УДК 004.056.5

А.О. Краснопольський, к.т.н.

АДАПТАЦІЯ БІЗНЕС ПРОЦЕСІВ ПІДПРИЄМСТВА ДО ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КЕРУВАННЯ РИЗИКАМИ

Національний авіаційний університет

rit@nau.edu.ua

В статті наведено алгоритм адаптації бізнес процесів підприємства до технологій керування кібернетичними ризиками. Подано рекомендації та очікувані результати.

Ключові слова: *захист інформації, керування ризиками, бізнес-процес.*

Постановка проблеми

Нові типи загроз вимагають трансформації застарілих процесів використання і захисту інформаційних активів. Компанія RSA в новому звіті «Трансформація інформаційної безпеки: процеси орієнтовані на майбутнє» дає рекомендації з модернізації керування кіберризиками [1].

Постановка завдання

Компанії можуть одержати нові конкурентні переваги шляхом трансформації застарілих процесів використання і захисту інформаційних активів. Експерти відзначають, що бізнес підрозділи в компаніях усе активніше беруть участь у керуванні інформаційними ризиками. При цьому застарілі процеси забезпечення безпеки перешкоджають інноваціям і утруднюють успішну боротьбу з новими ризиками кібербезпеки. Фахівці рекомендують службам інформаційної безпеки тісніше взаємодіяти з функціональними бізнес-підрозділами для створення нових систем і процесів, що допомагають швидше і точніше виявляти, оцінювати і відслідковувати ризики кібербезпеки.

Основний матеріал

У числі способів поліпшити процеси забезпечення безпеки експерти називають кількісну оцінку ризиків, залучення бізнес підрозділів у ці процеси, оцінку засобів контролю над ризиками, проведення оцінок ризиків зовнішніми спеціалізованими організаціями і виявлення загроз. Існує ряд основних рекомендацій для керівників служб IT безпеки з розвитку програми забезпечення інформаційної безпеки, що допоможуть бізнес-підрозділам перетворити ризики в джерела нових конкурентних переваг.

1. Перенос уваги з технічних активів на критично важливі бізнес-процеси (БП). Необхідно вийти за рамки технічної концепції захисту інформаційних активів і разом з бізнес-підрозділами задокументувати критично важливі БП, щоб сформувати повну картину використання інформації в компанії [2], [5].
2. Оцінка ризиків кібербезпеки з погляду бізнесу. Описати ці ризики в термінах і цифрах, зрозумілих бізнесу, і інтегрувати їх у загальний процес оцінки бізнес-ризиків [3], [5].
3. Оцінка ризиків з боку бізнес-підрозділів. Впровадити автоматизовані засоби відстеження інформаційних ризиків, щоб бізнес-підрозділи могли активно брати участь у виявленні небезпечних ситуацій і запобіганні ризиків, підвищуючи свою частку відповідальності за безпеку компанії.
4. Перевірка засобів контролю. Розробити і задокументувати методи збору даних для систематичного підтвердження ефективності засобів контролю [4].
5. Розробка методик збору даних про ризики. Цілеспрямовано формувати архітектуру даних про ризики, що буде поліпшувати видимість і розширювати можливості аналітики. При ідентифікації релевантних джерел даних орієнтуватися на типи задач, що вирішує аналітика даних.

Рекомендації та можливі очікувані результати наведено в таблиці.

Таблиця 1

Адаптація бізнес процесів

Етап	Рекомендації	Результати
1	Зрозумійте БП з початку до кінця. Залучайте співробітників бізнес-підрозділів до документуванню робочих процесів	Вміння розрізняти «нормальну» і «ненормальну» поведінку в рамках БП. Чітке уявлення про те як хакери можуть нашкодити БП. Впровадження заходів безпеки які будуть ефективно захищати бізнес
2	Оцінюйте ризики інформаційної безпеки у фінансових втратах. Складіть сценарії імовірності інцидентів і їхнього впливу на бізнес. Удосконалюйте методики оцінки ризиків у грошових вираженнях	Можливість точніше зважувати ризики інформаційної безпеки і вигоди для бізнесу. Довести велику важливість ризиків ІБ у порівнянні з іншими ризиками. Доступно пояснити бізнес-підрозділам істотність ризиків і адекватність стратегії з їх мінімізації
3	Автоматизуйте процедуру оцінки ризиків. Стежте за тим які ризики виявляються, оцінюються, усуваються. Змініть процедуру прийняття ризиків, щоб приймати великі ризики для короткострокових проектів	Можливість комплексно оцінювати ризики інформаційної безпеки. Бізнес-підрозділи зможуть керувати своїми ризиками і нести за це відповідальність. Компанія буде використовувати більше короткострокових можливостей
4	Упроваджуйте процедури для систематичного збору доказів і моніторингу дотримання заходів безпеки. Документуйте і переглядайте заходи безпеки, зосереджуючись на найважливіших. Автоматизуйте збір даних і створення звітності	Можливість оптимізувати заходи безпеки. Аудит більше не буде відволікати співробітників бізнес-підрозділів від роботи. Оцінка власної інфраструктури і постачальників стане більш точною
5	Подумайте на які питання про безпеку може відповісти аналітика даних. Розробіть сценарії використання аналітики й уточнюйте моделі прогнозів. Збирайте для аналізу дані з внутрішніх БП, а також інформацію про загрози з зовнішніх джерел	Можливість визначити релевантні джерела даних і отримувати з них необхідну інформацію. Можливість правильно інтерпретувати дані. Аналітика даних буде давати більш точні результати

Одна з практичних вигід це ризик орієнтована інтерпретація отриманих оцінок інформаційної безпеки.

Висновки за результатами аудита інформаційної безпеки (ІБ) можуть вказувати на необхідність коригувальних і превентивних дій, спрямованих на поліпшення системи забезпечення ІБ організації. Такі дії не розглядаються як частина аудита ІБ або самооцінки ІБ, і рішення про їх проведення приймає організація, що перевіряється. Однак для прийняття подібних рішень необхідна зрозуміла для керівництва організації, сформульована в термінах бізнесу інтерпретація результатів аудита або самооцінки ІБ.

Інтерпретація результатів аудита або самооцінки ІБ являє собою пояснення, яке зв'язує кількісну оцінку показників з діями з поліпшення системи забезпечення ІБ організації, необхідними для зниження ризиків БП мовою споживачів результатів аудита або самооцінки ІБ, тобто керівництва організації.

Сукупність атрибутів, що містяться в приватних показниках або у моделях зрілості процесів забезпечення ІБ, являє собою еталонні моделі процесів, що піддаються оцінці.

Вихідні дані оцінки процесу включають сукупність оцінених за допомогою показників атрибутів процесу, що представляють собою профіль оцінюваного об'єкта. Отриманий у результаті оцінки профіль процесу може не відповідати ні еталонному, ні цільовому профілю процесу. Така невідповідність указує на наявність ризику ІБ.

Зв'язаний із процесом ризик ІБ випливає з недостатнього менеджменту процесу й оцінюється виходячи з рівня уразливостей і потенційних наслідків, якщо реалізуються відповідні загрози.

Таким чином, якщо визначена розбіжність між цільовим і оціненим профілем процесу, то можна затверджувати, що існує уразливість у системі забезпечення ІБ організації. Для кожної розбіжності необхідно визначити і зафіксувати:

– характер уразливості;
– джерело або причину уразливості;
– потенційні негативні наслідки для кожного БП у випадку подальшого існування негативності;
– міри, що повинні бути прийняті для усунення або зменшення уразливості;
– які будуть витрати, вигоди і ризик усунення або зменшення уразливості.

Інформаційна безпека - один з видів безпеки, визначається через «стан захищеності», неявно адресуючи нас до категорій психології, зокрема впевненості і довіри в безпеці. Ця впевненість орієнтована на соціум - людини або групу осіб, які очікують або ж прагнуть досягти деякі цілі і роблять для цього певні дії.

Впевненість усвідомлюється за допомогою перегляду даних довіри, отриманих у результаті процесів оцінювання і заходів під час розробки, розгортання і дії, і в результаті досвіду за реальним використанням об'єкта довіри. Будь-які заходи, що можуть зменшити невизначеність шляхом представлення даних, що свідчать про правильність, ефективність і якість атрибутів об'єкта довіри, формують основу довіри безпеки.

Якщо виходити з передумов, що безпека це прагнення до порядку, то, з огляду на мале число існуючих специфічних для безпеки методів (стандартів, що відносяться до забезпечення безпеки на різних стадіях життєвого циклу систем, процесів, продукції, довіри до персоналу і т.д.), кожний з існуючих методів довіри привносить свій внесок у впевненість у безпеці. Усе, що може бути використане для створення аргументації для впевненості в безпеці і зменшення в зв'язку з цим невизначеності (ризику), має велике значення [4].

Висновки

У сучасному цифровому світі успішне впровадження інновацій неможливо без переоцінки заходів для керування ризиками кібербезпеки. Служби ІТ-безпеки повинні перейти від пасивного підходу, заснованого на захисті периметра компанії, до проактивного співробітництва з бізнес-підрозділами. Якщо БП будуть оновлені відповідно до рекомендацій наведених вище, компанії зможуть краще представляти ризики і керувати ними, отримуючи при цьому вигоду. Якщо документування БП стане загальною задачею, то отримані результати максимально точно відіб'ють ризики, що маються в системі. Керівники служб ІТ-безпеки ніколи не зрозуміють цінність конкретної інформації для бізнесу краще власників БП, а вони, у свою чергу, ніколи не передбачать кіберзагрозу краще фахівців служби безпеки.

Список літератури

1. Переосмыслить процессы управления рисками!//ИТМ. Информационные технологии для менеджмента. – 2014. - №3. – С. 46-47.
2. Петренко С. А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов – М.: Компания АйТи, 2006. – 400 с.
3. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев – СПб.: БХВ-Петербург, 2003. – 688 с.
4. Аудит информационной безопасности / А. Курило, С. Зефиров, В. Голованов [и др.] – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
5. Краснопольський А. Використання ринкових вимог у формуванні контенту навчальної дисципліни// Вісник Інженерної академії України. –2014. – №1. – С. 289-291.