

Podporované oblasti kybernetické bezpečnosti z evropských fondů - technické prostředky

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

Disclaimer



- Prezentace je informativní.
- Informace v prezentaci vycházejí z informací dostupných autorovi ke dni zpracování.
- Pokud je někde jako příklad uvedena konkrétní technologie, neznamená to její preferenci ani vhodnost v každém případě.

Rámcově k financování



- **Detail je v gesci MMR**
- Jaké programy
 - IROP – celá ČR mimo Prahu
 - Národní plán obnovy – i Praha
- Kdy to bude
 - Programový dokument pro IROP je v EK – schváleno bude cca v červnu, stejně tak budou výzvy
- Mělo by být obdobné jako v minulosti IROP – výzva č. 10
- Podporovány budou technické opatření z VKB – hlava II - od § 17 dál
- Pro koho to bude
 - pro KII, VIS, PZS (i další systémy veřejné správy?)
- Na co se bude možno čerpat
 - Kapitálové výdaje – investiční prostředky na pořízení a služby pro uvedení do provozu (nastavení)
- Kdo bude co posuzovat
 - Projektovou žádost prozkoumá CRR – formality a přijatelnost, věcně to budou zkoumat externí hodnotitelé a OHA – bude pod CRR – bude se to bodovat a kdo bude mít dost bodů bude mít proplaceno

Bezpečnostní opatření ve VKB



○ Co je bezpečnostní opatření?

- ZKB §4 odst. 1) Bezpečnostním opatřením se rozumí **souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací** v informačních systémech a **dostupnosti a spolehlivosti služeb** a sítí elektronických komunikací v kybernetickém prostoru.

○ Implementace

- ZKB §4 odst. 2) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny **zavést a provádět bezpečnostní opatření v rozsahu nezbytném** pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a **vést o nich bezpečnostní dokumentaci**.

○ Princip VKB

- VKB §3 písm. a) **stanoví s ohledem na požadavky dotčených stran a organizační bezpečnost rozsah systému řízení bezpečnosti informací**, ve kterém určí organizační části a aktiva, jichž se systém řízení bezpečnosti informací týká,
- VKB §3 písm. b) stanoví **cíle systému řízení bezpečnosti informací**,
- VKB §3 písm. c) pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a **hodnocení rizik zavede přiměřená bezpečnostní opatření**,

Bezpečnostní opatření (§ 5 ZKB, VKB)



Organizační:

- a) systém řízení bezpečnosti informací,
- b) řízení rizik,
- c) bezpečnostní politika,
- d) organizační bezpečnost,
- e) stanovení bezpečnostních požadavků pro dodavatele,
- f) řízení aktiv,
- g) bezpečnost lidských zdrojů,
- h) řízení provozu a komunikací,
- i) řízení přístupu osob,
- j) akvizice, vývoj a údržba,
- k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- l) řízení kontinuity činností a
- m) kontrola a audit.

Technická:

- a) fyzická bezpečnost,
- b) nástroj pro ochranu integrity komunikačních sítí,
- c) nástroj pro ověřování identity uživatelů,
- d) nástroj pro řízení přístupových oprávnění,
- e) nástroj pro ochranu před škodlivým kódem,
- f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů,
- g) nástroj pro detekci kybernetických bezpečnostních událostí,
- h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- i) aplikační bezpečnost,
- j) kryptografické prostředky,
- k) nástroj pro zajišťování úrovně dostupnosti informací a
- l) bezpečnost průmyslových a řídicích systémů.

Technická bezpečnostní opatření ve VKB I.



- Fyzická bezpečnost (§ 17 VKB)
 - Ochrana na úrovni a v rámci objektů
- Bezpečnost komunikačních sítí (§ 18 VKB)
 - Vhodně navržená topologie, aktivní prvky umožňující segmentaci sítě a filtraci provozu, autentizační mechanismy, šifrování síťové komunikace
- Správa a ověřování identit (§19 VKB)
 - Hesla, dvoufaktorová autentizace
- Řízení přístupových oprávnění (§20 VKB)
 - Pro aplikace i uživatele, definice práv pro čtení, zápis a změny oprávnění, centralizovaná správa
- Ochrana před škodlivým kódem (§21 VKB)
 - Ověřování a kontrola komunikace, síťový provoz, antiviry, antispy, antivir, pravidelná aktualizace,
- Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů (§22 VKB)
 - Sběr informací o provozních a bezpečnostních činnostech, logování

Technická bezpečnostní opatření ve VKB II.



- Detekce kybernetických bezpečnostních událostí (§ 23 VKB)
 - Nástroj pro kontrolu a případně zablokování komunikace mezi a v rámci sítí, sondy, skenery zranitelnosti
- Sběr a vyhodnocování kybernetických bezpečnostních událostí (§ 24 VKB)
 - Poskytování informací pro určené bezpečnostní role o detekovaných událostech, Nepřetržité vyhodnocování událostí s cílem identifikace incidentů, SIEM
- Aplikační bezpečnost (§25 VKB)
 - Bezpečnostní testy zranitelnosti aplikací, které jsou přístupné zvnějšku, testy aplikací, penetrační testy...
- Kryptografické prostředky (§26 VKB)
 - Stanovení vhodné úrovně šifrování, pravidel pro šifrování, správa klíčů, odolné algoritmy
- Zajišťování úrovně dostupnosti informací (§ 27 VKB)
 - Kontinuita činností, DRP, zálohování, vhodná topologie, redundance, virtualizace, ...
- Bezpečnost průmyslových a řídicích systémů (§ 28 VKB)
 - Omezení fyzického přístupu, propojení a vzdáleného přístupu, segmentace, ...



§ 17 - Fyzická bezpečnost

- Prvky fyzické ochrany sloužící k zajištění, sjednocení a k centralizování bezpečnosti
- Zvláště pak systémy technické ochrany (STO), jejichž součástí je kamerový systém (CCTV)
- Prvky elektronické kontroly vstupu (EKV)
- Poplachový zabezpečovací a tísňový systém (PZTS)
- Protipožární zabezpečovací systémy (PZS) – související např. se serverovny
- Prostředky pro centrální správu STO (HW i SW)-Integrační platformy
- K eliminaci rizik mohou sloužit také pasivní prvky ochrany, např. certifikované mříže, dveře, fólie
- Technická zařízení kontroly vstupu – rámy, RTG, scannery a zařízení sloužící k provádění obranně technických prohlídek (OTP), pohybová čidla, rušičky, detektory atd.
- Případné stavební úpravy prokazatelně související se zmiňovanými změnami



§ 18 - Bezpečnost komunikačních sítí

- Segmentace sítí
- VLAN technologie, routery, switche,
- Firewally (perimetrový, interní, mikrosegmentační),
- WAF, technologie DMZ
- VPN technologie vzdáleného přístupu (interní a externí subjekty)
- Nástroje pro management a vzdálenou správu těchto síťových prvků,
- Šifrátory, Sandboxing, Honeypoty
- DDoS ochrana (také jako služba internetových providerů)



§ 19 - Správa a ověřování identit

- Nástroje pro centrální řízení a správu uživatelů v síti – např.
 - Active directory – nejvíce používáno
 - authenticator,
 - IAM (Identity & Access Management, IDM) – napojení na personální systémy



§ 20 - Řízení přístupových oprávnění

- Nástroj pro řízení přístupových oprávnění, služba pro správu identit
- Další nástroje pro 2FA + vícefaktorové ověření a jejich licenční pokrytí, tokeny, nástroje pro správu hesel, které nejsou freewarem – AD,



§ 21 - Ochrana před škodlivým kódem

- Antimalware
- Antispam
- Webfiltering, behaviorální analýza
- Sandboxing, honeypoty
- Ochrana koncové stanice, antivir
- Monitoring provozu a vyhodnocování v reálném čase, hledání škodlivých kódů a zranitelnosti v komunikaci
- Antivirové řešení - centrální správa
- Centrální správa a monitoring koncových stanic, centrální distribuce SW,
- Centrální správa aktualizací a záplat



§ 22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

- Technologie centrálního log managementu pro centralizovaný sběr, uložení a řízení retence logů
- Dostatečná velikost pro úložiště logů (18 a 12 měsíců podle typu určení systému)
- Systémy PIM/PAM - Privileged Identity and Access Management – hlídání přístupů s vysokými administrátorskými právy



§ 23 - Detekce kybernetických bezpečnostních událostí

- Síťové sondy,
- Technologie sledování síťového provozu s funkcionalitou detekce kybernetických bezpečnostních událostí
- IDS/IPS řešení – pro splnění požadavku i na blokaci by se mělo jednat o IPS



§ 24 - Sběr a vyhodnocení kybernetických bezpečnostních událostí

- Všechny technologie, které umožňují sběr a následné vyhodnocování a korelaci událostí/logů získaných z monitoringu síťového provozu z § 22 a § 23,
 - Threat intelligence, Threat protection, - organizations aggregate, correlate and analyze threat data
 - SIEM - Security Incident and Event Management



§ 25 - Aplikační bezpečnost

- Skenování zranitelností
- V rámci penetračního testování: Stroj na lámání hashů, DoS tester
- V rámci trvalého zabezpečení aplikací: zavedení bezpečnostních mechanismů jako TLS, DNSSEC.
- Ukládání zdrojových kódů – verzovací systémy



§ 26 - Kryptografické prostředky

- Síťové prvky, které podporují šifrovanou komunikaci,
- Bezpečné ukládání hesel,
- PKI – certifikační autorita, certifikáty
- Doporučené šifrovací algoritmy NÚKIB



§ 27 - Zajišťování úrovně dostupnosti informací

- Technologie pro zálohování (servery, racky, UPS, záložní napájení – např. dieselagregáty)
- Redundantní infrastruktura pro zajištění HA, NAS, disková pole, geoclustery,
- Záložní internetová konektivita, redundace WAN, LAN,
- Anti-DDoS protection (např. anti-DDoS protection protector), funkce scrubbing centra, čističky provozu



§ 28 - Průmyslové, řídicí a obdobné specifické systémy

- SCADA systémy – průmyslové řídicí systémy
- Laboratorní systémy, lékařské zobrazovací systémy(RTG)
- Systémy s dlouhou délkou životnosti
- Skenování zranitelností, penetrační testování
- Dodatečné technické způsoby ochrany

Technické prostředky a návaznost na externí služby

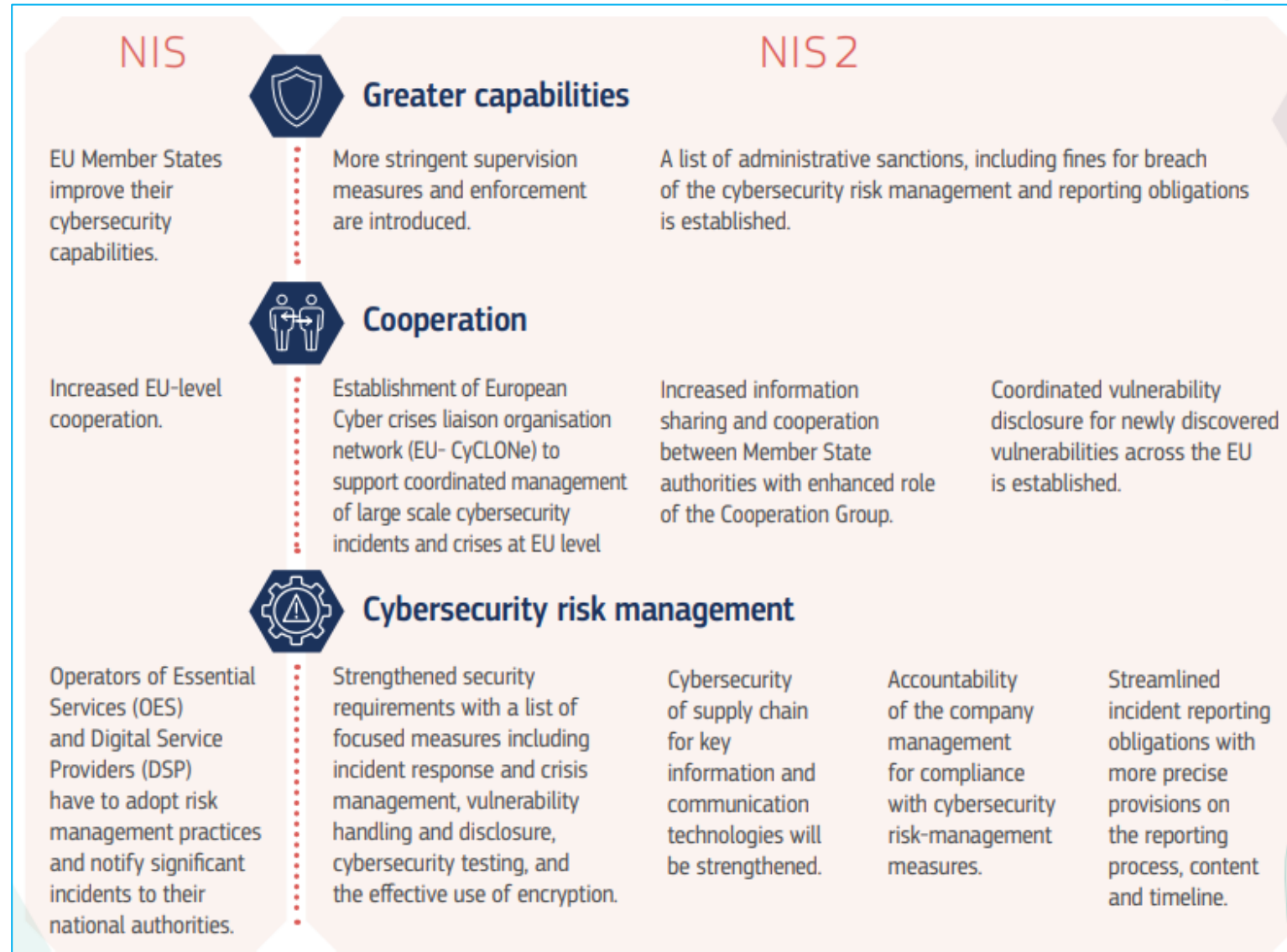


- Vlastním technické prostředky nemám lidské zdroje na provoz a údržbu těchto systémů
- Různé formy (modely) pronájmů a služeb
- Zvážit dlouhodobě vlastní možnosti
- SOC - Security Operations Centra
 - Vlastní
 - Zaměřená na určité segmenty (např. energetika)
 - Regionální

Výhled v oblasti regulace kybernetické bezpečnosti




- Na konci roku 2020 zahájena z podnětu Evropské Komise revize směrnice NIS – **tzv. směrnice NIS2**.
- prvotní návrh zveřejněn zde: [Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future \(europa.eu\)](#)
- Aktuální návrh zachovává mnoho institutů z původní směrnice NIS, většinu z nich však prohlubuje



Návrh NIS2 z pohledu zdravotnictví



- Původní směrnice NIS vycházela z předpokladu, že některé organizace nejsou na ICT závislé nebo ICT ovlivnitelné – návrh NIS2 toto opouští.
- Odvětví zdravotnictví zůstává zachováno →  Healthcare providers referred to in point (g) of Article 3 of Directive 2011/24/EU ⁽¹⁹⁾
- Upouští se od určování povinných subjektů na základě odvětvových a dopadových kritérií systému = povinnými osobami se **automaticky** stanovou všechny organizace **poskytující danou službu** („poskytování zdravotních služeb“), které naplní unijně unifikovaná kritéria:

poskytovatel zdravotních služeb má velikost středního nebo velkého podniku

(podle Doporučení Komise ze dne 6. března 2003 = **50 a více zaměstnanců nebo roční obrát nebo rozvaha více než 10 000 000 EUR**)

- doplňujícími kritérii jsou podle čl. 2 návrhu směrnice NIS2 i další podmínky **bez ohledu na velikost organizace** (především **možné narušení služby poskytované tímto subjektem by mohlo mít vliv na veřejný pořádek, bezpečnost, nebo ochranu zdraví** nebo že je **subjekt kritický vzhledem ke svému specifickému významu na regionální nebo vnitrostátní úrovni pro konkrétní odvětví** a další, které se však nejeví jako relevantní).
- s ohledem na formu směrnice může být národní právo v rámci transpozice při stanovování kritérií pouze přísnější
- Odpadá také jakékoliv rozdělování nebo stanovování menších množin ICT prostředků – vše v rámci organizace je nutno mít na paměti (jejich prioritizace a další práce s nimi je pak už součástí zákonných požadavků).



Dotazy?

Děkuji za pozornost!

nckb@nukib.cz