Informacja prasowa Gdańsk, 6 listopada 2024

**Firmy, pracownicy i milionowe kary za błędy w cyberbezpieczeństwie w 17 branżach**

**Wdrożenie unijnej dyrektywy NIS2 z zakresu cyberbezpieczeństwa, której implementacja w Polsce obejmie niebawem kilkadziesiąt tysięcy podmiotów z 17 sektorów, stawia przed krajowymi firmami istotne wyzwania organizacyjne, finansowe i technologiczne. Organy zarządzające będą musiały zwiększyć świadomość ryzyka i wdrożyć odpowiednie środki techniczne, operacyjne oraz organizacyjne, a także zadbać o politykę analizy ryzyka, obsługę incydentów, zarządzanie kryzysowe oraz bezpieczeństwo informatyczne łańcucha dostaw. Firmy będą musiały też położyć większy nacisk na cyberhigienę pracowników oraz przeszkolić kadrę, która – jak wynika z badania Grupy Progres – nie zawsze przestrzega zasad cyberbezpieczeństwa. Za złamanie przepisów będą groziły surowe kary finansowe, sięgające nawet 10 mln euro lub 2% rocznego obrotu. Nie ominą one również kierowników organizacji, którzy za swoje błędy mogą zapłacić karę w wysokości do 600% otrzymywanego wynagrodzenia.**

Wprowadzenie Dyrektywy NIS2 stanowi jedno z największych wyzwań regulacyjnych w zakresie cyberbezpieczeństwa, jakie do tej pory dotknęły polskie przedsiębiorstwa i instytucje. Nowe przepisy, nie tylko nakładają na firmy obowiązek spełnienia restrykcyjnych norm, ale także przenoszą znaczną część odpowiedzialności na organy zarządzające. W praktyce oznacza to, że członkowie zarządów będą musieli być świadomi ryzyka, jakie czyha w sieci oraz zapewnić odpowiednie zabezpieczenia. Czeka to ich już niebawem. 7 października ukazała się druga wersja projektu nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa („Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw”), która wprowadza do polskiego prawa unijną dyrektywę. Ministerstwo zapowiada, że do końca 2024 r. ma on zostać przyjęty przez Radę Ministrów, a następnie skierowany do parlamentu, aby nowe przepisy mogły wejść w życie na początku 2025 r.

**Długa lista wymogów**

W dobie coraz częstszych i bardziej zaawansowanych ataków w sieci, walka z nimi jest niezwykle istotna. Szczególnie, gdy weźmiemy pod uwagę ich skalę. Z danych Ministerstwa Cyfryzacji opublikowanych w połowie kwietnia 2024, wynika, że Polska znajduje się wśród 3 najbardziej atakowanych krajów na świecie, a liczba incydentów dotyczących cyberbezpieczeństwa wzrosła w ciągu roku (2022 do 2023) o prawie 200 proc. (z 30 tys. do 80 tys. rocznie).

– *Liczby dot. cyberataków mówią same za siebie, dlatego obowiązek wdrożenia rozbudowanych procedur na szeroką skalę jest konieczny. W przepisach, które już niebawem mają wejść w życie, obejmie on szeroką gamę branż, a to oznacza, że polski rynek staje przed ogromnym wyzwaniem dostosowania się do nowych wymogów, szczególnie w organizacjach, które wcześniej mogły nie traktować cyberbezpieczeństwa jako priorytetu –* **mówi Magda Dąbrowska, wiceprezeska Grupy Progres***.* – *Ich obowiązkiem już niebawem będzie wdrożenie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w firmie oraz zgłaszanie incydentów sieciowych.* *Lista wymogów jest długa, a przed zarządzającymi organizacjami i ich pracownikami poważne wyzwanie*, *szczególnie że – wbrew pozorom – na wdrożenie zmian nie ma zbyt dużo czasu* – **dodaje Magda Dąbrowska.**

Podmioty objęte nowymi przepisami zostaną zobligowane do zapewnienia swojej organizacji m.in. polityki analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługi incydentu, ciągłość działania czy zarządzania kryzysowego. Na liście wymaganych przepisami działań znajduje się też polityka i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie, podstawowe praktyki cyberhigieny i szkolenia z jej zakresu oraz bezpieczeństwo zasobów ludzkich, polityki kontroli dostępu i zarządzania aktywami.

Jednym z kluczowych aspektów nowych regulacji jest też zarządzanie ryzykiem w łańcuchach dostaw. W swojej prognozie cyberzagrożeń na 2030 rok ENISA przewiduje, że naruszenia bezpieczeństwa łańcucha dostaw będą w ciągu najbliższych lat jednym z najbardziej prawdopodobnych cyberzagrożeń. Nowe regulacje wychodzą naprzeciw tym przewidywaniom i zobowiązują podmioty do wdrożenia polityki bezpieczeństwa dostaw, w tym rygorystycznych kryteriów oceny, monitoringu oraz zabezpieczeń dostawców usług ICT. Przy wyborze dostawców, zwłaszcza chmurowych, kluczowa będzie analiza ich reputacji, gwarancji SLA, prawa do audytu, standardów bezpieczeństwa i certyfikacji.

**Pracownicy do przeszkolenia, co czwarty nie przestrzega zasad**

*– Kluczowym pytaniem jest, na ile polskie firmy są gotowe na tak kompleksowe zmiany. Czy posiadają zasoby, technologie i wiedzę niezbędne do wdrożenia tych wymogów? Równie istotna jest też kwestia gotowości pracowników, którzy będą musieli dostosować się do nowych procedur i rozwijać swoje kompetencje cyfrowe –* **zaznacza Magda Dąbrowska, wiceprezeska Grupy Progres.** *–* *Niezbędne będą intensywne szkolenia i kampanie edukacyjne, aby zwiększyć świadomość zagrożeń oraz wypracować kulturę cyberbezpieczeństwa na wszystkich szczeblach organizacji. Dla wielu przedsiębiorstw wdrożenie tych wymogów może wiązać się nie tylko z dużymi nakładami finansowymi, ale także z koniecznością reorganizacji procesów, co może okazać się sporym wyzwaniem w krótkim czasie –* **podkreśla Magda Dąbrowska.**

To, jak istotnym elementem w całej układance są sami pracownicy potwierdzają też badania Grupy Progres, które ujawniają problematyczne podejście osób zatrudnionych w organizacjach do cyberhigieny. Mimo że 75% badanych twierdzi, że nie korzystało z prywatnego e-maila w celach służbowych, to co czwarty ankietowany – aż 25% – przyznaje się do takiego działania, często na prywatnej poczcie ma też firmowe pliki i dokumenty służbowe.

Wśród osób, które korzystały z prywatnego e-maila do wykonywania obowiązków służbowych większość robiła to kilka razy, a nawet nagminnie. Najczęściej robili to z powodów tj. awaria służbowej skrzynki czy firmowych serwerów, praca poza biurem, po godzinach lub w weekendy, przepełniona skrzynka e-mail czy brak dostępu do niej na wyjeździe.

Na pytanie, czy Twoim zdaniem korzystanie z prywatnego maila do załatwiania służbowych spraw i przesyłanie na nie plików jest dopuszczalnym działaniem? 70% badanych odpowiedziało, że jest ono niedopuszczalne, a 30% twierdzi, że można to robić np. w wyjątkowych sytuacjach.

**Kara również dla pracownika**

**Według Magdy Dąbrowskiej,** kary nie są najlepszym sposobem na skuteczne i mądre wdrożenie zasad oraz wyrobienie nawyków cyberhigieny, ale z pewnością – w wielu przypadkach – będą skuteczne. **Wiceprezeska Grupy Progres dodaje**, że ich wysokość może wydawać się niewspółmierna do przewinienia, ale nauczeni doświadczeniem – np. wyższymi mandatami i idącym w parze spadkiem przypadków naruszenia przepisów ruchu drogowego – możemy uznać, że w dłużej perspektywie ich wysokość ma szansę przynieść skutek w postaci stosowania się do zasad i przepisów dot. cyberbezpieczeństwa. Tym bardziej, że kwoty za łamanie prawa będą dotkliwe.

W nowych przepisach przewidziano kary do 10 mln EUR lub 2% przychodów dla podmiotów kluczowych oraz do 7 mln EUR lub 1,4% przychodów dla podmiotów ważnych. W szczególnych przypadkach kara może wynieść do 100 mln zł, gdy naruszenia stanowią zagrożenie dla bezpieczeństwa państwa lub życia i zdrowia ludzi. Nowelizacja z października wprowadza także kary dla kierowników podmiotu kluczowego lub ważnego w wysokości do 600% otrzymywanego przez niego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

Może on otrzymać ją, jeśli np. nie wykonał co najmniej jednego z przypisanych mu obowiązków, o których mowa w ustawie, nie wyznaczył odpowiedniej liczby osób do kontaktu z podmiotami kluczowymi lub podmiotami ważnymi, albo do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, nie zapewnił użytkownikowi możliwości zgłoszenia cyberzagrożenia, incydentu lub podatności na nie związanych ze świadczoną usługą. Kara dla kierownika może być przyznana także, gdy przekaże on niepełne sprawozdanie końcowe z obsługi incydentu poważnego to jest niezawierające elementów takich jak szczegółowy opis incydentu poważnego, w tym spowodowanych zakłóceń i szkód, rodzaju zagrożenia lub jego przyczyny, która prawdopodobnie była źródłem incydentu, zastosowanych i wdrożonych środków ograniczających ryzyko, a w odpowiednich przypadkach transgranicznych skutków incydentu. Karze pieniężnej może także podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, którego zaniechanie w realizacji obowiązków miało charakter jednorazowy.

**17 sektorów musi zadbać o swoje życie w sieci**

Sektory objęte przepisami podzielono na dwie grupy. Pierwsza to sektory kluczowe, do których zaliczana jest energetyka (wydobywanie kopalin, energia elektryczna, ciepło, ropa i paliwa, gaz, energetyka jądrowa, dostawcy usług dla sektora energii, wodór), transport (lotniczy, kolejowy, wodny, drogowy), bankowość i infrastruktura rynków finansowych, ochrona zdrowia (udzielanie świadczeń zdrowotnych i zdrowie publiczne, produkcja i dystrybucja (substancji czynnych, produktów leczniczych i wyrobów medycznych), zaopatrzenie w wodę pitną i jej dystrybucja, zbiorowe odprowadzanie ścieków, infrastruktura cyfrowa (w tym komunikacja elektroniczna), zarządzanie usługami ICT, przestrzeń kosmiczna oraz podmioty publiczne (m.in. instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Urząd Komisji Nadzoru Finansowego, Narodowy Fundusz Zdrowia, Wody Polskie, Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych czy Polska Agencja Prasowa).

Druga grupa podmiotów to sektory ważne tj. usługi pocztowe, gospodarowanie odpadami (m.in. zbieranie, transport i przetwarzanie odpadów), produkcja, wytwarzanie i dystrybucja chemikaliów, produkcja, przetwarzanie i dystrybucja żywności, produkcja (wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, komputerów, wyrobów elektronicznych i optycznych, urządzeń elektrycznych, maszyn i urządzeń, gdzie indziej niesklasyfikowana, pojazdów samochodowych, przyczep i naczep oraz pozostałego sprzętu transportowego), badania naukowe, dostawcy usług cyfrowych (internetowej platformy handlowej, wyszukiwarki internetowej, platformy sieci usług społecznościowych).

Podmioty kluczowe to przede wszystkim firmy duże. W określonych przypadkach podmiotem kluczowym może być też firma mała lub średnia. Podmioty ważne to najczęściej mikro, mali lub średni przedsiębiorcy.

\*\*\*

**Holding Grupy Progres** jest jedną z największych agencji HR wśród firm z branży posiadających 100 proc. polskiego kapitału i działających na terenie całego kraju. W jej skład wchodzą spółki, z których najstarsza na rynku funkcjonuje od 2002 r. Grupa wspiera przedsiębiorstwa w całej Polsce w zakresie pracy tymczasowej (Progres HR), doradztwa biznesowego i szkoleń (Progres Consulting), rekrutacji stałych (Progres Permanent Recruitment), a także optymalizacji procesów (Progres Advanced Solutions). Rocznie zatrudnia niemal 20 tysięcy pracowników i realizuje 1,5 tysiąca projektów rekrutacyjnych. Posiada kilkadziesiąt oddziałów w Polsce i za granicą. Organizacja była wielokrotnie nagradzana w prestiżowych konkursach, plebiscytach i rankingach tj. m.in. Diamenty Forbesa (2017 r. – laureat), Gazele Biznesu (2020 r. – druga najdynamiczniej rozwijająca się firma w Polsce), Medal Europejski (2021 r.), Lider Polskiego Biznesu (2022 r.), Firma Przyjazna Cudzoziemcom (2022 r.) czy Ambasador Polskiej Gospodarki BCC (2023 r.). Grupa Progres jest członkiem Stowarzyszenia We!come – zrzeszającego pracodawców zatrudniających cudzoziemców w Polsce, posiada też certyfikat Równości Płac przyznawany przez Business Center Club.

**\*\*\***

**Biuro prasowe Grupy Progres:**

Kamila Tyniec

e-mail: k.tyniec@bepr.pl lub kom. +48 500 690 965