DGP | Cyberbezpieczeństwo

ekstra 14 lutego 2024, nr 32 (6197) dodatek informacyjno-promocyjny GAZETAPRAWNA.PL

> Dyrektywa NIS2 przyniesie istotne zmiany w zakresie podejścia do kwestii zapobiegania i reagowania na cyberataki
>
> **Justyna Wilczyńska-Baraniak,** Partnerka EY D3

Złą AI pokona tylko dobra

Wobec cyberataku sztucznej inteligencji człowiek może być bezbronny. Chyba, że odpłaci jej tą samą bronią D2

E-sklepy i ich klienci na celowniku

Rosnąca liczba i wartość transakcji oraz nowe możliwości transakcji kuszą przestępców D4

Fot. Shutterstock

Bezpiecznie już było

Rozwój sztucznej inteligencji, powszechna cyfryzacja, inwencja przestępców, rywalizacja światowych potęg gospodarczych czy wreszcie agresja Rosji, radykalnie zwiększyły poziom zagrożeń w cyberprzestrzeni

Instytucje, firmy, zwykli ludzie – na radarze cyberprzestępców są wszyscy bez wyjątku. Według Statista.com w styczniu 2024 r. z internetu korzystało 5,35 mld osób, czyli dwie trzecie ludzi na Ziemi.

Użytkownik internetu narażony jest na ataki, nawet wtedy, kiedy... śpi. Coraz więcej jego danych, także wrażliwych, znajduje się bowiem w cyfrowej chmurze, coraz więcej jego urządzeń komunikuje się z internetem bez przerwy. Dyrekcja Generalna Komisji Europejskiej ds. Sieci Komunikacyjnych, Treści i Technologii (DG CONNECT) szacuje, że w 2023 r. było na świecie 40 mld urządzeń podłączonych do internetu rzeczy (IoT) i w ciągu kolejnych trzech lat liczba ta wzrośnie do prawie 50 mld. To nie tylko smartfony, tablety, laptopy, routery czy smart-TV, ale też pralki, lodówki, roboty kuchenne i inne sprzęty AGD, drzwi, bramy garażowe, kamery monitoringu, e-nianie... I samochody oczywiście.

To oznacza jedno: potencjalnych celów przybywa, a prawda jest brutalna: jeśli ty możesz online sterować swoim urządzeniem, to haker – również.

21 proc.
Taki **odsetek ataków hakerskich w 2023 r.** dotyczył wykorzystania backdoorów (furtek) zostawionych najczęściej przez twórców oprogramowania w celu jego modyfikacji i doskonalenia, według raportu IBM X-Force

Fejki, luki, hejt

Google w raporcie „Cybersecurity Forecast 2024 Insights for future planning" przewiduje nasilenie dwóch rodzajów zagrożeń w sieci. Na czoło wysunęły się obecnie fałszywe treści – teksty, zdjęcia, filmy. Złoczyńcy fabrykują treści, podszywają się pod znane osoby, tworzą fikcyjne strony usług lub sklepów internetowych i umieszczają linki do nich w serwisach społecznościowych (m.in. FB), by dokonać kradzieży, oszustw, szantaży albo wprowadzić w błąd, bądź zmanipulować jednostki, grupy, a nawet całą opinię publiczną.

Drugą grupę zagrożeń dla przeciętnego użytkownika stanowią – rekordowo zaawansowane za sprawą rozwoju AI – ataki hakerskie na luki w zabezpieczeniach systemów informatycznych i w oprogramowaniu rozmaitych urządzeń. Luk jest mnóstwo również m.in. w bazach danych zawierających wrażliwe informacje. W 2023 r. głośno było o kradzieży personaliów, numerów PESEL i wyników badań ponad 50 tys. pacjentów z bazy polskiego laboratorium medycznego ALAB. Był to jeden z licznych ataków ransomware, czyli dla okupu.

Szczególnie zagrożeni w cyberprzestrzeni są z jednej strony seniorzy (padający ofiarą różnego typu oszustw), a z drugiej – najmłodsi użytkownicy. Z raportu NASK „Nastolatki 3.0 (2023)" wynika, że młodzi ludzie spędzają w internecie średnio 5 godzin i 36 minut na dobę w dni powszednie oraz 6 godzin i 16 minut w weekendy i święta. Od samego początku swej przygody (a zaczynają ją coraz wcześniej – średnio w wieku 8 lat i 5 miesięcy) narażeni są na szkodliwe treści oraz agresję i przemoc online, co rzutuje na ich psychikę i ma coraz częściej dramatyczne konsekwencje.

Wszystkie te zagrożenia – a to tylko wierzchołek góry lodowej – stanowią coraz większe wyzwanie dla państw wspierających rozwój cyfrowego społeczeństwa.

U progu cyberpandemii?

Państwa z ich instytucjami i infrastrukturą, także tą krytyczną, oraz przedsiębiorstwa są zanurzone w sieci od dawna, a wraz z kolejnymi etapami cyfryzacji – zanurzają się jeszcze głębiej. W cyberprzestrzeni działają platformy usług publicznych, firm i instytucji oraz systemy bankowe. Nic dziwnego, że cyberbezpieczeństwo stało się jednym z kluczowych sektorów rozwoju technologii, a jednocześnie fundamentem polityki publicznej i strategii firm.

– W złożonym krajobrazie 2023 r. sektor ten rósł zdecydowanie szybciej niż gospodarka światowa i – co znamienne – szybciej niż cały sektor technologiczny. Rok 2024 rok będzie krytyczny. Wszyscy liderzy, w polityce i biznesie, powinni się skupić na przygotowaniach do nadchodzącej z potężną siłą cyberpandemii – ostrzega Lucy Szaszkiewicz z 1Strike.io, firmy etycznych hakerów, których oprogramowanie w sposób ciągły, cykliczny i automatyczny hakuje systemy IT, by wskazać nie tylko pojedyncze podatności i furtki, ale aktualne scenariusze i techniki, jakie mogą zastosować cyberprzestępcy.

Michał Grzelak i Krzysztof Liedel, znani eksperci ds. bezpieczeństwa, już dekadę temu zwracali uwagę, że cyberprzestrzeń stała się jednym z kluczowych obszarów rywalizacji nie tylko przedsiębiorców i instytucji, ale też państw. Za pomocą narzędzi IT można z jednej strony dokonywać ataków na instytucje i infrastrukturę krytyczną krajów (ruch lotniczy, kolejowy, zapory wodne, systemy nawigacji...) – co grozi ich destabilizacją, z drugiej – wpływać na treści rozpowszechniane w mediach, a za ich pośrednictwem na sytuację gospodarczą i polityczną, w tym demokratyczne wybory (wśród przykładów podawane są wybory prezydenckie w USA w 2016 r. i referendum brexitowe).

W minionych latach cyberprzestrzeń była miejscem ataków z użyciem malware, wirusów i robaków, kradzieży tożsamości i danych, modyfikacji i niszczenia danych, blokowania dostępu do usług i szantaży dla okupu (ransomware), ataków socjotechnicznych (króluje phishing – wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję) i zaawansowanych ataków APT (advanced peristant threat).

Wrogie armie i służby wywiadowcze sięgają po coraz bardziej wyrafinowane techniki, które trudno wykryć i ukrócić bez ścisłej międzynarodowej współpracy. W 2023 r. udało się m.in. zablokować proceder Rosyjskiej Służby Wywiadu Zagranicznego polegający na wprowadzeniu groźnych zmian w oprogramowaniu trafiającym do tysięcy podmiotów na świecie. W kontrakcji wzięły udział: Służba Kontrwywiadu Wojskowego, CERT Polska, FBI, Amerykańska Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA), Narodowa Agencja Bezpieczeństwa (NSA), a także Brytyjskie Narodowe Centrum Bezpieczeństwa Cybernetycznego (NCSC). Publiczne instytucje wsparł Microsoft.

AI – potężna broń

W najnowszych raportach o cyberzagrożeniach na pierwszy plan wysuwa się stosowanie sztucznej inteligencji (AI) – zarówno w cyberatakach, jak i w systemach cyberbezpieczeństwa.

– Wraz z upowszechnianiem AI rośnie ryzyko nadużywania tej technologii przez cyberprzestępców, np. do tworzenia fałszywych informacji, wykradania danych, infiltrowania systemów zabezpieczeń – wylicza Krzysztof Silicki, twórca pierwszego w Polsce zespołu reagującego na zagrożenia w internecie (CERT NASK w 1996 r.), od 20 lat reprezentujący Polskę w Radzie Zarządzającej Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

Google wskazuje na coraz częstsze wykorzystanie AI do phishingu i jego głosowej odmiany – vishingu (voice phishing), a także ataków esemesowych i za pośrednictwem komunikatorów. Działania te opierają się na wprowadzających w błąd komunikatach tekstowych, głosowych, fotograficznych lub filmowych generowanych przez AI. Gartner, działająca w 100 krajach amerykańska firma analityczno-badawcza, uważa, że w 2024 r. „cyberbezpieczeństwo stanie się strategicznym priorytetem, którego nie będzie można odizolować w dziale IT". A Lucy Szaszkiewicz wskazuje wyzwania w tym obszarze: złoczyńcy dostrzegli powiększającą się przepaść między firmami i instytucjami o wysokim i niskim poziomie cyberodporności oraz na ich styku, dlatego atakują słabe ogniwa – podmioty średnie, szczególnie z obszaru energetycznego, finansowego i medycznego.

Za sprawą postępu technologicznego, zwłaszcza AI, przestępcy zyskali zdolność prowadzenia ataków złożonych, adaptacyjnych i trudnych do wykrycia znanymi metodami; konieczne stało się więc permanentne monitorowanie odporności każdej organizacji.

Regulacje prawne, takie jak: DORA, NIS2 czy Cyber Act oraz AI Act, pomagają porządkować cyberprzestrzeń, ale nie nadążają za nowymi zjawiskami związanymi z rozwojem technologii, co utrudnia firmom i instytucjom skuteczną odpowiedź na ryzyka w cyberprzestrzeni.

I instytucjom publicznym, i przedsiębiorcom brakuje kompetencji, by walczyć z nowym typem cyberzagrożeń, konieczna jest więc automatyzacja procesów cyberbezpieczeństwa z użyciem nowych narzędzi opartych na AI. To otwiera pole dla utalentowanych informatyków.

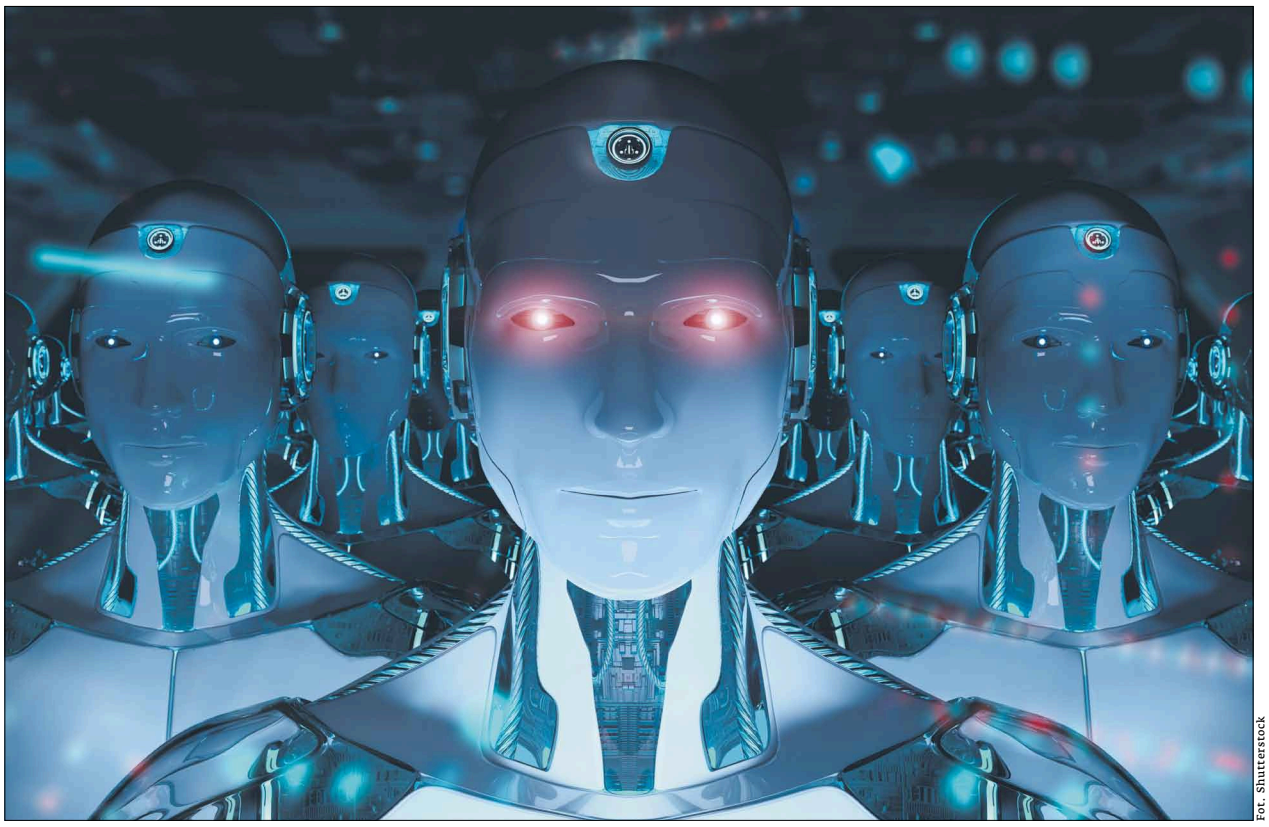
– W sektorze finansowym zacofana wcześniej Polska dołączyła dzięki technologiom cyfrowym do grona światowych liderów, Blik jest symbolem tej rewolucji. Dlaczego nie mielibyśmy powtórzyć tego sukcesu w sektorze cyberbezpieczeństwa? – stawia pytanie Lucy Szaszkiewicz.

Zbigniew Bartuś

Ten rok jest kluczowy dla cyberbezpieczeństwa

Zachodzą zmiany, cyberbezpieczeństwo nie będzie już tylko problemem działów IT – komentuje Lucy Szaszkiewicz z 1Strike.io. Więcej na: cyfrowa-gospodarka.gazetaprawna.pl

Złą AI pokona tylko dobra



Fot. Shutterstock

Robert Lewandowski i Andrzej Duda zachwalają intratne inwestycje, inkasent w wideorozmowie na WhatsAppie żąda dopłaty za prąd na wskazane konto, agent Rosji wygrywa wybory w RFN, smartfon rozpoczyna wojnę światową – katalog zagrożeń, jakie powoduje sztuczna inteligencja, jest właściwie nieograniczony

Członkowie działającego przy Komisji Nadzoru Finansowego zespołu ds. reagowania na incydenty związane z bezpieczeństwem komputerowym – CSIRT KNF (ang. Computer Security Incident Response Team) – już kilka razy w ostatnim czasie ostrzegali, że gwiazdor futbolu, prezydent RP i inne powszechnie znane osoby wcale nie występują w reklamach rzekomych „serwisów inwestycyjnych". Oszuści używają ich wizerunków i barwy głosów do wygenerowania deepfake'ów, aby zdobyć zaufanie potencjalnych ofiar. Tysiące Polaków powierzyło w ten sposób złoczyńcom lwią część albo nawet całe oszczędności życia. Najgłośniejsze na świecie ataki tego typu pozwoliły cyberprzestępcom zgarnąć jednorazowo nawet do 25 mln dol.

Jeszcze niedawno tego typu oszustwa na masową skalę były niemożliwe – z braku technologii. „Toy Story", pierwszy w dziejach firm długometrażowy stworzony w całości techniką komputerową, kosztował niespełna trzy dekady temu 30 mln dol. – większość tej kwoty poszło na zaprojektowanie rewolucyjnego programu do renderowania obrazów i na 117 najmocniejszych komputerów. Wygenerowanie jednej klatki zajmowało nawet 30 godzin (w filmie jest ich... 114 tys.). Dziś można wykreować tego typu film milion razy szybciej na komputerze domowym i oprogramowaniu opartym na sztucznej inteligencji.

Na łasce algorytmów

W wielu dziedzinach AI pozwoliła silnie zautomatyzować i przyspieszyć działania. Niestety, dzięki algorytmom przestępcy nie tylko tworzą fałszywe treści (teksty, zdjęcia, filmy, komunikaty głosowe), podszywając się pod krewnych ofiar lub osoby czy instytucje mające wzbudzić zaufanie, lecz także masowo rozsyłają fałszywe treści – za pomocą esemesów, e-maili, komunikatorów internetowych lub serwisów informacyjnych i społecznościowych. A to tylko część umiejętności sztucznej inteligencji, coraz szerzej wykorzystywanej nie tylko przez kryminalistów, lecz także przez tych, którzy prowadzą w cyberprzestrzeni niecne działania polityczne, gospodarcze i wojskowe w celu zdestabilizowania lub zniszczenia konkurentów albo wrogów.

W pierwszym kompleksowym raporcie NASK na temat bezpieczeństwa w epoce huraganowego rozwoju sztucznej inteligencji („Cyberbezpieczeństwo AI. AI w cyberbezpieczeństwie") Krzysztof Silicki, jeden z pionierów tej dziedziny, przywołując raporty Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, ENISA, zwraca uwagę, że systemy sztucznej inteligencji w sposób niespotykany w dziejach zwiększają liczbę i intensywność znanych dotąd zagrożeń w cyberprzestrzeni (m.in. przez wspomnianą automatyzację), a jednocześnie tworzą i stale poszerzają zupełnie nowy obszar zagrożeń – specyficznych dla algorytmów, modeli i danych wykorzystywanych przez AI.

Unia Europejska w dyrektywie NIS oraz kolejnych aktach prawnych przyjmowanych od 2016 r. uznaje za cyberincydenty nie tylko klasyczne ataki na infrastrukturę i usługi cyfrowe (jak DDoS, phishing, ransomware, łamanie haseł, wycieki danych), lecz także wszelkie zagrożenia, które powodują bądź mogą spowodować przerwy lub nieprawidłowe działanie usług cyfrowych. Eksperci podkreślają, że w przypadku AI awarie systemów, błędy w konfiguracji, programowaniu i treningu algorytmów oraz ataki powodujące nieprawidłowe działanie modeli opartych na sztucznej inteligencji mogą być źródłem zagrożeń na nieznaną wcześniej skalę. I to takich, które łatwo przenoszą się z cyberprzestrzeni do rzeczywistości. Błędy w algorytmie rozpoznawania twarzy na lotnisku wskażą niewinnego jako terrorystę (lub odwrotnie), błędy w algorytmie fiskusa mogą niszczyć podatników, w tym firmy, braki w procedurach weryfikacji źródeł i niedoskonałe mechanizmy animizacji otwierają drogę do wycieków wrażliwych danych i ich dowolnego wykorzystywania przez złoczyńców różnej maści.

Nieznane dotąd zagrożenia wynikają też z potencjalnej integracji rozrastających się cyfrowych baz danych i możliwości ich błyskawicznej, wielowątkowej analizy za pomocą AI. Pozyskane w ten sposób wrażliwe treści mogą służyć do kradzieży, oszustw, szantaży, manipulacji – i w skali indywidualnej, i na poziomie krajów (gdy dotyczą czołowych polityków lub wojskowych).

Równocześnie rośnie rola AI w cybermanipulacji jednostkami i zbiorowościami. Odpowiednio sfabrykowane i rozpowszechnione fałszywe informacje, uwiarygodnione za pomocą fałszywych zdjęć i filmów, mogą destabilizować sytuację gospodarczą (w tym np. notowania giełdowe czy walutowe) i polityczną przez kreowanie nieprawdziwego obrazu rzeczywistości, wzniecanie paniki, manipulowanie opinią publiczną.

Człowiek nie ma szans

Wkroczyliśmy w epokę, w której dobra AI, służąca ludziom do usprawniania i doskonalenia wielu procesów w biznesie, edukacji, informacji, komunikacji, medycynie, bankowości, administracji, a co za tym idzie – do poprawy poziomu i jakości życia, będzie nieustannie atakowana przez złą AI, wykorzystywaną do realizacji celów kryminalnych, politycznych i militarnych.

– Wnioski płynące z raportów ENISA wyraźnie wskazują, iż konwencjonalne zabezpieczenia systemów informatycznych muszą zostać wzbogacone o cały katalog zabezpieczeń wynikających ze specyficznych zagrożeń dla samouczących się algorytmów AI – stwierdza Krzysztof Silicki.

– Każdy człowiek i każde inteligentne urządzenie są podatni na ataki. Jeśli dołączymy do tego sztuczną inteligencję, przyszłość nie rysuje się kolorowo, zwłaszcza że już niebawem człowiek straci na rzecz AI pozycję najinteligentniejszej istoty na świecie – komentuje Mikko Hyppönen z WithSecure, uznany fiński ekspert ds. cyberbezpieczeństwa. Ostrzega, że żaden człowiek nie powstrzyma złej AI.

– Z jej atakami może sobie poradzić wyłącznie dobra AI, zaprzężona do boju przez specjalistów ds. cyberbezpieczeństwa – podkreśla.

Źródłem największego niepokoju w świecie wysokich technologii (i nie tylko) pozostaje to, że nawet topowi specjaliści IT nie mają pojęcia, w jaki sposób sztuczna inteligencja pokroju ChatGPT-4 robi to, co robi. Wiąże się tym obawa, że AI może się wymknąć spod ludzkiej kontroli. A wtedy nie będzie ani dobra, ani zła, tylko po prostu – z ludzkiego punktu widzenia – nieobliczalna i śmiertelnie groźna.

Naukowcy z Georgia Institute of Technology w Atlancie przetestowali w ostatnim czasie różne narzędzia sztucznej inteligencji – GPT-3.5 i GPT-4 firmy OpenAI, Claude 2 firmy Anthropic i Llama 2 firmy Meta. Eksperyment opisany przez „New Scientist" dowiódł ponoć, że ChatGPT-4, najsłynniejsza i najpopularniejsza w świecie AI (stworzona przez OpenAI), w celu „zaprowadzenia pokoju na świecie" jest gotowa przeprowadzić atak nuklearny.

Obosieczny AI Act

Kompleksową odpowiedzią UE na obawy i wątpliwości związane z żywiołowym rozwojem jest akt o sztucznej inteligencji (AI Act). Porozumienie w sprawie kluczowych punktów tej regulacji udało się zawrzeć w grudniu 2023 r., a na początku lutego 2024 r. ambasadorowie państw UE jednogłośnie je potwierdzili.

Prace nad AI Act nie przebiegają jednak gładko i bez konfliktów, a to dlatego, że zbyt restrykcyjne przepisy mogą podciąć skrzydła europejskim firmom (w tym start-upom) pracującym nad zaawansowanymi modelami sztucznej inteligencji. Wtedy Europa pozostanie w tyle za potentatami z USA, ale też z Chin, a być może także z Rosji. Oznaczałoby to nie tylko kolejne zapóźnienie w wyścigu technologicznym, lecz także – co może się okazać istotniejsze – bezbronność wobec ataków złej AI rozwijanej w krajach dalekich od demokracji i respektowania wartości leżących u podstaw AI Act. Byłby to kolejny kluczowy obszar, w którym zachodnia Europa uzależniłaby się de facto od wsparcia USA.

Na ten aspekt zwraca uwagę Francja, wspierana przez Niemcy i Włochy. Ostatecznie Francuzi przystali na kompromis, zastrzegając, że wdrożenie AI Act – zapewniając przejrzystość i etykę działań – nie może jednak utrudniać rozwoju konkurencyjnych modeli sztucznej inteligencji ani obciążać nadmiernie firm, których działalność wiąże się z wysokim ryzykiem.

KE chce, by do ostatecznego zatwierdzenia AI Act doszło jeszcze w tej kadencji: głosowanie na sesji plenarnej europarlamentu ma się odbyć w kwietniu, potem dokument musi uzyskać aprobatę właściwych ministrów wszystkich państw. Zakazy niedozwolonych praktyk zaczęłyby obowiązywać po sześciu miesiącach, a zobowiązania dotyczące modeli AI po roku od publikacji przepisów w Dzienniku Urzędowym UE. Większość pozostałych regulacji ma wejść w życie po dwóch latach.

Na co trzeba uważać

Przybierające na sile techniki ataków w cyberprzestrzeni z użyciem AI według Mikka Hyppönena:

- **Deepfake** – tworzenie fałszywych obrazów lub filmów, które mają imitować wygląd i głos prawdziwych osób lub zdarzeń
- **Deepscam** – wielkoskalowe oszustwa inwestycyjne, phishingowe, ataki ransmoware itp.
- **Duże modele językowe (LLM)** – AI typu ChatGPT w rękach cyberprzestępców jako automatyczny generator złośliwego oprogramowania
- **Automatyzacja ataków z użyciem złośliwego oprogramowania** w celu skokowego zwiększenia ich skuteczności, np. malware napędzane przez AI jest w stanie samoistnie zmieniać swój kod, uczyć się na własnych błędach i naprawiać je, aby uniknąć wykrycia i przystosować się do nowego środowiska
- **Luki zero-day** – AI pomaga błyskawicznie wyszukiwać nieznane autorom błędy w systemach i wykorzystywać je m.in. do akcji phishingowych, penetracji systemów, instalowania złośliwego oprogramowania i kradzieży danych

Kupię, sprzedam, oszukuję, czyli jak nie dać się okraść w internecie

O tym, jak działają internetowi oszuści, opowiadał Piotr Konieczny z niebezpiecznik.pl. Można go wysłuchać na: gazetaprawna.pl/podcasty

SUBIEKTYWNIE

Fot. Shutterstock

NIS2: wyzwania i szanse dla przedsiębiorców w Polsce

JUSTYNA WILCZYŃSKA-BARANIAK

partnerka EY, liderka Zespołu Prawa Własności Intelektualnej, Technologii i Danych Osobowych, adwokatka

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dalej: „dyrektywa NIS2" lub „NIS2") weszła w życie na początku 2023 r. Państwa członkowskie UE są zobowiązane do implementacji jej postanowień do krajowego porządku prawnego do 18 października 2024 r. Dyrektywa NIS2 ustanawia szereg wymogów w zakresie środków cyberbezpieczeństwa i raportowania incydentów. Przyniesie ona istotne zmiany w zakresie podejścia do kwestii zapobiegania i reagowania na cyberataki.

Szeroki zakres

Z raportu CSO Council „W oczekiwaniu na NIS2. Stan przygotowań. Badanie CSO Council" wynika, że organizacje, które były już objęte regulacją NIS lub wytycznymi sektorowymi, są bardziej zaawansowane w przygotowaniach do wdrożenia nowych wymogów wynikających z NIS2. Natomiast przedsiębiorstwa, które dotąd nie podlegały regulacjom, w większości czeka jeszcze wiele pracy nad dostosowaniem się do wytycznych. Warto równocześnie nadmienić, że co czwarta firma objęta przepisami dyrektywy nie ma jeszcze świadomości, że nowe przepisy będą jej dotyczyć.

Dyrektywa NIS2 dotknie tzw. podmioty kluczowe i ważne. Kategorie te zastępują pojęcia znane z dyrektywy NIS – operatorów usług kluczowych i dostawców usług cyfrowych.

Dyrektywa NIS2 wskazuje sektory, w których działają podmioty kluczowe i ważne. Otóż ma ona zastosowanie w sektorach: energetyki, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, zarządzania usługami ICT, podmiotów administracji publicznej oraz przestrzeni kosmicznej (podmioty kluczowe). Ma również zastosowanie do podmiotów ważnych, to jest prowadzących działalność w sektorach: pocztowym, wytwórczym, żywności, zarządzania odpadami, chemikaliów, dostawców usług cyfrowych oraz research.

NIS2 obowiązuje wszystkie podmioty, które prowadzą działalność w wymienionych gałęziach gospodarki i są uznawane za średnie lub duże przedsiębiorstwa, czyli zatrudniają co najmniej 50 pracowników i ich roczny obrót i (lub) roczna suma bilansowa przekracza 10 mln euro. Nowa dyrektywa obejmie także mikroprzedsiębiorstwa i małe przedsiębiorstwa, jeżeli spełnią kryteria wskazujące na ich kluczową rolę dla społeczeństwa, gospodarki lub określonych sektorów, lub typów usług.

Wdrożenie regulacji

Transpozycja NIS2 jest szansą na uporządkowanie przepisów dotyczących cyberbezpieczeństwa w Polsce. Niemniej wymaga ona szerokich konsultacji społecznych ze wszystkimi podmiotami reprezentującymi 18 sektorów objętych regulacją. Szacuje się, że w przeciwieństwie do kilkuset podmiotów, do których obecnie stosuje się ustawę o krajowym systemie cyberbezpieczeństwa, dyrektywa NIS2 nakłada obowiązki na kilka do kilkunastu tysięcy polskich przedsiębiorstw i podmiotów publicznych.

Dotychczasowe doświadczenia związane z niedoszłą nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa (UKSC) wskazują, że implementacja dyrektywy NIS2 do polskiego porządku prawnego będzie procesem długotrwałym. Prace nad nowelizacją UKSC trwały ponad trzy lata i we wrześniu poprzedniego roku projekt został wycofany.

Zgodnie z terminem transpozycji dyrektywa NIS2 powinna zostać wprowadzona do polskiego porządku prawnego do 18 października 2024 r. Po tym terminie polscy przedsiębiorcy oraz podmioty publiczne będą zobowiązane do stosowania nowych środków w zakresie cyberbezpieczeństwa.

Analizując modele zaproponowane w innych państwach członkowskich, wydaje się, że istnieją dwa najbardziej prawdopodobne scenariusze:

- gruntowna nowelizacja UKSC,
- przyjęcie nowej ustawy uchylającej poprzednią.

Z perspektywy biznesu i pewności obrotu prostszym i pewniejszym rozwiązaniem byłoby uchwalenie nowej ustawy i zamknięcie skomplikowanego rozdziału, jaki stanowiły kolejne próby nowelizacji UKSC.

Należy mieć także nadzieję, że transpozycja NIS2 nie będzie odbywała się w pośpiechu i proces legislacyjny zostanie przeprowadzony z szerokim udziałem ekspertów, przedstawicieli biznesu oraz organizacji społecznych.

Wyzwaniem związanym z wdrożeniem NIS2 są środki cyberbezpieczeństwa. To priorytet zarówno dla państw członkowskich UE, które będą musiały wprowadzić efektywny mechanizm egzekwowania wprowadzenia tych środków, jak i dla przedsiębiorstw objętych dyrektywą NIS2.

> Co czwarta firma objęta przepisami dyrektywy nie ma jeszcze świadomości, że nowe przepisy będą jej dotyczyć

W NIS2 znajduje się lista 10 środków cyberbezpieczeństwa (art. 21 ustęp 2 lit. a–j). Obejmuje ona m.in. wprowadzenie zasad dotyczących: zarządzania ryzykiem, bezpieczeństwa łańcucha dostaw oraz określonych środków technicznych, takich jak kryptografia czy uwierzytelnianie wieloskładnikowe.

Należy wskazać, że państwa członkowskie w dużej mierze trzymają się katalogu środków przewidzianych w tekście dyrektywy NIS2. Takie wnioski wyciągnąć można z analizy projektów w Chorwacji, Niemczech, Belgii czy Finlandii.

Stawia to zatem przed polskim ustawodawcą pytanie, czy w ramach polskiego procesu implementacji dyrektywy NIS2 należy rozbudować katalog środków cyberbezpieczeństwa, czy też poprzestać na 10 wymogach z dyrektywy NIS2.

W mojej ocenie konieczne jest przede wszystkim zapewnienie proporcjonalnego stosowania wymogów NIS2. Zgodnie z art. 21 ust.2 NIS2 w ramach analizy proporcjonalności należy wziąć pod uwagę:

- stopień narażenia na ryzyko,
- wielkość podmiotu,
- prawdopodobieństwo wystąpienia incydentów,
- skutek wystąpienia incydentu dla społeczeństwa oraz gospodarki.

Tak sformułowana zasada proporcjonalności tworzy pewien „bezpiecznik" dla adresatów NIS2. Pozwala na dokonanie samodzielnej oceny, w jaki sposób wdrożyć określone obowiązki. Może to być istotne przy wdrażaniu wymogów związanych z bezpieczeństwem łańcucha dostaw. Jako przykład można podać sytuację, w której organ wymaga szeroko zakrojonej kontroli poddostawców. W takiej sytuacji należy zbadać, czy nakaz organu nie sięga za daleko, a kluczowym mechanizmem będzie tu właśnie test proporcjonalności. Zasada proporcjonalności powinna pozwolić na ocenę, który poddostawca i w jakim stopniu jest kluczowy z perspektywy bezpieczeństwa łańcucha dostaw.

Zgłaszanie incydentów

Dyrektywa NIS2 wprowadza także istotne zmiany w zakresie raportowania incydentów.

Z procesem raportowania incydentów wiąże się wiele wyzwań. Przede wszystkim podmioty kluczowe i ważne będą musiały dostosować swoją strukturę organizacyjną tak, aby odpowiednio szybko zebrać informacje o incydencie i przesłać je do właściwego organu nadzorczego. Co równie ważne, za proces ten odpowiedzialni będą członkowie zarządu, również ci niezajmujący się bezpieczeństwem informacji i IT. Wymusza to przeprowadzenie odpowiednich szkoleń i wdrożenie mechanizmów, które pozwolą zminimalizować ryzyko odpowiedzialności zarządu za błędy w raportowaniu incydentów.

NIS2 to nie tylko wymogi i kary – dla podmiotów kluczowych mogące wynosić nawet 10 mln euro lub 2 proc. całkowitego rocznego obrotu. Z procesem implementacji dyrektywy wiążą się liczne szanse dla przedsiębiorców. Szczególnie warto zwrócić uwagę, że uporządkowanie kwestii cyberbezpieczeństwa na poziomie UE zwiększy pewność prawa oraz podniesie poziom cyberbezpieczeństwa w państwach członkowskich. Pozytywnie wpłynie to na pozycję rynkową podmiotów inwestujących i dbających o poziom cyberbezpieczeństwa w swojej organizacji.

Fot. Shutterstock

Na celowniku e-sklepy oraz ich klienci

Dynamiczny rozwój e-commerce stwarza cyberprzestępcom coraz to nowe możliwości. Do cyberataków posuwa się czasami nawet rynkowa konkurencja

Szacuje się, że rosnąca branża e-commerce pada ofiarą już niemal jednej trzeciej wszystkich ataków cyberprzestępców. Do tego są one coraz bardziej wyrafinowane, choć wśród najbardziej popularnych pozostają te sprawdzone i dające najwięcej korzyści. Mowa o odmowie dostępu do usługi, czyli DOS (ang. Denial Of Service), gdzie cyberprzestępca stara się zająć całą dostępną moc serwera, na którym jest e-commerce lub marketplace.

– Można to porównać z rurami wodnymi, gdzie nagle ktoś, kto nie korzysta z prysznica, odkręca bardzo dużą liczbę kurków, tym samym znacząco zmniejszając lub całkowicie eliminując strumień dla potrzebujących. Przekładając to na informatykę, użytkownik nie będzie mógł dokonać zakupu, a tym samym firma handlowa odnotuje stratę – tłumaczy Andrzej Targosz, partner Bitspiration Booster, funduszu inwestującego m.in. w obszar cybersecurity.

Paweł Peryga, Head of DevOps Unity Group, wskazuje, że kolejną grupą ataków są te prowadzące do kradzieży danych, wyłudzeń zamówień. I podkreśla, że zazwyczaj widać je od razu, bo powodują niedostępność sklepu, zaszyfrowanie danych lub po dość krótkim czasie, przez wyłudzenia zamówień, kradzieże danych.

– Są to ataki realizowane przez hakerów indywidualnych czy wręcz całe grupy przestępcze. Od jakiegoś czasu obserwujemy ataki nieco bardziej wyrafinowane i realizowane przez konkurencję, np. kradzież zdjęć i opisów produktowych, wykupowanie produktów w celu obniżenia stanów magazynowych, czy np. analizę cen produktów i sprzedaż taniej. Są to rzeczy, które nie są oczywistymi przestępstwami, ale mają silne konsekwencje na konkurencyjnym rynku – dodaje Paweł Peryga.

Drzwi szeroko otwarte

Zabezpieczenie przed atakiem DoS i DDoS (odmiana DoS, następuje z wielu źródeł), zdaniem ekspertów nie jest trudne. Wystarczy mieć dobrze zaprojektowaną infrastrukturę i dobre serwery oraz łącza. Większość podmiotów na rynku e-commerce czy marketplace zdaje sobie sprawę z tego zagrożenia oraz całkiem dobrze sobie z nim radzi.

Dużo poważniejszym, bo uderzającym również w bezpieczeństwo klientów, jest atak obliczony na kradzież tożsamości cyfrowej użytkownika serwisu e-commerce. Jak mówią eksperci, włamanie na konto użytkownika na platformie e-commerce nie zagraża może tak bardzo finansom jak wejście na konto bankowe, jednak wielu z nas używa tych samych loginów i haseł do różnych serwisów, w tym skrzynki pocztowej.

– Jeżeli tak jest, to wyobraźmy sobie sytuację, że dane dostępowe do platformy e-commerce, z której korzystamy, to nasz adres e-mailowy i jedynie hasło. Po przejęciu takich danych i przy założeniu, że dokładnie tym samym hasłem logujemy się do naszej skrzynki pocztowej, intruz ma szeroko otwarte drzwi do przejęcia naszej poczty. Dostęp do skrzynki pocztowej daje natomiast możliwość przeprowadzenia resetu hasła we wszystkich platformach, do których się logujemy, zatem intruz finalnie uzyska dostęp do tych serwisów na takich samych uprawnieniach, na jakich robimy to my. A to już może mieć większy wpływ na nasze finanse – zauważa Andrzej Targosz.

Phishing jest szczególnie niebezpieczny w przypadku e-commerce – tani i łatwy do przeprowadzenia, nawet dla początkującego cyberintruza z zasobem wiedzy na poziomie informatyki szkoły średniej.

Poza tym e-sklepy są narażone na ataki typu ransomware polegające na zaszyfrowaniu danych, a następnie żądaniu okupu.

– W przypadku usług typu SaaS czy infrastruktury w modelu pay-as-you-go można natomiast mówić o nowym typie ataku, tzw. denial of wallet, czyli takim obciążaniu serwisu, aby wygenerować jak największy koszt po stronie operatora sklepu – zauważa Paweł Peryga.

Silne i iluzoryczne zabezpieczenia

Wina za skuteczność ataku spada na firmę, czyli e-sklep czy platformę zakupową, bo to jej obowiązkiem jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Dobra infrastruktura, serwery i łącza to podstawa, ale działania muszą być kompleksowe. Nie przypadkiem mówi się bowiem o „systemie bezpieczeństwa", a ten jest silny tak, jak mocne są jego najsłabsze ogniwa.

– A w wielu przypadkach są nimi ludzie. Nie możemy zapominać o ich szkoleniu, rozwoju i wyczulaniu na podejrzane kwestie. Przed ujawnieniem hasła administratora do systemu, klucza API nie uchroni nas nawet najbardziej wyrafinowany system, jeśli jakiś nasz pracownik po prostu to udostępni atakującemu. Od ludzi więc trzeba zacząć – twierdzi Paweł Peryga i dodaje, że w idealnym świecie to sami użytkownicy powinni zwracać uwagę na stopień zabezpieczeń i unikać logowania się do systemu niemającego zabezpieczenia dwuskładnikowego.

W dalszej kolejności jest mnóstwo obszarów, którymi można się zająć technicznie, czyli systemy inspekcji ruchu sieciowego (IDS/IPS), ukrycie sklepu za systemem anty-DDoS, anty-bot czy Web Application Firewall. E-commerce może liczyć na dopasowaną do ich potrzeb ofertę.

– Narzędzi jest tutaj bardzo wiele, a rynek ten jest już bardzo dojrzały i ma dostawców wdrażających komplet potrzebnych rozwiązań. Dostawcy ci mają już ofertę wyspecjalizowaną dla sklepów e-commerce i dobrze znają ich potrzeby w zakresie cybersecurity. Są gotowi też pokazać czy uruchomić takie systemy w formie testowej w ramach darmowego okresu próbnego – wylicza Paweł Peryga.

Z kolei użytkownicy powinni znaleźć w ustawieniach swojego konta funkcję, która nazywa się „silne uwierzytelnienie", „drugi składnik" czy „podniesienie poziomu bezpieczeństwa konta".

– Jeżeli platforma daje taką możliwość, to bezwzględnie powinniśmy z niej skorzystać, ponieważ usługa ta jest darmowa oraz znacznie podnosi poziom bezpieczeństwa nie tylko w zakresie usług e-commerce, lecz także innych naszych kont w internecie. Jeżeli będziemy korzystać z silnego uwierzytelniania wszędzie tam, gdzie to możliwe, to prawdopodobieństwo przejęcia naszych danych dostępowych jest mniejsze – zauważa Andrzej Targosz, podkreślając, że oczywistym wymogiem jest również stosowanie różnych loginów i haseł wszędzie tam, gdzie to możliwe. Przeglądarki internetowe pomagają w zapamiętywaniu loginów i haseł.

– Należy jeszcze raz podkreślić, że dziś samo zabezpieczenie w postaci loginu i hasła jest iluzoryczne. Właściwym zabezpieczeniem jest aktywny mechanizm silnego uwierzytelniania. Być może nie zdajemy sobie z tego sprawy, ale codziennie logujemy się do swojego telefonu w sposób, który może przypominać bezpieczne logowanie z wykorzystaniem FIDO (ang. fast identity online – red). To nie do końca ten sam mechanizm, ale doświadczenie użytkownika jest dokładnie takie samo. Wszystkie telefony, które nie są starsze niż sześć lat, mają wbudowany mechanizm oparty na bardzo bezpiecznym i jedynym odpornym na phishing mechanizmie FIDO. Coraz więcej dostawców usług internetowych w tym e-commerce decyduje się na wykorzystanie tego standardu w ochronie kont swoich klientów na platformie sprzedażowej – mówi Andrzej Targosz.

Prowadząc e-sklep, warto pamiętać, by na czarną godzinę mieć niezawodny system kopii bezpieczeństwa. Wysokiej jakości backup (kopia zapasowa) przechowywana w bezpiecznej lokalizacji oraz plan disaster-recovery uchroni przed poważnymi problemami biznesowymi

Poza tym należy zadbać o zabezpieczenie e-sklepu przed atakami i wyciekami danych przez instalacje programu antywirusowego. Bez tego wszystkie inne działania nie odniosą skutku.

Ile trzeba wydać

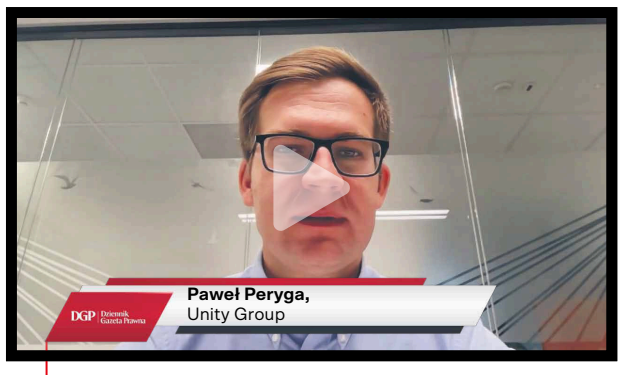
Bezpieczeństwo oczywiście kosztuje i nie jest to wydatek jednorazowy. Trzeba je okresowo testować, czy to w formie testów penetracyjnych, czy przeciążeniowych. Należy sprawdzać sprawność backupu i 1–2 razy do roku wykonywać próbne odtworzenie zgodnie z disaster recovery plan. Eksperci szacują koszty bezpieczeństwa w e-commerce na 3–5 proc. TCO (całkowitego kosztu posiadania).

– Są to niestety rzeczy, które trudno „sprzedać" w organizacji. Szczególnie takiej, w której jeszcze nigdy nie było poważniejszych incydentów bezpieczeństwa. Niestety dopiero tego typu zdarzenia uczą organizacje i powodują, że w budżecie pozycja „security" w ogóle znajduje swoje miejsce. Dlatego też o bezpieczeństwie często mówi się w kategoriach straszenia. Czy to dobra metoda. Na pewno nie dla świadomych liderów, osób odpowiedzialnych za IT. W dojrzałych organizacjach dyrektor e-commerce pracuje ramię w ramię z dyrektorem IT, a coraz częściej obaj zasiadają w zarządzie i mają ogromny wpływ na budżet – komentuje Paweł Peryga.

Eksperci ostrzegają, że bagatelizowanie tych kwestii to proszenie się o kłopoty.

– Koszty implementacji standardu FIDO nie są wysokie – mówi Andrzej Targosz. I dodaje, że to standard dostępny dla wszystkich i sam w sobie nic nie kosztuje. Jeżeli za usługą e-commerce stoi organizacja, która ma własnych programistów, to może podjąć się takiej implementacji samodzielnie. Jeżeli woli jednak delegować te działania do kogoś, kto robi to na co dzień i zna się na implementacji mechanizmów silnego uwierzytelniania, takie firmy możemy znaleźć również na rodzimym rynku.

Poza tym dostępne są również narzędzia, które nie wymagają żadnych zmian w platformie e-commerce i potrafią standard FIDO oraz inne mechanizmy chroniące użytkowników zaimplementować całkowicie bezinwazyjnie. Czyli bez zmian w kodzie serwisu e-commerce i bez dodatkowych wymagań po stronie użytkowników serwisu. W przypadku ostatniego wariantu uruchomienie usługi silnego uwierzytelniania dla wszystkich klientów platformy e-commerce to projekt na dni lub tygodnie w zależności od organizacji po stronie właściciela platformy e-commerce.

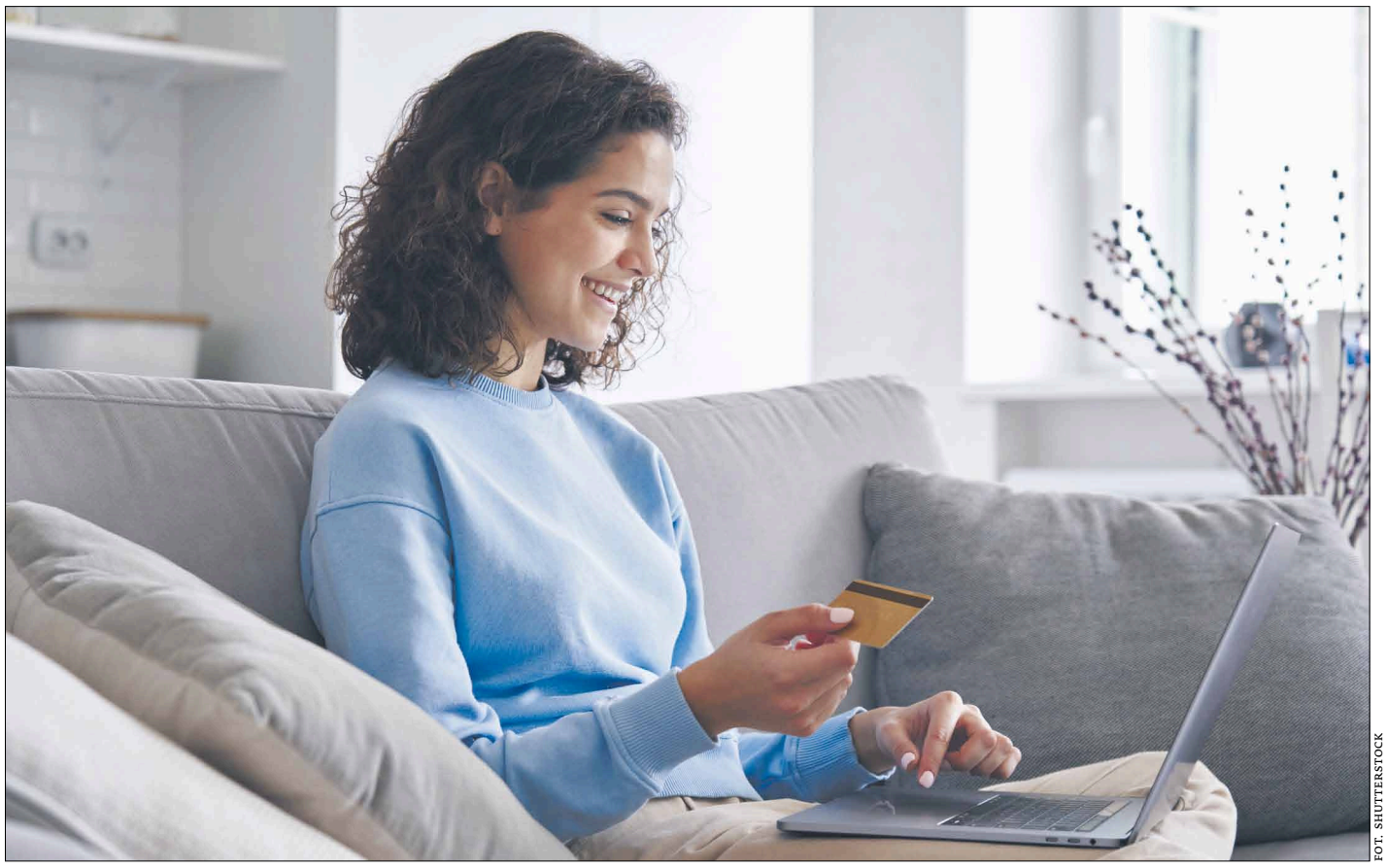


Na transformację handlu trzeba patrzeć całościowo

O niuansach związanych z cyberbezpieczeństwem w e-commerce mówi Paweł Peryga, Head of DevOps Unity Group – więcej na: cyfrowa-gospodarka.gazetaprawna.pl

Jak ochronić swoje finanse przed cyberprzestępcami?

Choć popularność bankowości internetowej rośnie, część klientów podchodzi do niej z dystansem. Jednym z głównych powodów jest obawa o bezpieczeństwo danych, a tym samym – o oszczędności zgromadzone na koncie. Alior Bank przypomina ważne zasady, których stosowanie pomoże obronić się przed cyberprzestępcami.



FOT. SHUTTERSTOCK

Zadbaj o silne hasło

Silne hasło to podstawa zapewnienia bezpieczeństwa informacji chronionej w sieci – szczególnie, jeśli celem jego stosowania jest ochrona dostępu do pieniędzy. Nie może być to kombinacja cyfr związanych np. z datą urodzenia użytkownika. W procesie jego tworzenia zaleca się łączenie małych i dużych liter, korzystanie z cyfr oraz znaków specjalnych.

Należy pamiętać o tym, aby nie stosować hasła wykorzystywanego do bankowości internetowej w innych serwisach. Jeśli mamy trudność w zapamiętaniu danych do logowania, można skorzystać z menadżera haseł.

Hasło do bankowości internetowej powinno być zmieniane systematycznie, najlepiej co kilka miesięcy. Niektóre banki informują klientów o konieczności jego modyfikacji podczas logowania do systemu.

Siła hasła zależy też od jego ochrony przez użytkownika. Należy szczególnie zwracać uwagę na to, czy hasło do bankowości wpisujemy w serwisie bankowym, np. weryfikując adres strony. Wszelkie próby żądania danych logowania do bankowości przez stronę, która nie jest serwisem banku, powinny zostać przez nas uznane za podejrzane.

Stosuj podwójne uwierzytelnienie

Warto korzystać z podwójnego (2FA, two-factor authentication) lub wieloskładnikowego (MFA, multi-factor authentication) uwierzytelnienia. Wprowadzenie dodatkowego elementu, takiego jak autoryzacja przez SMS, token czy akceptacja powiadomienia w aplikacji mobilnej sprawia, że nawet w przypadku, w którym oszust uzyska hasło, dostęp do konta będzie nadal uwarunkowany drugim elementem. W przypadku bankowości internetowej dodatkowe zabezpieczenia są obligatoryjne.

- Przestępcy niestety doskonale zdają sobie sprawę z popularności metody 2FA i dostosowują swoje techniki ataku. Warto być świadomym potencjalnych zagrożeń, takich jak fałszywe bramki płatności, które prowadzą do nieprawdziwych stron logowania do banku poprzez które przestępcy starają się pozyskać dane uwierzytelniające. Atakujący często próbują nakłonić do nieświadomego ujawnienia danych, np. wywierając presję czasu – mówi Bartłomiej Dyrga, Menedżer Zespołu Utrzymania Cyberbezpieczeństwa w Alior Banku.

Aby skutecznie się bronić, trzeba uważnie czytać informacje dotyczące transakcji, zarówno w SMS, jak i w komunikatach PUSH. W razie wątpliwości co do autentyczności strony płatności, należy przerwać transakcję.

Nie klikaj w linki przesyłane przez niezweryfikowanego nadawcę w wiadomościach e-mail, SMS, czy też zawarte w bannerach.

Coraz więcej e-maili doskonale imituje komunikaty wysyłane przez banki, posługując się identyczną szatą graficzną oraz logotypami. Przestępcy często używają tych wiadomości w celu nakłonienia odbiorcy do kliknięcia w linki i udostępnienie wrażliwych danych. Ten typ manipulacji, znany jako phishing, obecnie należy do jednej z najczęściej stosowanych metod wyłudzenia. Podobny scenariusz przestępcy stosują w wiadomościach SMS.

Należy wiedzieć, że instytucje finansowe nigdy nie przesyłają linków do bankowości internetowej w e-mailach lub SMS-ach ani nie proszą o zalogowanie się, podanie PIN-u, numeru karty płatniczej czy zmianę hasła na stronie wskazanej przez aktywny link. Ważne jest, aby podejść z większą ostrożnością do otrzymywanych wiadomości. Nie chodzi o to, aby odrzucać wszystkie wiadomości jako potencjalnie fałszywe, lecz o to by z nieufnością podchodzić do komunikatów, których autor nie został zweryfikowany.

Warto zawsze sprawdzić szczegóły wiadomości, a więc z jakiego adresu została wysłana, czy nie zawiera ona literówek oraz czy zachowane są zasady gramatyki i ortografii. Chociaż cyberprzestępcy stają się coraz bardziej zręczni w swoich działaniach, to nadal popełniają drobne błędy, które można zauważyć przy dokładnej analizie.

Sprawdź poprawność adresu, z którym się łączysz

Przy logowaniu do konta bankowego należy zwrócić uwagę na certyfikat SSL. Internauci mogą go rozpoznać m.in. dzięki symbolowi zamkniętej kłódki oraz przedrostkowi „https" w adresie strony. Brak litery „s" w tym protokole oznacza, że użytkownik znajduje się na portalu, który nie szyfruje transmisji danych, co w rezultacie umożliwia stosunkowo łatwe przechwycenie informacji.

Weryfikację strony zawsze warto poprzedzić również sprawdzeniem jej certyfikatu. Aby to zrobić, należy kliknąć na ikonę zamkniętej kłódki i sprawdzić wszystkie wpisy zawarte w przedstawionym certyfikacie. Zaleca się również weryfikację poprawności adresu strony logowania do banku lub jego ręczne wprowadzanie.

Dbaj o bezpieczeństwo komputera i smartfona

W trosce o bezpieczeństwo danych, dobrze jest zabezpieczyć komputer przed ewentualnym atakiem hakera. W tym celu należy skorzystać ze sprawdzonego oprogramowania antywirusowego oraz dbać o jego aktualizację.

Należy pamiętać również o tym, aby z ograniczonym zaufaniem korzystać z ogólnodostępnych sieci Wi-Fi, które są bardziej narażone na ataki niż sieci prywatne. Jeśli jednak konieczne jest połączenie z darmowym hot-spotem, warto zaniechać czynności związanych z logowaniem do banku lub innych witryn zabezpieczanych hasłami.

Uważaj na podejrzane połączenia telefoniczne

W dobie obsługi zdalnej trzeba być wyczulonym na podejrzane połączenia telefoniczne. Spoofing to podszywanie się pod dowolny numer lub nazwę kontaktu w telefonie. Oznacza to, że mimo wyświetlanej na ekranie naszego telefonu nazwy dzwoniącego (np. Anna) czy numeru telefonu (np. infolinii banku), tak naprawdę dzwoni do nas lub pisze zupełnie inna osoba. Nie jest to złamanie zabezpieczeń banku, możliwość ataku wynika ze sposobu działania infrastruktury telekomunikacyjnej. Możliwe, że podczas takiego połączenia skontaktuje się z nami oszust, którego celem jest kradzież pieniędzy.

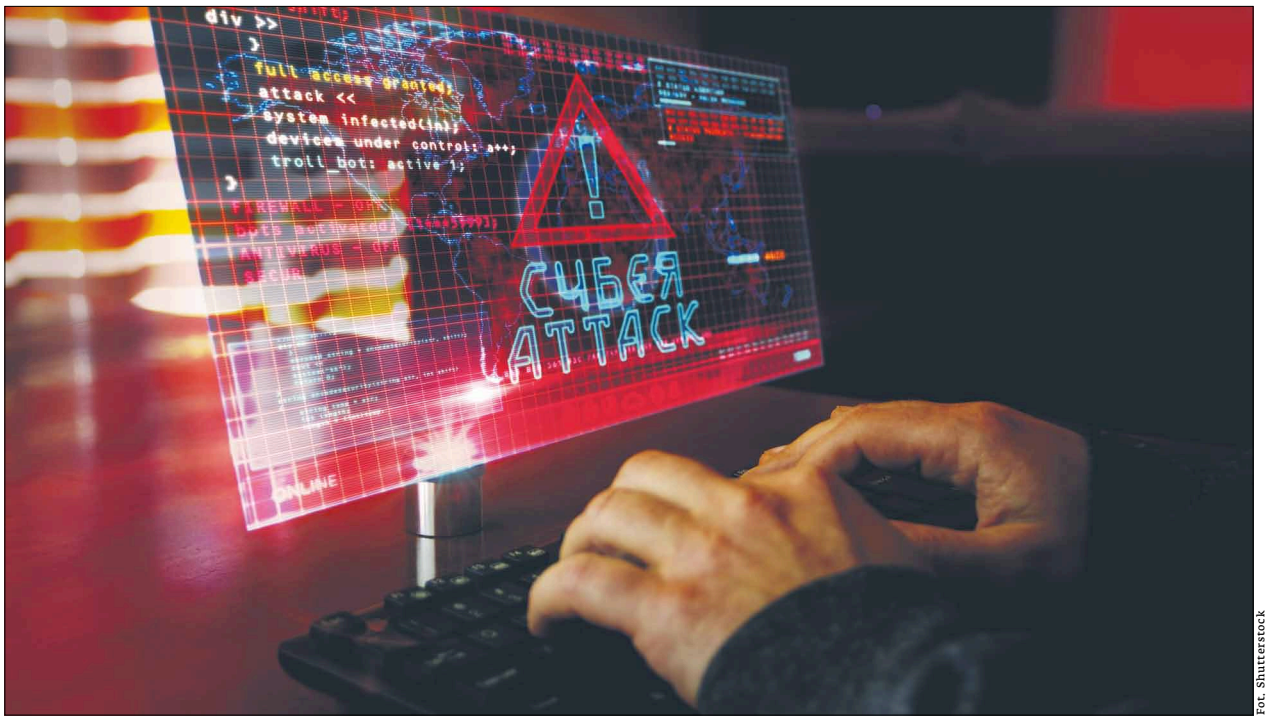
Przestępcy podczas kontaktu informują np. o zablokowaniu rzekomego przelewu na dużą kwotę, podejrzanej płatności kartą lub nieuprawionym kredycie. Wyłudzają wtedy hasła do bankowości elektronicznej, dane kart płatniczych, kody BLIK, nalegają na zainstalowanie aplikacji lub przelanie pieniędzy na „konto techniczne", które w rzeczywistości nie istnieje.

- Należy pamiętać, aby pod żadnym pozorem nie podawać loginu i hasła do bankowości internetowej oraz danych karty płatniczej. To poufne informacje, o które prawdziwy przedstawiciel banku nigdy nie zapyta. W przypadku żądania takich danych przez dzwoniącego, klient powinien natychmiast przerwać połączenie, odczekać chwilę, a następnie samodzielnie zadzwonić do instytucji, której rzekomy przedstawiciel się z nim kontaktował. Koniecznie należy wybrać oficjalny numer na klawiaturze numerycznej, a nie oddzwaniać na wcześniejsze połączenie. Należy zawsze mieć świadomość, że wyświetlony numer telefonu lub nazwa banku nie są gwarancją, że rozmawiamy z prawdziwym przedstawicielem. W Alior Banku dajemy możliwość ustalenia tzw. hasła zwrotnego na infolinii lub w oddziale banku, którego następnie klient może zażądać podczas rozmowy. Jeśli podany kod będzie niepoprawny, należy od razu zakończyć połączenie i poinformować o zdarzeniu bank. Weryfikować można również poprzez poproszenie bankiera o wysłanie komunikatu PUSH do aplikacji Alior Mobile – podkreśla Bartłomiej Dyrga.

Równie często przestępcy podszywają się pod bliską nam osobę, a następnie poproszą o „przypomnienie" jakiegoś hasła lub też podanie kodu BLIK bądź zapłatę poprzez dedykowany link, bo właśnie ta osoba płaci za zakupy i nie może autoryzować transakcji. Mogą to zrobić za pomocą SMS-a lub też internetowego komunikatora, aby nie wzbudzać podejrzeń w trakcie rozmowy. Warto w takiej sytuacji nie odpisywać, ale zadzwonić bezpośrednio do naszego znajomego i zweryfikować sytuację.

Oprócz najwyższej jakości zabezpieczeń kluczowe zadanie w tym procesie pełni edukacja, w szczególności z zakresu bezpiecznego korzystania z Internetu. Oszuści wciąż tworzą nowe sposoby wyłudzania danych, często wykorzystując ludzką wrażliwość i empatię.

Każdy klient powinien pamiętać, że każdorazowo ma prawo zgłosić nietypową sytuację do banku, a w przypadku podejrzenia, że doszło lub mogło dojść do popełnienia przestępstwa, również zawiadomić policję. Aktualne informacje o zagrożeniach i atakach na klientów bankowości w Polsce są publikowane na stronach Alior Banku, Związku Banków Polskich oraz Komisji Nadzoru Finansowego.



Fot. Shutterstock

Do obrony trzeba być przygotowanym

Przygotowanie strategii, zastosowanie narzędzi zabezpieczających, wdrożenie odpowiednich regulacji prawnych, działania, które zminimalizują skutki ewentualnych ataków oraz przeszkolenie pracowników to filary cyberbezpieczeństwa

Niemal 70 proc. firm doświadczyło w ubiegłym roku ataków cyberprzestępców. To o 5 proc. więcej niż w 2022 r. – wynika z raportu „Cyberbezpieczeństwo w polskich firmach 2023", spółki Vecto. Zapewnienie odpowiedniego poziomu cyberbezpieczeństwa jest jednym z największych wyzwań, z którymi muszą się obecnie zmierzyć przedsiębiorcy i instytucje. Bez względu na wielkość firmy czy branżę. Posiadane i przetwarzane informacje, także dane osobowe, są dobrem luksusowym, o które trzeba zadbać.

Zdaniem ekspertów działania podejmowane w tym zakresie będą determinowane przez dwa czynniki. Pierwszy to konieczność wdrożenia rozwiązań w odpowiedzi na nowe wymogi prawa unijnego i polskiego. Drugi – dostosowanie środków bezpieczeństwa teleinformatycznego do coraz bardziej zaawansowanych metod i narzędzi wykorzystywanych przez cyberprzestępców.

Nie daj się zaskoczyć

U podstaw wszystkich działań w zakresie cybersecurity, zarówno w zakresie wdrożenia rozwiązań technologicznych, jak i tych formalno-prawnych, czy nawet czysto biznesowych, np. personalnych, powinna leżeć spójna strategia.

– Uważam, że przedsiębiorcy powinni dysponować przygotowaną, wdrożoną i „przećwiczoną" procedurą na wypadek ataku hakerskiego. Powinni także zrozumieć, że zaplanowane działania są skuteczniejsze niż reagowanie ad hoc, gdy już dojdzie do incydentu naruszenia bezpieczeństwa, dane wyciekły, a czas nie działa na naszą korzyść. W obszarze cyberbezpieczeństwa nie ma miejsca na partyzantkę – tłumaczy Paweł Markiewicz, ekspert ds. cyberbezpieczeństwa i założyciel firmy M3M odpowiadającej za bezpieczeństwo danych w największych przedsiębiorstwach w Polsce.

I podkreśla, że ścieżka postępowania każdej organizacji powinna opierać się na co najmniej trzech krokach.

Pierwszym jest określenie kluczowych procesów operacyjnych i skupieniu się na ich zabezpieczeniu, np. procesu sprzedaży online czy logistycznego. Żadna organizacja nie jest w stanie zapewnić wysokiego poziomu bezpieczeństwa wszystkim realizowanym procesom.

– Należy przyjąć, że ataki hakerskie są więcej niż prawdopodobne i w związku z tym należy wiedzieć, co jest naszym „miękkim podbrzuszem", w co hakerzy mogą celować i które aspekty naszej działalności należy chronić najdokładniej – mówi Paweł Markiewicz.

Drugim jest odpowiedź na pytanie, jak organizacja chce chronić kluczowe procesy operacyjne? Pomocne będą wnioski z dotychczasowych działań budujących świadomość wśród pracowników w obszarze cyberbezpieczeństwa, wyniki badań audytowych i kontrolnych sprawdzających podatność na ataki infrastruktury IT, wnioski i obserwacje z realizowanych procesów wspierających cyberbezpieczeństwo.

– Mowa na przykład o takich procesach minimalizujących przetwarzane danych w organizacji, jak usunięcie danych nadmiarowych, zbędnych w realizacji celów biznesowych lub danych powtarzających się – wyjaśnia Paweł Markiewicz.

Trzecim jest przydzielenie odpowiedzialności i realizacji zaplanowanych w obszarze cyberbezpieczeństwa działań wyspecjalizowanemu pracownikowi lub ekspertowi zewnętrznemu. Outsourcing to nie tylko niższe koszty utrzymania, lecz także brak konieczności szkolenia wewnętrznego eksperta, ograniczenie nakładów na stanowisko pracy, oszczędność czasu i elastyczność.

– Inwestowanie nie tylko w zaawansowane technologie, lecz także w edukację pracowników i rozwijanie kultury bezpieczeństwa, to kluczowe elementy skutecznego zarządzania cyberbezpieczeństwem. W obliczu dynamicznie zmieniającego się krajobrazu cyberzagrożeń ciągłe monitorowanie, aktualizacje i dostosowywanie strategii są kluczowe dla minimalizacji ryzyka związanego z atakami, zapewniając ciągłość działania firmy. Efektywne i bezpieczne środowisko cyfrowe jest nieodzowne dla utrzymania konkurencyjności i zdolności do innowacji każdej współczesnej organizacji – wymienia Paweł Markiewicz.

Zwróć uwagę na nowe regulacje

Duże znaczenie dla bezpieczeństwa ma prawidłowe wdrożenie działań zmierzających do spełnienia wymagań nałożonych przez przepisy, np. DORA (Digital Operational Resilience Act), DSA (Digital Services Act) czy NIS2 (Directive on Security of Network and Information Systems). Wspomniane regulacje i przepisy wykonawcze do nich, które właśnie są wprowadzanie, służą poprawie poziomu bezpieczeństwa cyfrowego oraz operacyjnej odporności organizacji na przyszłe zagrożenia, co także wpływa korzystanie na spokój i bezpieczeństwo biznesu.

– Przedsiębiorcom prowadzącym działania biznesowe w obszarze „pieniądza" polecam uwadze np. zapisy wspomnianego rozporządzenia DORA, koncentrujące się na pięciu obszarach mających skutkować zwiększeniem odporności cyfrowej w sektorze finansowym – mówi Grzegorz Leśniewski, ekspert ds. prawa i compliance oraz inspektor ochrony danych osobowych. Jak dodaje, chodzi o:

- zarządzanie ryzykiem wspomaganym w szczególności przez: strategie i polityki bezpieczeństwa informacji, mechanizmy wykrywania nieprawidłowości, plany ciągłości działania, strategie backupów oraz plany komunikacyjne (wewnętrzne i zewnętrzne) dotyczące zaistniałych incydentów cybernetycznych.
- zarządzanie incydentami,
- testowanie cyfrowej odporności operacyjnej kluczowych systemów i aplikacji, czyli prowadzenie oceny bezpieczeństwa oraz testów penetracyjnych kluczowych systemów IT wspierających procesy biznesowe,
- zarządzanie ryzykiem stron trzecich obejmującym cenę dostawców, opracowanie i wdrożenie strategii wyjścia i planów przejścia oraz określenie kluczowych dostawców usług teleinformatycznych,
- wymianę informacji o zagrożeniach cybernetycznych oraz wynikach analizy tych zagrożeń.

Mówiąc o nowych regulacjach, nie można zapominać, że w zapisach przygotowywanej ustawy o ochronie sygnalistów, czyli osób zgłaszających naruszenia prawa, mają zostać ujęte zagadnienia dotyczące bezpieczeństwa sieci i systemów teleinformatycznych. Zgodnie z jej zapisami naruszeniem prawa określono działanie lub zaniechanie, mające na celu obejście przepisów zobowiązujących przedsiębiorców do określonej aktywności w obszarze cyberbezpieczeństwa.

Bądź krok przed przestępcami

„Tylko w 2022 r. przeciętny okup za odszyfrowanie danych kosztował polskie przedsiębiorstwa średnio 670 tys. zł, co często stanowi kwotę wielokrotnie wyższą niż inwestycje w skuteczne rozwiązania chroniące firmową infrastrukturę IT" – zauważają eksperci Vecto, podkreślając, że mowa o uśrednionych kosztach, bo są przypadki strat liczonych w dziesiątkach milionów złotych. Jak wynika z raportu firmy, 72,2 proc. badanych przedsiębiorstw rozważa zapłacenie okupu w przypadku wystąpienia incydentu ransomware. Analitycy wskazują, że 60 proc. naruszeń systemów ma w sobie element inżynierii społecznej i wpływu oraz manipulacji wywieranych wprost na ludzi. To właśnie na błędach użytkowników przestępcy najczęściej opierają swoje działania i są w tym brutalnie skuteczni.

– W mojej ocenie w 2024 r. przedsiębiorcy powinni się przygotować na znaczący wzrost częstotliwości cyberataków opartych na sztucznej inteligencji, a w szczególności zagrożeń ransomware, co umożliwia prowadzenie bardziej zaawansowanych operacji dostępu i gromadzenia przez cyberprzestępców danych – mówi Paweł Markiewicz, i dodaje, że działania pozorowane nie wystarczają, niezbędne są wdrożone adekwatne i skuteczne narzędzia monitorujące, np. oprogramowanie antywirusowe, polityka tworzenia kopii zapasowych, programy edukacyjne budujące świadomość pracowników, a także profesjonaliści zarządzający obszarem cyberbezpieczeństwa.

Pomocne w walce ze złośliwym oprogramowaniem mogą być algorytmy uczenia maszynowego. Pozwalają na szybszy i efektywniejszy monitoring ruchu sieciowego, triage incydentów oraz zautomatyzowaną reakcję w razie wystąpienia zagrożenia.

Ogranicz przechowanie danych

Nie da się jednak w pełni zabezpieczyć przed cyberprzestępcami.

– Planując działania minimalizujące skutki przyszłych potencjalnych cyberataków, organizacje powinny rozważyć migrację danych do chmury, np. Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), co w krótkiej perspektywie przyniesie wiele korzyści, np. elastyczność i skalowalność, oszczędność kosztów, wysoką dostępność i niezawodność, uproszczoną administrację, ale także wsparcie prawne i technologiczne oraz bezpieczeństwo – uważa Paweł Markiewicz.

Obowiązuje zasada: im mniej danych przechowuje się w organizacji, tym mniejsza ekspozycja na ryzyko nieuprawnionego dostępu do danych, ich kradzieży lub utraty.

– Najlepsze efekty w zakresie przeprowadzenia procesu minimalizacji danych dają działania manualne wsparte specjalistycznymi narzędzi IT, które w sposób zautomatyzowany lokalizują i identyfikują dane w środowisku IT, a następnie je klasyfikują, co pozwala skutecznie nimi zarządzać. Dzięki temu przedsiębiorstwo jest w stanie zidentyfikować np. dane zduplikowane oraz te, które już nie przydadzą się w dalszej działalności biznesowej – tłumaczy Paweł Markiewicz.

Zadbaj o pracowników

Eksperci z Eset podkreślają, że bezpieczeństwo zasobów jest też w rękach samych pracowników. Dlatego trzeba ich uczulić, by pamiętali o przestrzeganiu zasad. Wśród nich jest korzystanie z zaufanych źródeł, sprawdzanie stron, linków, z których się korzysta, zwracanie uwagi na treści, gdzie wymagane jest logowanie lub wykonanie przelewu, nieprzekazywanie ważnych informacji przez telefon, jeśli nie ma się pewności co do rozmówcy, weryfikowanie nadawcy wiadomości, nieudostępnianie dostępu do komputera nieznajomym osobom. Ważną zasadą jest też stosowanie silnych haseł zabezpieczających i regularne ich zmienianie. Elementem zabezpieczenia będzie poza tym uwierzytelnienie dwuskładnikowe (2FA) przy logowaniu do wewnętrznej sieci.

Co z cyberbezpieczeństwem w małych i średnich firmach

O sytuacji mniejszych przedsiębiorstw opowiada Paweł Markiewicz, założyciel firmy M3M – więcej na: cyfrowa-gospodarka.gazetaprawna.pl

Wrażliwe branże

- Po inwazji Rosji na Ukrainę w 2022 r. Polska stała się jednym z krajów najbardziej narażonych na ataki cybernetyczne ukierunkowane na infrastrukturę krytyczną. Dlatego największą czujność powinny wykazywać przedsiębiorstwa z sektora gazowego, energetycznego, transportu publicznego i opieki zdrowotnej. Można oczekiwać bowiem, że w tych obszarach liczba ataków będzie wzrastać lawinowo. Na zagrożenie szczególną uwagą powinny zwrócić branże: finansowa, technologiczna i przemysłowa.

PREZENTACJA

Hakerzy muszą dziś tylko umieć czytać i pisać

Rewolucja technologiczna postępuje w ekspresowym tempie. Świat wchodzi w erę szybkiego rozwoju sztucznej inteligencji, która jeszcze bardziej przyspieszy postęp. – Świadomość ryzyk cybernetycznych, a co za tym idzie – sprzedaż polis, które mają chronić przed skutkami finansowymi ataków, jest zdecydowanie największa w USA. Później jest Europa Zachodnia. W Polsce wciąż jesteśmy daleko w tyle – mówią Tomasz Dolata i Maciej Kleina z Grupy ERGO Hestia

Zainteresowanie ubezpieczeniem Cyber wyraźnie rośnie. Decyzje o zakupie takich produktów podejmują firmy świadome zagrożeń. Wciąż jednak wiele organizacji nie zdaje sobie sprawy ze skali problemu – mówi **Tomasz Dolata**

Firmy stawiają bardziej na wykorzystanie AI w celu zwiększenia sprzedaży, ograniczenia kosztów niż na prewencję. Ta zawsze pozostaje na ostatnim miejscu. Chętniej inwestuje się w procesy, które pomagają zarobić – mówi **Maciej Kleina**

Rozwój sztucznej inteligencji niesie za sobą szanse dla współczesnego świata, ale nie można zapominać również o potencjalnych zagrożeniach. Czego powinniśmy się obawiać?

M.K.: Wykorzystania technologii do nieuczciwych działań. Coraz łatwiej będzie paść ofiarą oszustwa. Zmieni się sposób przeprowadzania ataków, ale finał będzie ten sam – wykradane loginy, wyłudzane dane, oczyszczone z pieniędzy konta, żądania okupu za zwrot skradzionych danych itd.

W jaki sposób dochodzi do przestępstw?

T.D.: Bardzo popularne są ataki phishingowe, oparte choćby na wiadomościach e-mail lub SMS, które dziś w znaczący sposób wykorzystują AI. Do tego dochodzi podkładanie czyjegoś głosu, co uwiarygadnia komunikat przestępcy i sprawia, że jego działania mają większe szanse zakończyć się sukcesem. Wykorzystuje się to również w atakach na firmy. Gdy odbieramy telefon i słyszymy głos szefa, nie podajemy przecież w wątpliwość tego, że to właśnie on się z nami komunikuje. To jeden ze sposobów, by pozyskać wrażliwe dane. AI może być wykorzystywana do pisania oprogramowania łamiącego zabezpieczenia infrastruktury teleinformatycznej firm i instytucji.

M.K.: Dochodzi coraz częściej do ataków złośliwego oprogramowania, brutalnych i systematycznych, uderzających w infrastrukturę firmowej sieci. W modzie jest ransomware – oprogramowanie, które blokuje firmie dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych. Po ataku hakerzy zgłaszają się z propozycją okupu za przywrócenie stanu pierwotnego. W Stanach Zjednoczonych to prawdziwa plaga.

Dotychczas bycie hakerem wiązało się z pewną barierą. Trzeba było posiąść pewne umiejętności, wiedzę programistyczną, sprawnie poruszać się w dark necie, by kupić odpowiedni program, zapłacić za niego w bitcoinach itd. Dla wielu to bariera nie do przejścia. Teraz, gdy mamy AI, która za nas napisze program, wykreuje obraz, dźwięk, przełamie zabezpieczenia, wystarczy umiejętność czytania i pisania. Oszuści mają o wiele łatwiej.

T.D.: Z raportu przygotowanego przez CERT, rządowy ds. reagowania na incydenty komputerowe, wynika, że na pierwszym miejscu zagrożeń są oszustwa komputerowe, do których zalicza się phishing, a na drugim – złośliwe oprogramowanie i ataki typu ransomware. Te dwie pozycje odpowiadają za ponad 70 proc. incydentów.

Jak przygotować się na funkcjonowanie w nowych realiach?

M.K.: To trudne pytanie. Rewolucja technologiczna przebiega bardzo szybko, w niekontrolowany sposób. Będziemy wciąż zaskakiwani nowymi rozwiązaniami, programami tworzonymi w celach przestępczych. Trzeba korzystać z dostępnych na rynku narzędzi, by bronić się przed tym, co jest już znane. Inwestować, by mitygować zagrożenia, które powstają. Ale przede wszystkim być uważnym. Firmy powinny szkolić pracowników, osoby fizyczne z kolei powinny zainteresować się zagrożeniami i tym, jak ich uniknąć. Budować swoją świadomość.

T.D.: Ważna jest edukacja – w szkołach, w telewizji, poprzez kampanie społeczne. To może przynieść wymierny skutek. Istotne są też narzędzia prawne. Dziś samo prawo nie nadąża za postępującą cyfryzacją. To się musi zmienić.

Możemy walczyć z tymi zagrożeniami, które są rozpoznane, ale nie zabezpieczymy się przed tymi, które się dopiero tworzą. To oznacza, że jesteśmy na przegranej pozycji...

T.D.: Faktycznie pozostajemy krok, a nawet dwa kroki za sztuczną inteligencją. Firmy nie nadążają za hakerami. Sztuczna inteligencja jest coraz bardziej dostępna i powszechna, ten proces wciąż przyspiesza. Zawsze będziemy z tyłu. Możemy jedynie reagować na zagrożenia rozpoznane, mając świadomość, że za chwilę pojawią się kolejne wyzwania. Zdarzają się przecież ataki typu zero-day, wykorzystujące luki nieznane producentom oprogramowania, które są przecież wielkimi korporacjami zatrudniającymi całe grono specjalistów.

Nie da się wykonać ruchu wyprzedzającego i wykorzystać AI do wykrywania potencjalnych zagrożeń?

M.K.: Obawiam się, że „ciemna strona mocy", która może przynieść szybkie korzyści finansowe, będzie intensywniej rozwijana. Firmy stawiają bardziej na wykorzystanie AI w celu zwiększenia sprzedaży, ograniczenia kosztów niż na prewencję. Ta zawsze pozostaje na ostatnim miejscu. Chętniej inwestuje się w procesy, które pomagają zarobić.

Jak funkcjonować w takiej rzeczywistości?

M.K.: Trzeba wypracować skuteczne procedury działania, które uodpornią nas i nasze firmy na tego rodzaju kryzysy. Na przykład – nie otworzę pewnego rodzaju plików, bo nie pozwoli mi na to organizacja. Nie wyślę e-maila, jeśli nie zaszyfruję danych. Nie zainstaluję samodzielnie oprogramowania. Takie zabezpieczenia są już na porządku dziennym w wielu firmach. Procedury mają stanowić ochronę przed cyberprzestępcami. Podobnie każdy z nas będzie musiał uważać, co instaluje, upewniać się, czy rozmawia na pewno z właściwą osobą.

T.D.: Pewnie zmierzamy w kierunku powszechnego uwierzytelnienia dwuskładnikowego, które przecież już dziś funkcjonuje i staje się powszechniejsze. Aby zalogować się do firmowego komputera, trzeba będzie nie tylko podać hasło, lecz także wpisać informacje z SMS-a, potwierdzając, że ja to faktycznie ja. W przyszłości będzie to szło w tę stronę.

M.K.: Wyobrażam sobie np., że wysyłając wiadomość e-mailową do kontrahenta, będziemy wpisywać PIN. I aby tę wiadomość odebrać, druga strona będzie musiała wpisać ten sam PIN.

Czy tego typu zagrożenia mogą cofnąć nas w czasie? Sprawić, że wrócimy do okienek i bezpośrednich spotkań z agentem ubezpieczeniowym?

M.K.: Sądzę, że nauczymy się z tym jakoś żyć, podobnie jak w przypadku innych rewolucji, które dokonały się w przeszłości, a które również niosły za sobą zagrożenia. Wypadki samochodowe nie sprawiły przecież, że przesiedliśmy się z powrotem na konia. Oswoimy lęki, wypracujemy schematy działania. O ile zagrożenia nie będą bardzo poważne, nie będziemy się cofać.

T.D.: Sami z siebie cofać się nie będziemy, chyba że wymagać tego będzie druga strona – banki, urzędy itd. Ludzie cenią sobie komfort życia. Młode pokolenie jest za cyfryzacją, chce załatwiać sprawy zdalnie. Stanie w kolejce przed okienkiem bankowym jest dla większości z nich abstrakcją. Oni oczekują postępu, rozwoju technologii.

Ubezpieczyciele uwzględniają zagrożenia cyberatakami w swojej ofercie?

M.K.: Tak. Jednak trzeba podkreślić, że firmy nie zabezpieczą swojej infrastruktury, wykupując polisę ubezpieczeniową. Podobnie zresztą jak polisa nie uchroni domu przed pożarem czy auta przed wypadkiem. Należy zapobiegać, chronić infrastrukturę teleinformatyczną. Oceniając ryzyko klienta przed zawarciem umowy, zawsze zaczynamy od analizy zabezpieczeń, które on stosuje, a także wskazujemy, co wymaga poprawy.

Gdy już dojdzie do ataku, chronimy klientów przed konsekwencjami finansowymi takich zdarzeń. Firmy i instytucje muszą w takich sytuacjach nie tylko stawiać na nowo systemy informatyczne – grożą im też kary administracyjne za wyciek danych osobowych, pojawiają się koszty pracy prawników, zespołów PR pomagających wyjść ze szkody obronną ręką. Wszystko to kosztuje mnóstwo pieniędzy. Oferujemy też serwis informatyków śledczych, którzy w ciągu 24–48 godzin sprawdzają dokładnie, co się stało. To specjaliści działający w branży od ponad 20 lat. My pozyskujemy raport pozwalający określić odpowiedzialność za szkodę, a klient pełną informację o przyczynach incydentu.

Duże jest zainteresowanie tego typu polisami w Polsce?

T.D.: Zainteresowanie ubezpieczeniem Cyber wyraźnie rośnie. Decyzje o zakupie takich produktów podejmują firmy świadome zagrożeń. Sprzedaż się zwiększa, ale startuje z bardzo niskiego pułapu. Szkody, które na rynku pojawiają się regularnie, w zdecydowanej większości przypadków nie są nagłaśniane w przestrzeni publicznej. To sprawia, że firmy nie zdają sobie do końca sprawy ze skali zagrożenia.

Za granicą wygląda to inaczej?

M.K.: Polskę i Zachód dzieli pod tym względem duży dystans. Świadomość ryzyk cybernetycznych, a co za tym idzie – sprzedaż polis, które mają chronić przed skutkami finansowymi ataków, jest zdecydowanie największa w USA. Później jest Europa Zachodnia. W Polsce wciąż jesteśmy daleko w tyle. Świadomość rośnie, gdy incydenty są nagłaśniane. Kiedy spłonie fabryka, wszyscy o tym wiedzą. To działa na wyobraźnię. Tymczasem ryzyk cybernetycznych nie widać. Firmy nie chcą się chwalić, że były ofiarą ataku. Wiemy tylko o największych, spektakularnych akcjach, których nie da się ukryć. Zdecydowana większość szkód nie wychodzi na światło dzienne. One nie rezonują, wolniej buduje się świadomość dotycząca zagrożeń, poczucie, że taka sytuacja może dotknąć również mnie. Jednocześnie wiele krajowych podmiotów nie jest w stanie odpowiedzieć na podstawowe zagrożenia. Dlatego warto o tym głośno mówić, prowadząc akcje edukacyjne i zachęcać do inwestycji w rozwój zabezpieczeń oraz wypracowywania odpowiednich procedur, które pokrzyżują plany przestępcom.

Monika Borkowska

Mój sprzęt moją twierdzą

W codziennym użytkowaniu warto zadbać o bezpieczeństwo telefonów, komputerów, smart TV i innych urządzeń – czyli o swoje własne

W 2024 r. mija 20 lat od pojawienia się w Polsce pierwszej aplikacji bankowej na telefon. Z rozwiązania w erze przedsmartfonowej korzystała garstka entuzjastów, grono to radykalnie się poszerzyło wraz z upowszechnieniem się systemu iOS i Androida. Pierwsze iPhone'y pojawiły się w Polsce w 2008 r., pionierem Androida był HTC Dream sprzedawany nad Wisłą od 2009 r.

Obecnie, według danych Związku Banków Polskich publikowanych w raportach NetB@ank, liczba aktywnych użytkowników bankowych aplikacji mobilnych przekroczyła w Polsce 21 mln. Blisko 15 mln (71 proc.) to osoby logujące się przynajmniej raz w miesiącu do aplikacji mobilnej, a zarazem niekorzystające z bankowości za pośrednictwem komputera. Wśród małych i średnich przedsiębiorców z bankowości elektronicznej regularnie korzysta 2,5 mln. Co istotne, wykorzystują oni internet nie tylko do operacji bankowych, lecz także zarządzania biznesami. Wedle zeszłorocznego raportu EFL aż 70 proc. właścicieli firm robi to przy pomocy aplikacji w smartfonie, a 44 proc. – na laptopie lub innym urządzeniu mobilnym.

Router tarczą czy bramą piekieł?

Nowe narzędzia w połączeniu z szybkim internetem są efektywne i wygodne, jednak stworzyły zupełnie nowe pole działania dla przestępców. Jak się zabezpieczyć?

W domu i w firmie większość urządzeń łączy się z internetem przez router Wi-Fi – w dużym stopniu to od nas zależy, czy stanie się on furtką (albo szeroko rozwartymi wrotami) dla złoczyńców, czy też solidną tarczą chroniącą przed atakami z sieci. W pierwszym rzędzie warto się zaopatrzyć w router od wiarygodnego producenta i dostawcy – w ostatnich latach wybuchło kilka skandali związanych z wykryciem tzw. backdorów (czyli furtek dla wtajemniczonych) umieszczonych w routerach po to, by mieć do nich dostęp. Podejrzenie padało najczęściej na służby wywiadowcze Chin.

Po zakupie routera trzeba go odpowiednio zaprogramować, a więc m.in. zmienić domyślną nazwę sieci i hasło administratora, wybrać bezpieczny protokół, ustawić właściwe DNS-y (Domain Name System – tłumaczy nazwy domen na adresy IP) oraz mocne hasło do Wi-Fi. Eksperci zalecają wyłączenie zdalnego dostępu do routera i funkcji WPS (Wi-Fi Protected Setup , pozwala urządzeniom łączyć się z routerem bez hasła) oraz ograniczenie zasięgu Wi-Fi do niezbędnego minimum. Warto włączyć filtrowanie adresów MAC (sprzętowych) oraz stworzyć osobną sieć dla gości. Zdecydowanie rekomendowane jest wyłączanie routera, gdy nie jest używany.

Bezwzględnie należy pamiętać o aktualizacjach oprogramowania, wiele z nich służy łataniu wykrytych luk w zabezpieczeniach. To fundamentalne przykazanie dotyczy wszystkich urządzeń.

Skuteczna ochrona

Eksperci CERT Polska, działającego od 28 lat zespołu reagowania na zdarzenia naruszające bezpieczeństwo w internecie, stworzyli listę najświeższych zaleceń dla użytkowników globalnej sieci. Na szczycie umieścili bezpieczne hasła do kont i aplikacji. Informacje ujawnione przy okazji masowych wycieków z baz danych firm i instytucji obejmują często (obok nicków czy adresów e-mail) także hasła typu agnieszka1 lub zenek1234.

Hasło ma być trudne do odgadnięcia. Należy trzymać się zasady, że jedno jest używane tylko do jednej usługi.

Eksperci zdecydowanie rekomendują używanie dodatkowej weryfikacji przy logowaniu, np. poprzez uwierzytelnianie wieloskładnikowe. Najpopularniejsza stała się weryfikacja dwuetapowa – obok hasła trzeba użyć np. odcisku palca lub wprowadzić jednorazowy kod wysłany SMS-em, na adres e-mail albo wyświetlony w specjalnej aplikacji zainstalowanej na urządzeniu mobilnym (jak Microsoft Authenticator czy Google Authenticator). Do weryfikacji dwuetapowej służą także klucze U2F – niewielkie urządzenia podłączane do smartfona lub komputera via usb wykorzystujące zaawansowane metody kryptograficzne.

Mimo że popularne systemy operacyjne (Windows, iOS) zawierają dziś moduły chroniące przed złośliwym oprogramowaniem i typowymi rodzajami cyberataków, warto korzystać ze specjalnych programów antywirusowych. Trzeba pamiętać o regularnej aktualizacji, a jeśli wymaga ona restartu systemu, przeprowadzić to jak najszybciej i nie odkładać na „za trzy dni".

Przy korzystaniu z internetu trzeba zawsze stosować zasadę ograniczonego zaufania. Można mieć najefektywniejsze zabezpieczenia, a paść ofiarą własnej naiwności, nieostrożności lub nieuwagi. „Cyberprzestępcy stale szukają nowych sposobów i technik, by nas zmanipulować, nakłonić do podjęcia działań, które mogą prowadzić do utraty naszych danych lub pieniędzy. Wykorzystują nasze emocje, naiwność oraz brak czasu i życie w biegu. Dlatego jeśli otrzymasz wiadomość, która nakłania Cię do podjęcia natychmiastowych działań, zastanów się, czy jest ona prawdziwa. Uważaj również na różnego rodzaju wyjątkowe oferty, wygrane w loterii czy możliwość zainwestowania w kryptowaluty i inne sposoby na szybkie wzbogacenie się. Nie wchodź na strony, które wydają Ci się podejrzane" – radzą eksperci CERT NASK, rekomendując przy tym dbanie o prywatność w sieci: im więcej informacji o sobie dostarczymy dzięki zdjęciom, filmom, tekstom czy zachowaniom (także niewinnym lajkom), tym więcej broni dostarczamy przestępcom.

Przydatne zasady

Jak podnieść swoje bezpieczeństwo w sieci, radzi Piotr Konieczny, Niebezpiecznik.pl:

- płać kartą w internecie (dzięki procedurze chargeback odzyskasz pieniądze, które próbowali wyłudzić oszuści)
- rób kopie bezpieczeństwa, przydają się nie tylko po ataku szantażystów
- korzystaj z menedżera haseł, zadba o ich unikatowość i zmniejszy ryzyko związane z wyciekami danych
- zablokuj premium SMS – WAP Billing u operatorów komórkowych
- wgrywaj aktualizacje nie tylko na komputerze.

Przed ubezpieczeniem sprawdzamy higienę cyberbezpieczeństwa w firmie

W dobie cyfrowej gospodarki cyberzagrożenia to wyzwanie, z którym powinna się liczyć każda firma. O ubezpieczaniu ryzyk cybernetycznych i związanej z tym aktywności prewencyjnej ubezpieczyciela mówią Michał Balwiński i Marcin Gajkowski z Generali Polska.

Czy można ubezpieczyć firmę na okoliczność cyberataku?

Michał Balwiński: Jak najbardziej tak. Można ubezpieczyć firmę od realizacji ryzyka cybernetycznego, natomiast trzeba pamiętać, że to nadal jest ubezpieczenie. Tak samo jak w przypadku ubezpieczenia od ognia w przypadku cyberzagrożeń w firmie muszą obowiązywać zabezpieczenia. Ubezpieczenie samo w sobie nie zastępuje zarządzania ryzykiem w organizacji, natomiast jest tym zabezpieczeniem, które ma działać, kiedy wszystkie inne zawiodą. Ubezpieczenia od cyberryzyk coraz bardziej zyskują na znaczeniu. Cyfryzacja i automatyzacja różnych procesów postępują. Kiedy mamy do czynienia z ubezpieczeniem mienia firmowego i dochodzi do pożaru, to obejmuje on zazwyczaj jedną lokalizację. W przypadku zatrzymania głównych systemów informatycznych w firmie, która ma kilka lokalizacji, wszystkie te lokalizacje mogą się zatrzymać jednocześnie. Dlatego ubezpieczenie od cyberzagrożeń jak najbardziej powinno stać się obowiązkowym elementem programu ubezpieczeniowego w organizacji, i to niezależnie od tego, czy prowadzi ona produkcję, czy świadczy usługi.

Jakie warunki dotyczące bezpieczeństwa musi spełnić firma, żeby otrzymać ofertę od ubezpieczyciela?

Marcin Gajkowski: Kiedy ubezpieczamy dom, to ubezpieczyciel wymaga, żebyśmy dopełnili pewnych wymogów zachowania ostrożności, których oczekuje się od każdego rozsądnego człowieka. Na przykład, żebyśmy mieli dwa zamki w drzwiach i zamykali okna, wyjeżdżając z domu. Dokładnie tak samo jest w przypadku ubezpieczenia od ryzyk cybernetycznych i wszystkich innych ubezpieczeń. Oczekuje się, że ubezpieczony będzie się zachowywał rozsądnie i, przede wszystkim, że sam będzie chronił swoje sieci i systemy.

M.B: Przed przygotowaniem indywidualnej oferty dla klienta dokonuje się oceny ryzyka, która w Generali przebiega dwutorowo. Pierwszy etap to coś, co nazywamy prescreeningiem czy też OSINT-em sieciowym. Polega on na analizie publiczne dostępnych, wskazanych domen internetowych klienta pod kątem bezpieczeństwa. Szukamy słabych punktów, a jeśli takie znajdziemy, klient otrzymuje raport na ten temat z wyjaśnieniami, co może zweryfikować lub poprawić. W uproszczeniu: sprawdzamy higienę cyberbezpieczeństwa w danej organizacji na podstawie analizy bezpieczeństwa publicznej domeny. Na drugim etapie zadajemy klientowi wiele pytań o zabezpieczenia. Tu obowiązuje pewien standard minimalny – warunki, które powinny być spełnione, żeby otrzymać ofertę ubezpieczenia. W zależności od specyfiki klienta, skali jego działalności, skomplikowania rozwiązań lub urządzeń, które klient tworzy, te warunki mogą być zaostrzone. Dlatego na każdą organizację trzeba spojrzeć indywidualnie.

M.G.: W pewnym momencie doszliśmy do wniosku, że żeby pozyskać klientów i móc ich ubezpieczyć, powinniśmy im też jakoś pomóc. Staramy się wspierać działania o charakterze prewencyjnym. Dla przykładu zawsze dzielimy się z klientem raportem OSINT-owym. Nawet jeżeli nie otrzyma on od nas oferty, dostanie informację zwrotną, co powinien poprawić. Chcemy też podpowiadać klientom, z jakich technologii czy usług mogą korzystać, żeby wzmocnić zabezpieczenia. W listopadzie ub.r. wprowadziliśmy, we współpracy z naszym partnerem MCX Pro, promocję, zgodnie z którą nasz klient razem z polisą otrzymuje pakiet 10 kluczy uwierzytelniających Yubikey produkowanych przez firmę Yubico – lidera rynku tych zabezpieczeń. Oczywiście to, co my oferujemy, to jest tylko próbka, ale staramy się zainteresować klienta dostępnymi rozwiązaniami, podpowiadać mu, z czego może skorzystać. Jeżeli skorzysta z narzędzia, które poprawia jego bezpieczeństwo, to my możemy to uwzględnić np. w wysokości składki. Co ważne, nasza oferta jest skierowana nie tylko do dużych firm, lecz także do tych małych, w których często nie ma wydzielonych ról ds. cyberbezpieczeństwa i w związku z tym trudniej jest nadążać za najnowocześniejszymi rozwiązaniami.

To działania prewencyjne. A na jakie wsparcie może liczyć firma, kiedy dojdzie do cyberataku, np. do wycieku danych klientów?

M.B: Ubezpieczenie cyber ma charakter hybrydowy – składa się z trzech modułów. Pierwszy z nich to ubezpieczenie strat własnych, które pokrywa koszty reagowania na incydent (w tym koszty notyfikacji indywidualnej i urzędowej czy monitoringu kredytowego), przywrócenia danych i systemów do stanu sprzed szkody, zwrot zapłaconych w wyniku incydentu kar czy koszty wynikające z działań PR-owskich po zdarzeniu cyber. W wypadku postępowań administracyjnych i sądowo-administracyjnych zapłacimy też koszty ochrony prawnej. Drugi moduł obejmuje ubezpieczenie odpowiedzialności cywilnej związanej z ryzykiem cybernetycznym, czyli kwestie roszczeń, które są zgłaszane do ubezpieczonego przez osoby, które ucierpiały na skutek wycieku danych, naruszenia bezpieczeństwa sieci ubezpieczonego czy publikacji multimedialnych naruszających własność intelektualną lub reputację. Trzeci moduł nazywamy odpowiedzią na incydent. To odpowiednik polisy assistance, tyle że dla incydentów cybernetycznych. W sytuacji, kiedy doszło do wycieku danych osobowych, ubezpieczony może się skontaktować ze specjalistami z zakresu czy to security operations center, czy informatyki śledczej, którzy zweryfikują, co się wydarzyło w firmie, skoordynują działania naprawcze i przedstawią propozycję działań zapobiegających, żeby incydent się nie powtórzył.

M.G: By posłużyć się przywołaną już analogią do ubezpieczenia majątku: w pierwszej kolejności koncentrujemy się na gaszeniu pożaru. To jest oczywiście usługa, którą my organizujemy i która jest dostępna dla posiadacza polisy. Ubezpieczony dysponuje całodobowym numerem telefonu lub adresem e-mailowym do naszego partnera, który zapewnia wsparcie, kiedy dojdzie do incydentu. Jako ubezpieczyciel opłacamy utrzymanie takiej infrastruktury dla klientów.

A czy ubezpieczenie pokryje zapłatę okupu żądanego przez cyberprzestępców?

M.G.: Nie licząc sytuacji wyjątkowych, tego nie ubezpieczamy. W przypadku zapłaty okupu nie ma pewności, że przestępca okaże się „uczciwy" i odszyfruje ofiarę, czy nie będzie korzystał z danych albo nie sprzeda ich w darknecie. Nie wiemy też, komu płacimy, kto za tym stoi, czy to nie jest organizacja terrorystyczna, czy zapłata okupu nie wygeneruje kolejnego problemu w postaci naruszenia sankcji międzynarodowych.

M.B.: Jest jeszcze jeden bardzo ważny aspekt. Jeżeli będziemy płacić cyberprzestępcom, to będą przeprowadzać coraz więcej ataków, bo będą mieli na to fundusze.