CryptoPanel

edycja #27

Już za moment zaczynamy...

CryptoPanel

edycja #27

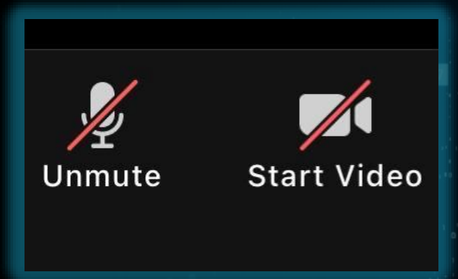
THALES
Building a future we can all trust

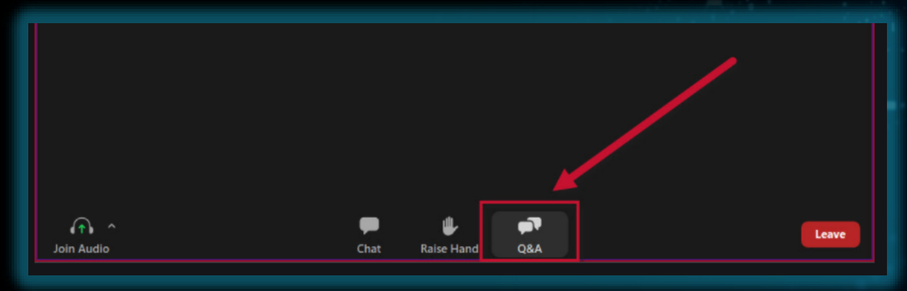
imperva
a Thales company

CLICO

CryptoPanel

edycja #27





CryptoPanel

6 MAJA 11:00

DORA – jak rozwiązania ochrony danych Thales pomagają spełnić wymagania unijnego rozporządzenia.

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel

Dyskusje poprowadzą: Piotr Majek i Jarosław Ulczok

Dora...

Nis2...

Joanna Rzepka

Channel Sales Manager
Joanna.rzepka@thalesgroup.com
mob. +48 600 537 666

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

problem

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Nasz problem (czyli Ty masz problem)

- Nasza firma prowadzi działalność na ogólnie pojętym rynku finansowym
- Z wejściem rozporządzenia DORA jesteśmy zobligowani do wprowadzenia zmian w naszych systemach ICT do jej spełnienia
- Co z innymi regulacjami (NIS2, RODO, …)?
- Jakich rozwiązań do ochrony danych może użyć?
- …

- Musimy również uzyskać informacje o sposobach zarządzania ryzykiem od naszych poddostawców ICT
- Kontrakty opieki (maintenance) są kwalifikowane przez nas jako usługi ICT, w związku z czym mamy obowiązek umieścić odpowiednie zapisy w umowach i wymagać określonych zachowań od dostawców (np. zgłaszania incydentów i podatności)
- …

Geneza

Słownik języka polskiego PWN*

geneza

1. «czynniki, które złożyły się na powstanie i rozwój czegoś»
2. «sposób powstawania i rozwoju czegoś»

Słownik języka polskiego pod red. W. Doroszewskiego*

…w zasadzie są dwa…

Powody, dla których podmioty wprowadzają rozwiązania ochrony danych:

Bezpieczeństwo

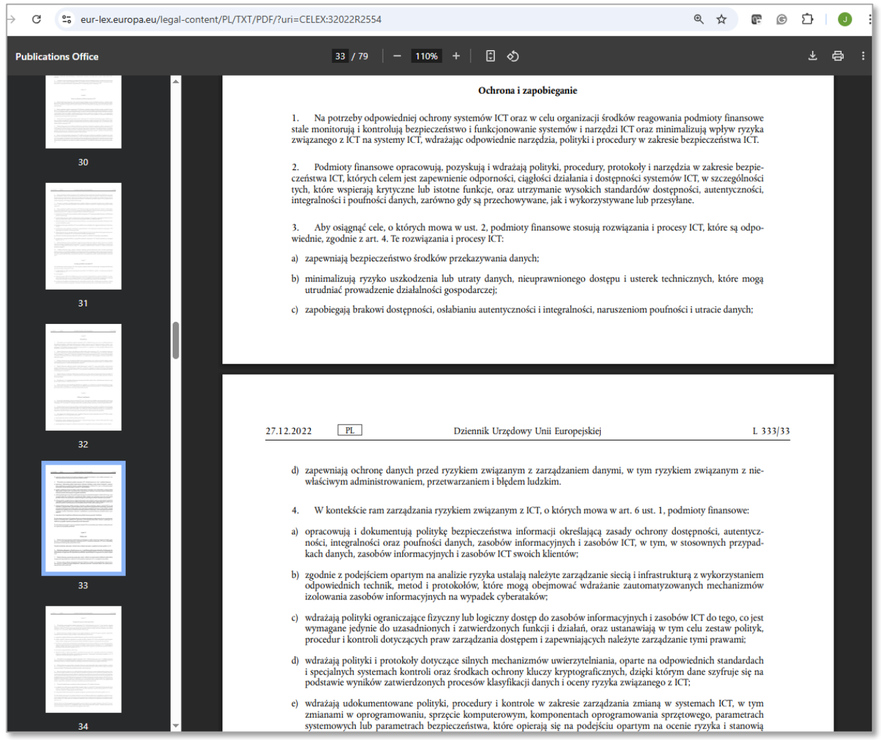
Zgodność

NIS2, DORA, CER, PCI, KSC, KNF, ISO…

Kluczowe wymagania regulacyjne dla Europy

	DORA	NIS 2	GDPR	PCI DSS 4.0	ISO 27001:2022
Czego dotyczy?	Ustala jednolite wymagania dotyczące bezpieczeństwa sieci i systemów informacyjnych w celu zwiększenia odporności instytucji finansowych na cyberataki	Ma na celu ograniczenie zagrożeń dla sieci i systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych oraz zapewnienie ciągłości.	Zostało zaprojektowane w celu poprawy ochrony danych osobowych i zwiększenia odpowiedzialności za naruszenia danych; reguluje użycie, przetwarzanie i przechowywanie danych osobowych.	Standaryzuje środki bezpieczeństwa, które muszą być wdrożone przez firmy przetwarzające dane kart płatniczych.	Najbardziej znany na świecie standard systemów zarządzania bezpieczeństwem informacji (ISMS). Zapewnia wytyczne dotyczące ustanawiania, utrzymywania i doskonalenia ISMS.
Kogo dotyczy?	Instytucje finansowe oraz kluczowych poddostawców usług ICT (np. dostawcy usług chmurowych i analityki danych).	Infrastruktura krytyczna, taka jak energetyka, transport, sektor finansowy, zdrowotny oraz kluczowi dostawcy usług.	Wszystkie organizacje w UE oraz organizacje zagraniczne przetwarzające dane osobowe obywateli UE.	Organizacje przetwarzające dane kart płatniczych.	Organizacje ze wszystkich sektorów gospodarki: prywatne, publiczne i non-profit.
Kary	10 mln EUR lub 2% globalnego rocznego obrotu.	10 mln EUR lub 2% globalnego rocznego obrotu.	10 mln EUR lub 2% globalnego rocznego obrotu.	- Grzywny do 100 000 USD - Zatrzymanie przetwarzania kart płatniczych	Brak kar, ale certyfikacja ISO 27001 może pomóc w ochronie przed karami wynikającymi z innych przepisów.
Jak Thales pomaga?	Wsparcie w zakresie zarządzania ryzykiem ICT (rozdział II) oraz zarządzania ryzykiem związanym ze stronami trzecimi ICT (rozdział V).	Thales wspiera organizacje w spełnieniu wymagań NIS 2, pomagając we wdrożeniu środków zarządzania ryzykiem cyberbezpieczeństwa określonych w rozdziale 21.	Pomoc w spełnieniu wymagań RODO, poprzez dostarczenie rozwiązań zabezpieczających dane osobowe i ich bezpieczeństwo.	Thales oferuje kompleksowe rozwiązania sprzętowe i programowe pomagające organizacjom spełniać kluczowe zasady PCI DSS.	Thales wspiera organizacje w spełnianiu wymagań ISO 27001, pomagając wdrażać niezbędne środki bezpieczeństwa wymienione w Aneksie A dotyczącym Kontroli Bezpieczeństwa Informacji.

DORA



[Treść rozporządzeni w j. Polskim: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022R2554](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022R2554)

Dobra strategia ochrony danych - wdrożona, utrzymywana i rozwijana poprawnie - umożliwia spełnienie wielu wymagań rozporządzenia DORA w zakresie zarządzaniem ryzykiem IT i poprawy cyfrowej odporności operacyjnej.

CryptoPanel

rozwiązanie

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Zgodność z

Digital Operational Resilience Act (DORA)

Thales pomaga organizacjom spełniać wymagania regulacji DORA poprzez realizację wymagań zawartych w **rozdziale II** dotyczącym zarządzania ryzykiem oraz w **rozdziale V** dotyczącym zarządzania ryzykiem związanym z firmami trzecimi.

Wymaganie	Art. DORA	Wspierające rozwiązanie Thales
Chapter II: ICT Risk Management		
Identify and classify	8.1	Data Discovery and Classification
Protect data at rest, in use or in transit	9.2	Transparent Encryption; Tokenization; High Speed Encryptors (HSE)
Access management	9.3,b 9.4,c	Identity and Access Management; Consent and Preference Management; Transparent Encryption
Implement multi-factor authentication	9.4	SafeNet Trusted Access
Securely manage cryptographic keys	9.4	Enterprise Key Management; Hardware Security Modules (HSMs)
Monitor and detect anomalous activities	10.1	SafeNet Trusted Access; Transparent Encryption
Chapter V: Managing of ICT Third Party Risk		
Mitigate risks of third-party service providers	28.8	Cloud Key Management; Transparent Encryption

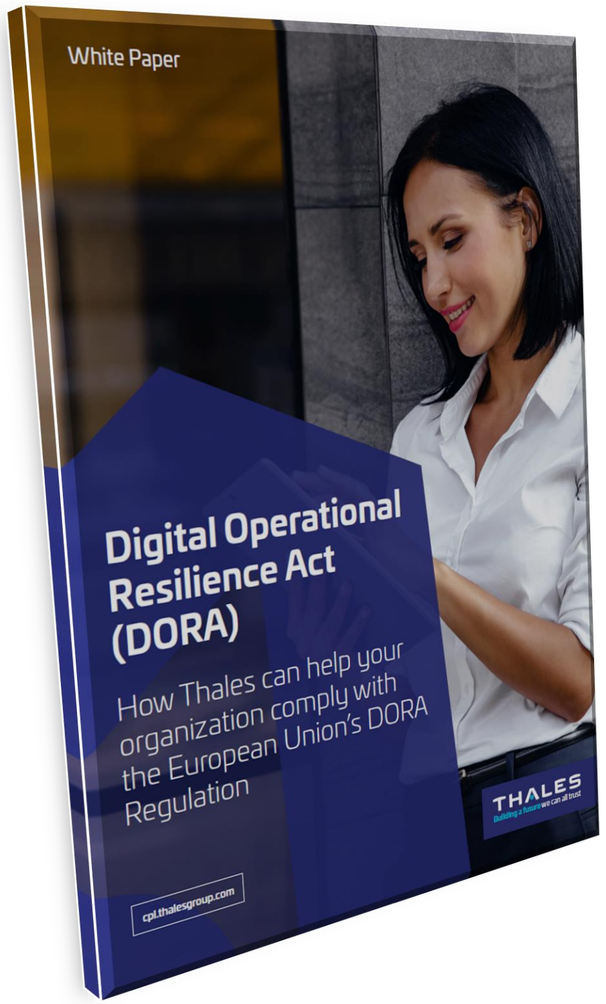
Jak rozwiązania Thales (DataSec) pomagają w spełnieniu DORA?

Wymaganie DORA	Rozwiązanie z Thales	
8.1: *„…**identyfikować, klasyfikować** i odpowiednio dokumentować zasoby informacyjne…"*	 **CipherTrust Data Discovery and Classification**	Identyfikuje wrażliwe dane ustrukturyzowane i nieustrukturyzowane w środowiskach lokalnych i chmurowych. Wbudowane szablony umożliwiają szybkie wykrywanie danych regulowanych, wskazują ryzyka bezpieczeństwa i pomagają zidentyfikować luki w zgodności.
9.2: *„…utrzymywać wysokie standardy dostępności, autentyczności, integralności i poufności **danych w spoczynku, podczas użytkowania oraz w transmisji…"***	 **CipherTrust Transparent Encryption**	Zzapewnia szyfrowanie danych w spoczynku dla plików, folderów oraz kontrolę dostępu uprzywilejowanych użytkowników. Chroni dane wszędzie — lokalnie, w chmurze oraz w środowiskach Big Data i kontenerowych
	 **CipherTrust Tokenization**	Umożliwia pseudonimizację wrażliwych danych w bazach danych z zachowaniem możliwości analizy danych zbiorczych, bez ujawniania danych podczas analizy czy w raportach.
	 **High Speed Encryptor (HSE)**	Zapewnia niezależne od sieci szyfrowanie danych w transmisji (data-in-motion), zabezpieczając dane, wideo, głos i metadane podczas przesyłania między lokalizacjami lub między środowiskiem lokalnym a chmurą i z powrotem.
9.3.b: „…minimalizować ryzyko nieautoryzowanego dostępu…"	 **OneWelcome Identity & Access Management**	Ogranicza dostęp użytkowników wewnętrznych i zewnętrznych na podstawie ich ról oraz kontekstu. Stosuje polityki autoryzacji, aby upewnić się, że odpowiedni użytkownik otrzymuje dostęp do właściwego zasobu we właściwym czasie.
9.4.c: *Wdrażać polityki **ograniczające fizyczny i wirtualny dostęp do zasobów systemów ICT i danych tylko do tego, co jest wymagane dla uzasadnionych i zatwierdzonych funkcji.***	 **OneWelcome Consent and Preference Mgmt.**	Umożliwia organizacjom pozyskiwanie zgody użytkowników końcowych, zapewniając przejrzystość w zakresie dostępu do danych i umożliwiając zarządzanie danymi, do których organizacja ma uprawnienia.
	 **CipherTrust Transparent Encryption**	Umożliwia wieloskładnikowe uwierzytelnianie (MFA) z najszerszym zakresem metod sprzętowych i programowych oraz form faktorów. Pozwala organizacjom adresować różnorodne scenariusze użycia, poziomy bezpieczeństwa oraz wektory zagrożeń w ramach zunifikowanych polityk.
9.4.d: „… mechanizmy silnego uwierzytelniania…"	 **SafeNet Trusted Access**	Umożliwia wieloskładnikowe uwierzytelnianie (MFA) z najszerszym zakresem metod sprzętowych i programowych oraz form faktorów. Pozwala organizacjom adresować różnorodne scenariusze użycia, poziomy bezpieczeństwa oraz wektory zagrożeń w ramach zunifikowanych polityk.

Jak rozwiązania Thales (DataSec) pomagają w spełnieniu DORA?

Wymaganie DORA	Rozwiązanie z Thales	
9.4.d: „…środki ochrony kluczy kryptograficznych, *za pomocą których dane są szyfrowane."*	**Luna HSMs**	Chronią klucze kryptograficzne i zapewniają sprzętowe moduły bezpieczeństwa (HSM) zgodne z FIPS 140-2 Level 3, odporne na manipulację, przeznaczone do bezpiecznego przetwarzania kryptograficznego, generowania i ochrony kluczy, szyfrowania i innych operacji.
	CipherTrust Enterprise Key Management	Usprawnia i wzmacnia zarządzanie kluczami w chmurze i środowiskach lokalnych dla własnych systemów szyfrowania oraz aplikacji firm trzecich.
10.1: „…wykrywać nietypowe aktywności… monitorować aktywność użytkowników…"	**CipherTrust Transparent Encryption**	Generuje logi bezpieczeństwa przyspieszające wykrywanie zagrożeń, współpracując z narzędziami SIEM i systemami bezpieczeństwa. Funkcje ochrony przed ransomware pozwalają administratorom na wykrywanie i blokowanie podejrzanych aktywności zanim ransomware się rozprzestrzeni.
	OneWelcome Identity & Access Management	Łączy funkcje pojedynczego logowania (SSO) i polityk dostępowych opartych na scenariuszach w chmurowym rozwiązaniu do zarządzania dostępem. Obszerne, zautomatyzowane raporty rejestrują wszystkie aspekty dostępu i uwierzytelniania w formie logów, które mogą być przesyłane do systemów SIEM.
28.8: „Dla usług ICT [stron trzecich] wspierających krytyczne lub istotne funkcje, **instytucje finansowe powinny wdrożyć strategie wyjścia."**	**CipherTrust Cloud Key Management**	Ogranicza ryzyko związane z dostawcami usług zewnętrznych dzięki utrzymaniu kluczy szyfrujących lokalnie, pod pełną kontrolą instytucji finansowej — bez przekazywania ich do chmury publicznej.
	CipherTrust Transparent Encryption	Zapewnia pełne rozdzielenie ról, gdzie tylko autoryzowani użytkownicy i procesy mogą przeglądać zaszyfrowane dane. Dzięki temu pracownicy dostawców usług chmurowych, np. inżynierowie wsparcia czy administratorzy baz danych, nie mają dostępu do danych w formie jawnej.

Jak rozwiązania Thales + Imperva (DataSec) pomagają z DORA



Mapping Thales Capabilities to DORA Requirements

Requirement	How Thales helps	Solution Areas
ICT Risk Management and Governance		
Article 8.1: "...**identify, classify** and adequately document information assets..."	• Discover and classify potential risk for all public, private, and shadow APIs. • Identify structured and unstructured sensitive data at risk on-premises and in the cloud. • Identify current state of compliance, documenting gaps, and providing a path to full compliance.	**Application Security** API Security **Data Security** Data Discovery & Classification Data Risk Analytics Vulnerability Management
Article 9.2: "...**maintain** high standards of availability, authenticity, integrity and **confidentiality of data, whether at rest, in use or in transit.**"	• Encrypt data-at-rest on-premises, across clouds, and in big data or container environments. • Pseudonymize sensitive information in databases. • Protect data in motion with high-speed encryption. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document.	**Data Security** Transparent Encryption Tokenization Key Management High Speed Encryption Data Governance Data Activity Monitoring
Article 9.4, b: "...implementing automated mechanisms **to isolate affected information assets in the event of cyber-attacks;**"	• Detect and prevent cyber threats with web application firewall, ensuring seamless operations and peace of mind. • Safeguard critical network assets from DDoS attacks and Bad Bots while continuing to allow legitimate traffic. • Data activity monitoring for structured and unstructured data across cloud and on premises systems.	**Application Security** Web Application Firewall DDoS Protection Bot Protection API Protection **Data Security** Data Activity Monitoring Data Risk Analytics

Article 9.4, c: "...**implement policies that limit the physical and virtual access** to ICT system resources and data to what is required only for legitimate and approved functions and activities..."	• Limit the access of internal and external users to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Leverage smart cards for implementing physical access to sensitive facilities.	**Identity & Access Management** Workforce Access Management **Data Security** Transparent Encryption Data Risk Analytics
Article 9.4, d: "...implement policies and protocols for **strong authentication** mechanisms..."	• Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods and form factors. • Build and deploy adaptive authentication policies based on the	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication

https://cpl.thalesgroup.com/resources/compliance/dora-compliance-solutions-for-financial-sector-white-paper

Z grubsza, „To by było na tyle”

NARODOWE CENTRUM KULTURY

Dawno, dawno temu, jakoś tak pod koniec XX w., aktor, satyryk i radiowiec co się zowie Jan Tadeusz Stanisławski pozwolił sobie - na antenie - na żart językowy: zakończył swój monolog słowami „To by było na tyle”. Była to kontaminacja (świadoma oczywiście) dwóch formułek kończących: „to byłoby wszystko” i „to tyle na dziś”. Nowe sformułowanie, żartobliwe a krągłe, spodobało się publiczności, więc

Ale..

Wprowadzanie zgodność z Rozporządzeniem DORA przez podmioty finansowe powoduje, że…

…instytucje finansowe muszą wymagać od swoich dostawców spełnienia wymagań (Supply Chain Risk Management) w tym od Thales CPS i Imperva.

Jednakże…

- Imperva or Thales are NOT directly regulated under DORA

Jednak dokładamy starań!

Rozporządzenie DORA

Rozporządzenie o cyfrowej odporności operacyjnej – rozporządzenie Unii Europejskiej 2022/2554 wymagające od podmiotów finansowych poprawy odporności operacyjnej w środowisku cyfrowym.

Source: Wikipedia

Jak firma Thales wypełnia wymagania regulacji DORA, **jako zewnętrzny dostawca usług ICT** (DPoD), zapewniając cyfrową odporności operacyjnej dla firm sektora finansowego?

Ensuring Digital Operational Resilience with Thales Data Protection on Demand (DPoD)

https://cpl.thalesgroup.com/resources/encryption/dora-compliance-thales-dpod-white-paper

Co robimy w zakresie swoich usług (w DPoD) dla przestrzegania DORA

Firma Thales jako zewnętrzny dostawca usług dla firm z sektora finansowego przygotowała opis w jaki sposób usługi zarządzania kluczami, szyfrowania plików oraz modułów HSM dostępne na platformie Thales Data Protection on Demand (DPoD) pomagają spełniać zgodność z rozporządzeniem DORA.

Ponadto frima Thales - jako zewnętrzny dostawca usług - sam przestrzega zapisów rozporządzenia DORA, zapewniając dodatkową warstwę zaufania dla instytucji finansowych korzystających z jego usług. Aby zagwarantować zgodność DPoD z tymi wymaganiami, Thales wdrożył rygorystyczny program zgodności, który obejmuje m.in:

- **Samoocenę (self-assessment) – regularne wewnętrzne audyty oceniające zgodność z wymaganiami DORA.**
- **Oceny zewnętrzne (external-assessment)– współpracę z zewnętrznymi audytorami, którzy przeprowadzają niezależne analizy zgodności z DORA oraz innymi regulacjami.**

Dzięki jasno określonemu celowi i udokumentowanemu doświadczeniu w dostarczaniu rozwiązań chroniących dane, a także certyfikatom takim jak ISO 27001, SOC 2 i CSA STAR Level 2, platforma DPoD zapewnia solidne podstawy cyberbezpieczeństwa oraz silne zaangażowanie w zarządzanie ryzykiem ICT.

Thales a DORA?

Dokument z opisem starań dot. wypełnienia regulacji DORA obejmuje tylko usługi w DPoD.

- Ponieważ to faktycznie usługi ICT, dla których definiujemy SLA.

Jednakże klienci upatrują licencje w postaci subskrypcji (*term based*) oraz opiekę do produktów sprzętowych (*maintenance*) jako rodzaj usługi świadczonej przez Thales.

- CipherTrust Manager, Luna 7 HSM, itd.

… i oczekują podpisania dodatkowych umów (sic!) **do EULA lub kontraktów wsparcia.**

- Umowy z klientami końcowymi może procesować tylko dział prawny Thales (Legal)
- Trudny i długotrwały proces i poza zakresem Sales i Pre-Sales.
- Co ciekawe, takie żądania otrzymaliśmy tylko z RP, nie obserwujemy tego w innych krajach CEE.

Uwaga końcowa #1

„Specifically on DORA, the approach we are taking is to review each customer/financial entity's standard addendum template.

As DORA indirectly affects Thales (versus directly affecting the financial entities), we have decided this is the appropriate response. We have been engaging with customers for the last few months on this process on a case-by-case basis. „

Thales Legal Representative

W przypadku DORA nasze podejście polega na przeglądaniu standardowego szablonu dodatku każdego klienta/podmiotu finansowego. Ponieważ DORA pośrednio wpływa na Thales (a nie bezpośrednio na podmioty finansowe), uznaliśmy, że jest to właściwa odpowiedź. Przez ostatnie kilka miesięcy współpracowaliśmy z klientami w tym procesie, rozpatrując każdy przypadek indywidualnie.

Właściwy zespół do kontaktu w sprawach związanych z tymi kwestiami to:
cplcommerciallegal@thalesgroup.com

CryptoPanel

podsumowanie

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Coś na wynos

Dobra strategia ochrony danych - wdrożona, utrzymywana i rozwijana poprawnie - umożliwia spełnienie wielu wymagań rozporządzenia DORA (i innych) w zakresie zarządzaniem ryzykiem IT i poprawy cyfrowej odporności operacyjnej.

Czego potrzebujemy?

- Rozporządzenia DORA (i innych) nie dla się zaadresować poprzez zakup takiego czy innego rozwiązania.
- Musimy podjąć działania, konkretny produkt lub rozważanie mogą jedyne pomóc.
- Potrzebna jest strategia ochrony danych budowa w oparciu o platformę.

Analysts advise a platform approach to improve data security

> By 2025, **30%** of enterprises will have adopted broad-spectrum data security platforms, up from less than 10% in 2021, due to the pent-up demand for higher levels of data security and the rapid **increase in product capabilities.**

Gartner. 2023
Strategic Roadmap for Data Security Platform Adoption

The Gartner Approach

…strategia…

ZNAJDŹ

Znajdź wrażliwe dane, gdziekolwiek się znajdują, i klasyfikuj je

CHROŃ

Chroń wrażliwe dane za pomocą szyfrowania lub tokenizacji

KONTROLUJ

Kontroluj dostęp do danych i centralizuj zarządzanie kluczami i politykami

…uwag praktycznych kilka: budowa strategii ochrony danych

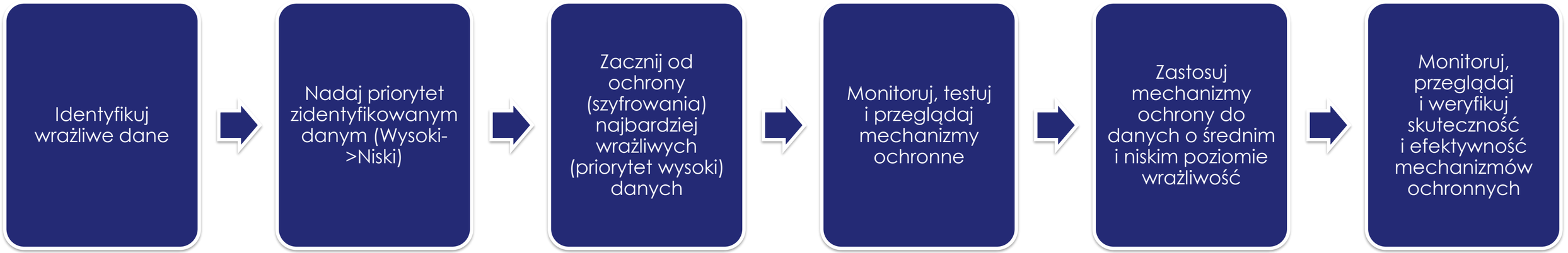
Ochrony danych nie da się wprowadzić z dnia na dzień

Należy określić szczegółową i jasną strategię, biorąc pod uwagę wiele krytycznych czynników, takich jak:

- Poziomy wrażliwości danych, lokalizacje, typ i rozmiar danych
- Dostępność danych
- Poziomy zapewnienia bezpieczeństwa
- Typy infrastruktury
- Procedury wymagające dostępu do danych (mapowanie danych na procesy)
- Krótko- i długoterminowe cele biznesowe, które mają wpływ na dane wrażliwe
- Dojrzałość organizacyjna w zakresie ochrony danych
- Bieżące kontrole, polityki wewnętrzne i procedury w zakresie ochrony danych
- Lokalne i międzynarodowe prawo oraz przepisy i regulacje (KSC, RODO, NIS2, **DORA,** CER, CR**A**…)
- Przepisy branżowe (np. KNF, …)
- Nadchodzące aktualizacje technologiczne i biznesowe (komputer kwantowy, rekomendacje NIST, ABW,

…uwag praktycznych kilka: strategia ochrony danych, jak wdrażać?

- **Strategię ochrony danych wdrażaj stopniowo**
- **Zawsze monitoruj i przeglądaj skuteczność i wydajność wdrożonych środków ochrony**
  - Czy ochrona spełniają swoje cele? Jak wdrożone środki obciążają zasoby?
- **Kiedy dostatecznie przetestowane, zaimplementuj kolejne środki**
- **Prośba osobista: uwzględnij ochronę danych na możliwie wczesnym etapie swoich projektów**



THALES

CryptoPanel

teraz pytania i odpowiedzi

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel