Bezpečný provoz v infrastruktuře poskytovatelů

Jakub Rejzek

Výbor Nezávislého ICT průmyslu

Zákon o kybernetické bezpečnosti – návrh 2Q/2023

- Současný, stále platný zákon dle NIS1 definuje základní infrastruktury-oborová kritéria

- Současná, stále platná vyhláška stanovuje objemová a dopadová kritéria
  = drtivou většinu MSP kritéria současné úpravy ZKB míjí, nejsou základní infrastrukturou.
- I současná regulace ale stanoví povinnost prověřovat důvěryhodnost dodavatelů a řídit rizika (§8 82/2018Sb.)

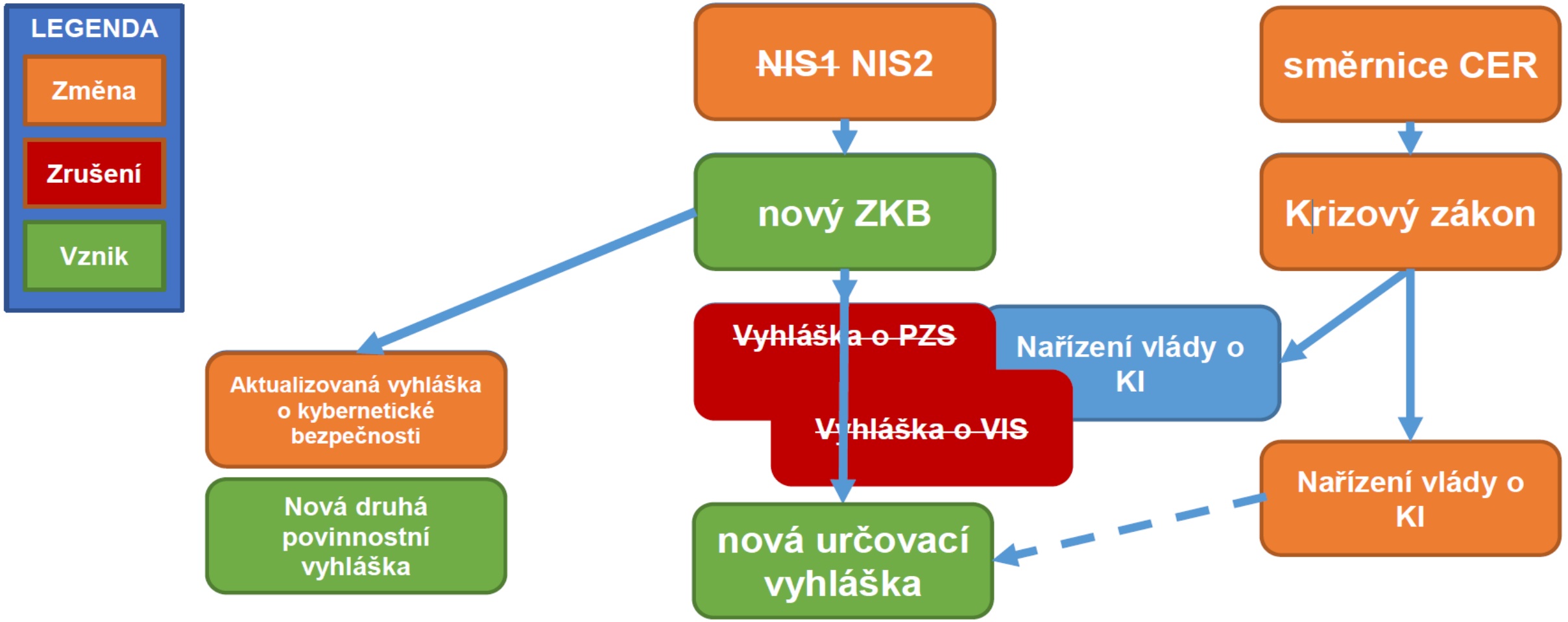
Nová Směrnice EU o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2, rozšiřuje oblast regulace. V ICT oborech jsou tak dotčení regulací všichni podnikatelé poskytující veřejně dostupné služby; odvětví „Digitální infrastruktury“.

- do odvětví digitální infrastruktury se nově řadí také poskytovatelé služeb cloud computingu, služeb datových center, sítí pro doručování obsahu, služeb vytvářejících důvěru, veřejných sítí elektronických komunikací, služeb elektronických komunikací (jsou-li jejich služby veřejně dostupné),

- nově se pod NIS2 řadí také subjekty v odvětví veřejné správy (ústřední subjekty veřejné správy, orgány samosprávy).

článek Jakub Rejzek - https://www.lupa.cz/clanky/provozovatelum-siti-a-it-sluzeb-se-nova-kyberbezpecnostni-regulace-nevyhne/

Teze nového ZKB



Výbor Nezávislého ICT průmyslu

NIS2 a Mechanismus

- Doporučení NUKIB pro hodnocení důvěryhodnosti dodavatelů a technologií do 5G sítí v ČR

Hlavní teze:

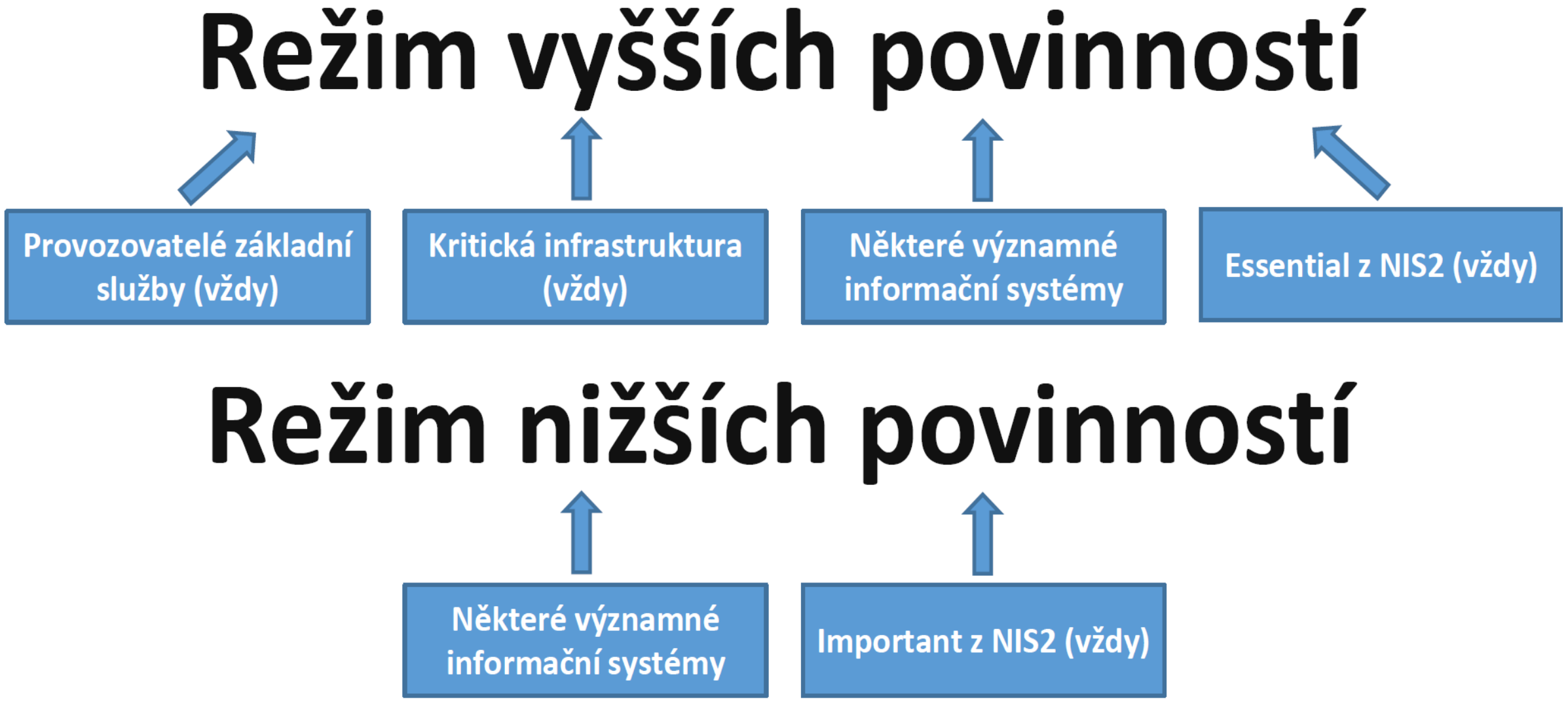
- Regulované subjekty budou rozdělené podle velikosti na dva režimy:
- Important and Essential (Režim nižších povinností a Režim Vyšších povinností)

Provozovatelé ~~Základní služby~~ (Strategické infrastruktury státu) - Speciální kategorie pro Mechanismus prověřování bezpečnosti dodavatelského řetězce.

- Dvě regulace v jednom návrhu zákona, týkající se stejné věci – BDŘ.
- NUKIB: Koordinované posouzení rizik dle čl. 22 NIS2, na které odkazovaný recitál 91 NIS2 míří, představuje proces posouzení rizik spojených s dodavateli na úrovni Evropské unie, kdežto mechanismus prověřování bezpečnosti dodavatelských řetězců, obsažených v aktuálním návrhu zákona o kybernetické bezpečnosti, představuje vnitrostátní proces, hodnotící kritéria důležitá pro bezpečnost České republiky. Z tohoto důvodu se tyto dva systémy posuzování rizik, resp. hrozeb, procesně i co do kritérií posuzování liší.

- Aktuálně navrhované kritérium je 100 000 aktivních přípojek nebo 350 000 SIM karet pro BDŘ dle Mechanismu.

NIS2 a Mechanismus



Výbor Nezávislého ICT průmyslu

NIS2 a Mechanismus

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

Základním kritériem pro posouzení velikosti podnikatele je počet zaměstnanců, velikost ročního obratu a bilanční suma roční rozvahy (velikost aktiv). Údaje, které se mají použít pro stanovení počtu zaměstnanců a finančních veličin, jsou údaje vztahující se k poslednímu uzavřenému zdaňovacímu období vypočtené za období jednoho kalendářního roku.

- Za **drobného, malého a středního podnikatele** se považuje podnikatel, který zaměstnává méně než 250 zaměstnanců a jeho roční obrat nepřesahuje 50 milionů EUR nebo jeho bilanční suma roční rozvahy nepřesahuje 43 milionů EUR.
- V rámci kategorie malých a středních podniků jsou **malé podniky** vymezeny jako podniky, které zaměstnávají méně než 50 osob a jejichž roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR.
- V rámci kategorie malých a středních podniků jsou **drobní podnikatelé** vymezeni jako podnikatelé, kteří zaměstnávají méně než 10 osob a jejichž roční obrat nebo bilanční suma roční rozvahy nepřesahuje 2 miliony EUR.

Výbor Nezávislého ICT průmyslu

Současná opatření pro posílení KB

- Doporučení NUKIB pro hodnocení důvěryhodnosti dodavatelů a technologií do 5G sítí v ČR

Hlavní teze:

- Vodítko pro dodávky informačních a komunikačních systémů KI v ČR.
  - vlastnická struktura
  - prokázat princip „Security by design“
  - účinná bezpečnostní pravidla a procesy

- Principy
  - strategická
  - obchodní
  - technicko-bezpečnostní

- Operátoři by podle doporučení měli například sledovat, zda je dohledatelná vlastnická struktura dodavatelské firmy, zda má sídlo ve státě s demokraticky volenou vládou a nezávislým soudním systémem, který dlouhodobě nebo systematicky neporušuje mezinárodní právo.

Náklady na regulaci

*„Náklady na dodržování regulace jsou nejen náklady vznikající podnikům i jiným stranám, na které je právní úprava zacílena, v souvislosti s přijímáním opatření nezbytných k dodržení požadavků právní úpravy, ale i administrativní zátěž a náklady veřejné správy související s vynucováním regulace.“**

*Zdroj: Metodika Vlády ČR pro měření celkových nákladů plnění povinností vyplývajících z regulace

Jaké povinnosti bude muset regulovaný subjekt plnit?

Povinný subjekt bude muset plnit dvě základní kategorie opatření; technické a netechnické. V první řadě je to povinnost přijmout vhodná a přiměřená odpovídající technická a organizační opatření k řízení bezpečnostních rizik. Opatření musí zahrnovat tyto základní aspekty:

- analýzu rizik a politiku bezpečnosti informačních systémů
- řešení incidentů včetně prevence a reakce na ně, opět technické i netechnické kategorie opatření
- řízení kontinuity provozu a krizové řízení; včetně například cvičení přechodu na nedigitální provoz v nouzovém režimu
- zabezpečení dodavatelského řetězce včetně bezpečnostních aspektů týkající se vztahů mezi subjekty, jeho dodavateli či poskytovateli služeb. Opět zde řešíme technické a netechnické aspekty
- zabezpečení pořizování, vývoje a údržby sítě a informačních systémů včetně zveřejňování informací o zranitelnostech a jejich řešení, myšleno především nadřízeným a odpovědným orgánům – v našem případě pravděpodobně NÚKIB nebo CSIRT
- vytvářet politiky a postupy, včetně auditů a penetračních testů s účelem posouzení účelnosti opatření řízení rizik KB
- subjekty budou povinny používat kryptografii a šifrování

K § 15 - v zákoně je jenom výčet bezpečnostních opatření. Ve vyhláškách je pak specifikované, co je tím konkrétně myšleno (§ 11 vyšších povinností a § 6 nižších povinností).

V podstatě každý subjekt(= nižší povinnosti) bude muset plnit toto:

§ 6

Bezpečnost lidských zdrojů

Povinná osoba v rámci bezpečnosti lidských zdrojů

a) stanoví politiku bezpečného chování uživatelů, v rámci které zohledňuje relevantní témata uvedená v příloze č. 4 této vyhlášky,

b) stanoví pravidla rozvoje bezpečnostního povědomí, včetně pravidel pro tvorbu hesel dle § 9,

c) v souladu s pravidly rozvoje bezpečnostního povědomí provádí vstupní školení v oblasti kybernetické bezpečnost,

d) v souladu s pravidly rozvoje bezpečnostního povědomí provádí pravidelná školení v oblasti kybernetické bezpečnosti,

e) v rámci školení podle písm. c) a d) zohledňuje relevantní témata uvedená v příloze č. 4 této vyhlášky,

f) vede přehledy o školeních podle písm. c) a d),

g) zajistí potřebná odborná teoretická i praktická školení administrátorů a osoby odpovědné za kybernetickou bezpečnost v souladu s jejich pracovní náplní,

h) zajistí kontrolu dodržování bezpečnostní politiky a

i) určí pravidla a postupy pro řešení případů porušení stanovených pravidel.

Zároveň ale podle § 4 musí povinná osoba vést dokumentaci zahrnující oblasti uvedené v příloze 2, a tam je zároveň další bezpečnost lidských zdrojů:

1. *Politika bezpečnosti lidských zdrojů*

a) *Pravidla rozvoje bezpečnostního povědomí a evidence přehledů o školeních.*

b) *Bezpečnostní školení nových zaměstnanců.*

c) *Stanovení periody pro pravidelná školení.*

d) *Pravidla pro řešení případů porušení bezpečnostní politiky.*

e) *Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice*

I. *vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu,*

II. *změna přístupových oprávnění při změně pracovní pozice,*

III. *předání odpovědností při změně pracovní pozice nebo ukončení pracovního vztahu s administrátory nebo osobou odpovědnou za kybernetickou bezpečnost.*

- *Pravidla bezpečného chování uživatelů včetně pravidel pro tvorbu hesel.*

Závěr

Obávat se jako investic do přístupové sítě nebo do rádiové části sítě, pokud jste MSP?

Není třeba, s jistotou nad 100 000 aktivních přípojek, ale vždy zpracujte risk analýzy a další požadované podklady. Což tak jako tak odpovídá zdravému přístupu Zero Trust Policy.

ale… regulace je nakažlivá, pokud jste dodavatelem regulovaného subjektu

Závěr

Klíčové fáze	Začátek	Konec
Zadání úkolu BRS	21. červen 2022	
Příprava návrhu	červen 2022	leden 2023
Konzultace návrhu se státem	listopad 2022	leden 2023
Konzultace návrhu s širokou veřejností	26. leden 2023	12. březen 2023
MPŘ + vypořádání	Q2 2023	Q3 2023
Legislativní proces	Q3 2023	Q3 2024
Účinnost a možné zahájení prověřování	Q4 2024	
První povinnosti hlášení dodavatelů	Q4 2025	

Bezpečnost provozu jako téma

Téma 1: je síťová bezpečnost prodejní argument?

- **velcí operátoři nasazují DNS security systémy**
- **přitom malí operátoři už od roku 2017 AI (tehdy neuronová síť) nasazovali na DNS resolvery**
- **DNS bezpečnostní produkty (například Whalebone PROFIT) umožní částečnou konfiguraci uživatelem**
- **slouží k de/aktivaci bezpečnostních funkcí a funkce filtrování obsahu, výběr kategorií, které se mají blokovat, a tvorbu vlastních blacklistů a whitelistů**

Bezpečnost provozu jako téma

Téma 2: zajistit úplné oddělení řídící a uživatelské roviny?

- **Deep packet inspection? Těšíme se na přednášku Davida Tichého z Profiber na KKDS, ještě uvidíme, jestli Olomouc nebo Plzeň.**

Téma 3: Dá se zobchodovat bezpečnostní detekce pro firemní zákazníky z SME podniků, kteří nemají dostatečné kapacity pro vlastní bezpečnostní řešení? V praxi, například, potkáváme podniky, které potřebují nastavit takovou bezpečnost, která by jim umožnila provozovat i starší výrobní stroje s nezáplatovatelnými OS. Nebo provozují kanceláře s BYOD stroji, u kterých nemají plnou správu nad sítí.

Děkuji Vám za pozornost.

Výbor nezávislého ICT průmyslu, z.s
jakub.rejzek@vnictp.cz