УДК 004.56

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КОМП'ЮТЕРНИХ ІНЦЕДЕНТІВ НА ПІДПРИЄМСТВАХ

О. П. Войтович, к.т.н., доцент
Вінницький національний технічний університет
o_voytovych@mail.ru

Створення глобального інформаційного середовища принципово змінило технології використання інформаційних ресурсів та їх взаємозв'язок з діяльністю людини. Все частіше виникають ситуації пов'язані з витоками інформації, блокуванням ресурсів або порушенням цілісності інформації. Особливо небезпечними є кіберзлочини в галузі банківських технологій, де все більше послуг надаються через системи Інтернет-банкінгу, збільшуючи ризики для підприємств.

Щоб запобігти повторним порушенням, необхідно аналізувати кожен інцидент, виявляти причини, накопичувати статистику. Що спричинило інцидент? Через які слабкі місця у захисті відбулося порушення? Які сліди залишив зловмисник? Коли трапився інцидент? На подібні питання і повинні дати відповідь результати дослідження інциденту.

Питанням розслідування комп'ютерних інцидентів у інформаційно-комунікаційних системах, присвячено багато досліджень. Зокрема все більшого розвитку набуває напрямок розслідування комп'ютерних інцидентів – digital forensics. Створюються лабораторії та центри досліджень, розробляється спеціалізоване програмне та апаратне забезпечення.

Одним з важливих завдань розслідування комп'ютерних інцидентів є збереження цифрових доказів таким чином, щоб в подальшому залишилась можливість використання їх у суді. Проте часто вимога локалізації інциденту та зменшення шкоди, що завдається, вступає в конфлікт з бажанням виявити зловмисника. В політиці безпеки організації пріоритети повинні бути розставлені наперед.

Іншою причиною того, що злочин залишається нерозкритим є недостатнє протоколювання подій, що відбуваються у атакованій системі. Майже всі сучасні операційні системи та мережеві системи мають потужні модулі протоколювання подій, проте часто з необізнаності (або з інших причини) IT-спеціалісти не вмикають необхідних механізмів протоколювання чи просто дуже часто перезаписують журнали подій. Відсутність необхідного рівня протоколювання особливо небезпечно при мережевих та віддалених атаках, які стають все більшою загрозою при використанні технологій Інтернет-банкінгу. Навіть якщо факт порушення інформаційної безпеки було виявлено і знайдені сліди зловмисника, він залишається невідомим, оскільки мережеві журнали подій не записувалися.

Ще одна суттєва помилка – це недотримання елементарних правил інформаційної безпеки як то: надійна автентифікація всіх користувачів, контроль за програмних забезпеченням, яке встановленому на їхніх комп'ютерах, використання надійних та перевірених рішень безпеки тощо.

Порушення безпеки може статися на будь-якому підприємстві, проте чи буде знайдена його причина та ліквідована можливість подібних порушень в подальшому, залежить від правильного проведення комп'ютерного розслідування.