POVINNOSTI VYPLÝVAJÍCÍ Z NAŘÍZENÍ DORA

POŽADAVKY NA DODAVATELE

A SOUVISEJÍCÍ AKTIVITY PROVÁDĚNÉ NA STRANĚ FINANČNÍ INSTITUCE V POZICI ODBĚRATELE (dále jen „ČSOB“)

ČSOB

jdeme vám naproti

ÚVOD DO PRAVIDEL DORA PRO ICT SLUŽBY

- **Co je DORA**: Nařízení Evropské unie o digitální provozní odolnosti pro finanční sektor (EU 2022/2554), které má zajistit, aby finanční instituce byly lépe připraveny na digitální hrozby a mohly účinně zvládat ICT rizika.
- **Cíl pravidel**: Ochránit kritické a důležité funkce finančních institucí před výpadky a bezpečnostními incidenty spojenými s ICT službami poskytovanými třetími stranami. DORA klade důraz na prevenci, odolnost a schopnost rychlé reakce.
- **Klíčové oblasti**:
  - **Řízení rizik**: Implementace postupů pro identifikaci, hodnocení a řízení rizik spojených s ICT službami.
  - **Bezpečnostní opatření**: Zajištění ochrany dat a ICT systémů před útoky a zranitelnostmi.
  - **Správa subdodavatelů**: Kontrola a dohled nad poskytovateli, kteří dodávají ICT služby, včetně řízení subdodavatelského řetězce.
  - **Reakce na incidenty**: Nastavení postupů pro rychlou a účinnou reakci na bezpečnostní incidenty.
- **Implementace v prostředí ČSOB**:
  - Smluvní dodatky pro dodavatele ICT služeb
  - Registr informací

AKTIVITY NA STRANĚ ČSOB

- **Řízení rizik poskytovatelů ICT služeb:**
  - ČSOB musí zajišťovat pravidelné hodnocení rizik poskytovatelů ICT služeb a musí přizpůsobit opatření na základě změn v jejich rizikovém profilu.
  - Musí zajistit, že poskytovatelé aktivně přispívají k efektivnímu řízení ICT rizik a že jsou jejich procesy zdokumentované a v souladu s požadavky DORA.
- **Monitorování a dodržování smluv:**
  - ČSOB provádí sledování výkonu poskytovatelů a musí zajistit, že dodržují stanovené SLA, a to ideálně nejméně jednou ročně, a bezpečnostní opatření.
  - ČSOB má právo provádět pravidelné audity a kontroly, aby ověřila dodržování smluvních a regulačních požadavků.

POŽADAVKY NA BEZPEČNOST A REAKCI NA INCIDENTY

Opatření:

- Bezpečnostní - Poskytovatelé ICT služeb musí zajistit ochranu dat ČSOB pomocí šifrování, pravidelného zálohování, a implementace bezpečnostních opatření pro ochranu před neoprávněným přístupem.
- Poskytovatelé musí mít zavedené plány pro zajištění kontinuity služeb a provádět pravidelné testy těchto plánů, aby bylo zajištěno, že jsou funkční a účinné.

Reakce na incidenty:

- Poskytovatelé musí bezodkladně hlásit kritické bezpečnostní incidenty a zranitelnosti, které mohou ovlivnit jimi dodávané služby.
- Poskytovatelé musí spolupracovat s ČSOB na identifikaci příčin incidentů, nápravě situace a implementaci opatření pro zabránění budoucím incidentům.

SPRÁVA SUBDODAVATELŮ

- **Schvalování subdodavatelů**:
  - Poskytovatelé mohou zapojit subdodavatele pouze s předchozím písemným souhlasem ČSOB. Každý subdodavatel musí být posouzen z hlediska rizik, zejména pokud jde subdodavatele v jiné geografické lokalitě a jejich vliv na bezpečnost a kontinuitu služeb.
  - Je nutné hodnotit potenciální rizika spojená s lokalitou subdodavatelů a zajišťovat, že jsou podniknuté veškeré kroky k ochraně dat ČSOB.
- **Odpovědnost a audit**:
  - Poskytovatelé nesou plnou odpovědnost za činnost svých subdodavatelů a musí zajistit, že plní stejné požadavky na bezpečnost a SLA.
  - ČSOB má právo provádět audity a kontroly subdodavatelů, aby se ujistila, že jsou dodržovány všechny standardy a opatření.

POVINNOSTI PŘI ZABEZPEČENÍ DAT

- **Ochrana dat**: Poskytovatelé musí garantovat, že všechna data ČSOB jsou bezpečně chráněna, pravidelně zálohována, a že lze data na žádost ČSOB předat nebo odstranit. Zároveň musí garantovat jejich odstranění po ukončení smlouvy.
- **Správa zranitelností**: Poskytovatelé jsou povinni neprodleně řešit zjištěné zranitelnosti v ICT systémech a zabezpečit, aby data zůstala chráněna i při nových hrozbách. Musí používat aktuální technologie a postupy pro zajištění bezpečnosti dat.

POVINNOSTI TÝKAJÍCÍ SE POSKYTOVATELŮ SLUŽEB PODPORUJÍCÍCH KRITICKÉ NEBO DŮLEŽITÉ FUNKCE

KRITICKÉ A DŮLEŽITÉ FUNKCE

- **Kritická a důležitá funkce**: Činnost, jejíž přerušení nebo selhání může zásadně ovlivnit stabilitu ČSOB nebo její schopnost plnit své klíčové závazky. Určení se řídí metodikou KBC.

- V průběhu existence funkce může být klasifikace funkce měněna z/na kritickou a důležitou dle aktuálních dopadů

- **ICT služba podporující kritické a důležité funkce**: Taková ICT služba, která je zásadní pro správné a bezpečné fungování definovaných kritických a důležitých funkcí.

POVINNOSTI PRO KRITICKÉ NEBO DŮLEŽITÉ FUNKCE

- **Účel DORA dodatku (specificky kapitoly 11)**: Stanovit specifická opatření, která mají zaručit, že ICT služby, jež podporují kritické nebo důležité funkce, zůstávají odolné vůči selhání a hrozbám. Cílem je minimalizovat dopad na ČSOB a zajistit nepřetržitou dostupnost těchto služeb.

- Poskytovatelé musí implementovat strategie, které zajistí, že i při vážném narušení zůstane provoz stabilní a funkční.

MONITOROVÁNÍ A HLÁŠENÍ

- **Pravidelné aktualizace**: Popis ICT služeb, včetně cílů výkonnosti a bezpečnostních opatření, musí být pravidelně revidován. To zajišťuje, že poskytovatelé, ale i ČSOB, mohou rychle reagovat na nové hrozby a přizpůsobit se měnícím se požadavkům a prostředí.

- **Hlášení důležitých událostí**: Poskytovatel je povinen oznámit ČSOB každou událost, která by mohla ovlivnit plnění služeb. To zahrnuje okamžité (do 24 hodin) hlášení o selháních, kybernetických útocích nebo jiných incidentech, které mohou narušit kritické funkce.

KONTINUITA PROVOZU

- **Plány kontinuity**: Poskytovatel musí zavést a udržovat detailní plány pro kontinuitu provozu, které zahrnují scénáře pro zvládnutí krizových situací. Tyto plány se musí pravidelně testovat, aby se zajistila jejich účinnost při skutečných incidentech.

- **Bezpečnostní opatření**: Implementace pokročilých technologií a procesů pro zabezpečení ICT služeb je klíčová. Opatření musí odpovídat aktuálním bezpečnostním standardům a být přizpůsobena povaze a závažnosti identifikovaných rizik.

POUŽÍVÁNÍ KNIHOVEN KÓDŮ A TLPT

- **Sledování knihoven kódů**: Poskytovatel musí mít zavedené procesy pro sledování používaných knihoven kódů (včetně open-source řešení), aby zajistil, že jsou aktuální a bez známých zranitelností. To zahrnuje pravidelné aktualizace a sledování verzí.
- **Penetrační testování vedené hrozbami (TLPT)**: Poskytovatelé musí být připraveni na testování bezpečnosti ICT služeb simulovanými kybernetickými útoky (TLPT), které provádí ČSOB nebo jím pověřená třetí strana. Tyto testy zajišťují, že jsou identifikovány a odstraněny slabiny systému. Výsledky musí být sdíleny a využity ke zlepšení bezpečnostních opatření a to i když je daný test proveden samostatně poskytovatelem.

PRÁVA NA AUDIT A SPOLUPRÁCE

- **Práva na audit**: ČSOB má právo provádět podrobné audity poskytovatelů ICT služeb. Tyto audity mohou zahrnovat kontrolu dokumentace, bezpečnostních opatření a prověřování systémů. Poskytovatel musí poskytnout neomezený přístup k datům a prostředkům potřebným pro audit.

- **Spolupráce**: Poskytovatel je povinen plně spolupracovat s ČSOB i s dohledovými orgány. To zahrnuje zajištění přístupu k informacím, účast na kontrolách a sdílení výsledků bezpečnostních testů. Poskytovatel musí také aktivně řešit a odstraňovat zjištěné zranitelnosti.

KLÍČOVÉ POZNATKY A SHRNUTÍ

KLÍČOVÉ POVINNOSTI

- **Řízení rizik**: Je nutné pravidelně hodnotit rizika související s poskytovateli ICT služeB a aktualizovat opatření.
- **Monitorování a audit**: Je nutné provádět pravidelné kontroly dodržování SLA a audity souladu se smluvními bezpečnostními požadavky.
- **Bezpečnostní opatření**: Poskytovatelé musejí implementovat vhodná bezpečnostní opatření, např. šifrování, zálohování, řízení kontinuity a v případě incidentů o nich musí bezodkladně informovat.
- **Řízení subdodavatelů**: Poskytovatelé před využitím subdodavatelů musí získat souhlas ČSOB s jejich využitím. Subdodavatelé musí dodržovat stejné podmínky jako poskytovatelé.
- **Reakce na incidenty**: Poskytovatelé musí spolupracovat na rychlé idenitifkaci a nápravě incidentů a zajištění bezpečnosti dat ČSOB.
- **Kontinuita provozu a testování**: Poskytovatele musí provádět pravidelné testy plánů kontinuity, včetně simulace krizových scénářů.

POSKYTOVATEL SLUŽEB PODPORUJÍCÍCH KRITICKÉ NEBO DŮLEŽITÉ FUNKCE

- **Množina poskytovatelů** služeb podporujících kritické nebo důležité funkce **není fixní**.
- **Může docházet k identifikaci nových poskytovatelů** na základě identifikace nových či reklasifikace stávajících kritických nebo důležitých funkcí.
- Obdobně **může docházet k vyřazení z poskytovatelů** služeb podporujících kritické nebo důležité funkce na základě změny klasifikace podporovaných služeb.

Děkujeme za pozornost

ČSOB
jdeme vám naproti