DOI: 10.6084/m9.figshare.9788483
УДК 681.324-75

Гордієнко Сергій Борисович
Кандидат технічних наук, доцент, завідувач кафедри Навчально-наукового інституту інформаційної безпеки
Національна академія Служби безпеки України, Київ
Манько Олександр Олексійович
Доктор технічних наук, професор
Одеська національна академія зв'язку ім. О.С. Попова, Одеса
Скубак Олександр Миколайович
Кандидат технічних наук, доцент, доцент кафедри Навчально-наукового інституту інформаційної безпеки
Національна академія Служби безпеки України, Київ
Харлай Людмила Олексіївна
Кандидат технічних наук
Київский коледж зв`язку, Київ

ПИТАННЯ БЕЗПЕРЕРВНОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. *Розглянуто актуальні питання безперервності функціонування інформаційних систем, що дає організаціям інструменти управління та процедури, які дають змогу контролювати широкий діапазон інцидентів та вразливостей. Визначені пріоритетні принципи, яких необхідно дотримуватись під час організації процесу реагування на інциденти, а також актуальні питання впровадження процедури управління безперервністю бізнесу на основі управління інформаційними інцидентами. Здійснено аргументацію питань сертифікації системи управління безперервністю бізнесу, яка є частиною загальної системи управління організацією та забезпечує супровід і удосконалення процесів забезпечення безперервності бізнесу (діяльності) організації.*

Ключові слова: інформаційні технології; інформаційна безпека; управління інцидентами; реагування на інциденти інформаційної безпеки; безперервність бізнесу

Вступ

У міру розширення сфери використання інформаційних систем і їх ускладнення, загострюється проблема забезпечення інформаційної безпеки (ІБ). Ігнорування проблем ІБ, практика «латання дірок» на сьогодні можуть обійтися компанії дуже дорого. Разом з тим, в більшості компаній організаційна складова системи ІБ опрацьована слабо.

Ще одна гостра проблема у сфері захисту даних пов'язана із забезпеченням безперервності функціонування інформаційних систем.

Наприклад, дані, як такі, часто не класифіковані, тобто компанія не має чіткого уявлення про те, які у неї є типи даних з позицій їх конфіденційності, критичності для бізнесу. А це тягне за собою цілий ряд проблем, починаючи від складнощів в обґрунтуванні адекватності заходів щодо захисту інформації та закінчуючи неможливістю при виникненні інциденту використовувати правові методи їх розслідування.

Для багатьох сучасних компаній, передусім фінансових організацій, виробничих холдингів, великих дистриб'юторів безперебійна робота інформаційних систем, що підтримують основний бізнес, і доступність даних стають критичним питанням. Збої в роботі систем призводять до переривання бізнес-процесів і відповідно до невдоволення клієнтів, штрафів та інших втрат.

Вирішити ці питання можна шляхом побудови ефективної системи управління інформаційною безпекою.

Порушення у сфері інформаційної безпеки можуть ставити під загрозу функціонування бізнес-систем і порушувати роботу бізнесу.

Впровадження інформаційних технологій привело до того, що істотно змінилися підходи до організації сучасних економічних процесів. Безперечні переваги, які несуть в собі ІТ, дали змогу не тільки вести бізнес більш ефективно, але й автоматизувати функціональні процеси [1].

Однак активне застосування інформаційних технологій зумовило ризики, з якими багато хто до цього не стикалися і навіть не знали про їх існування. З приходом високих технологій у світ бізнесу однією з найважливіших загроз є втручання кіберзлочинців в роботу установ різної сфери діяльності.

Існує значний перелік різних інцидентів інформаційної безпеки. Серед найбільш поширених відомі такі: DDoS-атаки (поширені атаки типу «відмова обслуговування»), шахрайство в системах дистанційного обслуговування, злам серверів і крадіжка конфіденційної інформації, витік важливих корпоративних даних, атака на репутацію шляхом розміщення наклепницької інформації в Інтернеті. Кожен з цих інцидентів наклав негативний відбиток на діяльність постраждалих компаній.

Постановка задачі

У зв'язку з активізацією діяльності комп'ютерних злочинців і прогнозованим зростанням кількості внутрішніх і зовнішніх інцидентів як в світі, так і в Україні перед службами інформаційної безпеки в організаціях гостро постає питання створення і послідовного застосування правил реагування на випадки порушення інформаційної безпеки та безперервності функціонування інформаційних систем.

Від підготовленості, своєчасності та ефективності реагування на інциденти інформаційної безпеки може залежати, чи виллється інцидент в незначну подію або стане катастрофою для бізнесу. Застосування системи управління інцидентами інформаційної безпеки дасть організаціям інструменти управління і процедури, що дадуть змогу контролювати широкий діапазон інцидентів і вразливостей [2].

Негативні наслідки широкого кола загроз інформаційній безпеці (починаючи від атак хакерів і закінчуючи діями інсайдерів, які використовують свої знання і права доступу до даних компанії для своєї вигоди) можна зменшити, використовуючи підхід до управління інцидентами інформаційної безпеки, описаний в міжнародному стандарті ISO / IEC 27035 : 2011.

Виклад основного матеріалу

Управління інцидентами в системі забезпечення ІБ

Управління інцидентами – одна з найважливіших процедур управління інформаційною безпекою.

Основне завдання процесу управління інцидентами ІБ – підвищення рівня захищеності інформаційної системи компанії, а також її інформаційних ресурсів.

Саме цей процес допомагає зрозуміти недоліки процесів і контролю, отримати вихідні дані для розроблення планів відновлення безперервності бізнесу і визначити ключові ролі персоналу в разі виникнення нештатних ситуацій.

Таким чином, будь-якій організації, яка серйозно відноситься до питань забезпечення інформаційної безпеки, необхідно реалізувати комплексний підхід до вирішення таких завдань:

– виявлення, інформування та облік інцидентів інформаційної безпеки;

– реагування на інциденти інформаційної безпеки, включно із застосуванням необхідних засобів для запобігання, зменшення і відновлення завданих збитків;

– аналіз інцидентів з метою планування превентивних заходів захисту і поліпшення процесу забезпечення інформаційної безпеки в цілому.

Насамперед важливо правильно і своєчасно усунути наслідки інциденту, а також мати можливість проконтролювати, які дії були виконані для цього.

Необхідно також розслідувати інцидент, що включає визначення причин його виникнення, винних осіб і конкретних дисциплінарних стягнень.

Далі, як правило, слід зробити оцінку потреби в діях щодо усунення причин інциденту, якщо потрібно – реалізувати їх, а також виконати дії щодо попередження повторного виникнення інциденту.

Крім того, важливо зберігати всі дані про інциденти інформаційної безпеки, оскільки статистика інцидентів інформаційної безпеки допомагає усвідомлювати їх кількість і характер, а також зміни в часі.

За допомогою інформації про статистику інцидентів можна визначити найбільш актуальні загрози для компанії і відповідно максимально точно планувати заходи щодо підвищення рівня захищеності інформаційної системи компанії.

При організації процесу реагування на інциденти в будь-який нештатній ситуації, в порядку пріоритету, слід дотримуватися таких принципів:

1. Безпека співробітників і відвідувачів;
2. Стримування інциденту і мінімізація шкоди;
3. Безпека активів організації;
4. Безпека інформаційних ресурсів;
5. Відновлення відповідно до вимог бізнесу;
6. Розслідування інциденту;
7. Вживання заходів щодо недопущення повторення інциденту.

Ці сім очевидних кроків – сім важливих правил, яких слід дотримуватися, щоб ефективно побудувати процеси управління інцидентами інформаційної безпеки.

Реагування на інциденти

Своєчасне та ефективне реагування на інциденти в системі безпеки є надзвичайно важливим для мінімізації потенційного впливу таких інцидентів на репутацію організації.

Як правило, про виникнення інцидентів в системі інформаційної безпеки компанії намагаються не заявляти відкрито, щоб не дискредитувати себе і не давати додаткову "зброю" конкурентам або кримінальним структурам, які останнім часом проявляють підвищений інтерес до можливостей інформаційних технологій. В результаті, хоча кількість інцидентів ІБ стає дедалі більше, відомості про них, як правило, тримаються в секреті, а ми дізнаємося лише про ті нечисленні інциденти, інформація про які "просочилася" в пресу.

Зворотний бік такої інформаційної непрозорості – труднощі пошуку фахівців, які могли б провести роботи з розслідування інцидентів або вибудовування в компанії процесу реагування на інциденти.

Першопричиною настання події інциденту інформаційної безпеки є потенційна здатність зловмисника отримати необгрунтовані привілеї для доступу до активу організації. Оцінити ризик подібної можливості і прийняти правильне рішення про захист, становить основну задачу команди реагування [3].

Кожен ризик повинен бути пріоритезований і оброблений відповідно до політики оцінки ризиків прийнятої в організації. Оцінка ризиків розглядається як перманентний процес, метою якого є досягнення прийнятного рівня захисту, іншими словами, повинні бути впроваджені достатні заходи захисту активу від необґрунтованого або неправомірного використання. Оцінка ризиків сприяє класифікації активів. Критичні, з точки зору ризиків, активи здебільшого також є критичними для бізнесу організації.

Реалізація проекту управління безперервністю бізнесу

Процедура реагування на інциденти інформаційної безпеки є одним з основних джерел даних для аналізу стану впровадження процедур управління безперервністю бізнесу на основі управління інформаційними інцидентами [3].

Управління безперервністю бізнесу (Business Continuity Management або BCM) – бізнес-процес, який відповідає за управління ризиками, які можуть серйозно вплинути на бізнес. BCM захищає інтереси ключових зацікавлених сторін, репутацію, бренд і діяльність зі створення цінності. Процес BCM включає в себе зниження ризиків до прийнятного рівня і планування способів відновлення бізнес-процесів в разі порушення бізнесу. BCM встановлює цілі, охоплення і вимоги по відношенню до управління безперервності IT-послуг.

Головним питанням реалізації проекту управління безперервністю бізнесу є План забезпечення безперервності бізнесу (Business Continuity Plan або BCP), який складається з Планів забезпечення безперервності послуг та Планів відновлення послуг і визначає кроки, необхідні для відновлення бізнес-процесів в разі порушення їх функціонування.

План також повинен містити інформацію про події, які є підставою для його ініціювання; людей, які повинні бути задіяні в реалізації плану; засоби комунікацій і т.п. [1]

Управління безперервністю послуг фокусується на значущих негативних подіях, які ITIL називає "катастрофами" для бізнесу. Менш значущі події розглядаються в рамках процесу управління інцидентами. Те, чи є якась конкретна подія катастрофою, залежить від організації, в якій вона відбулася. Розмір і значущість негативного впливу події на бізнес, наприклад, фінансові втрати або втрата репутації, вимірюється в рамках Аналізу впливу на бізнес. Аналіз впливу на бізнес визначає мінімальні вимоги до критичності.

В рамках управління безперервністю послуг повинні виконуватись такі основні дії:

1. Аналіз впливу на бізнес для кількісної оцінки впливу втрати послуги на бізнес;
2. Аналіз ризиків – ідентифікація та оцінка ризиків з метою визначення потенційних загроз безперервності і оцінки ймовірності їх здійснення;
3. Формування планів забезпечення безперервності, інтегрованих в плани BCM.
4. Тестування планів забезпечення безперервності;
5. Безперервне здійснення планів і управління ними.

У світовій практиці існують компанії, які проводять повний цикл робіт зі створення систем управління безперервністю бізнесу відповідно до вимог стандартів і чинного законодавства, включаючи їх подальшу сертифікацію і реєстрацію в авторитетних міжнародних органах зі сертифікації систем менеджменту.

Система управління безперервністю бізнесу (СУББ) являє собою частину загальної системи управління організацією, що забезпечує створення, впровадження, експлуатацію, моніторинг, аналіз, супровід і вдосконалення процесів забезпечення безперервності бізнесу (діяльності) організації. СУББ включає в себе організаційну структуру, політики, процеси планування і управління, обов'язки, процедури і ресурси.

Найважливішою складовою сучасної СУББ є система управління безперервністю інформаційно-технологічних сервісів (БІТС), що являє собою сукупність політик, стандартів, процесів та інструментів, за допомогою яких компанії не тільки покращують свої можливості з реагування на серйозні відмови систем, але і підвищують здатність

до відновлення після серйозних інцидентів таким чином, щоб запобігти відмові критично важливих систем і сервісів. Управління БІТС спрамовано на оброблення ризиків, здатних надати раптовий серйозний вплив, піддаючи безперервність бізнесу безпосередній загрозі [4].

Під сертифікацією СУББ організації за вимогами британського стандарту BS 25999-2: 2007 розуміється комплекс організаційно-технічних заходів, що проводяться незалежними акредитованими аудиторами, в результаті яких підтверджується наявність та належне функціонування рекомендованих Стандартом механізмів забезпечення безперервності бізнесу, оцінюється повнота і правильність їх реалізації, а також їх адекватність потребам організації та існуючих ризиків.

Сертифікат відповідності BS 25999-2, виданий уповноваженим і авторитетним органом, є важливим показником надійності організації і високого ступеня захищеності її активів і бізнес-процесів у разі інцидентів і порушень нормального ходу діяльності.

Сертифікація СУББ за вимогами BS 25999-2 дає змогу підвищити ступінь привабливості організації на внутрішньому і зовнішньому ринках, сприяє формуванню сприятливого іміджу в очах клієнтів, партнерів, акціонерів, аудиторів, державних регулюючих органів; сприяє розширенню сфери діяльності організації на міжнародному рівні. Наявність цього сертифіката є серйозною конкурентною перевагою при участі в тендерах, а також при прийнятті рішення про вибір ділового партнера, підрядника, постачальника продуктів або послуг.

Процедура сертифікації чинить серйозний мотивуючий і мобілізуючий вплив на персонал компанії: підвищується рівень обізнаності співробітників, ефективніше виявляються і усуваються недоліки і невідповідності, що сприяє підвищенню стратегічної і тактичної здатності організації планувати свої дії і реагувати на інциденти і порушення нормального ходу діяльності з метою продовження бізнес-операцій на прийнятному рівні. Сертифікація СУББ є добровільною процедурою [5 – 9].

Висновки

Відповідно до положень ДСТУ ISO/IEC 27001:2015 (Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги), а також багатьох інших стандартів, управління безперервністю бізнесу та управління інцидентами є одними з основних областей контролю і необхідною складовою будь-якої системи менеджменту інформаційної безпеки. Хоча ці галузі контролю виходять далеко за рамки питань інформаційної безпеки (ІБ є для них лише однією зі складових), вибудовувати відповідні процеси в організаціях часто доводиться саме фахівцям з ІБ, часом значно розширюючи межі своєї професійної компетенції і посадових повноважень. В цьому випадку інформаційна безпека стає основним двигуном процесів забезпечення безперервності бізнесу, формуючи методологічну базу для оцінки ризиків та аналізу впливу на бізнес надзвичайних ситуацій, управління інцидентами, розробки стратегії, політики і планів забезпечення безперервності інформаційно-комунікаційних технологій і бізнесу в цілому, розробки та підтримки в актуальному стані контакт-листів, аварійно-відновлювальних процедур, реєстрів інформаційних та ІТ-активів і т.п.

Створювана таким чином система управління безперервністю бізнесу стає похідною від наявної системи управління інформаційною безпекою організації, наслідуючи від останньої відповідні принципи управління і механізми контролю.

Це, звичайно, не означає, що відповідальність за безперервність бізнесу та управління надзвичайними ситуаціями тепер покладається на фахівців з інформаційної безпеки. Для цього потрібно інший рівень компетенції і повноважень.

Список літератури

1. Гладиш С. В., Кононович В. Г., Тардаскін М. Ф. Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування // Зв'язок. – 2007. – № 8. – С. 28–31.

2. Гладиш С.В. Інтелектуальна система керування інцидентами інформаційної безпеки телекомунікаційних мереж // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та інформаційна безпека в науці, техниці та освіті ІНФОТЕХ-2007». – Севастополь: СевНТУ, 2007. – С. 53–57.

3. Гладиш С.В. Реагування та обробка інцидентів інформаційної безпеки в мережі GSM //

4. Вісник Державного університету інформаційно-комунікаційних технологій. – 2008. – № 1. – С. 58–72.

5. Коробко В.В., Скоропаденко А.П., Задоя Г.М., Вовк В.М. Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты // Зв'язок.— 2004. – № 1. – С. 39–45.

6. Сакович Л.М., Політов В.І. Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку // Зв'язок. – 2000. – № 5. – С. 37–39.

7. ISO/IEC TR 18044:2004. Information technology Security techniques Information security incident management.

8. ISO/IEC 27001:2005. Information technology Security techniques Information security management systems Requirements.

9. ISO/IEC 17799:2005. Information technology Security techniques Code of practice for information security management.

10. Гордієнко С.Б. Аналіз доцільності реалізації заходів щодо забезпечення інформаційної безпеки [Текст] / С.Б. Гордієнко, О.О. Манько, В.О. Манько, О.М. Скубак // Управління розвитком складних систем. – 2018. – № 36. – С. 89 – 94.

Стаття надійшла до редколегії 11.03.2019

Гордиенко Сергей Борисович
Кандидат технических наук, доцент, заведующий кафедрой Учебно-научного института информационной безопасности
Национальная академия Службы безопасности Украины, Киев
Манько Александр Алексеевич
Доктор технических наук, профессор
Одесская национальная академия связи им. А.С. Попова, Одесса
Скубак Александр Николаевич
Кандидат технических наук, доцент, доцент Учебно-научного института информационной безопасности
Национальная академия Службы безопасности Украины, Киев
Харлай Людмила Алексеевна
Кандидат технических наук
Киевский колледж связи, Киев

ВОПРОСЫ НЕПРЕРЫВНОСТИ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. *Рассматрены актуальные вопросы непрерывности функционирования информационных систем, которые дают организациям инструменты управления и процедуры, позволяющие контролировать широкий диапазон инцидентов и уязвимостей. Определены приоритетные принципы, которых необходимо придерживаться при организации процесса реагирования на инциденты. Определены актуальные вопросы внедрения процедуры управления непрерывностью бизнеса на основе управления информационными инцидентами. Осуществлена аргументация вопросов сертификации системы управления непрерывностью бизнеса, которая является частью общей системы управления организацией и обеспечивает сопровождение и усовершенствование процессов обеспечения непрерывности бизнеса (деятельности) организации.*

Ключевые слова: информационные технологи; информационная безопасность; управление інцидентами; реагирование на инциденты информационной безопасности; непрерывность бизнеса

Gordienko Sergey Borisovich
PhD (Eng.), Associate Professor, Associate Professor of the Educational and Scientific Institute of Information Security
National Academy of Security Service of Ukraine, Kyiv
Manko Alexander Alexeyevich
DSc (Eng.), Professor of Odessa National Academy of Telecommunications named O.S. Popov
Odessa National Academy of Telecommunications named O.S. Popov, Kyiv
Skubak Alexander Nikolaevich
PhD (Eng.) Associate Professor, Associate Professor of the Educational and Scientific Institute of Information Security
National Academy of Security Service of Ukraine, Kyiv
Kharlai Liudmila Alekseevna
PhD (Eng.)
Kyiv College of Communicacion, Kyiv

ISSUES THE CONTINUITY OF INFORMATION SYSTEMS FUNCTIONING

Abstract. *This article deals with current issues of the continuity of information systems. It provides organizations management tools and procedures to control a wide range of incidents and vulnerabilities. Priority principles have been identified that must be followed when organizing an incident response process. Current issues of implementing of the business continuity*

management procedure are identified. It based on the information incident management. The reasoning of the issues of certification of the Business Continuity Management System has been implemented. This system is part of the overall management of the organization and provides support and improvement of the processes of ensuring the continuity of the business (activity) of the organization.

Key words: information technology; information security; incident management; response to information security incidents; business continuity

References

1. Gladysh, S.V., Kononovich, V.G., Tardaskin, M.F. (2007). Distribution of Responsibility for Reaction and Processing of safety incidents in the Information and Telecommunication Network of Public Use. Communication, 8, 28 – 31. (in Ukrainian)

2. Gladysh, S.V. (2007). Intelligent system for information security incident management of telecommunication networks. Materials of the international scientific-practical conference "Information Technologies and Information Security in Science, Technology and Education INFOTECH-2007". Sevastopol: SevNTU, p. 53 – 57. (in Ukrainian)

3. Gladysh, S.V. (2008). Reaction and processing of information security incidents in the GSM network. Bulletin of the State University of Information and Communication Technologies, 1, 58 – 72. (in Ukrainian)

4. Korobko, V.V., Skoropadenko, A.P., Zadoya, H.M., Vovk, V.M. (2004). Integrated system for collecting information on extreme states of telecommunication networks and their protection. Communication, 1, 39 – 45. (in Russian)

5. Sakovych, L.M., Politov, V.I. (2000). Use of decision support system during operation and repair of communication facilities and equipment. Communication, 5, 37 – 39. (in Ukrainian)

6. ISO/IEC TR 18044:2004. Information technology Security techniques Information security incident management.

7. ISO/IEC 27001:2005. Information technology Security techniques Information security management systems Requirements.

8. ISO/IEC 17799:2005. Information technology Security techniques Code of practice for information security management.

9. Gordienko, Sergij, Manko, Olexandr, Manko, Volodimir & Skubak, Olexandr, (2018). Analysis of advisability of implementation of means. Management of Development of Complex Systems, 36, 89 – 94.

Посилання на публікацію

APA *Gordienko, Sergij, Manko, Olexandr, Skubak, Olexandr & Kharlai, Liudmila. (2019). Issues of the continuity of information systems functioning. Management of Development of Complex Systems, 38, 76 – 81, dx.doi.org\10.6084/m9.figshare.9788483.*

ДСТУ *Гордієнко С.Б. Питання безперервності функціонування інформаційних систем [Текст] / С.Б. Гордієнко, О.О. Манько, О.М. Скубак, Л.О. Харлай // Управління розвитком складних систем. – 2019. – № 38. – С. 76 – 81, dx.doi.org\10.6084/m9.figshare.9788483..*