Vyhláška č.410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Online přednáška portal.nukib.gov.cz

TLP: CLEAR

Sára Vavřičková
Viktor Kozák
odbor kontroly

Informace na úvod

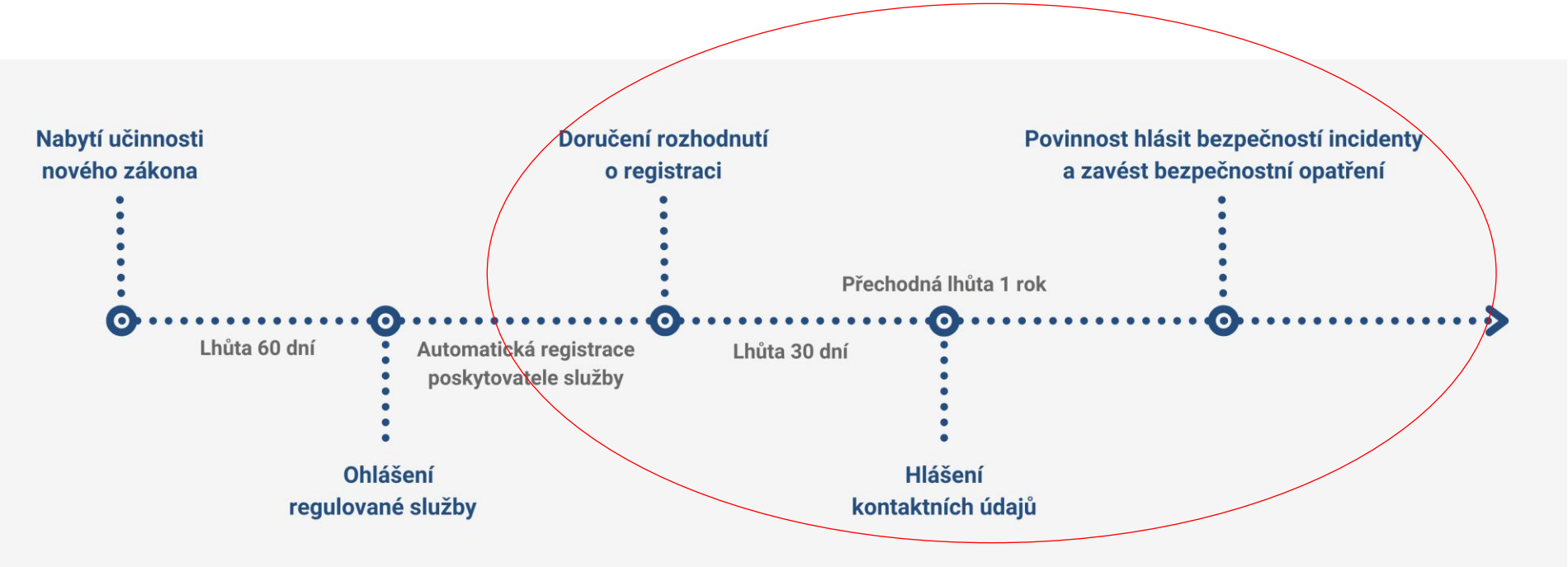
Tento materiál slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů.
Tento materiál se primárně zaměřuje na oblast bezpečnostních opatření pro poskytovatele v režimu nižších povinností.
Tento materiál nenahrazuje a nepokrývá všechny detaily zákona o kybernetické bezpečnosti a jeho prováděcích předpisů.

Obsah prezentace

- Vyhláška o kybernetické bezpečnosti
- Rozsah řízení kybernetické bezpečnosti
- Bezpečnostní opatření požadované vyhláškou
  - Neopominutelná bezpečnostní opatření
  - Vyhodnotitelná bezpečnostní opatření

Vyhláška o kybernetické bezpečnosti

- vychází ze základních principů řízení kybernetické bezpečnosti, které vedou k zavádění a provádění **přiměřených bezpečnostních opatření** v rozsahu řízení kybernetické bezpečnosti, který je poskytovatel regulované služby povinen určit
- Přechodná lhůta – 1 rok



Viz samostatná přednáška Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Rozsah řízení kybernetické bezpečnosti

- **Nezbytná prerekvizita pro funkční řízení bezpečnosti – je nutno vědět jaké služby jsou poskytovány a na čem jsou závislé**

Součástí rozsahu řízení kybernetické bezpečnosti jsou **aktiva související s poskytováním regulované služby**

= stanovený rozsah

Řízení aktiv – určení primárních a podpůrných aktiv

Dle § 12 zákona *č. 264/2025 Sb., o kybernetické bezpečnosti* – Stanovení rozsahu řízení kybernetické bezpečnosti

- Bezpečnostní opatření požadovaná vyhláškou je nutné implementovat v takto stanoveném rozsahu řízení kybernetické bezpečnosti

Viz samostatná přednáška Zákon č. 264/2025 Sb., o kybernetické bezpečnosti

Bezpečnostní opatření

Organizační a technická opatření

- § 3 systém zajišťování minimální kybernetické bezpečnosti,
- § 4 požadavky na vrcholné vedení,
- § 5 bezpečnost lidských zdrojů,
- § 6 řízení kontinuity činností,
- § 7 řízení přístupu,
- § 8 řízení identit a jejich oprávnění,
- § 9 detekce a zaznamenávání kybernetických bezpečnostních událostí,
- § 10 řešení kybernetických bezpečnostních incidentů,
- § 11 bezpečnost komunikačních sítí,
- § 12 aplikační bezpečnost a
- § 13 kryptografické algoritmy
- § 14 Stanovení významnosti dopadu kybernetického bezpečnostního incidentu

Neopominutelná vs. Vyhodnotitelná

Neopominutelná

Základní bezpečnostní požadavky, které je poskytovatel regulované služby **povinen zavést.**

- § 3 Systém zajišťování minimální kybernetické bezpečnosti
- § 4 Požadavky na vrcholné vedení
- § 5 Bezpečnost lidských zdrojů
- § 6 Řízení kontinuity činností
- § 10 Řešení kybernetických bezpečnostních incidentů

Vyhodnotitelná

Poskytovatel regulované služby **musí zvážit v jaké míře**, případně zdali vůbec bude daná bezpečnostní opatření zavádět, aby to bylo přiměřené bezpečnostním potřebám organizace.

- § 7 Řízení přístupu
- § 8 Řízení identit a jejich oprávnění
- § 9 Detekce a zaznamenávání kybernetických bezpečnostních incidentů
- § 11 Bezpečnost komunikačních sítí
- § 12 Aplikační bezpečnost
- § 13 Kryptografické algoritmy

Neopominutelná bezpečnostní opatření

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

Cíl bezpečnostního opatření: Zajištění minimální kybernetické bezpečnosti zavedením základních bezpečnostních opatření, která zohledňují bezpečnostní potřeby poskytovatele regulované služby.

- ***Bezpečnostní opatření***
- ***Přehled bezpečnostních opatření***
- ***Bezpečnostní politika a bezpečnostní dokumentace***
- ***Používání a manipulace technických aktiv***
- ***Smlouvy s dodavateli***
- ***Akvizice, vývoj a údržba***

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

- ***odst. 1 - Bezpečnostní opatření***
  - Zavést a provádět přiměřená bezpečnostní opatření, která zohledňují jeho bezpečnostní potřeby.
  - V rozsahu řízení kybernetické bezpečnosti, je třeba, aby došlo k zavedení alespoň následujících bezpečnostních opatření:
    - § 3 Systém zajišťování minimální kybernetické bezpečnosti
    - § 4 Požadavky na vrcholné vedení
    - § 5 Bezpečnost lidských zdrojů
    - § 6 Řízení kontinuity činností
    - § 10 Řešení kybernetických bezpečnostních incidentů

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

- ***odst. 2 - Přehled bezpečnostních opatření***
  - Náhled na aktuální stav všech bezpečnostních opatření uvedených ve vyhlášce
  - Obsah přehledu bezpečnostních opatření:
    - **Přehled všech zavedených** bezpečnostních opatření, včetně popisu jejich zavedení.
    - **Přehled** všech bezpečnostních opatření, která **budou zavedena**
      - s termínem jejich zavedení,
      - jejich priority zavedení a
      - určení odpovědné osoby za jejich zavedení.
    - **Přehled všech nezavedených** bezpečnostních opatření, včetně odůvodnění jejich nezavedení
  - Vedení přehledu bezpečnostních opatření:
    - Listinná nebo elektronická podoba
    - Pravidelná aktualizace a přezkum, alespoň jednou za rok
    - Uchování jednotlivých přehledů alespoň po dobu 4 let

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

Vyhodnocení účinnosti zajišťování kybernetické bezpečnosti					2024
Bezpečnostní opatření podle vyhlášky	**Stav bezpečnostního opatření**	**Popis bezpečnostního opatření**	**Termín zavedení bezpečnostního opatření**	**Priorita zavedení bezpečnostního opatření**	**Odpovědnost za bezpečnostního opatření**
§ 6 písm. a)	Zavedeno	Politika bezpečného chování uživatelů je v dokumentu BP04_Bezp_lidskych_zdroju v kapitole „1 - Politika bezpečného chování uživatelů“ a jsou v ní zohledněna relevantní témata z přílohy č. 3.	-	-	-
§ 6 písm. b)	Zavedeno	Pravidla rozvoje bezpečnostního povědomí jsou stanovena v dokumentu Bezp_lidskych_zdroju v kapitole „2 - Rozvoj bezpečnostního povědomí“, kde jsou také pravidla pro tvorbu hesel, konkrétně v podkapitole „2.1. Pravidla pro tvorbu hesel“.	-	-	-
§ 9 odst. 2	V procesu	V současnosti společnost zavádí vícefaktorovou autentizaci.	Q2 2025	1	Petr Horák (IT oddělení)
§ 9 odst. 4 písm. a) číslo 2	Nezavedeno	Starší SCADA ve výrobě neumožňuje zadání hesla o délce více než 12 znaků.	-	-	-
§ 10 odst. 1 písm. c)	Zavedeno	Spouštění obsahu z vyměnitelných zařízení je na všech noteboocích zakázáno, a to podle dokumentu XXX.	-	-	-

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

- ***odst. 3 - Bezpečnostní politika a bezpečnostní dokumentace***
  - Vytvoření a schválení bezpečnostní politiky a bezpečnostní dokumentace
  - Stanovená pravidla a postupy je nutné:
    - pravidelně přezkoumávat a aktualizovat,
    - dodržovat a jejich dodržování vynucovat a kontrolovat.

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

- ***odst. 4 - Používání a manipulace technických aktiv***
  - stanovením a zavedením pravidel ochrany a přípustných způsobů používání aktiv
  - Pravidla a postupy je nutné stanovit pro:
    - označování aktiv,
    - manipulaci s aktivy a
    - likvidaci aktiv

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

- ***odst. 5 - Smlouvy s dodavateli***
  - Plnění požadavků zajišťování kybernetické bezpečnosti i po dodavatelích
  - Příloha č. 2 vyhlášky – stanovené minimum
  - Jedná se např. o ustanovení:
    - zajišťující bezpečnost informací,
    - sankce za porušení smlouvy,
    - upravující povinnost dodavatele dodržovat pravidla pro dodavatele stanovená poskytovatelem regulované služby,
    - o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy nebo
    - řízení změn.

§ 3 Systém zajišťování minimální kybernetické bezpečnosti

- ***odst. 6 - Akvizice, vývoj a údržba***
  - Stanovení jasných požadavků na zajištění kybernetické bezpečnosti a vyžadování jejich dodržování

§ 4 Požadavky na vrcholné vedení

Cíl bezpečnostního opatření: Zapojení vrcholného vedení do řízení kybernetické bezpečnosti.

- ***písm. a) - Určení osoby pověřené kybernetickou bezpečností***
  - Osoba, která disponuje svěřenými pravomocemi k řízení a rozvoji kybernetické bezpečnosti, dohledem nad jejím stavem a pravidelnou komunikaci s vrcholným vedením
- ***písm. b) Absolvování školení***
  - Pravidelné školení v oblasti kybernetické bezpečnosti
- ***písm. c) Zajištění zdrojů***
  - Dostatečné zdroje (finanční, personální a technické) nezbytné k dosažení požadované úrovně kybernetické bezpečnosti

§ 4 Požadavky na vrcholné vedení

- ***písm. d) - Pravidelné sledování stavu zavádění bezpečnostních opatření***
  - Klíčovým dokumentem je „Přehled bezpečnostních opatření“
- ***písm. e) - Podpora neustálého zlepšování zajišťování kybernetické bezpečnosti***
- ***písm. f) - Stanovení priorit obnovy***
  - Mít jasné stanovené priority obnovy

§ 5 Bezpečnost lidských zdrojů

Cíl bezpečnostního opatření: Průběžné vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti a udržování povědomí o důležitosti dodržování pravidel zaměstnanci v této oblasti.

- ***odst. 1 písm. a) - Politika bezpečného chování uživatelů***
  - Příloha č. 3 – doporučená témata pro rozvoj bezpečnostního povědomí jako jsou např.:
    - škodlivé programy a jejich projevy,
    - on-line identita, digitální stopa a její minimalizace a
    - aktuální hrozby v kybernetické bezpečnosti.
- ***odst. 1 písm. b) - Pravidla rozvoje bezpečnostního povědomí***
  - Stanovit pravidla pro vrcholné vedení, uživatele, administrátory a osoby pověřené kybernetickou bezpečnostní
  - Pravidla pro tvorbu hesel

§ 5 Bezpečnost lidských zdrojů

- ***odst. 1 písm. c) - Kontrola dodržování pravidel***
- ***odst. 2 - Školení v oblasti kybernetické bezpečnosti***
  - Poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice
  - Vstupní a pravidelná školení v oblasti kybernetické bezpečnosti
  - Odborná školené – administrátoři a osoby pověření kybernetickou bezpečností
- ***odst. 3 - Vést přehledy o provedených školení a seznamy zúčastněných osob***

§ 6 Řízení kontinuity činností

Cíl bezpečnostního opatření: Schopnost rychle a účinně reagovat na mimořádné situace, např. kybernetický bezpečnostní incident či přírodní katastrofy, které mohou regulovanou službu jakýmkoliv způsobem ovlivnit.

- **Proaktivní bezpečnostní opatření = reaktivní bezpečnostní opatření**
- ***písm. a) - Stanovení postupů obnovy technických aktiv***
  - Stanovení tří základních atributů:
    - priorita,
    - pořadí a
    - postup.
- ***písm. b) - Stanovení povinností a odpovědností***

§ 6 Řízení kontinuity činností – zálohování

- ***Písm. c)* – vytváření záloh, nezbytných zejména pro účely obnovy regulované služby**
- Pravidelné zálohy
  - Stanovení periody, která se bude dodržovat
- Informací a dat
  - Obsah, se kterým organizace pracuje
- Konfigurací a nastavení technických aktiv
  - Nastavení virtualizace, síťových prvků, ACL pravidel, bezpečnostních nástrojů atd.
- Doporučení: Inspirovat se požadavky na zálohování z vyššího režimu
  - Ochrana záloh a jejich dat před narušením jejich dostupnosti a integrity
  - Testování dostupnosti, integrity a obnovitelnosti u těchto záloh
  - Oddělení zálohovacího prostředí od jiných prostředí prostřednictvím segmentace komunikační sítě

§ 10 Řešení kybernetických bezpečnostních incidentů

Cíl bezpečnostního opatření: Nastavení procesů pro řešení kybernetických bezpečnostních incidentů.

- ***písm. a) - Oznámení***
  - Neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti
- ***písm. b) - Metodika pro posuzování***
  - Určení významnosti dopadu - v souladu s § 14 vyhlášky
- ***písm. c) a d) - Detekce kybernetických bezpečnostních událostí***
  - v souladu s vytvořenou metodikou
- ***písm. e) a f) - Hlášení kybernetického bezpečnostního incidentu*** (v souladu s § 15 zákona)
  - Závěrečná zpráva o jeho vyřešení v souladu s § 16 zákona
  - ***(viz samostatná přednáška Zákon č. 264/2025 Sb., o kybernetické bezpečnosti)***

§ 14 Stanovení významnosti dopadu KBI

Cíl bezpečnostního opatření: Způsob určení významnosti kybernetického bezpečnostního incidentu na poskytování regulované služby.

- ***odst. 1 – Stanovení hodnot v rámci metodiky***
  - Únosné míry újmy – souhrn nejvyšší škody a nemajetkové újmy vzniklé v souvislosti s kybernetickým bezpečnostním incidentem
  - Oblasti pro posouzení významnosti dopadu kybernetických bezpečnostních incidentů:
    - provozní dopad,
    - množství zasažených osob,
    - zdroje potřebné pro obnovu,
    - typ a umístění dotčených aktiv,
    - citlivost a
    - přímou příčinu, je-li poskytovateli známa.
- ***odst. 2 – posouzení významnosti dopadu kybernetického bezpečnostního incidentů***
  - Překročení metodikou stanovené hodnoty

Vyhodnotitelná bezpečnostní opatření

§ 7 Řízení přístupu – řízení přístupu k aktivům

- ***Odst. 1* – řízení identifikátorů a přístupových práv a oprávnění**
- *Písm. a), b)* – Identifikátory
  - Jedinečné (jmenné) identifikátory pro jednotlivé uživatele přistupujícím k aktivům
    - Omezení přístupových práv a oprávnění na pouze nezbytně nutná
    - Oddělení uživatelských a administrátorských oprávnění jedné osoby
  - Účty technických aktiv a jejich identifikátory a přístupová práva a oprávnění

- *Písm. c)* – Bezpečnostní opatření u mobilních zařízení přistupujících k aktivům včetně těch mimo správu organizace
  - Např. zavedení tzv. Mobile device management

- *Písm. d), e), f)* – Přístupová práva a oprávnění
  - Pravidelný přezkum přístupových práv a oprávnění
  - Uživatel změnil pracovní pozici – bezodkladná změna/odebrání jeho přístupových práv a oprávnění
  - Uživatel ukončil smluvní vztah – bezodkladná změna/odebrání jeho přístupových práv a oprávnění
    + deaktivace účtu

§ 7 Řízení přístupu – fyzická bezpečnost

- ***Odst. 2* – zajištění fyzické bezpečnosti pro prevenci narušení bezpečnosti poskytování regulované služby**
- Zajištění fyzické bezpečnosti u aktiv organizace
  - Např. servery, zálohy, síťové prvky, atd.
- Zamezení neoprávněnému přístupu
  - Např. umístění do serverovny s bezpečnostními dveřmi, funkčním klíčovým režimem a knihou návštěv
- Předcházení poškození
  - Např. protipožární ochrana, dvojitá podlaha, záplavová čidla atd.
- Předcházení odcizení, zneužití a zásahů do nich
  - Zamezení neoprávněnému přístupu, kamerový systém, dohled nad přistupujícími osobami, uzamykatelné racky, zaslepené porty, atd.

§ 8 Řízení identit a jejich oprávnění – specifikace nástroje

- ***Odst. 1* – specifikace nástroje na řízení identit a přístupových práv a oprávnění**
- Používání nástroje, který:
  - *Písm. a)* – řídí počet neúspěšných pokusů o přihlášení
    - Lze u něj nastavit, že se účet po určeném počtu neúspěšných pokusů zablokuje
  - *Písm. b)* – opětovně ověřuje identitu po době nečinnosti
    - Umožňuje, aby se účet po určité době nečinnosti sám uzamknul a uživatel se musel znovu autentizovat
  - *Písm. c)* – zajišťuje odolnost přenášených autentizačních údajů
    - Zajišťuje, že autentizační údaje jsou uloženy a přenášeny v bezpečné formě, např. v hashi
  - *Písm. d)* – řídí přístupová práva a oprávnění pro čtení a zápis a pro změnu oprávnění
    - Umožňuje řídit práva a oprávnění jednotlivých účtů nebo skupin účtů

§ 8 Řízení identit a jejich oprávnění – způsoby autentizace

- ***Odst. 2, 3, 4* – možné druhy a způsoby autentizace**
- *Odst. 2* – Využití autentizačního mechanismu založeného na vícefaktorové autentizaci
  - Nejbezpečnější způsob autentizace, např. heslo + autentizační token (autentizační aplikace v telefonu)

- *Odst. 3* – Do splnění odst. 2 využití autentizace založené na kryptografických klíčích nebo certifikátech
  - Alternativa k odst. 2, využití např. samotných čipových karet nebo jiných kryptografických prostředků k autentizaci

- *Odst. 4* – Do splnění odst. 3 využití autentizace s dostatečně silnou politikou hesel
  - Alternativa k odst. 3, politika hesel splňující uvedené požadavky a její technické vynucování
  - Požadavky na:
    - Délku
    - Komplexitu
    - Dobu, kdy se heslo může/nemůže změnit
    - Zamezení používání stejného hesla

§ 8 Řízení identit a jejich oprávnění – ochrana aut. údajů

- ***Odst. 5* – další požadavky v rámci řízení identit**
- *Písm. a)* – Zajištění důvěrnosti při vytváření výchozích aut. údajů a při obnově přístupu
  - Zajištění, aby tato hesla znal pouze uživatel, který heslo bude používat
- *Písm. b)* – Zajištění změny výchozího nebo obnovovacího hesla po prvním použití
  - Zajištění, aby si uživatel po prvním zadání tohoto hesla musel nastavit vlastní heslo
- *Písm. c)* – Zneplatnění obnovovacího hesla do 24 hodin od jeho vytvoření
  - Zajištění, aby v případě nevyužití tohoto hesla muselo být vygenerováno nové
- *Písm. d)* – Bezodkladná změna hesla v případě podezření na jeho kompromitaci
  - Organizační opatření, kdy uživatel nebo administrátor vynutí změnu hesla v případě podezření na jeho vyzrazení
  - Např. v případě podezření na únik databáze hesel na dark web
- *Písm. e)* – Zabezpečení speciálních účtů určených pro obnovu po incidentu
  - Zabezpečení speciálních např. „root“ účtů využívaných k obnově systémů
  - Např. vygenerováním dlouhého náhodného hesla a jeho uložení do zapečetěného trezoru

§ 9 Detekce a zaznamenávání KBU – detekce

- ***Odst. 1* – nástroje pro detekci a blokování nežádoucí komunikace a obsahu**
- *Písm. a)* – Ověřování a kontrola přenášených dat na perimetru sítě + blokování nežádoucí komunikace
  - Např. firewall nebo IDS/IPS
- *Písm. b)* – Nástroj na nepřetržitou a automatickou ochranu před škodlivým kódem na koncových stanicích a serverech
  - Např. antivirus nebo EDR/XDR
- *Písm. c)* – Řízení automatického spouštění obsahu
  - Zakázaný „autorun“ u výměnných zařízení, blokování neschválených aplikací nebo třeba maker
- *Písm. d)* – Informování o detekovaných bezpečnostních událostech relevantním osobám
  - Např. prostřednictvím SMS, telefonu nebo e-mailu odpovědné osobě
- *Písm. e)* – Pravidelná a bezodkladná aktualizace uvedených nástrojů
  - Nejen nástrojů, ale i jejich pravidel a databází (např. virové databáze)

§ 9 Detekce a zaznamenávání KBU – zaznamenávání

- ***Odst. 2 + 3* – zaznamenávání detekovaných událostí (logování)**
- *Odst. 2 písm. a)* – Detekce bezpečnostních a relevantních provozních událostí podle bezpečnostních potřeb
  - Bezpečnostní události typu detekce škodlivého kódu, činnosti provedené administrátory nebo např. manipulace s účty
  - Provozní události typu překročení povolené teploty technického aktiva nebo např. zvýšený provoz v komunikační síti

- *Odst. 2 písm. b)* – Záznamy musí obsahovat následující informace:
  - Datum a čas události vč. časového pásma
    - Doporučení navíc: synchronizace jednotného času u všech technických aktiv
  - Typ činnosti
  - Jednoznačnou identifikaci technického aktiva a účtu původce události
  - Úspěšnost/neúspěšnost činnosti

- *Odst. 3* – Doba uchovávání záznamů dle bezpečnostních potřeb
  - Doporučená doba je 12 měsíců

§ 11 Bezpečnost komunikačních sítí – segmentace

- **Rozdělení komunikační sítě na logické segmenty a omezení síťové komunikace na minimum**
- *Písm. a), b)* – Segmentace komunikační sítě a řízení komunikace na jejím perimetru
  - Logické rozdělení komunikační sítě na menší segmenty, např. prostřednictvím VLAN
    - Oddělení produkčního prostředí od zálohovacího, ideálně ještě např.
      - Oddělení serverů a koncových stanic
      - Oddělení uživatelských a správcovských stanic
      - Oddělení síťových tiskáren od ostatních technických aktiv
      - Oddělení produkčního, testovacího a vývojového prostředí
      - Oddělení veřejného připojení/Wi-Fi od zbytku sítě
      - Zavedení DMZ (tzv. „demilitarizované zóny“)
  - Řízení příchozí a odchozí komunikace na perimetru komunikační sítě, např. prostřednictvím firewall
    - Omezení této komunikace na naprosté minimum např. formou whitelistu na firewall
    - V ideálním případě je vhodné nad požadavek vyhlášky řídit i komunikaci mezi segmenty

§ 11 Bezpečnost komunikačních sítí – vzdálený přístup

- **Zajištění bezpečného přenosu dat a informací v rámci komunikační sítě**
- *Písm. c)* – Užívání aktuálně odolných kryptografických prostředků
  - Např. užívání HTTPS namísto HTTP, SSH namísto Telnet atd.

- *Písm. d)* – Požadavky na vzdálené připojení do interní sítě nebo na vzdálenou správu technických aktiv
  - Omezení těchto připojení na nezbytně nutná a vedení přehledu o uživatelích a administrátorech užívajících tato připojení
    - Omezení přistupujících se osob na nezbytné minimum
    - Rušení již nepotřebných přístupů
    - Vedení přehledu o těchto přístupech
  - Bezpečnostní opatření zajišťující důvěrnost a integritu vzdálených připojení a správy
    - Využívání např. VPN nebo SSH pro zajištění důvěrnosti a integrity

§ 12 Aplikační bezpečnost

- **Udržování aktuálnosti technických aktiv a technické řízení zranitelností**
- *Písm. a)* – Bezodkladná aplikace schválených aktualizací
  - Nastavení procesu aktualizací technických aktiv a jejich vynucování
  - Prověření a schválení těchto aktualizací v testovacím prostředí
- *Písm. b)* – Řízení zastaralých technických aktiv
  - Vedení jejich evidence
    - Vytvoření dokumentu s evidencí těchto aktiv nebo označení těchto aktiv v rámci již existující evidence
  - Zavedení alternativních bezpečnostních opatření
    - Např. hardening, oddělení od běžného prostředí, jejich nahrazení (částečné) či omezení používání
  - Omezení jejich komunikace na nezbytně nutnou
    - Umístění těchto aktiv do vlastního segmentu a omezení komunikace s ním na nezbytně nutnou
- *Písm. c)* – Provádění skenování zranitelností
  - Pravidelné využití automatizovaného nástroje na skenování zranitelností
  - Aplikace bezpečnostních opatření u zjištěných zranitelností

§ 13 Kryptografické algoritmy

- **Kryptografická ochrana technických aktiv a komunikace technických aktiv a lidí**
- *Odst. 1* – Kryptografická ochrana technických aktiv a jejich komunikace
  - *Písm. a)* – Používání aktuálně odolných kryptografických algoritmů
    - Bezpečné protokoly, jako je HTTPS nebo SSH
    - Aktuálně odolné kryptografické algoritmy, jako je moderní šifrování nebo dostatečně dlouhé klíče
  - *Písm. b)* – Bezpečné nakládání s kryptografickými algoritmy
    - Např. zajištění informační bezpečnosti privátních klíčů
  - *Písm. c)* – Zohledňování doporučení v oblasti kryptografických algoritmů, které vydává NÚKIB
    - K dispozici zde: https://nukib.gov.cz/cs/infoservis/doporuceni/
- *Odst. 2* – Zajištění bezpečné hlasové, audiovizuální, textové, e-mailové nebo nouzové komunikace v organizaci
  - Kryptografická ochrana důvěrnosti a integrity této komunikace, např. end-to-end šifrováním

Děkuji za pozornost

https://portal.nukib.gov.cz/

regulace@nukib.gov.cz