здійснює особа, яка є співробітником компанії, яка володіє необхідним обсягом інформації про режим роботи та заходи захисту.

Одна з загроз, від яких дуже важко знайти ефективний спосіб захисту, – зловживання службовими повноваженнями. У багатьох системах передбачено надання доступу привілейованому користувачеві, яким може бути системний адміністратор, до всіх файлів та пошти будь-якого користувача.

Також збитки можуть бути завдані при сервісному обслуговуванні, тому що сервісний інженер отримує необмежений доступ і має можливість в обхід захисних бар'єрів підібратися до будь-якого файлу.

Література:

1. Довгань О.Д., Доронін І.М.. Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки: монографія / О.Д. Довгань, І.М. Доронін; НАПрН України, НДІІП К.: Видавничий дім «АртЕк». 2017. 107 с. URL: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf
2. Інформаційна безпека держави: навч. посіб. Для студ. спец. 6.170103 «Управління інформаційною безпекою» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ. безпека держ. New booklet 1.pdf?sequence=1&isAllowed=y
3. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2021. № 6 (червень). 261с - URL: http://ippi.org.ua/sites/default/files/2021-6.pdf