УДК 004.056
DOI: 10.31673/2409-7292.2020.042832

Запорожченко М.М.

АНАЛІЗ ТА ВИЗНАЧЕННЯ СПОСОБІВ ЗМЕНШЕННЯ КРИТИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одною з ключових вимог для захисту інформаційних активів організації є забезпечення належного управління ризиками інформаційної безпеки. В процесі управління ризиками мають здійснюватися їх ідентифікація, оцінка, аналіз та обробка з метою зміни значення ризику до прийнятного рівня. В статті пропонується розглянути способи зменшення інформаційних ризиків, що можуть бути викликані критичними категоріями загроз та вразливостей.

Ключові слова: управління ризиками інформаційної безпеки, обробка ризиків, зменшення ступеня інформаційних ризиків.

Вступ

Зі зростанням кількості загроз інформаційної безпеки зростає і залежність бізнесу від вдалого управління ризиками, викликаними цими загрозами. Адже своєчасне та правильне прийняте керівництвом рішення стосовно необхідних заходів впливу на ризики дозволить мінімізувати втрати, яких може зазнати організація. Отже, діяльність, спрямована на зменшення ступеня ризиків інформаційної безпеки, в сучасних умовах є актуальною і вкрай необхідною для більшості організацій. Процес управління ризиками повинен бути інтегрований в основні процеси діяльності організації та повинен бути задіяний в процесі прийняття управлінських рішень. Ризик-менеджмент повинен бути невід'ємною частиною цілей організації, корпоративного управління, лідерства та відповідальності, стратегії, задач і діяльності організації та не повинен відокремлюватися від них. Сам процес управління ризиками інформаційної безпеки складається з декількох етапів і є ітеративним. Етапами процесу ризик-менеджменту є встановлення контексту, оцінка ризику, його обробка та прийняття. На всіх етапах процесу може проводитися комунікація та моніторинг ризику.

Після того, як ризики були оцінені та результати оцінки достатні та задовільні для продовження процесу, проводиться етап обробки ризиків. Він передбачає наявність переліку ризиків з призначеними пріоритетами відповідно до критеріїв оцінки небезпечності ризиків. Метою даного етапу є вибір стратегії обробки ризиків. Зменшення ступеня інформаційних ризиків є однією зі стратегій обробки ризиків. Вона полягає в тому, що ризик повинен бути зменшений за допомогою заходів і засобів контролю й управління таким чином, щоб залишковий ризик при наступній ітерації процесу управління ризиками був оцінений як допустимий. Характеристики ризиків, такі як ймовірність реалізації загрози та (або) величина втрат внаслідок її реалізації, модифікуються для зменшення кількісного чи якісного значення ризику. В статті пропонується розглянути способи зменшення ступеня ризиків.

Постановка проблеми та визначення завдань дослідження

В багатьох організаціях недостатня увага приділяється процесу управління ризиками інформаційної безпеки, в той час як в деяких цей процес взагалі відсутній. В статті розглянуто основні деструктивні фактори, які впливають на стан інформаційної безпеки організації, та надано перелік заходів, які можуть бути впроваджені для початкового покращення цього стану.

Метою даної статті є визначення ефективних способів зменшення ступеня ризиків інформаційної безпеки, які можуть бути викликані критичними категоріями загроз та вразливостей.

Виклад основного матеріалу

Як було сказано раніше, ризик є невід'ємною складовою діяльності будь-якої організації, адже неможливо повністю убезпечити бізнес від ризиків. Для успішного функціонування необхідно ідентифікувати, аналізувати та реагувати на ризики, що виникають, відповідно до цілей та ризик-апетиту організації. Якщо ці дії не будуть виконані,

з високою ймовірністю бізнес зазнає втрат, пропорційних його величині та цінності його активів.

Відсутність управління ризиками. Виходячи з цього, основною і очевидною загрозою для організації є власне відсутність ефективного управління ризиками та корпоративного управління. Вона може призвести до підвищення схильності організації до ризику й упущення певних можливостей для бізнесу, впровадження неефективних політик та неадекватне використання інвестицій на інформаційну безпеку. Для зменшення ступеня даного ризику рекомендується створити структуру управління, що дозволить створити послідовний підхід з визначенням відповідальних осіб до управління ризиками інформаційної безпеки. Також необхідно визначити ризик-апетит організації – той рівень інформаційного ризику, який вона може прийняти. Цей рівень обирається в залежності від цілей організації та документується для того, щоб допомогти у прийнятті рішень стосовно ризиків.

Керівництво компанії повинно приділяти увагу ризикам впливу на інформаційні активи організації з боку загроз інформаційної безпеки. Для цього рекомендується створити та регулярно перевіряти та оновлювати корпоративний реєстр ризиків, куди слід заносити всі дані щодо наявних і потенційних ризиків. Для покращення обізнаності в сфері актуальних загроз представники організації можуть стати партнерами з обміну знаннями з іншими організаціями чи правоохоронними органами, в результаті чого можуть бути визначені нові ризики, що стосуються вашої організації, а також від партнерів може бути отримана інформація щодо ефективних заходів зниження ступеня ризику інформаційної безпеки стосовно кожного з них.

Рекомендується створити всеохоплюючу корпоративну політику управління ризиками інформаційної безпеки, яка буде підтримувати цілі ризик-менеджменту та визначати стратегію управління ризиками для організації. Також слід пам’ятати, що з часом характеристики ризику можуть змінюватися, тобто він може змінювати своє значення, тому необхідно забезпечити безперервний процес управління і моніторингу ідентифікованих ризиків. За умови достатнього фінансування слід впровадити фізичні, технічні, процедурні та кадрові заходи та засоби захисту.

Не можна забувати і про співробітників, оскільки більша частина інцидентів виникає саме внаслідок навмисних чи випадкових дій співробітників організації. Тому необхідно слідкувати, щоб проводилося їх належне навчання, особливо за умови, якщо їх надано доступ до критичних активів, та підтримувати їх обізнаність. Можна залучати співробітників до програм по обміну знаннями з колегами по бізнесу. Необхідно ретельно перевіряти та мотивувати співробітників з метою мінімізації ймовірності спричинення ними негативного впливу на бізнес внаслідок злого наміру.

Недостатній захист корпоративних мереж. Реалізація цієї загрози внаслідок невдалої архітектури мережі, яка може бути використана як внутрішніми, так і зовнішніми порушниками, може призвести до витоку конфіденційної корпоративної інформації або несанкціонованого доступу, який призведе до порушення цілісності, конфіденційності та доступності інформації. Також внаслідок цього можуть бути розповсюджені шкідливі програми. Вони можуть бути завантажені, наприклад, в якості безкоштовного програмного забезпечення, а потім випадково чи навмисно передаватися співробітниками всередині та за межі організації.

Внаслідок підключення до ненадійних мереж виникає вразливість “відмови в обслуговуванні”, коли користувачі втрачають доступ до інформації та послуг. Також слід пам’ятати, що зловмисники можуть здійснити несанкціонований доступ через вразливості мереж для порушення конфіденційності, доступності та цілісності інформації, послуг та систем. У випадку, якщо мережа була скомпрометована зловмисниками, організація може зазнати репутаційних збитків і послабити чи втратити довіру її клієнтів, якщо вони дізнаються про цей інцидент, наприклад, в разі несанкціонованої зміни веб-сайту організації.

Для зменшення ступеня ризику рекомендується посилити охорону мережевого периметру: обмежити доступ до мережевих портів, протоколів та додатків. Необхідно перевіряти мережевий трафік, який передається та отримується, на наявність трафіку, який не є необхідним для підтримання бізнес-процесів організації. Слід взяти під контроль всі вхідні та вихідні мережеві з'єднання та впровадити технічні засоби захисту, які дозволять виявити шкідливі програми.

Обов'язково слід встановити брандмауери, які дозволять сформувати буферну зону між ненадійною зовнішньою мережею і внутрішньою мережею організації. Набір правил брандмауеру за замовчуванням повинен забороняти отримання та передачу будь-якого трафіку, тому необхідно створити перелік правил, які будуть дозволяти взаємодіяти авторизованим протоколам, портам та додаткам тільки з авторизованими мережами. Окрім брандмауерів, слід встановити антивірусні програми для перевірки отриманих та відправлених даних на мережевому периметрі організації та окремо всередині організації. Доцільніше буде, якщо антивірусні програми, використовувані на периметрі та всередині організації, будуть відрізнятися, оскільки це може забезпечити більш глибокий захист.

Для додаткового захисту рекомендується виділити, згрупувати та ізолювати критично важливі для організації інформаційні активи та застосувати до них відповідний контроль мережевої безпеки. Бездротовим пристроям слід дозволити підключатися тільки до надійних та перевірених бездротових мереж, також в наявності повинні бути засоби захисту, які дозволять виявити місцезнаходження несанкціонованих бездротових точок доступу. За можливості слід убезпечити внутрішні IP-адреси від зовнішніх мереж та зловмисників, наприклад, за допомогою NAT (Network Address Translation).

Рекомендується проводити моніторинг мережі за допомогою інструментів виявлення та попередження мережевого вторгнення. Для забезпечення нормальної роботи налаштування цих інструментів слід довірити кваліфікованому співробітнику чи групі співробітників. В результаті трафік буде відстежуватися на предмет незвичайної, підозрілої чи шкідливої вхідної та зовнішньої активності, що може бути ознакою атаки чи спробою атаки на мережу. Слід належним чином навчати та тренувати співробітників, які будуть керувати системою та виявленими подіями. За умови достатньої кваліфікації та фінансування можна проводити тести на проникнення, для визначення вразливих місць та перевірки адекватної реалізації засобів захисту. [1]

Неефективне управління правами доступу. Дана категорія загроз може призвести до зловживання привілеями, коли діями авторизованих користувачів буде зламана ІКТ-система організації внаслідок навмисних чи випадкових дій. Наприклад, може бути змінена її конфігурація, в результаті чого може бути порушена конфіденційність, доступність і цілісність інформації чи системи. Також внаслідок компрометації облікового запису користувача, потенційний порушник зможе отримати такі ж привілеї в системі, як і володілець облікового запису, після чого шукатиме способи отримати повний доступ до системи. Як один із можливих результатів може бути несанкціоновано модифіковано засоби захисту та видалено журнали обліку та аудиту з метою приховування своєї діяльності порушником.

Для запобігання зловживання привілеями з боку співробітників рекомендується перед призначенням їх на посаду проводити їх перевірку, ступінь якої буде залежати від конфіденційності інформації, з якою вони будуть працювати. Також необхідно регулярно перевіряти облікові записи співробітників, починаючи з їх призначення на посаду до можливого звільнення. Після звільнення співробітника його обліковий запис повинен бути видалений. Невикористовувані облікові записи також слід видалити чи тимчасово деактивувати.

В політиці безпеки організації слід вказати вимоги до поводження з паролями: їх якість, час дії тощо. За можливості система повинна генерувати випадкові паролі та призначати їх користувачам, в іншому випадку, користувач сам обирає пароль, який відповідає за рівнем

складності та якістю до вимог, зазначених в політиці. В деяких випадках крім пароля може бути використано додатковий фактор автентифікації.

Рекомендується також обмежити права доступу співробітників, за принципами "знає той, хто повинен знати" та "доступ за необхідності". Це означає, що співробітникам надається доступ тільки до тієї інформації і тільки до тих засобів обробки і захисту інформації, які необхідні їм для виконання службових обов'язків.

Слід пильно контролювати кількість привілейованих облікових записів критично важливих ролей, наприклад, ролі системного адміністратора чи адміністратора баз даних. Привілейовані права доступу повинні бути призначені по мінімуму, але таким чином, щоб їх було достатньо для нормального виконання функціональних задач. Повинен проводитися постійний моніторинг процесу призначення привілейованих прав доступу для переконання в тому, що привілеї відповідають службовим обов'язкам співробітників, які ними володіють.

Привілейовані права доступу повинні переглядатися частіше, ніж звичайні, з метою виявлення можливого несанкціонованого їх отримання користувачами. В корпоративній політиці слід зазначити термін дії привілейованих прав доступу. Співробітникам, яким були надані такі права, слід заборонити використовувати їх для ризикових чи повсякденних дій користувачів, наприклад, для отримання доступу до некорпоративної електронної пошти або доступу до мережі Інтернет. Тому таким співробітникам слід також виділити звичайні, непривілейовані права доступу.

Доцільно буде слідкувати за діями користувачів з привілейованими правами доступу на предмет несанкціонованого створення нових облікових записів, зміни паролів, видалення активних облікових записів та журналів аудиту. Слід відстежувати спроби несанкціонованого доступу до конфіденційної інформації з боку користувачів, яким вона не потрібна для виконання службових обов'язків. Необхідно проінформувати всіх співробітників стосовно політики прийнятного використання облікових записів та ознайомити з відповідальністю за невиконання вимог політики.

Обізнаність співробітників. Значна кількість організацій не розроблює свою політику безпеки і не навчає співробітників питанням із забезпечення інформаційної безпеки. Як наслідок, такі організації піддаються негативному впливу внаслідок реалізації загроз, пов'язаним з недостатньою обізнаністю співробітників. Так, внаслідок відсутності політики і правил, які визначають допустимі дії користувачів, співробітник може неприпустимим чином використовувати систему, що може призвести до компрометації особистою чи конфіденційної комерційної інформації, що в свою чергу може бути причиною юридичних санкцій та репутаційних збитків для організації.

Іншою загрозою може бути використання співробітниками організації власних знімних носіїв інформації та пристроїв. Знов, якщо співробітники не ознайомлені з політикою безпеки або якщо її не створено, вони можуть під'єднати власні пристрої до корпоративної інфраструктури, вважаючи, що це є припустимим. Як результат, можуть бути імпортовані шкідливі програми або може бути скомпрометована особиста чи конфіденційна комерційна інформація.

Якщо співробітники недостатньо обізнані а безпечному використанні систем, якими вони користуються, вони можуть випадково скомпрометувати систему і потенційно порушити конфіденційність, цілісність та доступність інформації, що в ній зберігається. Також слід навчати співробітників виявляти інциденти, оскільки несвоєчасне його виявлення та початок реагування може призвести до збільшення його наслідків.

Слід зазначити, що співробітники-користувачі залишаються основною мішенню зловмисників, оскільки ймовірність успіху вища при використанні зловмисником соціальної інженерії, фішингу, ніж технічної атаки. До того ж, це не потребує значної кількості фінансових та інших ресурсів, і для компрометації системи зазвичай вистачає одного розкритого облікового запису. Також самі співробітники можуть бути джерелом загрози та самостійно нанести шкоди організації. Причиною цього може бути зміна в особистому житті співробітника, що може зробити його вразливим до застосування психологічного впливу або

примусу, в результаті якого він може знищувати або передавати конфіденційну інформацію конкурентам чи іншим зацікавленим у нанесенні шкоди організації сторонам. Також якщо співробітник невмотивований або ображений на керівництво чи на організацію, він так само може вкрасти, продати чи знищити інформацію, а також нанести шкоди фізичному обладнанню.

Для зменшення ступеня ризиків, пов'язаних з обізнаністю співробітників, необхідно створити політику безпеки організації, в якій буде описано допустимі дії користувачів. В процесі призначення на посаду нові співробітники повинні бути ознайомлені з персональною відповідальністю за дотримання правил, описаних у політиці безпеки організації. Обов'язковим є регулярне проведення перепідготовки співробітників з питання інформаційних ризиків, які стосуються організації та співробітників, під час їх роботи та під час дозвілля. Співробітників, які займаються питанням інформаційної безпеки, слід мотивувати на їх розвиток. Можна створити механізми для перевірки ефективності навчання з питань інформаційної безпеки, яке слід проводити для всього персоналу. Цей механізм працюватиме, базуючись на зворотному зв'язку.

Рекомендується сприяти культурі сповіщення про інциденти, що надасть можливість співробітникам висловлювати свою тривогу стосовно неефективних методів забезпечення інформаційної безпеки топ-менеджерам, при цьому не боячись звинувачень з їх боку. Також слід встановити формалізований дисциплінарний процес, щоб співробітники були проінформовані, що будь-яке зловживання політикою безпеки організації призведе до дисциплінарних заходів, спрямованих проти винних співробітників. [2]

Висновки та рекомендації

Незмінним залишається те, що саме співробітники залишаються найслабшою ланкою в інформаційній безпеці організації. Зловмисники користуються тим, що використати людину та отримані від неї дані за допомогою соціальної інженерії, фішингу або різних видів шахрайства дешевше та зазвичай легше, ніж провести вдалу технічну атаку на захищену інформаційну систему організації. І у зв'язку зі зростанням складності різноманітних засобів захисту, ця тенденція ймовірніше за все залишиться незмінною. Тому першочергово доцільніше буде приділити увагу саме убезпеченню себе від загроз, що містять в собі людський фактор.

Перед призначенням на посаду всі співробітники, яким за посадою буде надано доступ до критичної інформації і активів, повинні проходити перевірку та вони повинні бути ознайомлені з політикою безпеки і відповідальністю за її порушення. Співробітники потребують належного навчання, підготовки та постійного розвитку та вдосконалення їх навичок. Також необхідний контроль та мотивація працівників. За можливості треба слідкувати за психологічним станом чи змінами в поведінці співробітників з метою попередження потенційного спричинення збитку організації з їх боку. Призначати права доступу необхідно таким чином, щоб доступ до інформації та активів надавався лише в межах службових обов'язків. Співробітники з привілейованими правами доступу повинні піддаватися більш пильному контролю та їх права повинні переглядатися частіше.

Перелік посилань

1. An Ongoing Project: A Cyber Risk Mitigation Strategy [Електронний ресурс] // - Режим доступу: https://www.getsmarter.com/blog/market-trends/an-ongoing-project-a-cyber-risk-mitigation-strategy/ (19.10.2020)

2. Danny Timmins 5 Steps to Reducing Cyber Security Risk [Електронний ресурс] // - Режим доступу: https://www.mnp.ca/en/posts/5-steps-to-reducing-cyber-security-risk (20.10.2020)

Надійшла: 04.11.2020 Рецензент: д.т.н., с.н.с. Лаптєв О.А.