УДК 004.056:355.451]:005.7

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ

Гапонюк К.В.
Науковий керівник - к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел. +38(067) 355-88-54

One of the main aspects of security issues in the organization is considered. The threat of hacking due to lack of awareness of personnel in the field of information protection, which poses a privacy risk for the company to its employees, was analyzed.

В доповіді розглядається питання забезпечення інформаційної безпеки в офісному приміщенні. Актуальністю даної роботи є необхідність захисту конфіденційних даних, інформації та відомостей, розголошення або спотворення яких може спричинити за собою негативні наслідки для працівників та компанії в цілому.

У результаті опитування Cyber Breaches Survey за 2022 рік, було виявлено існування нестачі розуміння питань кібербезпеки серед найманого персоналу, та відсутність розуміння ефективного управління кіберризиками на рівні управління організації.

Важливо усвідомлювати, що будь-яка організація, яка покладається на цифрові технології, піддається ризику кіберінциденту [1]. Кіберзлочинці намагатимуться використати слабке місце (чи вразливість) у системі, незважаючи на те, кому ця система належить, чи розмір організації.

Більшість кіберзломів не є результатом «складних і витончених атак». Переважна більшість атак все ще базується на добре відомих методах таких як фішингові електронні листи.

Цифрова революція дає величезні переваги, але також приносить нові ризики, які ми повинні розуміти та боротися з ними, враховуючи нашу зростаючу залежність від кіберпростору.

Щоб належним чином забезпечити інформаційну безпеку організації, вона має бути інтегрована в організаційне управління ризиками та прийняття рішень, а всі бізнес-підрозділи організації мають чітко розуміти свої зобов'язання та відповідальність щодо кібербезпеки.

Наприклад:

- технічні команди повинні розуміти важливість безпеки та захисту даних і систем за допомогою відповідних засобів контролю;
- людські ресурси повинні забезпечити кібербезпеку протягом усього життєвого циклу персоналу з відповідними вказівками, політикою та підтримкою для робочої сили;

- комунікаційні та маркетингові команди, які керують даними та маркетинговими службами, повинні співпрацювати з управлінням, щоб підготуватися до спілкування з клієнтами та пресою, щоб вони були готові до ряду інцидентів (таких як втрата операційних можливостей або порушення даних);
- юридичні команди повинні усвідомлювати важливість обробки та захисту контрактів і юридичних документів, щоб вони не потрапили в руки конкурентів, а також повинні гарантувати ризики відповідальності, що виникають через потенційні кіберінциденти під час операцій;
- команди з кібербезпеки повинні розробляти та впроваджувати політики, які захищають дані співробітників і клієнтів від несанкціонованого доступу;
- команди із закупівель повинні враховувати кіберризики під час переговорів із потенційними постачальниками послуг, від програмного забезпечення та апаратного забезпечення до наймання підрядника, і включати управління кіберризиками в управління контрактами в ланцюжку постачання.

Також для забезпечення надійного збереження інформації, управління компанії має визнавати, що злочинець (який може варіюватися від незадоволеного працівника до особи, яка фінансується державою і має намір викрасти інтелектуальну власність) зможе отримати доступ до системи.

Це означає, що потрібно мати засоби контролю, щоб мінімізувати шкоду, яку вони можуть завдати, опинившись усередині. Це можна забезпечити шляхом обмеження їх доступу до послуг та інформації. Моніторинг і ведення журналів є ключовими для можливості якомога швидше виявити ознаки зловмисної діяльності та обмежити шкоду, яку вони можуть завдати.

Список використаних джерел:

1. Інструменти кібербезпеки для плат | Керівництво | Головна сторінка. URL: https://www.ncsc.gov.uk/collection/board-toolkit (дата звернення 09.04.2023)