3. Woo-Ri Lee, Haejong Lee, Eun Woo Nam, Jin-Won Noh, Jin-Ha Yoon, Ki-Bong Yoo «Comparison of the risks of occupational diseases, avoidable hospitalization, and all-cause deaths between firefighters and non-firefighters: A cohort study using national health insurance claims data» / Front Public Health, 2023, Jan 16;10. – Access mode: DOI:: 10.3389/fpubh.2022.1070023

4. Sara Alves, Josiana Vaz, Adília Fernandes «Occupational health of firefighters: a systematic review» / International Symposium on Occupational Safety and Hygiene (SHO'23), pp. 56-66. – Access mode: doi.org/10.24840/978-989-54863-4-2_0056-0066

УПРАВЛІННЯ РИЗИКАМИ ВНУТРІШНІХ ЗАГРОЗ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Третьяков О.В.
Національний університет «Київський авіаційний інститут», Київ, Україна

Ризик визначається як можливість навмисного або ненавмисного заподіяння шкоди організації шляхом неналежного використання її ресурсів особою, яка має до них авторизований доступ. Під доступом мається на увазі як фізичний, так і віртуальний доступ, а ресурси включають інформацію, процеси, системи та обладнання [1].

Метою доповіді є розроблення підходу до оцінки ризику внутрішніх загроз та можливих шляхів управління ними задля підвищення безпеки і стійкості об'єктів критичної інфраструктури.

У роботі проаналізовани інциденти з безпекою з наявним наміром заподіяти шкоду, спричинені інсайдерами, які можуть виникати різними способами: насильство або загрозу насильства інших працівників; саботаж (умисне пошкодження обладнання або розкриття конфіденційної інформації); крадіжка ресурсів, конфіденційних даних або інтелектуальної власності організації задля отримання особистої вигоди; промислове шпигунство; шахрайські дії з метою отримання особистої вигоди [2].

У доповіді наведено основні індикатори виявлення внутрішніх ризиків, в яких відіграють роль як люди, так і технології. Ключова умова – визначити межі норми поведінки, що дозволить легше виявляти незвичні дії. До основних індикаторів віднесено:

1) зміни в діях користувача (колеги, керівники та партнери здатні помітити зміни в поведінці схильного до ризику інсайдера, який має на меті спричинити інцидент із безпекою даних);
2) послідовність пов'язаних ризикованих дій з конфеденційними даними, матеріалами тощо;
3) аномальний доступ до системи (потенційні внутрішні ризики можуть починатися з того, що користувачі отримують доступ до ресурсів, які зазвичай не потрібні їм для роботи);
4) перевищення повноважень доступу без чіткого ділового обґрунтування;

5) аномальна ексфільтрація даних (користувач раптово ділиться незвично великим обсягом конфіденційних даних або завантажує його);

6) ексфільтрація даних, яка зростає разом зі звільненнями та може бути як навмисною, так і ненавмисною;

7) погрози, переслідування або дискримінації співробітників.

Цілісна програма керування внутрішніми ризиками, яка визначає пріоритетність відносин між працівниками та роботодавцем та інтегрує елементи керування конфіденційністю, може зменшити кількість потенційних внутрішніх інцидентів із безпекою, і прискорити їх виявлення.

Нещодавнє дослідження, проведене корпорацією Майкрософт, виявило, що компанії з цілісною програмою керування внутрішніми ризиками на 33% частіше швидко виявляють ризики витоку інсайдерської інформації, та на 16% частіше швидко усувають такі ризики, ніж компанії з більш фрагментарним підходом.

Організації можуть цілісно підходити до боротьби із внутрішніми ризиками, зосереджуючи увагу на процесах, людях, інструментах та освіті.

Створення довіри серед працівників починається з визначення їхньої конфіденційності пріоритетом. необхідно впровадити багаторівневий процес затвердження для ініціювання внутрішніх розслідувань, щоб сприяти створенню відчуття комфорту за допомогою програми керування внутрішніми ризиками.

Важливо перевіряти дії тих, хто проводить розслідування, щоб переконатися, що вони не перевищують свої повноваження. Збереженню конфіденційності також сприятиме упровадження елементів керування доступом на основі ролей для обмеження кількості членів команди безпеки, які можуть отримати доступ до даних розслідування. Знеособлення імен користувачів під час розслідувань може додатково захистити конфіденційність працівників.

ІТ-відділи та відділи безпеки повинні нести основну відповідальність за керування внутрішніми ризиками, але важливо залучати до цих зусиль усіх працівників компанії. Відділи кадрів, юридичні відділи відіграють важливу роль у визначенні політик, спілкуванні із зацікавленими сторонами та прийнятті рішень під час розслідування. Щоб розробити більш комплексну та ефективну програму керування внутрішніми ризиками, організаціям слід залучити до цього процесу співробітників, що представляють усі напрямки діяльності компанії.

Працівники відіграють важливу роль у запобіганні інцидентів із безпекою, що робить їх першою лінією захисту. Щоб захистити ресурси компанії, потрібна підтримка всіх працівників, що, у свою чергу, підвищує безпеку організації в цілому. Одним із найефективніших способів забезпечення підтримки всіх працівників є навчання. Навчаючи працівників, можна зменшити кількість ненавмисних інцидентів внутрішніх ризиків. Важливо роз'яснювати, як інциденти внутрішньої безпеки можуть вплинути на компанію, та її працівників.

Крім того, дуже важливо обговорювати політики захисту даних і навчати працівників уникати потенційного витоку даних.

Позитивні стримувальні фактори, такі як події, спрямовані на підвищення морального стану працівників, ретельний інструктаж, постійне навчання та тренування з безпеки даних, ефективний зворотний зв'язок та програми з балансу роботи та особистого життя можуть зменшити ймовірність внутрішніх ризиків.

Залучаючи працівників у ефективний і проактивний спосіб, позитивні стримувальні фактори усувають джерела ризику та сприяють розвитку культури безпеки в організації.

Ефективний захист організації від внутрішніх ризиків вимагає не лише впровадження найкращих інструментів безпеки; але й інтегрованих рішень, які забезпечують видимість і захист на рівні підприємства. Інтегровані рішення з керування безпекою даних, ідентичністю та доступом, розширеного виявлення та реагування (XDR), а також керування захистом інформації (SIEM) дозволяють командам безпеки ефективно виявляти та попереджати інциденти внутрішньої безпеки.

Для сучасного робочого місця характерними є динамічні ризики безпеки з різними факторами, що постійно змінюються. Це ускладнює виявлення й реагування на них.

Втім, організації можуть миттєво виявляти та зменшувати внутрішні ризики завдяки використанню машинного навчання та штучного інтелекту, забезпечуючи адаптивну та орієнтовану на людей безпеку.

Ця передова технологія допомагає організаціям зрозуміти, як користувачі взаємодіють із даними, обчислюють і призначають рівні ризиків, а також автоматично налаштовують відповідні елементи керування безпекою. За допомогою цих інструментів організації можуть оптимізувати процес виявлення потенційних ризиків і визначити пріоритети використання своїх обмежених ресурсів для запобігання діям з внутрішніми ризиками високого ступеню. Це заощаджує цінний час для команд безпеки та посилює безпеку даних.

Захиститися від внутрішніх загроз може бути складно, оскільки природно довіряти тим, хто працює в організації та разом з нею.

Швидка ідентифікація найкритичніших внутрішніх ризиків та визначення пріоритетів використання ресурсів для розслідування та усунення цих ризиків вкрай важливі для зменшення впливу потенційних інцидентів і порушень безпеки.

Список літератури

1. Герасименко О. М. Моделювання системи забезпечення кадрової безпеки суб'єкта господарювання. *Актуальні проблеми економіки*. 2012. № 2. С. 118–124.

2. Панченко В. А. Схематика дій інсайдерів у системі кадрової безпеки суб'єктів господарювання. *Підприємництво і торгівля*. 2018. Вип. 22. С. 101-107.