УДК 004.056

Криловецький Б. С.
магістрант
Львівський державний університет безпеки життєдіяльності
Кухарська Н. П.
кандидат фізико-математичних наук, доцент
Львівський державний університет безпеки життєдіяльності

ПЕРСОНАЛ – ДЖЕРЕЛО ВНУТРІШНІХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Знаменитому британському політику XX століття Уїнстону Черчиллю належить геніальна фраза: “Хто володіє інформацією, той володіє світом”. У наші часи – часи жорсткої ринкової конкуренції, це твердження актуальне як ніколи. Питання збереження конфіденційності інформації зараз хвилює майже кожне підприємство незалежно від форми власності, обсягів і характеру виробництва або послуг, що надаються. Перешкодити витоку інформації є чи не найголовнішим завданням на сьогодні керівництва будь-якої компанії у різних частинах світу. Для кращого розуміння масштабності та важливості вирішення цієї проблеми подамо результати дослідження, проведеного у 2014 році незалежною і вельми авторитетною міжнародною організацією Ponemon Institute. Середня вартість у світі одного витоку інформації для компанії складає 3,5 млн. доларів [1].

Величезна кількість випадків, коли бізнесу було нанесено непоправні збитки, пов’язана з діями персоналу організації. Під час опитування Infosecurity Europe 2014 [2], ініційованого Британським інститутом стандартизації (BSI), 37 % респондентів заявили, що, на їх думку, основну небезпеку для бізнесу працедавця створюють внутрішні загрози, а саме нелояльна, а часом, навіть, і злочинна поведінка працівників організації. Службовців, які можуть завдати шкоди корпоративним інтересам, побоюються навіть більше, ніж кібератак:

15 % учасників цього ж опитування з насторогою ставляться до персональних мобільних “девайсів”, які працівники підприємства приносять з собою.

Згідно з результатами досліджень компанії SearchInform [3], сьогодні більше 55 % персоналу у країнах СНД і Прибалтики готові передати важливу для компанії конфіденційну інформацію конкурентам, журналістам або контролюючим органам. При цьому майже 20 % з них зможуть це зробити абсолютно безоплатно.

Крадіжки і продаж конфіденційної інформації, кримінальні дії з використання інфраструктури працедавця, розголошення інформації з обмеженим доступом, фальсифікація звітності, несанкціоновані комунікації з пресою і конкурентами, саботаж IT-інфраструктури організації, зговори з метою отримання відкотів, розкрадання інформаційних чи матеріальних активів працедавця, зловживання службовими повноваженнями, приховування правопорушень, – це неповний перелік інцидентів інформаційної безпеки (ІБ), напряму пов’язаних з персоналом підприємства.

Інцидентом за участю працівника організації (нападом, атакою) будемо називати подію, спричинену навмисним використанням (або невикористанням – бездіяльністю) працівником службових повноважень та (або) знань, що призвела (або з високою ймовірністю могла призвести) до негативних наслідків для організації.

До службових повноважень, які можуть бути використані працівником небажаним для організації чином, віднесемо такі:

- Доступ до конфіденційної, службової чи таємної інформації (наприклад, персональних даних, інформації, що становить комерційну, професійну чи банківську таємниці).
- Повноваження в рамках корпоративного управління (керівництво, планування, координація, контроль, узгодження, ініціатива щодо внесення змін, ознайомлення з документами та ін.).
- Доступ до інформаційних систем організації на різних рівнях: на рівні апаратного забезпечення, на рівні операційної системи, на мережевому рівні,

на рівні адміністрування прикладних програм і баз даних, на рівні користувача прикладних програм (за винятком систем загального доступу, таких як публічний веб-сайт, банкомати, термінали платіжної системи і т.п.).

– Фізичний доступ на об'єкти організації (доступ до засобів обробки інформації, зовнішніх носіїв інформації і т.д.).
– Використання телефонного, радіо та інших видів зв'язку з терміналів на території організації.
– Інші повноваження.

Зауважимо, використання працівниками службових повноважень та знань ІТ-середовища організації у цілях, що суперечать інтересам організації, є однією з найбільш небезпечних щодо можливих негативних наслідків загроз інформаційній безпеці організації. Практика показує, що дії власних працівників є вкрай непередбачуваними, так як вони, у порівняні з зовнішніми зловмисниками, мають значно більше можливостей для несанкціонованого доступу чи крадіжки інформації. Зокрема, внутрішні зловмисники потенційно володіють значними часовими ресурсами для отримання необхідних знань, підготовки і проведення атаки.

Різні загрози ІБ від персоналу не рівноймовірні між собою через те, що різним загрозам відповідають різні мотиви, різні можливості їх здійснення, різна привабливість результату для зловмисника. Разом з тим, основною причиною виникнення загроз ІБ від персоналу є конфлікт інтересів – приховане протиріччя між службовими обов'язками працівника перед організацією та його особистими інтересами.

Існує декілька підходів до класифікації внутрішніх зловмисників. Один з перших кроків у цьому напрямку зробила компанія IDC – постачальник досліджень і організатор конференцій в галузі інформаційних технологій. За версією IDC [4], екосистема внутрішніх порушників має чотири рівні:

“Громадяни” – лояльні службовці, які дуже рідко (якщо взагалі коли-небудь) порушують корпоративну політику і в основному не є загрозою безпеки.

“Порушники” – складають більшу частину персоналу організації. Ці

працівники дозволяють собі невеликі вольності, такі які: робота з персональної web-поштою, здійснення on-line покупок, гра в комп'ютерні ігри і т.д. Хоча такі дії і створюють загрозу інформаційній безпеці, проте інциденти, спричинені ними, є випадковими.

“Відступники” – працівники, які більшу частину робочого дня роблять те, що вони робити не повинні. Ці службовці зловживають привілеями в межах своєї компетенції, такими, наприклад, як доступ до корпоративних ресурсів, доступ до мережі Інтернет, право використання комп’ютера. Вони самовільно встановлюють P2P-клієнти і в подальшому використовують їх для передачі конфіденційної корпоративної інформації, зацікавленим в ній, зовнішнім адресатам. Таким чином, “відступники” створюють серйозну загрозу безпеці інформації.

“Зрадники” – службовці, які навмисно і регулярно піддають інформацію з обмеженим доступом небезпеці. Зазвичай, це вони роблять за фінансову винагороду від зацікавлених сторін. Такі працівники представляють найбільшу загрозу, їх складно викрити, так як вони доволі продумано і обережно чинять свої противоправні дії.

Література

1. Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis [Electronic resource]. – Access of mode : http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

2. Инсайдеры – главная угроза информационной безопасности бизнеса [Электронный ресурс]. – Режим доступа :http://ohrana.ru/articles/63829/

3. Человеческий фактор при утечке информации [Электронный ресурс] // F+S: технологии безопасности и противопожарной защиты. – 2014, №5. – С.70-71. – Режим доступа : www.security-info.com.ua

4. Равилов Д. Методы классификации внутренних нарушителей [Электронный ресурс] // infoCOM.UZ. – Режим доступа : http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/