VÁŠ PARTNER PRO KYBERNETICKOU BEZPEČNOST

DORA (Digital Operational Resilience Act) je nařízení Evropské unie, které stanovuje pravidla a požadavky na zajištění digitální odolnosti finančních institucí a dalších organizací. Bylo přijato za účelem posílení bezpečnosti, ochrany dat a prevence kybernetických útoků v digitálním prostoru a vstoupilo v platnost 16. ledna 2023. Dotčené organizace mají 24 měsíců na jeho implementaci.

KYBERNETICKÁ ODOLNOST VE FINANČNÍM SEKTORU

Provozní hrozby v sektoru finančních služeb jsou na vzestupu. Proto se nařízení DORA nezabývá pouze jednorázovou implementací nových předpisů. Jeho cílem je naopak nastavení dlouhodobé odolnosti organizací vůči měnícím se hrozbám ve stále složitějším technologickém prostředí. To s sebou nese řadu nových povinností.

POVINNOSTI DOTČENÝCH ORGANIZACÍ

- Rámec řízení rizik – zavedení spolehlivých procesů pro řízení rizika a komplexní a účinný rámec pro jejich řízení.
- Zavedení bezpečnostních opatření – zavedení technických, organizačních, procesních nebo administrativních bezpečnostních opatření.
- Bezpečnostní incidenty – implementace funkčního procesu pro řízení kybernetických incidentů. Od identifikace a popsání postupu, přes proces obnovy dat, odstranění příčin incidentu až po notifikaci dohledového orgánu.
- Penetrační testy – pravidelné testování digitální odolnosti formou penetračních testů. Testování jednotlivých systémů a aplikací, ověřování funkčnosti procesů řízení kybernetických incidentů apod.
- Kontrola dodavatelů, subdodavatelů a dalších článku v dodavatelském řetězci aneb řízení rizika třetích stran a monitoring.

DOTČENÉ ORGANIZACE

FINANČNÍ SUBJEKTY:

- úvěrové instituce,
- platební instituce,
- instituce elektronických peněz,
- investiční podniky,
- poskytovatelé služeb souvisejících s kryptoaktivy,
- centrální depozitáře cenných papírů,
- ústřední protistrany,
- obchodní systémy,
- registry obchodních údajů,
- správci alternativních investičních fondů a správcovské společnosti,
- poskytovatelé služeb hlášení údajů,
- pojišťovny a zajišťovny,
- zprostředkovatelé pojištění, zprostředkovatelé zajištění a zprostředkovatelé doplňkového pojištění,
- instituce zaměstnaneckého penzijního pojištění,
- ratingové agentury,
- statutární auditoři a auditorské společnosti,
- správci kritických referenčních hodnot,
- poskytovatelé služeb skupinového financování.

POSKYTOVATELÉ SLUŽEB TŘETÍCH STRAN V OBLASTI ICT (PŘÍKLADY)

- **poskytovatelé služeb cloud computingu,**
- **poskytovatelé služeb datových center,**
- **poskytovatelé software,**
- **služby analýzy dat,**
- **subjekty poskytující činnosti související se zpracováním plateb nebo provozující platební infrastrukturu,**
- **apod...**

ODPOVĚDNOST ZA PLNĚNÍ POVINNOSTÍ

Odpovědnost za plnění požadavků nese vedení dané organizace. To bude odpovědné za přezkoumání, schválení, zavedení a aktualizaci rámce řízení rizik.

ZAJISTĚTE SI DIGITÁLNÍ ODOLNOST VAŠÍ ORGANIZACE V SOULADU S NAŘÍZENÍM EU S CRA A ZÍSKEJTE CERTIFIKÁT SOULADU S NAŘÍZENÍM DORA. NABÍZÍME VÁM TYTO SLUŽBY:

I. ANALÝZA A HODNOCENÍ RIZIK

- Identifikace kritických oblastí,
- Hodnocení rizik dle nařízení DORA.

II. TECHNICKÝ AUDIT

- Zhodnocení výsledků penetračního testování,
- Kontrola zabezpečení podle požadavků nařízen DORA,
- Zálohování a obnova dat.

III. HODNOCENÍ SOULADU A DOKUMENTACE

- Identifikace kritických oblastí,
- Dokumentace zajištění a doporučená nápravná opatření,
- Vypracování závěrečné zprávy.

PROČ S CRA?

- Máme rozsáhlé zkušenosti v oblasti ICT, bezpečnosti a regulace IT,
- Kvalifikace, schopnosti a znalosti v oblasti kybernetické a informační bezpečnosti včetně testování metodou Red Team v případě penetračních testů,
- Jsme provozovatelem kritické infrastruktury státu a členem bezpečnostního projektu Fenix,
- Máme dostatečné profesní pojištění,
- Jsme certifikovaným držitelem všech bezpečnostních norem (ISO/IEC 27001:2013, ISO/IEC 27017:2017, ISO/IEC 27018:2019, SOC 2 type 1 a 2),

- Poskytujeme služby na míru vašim specifickým potřebám s nepřetržitou podporou. Víme, co potřebujete a dokážeme vám pomoci.

PŘIPRAVTE SE NA BUDOUCNOST!
ZAJISTĚTE, ŽE VAŠE ORGANIZACE SPLŇUJE VŠECHNY POŽADAVKY NA DIGITÁLNÍ ODOLNOST.