УДК 004.056

В.В. Миронюк

ЦІЛІ ТА ЗАДАЧІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вінницький національний технічний університет

Анотація

Розглянуто основні цілі та завдання процесу управління інцидентами інформаційної безпеки та основні задачі інформаційно-аналітичної служби.

Ключові слова: інцидент інформаційної безпеки, інформаційно-аналітична служба.

Abstract

The main purposes and problems of the information security incident management process are considered. Also the main targets of informational-analytical service are considered.

Keywords: incident of information security, informational-analytical service.

Вступ

Жоден найдосконаліший захід, спрямований на зменшення ризиків інформаційної безпеки - досконало відпрацьована політика або найсучашніший міжмережевий екран не може гарантувати неможливість виникнення в інформаційному середовищі подій, що потенційно несуть загрозу організації. Складність та різноманітність середовища діяльності сучасного бізнесу зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також існує ймовірність реалізації нових, невідомих дотепер, загроз інформаційній безпеці.

Таким чином, будь-якій організації, що серйозно ставиться до питань забезпечення інформаційної безпеки (ІБ), необхідно вирішити такі завдання [1]:

- виявлення, інформування та облік інцидентів інформаційної безпеки(ІІБ);
- реагування на ІІБ, зокрема застосування необхідних засобів для запобігання, зменшення і відновлення після заданого збитку;
- аналіз ІІБ, що відбулися, з метою планування превентивних заходів захисту і поліпшення процесу забезпечення інформаційної безпеки в цілому.

Процес управління інцидентами інформаційної безпеки (УІІБ) покликано забезпечити підприємство можливістю своєчасного виявлення інциденту та якомога швидшого реагування на нього за допомогою коректно обраних засобів підтримки.

Цілі та задачі управління інцидентами інформаційної безпеки

Основною задачею УІІБ можна визначити оперативне відновлення нормальної роботи підприємства і звести до мінімуму негативний вплив інциденту на діяльність організації з метою підтримки якості і доступності служб (сервісів) на максимально можливому рівні.

Цілі управління інцидентами:

- відновлення нормальної роботи служб в найкоротші терміни;
- зведення до мінімуму впливу інцидентів на роботу організації;
- забезпечення злагодженої обробки всіх ІІБ і запитів обслуговування;
- зосередження ресурсів підтримки на найбільш важливих напрямках;
- надання відомостей, які роблять можливим оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління.

Управління інцидентами інформаційної безпеки – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються інформаційних систем, а на виході цих процесів отримують інформацію про причини інциденту,

що відбувся, про збиток, нанесений організації, і заходи, які необхідно вжити для того, щоб інцидент не повторився у майбутньому. Таким чином, УІІБ спрямовано на вдосконалення системи забезпечення безпеки підприємства. Крім того, одержувані на виході дані є, по суті, єдиною об'єктивною інформацією для визначення ймовірності загроз при аналізі ризиків.

Специфічні питання УІІБ розглядаються та регламентуються такими міжнародними та національними нормативними документами [1]: ISO 20000, ISO/IEC 27001, ISO/IEC 27035, CMU/SEI-2004-TR-015, NIST SP 800-16, ITU-T X-1051, ITU-T E.409, ГОСТ Р ІСО/МЕК 18044.

Також необхідно усвідомлювати, що УІІБ не запобігає нанесенню збитку компанії (як правило, компанія вже понесла збиток, пов'язаний з інцидентом), проте розслідування інциденту і своєчасне впровадження превентивних та корегувальних заходів знижує ймовірність його повторення. Можна відзначити, що статистика інцидентів інформаційної безпеки має особливу цінність для компанії як показник ефективності функціонування системи управління інформаційною безпекою.

Статистика інцидентів може використовуватись для рішення базових задач інформаційно-аналітичної служби (ІАС) на рівні підприємства і держави. Базовими задачами ІАС є [2]:

- забезпечення своєчасного надходження надійної та всебічної інформації з поставленого питання;
- опис сценарія дій конкурентів, котрі можуть зачіпати поточні інтереси фірми;
- здійснення постійного моніторингу подій у зовнішньому конкурентному середовищі та на ринку, котрі можуть мати значення для інтересів фірми;
- забезпечення безпеки власних інформаційних ресурсів;
- забезпечення ефективності та виключення дублювання при зборі, аналізі та розповсюдженні інформації.

В концептуальному відношенні інформаційно-аналітична діяльність повинна представляти собою єдину систему аналізу, контролю та прогнозування зовнішньої та внутрішньої ситуації на підприємстві. Всі напрямки аналітичної роботи повинні бути пов'язані деякою логікою взаємодії.

Висновки

З часом, у процесі розширення сфери використання інформаційних систем та їх ускладнення, проблема забезпечення інформаційної безпеки загострюється. Безпеку вже неможливо забезпечити одним лише набором технічних засобів і підтримувати тільки силами підрозділу безпеки. Саме тому з'являється необхідність у впровадженні ІАС, яка покликана бути єдиною та взаємопов'язаною структурою забезпечення підприємства достовірною та аналітично підготовленою інформацією, що використовується для прийняття ефективних рішень з усіх напрямків безпеки бізнесу.

Забезпечення безперервності функціонування бізнесу в критичних ситуаціях є однією з фундаментальних складових його успішності. Тому можна відзначити, що надання відомостей, які роблять можливим оптимізувати процеси підтримки управлінських рішень, зменшити кількість інцидентів і спланувати управління інформаційною безпекою, є одним з найважливіших аспектів захисту інформаційного середовища підприємства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки. / О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. НА СБ України, 2014. - 190с.

2. Ярочкин В.И. Корпоративная разведка / В.И. Ярочкин, Я.В. Бузанова, М.: Ось-89, 2004, с. 127

Миронюк Віталій Володимирович — аспірант кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: vitmir1001@gmail.com

Науковий керівник: ***Дудатьєв Андрій Веніамінович*** — канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: dudatyev.av@gmail.com

Mironyuk Vitaliy V. — postgraduate student, Department of Chair Information Protection, Vinnytsia National Technical University, Vinnytsia, email : vitmir1001@gmail.com

Supervisor: ***Dudatyev Andriy V.*** — Cand. Sc. (Eng.), Associated Professor of Chair Information Protection, Vinnytsia National Technical University, Vinnytsia