RAPORT

iTWIZ.

Gen. bryg. Karol Molenda: **wystawiliśmy w Polsce bitną cyberarmię**

NIS2: dyrektywa na czasy transformacji cyfrowej

Od Ukrainy po całą Europę: **cyberkonflikt osiąga punkt zwrotny**

Rynek cyberbezpieczeństwa z solidnymi **prognozami wzrostu**

Łukasz Wojewoda

KPRM będzie aktywnie koordynować i wspierać wdrażanie dyrektywy NIS2 przez polskie firmy

www.itwiz.pl

Wystawiliśmy w Polsce bitną cyberarmię

Z **gen. bryg. Karolem Molendą,** dowódcą Komponentu Wojsk Obrony Cyberprzestrzeni, rozmawiamy o ich potencjale oraz perspektywach stałego rozwoju i wzmacniania naszej cyberarmii. Ciężka praca, poczucie misji i wielki talent żołnierzy sprawiają, że rosyjskie grupy typu Advanced Persistent Threats nie są w stanie przełamać naszej cyberobrony.

Czym zajmuje się Komponent Wojsk Obrony Cyberprzestrzeni? Jak definiujemy cyberprzestrzeń? Czy KWOC chroni całą „polską" cyberprzestrzeń i wszystkich polskich użytkowników, czy tylko „wojskową" cyberprzestrzeń?

Staram się nie zaczynać rozmowy od uzgadniania definicji, bo nie skończymy. Ale dobrze, spróbujmy. Wojska Obrony Cyberprzestrzeni są niezbędnym elementem każdej nowoczesnej armii… Komponent Wojsk Obrony Cyberprzestrzeni to nie nowy rodzaj sił zbrojnych, ale formacja specjalna, działająca w wymiarze Defensive Operations, Offensive Operations oraz Intelligence, Surveillence and Reconessaince, a więc DSO, OSO i IRS według terminologii NATO. Zajmujemy się więc cyberobroną, cyberatakiem i cyberrozpoznaniem.

Zapytam inaczej: jak ocenia Pan rozwój sytuacji w cyberprzestrzeni? Czy zmierzamy w stronę modelu, w którym dobrze strzeżone, bezpieczne i połączone bezpiecznymi szlakami cyberprzestrzenie będą przedzielone cyfrowymi „Dzikimi Polami"?

Mogę wyrazić w tej kwestii tylko własne, subiektywne zdanie. Systemy wojskowe są łakomym kąskiem, dlatego na ich ochronie się skupiamy. Ale nasze zaangażowanie dotyczy także ochrony całej przestrzeni polityczno-gospodarczej Rzeczypospolitej w wymiarze cyber.

Czy będziemy w stanie bronić poszczególnych cyfrowych „miast" i „dróg" pomiędzy nimi, samych „miast", czy może uczynimy całą cyberprzestrzeń bezpieczną?

Zakładam, może optymistycznie, że dążymy do bezpieczeństwa całej cyberprzestrzeni. Ale też można powiedzieć, że na tych cyfrowych szlakach zawsze dużo będzie zależało od zachowania samych podróżujących.

> Wojska Obrony Cyberprzestrzeni to nie nowy rodzaj sił zbrojnych, ale formacja specjalna, działająca w wymiarze Defensive Operations, Offensive Operations oraz Intelligence, Surveillence and Reconessaince. Zajmujemy się więc cyberobroną, cyberatakiem i cyberrozpoznaniem.

Jest jednak jeszcze inny wymiar tego przenikania świata cyfrowego i rzeczywistego. Możemy zapewnić, że w porę uchronimy od większości zagrożeń i ataków – w zarodku albo u granic – społeczność, której strzeżemy. Natomiast nawet w ramach regulacji i zasad, jakie sobie wytworzymy do bezpiecznego funkcjonowania w cyberprzestrzeni, nadal mogą przenikać do niej elementy operacji psychologicznych PsyOps czy info-dezinformacyjnych InfoOps.

Takim wrogim operacjom dają doskonałe pole do działania cyfrowe kanały, w szczególności media społecznościowe. Są to: budowa baniek informacyjnych i psychologicznych, formatowanie profili, następnie popychanie do rezonowania określonych przekazów, tworzenie całych sieci świadomych i nieświadomych „pudeł rezonujących" przekaz, albo piętrowe przekazy, pochodzące np. z Federacji Rosyjskiej. Te działania są widoczne jak na dłoni.

Schematy są stare, bo to wszystko opisane zostało w „Montażu" Vladimira Volkoffa, klasycznej dla teorii dezinformacji powieści zawierającej opis technik budowy takich wielkoskalowych operacji.

Tylko dołóżmy sobie do tego skalę i dynamikę środowiska i społeczeństwa scyfryzowanego. Wywoływanie określonych reakcji trwa szybciej, a efekty są intensywniejsze.

Oba te obszary są poza zakresem naszych dzisiejszych podstawowych zadań, ale niekiedy – wcale zresztą nie incydentalnie – wkraczamy w nie. I wydaje mi się, że docelowo niezbędne będzie poszerzenie działań również na te sfery. Po to, aby obejmując taki pełniejszy kontekst, skuteczniej przeciwdziałać wrogim posunięciom.

Co bardzo poszerza nam definicję tej chronionej przez DKWOC cyberprzestrzeni, a w zasadzie rozmywa granice między światem fizycznym a wirtualnym.

> Wojska Obrony Cyberprzestrzeni w roku 2023 są sumą wcześniej rozproszonych, funkcjonujących w wojsku osobno jednostek organizacyjnych odpowiadających za informatykę, kryptologię, cyberbezpieczeństwo i łączność.

To nie jest abstrakcja, tylko usankcjonowanie rzeczywistej sytuacji. Tej granicy dziś nie ma. Zabawne, ale w tej chwili przypomniała mi się sytuacja z początków budowy Wojsk Obrony Cyberprzestrzeni. Pewien znany prawnik opublikował komentarz, w którym wysnuwał tezę, że jeśli wojsko ma bronić przestrzeni państwowej, a cyberprzestrzeni ściśle polskiej nie da się określić granicami, to wojska cyber w ogóle nie powinny działać. To było raptem w 2019 roku. Bardzo jestem ciekaw jak dzisiaj, w obecnej sytuacji geopolitycznej, ów prawnik zaktualizowałby swój komentarz i gdzie byśmy byli, gdybyśmy go wówczas posłuchali.

Wróćmy do samej struktury DKWOC. To w pewnej mierze efekt serii fuzji organizacyjnych i informatycznych?

Wojska Obrony Cyberprzestrzeni w roku 2023 są sumą wcześniej rozproszonych, funkcjonujących w wojsku osobno jednostek organizacyjnych odpowiadających za informatykę, kryptologię, cyberbezpieczeństwo i łączność. Funkcjonowały one pod różnym kierownictwem, często w różnych łańcuchach dowodzenia.

Istniała ogromna instytucja – Inspektorat Informatyki – która odpowiadała za budowanie systemów sieci teleinformatycznych oraz zapewnianie usług w resorcie obrony narodowej i siłom zbrojnym. Działała też osobna jednostka, odpowiedzialna za bezpieczeństwo. W relacji między nimi, ta silniejsza narzucała drugiej zwierzchnictwo. One nawet ze sobą nie tyle konkurowały, ile trudno było znaleźć równowagę pomiędzy oboma elementami. Spory rozstrzygano aż na poziomie wiceministra czy ministra.

Oczywiście przy tym wszystkim ten podział był zgodny z klasycznymi, najlepszymi praktykami ze świata cywilnej informatyki.

Czyli sytuującymi cyberbezpieczeństwo gdzieś obok IT, ale raczej poniżej.

Jednym z naszych zadań było więc połączenie tych rozproszonych jednostek. Autorem pomysłu fuzji był Tomasz Zdzikot, wówczas pełnomocnik Ministra Obrony, który zdefiniował projekt Cybermil.pl. Konsolidacja pod jednym dachem wszystkich kompetencji resortu Obrony Narodowej w ramach Cyber, Krypto i IT nie udałaby się, gdyby nie minister Mariusz Błaszczak, którego wsparcie w tym procesie jest nie do przecenienia. W 2019 roku przeprowadziliśmy połączenie dwóch ogromnych jednostek z osobnymi budżetami – Inspektoratu Informatyki i Narodowego Centrum Kryptologii. Powstało Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC). Było to ogromne wyzwanie, znane zapewne większości CIO, projekt, w którym większość zespołu pracowała po 20 godzin na dobę. Nie mogliśmy wyłączyć ani zakłócić żadnego procesu. Działaliśmy na żywym organizmie.

> Gdybyśmy prowadzili tylko operacje cyberobronne – to dawałoby naszym przeciwnikom poczucie bezkarności, przewagę psychologiczną. Przeciwnik musi mieć świadomość ryzyka nadziania się na kontrę, jak w meczu bokserskim.

Jakie definiowano korzyści na tym etapie?

Po pierwsze, konsolidacja wszystkich kompetencji cyber w dyspozycji MON. Istnienie centralnej jednostki znakomicie ułatwia kontakty i współpracę międzynarodową. Po drugie, powstałe NCBC stało się właściwym fundamentem do utworzenia Wojsk Obrony Cyberprzestrzeni. Jako pełnomocnik ministra zostałem wyznaczony do ich utworzenia. W 2019 roku opracowano i zatwierdzono koncepcję WOC. Wtedy określiliśmy, że mamy doprowadzić do budowy kompetencji pozwalających na prowadzenie pełnego spektrum działań w cyberprzestrzeni.

Dlaczego trzy elementy: obronne, cyberrozpoznawcze oraz ofensywne miały powstać od razu?

Gdybyśmy prowadzili tylko operacje cyberobronne – to dawałoby naszym przeciwnikom poczucie bezkarności,

przewagę psychologiczną. Przeciwnik musi mieć świadomość ryzyka nadziania się na kontrę, jak w meczu bokserskim. Inaczej jesteśmy skazani na porażkę, do wyboru tylko – na punkty lub przez nokaut.

Czas naglił. Nasze Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni powstało więc w ciągu 2 lat, choć np. Amerykanie budowali swoje przez lat 10. Postanowiliśmy też uczyć się na błędach innych. Dlatego bardzo szybko wdrożyliśmy czwarty filar DKWC – współpracę międzynarodową. Już w 2019 roku podpisaliśmy porozumienie z United States CyberCommand. Aby do tego doszło, musieliśmy jednak udowodnić, że jesteśmy partnerem godnym uwagi, co się udało. Innym naszym partnerem w budowie kompetencji szybko stał się również Izrael.

Wróćmy jeszcze do kwestii proaktywnej, a nie tylko reaktywnej działalności WOC, jakie stworzyła Ustawa o obronie Ojczyzny. Co w praktyce to oznacza?

Wychodzimy z założenia, że naszym zadaniem jest utrudnienie przeciwnikowi ataku i podniesienie kosztów prowadzenia przez niego operacji. Polujemy więc na przeciwników w naszych sieciach i poza nimi.

Musimy mieć zdolności działania w cyberprzestrzeni zarówno w strefie niebieskiej, czerwonej, jak i szarej, bo przeciwnik atakuje chętnie również pod obcą flagą, z cyberprzestrzeni neutralnej lub zaprzyjaźnionej, pozornie bezpiecznej.

Chcemy być gotowym do działania, a nie tylko reagować, a także uczyć się przeciwnika, poznawać jego taktyki, by skuteczniej przeciwdziałać atakom.

Punkt wyjścia naszych działań definiuje prawo międzynarodowe. Jest nim prawo każdego państwa do samoobrony, więc dowódca WOC nie może dowolnie atakować. Mamy środki i narzędzia, aby się bronić i aktywnie działać, zakłócać rozwój ataku, uderzając także w „pozycje wyjściowe" agresora. Każde nasze działanie podlega analizom prawnym.

Dziś, jeżeli chodzi o budowę WOC, jesteśmy w innym miejscu niż w roku 2019. Nie zawiódł nas zdrowy rozsądek. Zbudowaliśmy kompetencje i wzmożone działanie grup APT pod egidą rosyjską nie robi dzisiaj na nas wrażenia. W 2023 roku, na progu drugiego roku wojny na Ukrainie, nasze cele operacyjne są dojrzałe. Eksperci mają niezbędne umiejętności. Działają 24/7 pod ogromną presją tych grup, a nie doszło do przełamania naszych zabezpieczeń, i to pomimo wielu różnych typów ataków, przy realizacji wielu scenariuszy...

A kontratak?

Mogę powiedzieć w tej kwestii tylko tyle, że celem naszych obserwacji jest również ustalenie podatności przeciwnika. Każdy je ma, ale często ci, którzy działają ofensywnie, słabiej dbają o własną cyberhigienę i łatwiej demonstrują podatności. Nie jest tak, że nie są do namierzenia.

Wojska Obrony Cyberprzestrzeni z tego opisu wydają się bliższe siłom wywiadowczym. Tylko chyba skala cyfryzacji sprawia, że stają się ugrupowaniem tak silnym, tak licznym i o takiej intensywności działania?

Bardziej używałbym analogii do rozpoznania i zwiadu. Wywiad działa bardziej na zewnątrz. W cyberprzestrzeni interakcje z przeciwnikiem zachodzą przede wszystkim w naszych sieciach. Na naszych salach operacyjnych przeciwnik często wchodzi w zdefiniowane przez nas przestrzenie i wydaje mu się, że działa swobodnie, bez naszej wiedzy. Tymczasem obserwujemy go i rozpoznajemy cały czas jego sposób działania, umiejętności, taktykę, procedury, zakresy zainteresowania. Wywiad takie dane pozyskuje bardziej na zewnątrz. My natomiast uczymy się dużo od przeciwnika.

Porozmawiajmy o modelu pozyskiwania i utrzymania tych kompetencji. Ze względu na zakres działania Wojska Obrony Cyberprzestrzeni sprawiają wrażenie bardzo interdyscyplinarnego zespołu „wymiennych" ekspertów. Podobnego do DevSecOps, skoro w ich pieczy znajduje się też dostarczanie infrastruktury i rozwiązań. To wyróżniało WOC od organizacji i koncepcji działających w przestrzeni publicznej, komercyjnej, gdzie wydaje mi się panuje większa specjalizacja, aby nie powiedzieć silosowość.

Mogę śmiało stwierdzić, że WOC to moja podróż życia.

> Punkt wyjścia naszych działań definiuje prawo międzynarodowe. Dowódca WOC nie może zatem dowolnie atakować. Mamy środki i narzędzia, aby się bronić i aktywnie działać, zakłócać rozwój ataku, uderzając także w „pozycje wyjściowe" agresora.

Mamy ludzi o wielkim potencjale intelektualnym, a przy tym niezwykle głodnych wiedzy, samorozwoju. Jest to potrzebne, ponieważ na naszych salach operacyjnych nie wystarczą umiejętności, niezbędna jest kreatywność. Taki profil udało się nam naszkicować i on funkcjonuje – na co dzień widzę radość zespołu, zmieniającego często „kapelusze".

Zespoły krypto także są niezwykłe, podejmują np. już dziś problemy kryptografii postkwantowej. Nasze algorytmy mają być odporne na deszyfrowanie za pomocą komputerów kwantowych.

Z wojska wychodzi innowacja, która może uczynić odporną również naszą gospodarkę?

Jako siły zbrojne musimy to adresować najwcześniej – bez wchodzenia w szczegóły powiem tylko, że Jerzy Różycki, Henryk Zygalski, Marian Rejewski (matematycy polskiego wywiadu, którzy pierwsi złamali kod Enigmy – przyp. red.), gdyby się u nas pojawili, byliby bardzo zadowoleni ze swoich następców.

To moje poczucie podzielają także zagraniczni partnerzy, którzy są pod wrażeniem, że nam się udało w ciągu 3–4 lat ten potencjał intelektualny utrzymać i bardzo rozwinąć. Widać to np. podczas spotkań wspólnego Cyber Command NATO dwa razy do roku, gdzie prezentujemy nasz potencjał, gdzie możemy porównać się z innymi. Wracam stamtąd zawsze z dumą.

Widać, jak się rozwijamy, podczas gdy niektóre kraje stoją w miejscu, de facto się cofając. Niestety większość armii, również wielkich, outsourcuje najwyższy poziom kompetencji. Ich rozwiązania i algorytmy tworzą po prostu BigTechy. Oni, jako dowódcy, definiują potrzebę i to jest im dostarczane przez zaufane podmioty, ale z przestrzeni komercyjnej.

Co zatem przekonuje talenty do wstępowania do WOC? Wątpię, aby wojsko było w stanie zapłacić więcej niż podmioty rynkowe specjalistom cyberbezpieczeństwa.

Sukces opiera się na budowie całego ekosystemu. Podstawowym elementem jest odpowiednia kultura. Utrzymania ludzi w zespole wymagamy od liderów. Dobry dowódca nie powinien przeszkadzać, a doskonały powinien dodatkowo pomagać.

Stąd też bardzo duży nacisk kładę na budowę przywództwa. W wojsku to trudne, bo tradycyjnie przełożony ma zawsze rację. Muszę to zmieniać. Dowódca podejmuje decyzję i bierze odpowiedzialność za nią, i za żołnierzy. Ale bazuje na wiedzy żołnierzy, którzy często przerastają go umiejętnościami czy talentem. Decyzja rodzi się podczas burzy mózgów. Powstaje wówczas rozwiązanie problemu i może je dostarczyć młody kapitan czy porucznik. Pułkownik ma inne zadania związane z przywództwem, zgraniem zespołu. Wchodzenie na salę operacyjną i komenderowanie byłoby nieodpowiednie.

> Na naszych salach operacyjnych przeciwnik często wchodzi w zdefiniowane przez nas przestrzenie i wydaje mu się, że działa swobodnie, bez naszej wiedzy. Tymczasem obserwujemy go i rozpoznajemy cały czas jego sposób działania, taktykę, procedury...

Wszyscy moi dowódcy przeszli szkolenia z psychologami z przywództwa nt. umiejętności miękkich, by uczynić tę współpracę efektywniejszą. Wymagamy też kultury w zakresie kontaktu z informacją niejawną i uzyskania – w toku szkolenia – statusu dostępu aż do najwyższych klauzul. Nakładamy na piękny umysł obciążenia. Jeśli lider ich nie przepracuje z nimi indywidualnie, to sobie z nimi nie poradzą.

Podsumowując, największe wyzwanie dotyczy posiadania odpowiednich liderów, szefów zespołów. Bo specjalistów chętnych i zdolnych jest wielu. Mamy – jako naród – niespotykane umiejętności matematyczne, ale co innego samotne wilki, a co innego zespół. Nasze operacje wymagają pracy zespołowej.

Czy praca nad technikami przywództwa przynosi efekty? Zespoły się zgrywają?

Tak, mamy tego dowody międzynarodowe, np. na ostatnich ćwiczeniach Locked Shields udało się ułożyć polski zespół i zgrać tak, że zajął w 2022 roku 1. miejsce w NATO i 2. na świecie, po Finlandii. 100-osobowy zespół polsko-litewski – kierowany przez naszego oficera – osiągnął sukces w tych najcięższych, NATO-wskich ćwiczeniach odwzorowujących realistycznie obronę różnych systemów państwa w trakcie ciągłego ataku.

To pokazuje, gdzie jesteśmy jako wojsko i jako kraj. Mam przekonanie, że w przypadku ataku podobnego do tego na

infrastrukturę cyfrową w Estonii, zebralibyśmy zespół, który potrafiłby stawić mu czoła. W przypadku wojny musimy także umieć skoordynować pracę różnych CSIRT-ów, które przechodzą pod dowództwo MON. Nie da się tego zrobić bez wcześniejszego przygotowania, zapoznania.

Biorąc pod uwagę sytuację i doświadczenia z Ukrainy, to wojsko bierze odpowiedzialność za ochronę infrastruktury krytycznej. Podobne są też doświadczenia partnerów z zagranicy. W trakcie ataku na Colonial Pipeline w 2021 roku generał Paul Miki Nakasone, szef US CyberCommand, również został poproszony o wsparcie cyberwojsk amerykańskich.

A dalszy rozwój – jakie ma znaczenie, jakie są możliwości?

Stworzyliśmy Eksperckie Centrum Szkolenia Cyberbezpieczeństwa. Pozwala to szkolić kadry w myśl naszych potrzeb. Żołnierze z zaciągu, prosto z uczelni, szybko przekonują się, że uczelnia była przedszkolem i osoba z rocznym doświadczeniem z sali operacyjnej może mu w jednej chwili pokazać miejsce w szyku.

Ten ekosystem jest w wymiarze rozwoju nawet szerszy, ponieważ od 2019 roku działa Wojskowe Liceum Informatyczne przy Wojskowej Akademii Technicznej z naszym wsparciem pedagogicznym. Pierwsi abiturienci uzyskali średnią 96% z matematyki rozszerzonej na maturze. Aż 20 z 25 z nich zdecydowało się wstąpić na WAT. Ponadto w 16 szkołach w Polsce, w miejscowościach do 150 tys. mieszkańców, powołaliśmy klasy cyberbezpieczeństwa – to program „CYBER.MILz klasą". Nasi eksperci stworzyli specjalistyczny program nauczania, obejmujący m.in. informatykę na poziomie rozszerzonym, kryptografię, algorytmikę czy cyberbezpieczeństwo. Jesteśmy obecni w tych szkołach i zachęcamy, aby ich absolwenci założyli mundur.

> Zespoły krypto Wojsk Obrony Cyberprzestrzeni są niezwykłe, podejmują np. już dziś problemy kryptografii postkwantowej. Nasze algorytmy mają być odporne na deszyfrowanie za pomocą komputerów kwantowych.

> Nawet w ramach regulacji i zasad, jakie sobie wytworzymy do bezpiecznego funkcjonowania w cyberprzestrzeni, nadal mogą przenikać do niej elementy operacji psychologicznych PsyOps czy info-dezinformacyjnych InfoOps, w szczególności w mediach społecznościowych.

Nie tylko polujemy więc na talenty, ale pomagamy je wyszukiwać i kreować.

Jak wygląda utrzymanie zespołów? Przytaczam często przykład Szymona Krupy z UM Warszawy, który – nie mogąc konkurować z rynkiem – stosował kontrolowaną rotację. Ale w cyberwojskach to chyba niemożliwe.

Pamiętam, jak generał Nakasone doradzał mi: opłać kandydatom studia. Odpowiadam: mamy to zagwarantowane w konstytucji. To może pakiet medyczny? Mówię: dziś to na naszym rynku minimum. A jak jeszcze dowiedział się, że żołnierz może odejść w pół roku – po prostu zdjąć mundur – to przyznał, że mamy prawdziwe wyzwanie.

Model utrzymania kompetencji obejmuje wspominane organiczne inicjatywy rozwojowe. Ponadto Minister Obrony Narodowej przyjął specjalne dodatki dla żołnierzy realizujących zadania cyberbezpieczeństwa wliczane do emerytury. Ale nigdy nie będziemy się w tych kategoriach ścigać z biznesem.

Mamy jednak historię, etos, który pozwala nam sformułować dobrą odpowiedź na klasyczne pytanie Simona Sineka o organizację: „why?". Trzeba znaleźć własną tożsamość i cel, który może przyciągnąć podobnie myślących. Formułując tę odpowiedź – komunikując nasze cele, podejście, kulturę i przedstawiając środki, jakimi można to realizować – uzyskujemy mocny odzew z rynku pracy.

Ja sam zazdroszczę wstępującym w nasze szeregi żołnierzom. Uzyskują dostęp do najnowocześniejszych rozwiązań i technologii, do których ja kończąc studia, dostępu

nie miałem. Tego, nie ma co kryć – armia może sobie na nie pozwolić. Patrząc na sytuację na świecie – nie ma wyboru, tylko musi zapewnić narzędzia, broń, która będzie pozwalała efektywnie wykorzystać potencjał cyberżołnierzy. W Polsce żadna inna organizacja – może poza służbami specjalnymi – nie może sobie na to pozwolić.

Po drugie nasi żołnierze traktowani są jak podmiot, a nie przedmiot – paradoksalnie, bo wojsko z tym się nie kojarzy. Nie są śrubką w machinie generującej przychód, jak nieuchronnie w każdej firmie komercyjnej. Szkolenie czy konferencje to są rozchody dla firmy. Dla nas to jest inwestycja w kapitał intelektualny, której nie skąpimy, a to jest przejawem wspomnianego upodmiotowienia. Ale jest jeszcze jedna rzecz, której ogromnie żołnierzom zazdroszczę – to zadania, które realizują. To są sprawy tej rangi i skali, że nigdzie indziej nie są dostępne.

Nowością w tym ekosystemie jest ścieżka rozwoju. Możliwości awansu nie są już iluzoryczne, jak kiedyś przed absolwentem łączności czy elektroniki podejmującym służbę. Ścieżkę od szeregowca do generała dowódcy przejść może każdy, ale nie każdy musi. Wzorem organizacji komercyjnych mamy także ścieżkę ekspercką, która nie wymaga budowy kompetencji przywódczych. Nie każdy musi być liderem i szefem zespołu, aby cieszyć się szacunkiem i rozwijać się w WOC.

Wszyscy wiemy również, że dla inżynierów w większości cel najczęściej jest ważniejszy niż pieniądze. Oczywiście one muszą być godziwe i o to dbamy, ale musi być też jasno zarysowany sens, cel, etos służby. To – w połączeniu ze spójnym ekosystemem – sprawia, że służba w DKWOC cieszy się dużym zainteresowaniem.

Dodatkowe środki na wynagrodzenie, dostęp do technologii, kultura organizacyjna i odpowiedź na kluczowe pytanie: „po co?" składają się na obecne powodzenie. Znam przypadki, że na niektóre osoby z naszych zespołów notorycznie polują rekruterzy i słyszę z rynku plotki, że moi żołnierze dostali taką czy inną ofertę – ale ze względu na warunki, atmosferę, kulturę panującą w DKWOC – zostali.

Wojskowa Akademia Techniczna często przewija się w naszej rozmowie.

Podsumowując ten wątek, chciałbym wrócić do tego, w jaki sposób WAT przygotowuje ludzi odpowiednich dla Wojsk Obrony Cyberprzestrzeni. Muszę powiedzieć, że – zwłaszcza w kontekście wyzwania, jakim jest przywództwo generacji Z – to wielka praca. Dlatego, że temu pokoleniu, przyzwyczajonemu od początku do handicapów, na wstępie stawia się wysoko poprzeczkę. Może ucierpieć na tym uczelnia, jeśli 6-tygodniowego, podstawowego wyszkolenia wojskowego nie wytrwa jakiś wybitny intelekt, ale chodzi także o wybór pewnego profilu psychologicznego. On może się kształtować, choć w obrębie pewnych predyspozycji. Żołnierz po prostu musi umieć działać w stresie i pod presją czasu. To nie może się zmienić dlatego, że generacja Z jest inaczej wychowywana w domu.

Odsiew na dzień dobry, a potem program wręcz przeładowany. I to się sprawdza?

W ostatecznym rozliczeniu bardzo. Mieliśmy nawet anegdotyczne sytuacje, kiedy przedstawiciele sojuszniczych zespołów nie mogli nawiązać w naszym gronie równorzędnej dyskusji i pozostawała im „łatwiejsza" rozmowa z kontraktorami. WAT tworzy wręcz naukowca w mundurze. Sam wspominam te studia, kiedy na kursie modulacji detekcji miałem tak wymagającego wykładowcę, że na koniec schematy modulatorów układałem w głowie, „a vista".

Wojskowa Akademia Techniczna uczy, wymaga i kształtuje charakter. Zatem w mojej osobistej opinii nie ma nic dziwnego w tym, że absolwenci akurat WAT licznie obsadzają stanowiska liderów IT na rynku. WAT uczył też szukania kreatywnych rozwiązań problemów itd.

Pamiętam, kiedy sam kilka tygodni po przydziale do pierwszej jednostki i dowodzeniu poborowymi miałem dłuższą chwilę refleksji czy dobrze wykorzystuję to wszystko, czego się nauczyłem. Bo na początku XXI wieku do wojska szły osoby, które sobie nie załatwiły odroczenia. A ja po napisaniu pracy o mobilności IP v6 musiałem uczyć niektórych poborowych podstawowych zasad higieny. Dopóki nie powstało NCBC, a teraz DKWOC, dopóty wielu absolwentów WAT po prostu szło na rynek cywilny. Dla armii w większości byli straceni. Mnie się udało, bo zacząłem zabiegać o przeniesienie w odpowiednie miejsce. Ale wielu kolegów na pewno nie wytrzymało.

Dziś otwieramy drzwi dla najlepszych absolwentów, a jako DKWOC mamy „zbójeckie prawo" do pierwszeństwa oferowania im pracy. Utrzymamy w ekosystemie kompetencje i rozwiniemy je. Zdefiniowaliśmy i zaadresowaliśmy wszystkie ryzyka w naszej sytuacji. I to działa.

Wywiad przeprowadził
Szymon Augustyniak

omnilogy

Omnilogy:

Proponujemy naturalne, ale nieoczywiste podejście do bezpieczeństwa

Z **Tomaszem Płońskim**, CTO w Omnilogy, rozmawiamy o punktach styku pomiędzy bezpieczeństwem i obserwowalnością środowisk IT, możliwościach analizy i wykrywania podatności bezpośrednio na poziomie wykonywanego kodu aplikacji, a także o niezbędnych wnioskach z podatności Log4Shell oraz sposobach rozwiązań Dynatrace i Sysdig.

Cyberbezpieczeństwo i obserwowalność to, według prognoz, jedne z najważniejszych priorytetów w zakresie inwestycji z obszaru IT. Rzadko jednak występowały w parze…

To jest jeden z mitów, które należy obalić. Jak nigdy dotąd, połączenie obserwowalności i bezpieczeństwa staje się czymś tak oczywistym, że aż trudno sobie wyobrazić, że do tej pory traktowaliśmy je oddzielnie. Wiele osób nie potrafi dostrzec tego, co faktycznie łączy te dwa światy. Mówię tutaj o danych. Bezpieczeństwo obejmuje tworzenie procedur i standardów, ale opiera się przecież na systemach, które analizują dane nt. zachowania użytkowników i aplikacji.

Jeżeli popatrzymy z kolei na obserwowalność, to już w jej definicji znajduje się możliwość pomiaru bieżącego stanu systemu na podstawie generowanych przez ten system danych, takich jak logi, metryki i trace'y. W nowoczesnych środowiskach każde urządzenie, oprogramowanie, komponent infrastruktury chmurowej, każdy kontener i każda mikrousługa tworzy zapisy aktywności.

> Platforma Dynatrace analizuje wykonywany kod aplikacji na poziomie każdej transakcji. Widzimy rzeczywiste ścieżki komunikacji oraz zakres danych, do których poszczególne komponenty środowiska mają dostęp. Taka wiedza jest ogromnym ułatwieniem dla zespołów CyberSec.

Celem obserwowalności jest zrozumienie, co dzieje się we wszystkich tych środowiskach i technologiach. W ten sposób obserwowalność zapewnia nowe narzędzia do wykrywania i rozwiązywania problemów, co przekłada się na większą niezawodność i wydajność systemów, a także na zadowolenie użytkowników lub klientów. Cyberbezpieczeństwo analizuje dane z tych samych środowisk i z tych samych komponentów. Dane są więc z jednej strony spoiwem tych dwóch światów, a z drugiej – sprawiają, że obie dziedziny znajdują wspólny język.

Czy podobną spójność widać już na poziomie narzędzi wykorzystywanych w kontekście bezpieczeństwa i utrzymania infrastruktury?

Odpowiedź zależy od stosowanych narzędzi. Na poziomie technicznym kwestie bezpieczeństwa oraz monitoringu IT są nadal często postrzegane w sposób od-

> W definicji obserwowalność znajduje się możliwość pomiaru stanu systemu na podstawie generowanych przez ten system danych, takich jak logi, metryki i trace'y. Każde urządzenie, oprogramowanie, komponent chmurowy, kontener, mikrousługa generuje zapisy aktywności.

rębny. Takie rozumienie wynika z faktu, że działy cyberbezpieczeństwa, co do zasady, korzystają z dużej liczby zróżnicowanych narzędzi, patrzą na zagrożenia z wielu perspektyw i na wielu poziomach. W kontekście utrzymania infrastruktury ciągle odnosimy się zaś głównie do statycznego monitoringu. Obserwowalność to jednak zdecydowanie coś więcej.

Jako Omnilogy oferujemy klientom platformę obserwowalności Dynatrace, obserwowalności, a nie monitoringu. Jej nadrzędnym zadaniem – poza zbieraniem danych telemetrycznych z obserwowanych komponentów – jest zrozumienie i analizowanie zależności między tymi danymi i ich źródłami. Zależności te mają kluczowe znaczenie zarówno w kontekście prac mających na celu zapewnienie jak największej sprawności infrastruktury IT, jak i w procesie analizy skali zagrożeń.

Platforma Dynatrace analizuje wykonywany kod aplikacji na poziomie każdej transakcji. Widzimy więc dokładnie rzeczywiste ścieżki komunikacji oraz zakres danych, do których poszczególne komponenty środowiska mają dostęp. Taka wiedza jest ogromnym ułatwieniem dla zespołów odpowiedzialnych za bezpieczeństwo.

Czy oprogramowanie Dynatrace pozwala także na wykrywanie zagrożeń?

Tak, choć jest to szerszy temat. Zacznijmy od najprostszego przypadku. Dynatrace jako rozwiązanie agentowe analizuje kod uruchamiany w poszczególnych aplikacjach. Mogą to być samodzielne aplikacje, ale także mikroserwisy, aplikacje działające w kontenerach, w chmurze prywatnej czy publicznej. Mogą być to również aplikacje typu serverless – jak Azure Functions czy AWS Lambda. Jednocześnie, oprogramowanie Dynatrace bazuje na algorytmach AI, wykrywających anomalie w stosunku do tego, co zostało sklasyfikowane jako normalne zachowanie danego systemu. Może więc – w pełni automatycznie – wykrywać profile zachowania aplikacji odbiegające od normy, np. zwiększony poziom ruchu, błędnych logowań lub błędów biznesowych.

To właśnie dzięki takim obserwacjom można w bardzo łatwy sposób wykrywać potencjalne zagrożenia czy próby naruszenia polityk bezpieczeństwa. W jednej z organizacji, dzięki tego typu funkcjonalności, bardzo szybko wykryliśmy próbę skopiowania bazy klientów przez automat przeszukujący w godzinach nocnych zbiory danych przy użyciu losowo generowanych identyfikatorów. Tego typu możliwości, choć być może nie są wprost związane z bezpieczeństwem, Dynatrace zapewnia w bardzo naturalny sposób. Przykładem dedykowanej funkcjonalności bezpieczeństwa w ramach tej platformy jest wykorzystanie agenta analizującego uruchamiany kod aplikacji do wykrywania podatności potencjalnie w tym kodzie istniejących.

Czy chodzi o tego samego agenta Dynatrace, który zbiera dane telemetryczne?

Dokładnie tego samego oraz stojącą za nim sztuczną inteligencję. Agent ma dostęp do załadowanych bibliotek, analizuje kod wykonywanych transakcji. Nie trzeba zatem na serwerach instalować dodatkowego narzędzia. Nie trzeba też wykonywać żadnych dodatkowych skanów. Dynatrace synchronizuje się z publicznymi bazami podatności – m.in. SNYK i NVD – i sprawdza uruchomiony kod aplikacji pod kątem znanych luk. Co ważne, takie rozwiązanie działa w trybie ciągłym i nie powoduje żadnego narzutu wydajnościowego na obserwowaną aplikację.

Równolegle, wszystkie gromadzone dane są interpretowane w czasie rzeczywistym – sztuczna inteligencja tworzy model analizowanych aplikacji oraz mapę powiązań między komponentami na poziomie fi-

zycznym i logicznym. Poza tym na bazie przyjętego modelu ocenia poziom ryzyka – rozumie bowiem zależności oraz kontekst zbieranych danych. W przypadku wykrytych podatności Dynatrace – oprócz wskazania ich istnienia – dodatkowo analizuje czy dany komponent jest dostępny z sieci publicznej oraz czy ma dostęp do baz danych. Dostarcza więc komplet informacji o tym, jakie usługi lub bazy danych mogą być zagrożone wskutek odnalezionej w kodzie aplikacji podatności.

Jak dużym ułatwieniem dla zespołów odpowiedzialnych za bezpieczeństwo IT jest tego rodzaju funkcjonalność?

Ogromnym! Działy bezpieczeństwa z reguły zasypywane są informacjami o kolejnych incydentach, faktycznych lub potencjalnych. W efekcie, skuteczność ich pracy zależy w dużej mierze od umiejętności właściwego definiowania priorytetów i planowania prac, tak aby w pierwszej kolejności rozwiązywać zgłoszenia, które mają naprawdę krytyczne znaczenie. Tymczasem zdecydowana większość informacji o wykrytych podatnościach to fałszywe alarmy albo podatności o małym prawdopodobieństwie wykorzystania.

Warto pamiętać, że każda podatność raportowana z publicznej bazy ma ocenę ryzyka CVSS w skali od 0 do 10, gdzie 10 oznacza maksymalny poziom ryzyka. Jest to metryka przydatna, jednak oderwana od kontekstu danej organizacji. Nie znając kontekstu, w którym działa komponent z wykrytą podatnością, nie mamy podstaw, aby określić rzeczywisty poziom ryzyka. Każdy alarm musimy analizować z najwyższą uwagą.

W tym kontekście podejście Dynatrace wyróżnia m.in. funkcjonalność automatycznej oceny poziomu zagrożenia – bardzo trafnej zresztą. Platforma Dynatrace definiuje bowiem własny wskaźnik zwany Davis Security Score, który wyjściowo bazuje na ocenie CVSS, ale zrewidowany pod kątem konfiguracji konkretnego środowiska. Przykładowo, system Dynatrace jest w stanie zmniejszyć ocenę ryzyka, jeśli do komponentu, w którym wykryta została podatność, nie można dostać się z sieci publicznej – czyli potencjalny atak jest mniej prawdopodobny – lub też nie ma on dostępu do bazy danych, zatem ryzyko kompromitacji danych jest mniejsze. Ponadto, dla każdej zidentyfikowanej podatności Platforma Dynatrace dostarcza informację o ewentualnym istnieniu publicznych eksploitów, za pośrednictwem których realizowana jest największa liczba ataków. Tego rodzaju selekcja odbywa się na poziomie każdego komponentu z osobna, co pozwala odpowiednio ustawić priorytety zadań w przypadku jednoczesnego wykrycia podatności na wielu komponentach – tak jak miało to miejsce w przypadku luki Log4Shell.

> Dynatrace synchronizuje się z publicznymi bazami podatności – m.in. SNYK i NVD – i sprawdza uruchomiony kod aplikacji pod kątem znanych luk. Takie rozwiązanie działa w trybie ciągłym i nie powoduje żadnego narzutu wydajnościowego na obserwowaną aplikację.

Z jakimi nakładami pracy wiąże się konfiguracja funkcji Application Security w Dynatrace?

Nie trzeba nic konfigurować. Wykorzystywana jest tu wyłącznie natywna funkcjonalność agenta i samej platformy. Jedyne, co trzeba zrobić, to zdecydować czy alarmy bezpieczeństwa chcemy obserwować w samym Dynatrace, czy zintegrować je z centralną konsolą SOC. Tego typu funkcjonalność jest trudna do przecenienia – zdolność do wykrywania podatności w stosowanych bibliotekach w czasie prawie rzeczywistym, bez obciążania systemu monitorowanego, bez żadnej konfiguracji jest dzisiaj niezbędna. Funkcjonalność Application Security diametralnie zmienia możliwości wykrywania podatności. Dotychczas standardową praktyką dla większości – tych bardziej świadomych – organizacji było wykonywanie skanów pod kątem podatności w środowiskach produkcyjnych regularnie, ale rzadko – na przykład raz na tydzień. Takie skany są kosztowne, a jednocześnie zwykle generują dużą liczbę fałszywych alarmów. Z kolei ich niewystarczająca częstotliwość sprawia, że luka w publicznie dostępnej usłudze może być otwarta przez kilka dni.

Dynatrace eliminuje takie ryzyko w sposób automatyczny. Automatyzacja wykrywania podatności jest szczególnie istotna w projektach transformacji cyfrowej zakładających modernizację aplikacji za sprawą mikroserwisów i chmury obliczeniowej, które znacząco zwiększają dynamikę zmian i skomplikowanie powiązań w aplikacjach. Dynatrace swoim rozwiązaniem wychodzi naprzeciw tym wyzwaniom dzięki zastosowaniu automatyzacji i AI.

Wykrywanie podatności to jednak nie wszystko…

Faktycznie. Prawdziwa siła Platformy Dynatrace objawia się w funkcjonalności analizy własnego kodu pod kątem możliwości przeprowadzenia ataków. Innymi słowy, zapewnia ona możliwość oceny czy tworzony w organizacji kod nie zawiera błędów, które mogą być wykorzystane przez cyberprzestępców. Jest to o tyle istotne, że kod aplikacji jest dziś tworzony w ogromnym tempie. Jeśli zestawimy ten fakt z problematyką luki kompetencyjnej i koniecznością zatrudniania początkujących deweloperów, to błędy w kodzie oprogramowania stają się wręcz naturalne.

Takie błędy, nawet najmniej oczywiste, potencjalnie mogą generować nowe podatności. Dlatego, analizując kod wykonywany na poziomie każdej transakcji, agent Dynatrace jest w stanie stwierdzić, czy jest on w pełni bezpieczny, czy może zostać wykorzystany na potrzeby ataku. Oczywiście, analogicznie, jak w przypadku wykrywania podatności bibliotek, automatycznie wykonywana jest też analiza

ryzyka, ekspozycji na atak i naruszenia bezpieczeństwa danych.

Ponadto, taka analiza dostarcza konkretnych informacji o typie każdej podatności, stwierdzając, czy pozwala ona na przeprowadzenie ataku typu SQL Injection, Command Injection czy Improper Input Validation. Programista otrzymuje więc kompletną informację na czym polega problem wraz ze wskazaniem miejsca w kodzie, w którym taka podatność występuje – nie zostaje mu nic innego jak rozpocząć naprawę.

A co w sytuacji, kiedy taka podatność zostanie wykorzystana do przeprowadzenia ataku jeszcze zanim zostanie naprawiona?

Istnieją dwa scenariusze. W pierwszym z nich agent Dynatrace wykryje atak, zaraportuje użycie luki i wskaże całą ścieżkę ataku, włącznie z informacjami o tym, do jakich danych próbowano się dostać. Drugi scenariusz działania jest szerszy. Zakłada bowiem, że po wykryciu próby ataku agent Dynatrace zablokuje kod wykonywanej transakcji – tylko tej konkretnej, dzięki czemu cała aplikacja pozostaje w pełni funkcjonalna. Decyzja o tym, w jakim trybie pracuje agent, to jedyna istotna konfiguracja, którą trzeba wykonać.

W jaki sposób rozwiązania Dynatrace ułatwiają prowadzenie takich analiz?

Scenariusz przeszukiwania olbrzymich ilości danych w kontekście bezpieczeństwa był impulsem do odejścia od tradycyjnych systemów indeksujących logi. Na potrzeby Dynatrace stworzono autorską koncepcję „Grail Data Lakehouse", która nie wymaga m.in. indeksowania i umożliwia budowanie wynikowej struktury danych w locie. Mechanizmy równoległego przetwarzania pozwalają na natychmiastowy dostęp do danych historycznych, tak samo jak do danych bieżących. Dzięki temu zyskujemy dowolność przy robieniu analizy typu post mortem, a dział bezpieczeństwa może z łatwością poszukiwać nieprzewidzianych wcześniej zależności.

Mówiliśmy o bezpieczeństwie aplikacji w środowiskach produkcyjnych, a co z ochroną środowisk przedprodukcyjnych, typowych dla świata DevSecOps?

DevSecOps, podobnie jak DevOps, bazuje na automatyzacji i możliwości szybkiego dostępu do wskaźników pozwalających na ocenę jakości dostarczanego oprogramowania. Dostępną w platformie Dynatrace funkcjonalność Application Security można z powodzeniem wykorzystać do automatycznej oceny wydań pod kątem braku istotnych podatności i na podstawie dostarczonych danych np. wstrzymać promocję konkretnego wydania aplikacji do kolejnych środowisk.

Czy zautomatyzować można także kwestie, takiej jak weryfikacja konfiguracji aplikacji pod kątem zgodności z obowiązującymi w organizacji politykami?

Oczywiście! Tego typu potrzebom świetnie odpowiada rozwiązanie Sysdig – dedykowane narzędzie, które rekomendujemy w projektach chmurowych, zarówno w obszarze chmury prywatnej, jak i chmury publicznej. Jesteśmy bowiem w stanie włączyć Sysdig w proces tworzenia infrastruktury w modelu GitOps – Infrastructure as Code, a rozwiązanie to automatycznie zidentyfikuje potencjalne ryzyka i niezgodności z politykami w szablonach konfiguracji oraz pozwoli zablokować ich wykorzystanie. Podobnie w przypadku obrazów maszyn.

> Dynatrace definiuje własny wskaźnik zwany Davis Security Score, który bazuje na ocenie CVSS, ale zrewidowany pod kątem konfiguracji konkretnego środowiska. Zmniejsza np. ocenę ryzyka, jeśli do komponentu, w którym wykryta została podatność, nie można dostać się z sieci publicznej.

W efekcie, Sysdig zapobiega uruchomieniu aplikacji, która nie spełnia standardów bezpieczeństwa. W ramach projektów, które realizujemy przy użyciu Sysdig, jesteśmy w stanie sprawdzić zgodność konfiguracji z takimi standardami, jak CIS benchmarks, NIST 800-53, SOC2 czy PCI-DSS. Zapewniamy poświadczenia, które mogą być wykorzystane do wewnętrznych i zewnętrznych audytów.

Co więcej, właśnie Sysdig pomaga w nadawaniu uprawnień minimalnych, sugerując odpowiednie zasady, tak aby eliminować przypadki przydzielania nadmiarowych przywilejów. Jest to o tyle ważne, że struktura uprawnień w środowiskach chmurowych jest bardzo granularna, skomplikowana i stale się rozrasta.

Czy zapewnienie bezpieczeństwa środowisk aplikacyjnych opartych na zasobach chmurowych wymaga zupełnie innego rozłożenia ciężaru działań w obszarze bezpieczeństwa IT?

Zdecydowanie tak. Nie ma przypadku w tym, że kładziemy dzisiaj nacisk na bezpieczeństwo samej aplikacji i konkretnych zasobów chmurowych. Największy wpływ mamy bowiem na to, co uruchamiamy i na to, gdzie uruchamiamy. Dobierając odpowiednie techniki i narzędzia, a także włączając bezpieczeństwo w procesy DevOps, jesteśmy w stanie stworzyć rozwiązania, które w sposób w pełni zautomatyzowany pozwolą na zapewnienie bezpieczeństwa opartego na warstwie aplikacji i infrastruktury. Myślę, że w tym kontekście oferta Omnilogy jest naprawdę unikalna. Jesteśmy blisko procesów zagwarantowania niezawodności, a nie da się zapewnić niezawodności bez bezpieczeństwa aplikacji. Znamy się na tym, choć – przyznaję – proponujemy naturalne, ale ciągle nieoczywiste podejście.

Wywiad przeprowadził
Piotr Waszczuk

NIS2: będziemy aktywnie koordynować i wspierać wdrażanie dyrektywy przez polskie firmy

Z **Łukaszem Wojewodą,** dyrektorem Departamentu Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów, rozmawiamy o diagnozie gotowości firm do wdrożenia dyrektywy NIS2; wsparciu ze strony administracji; korzyściach i sposobach komunikacji transformacji podejścia do cyberbezpieczeństwa.

Co jest najważniejszą zmianą z perspektywy krajowej, państwowej, którą wprowadza dyrektywa NIS2 i jak jesteśmy na nią przygotowani?

NIS2 jest dyrektywą horyzontalną. Założeniem jest, aby objęła tymi samymi wymaganiami wszystkie kraje Unii Europejskiej. Będzie to wyzwanie dla administracji publicznej i dla firm.

Pod parasolem dyrektywy NIS2 znajdzie się znacznie więcej podmiotów. Dotychczasowe sektory rozbudowano o nowe rodzaje podmiotów. Przykładowo w sektorze infrastruktury cyfrowej zostaną ujęci operatorzy chmury obliczeniowej, a także operatorzy telekomunikacyjni, którzy dotąd pozostawali na uboczu unijnej legislacji CyberSec.

Mamy kilka nowych sektorów kluczowych, by wymienić choćby sektor ścieków czy dostawców usług zarządzanych. Dodano kilka nowych sektorów istotnych – usługi kurierskie, pocztowe, co ważne, bo wiele ataków socjotechnicznych jest kierowanych na ten sektor.

Warto też zauważyć, że operatorzy usług chmurowych oraz administracja publiczna zostały dodane do zakresu dyrektywy przy naszych staraniach. To nie jest tak, że jesteśmy tylko odbiorcą dyrektywy. Zgłaszaliśmy swój punkt widzenia i potrzeby. Cieszę się więc, że znalazły one ostatecznie odzwierciedlenie w dyrektywie. Administracja publiczna znalazła się w gronie sektorów kluczowych i to w takim wydaniu, gdzie objęcie NIS2 będzie pomocą, a nie kolejnym obciążeniem.

Na czym polega uwzględnienie polskich postulatów w NIS2?

Administracja obejmuje samorządy i instytucje centralne. One współpracują, są współzależne, ale pozostają autonomiczne w dużej mierze. Natomiast NIS2 zakłada, że podlegać będą tym samym wymogom. Upraszczając, ad-

ministracja stanie się sektorem ze wspólnym standardem. Nie jedyni to postulowaliśmy. Ale sygnalizowaliśmy te zapisy jako potrzebne do podnoszenia ogólnego poziomu cyberbezpieczeństwa. Zapis harmonizuje się z naszą narodową strategią cyberbezpieczeństwa. Dowodzi to, że nie jesteśmy zdani wyłącznie na propozycje innych państw.

Włączenie administracji samorządowej i centralnej jest pewną gwarancją, że rozwój CyberSec będzie się dokonywał spójnie. Na ile był to dotąd problem?

Mamy wiele sygnałów z konferencji, że np. zmiany, które chcieliby wprowadzać decydenci cyberbezpieczeństwa w samorządach, znajdują zrozumienie, ale muszą przechodzić dość żmudną ścieżkę akceptacji. Nie zawsze też z powodzeniem te postulaty są realizowane, choćby zgoda na dodatkowe finansowanie.

Łatwiej to uzyskać, kiedy przesłanką dodatkową jest wprost sformułowane „prawnie oczekiwane". Administracja publiczna jest ważnym elementem funkcjonowania państwa i także potrzebuje jasno sformułowanego zestawu wymagań. Można powiedzieć, że przecież mamy np. standardy Krajowych Ram Interoperacyjności (KRI), tylko że dążymy do tego, aby wszystkie rzeczy związane z cyberbezpieczeństwem płynęły z jednego aktu.

Dlatego jeśli mamy Ustawę o Krajowym Systemie Cyberbezpieczeństwa, to implementacja NIS2 odbędzie się poprzez kolejną nowelizację tej ustawy.

Czeka nas zatem nowela noweli Ustawy o KSC?

Mamy już rozpoczęty proces i wypatrujemy jego końca. Cofnięcie nowelizacji do ponownego zaprojektowania, uwzględniając NIS2, nie byłoby dobrym rozwiązaniem. Znaczna część wymagań zawartych w NIS2 znajduje się już w nowej wersji KSC. Są w naturalny sposób częścią strategii rozwoju cyberbezpieczeństwa realizowanych przez podmioty na rynku czy w administracji. Dzięki temu możemy mówić o ewolucji, a nie rewolucji.

Wdrożenie NIS2 z punktu widzenia podmiotów i instytucji nie powinno być wielkim zrywem, ale etapem zaplanowanego continuum. Nowela jako instrument prawny ma jednak ograniczoną pojemność. Dlatego pragniemy uchwalenia obecnej nowelizacji, a w kolejnym kroku NIS2. Bezpośrednio po jej uchwaleniu, rozpocznie się nowy proces legislacyjny, który wprowadzi pozostałe, nieuwzględnione elementy oraz zmiany wynikające z NIS2.

Należy więc w latach 2023–2024 spodziewać się legislacyjnego miniserialu o cyberbezpieczeństwie.

> Pod parasolem dyrektywy NIS2 znajdzie się znacznie więcej podmiotów. Przykładowo w sektorze infrastruktury cyfrowej zostaną ujęci operatorzy chmury obliczeniowej, a także operatorzy telekomunikacyjni, którzy dotąd pozostawali na uboczu unijnej legislacji CyberSec.

Mamy wyznaczony termin wprowadzenia dyrektywy NIS2 do systemu prawnego. Jest to koniec 2024 roku. To iteracyjne podejście, o którym mówię, jest z punktu widzenia prawnej logistyki najszybszym i najpewniejszym sposobem sprostania temu kalendarzowi.

Robimy co możemy, ale nadal jest kilka elementów, które wymagają wyjaśnienia. Dlatego nie wyszliśmy z nowelizacją KSC poza poziom Stałego Komitetu Rady Ministrów. Z punktu widzenia Departamentu Cyberbezpieczeństwa KPRM, dążymy do zakończenia tematu obecnej noweli i następnie rozpoczęcia procesu nowelizacji związanego z NIS2. Robimy to również z myślą o wdrożeniu wymogów przez firmy w Polsce.

Poziom unijny – a więc kształt dyrektywy NIS2 – utwierdza nas w przekonaniu, że planując zmiany w KSC, szliśmy właściwą drogą. Przykład stanowią testy bezpieczeństwa czy dodanie przedsiębiorców komunikacji elektronicznej do KSC. Odpowiednie zapisy znajdują się i w obecnej noweli, i w NIS2.

Na ile wyzwaniem jest czas. Nie pytam o wyznaczony termin, ale pragmatyczną potrzebę polskiej gospodarki, polskiego państwa. Jak pilnie potrzebujemy tego podniesienia poziomu bezpieczeństwa, jaki zapowiada NIS2?

Jest kilka kluczowych terminów w kalendarzu implementacji NIS2. Pierwszy to 21 miesięcy od przyjęcia dyrektywy. Termin ten upływa 17 października 2024 roku. Wydawałoby się dużo czasu, ale doświadczenia z obecną nowelą każą uznawać to za termin niedługi. Oczywiście im szybciej to zrobimy, tym lepiej. Z naszego punktu widzenia każda chwila ma znaczenie dla jakości i bezpieczeństwa.

> Znaczna część wymagań zawartych w NIS2 znajduje się już w nowej wersji KSC. Są w naturalny sposób częścią strategii rozwoju cyberbezpieczeństwa realizowanych przez podmioty na rynku czy w administracji. Dzięki temu możemy mówić o ewolucji, a nie rewolucji.

Czy uda się zatem wdrożyć NIS2 szybciej?

Trudno powiedzieć, bo legislacja to gra zespołowa. Możemy przyjąć, że ze swojej strony jak najszybciej przełożymy zapisy dyrektywy na projekt prawa do procedowania. Ale musimy uwzględnić obecną nowelizację KSC, której ostateczny kształt będzie pewny dopiero w momencie uchwalenia ustawy.

Drugi istotny element to rok wyborczy. Będziemy jesienią mieli nowy rząd. Pewne procesy legislacyjne będą musiały ruszyć od nowa. Patrząc zatem realnie, październik 2024 roku to termin do osiągnięcia i zarazem najbardziej prawdopodobny.

Jak przedstawia się w tym kontekście kwestia gotowości polskich firm do wdrożenia NIS2?

Nowelizacja przyniesie poszerzenie listy sektorów i podmiotów objętych NIS2. Ta wiedza już jest. Konsultacje z firmami objętymi NIS2 po nowelizacji będą bardzo potrzebne. Otwartość administracji publicznej w tej komunikacji będzie istotna. Jest ona niezbędna, tak jak niezbędny jest proces konsultacji, a częściowo edukacji podmiotów i sektorów.

Te konsultacje mają także charakter w pewnym sensie negocjacji, bo chcemy uwzględnić opinie, obserwacje, ale i postulaty, potrzeby dotyczące wdrażania. Firmy nie działają w próżni, wdrożenie NIS2 nie odbywa się bez kontekstu ich sytuacji biznesowej, rynkowej. Jesteśmy otwarci na uzyskanie kompromisu pozwalającego stworzyć zapisy, które będą żywe i działające.

Jaki feedback, w jakich obszarach Departament chciałby uzyskać? Co chce zdiagnozować, jeśli chodzi o świadomość, propozycje, sugestie?

Najbardziej interesuje nas ocena, na podstawie tego, co zapisane jest w dyrektywie, jakim wyzwaniem będzie adaptacja. Bardzo wartościowe będzie oszacowanie niezbędnego nakładu pracy, kosztu. To będzie potrzebne sektorowo, ale też indywidualnie.

Oczywiście im większe przedsiębiorstwo, tym poziom cyberbezpieczeństwa wyższy – tyle mówią dane GUS. Są pewne działy gospodarki, gdzie – bez względu na wielkość – podmiot będzie podlegał przepisom wynikającym z dyrektywy. To stwarza trudność w oszacowaniu, a co za tym idzie – w określeniu, jakimi środkami moglibyśmy wesprzeć tę transformację cyberbezpieczeństwa.

Jakimi środkami wsparcia może dysponować administracja centralna, w szczególności odpowiedzialny za implementację Departament Cyberbezpieczeństwa?

Dane z GUS, dane z programów, jak np. Cyfrowa Gmina, mających komponent bezpieczeństwa – nadal to wycinek, a ponadto deklaratywna wiedza. Doświadczenie uczy, że to nie-

koniecznie wprost oddaje rzeczywistość. Ostatnio w bardzo roboczych kontaktach usłyszałem, że ankiety tego typu to w przypadku cyberbezpieczeństwa 30–40% rzeczywistego stanu potrzeb czy dojrzałości. Ta relacja dotyczy szczególnie faktycznego poziomu w firmach bez styku z rynkiem ICT.

Zapisy w NIS2 to bardziej przełożenie doświadczenia i dobrych praktyk na horyzontalny wymiar. Upowszechnienie bezpieczeństwa na poziomie, który jest już stosowany, nie jest czymś nadmiernie złożonym, trudnym. Zawiera przy tym premię dla konsekwentnych, działających nie od wczoraj w zakresie cyberbezpieczeństwa firm. Podmiot zakwalifikowany przez dyrektywę powinien już dzisiaj indywidualnie szacować nakłady na tę zmianę.

Niestety, to będzie wymagało bardzo indywidualnej oceny. Trudno więc mówić o uniwersalnych narzędziach, jakimi moglibyśmy wspierać tę transformację.

Może jednak pomysły dotyczące ogólnej analizy wysiłku kapitałowego, organizacyjnego, kompetencyjnego byłyby potrzebne? O ile Departament Cyberbezpieczeństwa KPRM chciałby być przewodnikiem w tej transformacji… Dopytuję, ponieważ NIS2 jawi się jako świetny pretekst do ucywilizowania kwestii cyberbezpieczeństwa, podsunięcia nie tyle trwałych standardów, ile dynamicznych ram postępowania, procesu stałej optymalizacji architektury, sposobu postępowania w obszarze cyberbezpieczeństwa. To rodzaj długofalowej inwestycji w bezpieczną gospodarkę cyfrową. Kto miałby wziąć odpowiedzialność za poprowadzenie tej zmiany?

Oczywiście nie satysfakcjonuje nas sam fakt przeprowadzenia procesu legislacyjnego. Obecna ustawa jest w odpowiedzialności mojego Departamentu jako akt, za który merytorycznie odpowiadamy. Trudno byłoby mi się odciąć od NIS2 w wymiarze praktycznym. Naturalną komórką, od której każdy będzie oczekiwał odpowiedzi na pytania nie tylko „co", ale i „jak" wdrożyć, będzie właśnie Departament Cyberbezpieczeństwa KPRM.

Doświadczenia z obecnie obowiązującej ustawy, pierwszej implementacji NIS zostały przeanalizowane. Przy okazji obecnej nowelizacji KSC zbieraliśmy je także w toku spotkań roboczych z firmami, przedstawiając propozycje i pytając, jak mogą wpłynąć na ich biznes. Przypada nam również rola koordynująca na poziomie krajowym w przypadku NIS2 i nie chcemy się od niej uchylać. Jest pewna różnica semantyczna pomiędzy koordynatorem a przewodnikiem, ale zakładamy aktywność.

W pewnej mierze będzie to wynikało z efektów naszego procesu konsultacji, negocjacji, o którym wspominałem. Jeśli wyniknie potrzeba sformułowania np. jakiś ogólnych,

> Mamy wyznaczony termin wprowadzenia dyrektywy NIS2 do systemu prawnego. Jest to koniec 2024 roku. To iteracyjne podejście, o którym mówię, jest z punktu widzenia prawnej logistyki najszybszym i najpewniejszym sposobem sprostania temu kalendarzowi.

gotowych playbooków, najbardziej popularnych scenariuszy wdrożenia NIS2 – to mamy kompetencje i zasoby, aby je wytworzyć i upowszechniać.

Mamy taki pomysł, tylko nie będziemy go realizować bez jasno zdiagnozowanego zapotrzebowania. Nie wykluczamy, że ono właśnie się zwerbalizuje w procesie negocjacji i konsultacji z sektorami. Baza wiedzy zawiera już takie elementy, być może powstanie w jej ramach kontener poświęcony praktycznym aspektom wdrażania NIS2.

Na pewno nie będziemy koordynatorem, który rozdziela pracę, wydaje komunikaty dla prasy i czeka, aż wszystko samo się wydarzy.

Być może także doświadczenie modelu aktywności przy wprowadzaniu RODO byłoby cenne. To doświadczenie sprzed kilku lat, ale mocno związane z komunikacją. Czy dziś taki starter-pack komunikacyjny dla NIS2 również mógłby powstać? Jak np. Departament komunikowałby NIS2 przez pryzmat wartości, korzyści biznesowych z wdrożenia?

Bardzo ogólnie, poprzez podniesienie cyberbezpieczeństwa w podmiotach, „wycięcie" całych klas podatności i zagrożeń w obszarze cyberbezpieczeństwa, które dzisiaj są jeszcze powszechne. To będzie jak melioracja największych bagien cyberbezpieczeństwa.

Oczywisty argument, czy może prosta zachęta do aktywności: NIS2 daje bezwzględny argument w dyskusji z gremiami decydującymi o inwestycjach w firmie. To już nie jest zabawa, nawet jeśli nie każdy musi zrozumieć zagrożenia, to bardzo łatwo zrozumie wagę sankcji, jakie wynikają z niedostosowania do NIS2.

CSO i CIO powinni być zadowoleni z tej sytuacji, ale muszą uruchomić temat i starać się dobrze go ukierunkować. W przytoczonym przypadku RODO zbyt wiele było ponadmiarowych działań, wydatków, podjętych środków. Wymienione osoby mogą zaprojektować to inteligentnie, skutecznie, efektywnie kosztowo.

Trudniejsze, ale wcale nie bez szans jest wprowadzenie na firmowe forum argumentu utraconych korzyści z tytułu niemożności realizacji pewnych procesów, produktów cyfrowych bez zapewnienia bezpieczeństwa. Standardy NIS2 pozwolą wejść do ligi firm dostarczających cyfrowe usługi i produkty na pełnoprawnych warunkach – bezpiecznie, przy zminimalizowanym ryzyku.

Przypomnienie działających na wyobraźnię przykładów złamania zabezpieczeń to zawsze był wdzięczny sposób do poruszenia sumień i serc decydentów. Szczególnie dobrze przemawiają przykłady ransomware. Ich ofiary biznes może znać już bezpośrednio, a na pewno słyszał o tym z drugiej ręki.

Wdrożenie NIS2 w obszarze chociażby właściwych standardów i praktyk kopii zapasowych to zagrożenie niweluje. Mamy dobry timing, aby „strasząc" zarząd wizją ransomware, CSO i CIO pokazywał od razu dobre i usankcjonowane zapisami NIS2 rozwiązanie. Coraz więcej zarządów przyjmuje kryterium ciągłości działania i odporności biznesu za swoją odpowiedzialność, także usankcjonowaną prawnie.

Siła przebicia CSO i CIO zdecydowanie wzrasta. NIS zrobił w 2016 roku w tej mierze dużo, ale zabrakło mu elementu sankcji finansowej. RODO od początku było komunikowane w połączeniu lub przez pryzmat możliwych kar. Było to zresztą demonizowane, bo widzimy dziś przecież, że firmy nie upadają masowo przez te kary, ale w owym czasie spełniło swoją rolę. NIS2 również ma ten wyraźnie sformułowany element kar i zasad ich stosowania. Kary będą miały odstraszający charakter.

> Są pewne działy gospodarki, gdzie bez względu na wielkość podmiot będzie podlegał przepisom wynikającym z NIS2. To stwarza trudność w oszacowaniu, a co za tym idzie w określeniu, jakimi środkami moglibyśmy wesprzeć tę transformację cyberbezpieczeństwa.

Mimo że NIS wchodził w cieniu RODO, to NIS2 zdecydowanie wchodzi w pełnym słońcu. Skoro nie zadziałała siła argumentów, musi zadziałać argument siły. Najwyraźniej do takich wniosków doszli legislatorzy unijni. Osobiście wolałbym jednak, aby do NIS2 udało nam się przekonywać zdroworozsądkowo, poprzez edukowanie i pokazywanie korzyści.

Widać więc, że NIS2 przyniesie wielkie wyzwania komunikacyjne.

Wiele zależeć będzie od właściwego, wspólnego słownika pojęć. Jeśli dobrze i jednakowo będziemy te kwestie rozumieć, łatwiej uzyskamy kompromis. Druga kwestia to transparentność, która niejedno ma imię: dwustronnie administracja – rynek, także w odniesieniu do klientów. Para tych założeń musi znaleźć zastosowanie przy wdrażaniu NIS2.

Zapytam na koniec o wątek korzyści, które niesie uzyskanie wspólnego, europejskiego mianownika współpracy. Jak wygląda gotowość do współpracy w szerszym kontekście nowej organizacji międzynarodowej – European Cyber Crisis Liason Organisation Network EU CYCLONE. Jej obowiązek nakłada NIS2? Czemu ta współpraca ma służyć?

EU CYCLONE już funkcjonuje. To przykład, że NIS2 jako dokument nie tyle tworzy i mnoży nowe byty, ile sankcjonuje, nadaje charakter horyzontalny istniejącym inicjatywom. Obecnie z ramienia Polski do EU CYCLONE delegowanych jest 5 osób – 3 osoby na poziomie operacyjnym i 2 na poziomie zarządczym, mam zaszczyt być jedną z nich.

EU CYCLONE łączy poziom techniczny, sieć CSIRT's Network z poziomem politycznym, decyzyjnym. Ulepszanie dokonuje się cały czas. Te struktury biorą stały udział w ćwiczeniach, jak Cyber Europe, ukierunkowanych na sektor zdrowia. To pozwoliło sprawdzić, jak standardowe struktury operacyjne powinny na poziomie europejskim wyglądać.

Grupa EU CYCLONE – wymieniająca informacje techniczne o incydentach na poziomie ośrodków CSIRT – musi też wpływać na działanie polityczne, reakcję na zdarzenia. Grupa uczestniczy w spotkaniach Komisji, ENISY, wszystkich gremiów związanych z polityką bezpieczeństwa. Uczestniczyła również w pracach nad NIS2. A NIS namaściło CYCLONE na strukturę operacyjną. Efekt, to nadanie jej rzeczywistej sprawczości, zdolności skalowania i szybkość działania w odniesieniu do zagrożeń.

Wywiad przeprowadził
Szymon Augustyniak

Deloitte.

Wojciech Cabała,
konsultant, Deloitte Risk Advisory

Bartosz Olszewski,
konsultant, Deloitte Risk Advisory

Marcin Segit,
menedżer, Deloitte Risk Advisory

W stronę automatyzacji cyberbezpieczeństwa

Według raportu State of Cybersecurity 2022 opublikowanego przez ISACA, globalnie 42% firm doświadczyło w 2022 roku wzrostu liczby ataków wymierzonych w ich zasoby informacyjne. Mimo to organizacje są do przyszłości tego obszaru nastawione optymistycznie. Połowa z nich uważa, że nie stanie się celem cyberprzestępców, a 82% jest przekonanych, że firmowe zespoły do spraw cyberbezpieczeństwa zdołają wykryć zagrożenia i właściwie zareagować. Stoi to w kontraście z raportowanymi przez organizacje niedoborami odpowiednio wyszkolonej kadry, która może skutecznie przeciwdziałać atakom.

Firma Symantec podaje z kolei, że codziennie na świecie dochodzi do ok. 2200 cyberataków. Według wspomnianego raportu ISACA, najpowszechniejszymi metodami ataku stosowanymi przez cyberprzestępców w 2022 roku były socjotechniki (13%), zaawansowane trwałe zagrożenia (12%), wykorzystanie luk w niepoprawnej konfiguracji systemów IT (10%), ransomware (10%), ataki na niezałatane systemy informatyczne (9%) oraz Denial of Service (9%). Incydenty trzeba odpowiednio skategoryzować, przeanalizować, obsłużyć i zaraportować. Do tego dochodzą fałszywe trafienia (false positives), które należy oddzielić od rzeczywistych alertów. To wszystko wymaga zasobów, w tym odpowiednio licznego i przeszkolonego personelu.

Niedobór wykwalifikowanej kadry

Raport ISACA wskazuje, że obszar cyberbezpieczeństwa wciąż cierpi na niedobór odpowiednio wyszkolonych pracowników. W niemal 50% przebadanych firm zespoły liczą od zaledwie 2 do 10 pracowników. Oczywiście brak wykwalifikowanego personelu niesie wymierne skutki i firmy borykające się z lukami kadrowymi w obszarze cyberbezpieczeństwa stają się łatwym celem kolejnych ataków.

Spośród przedsiębiorstw biorących udział w badaniu 63% przyznało, że mają problemy z obsadzeniem stanowisk związanych z bezpieczeństwem informacji. Ponadto 60% respondentów wskazało także na problemy z zatrzymaniem wykwalifikowanej kadry w strukturach organizacji. Rynek niestety nie nadąża z uzupełnianiem braków, i to pomimo malejących oczekiwań związanych z wymogami dotyczącymi wykształcenia w zakresie cyberbezpieczeństwa, zwłaszcza w przypadku pozycji juniorskich.

Choć – zdaniem respondentów – poziom kompetencji technicznych rośnie, sfera umiejętności miękkich oraz znajomość zagadnień dotyczących transformacji chmurowej wciąż pozostawiają sporo do życzenia. Odpowiedzią na brak odpowiednich kwalifikacji są szkolenia wewnętrzne

W naszym raporcie 2023 Global Future of Cyber Survey – obejmującym ponad 1000 liderów z 20 krajów – wskazujemy, że „cyber" to coś więcej niż skupienie się na samej technologii – to również podstawa strategii rozwoju organizacji.

oraz zwiększone zaangażowanie zewnętrznych konsultantów. Przy czym chętniej w programy szkoleniowe inwestują firmy cechujące się wysoką dojrzałością w obszarze CyberSec. Robi to 64% z nich, w porównaniu do 50% organizacji o niskiej dojrzałości – wynika z raportu Deloitte 2023 Global Future of Cyber Survey.

Co interesujące, 42% przedsiębiorstw przepytanych przez ISACA uważa, że ich budżety przeznaczone na cyberbezpieczeństwo są odpowiednie, co oznacza wzrost o 5 punktów procentowych względem raportu z 2021 roku. Jest to również najwyższy wynik od czasów pierwszego badania ISACA z 2019 roku. Ponad 50% firm spodziewa się także wzrostu poziomu finansowania. Przy czym o ile 82% respondentów twierdzi, że kierownictwo ich organizacji widzi wartość w przeprowadzaniu ocen ryzyka cyberbezpieczeństwa, o tyle faktyczne coroczne działania w tym zakresie podejmowane są jedynie u 41% ankietowanych.

Automatyzacja cyberbezpieczeństwa

W naszym raporcie 2023 Global Future of Cyber Survey – obejmującym ponad 1000 liderów z 20 krajów – wskazujemy, że „cyber" to coś więcej niż skupienie się na samej technologii – to również podstawa strategii rozwoju organizacji. 91% przedsiębiorstw zgłosiło w 2022 roku co najmniej jeden incydent cyberbezpieczeństwa (to o 3 punkty procentowe więcej względem poprzedniego raportu), do tego aż 56% firm twierdzi, że poniosło związane z tym umiarkowane lub duże konsekwencje.

Wraz ze wzrostem zagrożenia silniej wybrzmiewają argumenty za inwestowaniem w cyberbezpieczeństwo, a sam obszar zaczyna być postrzegany jako jeden z czynników wzrostu. 86% respondentów wskazało, że inicjatywy mające na celu poprawę bezpieczeństwa informacyjnego miały znaczący, pozytywny wkład przynajmniej w jeden z istotnych obszarów biznesowych. Zwiększone nakłady finansowe pozwalają na wprowadzanie nowoczesnych rozwiązań. Dzięki sztucznej inteligencji i automatyzacji organizacje stają przed szansą zredukowania nakładu pracy poświęcanego na żmudne, powtarzalne czynności. Pozwala to także na szkolenie i przenoszenie specjalistów do ról i zadań bardziej strategicznych z punktu widzenia procesu i samej firmy.

Automatyzacja jest również odpowiedzią na braki kadrowe. Oczywiście obsługa systemów IT wymaga odpowiednio przeszkolonych specjalistów, jednak zautomatyzowane wykrywanie i klasyfikacja zdarzeń oraz w niektórych przypadkach także automatyczne ich przetwarzanie pozwalają uzupełnić luki w zasobach. Według raportu Deloitte, użycie zautomatyzowanych narzędzi do analizy zachowań, aby wykrywać i ograniczać wśród pracowników potencjalne ryzyka cyberbezpieczeństwa, deklaruje 76% respondentów – dla porównania, w raporcie z 2021 roku ich użycie zgłosiło tylko 53% badanych. Można się spodziewać, że ten odsetek będzie nadal rósł, gdyż wykorzystanie zautomatyzowanych narzędzi do analizy, wykrywania i ograniczania potencjalnego ryzyka cyberbezpieczeństwa jest już w zasadzie standardem.

Problemem bywa jednak natłok danych pochodzących m.in. z coraz bardziej zaawansowanych skanerów podatności od wiodących dostawców w tym obszarze oraz rozwiązań SIEM (Security Information

60%

firm przyznało, że mają problemy z obsadzeniem stanowisk związanych z bezpieczeństwem informacji. Ponadto 60% respondentów wskazało na problemy z zatrzymaniem wykwalifikowanej kadry w strukturach organizacji.

and Event Management) ułatwiających zarządzanie incydentami bezpieczeństwa. Ograniczona liczba specjalistów nie jest w stanie przetworzyć tych informacji w odpowiednio krótkim czasie.

Aby przyspieszyć procesy i ograniczyć do minimum zaangażowanie analityków, wdrażane są narzędzia typu SOAR (Security Orchestration Automation & Response), które umożliwią zbieranie danych z wielu źródeł informacji, agregowanie ich i następnie przetwarzanie na dostosowane do potrzeb organizacji procesy zarządzania incydentami i podatnościami. Co więcej, zautomatyzowanie części procesów oraz zagregowanie informacji w jednym systemie pozwala analitykom skupić się na meritum wynikającym z napływających alertów, a także skrócić czas potrzebny na reakcję i działania naprawcze.

Korzyści dla biznesu

Jak wynika z raportu 2023 Global Future of Cyber Survey, prawie 70% organizacji o wysokiej dojrzałości w obszarze cyber-

> Według naszego raportu, użycie zautomatyzowanych narzędzi do analizy zachowań, aby wykrywać i ograniczać wśród pracowników potencjalne ryzyka cyberbezpieczeństwa, deklaruje 76% respondentów (53% w roku 2021).

bezpieczeństwa dostrzega wpływ obszaru „cyber" zarówno na zwiększenie zaufania (dla 69% firm High cyber maturity, 57% Medium cyber maturity i 54% Low cyber maturity), jak i na szybsze wykrywanie potencjalnych problemów (odpowiednio: 69%, 53% i 49%).

Respondenci wskazali również pozytywny wpływ inwestycji w cyberbezpieczeństwo na obszary, takie jak poprawa reputacji marki (64%), wzrost przychodów (47%), wzrost operacyjności i stabilności łańcucha dostaw i poddostawców (59%), rekrutacja i zatrzymywanie talentów (49%), długoterminowa stabilność (64%), a także zaufanie klientów i wpływ na pozycję marki (62%).

Potrzeba automatyzacji procesów w organizacjach wciąż wzrasta, dotyczy to również obszaru cyberbezpieczeństwa. Automatyzacja, w tym także rozwiązania oparte na sztucznej inteligencji, może wesprzeć specjalistów w rutynowych i powtarzalnych działaniach. Dzięki temu będą mogli skupić się na bardziej strategicznych i funkcjonalnych zadaniach w ramach firmy, przynajmniej częściowo uwolnieni od zmagań z codziennym natłokiem alertów, incydentów i naruszeń bezpieczeństwa. Inwestycje w cyberbezpieczeństwo stają się również standardem, który w przyszłości będzie czynnikiem decydującym o zaangażowaniu i budowaniu relacji z kontrahentami, odbiorcami usług i indywidualnymi klientami.

NIS2: dyrektywa na czasy transformacji cyfrowej

Dyrektywa NIS2 rozszerza zakres stosowania przepisów dotyczących cyberbezpieczeństwa na nowe sektory gospodarki. Nakłada też – na podmioty kluczowe i ważne – wiele wymagań w zakresie wdrożenia środków zarządzania ryzykiem. Nowe przepisy przewidują także m.in. nową procedurę zgłaszania poważnych incydentów oraz nadają organom nadzorującym kompetencje do wydawania ostrzeżeń, poleceń i nakładania kar na podmioty niewywiązujące się z przepisów wprowadzanych przez dyrektywę.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 roku w sprawie środków na rzecz wysokiego, wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej (NIS2) zmienia rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148. Stanowi więc rewizję przyjętej w 2016 roku dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywy NIS).

Przyjęcie dyrektywy NIS2 jest reakcją unijnego prawodawcy na postępującą transformację cyfrową oraz pojawiające się wyzwania w obszarze cyberbezpieczeństwa. Celem nowych przepisów jest zapewnienie wysokiego poziomu odpowiedzialności za zarządzanie ryzykiem w bezpieczeństwie sieci IT, a także harmonizacja standardów przyjętych w krajach UE.

Jak pokazał przegląd obecnie obowiązującej dyrektywy NIS, w jej implementacji do porządków prawnych poszczególnych krajów nastąpiły istotne rozbieżności, które utrudniały prowadzenie działalności podmiotom oferującym towary lub usługi transgraniczne.

Zakres stosowania dyrektywy NIS2

W ramach rewizji prawodawca unijny rozszerzył zakres stosowania przepisów dotyczących cyberbezpieczeństwa w NIS2 na nowe sektory gospodarki. Przedmiotem regulacji objęte zostały m.in. sektor usług pocztowych i kurierskich, gospodarowania odpadami, produkcji oraz badań naukowych.

Dyrektywa NIS2 rozróżnia podmioty objęte zakresem jej wykorzystania na dwie kategorie – podmioty kluczowe i ważne, względem których stosowane będą różne sposoby nadzoru i egzekwowania przepisów. Jako podmioty kluczowe zakwalifikowane zostały m.in. średnie lub duże przedsiębiorstwa energetyczne, przedsiębiorstwa kolejowe, przewoźnicy lotniczy, instytucje kredytowe oraz dostawcy niektórych usług infrastruktury cyfrowej. Natomiast do kategorii podmiotów ważnych należą przykładowo operatorzy pocztowi, firmy spożywcze bądź niektóre przedsiębiorstwa produkcyjne. Państwa członkowskie UE zostały zobowiązane do ustanowienia wykazu podmiotów kluczowych i ważnych, a także podmiotów świadczących usługi rejestracji nazw domen.

Co do zasady, nowe przepisy znajdują zastosowanie tylko do tych podmiotów kluczowych lub ważnych, które spełniają definicję średniego przedsiębiorstwa lub przekraczają

Dyrektywa NIS2 rozróżnia podmioty objęte zakresem jej stosowania na dwie kategorie:

Podmioty kluczowe – wśród nich zakwalifikowano średnie i duże przedsiębiorstwa energetyczne, kolejowe, przewoźników lotniczych, instytucje kredytowe oraz dostawców niektórych usług infrastruktury cyfrowej.

Podmioty ważne – należą do nich m.in. operatorzy pocztowi, przedsiębiorstwa spożywcze bądź niektóre przedsiębiorstwa produkcyjne.

pułapy dla średnich przedsiębiorstw. Dyrektywa NIS2 przewiduje jednak pewne wyjątki w tym zakresie – niezależnie od wielkości przedsiębiorstwa, regulacja znajdzie zastosowanie m.in. względem kwalifikowanych dostawców usług zaufania, rejestrów nazw domen najwyższego poziomu oraz dostawców usług DNS.

Środki zarządzania ryzykiem w cyberbezpieczeństwie

Dyrektywa NIS2 nakłada na podmioty kluczowe i ważne wiele wymagań w zakresie wdrożenia środków zarządzania ryzykiem. Należą do nich w szczególności, obowiązek wprowadzenia polityki analizy ryzyka i bezpieczeństwa systemów IT, procedur służących ocenie skuteczności wprowadzonych środków, zapewnienie obsługi incydentów bezpieczeństwa oraz ciągłości działania po wystąpieniu sytuacji nadzwyczajnej, a także zarządzania kryzysowego.

W organizacjach objętych zakresem dyrektywy NIS2 należy wdrożyć podstawowe praktyki cyberhigieny, zagwarantować odpowiednie szkolenia, opracować polityki i procedury stosowania kryptografii, politykę kontroli dostępu i zarządzania aktywami. Aby wykazać zgodność z wymogami dyrektywy NIS2, państwa członkowskie mogą zastrzec konieczność stosowania konkretnych produktów, usług i procesów ICT certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa.

Zgłaszanie incydentów naruszenia bezpieczeństwa IT

Nowe przepisy obejmują też sposób zgłaszania incydentów. Aby zapewnić równowagę między szybkim zgłoszeniem, pozwalającym zahamować potencjalne rozprzestrzenianie się zagrożenia, a zgłoszeniem szczegółowym, które umożliwia wyciągnięcie wniosków, dyrektywa NIS2 przewiduje dwuetapową procedurę zgłaszania poważnych incydentów.

Obowiązek zgłaszania incydentów aktualizuje się jedynie w momencie wystąpienia incydentu poważnego. Zgodnie z definicją legalną, zawartą w dyrektywie NIS2, jest to incydent, który spowodował (lub może spowodować) dotkliwe zakłócenia operacyjne lub straty finansowe, bądź też wpłynął (lub jest w stanie wpłynąć) na inne osoby, powodując znaczne szkody majątkowe i niemajątkowe.

W sytuacji jego wystąpienia, zarówno podmioty kluczowe jak i ważne, zobowiązane będą do przedłożenia właściwemu organowi krajowemu tzw. wczesnego ostrzeżenia. Powinno to nastąpić w ciągu 24 godzin od chwili powzięcia wiedzy o danym incydencie. Na zgłoszenie incydentu, wraz ze

wskazaniem jego wstępnej oceny i analizy, podmioty będą miały 72 godziny, liczone od momentu wykrycia incydentu.

Nadzór i sankcje

Zarówno podmioty kluczowe, jak i podmioty ważne, w zakresie spełniania wymogów dyrektywy NIS2, podlegać będą nadzorowi odpowiednich organów krajowych. Organy nadzorujące uprawnione będą w szczególności do stosowania kontroli na miejscu, przeprowadzenia zdalnego nadzoru oraz audytów lub skanów bezpieczeństwa w stosunku do monitorowanych podmiotów.

Co istotne, względem podmiotów ważnych, działania te będą mogły zostać podjęte tylko w przypadku uprzedniego otrzymania przez organ dowodu lub informacji, że dana jednostka narusza przepisy dyrektywy (nadzór ex post). W razie stwierdzenia uchybienia w stosowaniu się do postanowień dyrektywy, nadzorującemu przysługiwać będą względem podmiotu naruszającego określone środki egzekwowania przepisów.

Do kompetencji organu nadzorującego należeć będzie m.in. wydawanie ostrzeżeń w zakresie dokonanych naruszeń, wiążących poleceń, nakazów, a także nałożenie lub zwrócenie się o nałożenie na organizację administracyjnej kary pieniężnej. W stosunku do podmiotu kluczowego, maksymalna wysokość kary pieniężnej przewidziana w przepisach krajowych powinna wynosić co najmniej 10 mln euro (lub 2% łącznego, rocznego światowego obrotu przedsiębiorstwa w poprzednim roku obrotowym), a w stosunku do podmiotu ważnego – 7 mln euro (lub 1,4 % światowego obrotu).

Termin na implementację przepisów dyrektywy NIS2 do ustawodawstw krajów członkowskich mija 17 października 2024 roku.

Znaczenie dyrektywy NIS2

Zagrożeń dla cyberbezpieczeństwa stale przybywa. W 2022 roku do CERT Polska zgłoszono o 176% więcej incydentów niż w roku poprzednim! To potwierdza, że każda organizacja powinna być przygotowana na wystąpienie incydentu cybernetycznego. Ponadto, obecna sytuacja geopolityczna fundamentalnie zmieniła globalny krajobraz cybernetyczny. Taki jest wniosek z raportu Threat Landscape 2022 opublikowanego przez agencję ds. cyberbezpieczeństwa ENISA w październiku 2022 roku.

> Unijny prawodawca rozszerzył zakres stosowania przepisów cyberbezpieczeństwa w NIS2 na nowe sektory gospodarki. Przedmiotem regulacji objęte zostały m.in. sektor usług pocztowych i kurierskich, gospodarowania odpadami, produkcji oraz badań naukowych.

> Aby wykazać zgodność z wymogami dyrektywy NIS2, państwa członkowskie mogą zastrzec konieczność stosowania konkretnych produktów, usług i procesów ICT certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa.

Połączenie stale rosnących zagrożeń cybernetycznych oraz niskiego poziomu dojrzałości w zakresie cyberbezpieczeństwa sektorów dotychczas nieobjętych zakresem podmiotowym dyrektywy NIS tworzy sytuację, w której firmy są bardziej podatne na cyberzagrożenia. Dyrektywa NIS2 ma stanowić odpowiedź na te zagrożenia i wzmocnić poziom cyberbezpieczeństwa oraz cyberodporności w Unii Europejskiej.

Zakres obowiązków nałożonych przez dyrektywę NIS2 uległ zwiększeniu w stosunku do zakresu określonego w dyrektywie NIS. Stanowić to będzie duże wyzwanie zwłaszcza dla podmiotów, które do tej pory nie były objęte dyrektywą NIS.

Ponadto wdrożenie wymogów dyrektywy NIS2 wymagać będzie posiadania wykwalifikowanych specjalistów, co również będzie stanowić wyzwanie wobec faktu, że – jak wynika z raportu firmy (ISC)2 – w Europie brakuje ok. 200 tys. specjalistów ds. cyberbezpieczeństwa. Jednak to, czy wdrożenie dyrektywy NIS2 będzie miało realny wpływ na wzrost poziomu cyberbezpieczeństwa, będzie zależało od dojrzałości podmiotów podlegających regulacji.

Podnoszenie standardów w zakresie cyberbezpieczeństwa oraz zdolności reagowania na różnego rodzaju incydenty powinno leżeć w interesie tych podmiotów, gdyż skuteczne zarządzanie incydentami cybernetycznymi pozwala ograniczyć ryzyko strat finansowych oraz utraty reputacji, jakie mogą być skutkiem wystąpienia incydentu.

Karolina Kulikowska,
Senior Associate w kancelarii DZP

Martyna Gruszka,
Associate w kancelarii DZP

Rynek cyberbezpieczeństwa z solidnymi prognozami wzrostu

Sukcesywnie rosną wydatki firm w Polsce na cyberbezpieczeństwo. W tym roku mają wzrosnąć o ponad 13%, do 2,4 mld zł. Stopniowo wzrasta też świadomość i nacisk na zabezpieczenie przede wszystkim danych przetwarzanych w przedsiębiorstwach. Konieczność ich zabezpieczenia akcentują coraz mocniej firmy przemysłowe.

W ostatnim czasie wzrasta znaczenie cyberbezpieczeństwa, co jest wynikiem postępującej digitalizacji kanałów komunikacji, dotarcia do klienta i postępującej transformacji cyfrowej. Ta ostatnia przynosi korzyści, zarówno dla przedsiębiorców, jak i dla konsumentów. Jednakże wraz z przenoszeniem coraz większej ilości zasobów do cyberprzestrzeni, wzrasta również ich ekspozycja na cyberataki.

Cyberprzestępcy korzystają z coraz bardziej kreatywnych sposobów łamania zabezpieczeń, sabotażu i wykradania danych przedsiębiorstw oraz użytkowników internetu. Bezpieczeństwo IT zyskało w ostatnich latach szczególnie na znaczeniu, najpierw za sprawą pandemii COVID-19, a obecnie na skutek wojny w Ukrainie. Co więcej, cyberwojna zasięgiem wykracza poza strony bezpośrednio zaangażowane w konflikt.

Coraz więcej ataków ransomware

Najnowsze badania PMR pokazują, że firmy w Polsce, podobnie zresztą do trendów widocznych globalnie, sygnalizują zwiększoną aktywność cyberprzestępców i wzrost liczby ataków ransomware. Co ciekawe, problem ten, który dotyczył dotąd głównie dużych podmiotów, coraz częściej obserwują firmy średnie.

Wartość (w mld zł) oraz dynamika (w %) rynku cyberbezpieczeństwa w Polsce, 2018–2024

	2018	2019	2020	2021	2022	2023p	2024p
Wartość	1,14	1,56	1,65	1,84	2,12	2,40	2,70
Dynamika	15,4	11,3	6,2	11,7	15,3	13,1	12,4

p – prognoza
Źródło: PMR, 2023 r.

Paradoksalnie im większy stopień digitalizacji zasobów i znaczenie danych i baz wykorzystywanych w firmach, tym większa ekspozycja na ryzyko. W porównaniu z sytuacją sprzed 2 lat, odsetek przedsiębiorstw doświadczających zagrożeń związanych z zaszyfrowaniem danych wzrósł w Polsce ponad 2-krotnie. Rośnie też niestety skuteczność takich ataków, choć firmy wypowiadają się na ten temat ostrożnie, niechętnie ujawniając fakt, że dane udało się skutecznie zaszyfrować.

Najpopularniejszą metodą odzyskania danych utraconych przez ransomware jest backup, który stosuje ponad 80% firm. Część organizacji zwraca uwagę, że musiały zrewidować dotychczasową politykę w tym zakresie. Problemem nie były ograniczenia budżetowe, ale stosowane podstawowe metody backupu, które nie dawały gwarancji odzyskania danych po zaszyfrowaniu firmy. W efekcie, coraz więcej przedsiębiorstw używa jednocześnie kilku metod odzyskania danych, w tym backupu w chmurze. Archiwizuje też dane cyklicznie w zewnętrznej lokalizacji, aby w sytuacji kryzysowej jak najszybciej przywrócić firmę do działania.

Jeśli chodzi o obawy związane z ransomware, przedsiębiorstwa najbardziej boją się utraty reputacji oraz wycieku danych mogących zaszkodzić ich klientom lub naruszyć zapisy RODO. Utrata zaufania klientów może doprowadzić do ich odpływu na rzecz konkurencji, co bezpośrednio przyczynia się do pogorszenia sytuacji przedsiębiorstwa na rynku.

Nacisk na zabezpieczenie danych

Historycznie firmy skupiały się najmocniej na zabezpieczeniu firmowej infrastruktury, serwerów i aplikacji. Obecnie priorytetem są dane i ich zabezpieczenie. Jest to trend widoczny zarówno w dużych, jak i średnich firmach. Jedne i drugie zdają sobie sprawę z rosnącego zagrożenia cyberprzestępczością i inwestują w zabezpieczenia i cyberbezpieczeństwo, jednakże duże firmy są bardziej skłonne do inwestycji w najnowsze technologie, które zapewnią im najlepszą ochronę.

Średnie przedsiębiorstwa inwestują w te obszary, które są kluczowe dla ich biznesu i dostępne w ich budżecie. W przypadku dużych – większe znaczenie na liście priorytetów w porównaniu ze średnimi ma niemalże każdy obszar. Duże przedsiębiorstwa wyżej na liście priorytetów stawiają też m.in. zabezpieczenie środowisk chmurowych, co wynika z wyższego nasycenia takimi rozwiązaniami.

Z badań PMR wynika, że najmocniej kwestię konieczności zabezpieczenia danych i doinwestowania tego obszaru akcentują duże firmy przemysłowe. Aż 65–70% z nich (w zależności od rodzaju przemysłu) wskazało ten obszar jako absolutnie priorytetowy i wymagający inwestycji związanych z cyberbezpieczeństwem. Jednym z powodów może być fakt, że w przemyśle funkcjonują systemy o wysokim stopniu złożoności i wrażliwości, które są ściśle powiązane z procesami produkcyjnymi. Dlatego utrata danych, w tym informacji o procesach produkcyjnych, może mieć poważne konsekwencje finansowe i operacyjne dla przedsiębiorstw.

Plany wydatków na cyberbezpieczeństwo w przedsiębiorstwach w Polsce z podziałem na obszary zabezpieczeń, 2023 r.

	Ogółem	Średnie firmy (50-249 pracowników)	Duże firmy (250+ pracowników)
Dane firmowe	7,6	7,6	8,2
Serwery i infrastruktura IT	7,6	7,6	8,0
Sieć	7,3	7,3	7,9
Systemy i aplikacje	7,2	7,2	7,6
Urządzenia końcowe – desktopy i laptopy	5,9	5,9	6,0
Środowiska chmurowe	5,8	5,7	6,4
Urządzenia końcowe – smartfony	5,4	5,6	5,2

n = 598
Ocena na skali od 1 do 10, gdzie 1 oznacza „W ogóle nie zamierzamy inwestować w ten obszar" do 10 oznaczającego „Zdecydowanie zamierzamy inwestować w ten obszar".
Źródło: PMR, 2023 r.

Odsetek (w %) przedsiębiorstw w Polsce wskazujących na plany inwestycyjne związane z zabezpieczeniem przetwarzanych danych, z podziałem na wielkość firm i główne branże, 2023 r.

	Ocena od 1 do 4	Ocena od 5 do 7	Ocena od 8 do 10
Ogółem	5	40	55
50–249 pracowników	5	41	53
250+ pracowników	6	26	68
Przychody 100 do 250 mln zł	6	40	54
Przychody od 250 mln zł	3	26	71
Produkcja maszyn i urządzeń	2	27	71
Przemysł spożywczy/FMCG	8	27	65
Transport, spedycja i logistyka	5	38	57
Budownictwo	7	42	51
Banki, finanse, ubezpieczenia	5	45	51
Utilities	7	43	50
Telekomunikacja i media	3	48	49
Handel detaliczny i hurtowy	4	49	47

n = 598
Ocena na skali od 1 do 10, gdzie 1 oznacza „W ogóle nie zamierzamy inwestować w ten obszar" do 10 oznaczającego „Zdecydowanie zamierzamy inwestować w ten obszar".
Źródło: PMR, 2023 r.

Kolejny aspekt to wzrost liczby ataków na firmy przemysłowe. Zabezpieczenie danych i zapewnienie wysokiego poziomu bezpieczeństwa może też być ważnym elementem strategii konkurencyjnej przedsiębiorstwa.

Wartość rynku i dwucyfrowy wzrost wydatków

Według prognoz PMR z I kwartału 2023 roku, wartość rynku cyberbezpieczeństwa w Polsce w latach 2023–2024 będzie rosła średniorocznie o ponad 12%, do 2,7 mld zł w roku przyszłym. Rynek ten definiujemy wąsko jako urządzenia zabezpieczające firmową sieć (głównie UTM i NGFW), rozwiązania aplikacyjne (od najbardziej podstawowych antywirusów po m.in. firewalle, antyspam/spyware, systemy IDS/IPS, DLP, anty-ATP, anty-DDoS, do kompleksowych systemów SIEM) oraz usługi (audyt, pentesty, doradztwo, SOC itp.).

Możliwa jest również szersza definicja obejmująca cały ekosystem, w tym przede wszystkim rynek rozwiązań chmurowych. Badania PMR potwierdzają, że w opinii odbiorców jedną z najważniejszych zalet chmury jest właśnie poprawa bezpieczeństwa przedsiębiorstwa w zakresie przetwarzanych danych. Migracja do chmury to element strategii w obszarze cyberbezpieczeństwa. Podobnie jest w przypadku usług backupu i data center, których głównym zadaniem jest właśnie bezpieczeństwo i ochrona przed utratą danych.

Gdyby do wartości rynku cyberbezpieczeństwa dodać chmurę obliczeniową, rynek usług data center, backup, hosting oraz inne obszary, takie jak zapewnienie bezpieczeństwa fizycznego, zasilanie awaryjne i informatykę śledczą, możemy już mówić o skali wyraźnie ponad 10 mld zł.

Paweł Olszynka,
dyrektor Działu Analiz Rynku ICT w firmie PMR

W tekście wykorzystano dane: z raportu PMR „Rynek cyberbezpieczeństwa w Polsce 2022. Analiza rynku i prognozy rozwoju na lata 2023–2027" **(bit.ly/3nw44g3)**, a także z najnowszej fali badania przedsiębiorstw zrealizowanego przez PMR w dniach 2–27 stycznia 2023 roku z użyciem techniki wywiadu telefonicznego wspomaganego komputerowo (CATI). PMR przeprowadził badanie na próbie 600 firm (MŚP i duże firmy). W badaniu uwzględniono populację firm na podstawie PKD głównego. Przedmiotem badania były zagadnienia z zakresu cyfrowej transformacji, cyberbezpieczeństwa, rozwiązań chmurowych i data center.

Microsoft

Na CYBERBEZPIECZEŃSTWO nie da się patrzeć wycinkowo

Z **Krzysztofem Malesą,** dyrektorem ds. strategii bezpieczeństwa w polskim oddziale Microsoft, rozmawiamy o niezbędnych zmianach w podejściu do CyberSec, koncepcji bezpieczeństwa opartego na analizie ryzyka i zerowym zaufaniu, roli cyberbezpieczeństwa w zapewnieniu ciągłości biznesu, a także o najważniejszych założeniach dyrektywy NIS2.

Jakich zmian w podejściu do cyberbezpieczeństwa wymagają dzisiejsze realia geopolityczne?

Rzeczywistość pokazuje, że na cyberbezpieczeństwo nie da się patrzeć wycinkowo. Nie ma sensu w tym skomplikowanym łańcuchu procesów, który nas otacza, skupiać się na zabezpieczaniu pojedynczych elementów. W przeszłości zależności gospodarcze były dużo prostsze. Dziś, współzależności pomiędzy systemami, które komunikują się wzajemnie bez udziału człowieka, są tak duże, że awaria w jednym miejscu może wywołać nieoczekiwany skutek w innym. Nie ma czegoś takiego jak liniowe, proste łańcuchy dostaw, które można chronić mechanicznie. Trzeba uruchomić wyobraźnię i przeprowadzić kompleksową analizę ryzyka. Takie podejście jest fundamentem dyrektywy NIS2.

> Nowe dyrektywy stawiają na myślenie. W NIS2 i CER wprost opisane jest podejście oparte na analizie ryzyka. Jest to o tyle istotne, że w bezpieczeństwo nie należy inwestować za wszelką cenę, bo to nie cyberbezpieczeństwo jest celem funkcjonowania większości organizacji.

Dlaczego potrzebna była zmiana zasad, które do tej pory obowiązywały podmioty związane z usługami lub infrastrukturą krytyczną?

Ponieważ od momentu opracowania obowiązujących dotychczas przepisów realia gospodarcze, geopolityczne, a także te związane wprost z cyberbezpieczeństwem zmieniły się w ogromnym stopniu. Pamiętajmy, że dyrektywa NIS2 zastępuje poprzedniczkę z 2016 roku. Przez tak długi czas podejście do bezpieczeństwa zmieniło się kompletnie, bo zmienił się modus operandi atakujących. Zwiększyła się również skala zjawiska ataków typu APT czy kampanii sponsorowanych przez wrogie państwa. To ataki, do których całe sztaby ludzi przygotowują się miesiącami po to, aby niezauważenie wejść do środowiska IT konkretnej organizacji i plądrować ją lub szpiegować całymi tygodniami. Są to zagrożenia, których na taką skalę wcześniej nie było.

Stąd też koncepcja bezpieczeństwa opartego na zerowym zaufaniu…

To prawda. Zagrożenia, z którymi mamy dziś do czynienia pokazują, że zgodnie z modelem zero-trust nie ma co przerzucać wszystkich sił na pilnowanie drzwi wejściowych. Zamiast tego trzeba chronić zasoby oraz tożsamość użytkowników, danych, aplikacji, urządzeń, sieci i infrastruktury. Jeśli chcemy chronić tożsamość, to mamy cały pakiet możliwości, który kryje się pod hasłem, takim jak dostęp warunkowy. Takie podejście pozwala nie tylko na proste sprawdzenie uprawnień, ale umożliwia też bieżącą ocenę ryzyka wynikającą z historii każdego użytkownika. Z tego, czy do tej pory zachowywał się odpowiedzialnie, jakie ma kwalifikacje, z jakich rozwiązań korzysta.

Po drugie, podejście zerowego zaufania zakłada, że dajemy użytkownikom dostęp jedynie do tych zasobów, które są im niezbędne do wykonywania pracy. To jedna z koronnych zasad nowoczesnego podejścia do bezpieczeństwa. Poza tym model zero-trust mówi, że dziś najistotniejsza nie jest kwestia zamknięcia drzwi przed intruzami, tylko uniemożliwienie im wykonywania szkodliwych ruchów po tym, jak już dostaną się do wnętrza organizacji. Ogromne możliwości w tym kontekście zapewnia dziś AI.

W jaki sposób sztuczna inteligencja może wspierać inicjatywy na rzecz zapewnienia bezpieczeństwa firmy w obszarze IT?

Skuteczne zabezpieczenia, które nie przeszkadzają użytkownikom

Oferowane przez Microsoft rozwiązania dysponują wieloma działającymi w sposób natywny mechanizmami z obszaru cyberbezpieczeństwa. Pozwalają m.in. na zapewnienie:

- **Kompleksowej klasyfikacji i ochrony danych wrażliwych** – rozwiązanie Microsoft Purview Information Protection pełni rolę pojedynczego narzędzia klasyfikacji danych w aplikacjach, usługach oraz urządzeniach, jak również rozwiązania zapewniającego ich ochronę m.in. podczas przesyłania wewnątrz organizacji i poza jej granicami. Wspiera szyfrowanie oraz tagowanie treści. Microsoft Purview Information Protection zapewnia ochronę dla zasobów lokalnych, które używają serwera Exchange lub SharePoint, lub serwerów plików, a także chroni treść przetwarzaną w aplikacjach Microsoft Office na różnych platformach i urządzeniach. Wspierane są m.in. Word, Excel, PowerPoint i Outlook oraz aplikacje zewnętrznych dostawców.
- **Bezpiecznego dostępu do wewnętrznych aplikacji bez potrzeby konfigurowania łączy VPN** – dostępna w ramach platformy chmurowej Microsoft Azure usługa Azure AD Application Proxy pozwala na zastosowanie bezpiecznego uwierzytelnienia Azure AD, wraz z MFA dla aplikacji obsługujących starsze standardy uwierzytelniania. Zapewnia też możliwość łatwiejszego sterowania ruchem sieciowym, niż jest to możliwe w przypadku wykorzystania innych rozwiązań.
- **Monitoringu mechanizmów tożsamości hybrydowej** – usługa Microsoft Azure AD Connect Health pomaga monitorować oraz uzyskiwać informacje o lokalnej infrastrukturze do obsługi tożsamości i w ten sposób wspiera uzyskanie niezawodności środowiska. Monitoring może obejmować zarówno kontrolery domeny Active Directory, systemy ADFS, jak i serwery synchronizacji Azure AD Connect. Wykorzystanie tej usługi wymaga jedynie zainstalowania agenta na każdym z lokalnych serwerów tożsamości.
- **Zarządzania urządzeniami końcowymi i ochrony danych w myśl koncepcji „zero-trust”** – rozwiązania dostępne w ramach grupy produktów Microsoft Intune gwarantują ujednolicone mechanizmy zarządzania urządzeniami końcowymi działającymi na różnych systemach operacyjnych, w tym: Windows, MacOS, Android, iOS oraz Linux, także urządzeń zwirtualizowanych. Microsoft Intune zapewnia również mechanizmy ochrony firmowych danych w sposób niewymagający ingerencji w konfigurację urządzeń końcowych, co ma znaczenie w przypadku wykorzystania prywatnego sprzętu pracowników. Rozwiązania tej grupy w sposób natywny wspierają też budowanie środowiska bezpieczeństwa w modelu tzw. zerowego zaufania. Dostępna w ramach Microsoft Intune konsola Endpoint Security pozwala na scentralizowane i spójne zarządzanie ustawieniami całego stosu technologii zabezpieczeń Microsoft – od konfiguracji systemu operacyjnego Microsoft Windows, przez usługi Microsoft Defender oraz Windows Firewall, po ustawienia przeglądarki Microsoft Edge.
- **Wysokiej skuteczności haseł definiowanych przez użytkowników** – usługa Azure AD Password Protection wykrywa i blokuje znane słabe hasła oraz ich warianty, a także frazy specyficzne dla określonej organizacji, tak aby zapewnić wysoką skuteczność haseł, jako pierwszej linii obrony przed nieautoryzowanym dostępem.
- **Funkcjonalności dostępu warunkowego** – dostępne w ramach usługi Microsoft Azure AD funkcje umożliwiają zapewnienie dodatkowych zabezpieczeń i wymuszenie dodatkowego uwierzytelniania, w zależności od zgromadzonych danych na temat zachowania konkretnych użytkowników i danych dotyczących m.in. ich lokalizacji, urządzenia oraz aplikacji, z której chcą skorzystać. Tworząc zasady dostępu warunkowego, można dostroić proces uwierzytelniania tak, aby nadmiernie nie obciążać użytkowników, zachowując jednocześnie najwyższe standardy ochrony zasobów organizacji.

Posłużę się przykładem: jeśli pracownik przychodzi do pracy i uruchamia komputer jak zawsze o 9.00 rano, to system uwierzytelnienia, np. biometrycznego, powinien przeskanować jego twarz, przywitać i umożliwić pracę. Gdyby jednak okazało się, że ten sam pracownik niespodziewanie próbuje się zalogować do systemu z biurowej sieci o 3.00 w nocy, to system powinien poprosić o dodatkowe uwierzytelnienie. Jeśli natomiast okaże się, że pracownik ten łączy się po IP połączonym z siecią firmową z nietypowej, zdalnej lokalizacji, to wymagane powinno być dodatkowe działanie, np. wykorzystanie klucza fizycznego.

Analogicznie możemy postępować przy ochronie danych, bo na to pozwala nam dziś uczenie maszynowe. Przykładowo, jeśli system zauważy, że do wiadomości e-mail załączamy dane osobowe, to przypomni o ryzykach z tym związanych. Można też zdefiniować proces, który zablokuje wysłanie takiej wiadomości poza organizację lub poprosi o dodatkową autoryzację przełożonego. Na tym polega właśnie nowoczesne myślenie o bezpieczeństwie, które nie jest uciążliwe dla użytkownika końcowego, ale pozwala uniknąć problemów wynikających z nieprzemyślanych działań lub nietypowych sytuacji.

Wróćmy do nowych dyrektyw związanych z cyberbezpieczeństwem. Jakie główne zmiany wprowadza NIS2 i Critical Entities Resillience?

Nowe dyrektywy stawiają na myślenie. W NIS2 i CER wprost opisane jest podejście oparte na analizie ryzyka. Jest to o tyle istotne, że w bezpieczeństwo nie należy inwestować za wszelką cenę, bo to nie cyberbezpieczeństwo jest celem funkcjonowania większości firm. Takim celem jest generowanie dochodu, a cyberbezpieczeństwo ma temu służyć.

Działania mające na celu zapewnienie bezpieczeństwa de facto sprowadzają się do zapewnienia ciągłości działania przedsiębiorstw – i na tym właśnie dyrektywy CER i NIS2 się koncentrują. W praktyce wiele osób postrzega NIS2 po prostu jako kolejną regulację. Mam jednak wrażenie, że tylko nieliczne osoby zdają sobie sprawę, jak wielu organizacji dotyka.

Jakie obowiązki nakłada dyrektywa NIS2 na przedsiębiorców?

NIS2 określa obowiązki państw członkowskich i uczestników systemu z punktu widzenia biznesowego. Wskazuje bowiem podmioty kluczowe i ważne. Co istotne, do tej pory, jeśli dana organizacja została uznana za operatora infrastruktury krytycznej albo dostawcę usług krytycznych, to otrzymywała decyzję administracyjną lub informację o wpisie do stosownego wykazu prowadzonego przez Rządowe Centrum Bezpieczeństwa.

Wraz z wprowadzeniem NIS2 prawie wszystkie firmy znajdą się pod takim parasolem i nie ma mechanizmu powiadamiania dla poszczególnych przedsiębiorstw czy instytucji. Konieczne staje się sprawdzenie, w jakim zakresie działalność naszej organizacji podlega nowym przepisom.

Jeśli np. jesteśmy producentem naczep, to bezpośrednio w NIS2 przedsiębiorstwa prowadzące taką działalność są określone mianem „ważnych". Podmioty ważne wg NIS2 mają obowiązki głównie w zakresie zarządzania ryzykiem, obsługi incydentów oraz udziału w obiegu informacji. W przypadku niewywiązywania się z takich zadań, podmiotom ważnym grożą kary finansowe.

Jednocześnie, duża część obowiązków związanych z cyberbezpieczeństwem jest nałożona na państwa członkowskie. Każde z nich ma ustanowić krajowy plan reagowania. Kraje mają uczyć się od siebie najlepszych praktyk. Poza tym państwo dostaje duże kompetencje nadzorcze i może podmiotom kluczowym wydawać wiążące instrukcje, a pomiotom ważnym – nakazać przeprowadzenie audytu bezpieczeństwa.

Jakich branż dotyczy dyrektywa NIS2?

W ujęciu ogólnym są to: energetyka, transport, bankowość, infrastruktura rynków finansowych, opieka zdrowotna, woda pitna i ścieki, infrastruktura cyfrowa, przestrzeń kosmiczna, administracja i zarządzanie usługami ICT. Warto jednak zajrzeć do szczegółowych przepisów. Nowym zbiorem są podmioty ważne. Mamy tam same nowe kategorie, w których znalazły się m.in. takie branże, jak: usługi kurierskie i pocztowe oraz produkcja, przetwarzanie i dystrybucja żywności.

Co mają robić takie podmioty?

Ich zadania można podzielić na trzy grupy. Najbardziej podstawowa dotyczy cyberhigieny oraz wdrożenia podejścia do bezpieczeństwa opartego na zerowym zaufaniu. Chodzi oczywiście o pewną filozofię bezpieczeństwa IT, a nie rozwiązanie konkretnego dostawcy.

Zasada zerowego zaufania to kwestia aktualizacji oprogramowania, konfiguracji urządzeń, zarządzania tożsamością, wprowadzenia zasady segmentacji sieci czy budowania świadomości użytkowników. Co ciekawe, jak pokazują analizy Microsoft, zdecydowana większość zdarzeń w obszarze cyberbezpieczeństwa zależy wprost od podejścia użytkowników oraz cyberhigieny całej organizacji.

Ważne jest to, że na członków organów zarządzających w podmiotach ważnych i kluczowych nałożono obowiązek przechodzenia regularnych szkoleń z zakresu cyberbezpieczeństwa.

Wspomniał Pan o trzech grupach obowiązków…

Drugą grupę stanowi obowiązek wejścia w system obiegu informacji o incydentach i obowiązek wczesnego ostrzegania, że doszło do incydentu w obszarze cyberbezpieczeństwa. Na wstępne ostrzeżenie mamy 24 godziny. Formalne zgłoszenie z oceną dotkliwości i skutków powinno nastąpić w ciągu 72 godzin, a sprawozdanie końcowe w ciągu miesiąca.

Kolejna grupa to kwestie organizacyjne, czyli obowiązek posiadania różnych polityk, analiz ryzyka, procedur, zaplanowania w świadomy sposób ciągłości działania w organizacji i zaprojektowania bezpieczeństwa łańcucha dostaw. Niewątpliwie jest to spora liczba zadań, choć one oczywiście jeszcze nie obowiązują, ponieważ muszą być wdrożone do polskiego systemu prawnego.

Od jakich działań przedsiębiorstwa uznane za ważne lub kluczowe powinny rozpocząć dostosowanie do nowych regulacji?

Najważniejsze jest przeprowadzenie analizy ryzyka, wdrożenie środków, które pozwolą to ryzyko ograniczyć, a także umiejętność zgłaszania poważnych incydentów. Jest to o tyle istotne, że za rażące nieprzestrzeganie zapisów tej dyrektywy przewidziane są dolegliwe kary.

W praktyce, nowe dyrektywy w pewnym stopniu sankcjonują dorobek biznesowy wielu organizacji. Wymagają bowiem szerokiego wykorzystania analizy ryzyka, a więc zrozumienia zagrożeń dla biznesu. Są bowiem takie ryzyka, które możemy minimalizować, i takie, na które nie mamy wpływu. W momencie, kiedy nie jesteśmy w stanie zarządzać takim ryzykiem, musimy nauczyć się zarządzać jego skutkami i minimalizować straty, kiedy będzie to potrzebne oraz korzystać ze wsparcia państwa.

Żaden biznes nie będzie w stanie samodzielnie walczyć z zakrojoną na szeroką skalę kampanią w obszarze cyberbezpieczeństwa. Chyba że jest to globalny dostawca, jak Microsoft. Po to są przewidziane przepisami linie wsparcia – sektorowe, branżowe i państwowe, a nawet wojskowe.

Niewiele powiedzieliśmy dziś o samej technologii…

Nie ma w tym przypadku. Bezpieczeństwo każdej organizacji opiera się na trzech filarach. Są to: ludzie, procesy i dopiero technologia, która je wspiera. Wszystkie te filary powinny być równoważne. Technologia jest niezbędna, ale nie jest wystarczająca do zapewnienia cyberbezpieczeństwa. Być może zabrzmi to dziwnie w ustach przedstawiciela firmy technologicznej, ale nie wolno wpadać w przeświadczenie, że technologia coś zrobi za mnie. Trzeba ją wdrożyć, wiedzieć do czego służy i właściwie wykorzystywać.

W kontekście NIS2 przede wszystkim nie należy odkładać przygotowań na ostatnią chwilę. Po drugie, nie można unikać udziału w różnych ćwiczeniach i stress-testach zapowiadanych przez Komisję Europejską. Do ćwiczeń trzeba podchodzić szczerze i nie lukrować rzeczywistości, bo jeśli coś się nie uda, to mamy czarno na białym wskazane, co musimy poprawić. Trzeba odrobić lekcję i krok po kroku odhaczać te obowiązki. Na początek warto zajrzeć do dyrektywy i sprawdzić, w jakim stopniu nas ta kwestia dotyczy.

Wywiad przeprowadził
Piotr Waszczuk

Od Ukrainy po całą Europę: cyberkonflikt osiąga punkt zwrotny

Punktem zwrotnym w dziedzinie cyberbezpieczeństwa w związku z konfliktem na Ukrainie był III kwartał 2022 roku. Raport Thales Cyber Threat Intelligence Report 2023 pokazuje, że cyberkonflikt wszedł w kolejną fazę – od cyberwojny skoncentrowanej na obszarze Ukrainy i Rosji do konfliktu hybrydowego o wysokiej intensywności, w którym ataki skierowane są przede wszystkim przeciwko Polsce oraz krajom bałtyckim i nordyckim.

W pierwszej fazie wojny dominowały celowane kampanie. Obecnie prorosyjscy haktywiści stosują głównie działania partyzanckie, wykorzystując ataki DDoS, aby czasowo uniemożliwić dostęp do serwerów i zakłócić działanie usług. Ataki te są częścią rosyjskiej strategii angażowania się w wojnę informacyjną jako sposobu na osłabienie podmiotów prywatnych i publicznych w państwach ościennych. Ataki coraz częściej dotyczą też kluczowych sektorów państwowych, takich jak lotnictwo, energetyka, infrastruktura zdrowotna, bankowość i instytucje publiczne.

Europa Wschodnia i Północna na pierwszej linii cyberkonfliktu

W ciągu ostatnich 12 miesięcy zmienił się zasięg terytorialny ataków prowadzonych przez prorosyjskie grupy hakerskie. Na początku konfliktu większość incydentów dotyczyła przede wszystkim Ukrainy (50,4% w porównaniu z 28,6% w trzecim kwartale 2022 roku, jednak w ciągu ostatnich sześciu miesięcy w krajach Unii Europejskiej odnotowano gwałtowny wzrost incydentów związanych z konfliktem (9,8% w porównaniu z 46,5% globalnych ataków).

46,5%

do tylu (z 9,8% 6 miesięcy temu) wzrosła liczba globalnych cyberataków związanych z konfliktem na Ukrainie w krajach Unii Europejskiej. Tymczasem na początku konfliktu większość incydentów dotyczyła Ukrainy (50,4% w porównaniu z 28,6% w III kwartale 2022 roku).

Tego lata w krajach UE było prawie tyle samo incydentów związanych z konfliktem, co w Ukrainie (85 wobec 86), a w pierwszym kwartale 2023 roku przytłaczająca większość incydentów (80,9%) miała miejsce już na terenie Unii Europejskiej. Coraz częściej celem ataków są również państwa kandydujące do członkostwa we Wspólnocie Europejskiej, takie jak Czarnogóra i Mołdawia: 0,7% ataków w pierwszym kwartale 2022 roku wobec 2,7% na koniec 2022 roku.

Polska z kolei doświadcza bezustannych i zmasowanych aktów cyberprzestępczości. W ciągu ostatniego roku na tym obszarze odnotowano rekordową liczbę, tj. 114 incydentów związanych z konfliktem. Wojenni haktywiści obrali sobie za cel szczególnie kraje bałtyckie (157 incydentów w Estonii, na Łotwie i Litwie) oraz kraje nordyckie (95 incydentów w Szwecji, Norwegii, Danii i Finlandii). W Niemczech w 2022 roku odnotowano 58 incydentów. Zgodnie z analizami ekspertów w innych krajach, takich jak Francja (14 ataków), Wielka Brytania (18), Włochy (14) i Hiszpania (4), intensywność cyberprzemocy jest mniejsza.

„W III kwartale 2022 roku Europa została wciągnięta w hybrydową cyberwojnę o wysokiej intensywności. Dla naszego kontynentu to absolutny punkt zwrotny, obserwujemy zwłaszcza ogromną falę ataków DDoS, szczególnie w krajach nordyckich i bałtyckich oraz w Europie Wschodniej. Działania w cyberprzestrzeni są obecnie kluczową bronią w arsenale nowych sposobów prowadzenia wojny, obok dezinformacji, manipulacji opinią publiczną, wojny ekonomicznej, sabotażu i taktyki partyzanckiej" – mówi Pierre-Yves Jolivet, VP Cyber Solutions, Thales.

61%

cyberataków zgłoszonych od lutego 2022 roku zostało dokonanych przez prorosyjskie grupy haktywistów, a w szczególności Anonymous Russia, Killnet i Russian Hackers Teams.

„W miarę jak konsekwencje konfliktu w Ukrainie rozlewają się na resztę Europy, państwa Europy Zachodniej powinny zwrócić szczególną uwagę na ten aspekt bezpieczeństwa narodowego. Prawdopodobieństwo ataków na infrastrukturę krytyczną znacząco wzrasta, a wojna w cyberprzestrzeni będzie nabierała przyspieszenia" – dodaje.

Od haktywistów wojennych do cyberharcerzy

Ze wszystkich cyberataków zgłoszonych na całym świecie od początku konfliktu, aż 61% zostało dokonanych przez prorosyjskie grupy haktywistów, a w szczególności przez Anonymous Russia, Killnet i Russian Hackers Teams, które od początku konfliktu prowadziły akcje przeciwko haktywistom z Ukrainy. Te nowe grupy działają w sposób znacznie bardziej ustrukturalizowany i korzystają z zasobów użytkowanych przez grupy cyberprzestępcze, w tym zasoby typu Botnet-as-a-Service, takie jak Passion Botnet.

Ich celem jest wywarcie nacisku na państwa zachodnie, które wspierają Ukrainę. Te grupy niezależnych, cywilnych haktywistów pojawiły się jako nowa strona konfliktu. Można je przyrównać do organizacji cyberprzestępczej o określonych celach i interesach politycznych, działającej z przekonania, ale nie wspieranej bezpośrednio przez rząd. Członkowie takich grup pochodzą z różnych środowisk i mają zaawansowane umiejętności techniczne.

W III kwartale 2022 roku nastąpiło przejście do fali ataków DDoS, w przeciwieństwie do I kwartału 2022 roku, w którym odnotowano wiele różnych rodzajów ataków, podzielonych mniej więcej po równo między wycieki danych i kradzież, ataki DDoS, szpiegostwo, kampanie wpływu, włamania, ataki typu ransomware, phishing, wiper i infostealer.

Najbardziej popularne formy ataku

Cyberatakujący od pół roku preferują jednak ataki DDoS (75%) przeciwko firmom i rządom. To systematyczne nękanie często ma niewielki wpływ operacyjny, ale podtrzymuje atmosferę niepokoju wśród zespołów bezpieczeństwa i decydentów. Ich celem nie jest wywarcie dużego wpływu operacyjnego, ale nękanie celów i zniechęcenie ich do wspierania Ukrainy.

Na drugim krańcu tego spektrum – jeśli chodzi o szkodliwość – znajdują się ataki typu wiper, które mogą zniszczyć systemy przeciwnika, a długotrwałe cyberszpiegostwo może wręcz podważyć integralność systemów bezpieczeństwa zaatakowanego. Należy jednak pamiętać, że przygotowanie takich rozwiązań trwa znacznie dłużej i wymaga większych zasobów. Dlatego destrukcyjne operacje cyberwojskowe – z komponentem szpiegostwa – stanowią jedynie 2% całkowitej liczby incydentów i są skierowane głównie przeciwko ukraińskim organizacjom sektora publicznego. Władze rosyjskie regularnie wykorzystują cybernetykę do wywierania presji na swoich przeciwników bez angażowania się w bezpośrednią konfrontację.

Akty wojny cybernetycznej wciąż mają miejsce na Ukrainie. Przykładem zmasowanych działań tego typu był dokonany w rocznicę wybuchu wojny (23 lutego 2023 roku) atak ATK256 (UAC-0056), który zasięgiem objął kilka istotnych ukraińskich instytucji publicznych. Choć na samej Ukrainie cyberwojna wciąż się nasila, coraz częściej uwaga państw zachodnich koncentruje się na działaniach partyzanckich prowadzonych na coraz szerszą skalę w całej Europie.

Coraz większa liczba sektorów pod presją

W I kwartale 2022 roku większość cyberataków była wymierzona w ukraińską obronną bazę przemysłową oraz administrację publiczną tego kraju. Obecnie cyberataki coraz częściej dotyczą także innych krajów europejskich i dotykają m.in. administrację publiczną (30 incydentów), sektor finansowy (162), sektor transportowy (132), telekomunikację (90), media (89) i sektor energetyczny (66). Chociaż wcześniej konflikt był stosunkowo mało dotkliwy, europejski sektor opieki zdrowotnej, rządy, przemysł, usługi IT i sektor lotniczy są coraz częściej celem ataków, których zadaniem jest wywarcie presji na zachodnie społeczeństwa.

Autor raportu – firma Thales – dostarcza rozwiązania z zakresu cyberbezpieczeństwa dla 90% największych, komercyjnych graczy internetowych oraz pomaga chronić systemy IT ponad 130 agencji rządowych i dostawców usług kluczowych. Zatrudniając ponad 3500 ekspertów ds. cyberbezpieczeństwa, firma zapewnia rządom i operatorom infrastruktury krytycznej zintegrowane rozwiązania w zakresie wykrywania i reagowania na incydenty, w tym informacje o zagrożeniach cybernetycznych, suwerenne sondy, dedykowane centra bezpieczeństwa i systemy szyfrowania, aby zapobiec naruszeniom danych. Wartość sprzedaży rozwiązań cyberbezpieczeństwa Grupy Thales wyniosła 1,5 mld euro w 2022 roku.

Adam Jadczak

Źródło: Thales Cyber Threat Intelligence Report, luty 2023 r.

ING Hubs Poland

Bierzemy udział w wyścigu z cyberprzestępcami, którzy nieustannie identyfikują nowe możliwości ataku

Z **Łukaszem Miedzińskim,** dyrektorem IT w Departamencie Attack Surface Management w Grupie ING, rozmawiamy o: specyfice pracy w tej jednostce; działalności zespołu pentesterów; geopolityce jako jednym z ryzyk dla sektora bankowości; największych obecnie zagrożeniach występujących w sektorze finansowym; o sposobach ochrony klientów i pracowników banków; koncepcji Layers Security; wykorzystaniu sztucznej inteligencji do identyfikacji zagrożeń oraz o wpływie NIS2 na sektor bankowy.

Czym zajmuje się Pan, pracując w Departamencie Attack Surface Management? Jak jest on duży? Czy pracuje dla całej Grupy ING?

Powstał on całkiem niedawno. Jest jednostką świadczącą usługi dla 26 krajów w Grupie ING. Odpowiadam w nim za polską część organizacji, którą budowałem przez ostatnich kilka lat. Obecnie liczy ona ok. 160 osób. Co do zakresu naszej działalności, to jest dość złożony, choć oczywiście skoncentrowany na cyberbezpieczeństwie.

Departament tworzą bowiem zarówno zespoły, które w sposób automatyczny wykrywają podatności przez tzw. Vulnerability Scanning, jak i zespół odpowiadający za testy penetracyjne, czyli testowanie efektywności naszych zabezpieczeń. Mamy też w strukturach zespoły deweloperskie oraz te skoncentrowane na roli Security Officera, czyli definiowaniu polityk bezpieczeństwa i stałej weryfikacji zgodności z nimi. W skrócie, pokazujemy to, w jaki sposób powinniśmy zabezpieczać nasze systemy.

Ponadto, od roku 2023 bardzo mocno jestem skoncentrowany na obszarze Cyber Security Protection. Odpowiada on za globalną implementację zabezpieczeń prewencyjnych, tzw. Preventing Controls, dla systemów i środowisk, zarówno w przestrzeni chmurowej, jak i on premise.

Na czym dokładnie polega Preventing Controls?

Preventing Controls polega na zdefiniowaniu i zaimplementowaniu zabezpieczeń systemów w taki sposób, aby uniemożliwić nieautoryzowane działania. Przykładowo, możemy tak skonfigurować stację roboczą, aby pracująca na niej osoba nie miała możliwości bezpośredniego wysłania plików poza organizację, np. na Google Drive. Zastosowane narzędzie nie ma wykrywać tego typu prób i wysyłać do nas powiadomień, tylko z góry zapobiegać usiłowaniom naruszenia bezpieczeństwa.

Jak liczna jest grupa pentesterów w departamencie? Jak wygląda jej działalność?

Mówimy o obszarze Offensive Security, a grupa ta liczy obecnie ok. 40 osób. Są to wysokospecjalizowani w cyberbezpieczeństwie inżynierowie, którzy symulują ataki na systemy Grupy ING. Odbywa się to w kilku etapach. W pierwszej kolejności wspomniani specjaliści badają, w jaki sposób można przełamać cyberzabezpieczenia naszej organizacji na poziomie infrastruktury. W kolejnym przeprowadzają próby przełamania zabezpieczeń aplikacji. Zarówno tych, które ING dostarcza klientom, jak i tych wykorzystywanych przez pracowników Grupy ING wewnątrz.

Na ostatnim etapie stosujemy najbardziej zaawansowane techniki przełamywania zabezpieczeń – tzw. Red Teaming – a więc symulację ataku hakerskiego. Przykładowo, chcemy sprawdzić, czy w Grupie ING istnieje możliwość wykonania nieautoryzowanego przelewu z kont bankowych klientów. W ramach tego celu są definiowane ścieżki, jakimi można wykonać takie operacje. Pentester zaczyna z zewnątrz, wykorzystując np. social media, identyfikuje osobę, która pozwoli mu uzyskać tzw. punkty styku do organizacji. W kolejnym kroku wykonuje na przykład operację phishingową, umożliwiającą uzyskanie dostępu do stacji roboczej. Dzięki zainfekowaniu stacji roboczej sprawdza, czy istnieją luki wewnątrz organizacji, czy da się do jej systemów dostać w nieautoryzowany sposób, i próbuje przeprowadzić atak zgodny z celem.

Następnie przygotowywany jest dokładny raport przedstawiający całą ścieżkę tego, w jaki sposób atak został wykonany, z detaliczną rekomendacją, jak można

zabezpieczyć się przed nim w przyszłości. Ostatnia faza to praca wszystkich inżynierów bezpieczeństwa nad tym, aby – na podstawie raportu – dokonać zmian w systemach i wdrożyć dodatkowe zabezpieczenia – czy to w warstwie Preventive, czy Detective.

Jak dużo „dziur" w systemach IT wykrywacie?

Jeśli chodzi o testy penetracyjne, to trzeba pamiętać, że oprócz nich wykonywane są również testy automatyczne – typu Source Code Review, Dynamic Code Review, czyli SAST i DAST– realizowane na poziomie developmentu. W ich ramach podatności są na bieżąco wykrywane i poprawiane. Zanim dana aplikacja zostanie zaimplementowana produkcyjnie. Kolejna faza to już pentesty, w ramach których pentester próbuje zidentyfikować niewykryte wcześniej podatności.

Podatności zdarzają się więc bardzo często. Żaden z systemów produkcyjnych nie jest w 100% bezpieczny. To jest rodzaj walki z wiatrakami. Z jednej strony tworzone są nowe zabezpieczenia czy implementowane dodatkowe narzędzia zabezpieczające systemy. Z drugiej strony zaś osoby, które te zabezpieczenia łamią, wymyślając nowe techniki, znajdują nowe podatności i wykorzystują je.

Mówi się, że jednym z kluczowych ryzyk w bankowości jest dziś geopolityka. Czy po wybuchu wojny na Ukrainie zwiększyła się liczba cyberataków skierowanych przeciwko bankom? Czy zmienił się ich charakter?

Charakter cyberataków raczej się nie zmienił. Natomiast rzeczywiście początek wojny i jej pierwsza faza – marzec, kwiecień i maj 2022 roku – wiązały się z bardzo dużym wzrostem ataków cyberprzestępców. Były one jednak skoncentrowane na instytucjach oraz organizacjach rządowych. Podobnie jest teraz.

Trudno jest zresztą zidentyfikować jedno główne zagrożenie wynikające z geopolityki. Oczywiście trzeba mieć takie ryzyka na uwadze, ale musimy skupiać się raczej na innych, większych zagrożeniach związanych z cyberbezpieczeństwem w sektorze finansowym.

> Jestem zwolennikiem koncepcji Layers Security, czyli budowania warstw, które pozwalają zabezpieczyć system na każdym kroku. Model ten przynosi bardzo dobre efekty.

Jakie zatem są te zagrożenia?

Występuje kilka obszarów, na których najbardziej się koncentrują cyberprzestępcy. Pierwszy z nich dotyczy użytkowników końcowych. Są to więc próby wyłudzenia pieniędzy od klientów banku, którzy korzystają ze smartfonów czy aplikacji online, aby np. zrobić przelew za zakupy w sklepach internetowych. Jeden z ostatnio bardzo popularnych ataków bazuje na wysyłkach SMS np. z prośbą o dopłacenie do przesyłki internetowej, w którym znajduje się link wymagający na dalszym etapie podania danych karty kredytowej. W ten czy inny sposób podając – czasem zupełnie nieświadomie – o jedną informację na zewnątrz za dużo, możemy stać się ofiarą bota, który co kilkanaście sekund będzie nam ściągał z konta niewielką kwotę. Na szczęście banki mają narzędzia, które próbują wykrywać tego typu próby wyłudzenia. Bez wątpienia jest to dziś bardzo wrażliwy obszar.

Drugi dotyczy prób ataków na systemy widoczne z poziomu internetu. Mogą to być np. aplikacje wykorzystywane do wykonywania transakcji bankowych czy operacji na naszych systemach. Trzeci zaś dotyczy sytuacji, kiedy cyberprzestępcy starają dostać się do wewnętrznych systemów banku poprzez próbę zainfekowania stacji roboczej pracownika. Może to być zarówno zwykły pracownik operacyjny oddziału, jak i osoba zajmująca się IT, która ma większe uprawnienia w zakresie dostępów do systemów IT.

W pierwszym i ostatnim z obszarów najsłabszym ogniwem jest człowiek. To on jest pierwszym punktem styku z organizacją i on jest najbardziej narażony na ataki, o których wspomniałem.

Odnotowujecie więcej ataków na infrastrukturę IT czy aplikacje?

Zdecydowanie więcej ataków skierowanych jest na aplikacje bankowe i użytkowników końcowych niż bezpośrednio na nasze systemy. Wynika to z faktu, iż technologie związane z bezpieczeństwem mocno się rozwinęły i zaatakowanie wprost systemu teleinformatycznego z zewnątrz jest bardzo trudne. Częstszym sposobem uzyskania dostępu są próby ataków na klientów i pracowników banków.

Jak więc chronić jednych i drugich?

Na pewno poprzez zwiększanie świadomości z jakimi atakami mogą te osoby mieć do czynienia i jak mają na nie reagować. Oczywiście musimy oddzielić warstwę użytkowników aplikacji, bo oni muszą mieć dużą świadomość tego, że nie mogą przekazywać danych do uwierzytelniania. Nie mogą też wykonywać operacji, które są inicjowane przez dzwoniącą osobę, podającą się za pracownika banku. Świadomość takich zagrożeń jest bardzo ważna.

Natomiast z punktu widzenia rozwiązań technicznych, cały czas dzieje się coś nowego. Wciąż opracowywane są nowe techniki i próby ograniczenia ryzyka przez błędy użytkownika, jak np. analiza behawioralna.

Bezwzględnie musimy też pamiętać o tym, aby włączać w naszych aplikacjach uwierzytelnianie dwuskładnikowe MFA (Multi-Factor Authentication). Ten prosty czynnik pozwala na znaczne obniżenie poziomu ryzyka. Poza tym warto włączyć dodatkowe funkcjonalności, które – w sposób automatyczny – będą wykrywać niebezpieczne operacje.

> Jeśli chodzi o testy penetracyjne, to trzeba pamiętać, że oprócz nich wykonywane są również przez nas testy automatyczne – typu Source Code Review, Dynamic Code Review, czyli SAST i DAST – realizowane na poziomie developmentu.

W jaki sposób zabezpieczacie siebie wewnętrznie?

Jestem zwolennikiem koncepcji Layers Security, czyli budowania warstw, które pozwalają zabezpieczyć system na każdym kroku. Model ten przynosi bardzo dobre efekty. W ramach tej koncepcji w pierwszej kolejności trzeba skoncentrować się na implementacji procesów bezpieczeństwa w wybranych obszarach.

Idąc po kolei, jeden z ważniejszych procesów polega na identyfikowaniu podatności, zarówno na warstwie infrastrukturalnej, jak i aplikacyjnej poprzez wykonywanie wspomnianego wcześniej Vulnerability Scanningu oraz SAST i DAST. Kolejny krok to aktywny monitoring systemów, w celu identyfikacji potencjalnych ataków, które w danym momencie są wykonywane. Z jednej strony ważna jest implementacja tego monitoringu na systemach operacyjnych i aplikacjach, a z drugiej – na urządzeniach użytkowników końcowych. Stosujemy do tego narzędzia Endpoint Detection Response. Dzięki temu monitorujemy to, co dzieje się na stacji roboczej i jesteśmy ostrzegani o próbach nadużyć.

Inny ważny punkt to wdrożenie zabezpieczeń prewencyjnych, których głównym celem jest niedopuszczanie do tego, aby pewne operacje mogły być wykonywane na systemie. Mówimy zatem o nienadawaniu zbyt wysokich uprawnień czy nawet totalnym blokowaniu pewnych aktywności, zwłaszcza jeśli mamy zespół, który jest mocno narażony na materializację ryzyka. Niestety, obecnie mamy dość mocno utrudnione zadanie, jeśli chodzi o tę kwestię, ponieważ po pandemii większość osób pracuje w formie hybrydowej. Komputery pracowników nie są dziś włączone na stałe do sieci wewnętrznej, która jest lepiej chroniona. Wszystkie systemy zabezpieczające powinny być zatem zaimplementowane bezpośrednio na stacji roboczej. Mam tu na myśli rozwiązania typu Cloud Proxy czy Protective DNS. Do tego dochodzą techniki EDR-owe do wykrywania aktywności cyberprzestępców.

Bardzo ważne jest również testowanie efektywności zabezpieczeń. Z jednej strony bowiem przez długi czas koncentrujemy się na tym, aby je wdrożyć i mieć

efektywne procesy. Z drugiej zaś musimy mieć świadomość, jak dobrze te zabezpieczenia funkcjonują. Dlatego też wykonywanie testów penetracyjnych, o których wspomniałem na początku, jest ważnym elementem całej układanki. Musimy mieć świadomość tego, gdzie są słabe punkty i na jakich działaniach powinniśmy się skupiać w kolejnym etapie.

Czy koncepcja Layer Security to must have, aby dobrze zabezpieczyć systemy bankowe?

To mocna podstawa. Ale oczywiście robimy dużo więcej. Jedna rzecz to opracowanie wszystkich procesów zabezpieczających, a druga to weryfikacja tego, czy one efektywnie działają. Poza tym cyberzagrożenia nieustannie ewoluują i nawet jeśli jeden proces działa dobrze, to może się okazać, że za trzy tygodnie trzeba go będzie zmienić, bo np. zmodyfikowano techniki cyberataków. Bierzemy więc udział w wyścigu z cyberprzestępcami, którzy nieustannie identyfikują nowe możliwości ataku.

Z niedawnego raportu EY i Instytutu Finansów Międzynarodowych wynika, że już 35% dyrektorów ds. ryzyka twierdzi, iż używa sztucznej inteligencji oraz uczenia maszynowego do identyfikowania zagrożeń w bankach. Jak to wygląda w Grupie ING?

Oczywiście też – na co dzień – mamy do czynienia z Artificial Intelligence i Machine Learning. Nie da się tego uniknąć, ponieważ technologia ta pozwala nam automatyzować i ulepszać pewne procesy, a jeśli sprawdza się ona w innych obszarach IT, to czemu miałaby nie działać w obszarze bezpieczeństwa?

Najszerzej wykorzystujemy ją w obszarze detekcji, czyli do monitorowania systemów, ale także do budowania modeli, które poprawiają wykrywalność zagrożeń. Jeśli mamy np. zbudowaną pewną linię bazową tego, co dzieje się na bieżąco w naszych systemach i tego, co jest w nich dozwolone, to algorytmy sztucznej inteligencji pomagają nam później identyfikować anomalie, które wymagają reakcji.

Kolejny obszar zastosowania AI/ML to analiza ogromnej ilości danych z naszych procesów security. Dotyczą one analizy danych o podatnościach czy ogólnych informacji o systemach jakimi zarządzamy, jak są one skonfigurowane, czy też jakie aplikacje i narzędzia są tam zainstalowane. Analityka wsparta algorytmami sztucznej inteligencji pozwala nam wyłuskać to, na czym mamy się skoncentrować, jeśli chodzi o procesy zabezpieczania czy reakcji na anomalie, które zidentyfikujemy w ramach realizacji procesów bezpieczeństwa IT.

Obszary, na których najbardziej się koncentrują cyberprzestępcy. Dotyczą one:

1. **Użytkowników końcowych** – są to więc próby wyłudzenia pieniędzy od klientów banku.
2. **Prób ataków na systemy widoczne z poziomu internetu.** Mogą to być np. aplikacje wykorzystywane do wykonywania transakcji bankowych czy operacji na naszych systemach.
3. **Sytuacji, kiedy cyberprzestępcy starają dostać się do wewnętrznych systemów banku** poprzez próbę zainfekowania stacji roboczej pracownika.

Generalnie sztuczna inteligencja to obecnie bardzo interesująca i rozwojowa technologia. Wszyscy zastanawiamy się, w jaki sposób moglibyśmy ją wykorzystać w jeszcze większym stopniu. Z drugiej strony, coraz częściej myślimy też o tym, kiedy zacznie nam ona przeszkadzać i kiedy sami będziemy musieli trochę lepiej się przed nią zabezpieczać. Bo w równym stopniu, jak wspiera nasze działania, tak robi to też w przypadku cyberprzestępców, którzy na pewno będą ją wykorzystywać na większą skalę, przygotowując cyberatak.

Jak daleko idzie automatyzacja w CyberSec? Czy sztuczną inteligencją będzie się z czasem dało zastąpić codzienną pracę specjalistów ds. cyberbezpieczeństwa, czy też pozostanie ona tylko technologią wspierającą ich pracę?

Na pewno nie jesteśmy jeszcze na tym etapie rozwoju, aby narzędzia te mogły całkiem zastąpić człowieka. W realizacji pewnych zadań są one pomocą, dzięki której można je wykonywać szybciej i bez dodatkowego nakładu pracy.

Natomiast wcale mnie nie zdziwi, jeśli za jakiś czas technologia ta będzie potrafiła zastępować człowieka w wykonywaniu określonych operacji. Jestem przekonany, że tak się stanie. Wszystko zależy jednak od poziomu zaawansowania danych obszarów cyberbezpieczeństwa. Są bowiem wśród nich takie, które wymagają wysokich kwalifikacji, i w których spojrzenie człowieka jest niezbędne.

Niedawno ogłoszono wejście w życie dyrektywy NIS2 dotyczącej cyberbezpieczeństwa. Jakie działania będzie musiał podjąć sektor bankowy, aby jej sprostać?

Jesteśmy jeszcze na etapie szczegółowej analizy wymagań w niej przedstawionych. Według mojej, wstępnej oceny liczba zmian, które wprowadza NIS2 w stosunku do poprzedniczki z roku 2016, nie jest dla banków zbyt duża. Zresztą wydaje się, że dyrektywa ta jest bardziej skoncentrowana na sektorze publicznym i instytucjach rządowych.

Poza tym na sektor finansowy od wielu już lat nakłada się rygorystyczne wymogi dotyczące cyberbezpieczeństwa. Pewne procesy – jak opracowanie planów ciągłości działania czy polityki zarządzania incydentami – które są zdefiniowane w NIS2, od dawna już mamy. Przypuszczam, że będą one wymagały jedynie dodania dodatkowych kroków czy nowych sposobów raportowania.

Nie spodziewałbym się większego przewrotu związanego z tą dyrektywą w sektorze bankowym. Bardziej „inwazyjne" z tego punktu widzenia jest rozporządzenie DORA niż NIS2. I pewnie to w tej materii będziemy mieli trochę więcej pracy.

Wywiad przeprowadził
Mikołaj Marszycki

Pomagamy klientom, którzy chcą używać rozwiązań SAP w sposób świadomy

Z **Jackiem Bugajskim,** prezesem zarządu w firmie SNOK, rozmawiamy o podejściu polskich firm do zabezpieczenia systemów klasy ERP; specyfice środowisk SAP w kontekście bezpieczeństwa, integracji z platformami SIEM oraz Security Operations Center, możliwościach oprogramowania SecurityBridge, wykrywaniu luk bezpieczeństwa i błędów w warstwie ABAP, a także usługach audytu i poprawy bezpieczeństwa środowisk SAP.

O bezpieczeństwie systemów klasy ERP nie mówi się zbyt dużo…

Ten temat faktycznie nie jest jeszcze w Polsce szczególnie popularny – pewnie dlatego, że jest dość trudny. Tymczasem należy pamiętać, że w systemach klasy ERP znajdują się dane krytyczne dla biznesu, a same rozwiązania tego typu mają zwykle kluczowe znaczenie dla funkcjonowania całej organizacji.

Ponadto, systemy tej klasy są często postrzegane jako pewnego rodzaju „czarne skrzynki" – złożone technicznie i skomplikowane w działaniu – i jako takie pozostają poza obszarem szczególnego zainteresowania działów bezpieczeństwa dopóty, dopóki ktoś nie przełamie ich zabezpieczeń.

Jednocześnie, zagrożeń wymierzonych wprost w takie systemy jest bardzo dużo. Mogą być to ataki generowane przez konkurencję, działania motywowane chęcią uzyskania okupu za zaszyfrowane dane, wreszcie ataki prowadzone przez sfrustrowanych pracowników czy osoby, które zmieniając pracę, chcą wyprowadzić trochę wiedzy biznesowej.

Jak wygląda poziom bezpieczeństwa u klientów SAP w Polsce?

W Polsce istnieje duży rozstrzał kompetencyjny pod względem podejścia do bezpieczeństwa. Dobitnie widać to w obszarze rozwiązań SAP. Niektóre organizacje nie mają dziś żadnych działów bezpieczeństwa, a kwestiami tymi zajmują się – niejako przy okazji – administratorzy SAP. Istnieją także firmy, które dysponują działem obsługi SAP i bezpieczeństwa, ale najczęściej są to dwa różne światy, które nie komunikują się ze sobą. Niewiele jest natomiast organizacji, w których te dwa działy współpracują ze sobą na bieżąco.

Dlaczego bezpieczeństwo systemów SAP jest tak często bagatelizowane?

Po pierwsze, kiedyś bezpieczeństwo środowisk SAP było tematem tabu, a wiedza na ich temat wśród hakerów należała do rzadkości. Bardzo wąska grupa osób na świecie zajmowała się włamywaniem do nich. Nie było również GitHuba i publikowanych publicznie informacji o lukach w oprogramowaniu SAP. W efekcie, szansa na to, że konkretna instalacja SAP stanie się celem ataku była niewielka.

Poza tym kiedyś SAP był systemem monolitycznym, napisanym we własnej technologii i nie korzystał z rozwiązań open source czy produktów firm trzecich. Dziś to się zmieniło. Niektóre elementy środowiska SAP są tworzone np. w Javie i wystawiane do internetu. Pokazał to przykład luki Log4Shell, która została wykorzystana do ataków na systemy SAP. Faktem jest, że SAP co miesiąc udostępnia poprawki i noty

bezpieczeństwa usuwające znane luki, ale hakerzy są znacznie szybsi. Jeśli uda im się wykorzystać taką lukę i dostać do wnętrza środowiska SAP, to jest to zagrożenie o charakterze krytycznym dla biznesu.

Druga kwestia to podejście do projektów zakładających wdrożenie oprogramowania SAP. Projekty takie są realizowane po to, aby pozyskać określoną funkcjonalność biznesową, ale w czasie przygotowań do takich wdrożeń mało czasu poświęca się aspektom związanym z technologią czy bezpieczeństwem. Wdrożenie jest realizowane szybko, a elementy istotne pod względem wzorcowej konfiguracji SAP oraz bezpieczeństwa są często pomijane, bo nie ma na nie czasu ani budżetu. Praktyka pokazuje, że środowiska SAP w Polsce wymagają dużo pracy, aby były idealnie zabezpieczone.

Które elementy środowiska SAP są najbardziej narażone na działania cyberprzestępców?

Wszystko zależy od konkretnej instalacji SAP, serwera aplikacyjnego, bazy danych, a nawet systemu operacyjnego serwera oraz SAP GUI. Jeśli nie zostały ściśle zdefiniowane uprawnienia, to wiele można „zepsuć" nawet z poziomu zwykłego użytkownika. Przykładowo, w 2022 roku wykryty został błąd, który pozwalał na wykonanie z kodu ABAP każdej komendy systemu operacyjnego z uprawnieniem administratora. Dawało to niewątpliwie duże możliwości ewentualnym atakującym.

Najciekawsze dane pozostają jednak we wnętrzu SAP. To, że atakujący uruchomi coś na systemie operacyjnym serwera, to może zdestabilizować działanie środowiska SAP, ale newralgiczne dane pozostaną w tabelach bazy danych SAP. Co innego, jeśli haker potrafi poruszać się wewnątrz świata SAP. Wówczas jest w stanie wydobyć wiele krytycznych informacji. Tego typu eskalacje najczęściej odbywają się przez serwer aplikacyjny, bo dostęp z poziomu bazy danych jest trudniejszy do zrozumienia przez średniej klasy hakera. Z poziomu serwera aplikacyjnego dostęp jest łatwiejszy.

Trzeba zatem chronić dostęp do systemu SAP, a tu przychodzi z pomocą promowana powszechnie polityka zero-trust, która zakłada, że ufamy tylko urządzeniom,

> SecurityBridge zapewnia skanowanie kodu ABAP pod kątem podatności. Jest więc w stanie wykryć potencjalne luki bezpieczeństwa powstałe – lub umieszczone celowo – bezpośrednio w kodzie aplikacyjnym SAP.

które znamy i użytkownikom, którzy się właściwie uwierzytelnią. Jeśli mamy to dobrze uszczelnione, to trudno jest włamać się do systemu SAP z zewnątrz organizacji. Nadal jednak spotykamy firmy, które mają wystawiony serwer bazodanowy razem z aplikacyjnym, więc nawet osoba nieposiadająca dostępu do SAP widzi te serwery w sieci wewnętrznej, co samo w sobie pozwala jej na podjęcie określonych działań.

W jakim stopniu bezpieczeństwo systemów SAP jest zależne od sposobu ich wdrożenia?

Mamy dziś trzy główne modele wykorzystania oprogramowania SAP. Pierwszy, znany od lat i najczęściej stosowany w Polsce, to model on-premise, który zakłada, że dana organizacja ma własne środowisko i to w ramach tego środowiska utrzymuje system SAP. W tym modelu poziom bezpieczeństwa oprogramowania i danych krytycznych jest w rękach osób, które tym środowiskiem zawiadują.

Drugi model zakłada wykorzystanie modelu chmurowego. Polskie firmy coraz częściej decydują się na używanie rozwiązań SAP na bazie zasobów udostępnianych w ramach tzw. publicznej chmury obliczeniowej – choćby na potrzeby obsługi wybranych modułów oprogramowania SAP, jak DRC lub HA, czy środowisk dewelopersko-testowych. W tym podejściu, jeśli chodzi o bezpieczeństwo, jest o tyle łatwiej, że jesteśmy w stanie bardzo szybko stworzyć środowisko i podpiąć pod nie różne mechanizmy bezpieczeństwa oferowane przez dostawcę usług chmury. Jako partner Microsoft mamy bardzo mocno rozeznane wszystkie narzędzia tej firmy, które można w łatwy i szybki sposób wdrożyć, aby podnieść poziom bezpieczeństwa SAP, nie angażując w to wszystkich zespołów IT w organizacji.

Trzecim podejściem jest oferta RISE with SAP. Zakłada ona model, w którym to SAP bezpośrednio oferuje klientom dostęp do oprogramowania SAP opartego na wybranej platformie chmurowej na zasadzie subskrypcji. W tym podejściu to producent, a zarazem dostawca usługi, dostarcza klientom mechanizmy zabezpieczające, aczkolwiek one także wymagają świadomego użycia, ponieważ nie zawsze mogą pasować do potrzeb danej firmy oraz polityk bezpieczeństwa.

Mamy już zapytania o przeglądy bezpieczeństwa bądź testy penetracyjne środowisk RISE with SAP – i takie projekty realizujemy, sprawdzamy, czy wszystkie mechanizmy oferowane przez SAP rzeczywiście są wdrożone i czy działają jak należy. Niezależnie od tego, że SAP w modelu RISE with SAP jest rozwiązaniem zarządzanym przez producenta, to takie instalacje także wymagają obsługi technologicznej od osób, które rozumieją charakterystykę danego projektu.

W jaki sposób SNOK prowadzi analizy poziomu bezpieczeństwa systemów SAP?

Nie jest naszą rolą wykonywanie przeglądów bezpieczeństwa całej organizacji, czyli przełamywanie się z zewnątrz do środka. Funkcjonujemy jako zaufana firma, działająca w ramach środowiska klienta. Wychodzimy więc od poziomu zewnętrznego konsultanta dysponującego najmniejszymi uprawnieniami albo osoby, która jest w stanie wpiąć komputer do sieci wewnętrznej – i na tej podstawie badamy co można zrobić.

Wchodząc do sieci wewnętrznej, widać jak na dłoni wszystkie serwery SAP, wówczas szukamy dziur po kolei na różnych poziomach – od systemu operacyjnego, przez bazę danych, po serwer aplikacyjny. Jeśli z powodzeniem zamkniemy ten etap ana-

> Dzisiaj systemy SAP generują bardzo dużo informacji, także do systemów SIEM. Dane te są jednak najczęściej niezrozumiałe dla nich. Dlatego zaoferowaliśmy produkt, który jest w stanie podnieść bezpieczeństwo rozwiązań SAP, jak również wykrywa próby włamań.

lizy, to kolejnym krokiem naszych działań jest dokonanie przeglądu bezpieczeństwa w roli konsultanta z najmniejszymi uprawnieniami SAP – i tu zwykle jest ogromne pole do popisu. Działamy delikatnie i pokazujemy wszystko, co można zrobić. Jesteśmy w stanie udowodnić swoje obserwacje, ale w tym zakresie najczęściej korzystamy ze środowisk testowych. Unikamy bowiem działań, które mogą zdestabilizować pracę systemu produkcyjnego.

Naprawdę jest to zwykle ciekawa przygoda, której w niektórych firmach towarzyszy wiele niespodziewanych odkryć. W grę wchodzą uprawnienia, które często są nieszczelne i udaje nam się zdobyć bardzo dużo. Stale zdarzają się domyślne hasła lub konta użytkowników. Często niezabezpieczone są też interfejsy integracyjne.

Poza odpowiednią konstrukcją aplikacji i wspomnianą weryfikacją treści podawanych za pośrednictwem różnego rodzaju interfejsów graficznych, kluczowe znaczenie ma odpowiednia budowa ról i uprawnień w systemie SAP. Trzeba przyznać, że ten obszar w polskich firmach nie wygląda dziś najgorzej, ponieważ architektura uprawnień jest zwykle naturalną częścią większości projektów wdrożeniowych i rozwojowych związanych z oprogramowaniem SAP. Bywa jednak, że w samych uprawnieniach znajdują się luki pozwalające np. użytkownikom o najniższych uprawnieniach wykonywać komendy zewnętrzne lub debugować kod. Jeśli takie luki istnieją w systemie testowym lub produkcyjnym, to wówczas włamywacz ma niemal otwartą drogę nawet do najbardziej newralgicznych obszarów środowiska SAP.

Kiedy jest najlepszy moment na podjęcie działań zmierzających do poprawy bezpieczeństwa systemów SAP?

Właśnie teraz. Świat SAP stoi przed wyzwaniem zmiany wersji systemu, konwersji do S/4HANA czy platformy RISE with SAP. W większości przypadków są to wdrożenia typu greenfield, zakładające implementację od nowa. Przy tej okazji, warto rozważyć dodatkowy wysiłek pozwalający zagwarantować, że nowe środowisko będzie odpowiednio zabezpieczone i zaangażować firmę wyspecjalizowaną w bezpieczeństwie SAP. Działając niezależnie od dostawcy systemu, będzie ona w stanie wypracować odpowiednie reakcje na różnego rodzaju zdarzenia.

Taki przegląd jest pierwszym krokiem. W kolejnym – pomagamy opracować strategię bezpieczeństwa w obszarze SAP. Co z tego, że podłączymy system SAP do platformy SIEM i pojawi się alert, że użytkownik Kowalski próbuje wydobyć tabele z listą płac. Jeśli nie mamy odpowiednich procedur reagowania, nie mamy SOC, który jest w stanie właściwie zareagować na

tego typu zdarzenia, to nadal nie osiągniemy oczekiwanego efektu.

Kwestii bezpieczeństwa środowisk SAP powinny przyjrzeć się też te organizacje, które nie przewidują zmiany modelu wykorzystania albo wersji używanego oprogramowania. Dzisiaj systemy SAP generują bardzo dużo informacji, także do systemów SIEM. Dane te są jednak najczęściej niezrozumiałe dla takich narzędzi i większości specjalistów ds. bezpieczeństwa.

Dlatego zdecydowaliśmy się zaoferować na polskim rynku unikalny produkt, który jest w stanie bardzo szybko podnieść bezpieczeństwo rozwiązań SAP, jak również koreluje i wykrywa próby włamań. Tłumaczy także informacje płynące z systemu SAP na język zrozumiały dla działów bezpieczeństwa, a jednocześnie unifikuje strumienie logów, tak aby były one łatwiejsze do wykorzystania.

W 2021 roku firma SNOK została polskim przedstawicielem SecurityBridge. Jaką rolę pełni to rozwiązanie?

SecurityBridge to produkt, który zabezpiecza SAP w wielu aspektach – i pełni rolę platformy SIEM działającej w środowisku ABAP. W odróżnieniu od innych rozwiązań klasy SIEM, jest to rozwiązanie, które rozumie, co dzieje się w środowisku SAP. Poza tym platforma SecurityBridge nie wymaga dodatkowych, dedykowanych serwerów, bo może być zainstalowana na instancji SAP i jest w stanie ujednolicić strumień logów SAP, tak aby był on użyteczny dla korporacyjnych rozwiązań klasy SIEM, jak na przykład: QRadar, Splunk Enterprise Security czy Palo Alto.

Jest to o tyle ważne, że – jak powiedzieliśmy wcześniej – natywne logi SAP niewiele mówią zespołom i uniwersalnym systemom bezpieczeństwa. Bezpośrednie podłączenie systemu SAP do rozwiązania klasy SIEM nie poprawi czytelności obrazu bezpieczeństwa całego środowiska, ponieważ – jeżeli w audyt logów bezpieczeństwa włączone są wszystkie parametry SAP – to jest ich tak dużo, że nikt, kto pracuje jako operator SOC, nie będzie w stanie zrozumieć i skorelować wszystkich zawartych tam informacji.

> Platforma SecurityBridge nie wymaga dodatkowych, dedykowanych serwerów, bo może być zainstalowana na instancji SAP i jest w stanie ujednolicić strumień logów SAP, tak aby był on użyteczny dla korporacyjnych rozwiązań klasy SIEM, jak np.: QRadar, Splunk czy Palo Alto.

Platforma SecurityBridge konsoliduje informacje z logów SAP i w sposób czytelny komunikuje do środowiska SIEM przypadki naruszenia zdefiniowanych polityk bezpieczeństwa. Co ważne, SecurityBridge jest w stanie ograniczyć skalę logów o 80–90%, a zarazem generować logi zrozumiałe dla działów bezpieczeństwa.

W praktyce oprogramowanie SecurityBridge, w zautomatyzowany sposób koreluje zdarzenia i może wykryć próby włamania do systemu SAP. Poza tym jest w stanie np. zablokować użytkownika naruszającego reguły bezpieczeństwa bezpośrednio w środowisku SAP. W połączeniu z zewnętrznym rozwiązaniem klasy SIEM może inicjować bardziej daleko idące reakcje na potencjalne zagrożenia.

Czy oprogramowanie SecurityBridge oferuje coś jeszcze?

Drugą rozbudowaną funkcjonalnością SecurityBridge jest badanie poziomu bezpieczeństwa danej konfiguracji środowiska SAP. Ma bowiem stały dostęp do bazy wszystkich not bezpieczeństwa SAP, więc jest w stanie zweryfikować aktualność poszczególnych komponentów środowiska, a co więcej, może zainicjować wdrażanie krytycznych poprawek bezpieczeństwa w sposób niewpływający na dostępność systemu.

Równocześnie, SecurityBridge zapewnia skanowanie kodu ABAP pod kątem podatności. Jest zatem w stanie wykryć potencjalne luki bezpieczeństwa powstałe – lub umieszczone celowo – bezpośrednio w kodzie aplikacyjnym SAP. Poza tym, ABAP może okazać się dodatkowym wektorem ataków dokonywanym z poziomu przeglądarki internetowej i poprzez różnego rodzaju interfejsy użytkownika.

Platforma SecurityBridge jest także w stanie wykrywać wycieki danych. Dobrze jest więc pomyśleć o niej jako o produkcie, który jest instalowany w momencie rozpoczęcia wdrożenia lub reimplementacji SAP, tak aby analizować całą ścieżkę transportową pod kątem luk w kodzie ABAP. Ponadto SecurityBridge może też skanować interfejsy pod kątem potencjalnych podatności. Jest to o tyle cenne, że obecnie środowisko SAP bardzo często pozostaje otwarte na inne rozwiązania czy źródła danych.

Jakiego rodzaju usługi świadczy zespół firmy SNOK na bazie platformy SecurityBridge?

W odpowiedzi na zdefiniowane uprzednio potrzeby zajmujemy się kompleksowym uruchomieniem i konfiguracją SecurityBridge. Prowadzimy również projekty pilotażowe, które zakładają m.in. dwutygodniowe testy rozwiązania SecurityBridge w środowisku testowym klienta. Dzięki temu pokazujemy rzeczywiste możliwości tego rozwiązania u klienta.

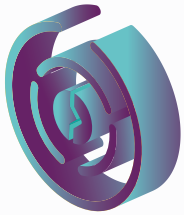
Zapewniamy też bieżące wsparcie, szkolenia i doradztwo w zakresie obsługi rozwiązania SecurityBridge oraz możliwości wykorzystania gromadzonej przez nie wiedzy pod kątem poprawy bezpieczeństwa infrastruktury danej organizacji. Jeśli firma nie dysponuje zasobami do przejęcia takich zadań, to jesteśmy w stanie przejąć odpowiedzialność za obszar bezpieczeństwa SAP.

Wywiad przeprowadził
Piotr Waszczuk

Nasza platforma,
Twoja chmura

platforma ochk

Wykorzystaj jej potencjał



Zabezpiecz dane przed cyberprzestępcami

Zapewnij zgodność z regulacjami

Zadbaj o suwerenność danych

Zbuduj rozwiązania hybrydowe

Zarządzaj infrastrukturą za pomocą kodu

www.platformaochk.pl