KOMPAS IT

DELL Technologies

Zgodność z DORA – efektywne strategie bezpieczeństwa cyfrowego

Rozporządzenie DORA (Digital Operational Resilience Act) stanowi kluczowy element europejskiego krajobrazu legislacyjnego, uzupełniając Dyrektywę NIS2. Podczas gdy NIS2 harmonizuje ogólny poziom cyberbezpieczeństwa w UE, zapewniając, że kluczowe firmy i organizacje osiągną wysoki poziom bezpieczeństwa cyfrowego, DORA koncentruje się na wzmocnieniu cyfrowej odporności operacyjnej sektora finansowego.
Rozporządzenie DORA nakłada na podmioty finansowe obowiązek wdrożenia kompleksowych strategii oraz narzędzi technologicznych, które gwarantują wysoką odporność cyfrową, aby zapewnić ciągłość operacyjną nawet w przypadku cyberataków. Równocześnie, NIS2 skupia się na zapewnieniu bezpieczeństwa łańcucha dostaw i ogólnym zarządzaniu ryzykiem cybernetycznym.

DORA jako lex specialis dla sektora finansowego ma pierwszeństwo wobec dyrektywy NIS 2, zgodnie z zasadą, według której prawo szczegółowe ma pierwszeństwo nad prawem ogólnym. DORA wyjaśnia i uzupełnia przepisy NIS2.

MOŻLIWOŚCI I ZASTOSOWANIE

Wysoki poziom cyfrowej odporności operacyjnej, gwarantujący **zgodność z DORA,** pomagamy osiągnąć dzięki zaawansowanym technologicznie i kompleksowym rozwiązaniom, oferując:

- **kompleksowość –** mapę rozwiązań IT, dostosowanych do konkretnego aspektu wymagań DORA;
- **innowacyjność –** nowoczesne technologie i usługi, stale aktualizowane, aby sprostać zmieniającym się zagrożeniom i regulacjom;
- **zaufanie i doświadczenie –** rozwiązania i eksperci Dell Technologies mogą być sprawdzonym partnerem w dostarczaniu efektywnych rozwiązań IT.

Kiedy szczególnie należy pamiętać o DORA?

- **Podczas wdrażania rozwiązań IT (w tym oprogramowanie i rozwiązania chmurowe):** DORA określa kluczowe zasady współpracy z dostawcami usług ICT na wszystkich etapach umów.
- **W trakcie implementacji nowych, krytycznych systemów IT, platform usługowych lub infrastruktury sieciowej:** Ustawa kładzie nacisk na bezpieczeństwo informacji i ciągłość usług, zgodnie z zasadą „Security by design”.
- **Podczas tworzenia lub modyfikacji procesów kluczowych dla biznesu:** DORA skupia się na zapewnieniu ciągłości operacyjnej i unikaniu pojedynczych punktów awarii.
- **Podczas świadczenia usług finansowych klientom:** Należy zapewnić nieprzerwane działanie, skutecznie chronić przed zagrożeniami, zarządzać ryzykiem, szybko reagować na incydenty oraz raportować je odpowiednim władzom.

Jak Dell Technologies może pomóc w osiągnięciu zgodności z DORA:

FILAR 1

Zarządzanie Ryzykiem ICT

Cyberbezpieczeństwo w cyfrowym łańcuchu dostaw i ciągość działania

Chodzi nie tylko o zarządzanie ryzykiem ICT, ale o włączenie ich do struktur nadzoru. Instytucje i krytyczni dostawcy usług są zobowiązani do ustanowienia kompleksowych ram, które identyfikują i adresują ryzyka oraz zapewniają konsekwentny nadzór i skuteczność tych procesów.

Zapewniamy bezpieczeństwo łańcucha dostaw poprzez implementację odpowiednich praktyk (jak selekcja i późniejszy audyt poddostawców do naszych rozwiązań) i mechanizmów, mających na celu eliminację możliwości instalacji złośliwego oprogramowania w całym cyklu życia komponentu infrastruktury ICT.

FILAR 2

Zarządzanie Incydentami ICT – klasyfikacja i raportowanie

Proces raportowania i ostrzegania o cyberbezpieczeństwie i podatnościach

Przejrzystość jest kluczowa w przypadku wystąpienia incydentów. Zarówno instytucje finansowe, jak i krytyczni dostawcy usług są zobowiązani do natychmiastowego raportowania znaczących zakłóceń związanych z ICT. Ten wymóg zapewnia, że władze są informowane o szczegółach incydentu, jego skutkach oraz podjętych działaniach naprawczych.

Dostarczamy rozwiązania do wykrywania, monitorowania, reagowania, odzyskiwania danych i przywracania dostępności usługi po incydencie, zwiększając zdolność do szybkiej reakcji i minimalizowania skutków cyberataków.

FILAR 3

Cyfrowe Testy Odporności Operacyjnej

Obowiązkowe i regularne cyfrowe testy odporności operacyjnej, przeprowadzane przez niezależne podmioty

Regularne testowanie reakcji na incydenty ICT i okresowe testowanie odporności jest niezbędne. Dzięki tym testom ujawniane są podatności, co daje instytucjom i krytycznym dostawcom usług jasną mapę drogową do wzmocnienia obrony ICT.

Zapewniamy wsparcie planowania i wdrażania testów odporności operacyjnej, zapewniając niezawodność i ciągłość działania w obliczu zagrożeń.

FILAR 4

Zarządzanie Ryzykiem Dostawców Zewnętrznych ICT

Zarządzanie ryzykiem ICT i ryzykiem dostawców zewnętrznych, takich jak OSS i łańcuch dostaw oprogramowania

Podmioty finansowe nie mogą działać w izolacji. Uznając potencjalne zagrożenia, DORA kładzie nacisk na konieczność dokładnych ocen ryzyka z tymi podmiotami oraz ustanowienia jasnych zobowiązań umownych, precyzujących odpowiedzialności.

Wdrożyliśmy i realizujemy zaawansowany program bezpieczeństwa rozwoju produktu i aplikacji. Oprogramowanie (włączając w to firmware na sprzęcie) rozwijamy zgodnie z Secure Development Lifecycle (SDL). SDL jest zgodny z zasadami normy ISO/IEC 27034. Jesteśmy aktywnie zaangażowani w rozwój wielu standardów bezpieczeństwa, takich jak SAFECode, BSIMM, and IEEE Center for Secure Design, które sami stosujemy w procesie wytwarzania oprogramowania. Szczegółowe informacje są dostępne do wglądu dla zainteresowanych działów bezpieczeństwa.

FILAR 5

Wymiana Informacji

Udostępnianie alertów bezpieczeństwa, zagrożeń i metod ich wykrywania, taktyk i procedur. Utrzymywanie poufności i zgodność z wymaganiami GDPR

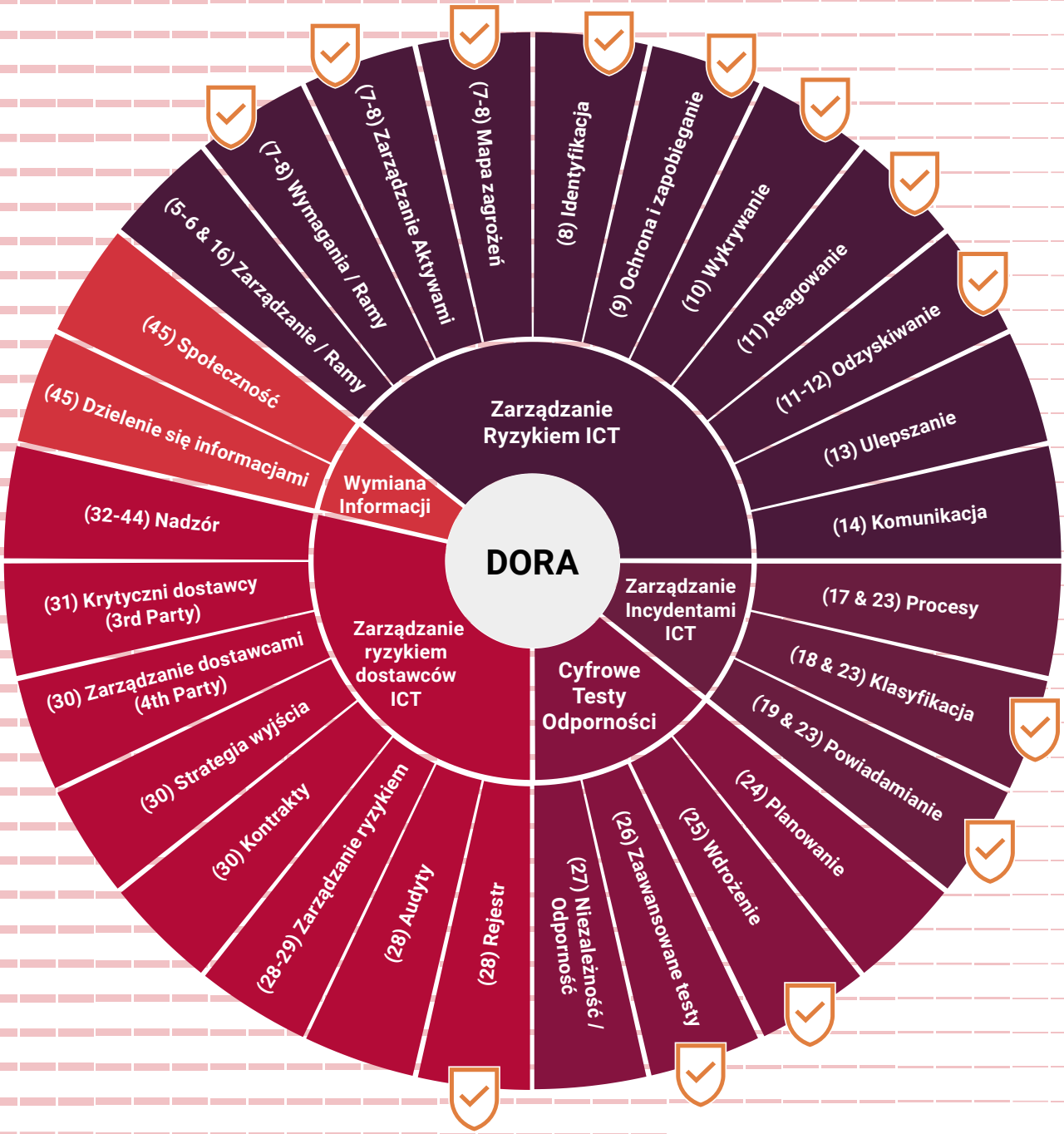
Wspólne uczenie się może być pozytywnym skutkiem incydentu. Instytucje i krytyczni dostawcy usług są zachęcani do dzielenia się szczegółami dotyczącymi incydentów ICT między sobą i z odpowiednimi władzami, wspierając kolektywną strategię obrony i zwiększając odporność całego sektora.

Infrastrukturę ICT od Dell Technologies dostarczamy wraz z platformą wymiany informacji o podatnościach wynikających z niezastosowania się do wskazówek dotyczących aktualizacji produktów. Platforma ta zawiera informacje o krytyczności danej podatności oraz wskazuje poprawki eliminujące wykazane podatności.

- odpowiedź technologiczna i możliwe wsparcie Dell Technologies

Zidentyfikuj najważniejsze podatności - szybko reaguj - działaj skutecznie.

Strategia Cyberbezpieczeństwa DORA



- odpowiedź technologiczna i możliwe wsparcie Dell Technologies

FILAR	(Artykuł DORA) OBSZARY	Szczegółowe wymagania DORA	Komentarze Ekspertów Dell Technologies	Rekomendowane narzędzia i rozwiązania Dell Technologies	
Zarządzanie Ryzykiem ICT	(5-6 & 16) Zarządzanie / Ramy	Określenie struktury zarządzania, roli i odpowiedzialności, dokumentacja i zatwierdzanie strategii	Systemy do zarządzania ryzykiem, np. GRC (Governance, Risk, and Compliance)		
	(7-8) Wymagania / Ramy	Tworzenie polityk bezpieczeństwa, regularne przeglądy zgodności, aktualizacje polityk	**Vulnerability Assessment & Management -** usługa mająca na celu pomoc organizacjom w identyfikacji podatności w ich obecnym środowisku oraz dostarczanie rekomendacji dotyczących ich usunięcia. **Ransomware Readiness Assessment -** usługa mająca na celu ocenę zastosowanej technologii, narzędzi, kontroli bezpieczeństwa oraz konfiguracji w zakresie ochrony i odzyskiwania danych po udanym ataku ransomware.	**Dell Advisory Services: Vulnerability Assessment & Management** **Dell Advisory Services: Ransomware Readiness Assessment**	✓
	(7-8) Zarządzanie Aktywami	Identyfikacja wszystkich aktywów, ocena ich wartości i ryzyka, monitorowanie cyklu życia aktywów	**Dell EMC OpenManage** zapewnia identyfikację i monitorowanie infrastruktury serwerowej oraz dryftowania konfiguracji. Informuje również o incydentach awarii. **Dell APEX AIOps Infrastructure Observability** raportuje stan aktualizacji komponentów infrastruktury w kontekście odkrytych podatności oraz zgodności z regułami najlepszych praktyk w zakresie bezpieczeństwa.	**Dell EMC OpenManage** **Dell APEX AIOps Infrastructure Observability**	✓
	(7-8) Mapa zagrożeń	Identyfikacja potencjalnych zagrożeń, ocena prawdopodobieństwa i skutków, mapowanie na cele organizacyjne	**Dell MDR to SIEM/SOC as a Service w 3 wydaniach:** - MDR with Secureworks Taegis XDR, - MDR with CrowdStrike Falcon XDR - MDR with Microsoft **APEX AIOps Incident Management** wykorzystuje AI do korelacji alertów pochodzących z wielu źródeł w czytelne incydenty.	**Dell Technologies Managed Detection and Response (MDR)** **APEX AIOps Incident Management**	✓
	(8) Identyfikacja	Regularna analiza ryzyka, identyfikacja nowych zagrożeń, aktualizacja rejestru ryzyka	**Vulnerability Assessment & Management -** usługa mająca na celu pomoc organizacjom w identyfikacji podatności w ich obecnym środowisku oraz dostarczanie rekomendacji dotyczących ich usunięcia.	**Dell Advisory Services: Vulnerability Assessment & Management**	✓
	(9) Ochrona i zapobieganie	Implementacja mechanizmów ochrony, kontrola dostępu, zabezpieczenia przed malware	**Zero Trust Assessment -** analiza obecnego stanu mechanizmów bezpieczeństwa oraz strategia dojścia do docelowego stanu Zero Trust zgodnego NIST Cybersecurity Framework.	**Dell Advisory Services: Zero Trust Assessment**	✓
	(10) Wykrywanie	Monitoring systemów, detekcja anomalii, analiza logów	**MDR to SIEM/SOC as a Service w 3 wydaniach:** - MDR with Secureworks Taegis XDR, - MDR with CrowdStrike Falcon XDR - MDR with Microsoft Monitorowanie, detekcje anomalii w zakresie Cyfrowego Bunkra realizuje **CyberSense, Superna Ransomware Defender** **APEX AIOps pracuje w trzech obszarach:** - Infrastruktura - proaktywne zarządzanie infrastrukturą Dell z uwzględnieniem bezpieczeństwa i dostępności środowiska; - Aplikacje - analiza pełnego stosu aplikacji dla zapewnienia dostępności i wydajności aplikacji; - Zarządzanie incydentami - wykorzystuje AI do korelacji alertów pochodzących z wielu źródeł w czytelne incydenty.	**Dell Technologies Managed Detection and Response (MDR)** **Dell Cyber Recovery (Cyfrowy Bunkier)** **APEX AIOps Incident Management** **APEX AIOps Infrastructure Observability** **APEX AIOps Application Observability**	✓
	(11) Reagowanie	Plan reagowania na incydenty, szkolenia, działania naprawcze	**Dell MDR to SIEM/SOC as a Service w 3 wydaniach:** - MDR with Secureworks Taegis XDR, - MDR with CrowdStrike Falcon XDR - MDR with Microsoft **APEX AIOps Incident Management** wykorzystuje AI do korelacji alertów pochodzących z wielu źródeł w czytelne incydenty.	**Dell Technologies Managed Detection and Response (MDR)** **APEX AIOps Incident Management**	✓
	(11-12) Odzyskiwanie	Plan przywracania operacji, testowanie planu odzyskiwania, utrzymywanie kopii zapasowych	**System kopii bezpieczeństwa** realizowany jest przez oprogramowanie Dell DPS lub Dell PPDM oraz medium przechowywania kopii Dell PP DataDomain. Rozszerzeniem systemu kopii bezpieczeństwa jest **Cyfrowy Bunkier,** który zapewnia m.in. kopie offline/air gap (kopia offline rekomendowana jest przez CERT Polska oraz ENISA w kontekście wytycznych DORA/NIS2). **Cyfrowy Bunkier** dotyczy: - kopii bezpieczeństwa - bazuje na DataDomain jako nośnik kopii - pamięci masowych o dostępie plikowym - bazuje na Dell Powerscale - pamięci masowych o dostępie obiektowym - bazuje na Dell ECS - pamięci masowych o dostępie blokowym - bazuje na Dell PowerMax W ramach **Dell MDR** oferowane są specjalizowane usługi odzyskiwania danych po incydencie : - Dell Services: Incident Recovery RetainerService (IRRS) - Dell Services: Incident Response & Recovery (IRR)	**System kopii bezpieczeństwa** oraz **Cyfrowy Bunkier (Dell Cyber Recovery Vault)**	✓
	(13) Ulepszanie	Analiza po incydentach, wnioski z testów, wdrażanie usprawnień	Systemy do analizy i raportowania ryzyka		
	(14) Komunikacja	Procedury komunikacji wewnętrznej i zewnętrznej, raportowanie do interesariuszy	Platformy do zarządzania incydentami i komunikacji wewnętrznej		

FILAR	(Artykuł DORA) OBSZARY	Szczegółowe wymagania DORA	Komentarze Ekspertów Dell Technologies	Rekomendowane narzędzia i rozwiązania Dell Technologies	
Zarządzanie Incydentami ICT – klasyfikacja i raportowanie	(17 & 23) Procesy	Dokumentowanie procedur, roli i odpowiedzialności, działania naprawcze	ITSM (IT Service Management)		
	(18 & 23) Klasyfikacja	Ustalanie kryteriów klasyfikacji incydentów, priorytetyzacja	**Dell MDR to SIEM/SOC as a Service w 3 wydaniach:** - MDR with Secureworks Taegis XDR, - MDR with CrowdStrike Falcon XDR - MDR with Microsoft	**Dell Technologies Managed Detection and Response (MDR)**	✓
	(19 & 23) Powiadamianie	Szybkie i skuteczne powiadamianie odpowiednich stron, zgodność z wymogami regulacyjnymi	**Dell MDR to SIEM/SOC as a Service w 3 wydaniach:** - MDR with Secureworks Taegis XDR, - MDR with CrowdStrike Falcon XDR - MDR with Microsoft **APEX AIOps Incident Management** wykorzystuje AI do korelacji alertów pochodzących z wielu źródeł w czytelne incydenty.	**Dell Technologies Managed Detection and Response (MDR)** **APEX AIOps Incident Management**	✓
Cyfrowe Testy Odporności Operacyjnej	(24) Planowanie	Tworzenie szczegółowych planów testów, ustalanie harmonogramu, określenie zasobów	Narzędzia do zarządzania projektami		
	(25) Wdrożenie	Przeprowadzenie testów zgodnie z planem, monitorowanie przebiegu, dokumentowanie wyników	**Usługi IRRS** i **IRR** pomagają oragnizacjom przygotować sie na atak oraz odtworzyć się po ataku.	**Dell Services: Incident Recovery Retainer Service (IRRS)** **Dell Services: Incident Response & Recovery (IRR)**	✓
	(26) Zaawansowane testy	Symulacje ataków, testy penetracyjne, analiza wyników i wdrażanie usprawnień	**Penetration Testing and Attack Simulation -** umożliwia przegląd środowiska klienta oraz uruchomienie Breach Attack Simulation (BAS) na wskazanych komponentach infrastruktury. **Ransomware Readiness Assessment -** usługa mająca na celu ocenę zastosowanej technologii, narzędzi, kontroli bezpieczeństwa oraz konfiguracji w zakresie ochrony oraz odtwarzania po udanym ataku ransomware.	**Dell Advisory Services: Penetration Testing and Attack Simulation** **Dell Advisory Services: Ransomware Readiness Assessment**	✓
	(27) Niezależność / Odporność	Zapewnienie, że testy są niezależne, regularne przeglądy i aktualizacje planów	Systemy redundancji i disaster recovery		
Zarządzanie ryzykiem dostawców zewnętrznych ICT	(28) Rejestr	Stworzenie szczegółowego rejestru dostawców, regularne aktualizacje, monitorowanie ryzyka	**Zarządzanie ryzykiem dostawców zewnętrznych ICT,** to nie tylko zarządzanie ryzykiem związanym z dostawcami, ale również stawianie wysokich wymagań dot. bezpieczeństwa produktów oraz ich zgodności z normami – tj. normy NIST SP 800-193 w zakresie ochrony przed cyberatakami oraz mechanizmy zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania zgodnie z normami NIST SP 800-147B i NIST SP 800-155.		✓
	(28) Audyty	Regularne audyty bezpieczeństwa dostawców, dokumentowanie wyników, wdrażanie działań naprawczych			
	(28-29) Zarządzanie ryzykiem	Identyfikacja i ocena ryzyk związanych z dostawcami, monitorowanie ryzyk			
	(30) Kontrakty	Stworzenie i monitorowanie kontraktów z dostawcami, zapewnienie zgodności z wymaganiami bezpieczeństwa			
	(30) Strategia wyjścia	Opracowanie planów na wypadek zakończenia współpracy z dostawcą, minimalizacja ryzyka			
	(30) Zarządzanie dostawcami (4th Party)	Monitorowanie i ocena ryzyk związanych z dostawcami 4th party			
	(31) Krytyczni dostawcy (3rd Party)	Identyfikacja krytycznych dostawców, regularna ocena ich wpływu na działalność			
	(32-44) Nadzór	Ciągły nadzór nad dostawcami, regularne przeglądy ryzyk, ocena zgodności z umowami			
Wymiana Informacji	(45) Dzielenie się informacjami	Stworzenie mechanizmów i platform do bezpiecznej wymiany informacji, zapewnienie zgodności z regulacjami	Platformy do współpracy i udostępniania informacji		
	(45) Społeczność	Budowanie sieci kontaktów, organizacja szkoleń, konferencji i warsztatów	Narzędzia do zarządzania społecznościami online		

KLUCZOWE FUNKCJE I KORZYŚCI

Zgodność z regulacjami DORA to nie tylko wymóg prawny, ale przede wszystkim inwestycja w bezpieczeństwo i stabilność operacyjną Twojej organizacji.

Aby sprostać aktualnym wymaganiom regulacyjnym, niezbędne jest przyjęcie odpowiednich rozwiązań technologicznych i operacyjnych, które zapewnią zgodność z przepisami DORA, NIS2, ustawie o KSC, czy Rekomendacji D. To obowiązek, ale i wyzwanie dla organizacji, które powinny:

- **zainwestować w nowoczesne technologie**
- **zoptymalizować strategię zarządzania ryzykiem oraz bezpieczeństwa infrastruktury IT**
- **podnieść świadomość cyberbezpieczeństwa wśród pracowników**
- **współpracować z zaufanym partnerem.**

Wybór sprawdzonych, solidnych rozwiązań cyberbezpieczeństwa pozwoli łatwiej osiągnąć zgodność z najnowszymi regulacjami prawnymi oraz skutecznie chronić dane i systemy przed rosnącymi cyberzagrożeniami utrzymując ciągłość działania i niwelując ryzyka współpracy z dostawcami usług zewnętrznych.

DORA to szereg bardziej precyzyjnych wymagań względem wytycznych NIS2:

Zarządzanie ryzykiem ICT
DORA Rozdział II (Artykuły 5-10) dodaje szczegółowe wymagania dotyczące polityk zarządzania ryzykiem ICT, regularnej aktualizacji polityk, szkoleń dla personelu, mechanizmów kontroli i audytu, co uzupełnia **NIS2 Rozdział IV, Sekcje 20-21.**

Zarządzanie incydentami związanymi z ICT, klasyfikacja i raportowanie
DORA Rozdział III (Artykuły 11-14) precyzuje szczegółowe procedury zarządzania incydentami, klasyfikację incydentów według ich wpływu, obowiązki raportowania oraz dokumentację i analizę po incydencie, co uzupełnia **NIS2 Rozdział IV, Sekcja 23.**

Testowanie cyfrowej odporności operacyjnej
DORA Rozdział IV (Artykuły 15-18) szczegółowo opisuje obowiązek regularnych testów penetracyjnych, ćwiczeń symulacyjnych oraz innych form testowania odporności operacyjnej i raportowania co uzupełnia **NIS2 Rozdział IV, Sekcja 24.**

Zarządzanie ryzykiem stron trzecich związanych z ICT
DORA Rozdział V, Sekcja I (Artykuły 19-21) precyzuje zasady zarządzania ryzykiem stron trzecich, wprowadzając szczegółowe wytyczne dotyczące oceny ryzyka związanego z dostawcami zewnętrznymi, wymogi dotyczące umów z dostawcami, monitorowania ich działalności oraz planowania ciągłości działania, co uzupełnia **NIS2 Rozdział V.**

Rejestracja i jurysdykcja
DORA Rozdział V, Sekcja II (Artykuły 22-23) precyzuje obowiązki rejestracji wszystkich dostawców usług ICT dla instytucji finansowych oraz określa jurysdykcję organów nadzoru, co uzupełnia w **NIS2 Rozdział V.**

Umowy o udostępnianiu informacji
DORA Rozdział VI (Artykuły 24-25) doprecyzowuje zasady dotyczące umów o udostępnianiu informacji między instytucjami finansowymi, co uzupełnia wytyczne **NIS2 Rozdział VI.**

Właściwe organy i nadzór
DORA Rozdział VII (Artykuły 26-30) szczegółowo opisuje role organów nadzorczych w sektorze finansowym, co uzupełnia **NIS2 Rozdział VII.**

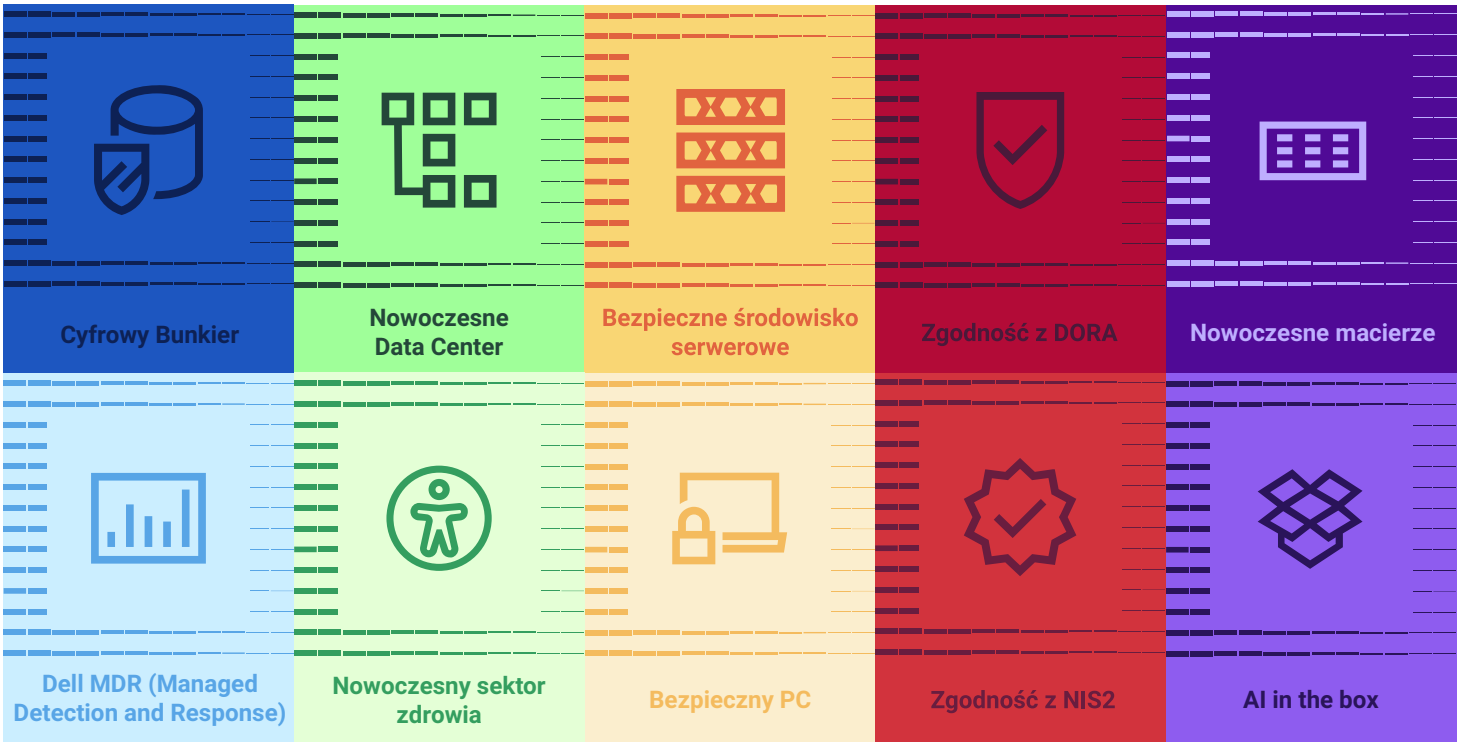
ZOBACZ TAKŻE

> Zgodność z NIS2 – cyberbezpieczeństwo w zgodzie z dyrektywą europejską

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

> Cyfrowy Bunkier – nowy standard cyfrowej odporności organizacji

Kompas IT – innowacyjne rozwiązania dla efektywności i cyfrowej odporności IT



Poznaj rozwiązania Dell Technologies

Porozmawiajmy o efektywnych strategiach bezpieczeństwa cyfrowego i zgodności z DORA

Bartosz Charlinski
Enterprise Architect

Bartosz.Charlinski@dell.com

Karol Smuś
Account Executive
Banking and Finance Sector Lead

Karol.Smus@dell.com

DELL Technologies