KOMPAS IT

DELL Technologies

Zgodność z NIS2 – cyberbezpieczeństwo w zgodzie z dyrektywą europejską

Dyrektywa NIS2 (Network and Information Security Directive 2) to europejskie przepisy mające na celu poprawę poziomu bezpieczeństwa sieci i systemów informacyjnych w całej Unii Europejskiej.
Wymaga od organizacji zwiększenia poziomu cyberbezpieczeństwa poprzez wdrożenie odpowiednich strategii zarządzania ryzykiem, raportowania incydentów oraz podnoszenia świadomości bezpieczeństwa.

NIS2 wejdzie w życie 17 października 2024 roku – do tego czasu firmy i instytucje mają czas na dostosowanie swoich systemów i procedur do nowych wymagań. Dell Technologies, dzięki zaawansowanym rozwiązaniom IT, może znacząco wspierać organizacje w spełnieniu tych wymagań, oferując nowoczesne technologie, konsultacje oraz wsparcie techniczne.

Dyrektywa NIS2 obejmuje szerszy zakres sektorów w porównaniu do NIS definiowane, jako:

- Sektory kluczowe – ich zakłócenie miałoby znaczący wpływ na funkcjonowanie społeczeństwa i gospodarki oraz których działalność jest kluczowa dla utrzymania podstawowych funkcji społecznych.
- Sektory ważne - mogą mieć wpływ na funkcjonowanie społeczeństwa i gospodarki, ale w mniejszym stopniu niż sektory kluczowe.

⚠ ROLA I ZNACZENIE

Konieczność dostosowania przepisów dotyczących cyberbezpieczeństwa oraz infrastruktury informatycznej o podwyższonym standardzie bezpieczeństwa znajdują swoje uzasadnienie w badaniach. Według raportu GDPI Index 2023* ponad połowa firm (54%) na rynku EMEA padła ofiarą cyberataku. Ich koszty ataków wzrosły dwukrotnie, osiągając średnio 1,41 mln dolarów w 2023 roku. Raport Innovation Catalyst wskazuje natomiast, że 83% respondentów doświadczyło cyberataku w ciągu ostatnich 12 miesięcy. Trzy najczęściej wymieniane problemy obejmowały złośliwe oprogramowanie, phishing i naruszenia danych. Odpowiedzią na te wyzwania i stale rosnący poziom zagrożeń, są akty prawne mające pomóc organizacjom wskazać niezbędny standard poziomu ochrony zasobów IT.

** – The Global Data Protection Index (GDPI) Report, 2024*
*** – Dell Technologies Innovation Catalysts Study, 2023*

Dyrektywa NIS2 nakłada na organizacje obowiązek wdrożenia solidnych ram zarządzania ryzykiem i bezpieczeństwem, które obejmują:

- **identyfikację i ocenę ryzyka,** poprzez regularne przeprowadzanie analiz ryzyka, identyfikację potencjalnych zagrożeń i wdrażanie środków zaradczych;
- **obsługę incydentu** rozumiana jako działania i procedury mające na celu zapobieżenie incydentowi, wykrywanie i analizowanie go, ograniczanie jego zasięgu lub reagowanie na niego i przywrócenie normalnego działania;
- **bezpieczeństwo łańcucha dostaw,**
- **implementację zabezpieczeń technicznych i organizacyjnych,** takich jak firewall, systemy detekcji i zapobiegania włamaniom (IDS/IPS), szyfrowanie danych, oraz segmentacja siecina każdym poziomie organizacji,
- współpracę z odpowiednimi organami oraz wymiana informacji na temat zagrożeń i incydentów z innymi podmiotami;
- regularne audyty i oceny zgodności z politykami i procedurami bezpieczeństwa, aby zapewnić ciągłe doskonalenie.

⚠ Podstawowe praktyki skutecznego zarządzania cyberbezpieczeństwem

Aby skutecznie zarządzać cyberbezpieczeństwem w organizacji zgodnie z dyrektywą NIS2, należy wdrożyć szereg kluczowych praktyk, które pomagają minimalizować ryzyko cyberzagrożeń i zapewniają ciągłość działania systemów informacyjnych. Najważniejsze praktyki, które są kluczowe dla skutecznego zarządzania cyberbezpieczeństwem wg. Dyrektywy to:

1 **Wdrożenie strategii cyberbezpieczeństwa sieci i systemów informatycznych.**
2 **Zarządzanie ryzykiem cybernetycznym, zgodnie z opracowaną strategią zarządzania ryzykiem.**
3 **Szybkie i skuteczne zgłaszanie incydentów do odpowiednich organów.**
4 **Podnoszenie świadomości cyberbezpieczeństwa w całej firmie.**
5 **Współpraca z innymi podmiotami, wymiana informacji i wspólne reagowanie na zagrożenia.**
6 **Bezpieczeństwo Łańcucha Dostaw.**
7 **Implementacja Zabezpieczeń Technicznych i Organizacyjnych.**

⚠ **Implementacja dyrektywy NIS2 do polskiego porządku prawnego nastąpi poprzez nowelizację ustawy o Krajowy System Cyberbezpieczeństwa (KSC).**

Sankcje za nieprzestrzeganie NIS2 to m.in. kary finansowe, czy wstrzymanie (a nawet zakaz) działalności. Kary zależą od powagi naruszenia oraz wielkości organizacji.

MOŻLIWOŚCI I ZASTOSOWANIE

Organizacje stają przed koniecznością podjęcia decyzji, w jakie rozwiązania cyberbezpieczeństwa powinny zainwestować, aby najlepiej przygotować się do nowej rzeczywistości prawnej. Doskonałym wyborem będą **nowoczesne systemy zarządzania ryzykiem, narzędzia do wykrywania zagrożeń oraz platformy do obsługi incydentów. Kluczowy będzie wybór zaufanego dostawcy rozwiązań bezpieczeństw.**

Dell Technologies oferuje szeroki zakres produktów i usług, które mogą być stosowane w celu spełnienia wymagań NIS2:

- **Infrastruktura IT:** Serwery Dell PowerEdge i systemy przechowywania danych Dell EMC Storage zapewniają bezpieczeństwo i dostępność danych. Wielopoziomowe mechanizmy ochrony punktów końcowych (notebooków i stacji roboczych), zapewniają ochronę urządzeń przed zagrożeniami malware, ransomware i innymi atakami cybernetycznymi;
- **Backup i odzyskiwanie danych:** : Dell EMC Data Protection Suite zapewnia kompleksowe rozwiązania do backupu i odzyskiwania danych, kluczowe dla zachowania ciągłości działania.
- **Cyfrowy Bunkier** – zastosowanie koncepcji izolowanych kopii w zakresie:
  - Kopii bezpieczeństwa – Cyber Recovery Vault
  - Danych o dostępie blokowym – Dell PowerMax Cyber Vault
  - Danych o dostępie plikowym – Dell PowerScale Cyber Protection Suite
  - Danych o dostępie obiektowym – Dell ECS Cyber Vault
- **Zarządzanie ryzykiem:** Narzędzia Dell OpenManage oraz Dell APEX AIOps umożliwiają monitorowanie i zarządzanie ryzykiem IT.
- **Bezpieczeństwo punktów końcowych i sieci:** Rozwiązania Dell Managed Detection and Response (Dell MDR) zapewniają ochronę przed zagrożeniami cybernetycznymi.

ARCHITEKTURA – STRUKTURA I DZIAŁANIE

Rozwiązania Dell Technologies są zbudowane na skalowalnej i modularnej architekturze, co pozwala na ich łatwe dostosowanie do różnych potrzeb organizacji.
Dell Technologies, dzięki szerokiemu portfolio produktów i usług, jest w stanie kompleksowo wspierać organizacje w dążeniu do zgodności z dyrektywą NIS2, oferując nie tylko technologie i narzędzia, ale także wiedzę i doświadczenie w zakresie bezpieczeństwa IT:

Bezpieczna infrastruktura IT

Sprawdź Rekomendacje Kompas IT:

- Bezpieczne środowisko serwerowe – optymalizacja konfiguracji urządzeń i usług
- Bezpieczny PC – referencyjne mechanizmy ochrony dla laptopów i desktopów
- Nowoczesne macierze – efektywne rozwiązania do przechowywania danych
- Nowoczesne Data Center – bezobsługowa architektura i usługi chmury prywatnej

Rekomendowane rozwiązania

Dell Data Protection Suite - ciągłość działania, bezpieczeństwo informacji, ochrona Ransomware
Cyber Recovery UDS - ciągłość działania, bezpieczeństwo informacji,
Dell APEX AIOps - monitorowanie zasobów infrastruktury IT, monitorowanie podatności, predykcja zagrożeń,
Dell Technologies MDR - SIEM/SOC as a Service,
Dell PowerEdge - bezpieczny łańcuch dostaw i produkcji, wbudowane mechanizmy zabezpieczeń HwRoot of Trust,
Komputery osobiste - architektura Dell Trusted Workspace.

Usługi konsultingowe i wsparcie techniczne

Rekomendowane Usługi
Backup system healthcheck / assessment
Data recovery and DR procedures
LiveOptics – Audyt infrastruktury
Developing DR or BC Plan
Developing Business Impact Analysis and Risk Assessment

Usługi doradcze:
- Vulnerability Assessment
- Ransomware Assessment
- Zero Trust Assessemnt

Dyrektywa NIS2 stanowi istotny krok w kierunku zwiększenia bezpieczeństwa cyfrowego organizacji w całej Europie.
Aby osiągnąć zgodność z Dyrektywą NIS2, organizacje powinny:
- **zainwestować w nowoczesne technologie**
- **wdrożyć strategię zarządzania ryzykiem**
- **podnieść świadomość cyberbezpieczeństwa wśród pracowników**
- **współpracować z zaufanym partnerem.**

Wybór sprawdzonych, solidnych rozwiązań cyberbezpieczeństwa pozwoli łatwiej wdrożyć najnowsze wytyczne i skutecznie chronić dane i systemy przed rosnącymi zagrożeniami cybernetycznymi.

Niniejsze rekomendacje Dell Technologies oraz wytyczne dotyczące zgodności z ustawą o KSC zostaną zaktualizowane po uchwaleniu nowelizacji, aby zapewnić pełną zgodność z wymogami dyrektywy NIS2 i efektywne dostosowanie się do nowych przepisów obowiązujących lokalnie.

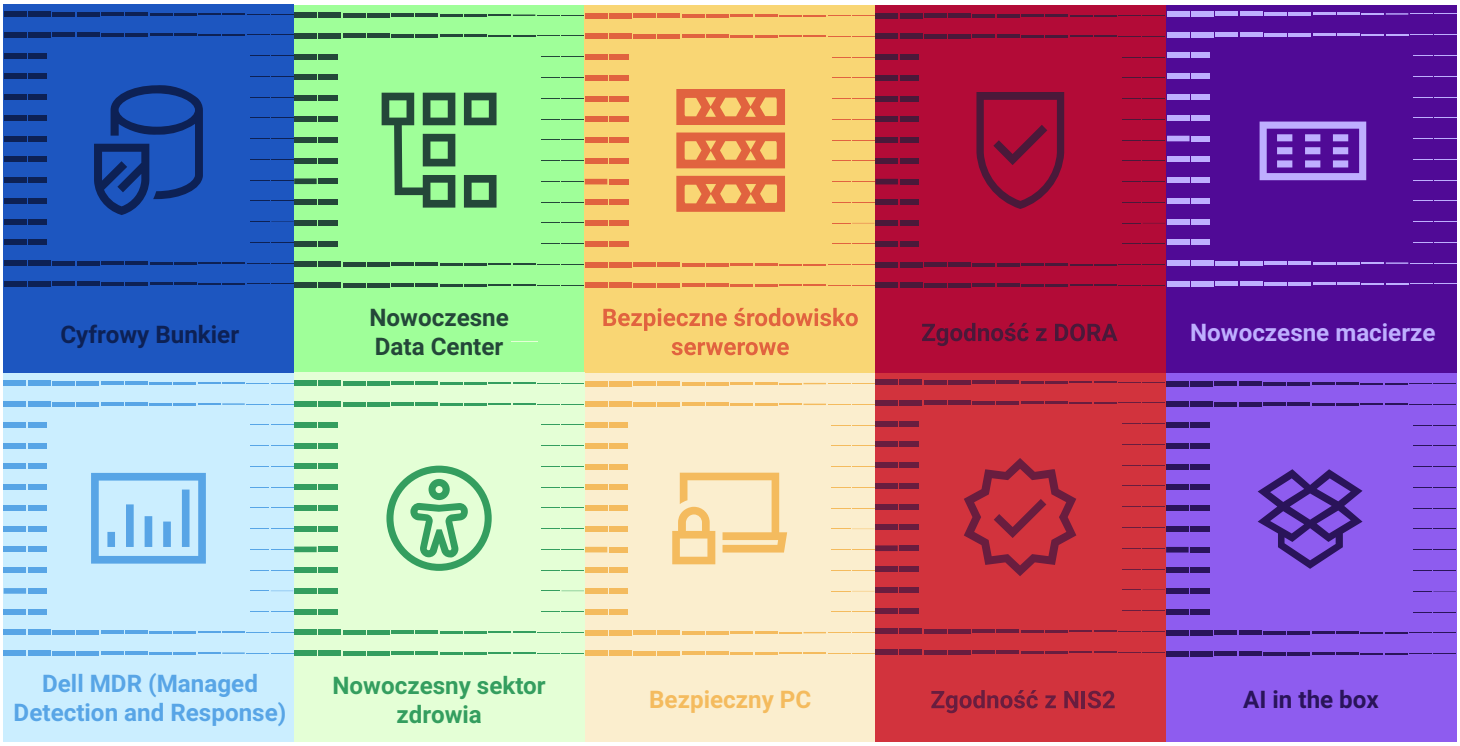
ZOBACZ TAKŻE

> Cyfrowy Bunkier – nowy standard cyfrowej odporności organizacji

Zgodność z DORA – efektywne strategie bezpieczeństwa cyfrowego

Dell MDR (Managed Detection and Response) – efektywne monitorowanie środowiska IT

Kompas IT – innowacyjne rozwiązania dla efektywności i cyfrowej odporności IT



Poznaj rozwiązania Dell Technologies

Porozmawiajmy, jak osiągnąć Zgodność z NIS2, czyli o cyberbezpieczeństwie w zgodzie z dyrektywą europejską

Bartosz Charlinski
Enterprise Architect
Dell Technologies

Bartosz.Charlinski@dell.com

DELL Technologies