

RiscRecon - W jaki sposób firmy mogą zachować zgodność z przepisami DORA?

Czym jest DORA i jaki są jej filary?

Zatwierdzony przez Parlament Europejski w listopadzie 2022 r. akt DORA EU (Digital Operational Resilience Act) pokazuje, jak zmienia się zgodność regulacyjna w sektorze finansowym. Po pełnym wdrożeniu akt ten pomoże dostosować strategię instytucji finansowych w zakresie bezpieczeństwa i prywatności do zmieniających się oczekiwań w zakresie odporności cyfrowej i zarządzania ryzykiem związanym z ICT. DORA skłoni firmy do skupienia się na wdrażaniu strategii odporności cyfrowej, której towarzyszyć będą stale ewoluujące ramy oceny ryzyka i bezpieczeństwa.

DORA ustanawia ramy dla każdego dostawcy usług sektora finansowego i jego dostawców, których należy przestrzegać, aby utrzymać odporność operacyjną. Niektóre z kluczowych filarów redukcji ryzyka obejmują:

- **Proaktywne zarządzanie ryzykiem i ład korporacyjny:** DORA określa wytyczne dotyczące minimalizacji ryzyka w sektorze finansowym. Wytyczne te zachęcają firmy do tworzenia bardziej dojrzałych programów zarządzania ryzykiem i wykorzystywania narzędzi do monitorowania usług ICT.
- **Testowanie odporności:** Aby zachować odporność w sektorze usług finansowych, firmy będą zobowiązane do wdrożenia procesów testowania i oceny ryzyka. Może to obejmować użycie zautomatyzowanych narzędzi do identyfikowania i rozwiązywania problemów, zanim zagrożą one działalności.
- **Udostępnianie danych wywiadowczych:** Wielu cyberprzestępców działających w branży finansowej może próbować atakować wiele organizacji jednocześnie. DORA zachęca do dzielenia się informacjami o zagrożeniach w celu zwiększenia świadomości potencjalnych zagrożeń cybernetycznych.
- **Zarządzanie łańcuchem dostaw:** DORA nakłada na instytucje finansowe surowe wymagania dotyczące zarządzania relacjami z dostawcami, takimi jak dostawcy usług ICT. Każda firma finansowa musi mieć wdrożone strategie zarządzania ryzykiem związanym z krytycznymi połączeniami z osobami trzecimi.
- **Zgłaszanie incydentów:** DORA stara się usprawnić proces zgłaszania, zachęcając do szybkiego dochodzenia i reagowania w celu zmniejszenia wpływu naruszeń. Szczegółowe informacje o naruszeniach mogą być również używane do wykrywania włamań w innych środowiskach sieciowych.
- **Audyty:** Dzięki przepisom DORA organy regulacyjne i instytucje finansowe są uprawnione do przeprowadzania audytów w całym łańcuchu dostaw sektora finansowego. Oznacza to, że firmy muszą mieć możliwość generowania raportów na żądanie.
- **Analiza retrospektywna:** DORA zachęca do badania i rewizji polityk w oparciu o incydenty zarówno wewnętrzne, jak i zewnętrzne. Ma to na celu zmniejszenie ryzyka, że wiele firm finansowych zostanie dotkniętych tymi samymi rodzajami ataków.

W jaki sposób RiskRecon może mi pomóc?

Dzięki RiskRecon firmy mogą kompleksowo oceniać ryzyko związane z osobami trzecimi i łańcuchem dostaw oraz proaktywnie monitorować swój krajobraz zagrożeń, upewniając się, że są one zgodne z najnowszymi przepisami. Wygodny ekosystem zapewnia kompleksową widoczność, cenne narzędzia do raportowania i dogłębną analitykę dla firm z różnych branż.

DORA Industry Standard					
Control ID	Control Description	Compliance			
Article 5 (2)	2. The ICT risk management framework referred to in paragraph 1 shall include strategies, policies, procedures, ICT protocols and tools which are necessary to duly and effectively protect all relevant physical components and infrastructures, including computer hardware, servers, as well as all relevant premises, data centres and sensitive designated areas, to ensure that all those physical elements are adequately protected from risks including damage and unauthorized access or usage.	Related Information	Rating	Issues	Issue Rate
		Hosting Providers	Info	-	-
		Geolocation Hosts	Info	-	-
Article 5 (3)	3. Financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, protocols and tools as determined in the ICT risk management framework. They shall provide complete and updated information on ICT risks as required by the competent authorities.	Assessment Criteria	Rating	Issues	Issue Rate
		Software Patching	A 10	0	0%
		Application Security	F 2.9	9	47%
		Web Encryption	F 3.9	5	6%
		System Reputation	A 10	0	0%
		Email Security	A 10	0	0%
		DNS Security	A 10	0	-
		Network Filtering	F 2.0	3	25%

1. Wizualizacja fragmentu automatycznego raportu dotyczącego spełnienia DORA

RiskRecon by Mastercard to innowacyjny dostawca rozwiązań, gotowy wspierać firmy w dążeniu do zgodności z DORA. Technologia RiskRecon zapewnia zautomatyzowaną ocenę ryzyka dostosowaną na do wymagań każdego użytkownika.

Czy powyższe rozwiązanie wpasowuje się w twoje potrzeby ?

Zapraszamy do zapoznania się z pełną prezentacją:

https://www.youtube.com/watch?v=1582Vgl2r_w

Zapraszamy do kontaktu w celu umówienia dedykowanej prezentacji:

kontakt@prianto.pl