Cyberbezpieczeństwo to nie Yeti – choć go nie widać to musi istnieć

Cyberzagrożenia to zjawiska często niewidoczne dla przeciętnego użytkownika. Ataki z zasady przebiegają w tle, a ich efekty mogą być odczuwalne dopiero po pewnym czasie, gdy ofiary tracą dostęp do zasobów finansowych czy cyfrowych. Mimo, że pozornie niedostrzegalne, skutki cyberzagrożeń są mierzone w milionach złotych.

Z badania Global Data Protection Index 2024[1] firmy Dell Technologies wynika, że w ubiegłym roku ponad połowa firm (55%) padła ofiarą cyberataku lub incydentu, który uniemożliwił dostęp do danych. Z kolei, jak podaje IBM[2], w 2024 roku średni koszt naruszenia danych na świecie wzrósł o 10 proc. i osiągnął 4,88 mln dolarów.

Gartner[3] prognozuje, że globalne wydatki na cyberbezpieczeństwo wzrosną o 15,1% w 2025 roku, osiągając wartość 212 mld dolarów. Oznacza to wzrost w stosunku do przewidywanych 183,9 mld dolarów w 2024 roku.

Cyfrowa transformacja napędza zagrożenia

Wkraczamy już w czwartą dekadę rozszerzającej się powszechnej dostępności technologii cyfrowej, która dzisiaj kształtuje obraz współczesnej gospodarki. Praktycznie w każdym aspekcie naszego życia stosujemy już rozwiązania cyfrowe, które wspierają pracę, zapewniają rozrywkę czy po prostu pomagają w codziennym życiu.

Cyberbezpieczeństwo odzwierciedla te przemiany. Kiedyś – jeszcze jako bezpieczeństwo IT – polegało na ochronie zasobów informatycznych, dziś skupia się na zabezpieczaniu procesów i danych, ze szczególnym naciskiem na przetwarzane w systemach dane użytkowników.

Zmieniające się otoczenie wymusza bardziej proaktywne podejście do cyberbezpieczeństwa. Sieć staje się bowiem areną coraz bardziej zaawansowanych ataków cybernetycznych. Przestępcy nadal sprawnie posługują się socjotechniką, wykorzystują ludzką ciekawość, lęki czy chęć zysku, podszywają się pod firmy i instytucje, by wyłudzić dane i środki finansowe.

Problem w tym, że skala zagrożeń rośnie i zwiększa się też powierzchnia możliwych do przeprowadzenia ataków. W pandemii nowe możliwości dla cyberprzestępców otworzyło przejście na pracę zdalną i hybrydową. Biorąc pod uwagę zmiany geopolityczne i nowe scenariusze wojny hybrydowej – rozumianej również jako rozszerzenie pola walki na cyberprzestrzeń – należy spodziewać się, że w przyszłości najistotniejsze zagrożenia będą płynęły z łańcucha dostaw i zależności od zaawansowanych komponentów technologicznych.

Rośnie kreatywność cyberprzestepców

W dobie popularyzacji technologii sztucznej inteligencji trzeba się też przygotować na coraz więcej ataków przygotowanych w oparciu o zaawansowane algorytmy AI, np. wykorzystujące narzędzia deepfake.

Jak wynika z Microsoft Digital Defense Report 2024[4], cyberprzestępcy coraz częściej koncentrują swoje działania na atakach na infrastrukturę IT dużych korporacji w celu wymuszenia okupu oraz na instytucjach finansowych, jak banki czy giełdy. Równocześnie rośnie liczba zagrożeń związanych z kradzieżą tożsamości i danych użytkowników –

[1] Global Data Protection Index 2024
[2] Cost of a data breach 2024 | IBM
[3] Gartner Forecast 2024
[4] Microsoft Digital Defense Report 2024

codziennie odnotowuje się aż 600 mln prób przejęcia loginów i haseł. Ataki phishingowe wykorzystujące fałszywe e-maile i strony logowania, a także oszustwa oparte na inżynierii społecznej, w których cyberprzestępcy podszywają się pod instytucje finansowe, stają się coraz bardziej wyrafinowane, stanowiąc jedno z największych wyzwań w obszarze cyberbezpieczeństwa.

Widać dokładnie transformację mającą zagwarantować atakującym możliwie najszerszy dostęp i możliwość wpływu na szerokie grono odbiorców, pozwalające na chirurgiczną precyzję w realizowaniu swoich celów. Zagrożenia związane z wyłudzeniami czy ransomware nie przestaną występować, po prostu te nowe, bardziej zaawansowane, staną się istotniejsze.

Niewidoczne działania, bolesne skutki

Ataki w cyberprzestrzeni mogą spowodować wyciek poufnych informacji, ogromne straty finansowe i finalnie, utratę reputacji organizacji. Firmy przechowują ogromne ilości danych klientów, pracowników i partnerów biznesowych, a zabezpieczenie ich stanowi kluczowy aspekt działalności i ochrony interesów każdego przedsiębiorcy. Rosnąca ilość informacji podlegających przetwarzaniu zwiększa ekspozycję na ryzyko, które trzeba właściwie ocenić.

Współczesne państwa również są coraz bardziej zależne od infrastruktury cyfrowej. Ataki na systemy krytycznej infrastruktury, takie jak elektrownie, sieci energetyczne czy systemy obronne, mogą mieć poważne konsekwencje dla bezpieczeństwa narodowego, prowadzić do awarii systemów informatycznych, co może zakłócić działanie firm, instytucji publicznych i innych organizacji.

Bez edukacji, prawa i technologii nie ma cyberbezpieczeństwa

Systemowe uporządkowanie kwestii cyberbezpieczeństwa podejmowane jest na poziomie regulacyjnym. Unijny akt o odporności cybernetycznej (CRA) czy dyrektywa NIS2 wymagają proaktywnego podejścia do bezpieczeństwa, wdrożenia procesów zarządzania ryzykiem i opracowania planów reagowania.

Jednak niezależnie od wymagań regulacyjnych wszystkie organizacje i każdy użytkownik z osobna powinni zweryfikować swoje zachowania w cyberprzestrzeni w kontekście ewolucji zagrożeń. Kluczowe jest ograniczone zaufanie i bardzo krytyczna postawa do wszelkich informacji – zwłaszcza takich, które nakłaniają do wykonania wcześniej nie planowanych działań lub mających na celu zmianę opinii.

Droga do zminimalizowania skutków ataków musi jednak w pierwszej kolejności prowadzić przez stosowanie mechanizmów technologicznych, narzędzi i środków organizacyjnych opartych na świadomości ludzi korzystających z dobrodziejstw ery cyfrowej.

W miarę jak technologia staje się bardziej powszechna, edukacja na temat bezpieczeństwa cyfrowego również się rozwija. Coraz więcej osób rozumie, że korzystanie z internetu i urządzeń elektronicznych wiąże się z pewnymi ryzykami. Użytkownicy są bardziej ostrożni w zakresie stosowania haseł i bezpiecznych zachowań w sieci (np. “klikanie” podejrzanych linków). Organizacje rządowe, instytucje edukacyjne i firmy prowadzą kampanie informacyjne na temat cyberbezpieczeństwa. To pomaga podnieść świadomość i zachęca do stosowania dobrych praktyk.

Coraz większa świadomość cyberbezpieczeństwa, stosowanie zaawansowanych technologii zabezpieczeń, a także wymiana informacji przyczynią się do wzrostu odporności całych sektorów gospodarki, a w tej perspektywie – całego społeczeństwa. Spierając się o to, czy

cyberbezpieczeństwo jest jak Yeti, chyba najlepiej, by było prawdziwe, ale niewidoczne dla nas.

Krzysztof Szczepański

Dyrektor Departamentu Bezpieczeństwa i Ryzyka, KIR