**Владислав Ткачик, Ірина Терещук**

**(Пирятин, Україна)**

**БЕЗПЕКА ІНФОРМАЦІЇ ПІДПРИЄМСТВА:**

**ОСНОВНІ ЗАГРОЗИ ТА ЗАСОБИ ЗАПОБІГАННЯ**

*Актуальність.* Всім відомий вислів «Хто володіє інформацією, той володіє світом». А хто володіє інформацією про конкурентів, отримує безпрецедентні переваги в боротьбі з ними. Прогрес зробив компанії залежними від інформаційних систем, а разом з цим - уразливими до атак кіберзлочинців, комп'ютерних вірусів, людського і державного фактору в такій мірі, що багато власників бізнесу вже не можуть відчувати себе в безпеці. Питання інформаційної безпеки стає наріжним каменем у діяльності організації, але цей же прогрес пропонує рішення, здатне захистити дані від зовнішніх зазіхань.

Будь-який витік інформації може призвести до серйозних проблем для компанії - від значних фінансових збитків до повної ліквідації. Звичайно, проблема витоків з'явилася не сьогодні, промислове шпигунство і переманювання кваліфікованих фахівців існували ще й до епохи комп'ютерної революції. Але саме з появою персональних комп'ютерів та інтернету виникли нові прийоми незаконного отримання інформації.

Якщо раніше для цього необхідно було вкрасти і винести з фірми цілі стоси паперових документів, то зараз величезні обсяги важливих відомостей можна запросто "злити на флешку", та заховати в кишеню. Також можна відправити викрадену інформацію за допомогою інтернет мережі, вдавшись до використання сімейства "руткітів", "троянів", "бекдор", "кейлоггеров" і "ботнетів", або просто знищити за допомогою вірусів, влаштувавши диверсію.

Причини загроз інформаційної безпеки

1. Неуважність і недбалість співробітників. Загрозу інформаційній безпеці компанії, як не дивно, можуть являти цілком лояльні співробітники які явно і не думають про крадіжку важливих даних. Ненавмисну шкоду конфіденційній інформації заподіюється з простої недбалості або непоінформованості працівників. Завжди є ймовірність того, що хто-небудь відкриє "фішингових лист" і впровадить вірус з особистого ноутбука на сервер компанії. Або, наприклад, скопіює файл з конфіденційною інформацією на планшет або флешку у відрядженні. І жодна компанія не застрахована від пересилання неуважним співробітником важливих файлів не за тією адресою. У такій ситуації інформація видається дуже легкою здобиччю.

**Прикладом цього є те як у 2010 році прототип смартфона iPhone 4 був залишений в барі одним із співробітників компанії Apple Греєм Пауеллом. До офіційної презентації гаджета залишалося ще кілька місяців, але знайшовший смартфон студент продав його за 5000 доларів журналістам Gizmodo, які зробили ексклюзивний огляд новинки [2].**

1. **Використання піратського програмного забезпечення. Іноді керівники компаній намагаються заощадити на придбанні ліцензійного програмного забезпечення. Але слід знати, що неліцензійні програми не дають захисту від шахраїв, зацікавлених в крадіжці інформації за допомогою вірусів. Володар неліцензійного програмного забезпечення не отримує технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками. За даними дослідження Microsoft, в семи відсотках вивчених неліцензійних програм було знайдено спеціальне програмне забезпечення для крадіжки паролів і персональних даних [3].**
2. **DDoS-атаки. Distributed-Denial-of-Service - «розподілена відмова від обслуговування» - це потік помилкових запитів від сотень тисяч географічно розподілених "хостів" (**хост - це **будь-який комп'ютерний пристрій, що має доступ до IP мережі), що блокують обраний ресурс одним з двох шляхів. Перший шлях - це пряма атака на канал зв'язку, який повністю блокується величезною кількістю непотрібних даних. Другий шлях - атака безпосередньо на сервер ресурсу. Недоступність або погіршення якості роботи публічних веб-сервісів в результаті атак може розтягуватися на досить тривалий час, від декількох хвилин до багатьох днів.**

**В кінці лютого 2017 року сервіс GitHub піддався атаці, і ця DDoS-атака стала найбільшою в історії — на піку трафік досягав 1,35 терабіт на секунду. Тепер, усього через кілька днів після цього, компанія Arbor Networks заявила про нову рекордну атаку на одного з американських інтернет-провайдерів. На цей раз трафік досягав вже 1,7 терабіт на секунду [1].**

1. **Віруси. Однією з найнебезпечніших на сьогоднішній день загроз інформаційної безпеки є комп'ютерні віруси. Це підтверджується багатомільйонним збитком, який несуть компанії в результаті вірусних атак. В останні роки істотно збільшилася їх частота і рівень шкоди. На думку експертів, це можна пояснити появою нових каналів проникнення вірусів. На першому місці як і раніше залишається електронна пошта, також віруси здатні проникати і через програми обміну повідомленнями. Збільшилася і кількість об'єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних веб-служб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори.**

**Останнім часом особливо активні стали так звані віруси-шифрувальники. Навесні і влітку минулого року мільйони користувачів постраждали від атак вірусів WannaCry, Petya, Petya 2.0, Misha. За інформацією Intel вірусом WannaCry заразилися 530 тисяч комп'ютерів, а загальний збиток компаній склав більше 1 млрд доларів [4].**

1. **Загрози з боку співвласників бізнесу. Саме легальні користувачі - одна з основних причин витоків інформації в компаніях. Такі витоку фахівці називають "інсайдерськими", а всіх "інсайдерів" умовно ділять кілька груп:**

* «Порушники» - середня ланка і топ-менеджери, що дозволяють собі невеликі порушення інформаційної безпеки - грають в комп'ютерні ігри, роблять онлайн-покупки з робочих комп'ютерів, користуються особистою поштою. Така недбалість здатна викликати інциденти, але частіше за все вони є ненавмисним. До речі, більшість зовнішніх атак відбуваються саме через особисті поштові скриньки або месенджери співробітників.
* «Злочинці». Найчастіше інсайдерами є топ-менеджери, які мають доступ до важливої інформації і зловживають своїми привілеями. Вони самостійно встановлюють різні додатки, можуть надсилати конфіденційну інформацію зацікавленим в ній третім особам і т.д.
* «Кроти» - співробітники, які навмисне крадуть важливу інформацію за матеріальну винагороду від компанії-конкурента. Як правило, це досить досвідчені користувачі, вміло знищують все сліди своїх злочинів. Спіймати їх в силу цього буває дуже складно.
* Ще одна категорія - це звільнені і скривджені компанію співробітники, які забирають з собою всю інформацію, до якої вони мали доступ.

1. Законодавчі перипетії. Державні органи безпеки та охорони порядку України наділені законним правом вилучати в ході перевірок обладнання та носії інформації. Оскільки велика частина важливих даних компанії зберігається в електронному вигляді на серверах, то в разі їх вилучення компанія на якийсь час просто зупиняє свою діяльність. Простої при цьому ніхто не компенсує, а якщо перевірка затягується, великі збитки можуть привести до припинення діяльності фірми. Вилучення обладнання - одна з найгостріших проблем сучасного бізнесу, при цьому приводом для нього може послужити все що завгодно - від рішення слідчого до рішення суду в рамках будь-якого кримінальної справи.

Методи захисту інформації

Хоча кількість загроз постійно зростає, з'являються все нові і нові віруси, збільшується інтенсивність і частота DDoS-атак, розробники засобів захисту інформації теж не стоять місці. На кожну загрозу розробляється нове програмне забезпечення або вдосконалюється вже наявне. Серед засобів інформаційного захисту можна виділити:

* Фізичні засоби захисту інформації. До них відносяться обмеження або повну заборону доступу сторонніх осіб на територію, пропускні пункти, оснащені спеціальними системами. Великого поширення набули HID-карти для контролю доступу. Наприклад, при впровадженні цієї системи, пройти в серверну або інше важливе підрозділ компанії можуть лише ті, кому такий доступ надано по протоколу.
* Базові засоби захисту електронної інформації. Це незамінний компонент забезпечення інформаційної безпеки компанії. До них відносяться численні антивірусні програми, а також системи фільтрації електронної пошти, що захищають користувача від небажаної або підозрілої кореспонденції. Корпоративні поштові скриньки обов'язково повинні бути обладнані такими системами, необхідна організація диференційованого доступу до інформації та систематична зміна паролів.
* Анти-DDoS. Грамотний захист від DDoS-атак власними силами неможливий. Багато розробники програмного забезпечення пропонують послугу анти-DDoS, яка здатна захистити від подібних загроз. Як тільки в системі виявляється "трафік" незвичайного типу або якості, активується система захисту, що виявляє і блокує його. При цьому коросний потік інформації надходить безперешкодно. Система здатна спрацьовувати необмежену кількість разів, до тих пір, поки загроза не буде повністю усунена.
* Створення резервних копій даних. Це рішення, що має на увазі зберігання важливої інформації не тільки на конкретному комп'ютері, але і на інших пристроях: зовнішньому носії або сервері. Останнім часом особливо актуальною стала послуга віддаленого зберігання різної інформації в «хмарі» дата-центрів. Саме таке копіювання здатне захистити компанію в разі надзвичайної ситуації, наприклад, при вилученні сервера органами влади.
* План аварійного відновлення даних. Крайній метод захисту інформації після втрати даних. Такий план необхідний кожній компанії для того, щоб в максимально стислі терміни усунути ризик простою і забезпечити безперервність бізнес-процесів. Якщо компанія з якихось причин не може отримати доступ до своїх інформаційних ресурсів, наявність такого плану допоможе скоротити час на відновлення інформаційної системи і підготовки її до роботи. У ньому обов'язково повинна бути передбачена можливість введення аварійного режиму роботи на період збою, а також всі дії, які повинні бути зроблені після відновлення даних. Сам процес відновлення слід максимально відпрацювати з урахуванням всіх змін системи.
* Шифрування даних при передачі інформації в електронному форматі (end-to-end protection). Щоб забезпечити конфіденційність інформації при її передачі в електронному форматі застосовуються різні види шифрування. Шифрування дає можливість підтвердити справжність інформації, що передається, захистити її при зберіганні на відкритих носіях, захистити програмне забезпечення і інші інформаційні ресурси компанії від несанкціонованого копіювання та використання.

Таким чином, в даній роботі розглянуті основні загрози та засоби запобігання загроз безпеки інформації підприємства. Описані в ній приклади не дають повної картини загроз, що можуть зашкодити підприємству та її власникам.

Людський розум та технічні засоби невпинно розвиваються і на кожен вид захисту з часом гарантовано з'явиться спосіб злому або проникнення. Саме тому захист інформації повинен здійснюватися комплексно, відразу по декількох напрямках. Чим більше методів буде задіяно, тим менша ймовірність виникнення загроз злому та витоку інформації, стійкіше положення компанії.

**Література:**

1. Найпотужніша DDoS-атака в історії [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://dt.ua.
2. Надо меньше пить [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://lenta.ru.
3. Нелицензионное программное обеспечение [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.microsoft.com.
4. WannaCry [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.microsoft.com.

**Науковий керівник:**

викладач Терещук Ірина Вікторівна.