gamatronic
INNOWACJE W ZARZĄDZANIU

Ochrona przed ransomware

Ataki ransomware coraz częściej atakują komputery zwykłych użytkowników, jak i maszyny firmowe. Polegają one na infekcji złośliwym oprogramowaniem i zablokowaniu danych znajdujących się na urządzeniach, aż do momentu opłacenia okupu przez ofiarę. Najczęściej do zarażenia dochodzi przez e-maile oraz media społecznościowe. Poniżej przedstawiamy kilka zasad, które pomogą zminimalizować ryzyko infekcji:

1. Zadbaj o backup

Na początek warto pamiętać o tym, by regularnie tworzyć kopie zapasowe, a najlepiej opracować plan kopii zapasowych i odzyskiwania. Przygotowane backupy natomiast powinno się przechowywać na osobnym, niepodłączonym do sieci urządzeniu.

2. Zaufaj profesjonalnym zabezpieczeniom

Czołowi producenci oprogramowania zabezpieczającego mają w swoich ofertach programy i narzędzia do skanowania e-maili, stron internetowych i plików oraz blokowania niebezpiecznych reklam i witryn. W każdym przypadku warto z nich skorzystać.

3. Pamiętaj o aktualizacjach systemu i urządzeń

Cyberprzestępcy nie próżnują i w miejsce jednego zablokowanego złośliwego oprogramowania tworzą trzy kolejne. Aby się przed zabezpieczyć, należy zawsze korzystać z aktualnego systemu operacyjnego oraz aktualizować urządzenia i oprogramowanie.

4. Aktualizuj oprogramowanie

Aktualne muszą być także oprogramowanie zabezpieczające i sprzęt. Dlatego też upewnij się, że antywirus oraz antymalware są zaktualizowane do najnowszej wersji.

5. Podziel sieć na strefy bezpieczeństwa

Sieć podzielona na strefy bezpieczeństwa to sposób na zapobiegnięcie rozprzestrzenienia się potencjalnych infekcji na całą sieć – malware nie wychodzi poza określoną strefę.

6. (Do pewnego stopnia) nie ufaj innym użytkownikom

Do większości infekcji dochodzi w wyniku nieodpowiedzialnego zachowania jednego z użytkowników. Warto więc zadbać o to, by każdy z nich miał nadane indywidualne prawa dostępu – tak, by liczba osób mogących sprowadzić nieszczęście była jak najmniejsza.

7. Uświadom użytkowników

Pracownicy mogą być nieświadomi czyhających zagrożeń. Warto poinformować ich o tym, by nie uruchamiali jakkolwiek podejrzanych plików i linków. W rzeczywistości bowiem to właśnie człowiek jest najsłabszym ogniwem w łańcuchu bezpieczeństwa.

A jeśli już dojdzie do infekcji, to co robić?

Rozpocząć należy od zgłoszenia przestępstwa policji oraz skontaktowania się z ekspertami ds. cyberbezpieczeństwa. Zdecydowanie nie należy opłacać okupu (wtedy wygrywają „oni”, a my i tak nie mamy pewności, że pliki zostaną odblokowane).