**Dyrektywa NIS 2 – czy dotyczy także twojej organizacji?**

* **Unijna dyrektywa NIS 2 weszła w życie na początku roku i reguluje istotne kwestie w zakresie cyberbezpieczeństwa firm i innych podmiotów.**
* **Celem implementacji NIS 2 do przepisów krajowych jest wzmocnienie cyberzabezpieczeń i poprawa zdolności reakcji na incydenty. To oznacza nowe obowiązki dla wszystkich – firm, instytucji i państwa.**
* **NIS 2 to również konkretne metody egzekwowania regulacji, m.in. kontrole administracyjne i kary pieniężne.**

Dyrektywa NIS 2 to odpowiedź Unii Europejskiej na stale rosnące cyberzagrożenia, które dotyczą wielu podmiotów prywatnych, publicznych i organów państwa. Aktualizuje i porządkuje ona przepisy unijne NIS z 2016 r. Najważniejsze zmiany, które wprowadza NIS 2 to wzmocnienie wymogów związanych z zarządzeniem ryzykiem przez przedsiębiorstwa. Przepisy mają na celu usprawnienie reagowania i zarządzania oraz wprowadzają obowiązek raportowania incydentów bezpieczeństwa. NIS 2 weszła w życie 16 stycznia 2023 roku, a na implementację dyrektywy do przepisów krajowych, państwa członkowskie UE mają czas do 17 października 2024 roku. Dla organizacji oznacza to szereg nowych zobowiązań, do których trzeba będzie się dostosować. Jakie to wymagania?

*– Przede wszystkim trzeba pamiętać, że implikacja NIS 2 do przepisów krajowych to proces, więc wszystkie podmioty, których to dotyczy, mają czas na dostosowanie się do spełniania nowych wymagań. Jednak już teraz warto wiedzieć, czy dyrektywa NIS 2 będzie dotyczyć naszej firmy lub instytucji, bo wprowadzenie tych zmian obejmuje wiele obszarów bezpieczeństwa sieci IT, czyli wdrożenia innych, często nowych i bardziej skomplikowanych rozwiązań. Podmioty, których dotyczą te regulacje podzielono według dwóch kategorii i zanim podejmiemy odpowiednie kroki, w pierwszej kolejności należy ustalić, czy nasza organizacja zalicza się do którejś z nich. A następnie warto skorzystać z wiedzy i wsparcia specjalistów –* mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

**Kogo dotyczy NIS 2?**

Podmioty podlegające NIS 2 podzielono według dwóch kategorii – „kluczowe” i „ważne”. Jednak obowiązki związane z osiągnięciem właściwego poziomu cyberbezpieczeństwa są takie same dla obu grup. Zostaną one sprecyzowane dopiero po przygotowaniu implementacji do NIS 2 na szczeblu krajowym – państwo ma więc na to czas do października 2024 roku. Kogo więc obejmie dyrektywa?

Będą to podmioty spełniające wymogi średniego przedsiębiorstwa w myśl prawa UE oraz większe organizacje. Każde państwo członkowskie przygotuje własny wykaz podmiotów kluczowych i ważnych, do 27 miesięcy po wejściu w życie NIS 2. Szacuje się, że w Polsce będzie to kilka tysięcy firm. O włączeniu organizacji do danej kategorii będzie decydował rozmiar przedsiębiorstwa, z nielicznymi wyłączeniami. A więc do podmiotów kluczowych zaliczane będą przedsiębiorstwa zatrudniające nie mniej niż 250 osób lub takie, których obroty roczne lub roczna suma bilansowa wynoszą poniżej 50 mln euro. Poza tym każda firma, która zostanie przez państwo uznana za organizację o znaczeniu strategicznym i wpisana na taką listę, może zostać podmiotem kluczowym.

Prościej rysuje się z kolei sytuacja dotycząca podmiotów ważnych – tutaj będą to albo organizacje z sektorów określonych dla podmiotów kluczowych, które podlegały wyłączeniu z tej listy, albo organizacje z jednego z sektorów określonych dla podmiotów ważnych.

**Jakie warunki trzeba będzie spełniać?**

Choć precyzowanie warunków na szczeblu krajowym jeszcze trwa, to już na tym etapie wprowadzania NIS 2 w życie wiadomo, jakie są ogólne wymagania wobec organizacji, których dotyczą nowe przepisy. Wśród nich znalazły się m.in.:

* dynamiczna analiza ryzyka i środki zarządzania ryzykiem, polityki bezpieczeństwa systemów teleinformatycznych (spełnieniem tego wymogu jest zbudowanie i wdrożenie w organizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z ISO 27001),
* zarządzanie incydentami (również zgodnie z ISO 27001),
* raportowanie incydentów do CSIRT na szczeblu krajowym lub podobnej organizacji,
* bezpieczeństwo łańcucha dostaw,
* plan ciągłości działania i zarządzania kryzysowego,
* polityki i procedury nabywania, rozwoju i utrzymania sieci i systemów informatycznych,
* polityki testowania i audytu zabezpieczeń,
* kryptografia i szyfrowanie
* szkolenia z cyberbezpieczeństwa.

Warto jeszcze podkreślić, że aby NIS 2 rzeczywiście spełniała swoją rolę, przygotowane zostały nowe narzędzia kontrolne i nadzorcze. Obejmują one: stosowanie kontroli doraźnych wobec podmiotów kluczowych, nakładanie administracyjnych kar pieniężnych oraz odpowiedzialność indywidualną.

*– W przypadku listy warunków do spełnienia, warto zwrócić szczególną uwagę na szkolenia w zakresie cyberzbezpieczeństwa. Z naszego doświadczenia wynika, że do incydentów dość często dochodzi z udziałem szeregowych pracowników instytucji. Wiedza na temat cyberzagrożeń wśród nich często bywa mniejsza niż w przypadku osób zatrudnionych w działach IT, dlatego częściej mogą oni ulegać manipulacjom hakerów. Ważne jest też nabywanie dobrych nawyków, jak choćby regularna zmiana haseł dostępowych. Tego typu praktyki są omawiane na szkoleniach, które powinny odbywać się cyklicznie, aby stale aktualizować wiedzę w zespole. Warto podkreślić, że ważnym elementem szkoleń jest część praktyczna, gdzie przeprowadzane są symulacje incydentów i omawia się reakcje na te zdarzenia. Zdobywanie wiedzy przez praktykę zawsze przynosi pozytywne rezultaty* –dodaje Patrycja Tatara ze Sprint S.A.

Stopień skomplikowania nowych przepisów w myśl NIS 2 oznacza, że podmioty, których dotyczą nowe przepisy, będą musiały skorzystać z wiedzy i doświadczenia specjalistów zewnętrznych. Przygotują oni nie tylko gotowe do wdrożenia rozwiązania, ale też doradzą, w jakiś sposób spełnić warunki nałożone przez NIS 2. Jedną z odpowiedzi na takie potrzeby jest konferencja Sprint Cyber Forum 2023, która odbędzie się 31 maja w Warszawie.

Źródło: Sprint S.A.