УДК 004.05

Я.Р. Лапшин
Західноукраїнський національний університет, Україна

АНАЛІЗ ЗАГРОЗ КІБЕРБЕЗПЕКИ ТА ДОСЛІДЖЕННЯ ЙОГО ВПЛИВУ

Y.R. Lapshin

ANALYSIS OF CYBER SECURITY THREATS AND RESEARCH OF ITS IMPACT

Коли питання стосується цифрової безпеки, найбільш важливий елемент є аналіз загроз. Це пов'язано з тим, що він передає важливу інформацію, необхідну для забезпечення безпеки IT-інфраструктури компанії. Можливість аналізувати великі обсяги даних з різних джерел майже в режимі реального часу дає аналітикам безпеки перевагу перед традиційними підходами до забезпечення безпеки. За даними Fundera, ринку фінансових рішень для малого бізнесу, статистика загроз кібербезпеки приводить компанії до тями й змушує їх зосереджувати свою увагу на питаннях інформаційної безпеки, з якою більшість із нас зустрічається постійно.

За даними 2021 року: – 43% усіх кібератак сконцентровані на малому бізнесі. – 60% малих підприємств, які стали жертвами кібератак, вимушені закритися впродовж п'яти - шести місяців. – Кіберзлочинність обходиться малому і середньому бізнесу більш ніж у 2,2 млрд. доларів на рік. – Число нових комп'ютерних порушень у галузі кібербезпеки зросло на 424%. – Охорона здоров'я – одна з галузей, найбільш схильна до кібератак. – 66% малих підприємств схвильовані можливостями атаки кіберзловмисниками. – 14% малих підприємств оцінили власні можливості зменшувати кіберзагрози і кібератаки як високоефективні. – 47% малих підприємств не розуміють, як захистити себе від кібератак. – 66% підприємств найбільше стурбовані компрометацією даних клієнтів і конфіденційністю їх даних. – Лише у 1 з 4 малих підприємств присутній персонал який вирішує питання інформаційної безпеки. Це всього 25% з усіх компаній. – 22% малих підприємств зашифровують свої дані.

Людський фактор і збої систем становлять понад 50% порушень інформаційної безпеки. Тобто найбільшою загрозою та основним ризиком є людина – працівник компанії або користувач. Також апаратне та програмне забезпечення, яке періодично стає сумнівним та неактуальним у досить короткий відрізок часу. Навіть з наявності стандартних заходів, буде не достатньо для того, щоб ваша команда з інформаційної безпеки була в курсі останніх загроз кібербезпеки. Через те що характер онлайн-загроз досить часто змінюється, оцінка аналітики загроз має ключове значення для любих підприємств. Саме тому основна частина фахівців з кібербезпеки рекомендують підключити послуги цілодобового моніторингу та аналізу, яка допоможе вам вберегтися від нападів зловмисників, а також відреагувати на непередбачену ситуацію.

Основна мета аналізу загроз полягає в тому, що вона дозволяє експертам з безпеки краще зрозуміти як може думати та що може зробити зловмисник. Отримані дані можуть показати на план, метод, мотиви, цілі та процедури, які були використані для здійснення атаки. Фактично, це призводить до покращення засобів безпеки, відносячи до них оцінку, розпізнавання, а також тривалість відповіді на ситуацію.

Література:

1. Що таке аналіз загроз в кібербезпеці? [Електронний ресурс]. https://datami.ua/shho-take-analiz-zagroz-v-kiberbezpetsi/

2. Cyber Security threats Statistics [Електронний ресурс]. https://www.fundera.com/resources/small-business-cyber-security-statistics/