**Konfiguracja urządzeń Zyxel oraz inne wyzwania dotyczące dyrektywy NIS2**

**Zyxel Networks Polska wraca do przemyśleń związanych z wdrożeniem w Polsce dyrektywy NIS2, które poruszał podczas swojego webinaru.**

**Czym jest NIS2?**

**NIS2 (Network and Information Security 2)** to unijna dyrektywa stworzona w celu podniesienia poziomu cyberbezpieczeństwa i zbudowania spójniejszych ram bezpieczeństwa cyfrowego w całej UE. Jej cele to: **zwiększenie bezpieczeństwa sieci i systemów informatycznych** w sektorach o kluczowym znaczeniu, **wzmocnienie zarządzania ryzykiem**, **poprawa zgłaszania incydentów** **cyberbezpieczeństwa**, **objęcie większej liczby sektorów i podmiotów** kluczowych lub ważnych dla funkcjonowania państwa i gospodarki, **wzmocnienie współpracy** **między państwami członkowskimi w zakresie cyberbezpieczeństwa** oraz **nałożenie większej odpowiedzialności na zarządy firm** za zgodność z przepisami dotyczącymi cyberbezpieczeństwa.

Państwa członkowskie UE, w tym Polska, miały czas do 17 października 2024 roku na wdrożenie przepisów NIS2 do swoich krajowych porządków prawnych. Jednak rzeczywistość jest nieco inna.

**Problemy przy wdrażaniu NIS2**

*Nadal nie mamy nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, która wdrożyłaby w Polsce wymagania dyrektywy* ***NIS2*** - mówił podczas majowego webinaru **Aleksander Styś**, VAR Account Manager, **Zyxel Networks Polska** (będzie ona dopiero w 2025 roku). - *To ważne, bo każda dyrektywa unijna, w przeciwieństwie do rozporządzeń (które działają bezpośrednio), potrzebuje krajowej ustawy, żeby jej wymagania faktycznie zaczęły obowiązywać w naszym kraju. Bez tej ustawy, jesteśmy w pewnym zawieszeniu.*

*Chociaż wciąż czekamy na ostateczną wersję ustawy, pracujemy już na skonsolidowanym tekście projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa* - dodał biorący udział w spotkaniu **Krzysztof Kowalski**, inspektor ochrony danych, **Kowalski ORG**. - *To jest istotna zmiana, ponieważ ten projekt szczegółowo opisuje obowiązki, jakie spadną na podmioty kluczowe i ważne po wejściu w życie nowych regulacji*.

**Zyxel** wskazuje na szereg problemów dla administratorów IT oraz firm: brak czasu i zasobów na czytanie ustaw, złożoność procesu audytu, presja czasu oraz ryzyko (IT wdraża zalecenia bez pełnego zrozumienia i weryfikacji ustaleń audytowych lub planu zarządzania ryzykiem).

**Propozycje rozwiązań problemów**

Jako jeden z kroków na drodze rozwiązania **Krzysztof Kowalski** wskazał na jasny podział odpowiedzialności. Audytem i analizą ryzyka powinni zajmować się specjaliści do spraw bezpieczeństwa lub audytorzy. Wdrożeniem zaleceń z kolei dział IT oraz administratorzy sieci.

Innym krokiem jest stosowanie razem uznanych norm międzynarodowych. Choć mogą one budzić obawy klientów, dają jasny i praktyczny opis zadań, pomagając przełożyć wymagania na konkretne działania techniczne. Dodatkowo możliwe jest selektywne podejście. Pokazuje to jeden z omawianych przykładów wdrożeń urządzeń **Zyxel** (w szpitalu wojewódzkim), gdzie skupiono się tylko na segmentacji sieci według ISO 27002 (a nie na całym wdrażaniu tej normy).

*Cała ta dyrektywa i nasza ustawa stawiają na mądre podejście – oparte na ryzyku. Chodzi o to, by dobierać środki bezpieczeństwa adekwatnie do tego, co realnie zagraża, a nie tylko odhaczać punkty na jakiejś abstrakcyjnej liście* - powiedział **Aleksander Styś**.

Inne rozwiązanie **Zyxel**, które zostało pomyślnie wdrożone, to **Nebula Control Center** w urzędzie miejskim dla zarządzania aktualizacjami (zgodnie z projektem ustawy wdrażającej **NIS2**).

*Urząd miejski ma rozproszoną infrastrukturę sieciową w kilku lokalizacjach. Musi wdrożyć efektywny i udokumentowany proces regularnych aktualizacji firmware'u tych urządzeń, aby zminimalizować ryzyko wykorzystania znanych luk. Ręczne sprawdzanie i instalowanie aktualizacji jest czasochłonne i podatne na błędy* - tłumaczył **Aleksander Styś**. - *Wszystkie urządzenia* ***Zyxel*** *w urzędzie są podłączone do chmury* ***Nebula****. Administrator widzi status ich oraz wersji ich oprogramowania w jednym miejscu*. ***Nebula*** *sama monitoruje dostępność nowych wersji firmware’u. A co najważniejsze, pozwala zaplanować proces aktualizacji.*

**Odpowiednie środki najważniejsze**

**Krzysztof Kowalski** przypomniał też, że administrator musi umieć wykazać dlaczego wybrał takie, a nie inne zabezpieczenia (podstawą jest przeprowadzona analiza ryzyka). *Przeglądając decyzje prezesa UODO, widzimy powtarzający się schemat. Kary administracyjne są często nakładane nie tylko za sam fakt naruszenia ochrony danych, ale przede wszystkim za brak wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo adekwatne do ryzyka* - wyjaśnił. - *Wiele decyzji punktuje brak regularnego testowania, mierzenia i oceniania skuteczności tych środków, brak analizy ryzyka związanego z przetwarzaniem czy brak weryfikacji podmiotów przetwarzających.*

**Aleksander Styś** zwrócił z kolei uwagę, że ogólne zasady i wymagania prawne należy przełożyć na konkretne działania konfiguracyjne - zgodnie z najlepszymi praktykami - w infrastrukturze sieciowej - w tym na urządzeniach **Zyxel**. Zacząć trzeba od minimalnych środków zarządzania ryzykiem w cyberbezpieczeństwie, które wymienia wymienia **art. 21, ust. 2 NIS2**:

l polityka analizy ryzyka i bezpieczeństwa systemów informatycznych,

l obsługa incydentów,

l ciągłość działania,

l bezpieczeństwo łańcucha dostaw,

l bezpieczeństwo w nabywaniu, rozwoju, utrzymaniu,

l ocena skuteczności środków,

l cyberhigiena i szkolenia,

l kryptografia i szyfrowanie,

l bezpieczeństwo zasobów ludzkich / kontrola dostępu,

l stosowanie MFA.

Urządzenia oraz platformy Zyxel oferują szereg rozwiązań, z których można tu korzystać. Na przykład **Zyxel CNM SecuReporter** - usługa analityczna i raportowa dla linii produktów **ZyWALL** i **Nebula**. *Jeśli potrzebujesz pomocy w konfiguracji Zyxel zgodnie z NIS2 lub audytu czy analizy ryzyka, skontaktuj się z nami lub naszymi autoryzowanymi partnerami. Nie zostawiamy Was samych z tym wyzwaniem* - mówią **Aleksander Styś** oraz **Aleksander Turski**, Sales Engineer, **Zyxel Networks Polska**.

**Całość webinaru można obejrzeć na kanale** [Zyxel Networks Polska](https://www.youtube.com/watch?v=EbBoEhVnk1k&amp;amp;t=239s&amp;amp;ab_channel=ZyxelNetworksPolska)

**Polecamy także artykuł:** [Zyxel Networks wzmacnia cyberbezpieczeństwo w zgodzie z dyrektywą NIS2](https://www.zyxel.com/pl/pl/newsroom/press-releases/zyxel-networks-wzmacnia-cyberbezpieczenstwo-w-zgodzie-z-dyrektywa-nis2) **oraz** [Obowiązki i implikacje NIS2 zbadane](https://www.zyxel.com/pl/pl/solutions/nis2-directive)