УДК 004.75

АНАЛІЗ ПІДХОДІВ ДО УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Цаволик Т.Г.[1)], Небесний І.В.[2)]
Тернопільський національний економічний університет
[1)]к.т.н., викладач, [2)]магістрант

І. Постановка задачі

Управління інцидентами - це важливий процес, який дозволяє компанії спочатку виявити інцидент, а потім запропонувати інструменти підтримки для їх вирішення якнайшвидше. Об'єктами системи моніторингу аварій є: обладнання (комутатори, маршрути, сканери, пристрої UTM); програмні системи (операційні системи, антивірусні шлюзи, персональні антивірусні системи, підсистеми обробки даних, наявні послуги та послуги); інформаційні ресурси, доступні в Інтернеті тощо); дії користувачів корпоративної мережі. Загалом система моніторингу поділяється на кілька рівнів прийняття рішень: на нульовому рівні спостереження здійснюється збір, обробка первинних даних, формування системи першого, другого та третього рівнів [1].

Робота на цих етапах виконується системним аналітиком для отримання експертної оцінки поточного стану та прогнозованого стану об’єктів моніторингу. На цих етапах динамічні знання системи реконструюються. На четвертому рівні особа, яка приймає рішення, на основі оцінок стану системи приймає рішення про дії керівництва щодо об'єктів системи спостереження та моніторингу.

ІІ. Мета роботи

Метою роботи є проведення аналізу підходів управління інцидентами інформаційної безпеки.

ІІІ. Управління інцидентами інформаційної безпеки

Основна складність управління інцидентами інформаційної безпеки полягає у відсутності налагодженої системи моніторингу інцидентів, оскільки часто відсутність інцидентів не означає, що система управління безпекою працює. правильно, коли інциденти не реєструються та не виявляються.

У багатьох організаціях не завжди можливо відстежити зміни кількості та характеру інцидентів інформаційної безпеки, оскільки не існує процедури управління інцидентами. Часто відсутність інцидентів не означає, що система управління безпекою працює належним чином, а просто, щоб інциденти не були вирішені або не виявлені. Загалом, основними труднощами, пов'язаними з управлінням інцидентами, є [2]:

- Визначення інциденту. У компанії немає техніки виявлення інцидентів, і працівники не знають, що таке інциденти. Це особливо важливо у випадку інцидентів інформаційної безпеки, коли вони не завжди перешкоджають нормальній роботі.

- Звіт про випадки. Часто працівники компанії не знають, хто і як повідомити про інцидент. Наприклад, формат звіту або список людей, які надсилають інциденти, не визначені.

- Запис інциденту. Відповідальні (навіть травмовані) люди часто не мають методології вирішення справ, яких немає в спеціальних журналах, або правил та строків.

- Усунути наслідки та причини інциденту. Як правило, організації не мають документально підтвердженого наказу, який би вказував дії щодо подолання наслідків та причин інциденту. В першу чергу така процедура повинна забезпечити, щоб вжиті заходи щодо усунення наслідків та причин інциденту не порушували процедуру розслідування: усунення наслідків інциденту не повинно "замітати сліди" ", щоб винуватців інциденту не вдалося ідентифікувати.

- Реалізація дій, покликаних унеможливлювати повторне виникнення інциденту.

Всі події, що порушують регламентовані процеси і можуть бути кваліфіковані як інциденти інформаційної безпеки, повинні стати основою для аналізу, який допоможе визначити їх характер, проявити системність і виробити рекомендації для вдосконалення системи ІБ, яка діє в компанії.

Висновок

У роботі проведений аналіз підходів до управління інцидентами інформаційної безпеки.

Список використаних джерел

1. European Network and Information Security Agency (ENISA) [Електронний ресурс]. – Режим доступу до ресурсу: http://www.enisa.europa.eu
2. Information technology. Security techniques. Information security management. Measurement : ISO/IEC 27004:2009 / International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2009. – 55 p.