NIS2 nadchodzi

PTI zapewni cyberbezpieczeństwo jednostkom samorządów

Wszystkim zaniepokojonym obowiązkiem żmudnego przygotowania firmy do wymagań NIS2 polecamy usługę FortCyber.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii – NIS2 – obowiązuje niemal od roku (https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2555). Polska ma zwykle spory poślizg w implementacji europejskiego prawa i tym razem też zalicza opóźnienie. Dopiero w październiku 2024 r. na stronie Rządowego Centrum Legislacyjnego udostępniono drugi projekt Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC), która implementuje NIS2.

Czasu coraz mniej

Z pewnością w 2025 r. dyrektywa zacznie obowiązywać, a to oznacza skokowy wzrost wymagań w zakresie cyberbezpieczeństwa, którym ogromna liczba firm będzie musiała sprostać (według różnych szacunków rządowych wymagania obejmą minimum 20 tys. podmiotów działających na rynku polskim). Większość z nich nawet o tym jeszcze nie wie. Nie wszyscy są świadomi, że mogą zaliczać się do grupy podmiotów ważnych lub krytycznych, bo tym razem to nie państwo je wskazuje, tylko organizacja musi sama ustalić, czy podlega nowym przepisom.

Nie pojawiły się dotychczas istotne kampanie informacyjne o samej dyrektywie, jej wymogach i terminach. Tę lukę próbuje w ramach swoich skromnych środków wypełnić „Domena". Temat NIS2 na naszych łamach gości dość często, w poprzednim numerze pisma o wymaganiach dyrektywy pisał obszernie Piotr Kościelniak i to w dość alarmistycznym tonie.

Czujność w sprawie NIS2 powinny wzmóc zwłaszcza firmy z branż: energetycznej, automotive, chemicznej, IT, medycznej, transportowej, bankowości, zarządzania wodą pitną, gospodarki ściekami oraz administracja publiczna. Eksperci zwracają uwagę, że dyrektywa jest bardzo konkretna: dokładnie wiadomo kogo dotyczy, wskazuje szczegółowo wymagane działania, definiuje zadania prawne, organizacyjne, techniczne, zawiera konkretne check-listy, określa finansową i prawną odpowiedzialność kierownictwa i organizacji za niespełnienie wymagań, wymaga stałego udokumentowanego spełniania kryteriów, a nie jednorazowego „papierowego" raportu.

Wraz z przyspieszoną informatyzacją urzędów i firm oraz cyfryzacją procesów poziom zagrożeń w sferze cyberbezpieczeństwa nieustannie rośnie. Według badań KPMG, ok. dwóch trzecich polskich firm w 2023 r. zarejestrowało incydent cyberbezpieczeństwa – jest to o 8 proc. więcej niż w roku poprzednim. W zeszłym roku niemal podwoiła się liczba zgłaszanych incydentów dotyczących cyberbezpieczeństwa (źródło CERT Polska), co pokazuje skalę zagrożenia. Według raportu ENISA 39% polskich firm nie ma żadnego specjalisty ds. cyberbezpieczeństwa, co czyni je atrakcyjnym celem dla cyberprzestępców.

Wdrożenie NIS2 nie jest więc spełnianiem wymagań stawianych przez UE w imię jakiegoś wyimaginowanego ujednolicenia minimalnego standardu cyberbezpieczeństwa w państwach UE, tylko wyrazem troski o własne, bezpieczne działanie. Część polskich firm pomału się do NIS2 przymierza, część czeka na wydanie ostatecznych przepisów krajowych (co po doświadczeniach z RODO jest w pewnym stopniu zrozumiałe). Trzeba tylko pamiętać, że firmy, które opóźniają wprowadzenie wymogów NIS2, narażają się na większe ryzyko skutecznego cyberataku na swoje zasoby, a także na dość dolegliwe kary ustawowe.

Niewypełnianie obowiązków (m.in. rejestracyjnych, dokumentacyjnych, dotyczących zgłoszeń) zagrożone jest wysokimi karami, wymierzanymi zarówno firmie, jak i członkom zarządów. Kary dla przedsiębiorstw mogą wynieść do 10 mln euro lub 2%

rocznych przychodów, nie mniej niż 20 000 zł (a w przypadku bezpośredniego i poważnego zagrożenia cyberbezpieczeństwa dla obronności czy bezpieczeństwa państwa nawet 100 mln zł). Kierujący jednostką ponosi odpowiedzialność za wdrożenie wymagań NIS bez względu na to, czy zadania wykonuje samodzielnie czy je powierza. Kara bezpośrednia dla kierownictwa może sięgać 6-krotnego miesięcznego uposażenia.

Na sprostanie rozbudowanym wymaganiom NIS2 potrzebne są odpowiednie środki finansowe i osobowe. Jak wynika z raportu KPMG z 2023 r., ponad połowa (57proc.) polskich firm przyznała, że największą barierą utrudniającą budowanie odpowiedniego poziomu zabezpieczeń jest brak wystarczających budżetów, a niemal połowa (47 proc.) wskazywała na trudności w znalezieniu i utrzymaniu odpowiednio wykwalifikowanych pracowników w obszarze cyberbezpieczeństwa. Od tego czasu specjalistów nie przybyło.

Firmy podlegające przepisom znowelizowanej UKSC będą miały obowiązek:

- stworzenia systemów zarządzania bezpieczeństwem informacji zgodnie z normami ISO 27001 oraz ISO 22301;
- wdrożenia zabezpieczeń chroniących przed incydentami cyberbezpieczeństwa zgodnie z analizą ryzyka oraz na podstawie najnowszego stanu wiedzy;
- dokonywania zgłoszeń incydentów do organu nadzorczego (wczesne ostrzeżenie w terminie 12h/24h, zgłoszenie w ciągu 72h) oraz powiadamiania o incydentach własnych użytkowników;
- wdrożenia nowej, rozbudowanej dokumentacji dotyczącej cyberbezpieczeństwa;
- prowadzenia na własny koszt audytu wstępnego w ciągu 12 miesięcy i regularnych audytów bezpieczeństwa co dwa lata przez osoby o odpowiednich kompetencjach oraz udostępniania wyników audytów organowi regulacyjnemu w ciągu 3 dni od ich otrzymania;
- rejestracji w krajowym systemie informatycznym S46 oraz wymiany informacji za jego pośrednictwem;
- zarządzania ryzykiem łańcucha dostawców usług ICT;
- zapewnienia dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń wśród własnych pracowników.

> *Większe firmy jakoś sobie z wymaganiami NIS2 poradzą, mniejsze będą miały problem. W szczególnie trudnym położeniu znajdzie się administracja państwowa, zwłaszcza na szczeblu samorządowym, od lat borykająca się z niedostatkiem środków.*

SPTI na odsiecz

Dla urzędów miast, gmin, starostw powiatowych i organizacji JST (bibliotek, szpitali, ośrodków pomocy społecznej, zakładów gospodarki komunalnej i placówek oświatowych) Polskie Towarzystwo Informatyczne przygotowało specjalną ofertę, pozwalającą na zapewnienie cyberbezpieczeństwa we wszystkich najważniejszych obszarach wskazywanych przez NIS2. Nad zakresem usługi FortCyber, dopasowanym do potrzeb, specyfiki oraz możliwości Jednostek Samorządu Terytorialnego, pracowali rzeczoznawcy PTI z wieloletnim doświadczeniem audytorskim. Jej istotną zaletą jest łatwość uruchomienia.

FortCyber zapewnia:

- zgodność organizacyjną i formalną z uregulowaniami prawnymi i standardami w obszarze cyberbezpieczeństwa w ramach stałej abonamentowej usługi, której koszty dostosowane są do wielkości i możliwości JST
- podnoszenie kompetencji pracowników JST i ich świadomości cyberzagrożeń
- ochronę techniczną komputerów i serwerów oraz monitorowanie zdarzeń i reagowanie na incydenty
- wsparcie prawne w przypadku wystąpienia incydentów cyberbezpieczeństwa

Eksperci PTI ocenią dojrzałość organizacji i dokonają analizy dokumentacji bezpieczeństwa. Dyrektywa wymaga ustanowienia przez kierownictwo organizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), którego rolą jest zapewnienie odpowiednich i proporcjonalnych środków technicznych i organizacyjnych służących do ochrony zasobów informacyjnych. Najważniejszym celem jest zapewnienie ciągłości działania usług kluczowych oraz minimalizowanie skutków wystąpienia potencjalnych incydentów cyberbezpieczeństwa. Na podstawie

prac analitycznych, obejmujących ocenę ryzyka, eksperci PTI przygotują raport ze stanu przygotowania organizacji na NIS2, a następnie opracują plan działań krótko- i długofalowych, który zapewni spełnienie technologicznych, organizacyjnych i formalnych wymagań NIS2. Ten plan będzie uwzględniał istniejące plany rozwoju podmiotu.

Jednostki Samorządu Terytorialnego, które wybiorą PTI na swojego przewodnika w obszarze NIS2, zyskają wiele wymiernych korzyści.

Warto zaufać ponad 40-letniemu doświadczeniu audytorskiemu Izby Rzeczoznawców PTI i zapewnić sobie fachowe wsparcie w trudnym procesie dostosowania podmiotu do wymagań NIS2. PTI zapewnia także dodatkowe rofesjonalne szkolenia, zakończone certyfikatem, w obszarach: zarządzania cyberbezpieczeństwem, świadomości cyberzagrożeń i sposobów ochrony. Szkolenia prowadzone są przez wyspecjalizowane centra szkoleniowe w ramach Zintegrowanego Systemu Kwalifikacji (ZSK) oraz Europejskiej Certyfikacji Umiejętności Komputerowych (ECDL).

FortCyber

Korzyści dla JST

- **Kompletność usługi**
  Pełny zakres zapewnienia bezpieczeństwa cyfrowego w zakresie przygotowanym dla Jednostek Samorządu Terytorialnego.
- **Krótki czas wdrożenia**
  Zapewnienie cyberopieki już po 6 tygodniach od podpisania umowy.
- **Wygodny model finansowania**
  Niski próg wejścia, usługa w modelu abonamentowym, umowa na 12 miesięcy.
- **Zgodność z regulacjami**
  Gwarancja stałej zgodności formalnej (procedury i dokumentacja) z obowiązującymi przepisami i regulacjami (KRI, KSC, NIS2).

- **Podnoszenie kompetencji pracowników**
  Stale aktualizowana wiedza pracowników w zakresie cyberbezpieczeństwa, możliwych form ataków oraz konieczności stosowania dobrych praktyk.
- **Zaufany partner**
  Usługa przygotowana przez Polskie Towarzystwo Informatyczne, wykonawca zapewnia najwyższą jakość.

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Zainteresowanych ofertą prosimy o kontakt za pośrednictwem strony

www. Fortcyber.pl

Znajdą tu Państwo wyczerpujące informacje o usłudze FortCyber. Publikujemy tam także biuletyny edukacyjne dotyczące cyberbezpieczeństwa. W pierwszym numerze przygotowaliśmy przegląd zagrożeń cybernetycznych, z którymi mierzą się polskie organizacje. Warto dowiedzieć się, jakie rodzaje ataków rozróżniamy, jak one przebiegają i poznać przykłady incydentów, które miały miejsce w polskich podmiotach publicznych i prywatnych w ostatnich latach.