NIS2 nadchodzi regulacyjne tsunami

W związku z wojną w Ukrainie Polska należy do grupy państw najczęściej atakowanych w cyberprzestrzeni. Mimo to prace nad wdrożeniem nowych reguł bezpieczeństwa systemów informatycznych się ślimaczą. Obecnie wiadomo już, że zakładany termin włączenia postanowień unijnej dyrektywy NIS2 do polskich przepisów nie zostanie dotrzymany. A pod względem nowych wymagań dla szerokiej grupy podmiotów te regulacje są prawdziwą rewolucją.

Pod presją zagrożeń ze strony profesjonalnych grup przestępczych oraz potencjalnej wojny w cyberprzestrzeni i aktów elektronicznego sabotażu, Unia Europejska zdecydowała o potrzebie zaostrzenia przepisów regulujących odporność biznesową w zakresie systemów IT. Obowiązująca od sześciu lat dyrektywa NIS (Network and Information Systems Directive), która przestała już być aktualna, została zastąpiona przez NIS2.

Nowe przepisy wprowadzają istotne zmiany w porządku prawnym – w szczególności znacznie poszerzają krąg instytucji i firm, które będą podlegać nowym regulacjom. Co więcej, wprowadzają również bardzo wysokie kary

Piotr Kościelniak
dziennikarz, popularyzator nauki

finansowe dla osób na kierowniczych stanowiskach, które nie dostosują swoich organizacji do postanowień NIS2.

> *Analizy rynkowe wskazują, że menedżerowie bardzo wielu firm, których zmiany będą dotyczyć, nie mają pojęcia o skali nadchodzącego wyzwania.*

Sytuację komplikuje dodatkowo fakt, że jeszcze nie zostały przyjęte przepisy wdrażające NIS2 do polskiego systemu prawnego i wyjaśniające wątpliwości co do interpretacji zapisów zawartych w dyrektywie. Wszystko to sprawia, że wdrożenie NIS2 może przynieść w najbardziej optymistycznym wariancie chaos, a w pesymistycznym – katastrofę.

Liczba ataków rośnie

Jednocześnie wzrasta zagrożenie cyberatakami prowadzonymi zarówno przez grupy hakerów działających dla zysku, jak i wysokospecjalizowanych sabotażystów pracujących na zlecenie nieprzyjaznych nam państw – głównie Rosji i Białorusi.

Według badań KPMG prawie dwie trzecie polskich firm w 2023 r. zarejestrowało incydent cyberbezpieczeństwa – jest to o 8 proc. więcej niż w roku poprzednim. Co dziesiąta firma odnotowała ponad 30 prób ataku, a co trzecia przyznała, że widzi wzrost intensywności cyberataków na swoją infrastrukturę.

Z kolei raport Pełnomocnika Rządu ds. Cyberbezpieczeństwa informuje o 80 tys. incydentów „obsłużonych" w 2023 r., co oznacza dwukrotny wzrost. Dane z pierwszego kwartału tego roku wskazują, że fala ataków wcale nie opada – prawdopodobnie w 2024 r. pobijemy nowy rekord aktywności hakerów. Zagrożenie dotyczy zarówno organizacji związanych z obronnością i MON, jak również producentów broni w Polsce. Dane z pierwszego kwartału tego roku wskazują, że liczba ataków na polską infrastrukturę nadal rośnie.

Wojna w Ukrainie, tocząca się nie tylko na konwencjonalnym polu walki, lecz także w cyberprzestrzeni, pokazała nam, które cele będą dla przeciwników atrakcyjne oraz jakimi metodami się posłużą. Na początku maja br. polskie instytucje rządowe zostały narażone na szkodliwe oprogramowanie, rozprowadzane przez grupę hakerów APT28, powiązaną ze służbami wywiadowczymi Rosji (informacja NASK-u). Co zaskakujące, wyrafinowani hakerzy z takich grup wydają się stosować dość prymitywne metody ataku, np. DDoS czy infekowanie komputerów oprogramowaniem kasującym dane. Popularne na terenie Polski są akcje phishingowe skierowane przeciw osobom korzystającym z usług Poczty Polskiej czy paczkomatów.

Na celowniku hakerów w Polsce znaleźli się przede wszystkim operatorzy energetyczni i telekomunikacyjni oraz firmy sektora finansowego, użyteczności publicznej, logistyczne, z branży spożywczej oraz media.

Gdy powstawał ten tekst, w ostatnim dniu maja br., w serwisie Polskiej Agencji Prasowej ukazała się nieprawdziwa depesza o częściowej mobilizacji zarządzonej w Polsce: „1 lipca 2024 roku ogłoszona zostanie w Polsce częściowa mobilizacja wojskowa. 200 tysięcy obywateli Polski, zarówno byłych wojskowych, jak i zwykłych cywilów zostanie powołanych do obowiązkowej służby wojskowej. Wszyscy zmobilizowani zostaną wysłani na Ukrainę". Zdaniem Ministra Cyfryzacji, Krzysztofa Gawkowskiego, wszystko wskazuje na to, że atak na PAP był prowadzony przez Federację Rosyjską, która dwa tygodnie wcześniej próbowała zrealizować włamanie i incydent na infrastrukturze krytycznej kraju.

Hakerzy zaczęli również celować w całe łańcuchy dostaw, szukając słabych punktów i możliwości masowej infekcji wszystkich firm korzystających ze sprzętu i usług zaatakowanych dostawców. W lutym 2024 r. około 100 szpitali w Rumunii padło ofiarą ransomware. Incydent był spowodowany atakiem na łańcuch dostaw. Hakerzy najpierw uzyskali dostęp do opracowanego przez zewnętrznego dostawcę systemu informatycznego do zarządzania procedurami medycznymi, dopiero za jego pośrednictwem mogli dostać się do sieci szpitalnych.

> *Właśnie za sprawą takich zagrożeń wymagania NIS2 obejmują nie tylko firmy działające w konkretnych sektorach, lecz również ich łańcuchy dostaw – wszystkich dostawców, podwykonawców i partnerów dostarczających sprzęt i usługi związane z IT i przetwarzaniem danych.*

Kto musi zacząć działać

Najważniejszym celem NIS2 jest podwyższenie poziomu ochrony danych w firmach działających na terenie Unii Europejskiej. Nowe przepisy stawiają w równej mierze na cyberbezpieczeństwo i zarządzanie ryzykiem, jak i na zapewnienie ciągłości działania instytucji i przedsiębiorstw. W tym celu państwa muszą opracować i wdrożyć krajową strategię cyberbezpieczeństwa bazującą na zasadach zawartych w NIS2. Strategia może odbiegać od postanowień dyrektywy, ale tylko wtedy, gdy przyjęte przez państwo zasady

będą jeszcze bardziej rygorystyczne. W ten sposób Unia chce zapewnić wspólny minimalny poziom bezpieczeństwa i gotowości na cyberataki.

Jednak chyba najistotniejsza zmiana NIS2 – i potencjalnie największe źródło problemów – to poszerzenie katalogu podmiotów objętych przepisami o cyberodporności. W miejsce operatorów usług kluczowych i dostawców usług cyfrowych (oraz podmiotów publicznych z Ustawy o Krajowym Systemie Cyberbezpieczeństwa w rygorze „starej" NIS) NIS2 wprowadza podmioty kluczowe i ważne. I o ile poprzednie rozwiązanie zakładało, że to odpowiednie organy państwa wskazują operatorów usług kluczowych, o tyle nowe przepisy wprowadzają zasadę samookreślenia.

> *A to oznacza, że to same organizacje i firmy będą oceniały, czy ich pozycja i wielkość sprawiają, że obowiązują ich regulacje NIS2. Jeśli ocenią źle, zostaną ukarane.*

NIS2 z założenia dotyczy firm dużych i średnich (powyżej 50 zatrudnionych, których roczny obrót przekracza 10 mln euro). W szczególnych przypadkach regulacjami mogą zostać objęte firmy mniejsze, o ile pełnią istotną funkcję dla społeczeństwa, działając w określonych sektorach gospodarki. Mogą to być nawet firmy małe – takie jak dostawcy usług DNS, usług weryfikacji tożsamości czy podpisów elektronicznych. Biorąc pod uwagę, że regulacje te obejmują również łańcuchy dostaw, może się okazać, że dopasować się do europejskich przepisów o cyberbezpieczeństwie będą musiały organizacje, które nie mają nawet własnych menedżerów ds. bezpieczeństwa danych czy wręcz korzystają z zewnętrznych usług w tej dziedzinie.

Kluczowe i ważne

Nowa dyrektywa wprowadza rozróżnienie na podmioty kluczowe oraz ważne. Podmioty kluczowe dostarczają usługi niezbędne do funkcjonowania gospodarki i społeczeństwa. To działalność w takich obszarach, jak: finanse i bankowość, ochrona zdrowia, energetyka, transport, kosmos, woda pitna, ścieki, infrastruktura cyfrowa i zarządzanie usługami ICT oraz administracja publiczna. Z założenia podmioty działające w tych sektorach będą uznane za kluczowe, jeżeli są wystarczająco duże (pod względem zatrudnienia i obrotów – ponad 250 osób i 50 mln euro obrotu).

Organizacje średnie działające w tych sektorach będą traktowane jako ważne, jeżeli ich działalność ma istotny wpływ na gospodarkę Unii Europejskiej. W tej kategorii znalazły się również podmioty średnie i duże działające w innych sektorach – na przykład świadczące usługi kurierskie i pocztowe, gospodarujące odpadami, produkujące lub dystrybuujące chemikalia oraz żywność, firmy produkcyjne i instytucje naukowe.

Czym różnią się podmioty kluczowe od ważnych? W praktyce opisywanej przez NIS2 jedynie trybem nadzoru. W przypadku podmiotów ważnych stosowany jest tzw. nadzór uproszczony, aktywowany dopiero po stwierdzonym incydencie bezpieczeństwa. Natomiast w przypadku podmiotów kluczowych nadzór oznacza m.in. regularne audyty i wyrywkowe kontrole.

No i wreszcie kary. Te są bardzo wysokie. Na podmioty kluczowe odpowiedni organ może nałożyć karę finansową sięgającą 10 mln euro lub co najmniej 2 proc. rocznego światowego obrotu – zastosowanie ma kwota wyższa. Podmioty ważne zagrożone są grzywnami 7 mln euro lub 1,4 proc. rocznego światowego obrotu. Słone opłaty nie wyczerpują katalogu środków dyscyplinujących. Na podmioty nieprzestrzegające postanowień dyrektywy organy nadzorcze mogą nałożyć nakazy, obowiązek wykonania audytu bezpieczeństwa, a także powiadomienia klientów o zagrożeniach, co potencjalnie może zrujnować reputację firmy.

Dyrektywa przewiduje również dotkliwe kary dla osób odpowiedzialnych za zaniedbania. Menedżerowie, którzy dopuścili do rażących naruszeń w obszarze cyberbezpieczeństwa, mogą spodziewać się upublicznienia informacji o naruszeniach (wraz z imiennym wskazaniem osoby odpowiedzialnej) oraz czasowego zakazu pełnienia stanowisk kierowniczych (dotyczy to podmiotów kluczowych). Celem tych przepisów jest odciążenie specjalistów IT i przełożenie odpowiedzialności o poziom wyżej – na członków zarządu, nadzorujących ich działanie i decydujących np. o budżecie na cyberbezpieczeństwo.

Błoga nieświadomość

Brzmi groźnie? Wielu polskich menedżerów zdaje się nie dostrzegać zagrożenia. 20 kwietnia 2024 r. w naszym kraju zarejestrowanych było 397 operatorów usług kluczowych. Po wprowadzeniu w życie regulacji NIS2 liczba organizacji, które mogą być sklasyfikowane jako podmioty ważne, zbliży się do 4 tys. – wynika z szacunkowych danych T-Mobile. W tej liczbie nie mieszczą się jednak firmy tworzące łańcuchy dostaw dla podmiotów ważnych. Rzeczywisty krąg podmiotów, które zostaną objęte regulacjami (i potencjalnie karane za niedostosowanie się do przepisów), może być zatem znacznie większy.

Problem z brakiem świadomości polskich menedżerów o nadchodzącej rewolucji w cyberbezpieczeństwie najlepiej ilustruje raport sporządzony przez CSO Council, EY i Trend Micro „W oczekiwaniu na NIS2: stan przygotowań". Jedna czwarta firm, z których wywodzili się ankietowani menedżerowie, nie wie, czy NIS2 ich obejmie i nie planuje w tej sprawie żadnych działań. Sektory gospodarki objęte wcześniej takimi regulacjami są dobrze przygotowane na

zmiany, jednak dla przedsiębiorstw zajmujących się handlem, logistyką czy produkcją obowiązki dotyczące cyberodporności to całkowita nowość.

Dla menedżerów IT największym problemem pozostaje brak implementacji postanowień NIS2 do polskiego systemu prawnego (nowelizacja ustawy o KSC) i tym samym brak wiedzy o szczegółowych rozwiązaniach – te dopiero niedawno się pojawiły w postaci projektu rządowego. Aż dwie trzecie nie wie, czy pozostały czas do wdrożenia rozwiązań dyrektywy jest wystarczający, bo nie znają szczegółowych rozwiązań. Co najciekawsze, prawie połowa (45 proc.) menedżerów biorących udział w ankiecie dotyczącej przygotowań do NIS2 nie wie, co to znaczy „być zgodnym" z postanowieniami dyrektywy.

Na ten problem zwracali również uwagę prawnicy obecni na konferencji Advanced Threat Summit 2023. Specjaliści ds. bezpieczeństwa danych i informatycy zwracali się do nich z prośbą o wyjaśnienie, w jaki sposób postanowienia dyrektywy przekładają się na realne rozwiązania. Na to pytanie trudno udzielić odpowiedzi, jeżeli nie ma obowiązujących przepisów krajowych.

Sposobem na przynajmniej częściowe rozwiązanie problemu braku świadomości menedżerów i specjalistów IT ma być akcja informacyjna prowadzona przez Ministerstwo Cyfryzacji. Wkrótce ma powstać strona internetowa z informacjami o NIS2, która pomoże podmiotom potencjalnie objętym NIS2 w samookreśleniu się. Również Polskie Towarzystwo Informatyczne zadeklarowało pomoc w przeprowadzeniu takiej kampanii informacyjnej, ze szczególnym uwzględnieniem jednostek samorządu terytorialnego.

– *Niezwykle istotne jest, by dotrzeć z prostym przekazem do wszystkich, którzy powinni być świadomi, co ich czeka* – mówił podczas webinaru PTI „Wdrożenie dyrektyw NIS2, CER" Krzysztof Silicki, główny doradca ds. cyberbezpieczeństwa, NASK i członek Rady ds. Cyfryzacji. – *Na szczęście w kwestii infrastruktury krytycznej nie zaczynamy od zera. Ale mamy też świadomość, że wprowadzenie tych zasad dla tak wielu nowych podmiotów może być bolesne. Oprócz regulacji i rozporządzeń są bowiem jeszcze zalecenia na przykład ws. reagowania Unii na zagrożenia infrastruktury krytycznej czy zalecenia postępowania w przypadku incydentów dużej skali i kryzysów. To jeszcze komplikuje i tak bardzo złożony krajobraz.*

Luka kadrowa na lata

Problem polskich przedsiębiorstw i instytucji potęguje obecna sytuacja na rynku pracy specjalistów ds. bezpieczeństwa informatycznego. Od wielu lat w tej dziedzinie nic się nie zmienia – to znaczy ekspertów brak i nic nie wskazuje na to, aby przed „godziną 0" miało się to zmienić. A to nie wróży dobrze tym, którzy pozostawiają sprawy cyberodporności na ostatnią chwilę.

Ten problem dostrzegli paneliści webinarowej dyskusji na temat wdrożeń NIS2 i CER. – *Niedostatek specjalistów ds. cyberbezpieczeństwa jest istotnym problemem. Przy dzisiejszym systemie szkolenia zaspokojenie potrzeb kadrowych w tej dziedzinie zajmie kilkadziesiąt lat* – podkreślał Wiesław Paluszyński, prezes Polskiego Towarzystwa Informatycznego. – *Potrzebne są szkolenia dla ludzi w podmiotach objętych NIS2. To musi być system szkoleń, który skończy się certyfikacją. Szkolenia, po których nie mamy potwierdzenia kompetencji, są zbędne.*

Pewną nadzieję uczestnicy spotkania upatrywali w rozwoju usług chmurowych, dzięki którym można szybko uruchomić np. SOC (Security Operations Center), korzystając z wykwalifikowanej kadry dostawcy takiej usługi, na co zwracał uwagę Marcin Karczmarczyk, dyrektor zarządzający Operatora Chmury Krajowej. Przypominał również, że rozwiązania chmurowe pozwoliły w znacznej mierze uchronić dane i zapewnić funkcjonowanie wielu systemów w Ukrainie.

Październik będzie w lipcu

Zgodnie z harmonogramem nowe przepisy zaczną obowiązywać 17 października 2024 r., jednocześnie zostaną uchylone postanowienia starej dyrektywy. Od 18 października w zasadzie powinniśmy znaleźć się już w nowej rzeczywistości, jeżeli chodzi o cyberbezpieczeństwo.

Tyle że nie ma najmniejszych szans, aby te przepisy – nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa – pojawiły się przed październikiem. Projekt nowelizacji zmieniającej ustawę o Krajowym Systemie Cyberbezpieczeństwa i implementujący postanowienia NIS2 do polskiego prawa liczy obecnie 129 stron. Pod obrady rządu trafił dopiero 24 kwietnia br., a miesiąc później zakończył się proces konsultacji społecznych.

Według wiceministra cyfryzacji Pawła Olszewskiego, dokument ma zostać przyjęty przez Radę Ministrów w III kw., a do końca tego roku zostanie uchwalony przez Sejm. Oznacza to, że krajowe rozwiązania będą opóźnione w stosunku do zakładanego w NIS2 harmonogramu. Ale to nie koniec – kolejny miesiąc przewidziano na wejście przepisów w życie, a podmioty objęte regulacjami będą miały jeszcze pół roku na wdrożenie zmian. Ministerstwo Cyfryzacji jest świadome opóźnienia, które sprawi, że najistotniejsze europejskie regulacje dotyczące bezpieczeństwa cyfrowego będą w Polsce martwe.

Projekt prawie nowy

Według ministra cyfryzacji Krzysztofa Gawkowskiego projekt składa się w 70 proc. z nowości, a w 30 proc. – z dojrzałości. Podmioty kluczowe i ważne (o tym, które są które i czy w ogóle obowiązuje je NIS2 będą musiały zdecydować same) będą mogły zarejestrować się w nowym systemie. Mają one otrzymać pomoc ze strony CSIRT-ów sektorowych

i poziomu krajowego. Menedżerowie z podmiotów kluczowych i ważnych odpowiedzialni za wdrożenia z zakresu cyberbezpieczeństwa będą musieli obowiązkowo (pod groźbą kary) przejść specjalne szkolenia.

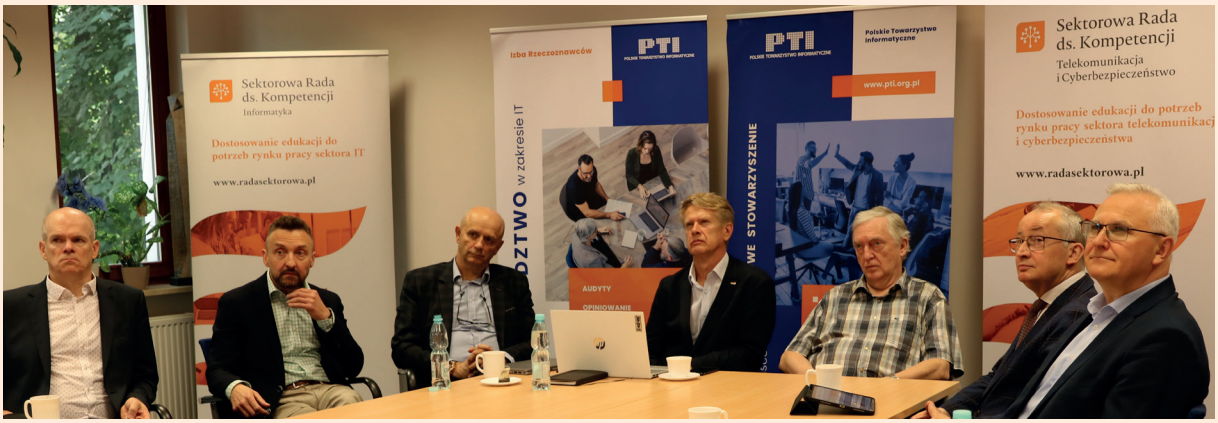
Firmy i instytucje będą musiały przygotować kompleksowy system zarządzania bezpieczeństwem informacji. Podmioty kluczowe i ważne zostaną zobowiązane do regularnych audytów bezpieczeństwa – w obecnej wersji projektu co dwa lata. Będą również musiały korzystać z systemu S46 jako głównego środka komunikacji między podmiotami objętymi KSC. Ma to być kanał pozwalający wymieniać wszystkie informacje o incydentach cyberbezpieczeństwa i wykrytych podatnościach. System S46 przejdzie istotną zmianę – oprze się na rozwiązaniach chmurowych, dzięki czemu znikną ograniczenia w przesyłaniu dokumentów i utrudnienia w dostępie. Do systemu trzeba się będzie podłączyć w terminie trzech miesięcy.

Projekt nowelizacji wprowadza również krótkie terminy raportowania o incydentach. Na przykład operator telekomunikacyjny będzie miał na to maksymalnie 12 godzin (inne podmioty kluczowe i ważne – 24 godziny).

Jak jednak podkreślał podczas webinaru PTI Marcin Wysocki, wicedyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, to dopiero projekt, a mimo formalnego zakończenia konsultacji poprawki w nim są nadal procedowane. – *Staramy się przeprowadzić procesy sprawnie i rzetelnie. Sama dyrektywa nie wiąże bezpośrednio podmiotów, konieczna jest implementacja do polskiego prawa* – tłumaczył. – *Dostaliśmy ponad 70 uwag przekładających się na setki stron tekstu w ramach konsultacji publicznych. Wynika z nich m.in., że powinniśmy trzymać się na poziomie minimalnej harmonizacji, czyli nie nakładać dalej idących obowiązków, niż przewiduje to NIS2.*

Marcin Wysocki przyznał również, że wiele firm potencjalnie znajdujących się w obszarach regulowanych przez NIS2 chciałoby mniej rygorystycznych zasad. – *Będziemy również zastanawiać się, czy dla podmiotów ważnych wymogi regulacyjne nie powinny być niższe – i czy jest to możliwe z punktu widzenia organów Unii Europejskiej.*

Przy okazji (bazując na unijnym zestawie środków dla cyberbezpieczeństwa sieci 5G, tzw. Toolbox 5G) zmieniono również bardzo istotny zapis dotyczący tzw. dostawców wysokiego ryzyka, czyli dostawców sprzętu i oprogramowania telekomunikacyjnego i komputerowego z Chin. O tym, kto jest „podejrzany", będzie decydował minister cyfryzacji. A firmy korzystające z usług takich dostawców zyskają dodatkowy czas na wymianę sprzętu i oprogramowania – w ostatniej wersji projektu mają na to 4 lata lub nawet 7 lat.



Wdrożeniu dyrektyw NIS2, CER poświęcony był czerwcowy webinar z cyklu „Prezesi zapraszają...", zorganizowany przez Polskie Towarzystwo Informatyczne i Związek Cyfrowa Polska. Uczestnicy spotkania od lewej: Paweł Krakowian (IT Solutions' Architect, HPE), Marcin Karczmarczyk (dyrektor zarządzający, Operator Chmury Krajowej), Wiesław Łodzikowski (dyrektor Biura Infrastruktury IT PKN Orlen), Jarosław Mojsiejuk (Rada ds. Cyfryzacji), moderator panelu, Wiesław Paluszyński (prezes Polskiego Towarzystwa Informatycznego), Witold Skomra (Rządowe Centrum Bezpieczeństwa) , Kazimierz Mordaszewski (dyrektor Departamentu Bezpieczeństwa i Zarządzania Kryzysowego, Ministerstwo Aktywów Państwowych).

Zdalny udział w spotkaniu wzięli: Jacek Łęgiewicz (Cyfrowa Polska), Krzysztof Silicki (główny doradca ds. cyberbezpieczeństwa, NASK, członek Rady ds. Cyfryzacji), Marcin Wysocki (wicedyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji).