УДК 004.056.5
В. Гуменюк
Тернопільський національний технічний університет імені Івана Пулюя

РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

UDC 004.056.5
V. Humenuk
(Ternopil Ivan Puluj National Technical University, Ukraine)

RECOMMENDATIONS FOR IMPROVING EFFICIENCY OF RISK MANAGEMENT IN ENTERPRISE INFORMATION SECURITY

Безпека інформації в Україні набуває актуальності з кожним роком, не тільки великі компанії, але і невеличкі підприємства організовують системи інформаційної безпеки. Під поняттям інформаційної безпеки ми маємо на увазі забезпечення цілісності, доступності а також конфіденційності інформації компанії а також, інфраструктурних, комунікаційних, апаратних, і програмних засобів для обробки і зберігання інформації. Об’єктами посягань зловмисників можуть бути персональні дані, банківські дані, ключі, корпоративна інформація (промислове шпигунство, клієнтські бази, чат тощо). Інтересами зловмисника можуть бути навіть ті дані, які на перший погляд не несуть ніякої цінності оскільки зловмисники можуть організовувати складну та розгалужену систему, яка складається з багатьох елементів.

Номери телефонів, адреси, імена родичів, особисті дані також можуть бути використані зловмисниками, що використовують соціальну інженерію для реалізації загроз. Яскравим прикладом використання соціальної інженерії є масове телефонне шахрайство яке використовується як проти пересічних людей, так і малих і великих компаній і навіть публічних людей. Саме тому важливо організовувати регулярні семінари з інформаційної безпеки для персоналу організації.

Необхідно розробити ефективну систему обробки і зберігання інформації, яка буде захищена від стратегічних загроз. Насамперед керівництво компанії повинно зосередитись на наступних питаннях:

1. Створення політики безпеки інформації, визначення правил захисту інформації, забезпечення доступності та цілісності даних.
2. Розподіл повноважень серед персоналу організації, а також призначення відповідальних за них.
3. Оцінка загроз, виявлення загроз, які можуть порушити доступність, цілісність і конфіденційність інформації, підготовка детального аналізу загроз для кожного стратегічного елемента інформаційної системи.
4. Розробка плану на випадок реалізації загрози, визначення алгоритму конкретних дій та процедури для ліквідації загрози, а також наслідків пов’язаних з її реалізацією або спробою реалізації.
5. Розробка та впровадження системи управління інформаційною безпекою, що проходить відповідно до добре розробленого проекту.
6. Аналіз запропонованих заходів контролю їх реалізація.
7. Моніторинг ефективності використовуваної системи управління безпекою, систематичне оновлення компонентів системи.

Управління інформаційною безпекою є надто важливим, щоб можна було обмежувати діяльність професіями, пов'язаними лише з комп'ютерними технологіями, необхідний фахівець, який займається безпосередньо забезпеченням комплексної системи інформаційної безпеки, який зможе оцінити всі загрози і ризики, і організувати ефективну систему забезпечення безпеки інформації.