10.4 Bezpečnost lidských zdrojů

Tento dokument popisuje opatření, které MUSÍ nebo BY MĚLO být implementováno pro:

- **Vytváření a udržování komplexního plánu rozvoje bezpečnostního povědomí.**
- **Zajištění procesů školení v souladu s ostatními bezpečnostními směrnicemi.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Bezpečnost lidských zdrojů (§ 9).

1 Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

Cíl: Zvyšování bezpečnostního povědomí v oblasti kybernetické bezpečnosti u všech zaměstnanců, stanovení pravidelných i jednorázových školení, zajištění seznámení dodavatelů s bezpečnostními politikami.

1.1 Postupy sestavení plánu rozvoje bezpečnostního povědomí

Společnost s ohledem na stav a potřeby systému řízení bezpečnosti informací a kybernetická bezpečnosti MUSÍ stanovit **plán rozvoje bezpečnostního povědomí (PRBP)**, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a vytvořit tak celkovou koncepci a strategii budování bezpečnostního povědomí.

Implementace plánu rozvoje bezpečnostního povědomí:

1.1.1 MUSÍ být určeny osoby odpovědné za realizaci jednotlivých činností uvedených v plánu.

1.1.2 Při sestavování PRBP MUSÍ být reflektována známá a potenciální rizika.

1.1.3 MUSÍ být stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.

1.1.4 Všechny relevantní cílové skupiny MUSÍ být obeznámeny s koncepcí a strategií PRBP a MUSÍ být informovány o pokroku v jeho zavádění.

1.1.5 Uživatelé, administrátoři a osoby zastávající bezpečnostní role MUSÍ být poučeni o jejich povinnostech a být pravidelně teoreticky i prakticky proškoleni. MUSÍ být zajištěna efektivní školení přizpůsobené jednotlivým rolím.

1.1.6 MUSÍ být zajištěna pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.

1.1.7 MUSÍ být zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

1.1.8 Společnost MUSÍ seznámit s platnými bezpečnostními politikami nejen tyto uživatele, ale i relevantní osoby dodavatele a kontrolovat jejich dodržování.

1.1.9 MUSÍ být určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role. MĚLY BY být

stanoveny případné sankce plynoucí z nedodržení nastavených opatření.

1.1.10 MUSÍ být prováděna aktualizace plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami.

1.1.11 Školící materiál pro jednotlivé role MUSÍ být pravidelně revidován a aktualizován.

1.1.12 MUSÍ být hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.

1.1.13 Zaměstnanci BY MĚLI být také proškoleni, jak se chovat v případě neobvyklého či podezřelého chování informačního nebo komunikačního systému, doručení nevyžádaného e-mailu, problémů s dostupností informací či služby nebo při jiné nestandardní situaci. Současně MUSÍ být seznámeni se způsobem, jak tyto neobvyklé situace hlásit.

1.1.14 MUSÍ být vedeny přehledy o školení podle plánu rozvoje bezpečnostního povědomí, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.1.15 MUSÍ být zajištěny potřebné zdroje a rozpočet na podporu PRBP.

1.1.16 MĚLY BY být zajištěny účinné mechanismy pro získávání zpětné vazbu ke školícím materiálům a jejich prezentování.

1.1.17 MĚLA BY být zajištěna podpora profesního rozvoje a certifikací pracovníků na plný nebo částečný úvazek a dalších pracovníků s významnými bezpečnostními povinnostmi.

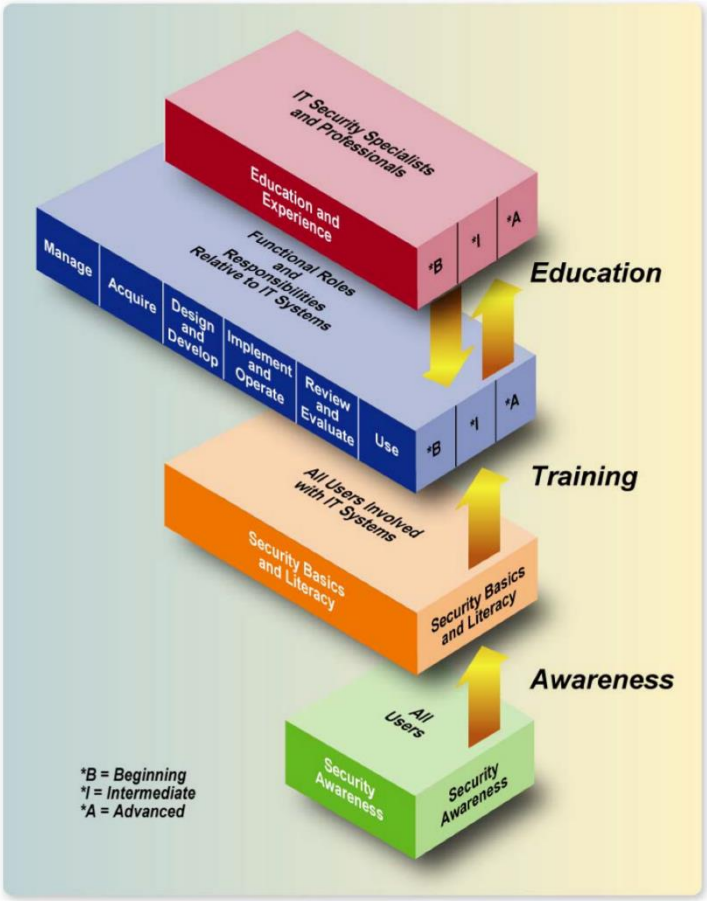
1.1.18 Implementace PRBP BY MĚLA mít následující fáze:

- návrh programu (plán)
- vytvoření programu
- implementace programu
- post implementace programu (vyhodnocení, zpětná vazba, neustálé zlepšování)

1.1.19 Vývoj bezpečnostního povědomí přizpůsobený jednotlivým rolím v rámci společnosti MUSÍ být kontinuální proces.

1.1.20 Po zavedení plánu rozvoje bezpečnostního povědomí BY MĚLA být získána zpětná vazba pro účely zpřesnění obsahu prováděných školení. Zpětná vazba MŮŽE být získána formou dotazníku (vzory dotazníků jsou například v publikaci NIST SP 800-16 v příloze D (1)).

1.1.21 Jako vzor pro budování bezpečnostního povědomí MŮŽE být využit model budování bezpečnostního povědomí SAE (Security Awareness Education) znázorněný na obrázku 1.



Obrázek 1: SAE model (Zdroj: (2))

Model SAE má tři úrovně – Awareness (povědomí), Training (školení), Education (vzdělání), čtvrtou úrovní může být Professional development (profesní rozvoj).

Základem SAE programu je **povědomí.** Publikace NIST SP 800-16 (1) definuje povědomí jako schopnost uživatele vyvarovat se takového chování, které by ohrozilo informační i kybernetickou bezpečnost. Za správné je považováno takové chování, které vede k účelnému a efektivnímu zacházení se svěřenými technologiemi. Budování bezpečnostního povědomí uživatelů by měly vést změně chování uživatele, popřípadě k posílení dobrých bezpečnostních postupů, umožnit jednotlivcům rozpoznat hrozby v zabezpečení informačních systémů a poskytnout jim návod, jak odpovídajícím způsobem jednat. Příkladem zvyšování bezpečnostního povědomí na první úrovni je šíření informací o ochraně před viry.

Na druhém stupni programu budování bezpečnostního povědomí se nachází **školení**. Publikace NIST SP 800-16 definuje školení jako poskytnutí relevantních a potřebných znalostí a dovedností k infomační a kybernetické bezpečnosti uživatelům. Vedoucí oddělení jsou povinni zajistit, aby všem jejich podřízeným byla poskytnuta odborná příprava a řádné školení. V rámci školení se usiluje o vytvoření potřebných dovedností. Školení o budování bezpečnostního povědomí se mělo opakovat v pravidelných intervalech, příp. tehdy, vyžaduje-li si to daná situace.

Vzdělávání v informační a kybernetické bezpečnosti se nachází na třetí úrovni programu budování bezpečnostního povědomí. Podle publikace NIST SP 800-16 vzdělávání integruje všechny potřebné

bezpečnostní znalosti a dovednosti různých dílčích funkcionalit do jednoho celku, který je obohacen o koncepty a zásady příbuzných oblastí (např. technologické a sociální), čímž dosahuje synergického efektu. Absolvent vzdělávání v bezpečnostním povědomí se stává odborníkem na informační a kybernetickou bezpečnost schopným stanovit vizi a řešit problematiku bezpečnosti proaktivně.

V rámci procesu vzdělávání se rozdělují uživatelé podle znalostí a zkušeností do tří skupin:

- **začátečníky** (B, Beginning) např. noví zaměstnanci,
- **středně pokročilé uživatele** (I, Intermediate) a
- **pokročilé uživatele** (A, Advanced).

Na základě skupin se definuje složitost a rozsah vzdělávacích kurzů. Pro každou z uvedených skupin MUSÍ být určen specifický cíl kurzu.

Profesionální rozvoj, nejvyšší úroveň SAE programu, obsahuje profesionální rozvoj odborníků na oblast řízení systému bezpečnosti informací. Smyslem této úrovně je zajistit, aby všichni uživatelé od začátečníků až po profesionály měli požadovanou úroveň znalostí a dovedností nezbytně nutných pro výkon jejich funkce. Při splnění stanovených podmínek a prokázání požadovaných kompetencí je možné v rámci profesionálního rozvoje získat certifikát. Příprava na certifikaci obvykle zahrnuje studium předepsaného penza znalostí nebo technických učebních osnov. To vše může být doplněno o praktické zkušenosti.

Školení bezpečnostního povědomí (Security awareness) je určeno pro všechny uživatele v rámci společnosti.

Školení základů kyberbezpečnosti a digitální gramotnosti (Security basics and literacy) je určeno všem uživatelům zapojených do IT systému.

Školení pro funkční role (Functional roles and responsibilities relative to IT system) je poskytováno uživatelům s přidělenou odpovědností za IT systém.

Vzdělání (Education) a **zkušenosti** (Experience) získávají specialisté a odborníci na bezpečnost IT.

PRBP BY MĚL mít následující strukturu (části zvýrazněné tučně jsou **povinné**):

- role a odpovědnosti PRBP (zejména **osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny**)
- stanovení cílů pro každou fázi plánu (budování povědomí, školení, vzdělávání profesní rozvoj, certifikace)
- rozdělení uživatelů (analýza) do skupin
- vytvoření školících materiálu dle skupin uživatelů
- určení cíle pro každou skupinu uživatelů
- témata, která je třeba řešit v každé relaci či kurzu
- metody nasazení pro každý aspekt programu (metodiky)
- **obsah a termíny poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role**
- **obsah a termíny poučení nových zaměstnanců.**
- **přehledy, které obsahují předmět jednotlivých školení a seznam osob, které školení absolvovaly**
- dokumentace, zpětná vazba a doložení o výuky
- **formy a způsoby hodnocení plánu**
- četnost opakování včetně aktualizace výukových materiálů
- kalkulace

1.2 Způsoby a formy poučení uživatelů

Všichni uživatelé (včetně dodavatelů) systémů a aplikací:

1.2.1 MUSÍ absolvovat školení o bezpečnostním povědomí a být dostatečně poučeni (školeni) o svých odpovědnostech.

1.2.2 MUSÍ být náležitě vyškoleni ve způsobu plnění svých povinností v oblasti IT/kybernetické bezpečnosti, před tím, než jim je umožněn přístup do systému.

1.2.3 MUSÍ porozumění jednotlivým krokům své činnosti v rámci systémů a aplikací, ke kterým mají přístup a dopadům svého chování, aby bylo sníženo riziko neúmyslných chyb a opomenutí souvisejících s užíváním systému kvůli nedostatku bezpečnostního povědomí.

1.2.4 MUSÍ být srozuměni se správným používáním hesla, zálohováním dat, využíváním antivirové ochrany, postupem hlášení jakýchkoliv podezřelých incidentů nebo porušení bezpečnostních zásad, dodržováním pravidel nastavených k odvrácení potenciálních útoků a šíření spamů nebo virů a udržováním aktuálnosti a platnosti bezpečnostních řešení (např. antivirových programů).

1.2.5 Nabyté znalosti získaní školeními BY MĚLY být ověřeny (např. zaslání testovacího pshishingového emailu atp.)

1.2.6 Školení pro uživatele BY MĚLO obsahovat:

- školení obecného bezpečnostní povědomí o chování v kyberprostoru (např. eLearning kurz s testem).

1.2.7 Školení pro dodavatele BY MĚLO obsahovat:

- seznámení se s pravidly řízení informační a kybernetické bezpečnosti EOP, aby nedošlo k narušení bezpečnosti ze strany dodavatele;
- předávání potřebných informací.

1.3 Způsoby a formy poučení garantů aktiv

Garant aktiva:

1.3.1 MUSÍ se pravidelně účastnit školení přizpůsobených pro danou roli, které schválilo vedení společnosti. Školení BY MĚLO probíhat jednou ročně v prezenční formě nebo v případě potřeby (při změně či bezpečnostním incidentu).

1.3.2 MUSÍ spolupracovat s vedením a podat informace o tom, které další školení by mohlo garantům pomoci lépe zabezpečit aktiva, za která odpovídají.

1.3.3 MUSÍ chápat kybernetickou bezpečnost jako nedílnou součást své práce.

1.3.4 MUSÍ porozumět povinnostem a odpovědnostem, které jsou kladeny společností a kybernetickým zákonem na garanty aktiv.

1.3.5 MUSÍ porozumět, jak implementovat a udržovat kontrolní mechanismy kybernetické bezpečnosti.

1.3.6 MUSÍ pochopit možnosti, jak zmírnit/eliminovat rizika působící na aktiva.

1.3.7 MUSÍ monitorovat stav zabezpečení aktiv, za které je garant odpovědný.

1.3.8 MUSÍ při odhalení narušení bezpečnosti bez odkladu náležitě reagovat (oznámit incident, aplikovat reaktivní opatření).

1.3.9 MUSÍ uplatnit znalosti získané školením.

1.3.10 MUSÍ mít znalost zákona o kybernetické bezpečnosti (ZKB, zákon č. 181/2014 Sb.) ve znění pozdějších předpisů a vyhlášky o kybernetické bezpečnosti (VKB, vyhláška č. 82/2018 Sb.) ve znění pozdějších předpisů (3).

1.3.11 MUSÍ mít znalost svěřeného aktiva.

1.3.12 Školení pro garanta aktiv BY MĚLO obsahovat:

- seznámení se s požadavky ZKB a VKB,
- technické školení.

1.4 Způsoby a formy poučení administrátorů

Administrátor:

1.4.1 MUSÍ prokázat dobrou znalost svěřeného technického aktiva.

1.4.2 MUSÍ se pravidelně účastnit školení přizpůsobených pro danou roli, které schválilo vedení společnosti. Školení BY MĚLO probíhat jednou ročně v prezenční formě nebo v případě potřeby (při změně či bezpečnostním incidentu).

1.4.3 Manažer kybernetické bezpečnosti BY MĚL pro administrátora nastavit pravidla profesního rozvoje (PD) dle plánu PD.

1.4.4 Školení pro administrátora BY MĚLO obsahovat:

- technické školení.

1.4.5 Konkrétní doporučení pro administrátory je uvedeno v příloze C.

1.5 Způsoby a formy poučení osob zastávajících bezpečnostní role

Pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí MUSÍ být zajištěna pravidelná odborná školení, přičemž vychází z aktuálních potřeb povinné osoby v oblasti kybernetické bezpečnosti.

1.5.1 Zaměstnanci zastávající bezpečnostní role a zaměstnanci na IT pozicích BY MĚLI kromě standardních školení absolvovat i specializovaná a odborná školení související s výkonem jejich pozice, včetně školení zaměřených na kybernetickou bezpečnost. V příloze č. 6 VKB jsou uvedeny požadavky na jednotlivé bezpečnostní role, z tohoto výčtu se MŮŽE vycházet při plánování odborných školení. Společnost MŮŽE při tvorbě školení na základě rolí vycházet také z publikace NIST SP 800-16 (Příloha C), kde se jsou jednotlivým rolím přiřazeny kompetence, znalosti (teoretické nebo praktické porozumění kompetencím) a dovednosti.

1.5.2 Při výskytu mimořádné události (např.: nová obecně známá hrozba, zvýšený výskyt phishingových e-mailů apod.) BY MĚLO být zorganizováno mimořádné školení, případně zaměstnance informovat jiným vhodným způsobem.

Manažer kybernetické bezpečnosti:

1.5.3 MUSÍ mít znalost ZKB a VKB.

1.5.4 MUSÍ mít odbornou znalost postupů při řízení kybernetické bezpečnosti.

1.5.5 Školení pro manažera kybernetické bezpečnosti BY MĚLO obsahovat:

- seznámení se s požadavky ZKB a VKB,
- seznámení s podstatou bezpečnostních opatření a efektivními způsoby k jejich zajištění.

Architekt kybernetické bezpečnosti:

1.5.6 MUSÍ mít znalost ZKB a VKB.

1.5.7 MUSÍ mít odbornou znalost postupů při řízení kybernetické bezpečnosti.

1.5.8 MUSÍ mít potřebné technické znalosti

1.5.9 Školení architekt kybernetické bezpečnosti BY MĚLO obsahovat:

- Seznámení se s požadavky ZKB a VKB
- Seznámení s podstatou bezpečnostních opatření a efektivními způsoby k jejich zajištění.
- Seznámení s bezpečnostními oblastmi technických opatření a efektivními přístupy k jejich zajištění.

Auditor kybernetické bezpečnosti:

1.5.10 MUSÍ mít znalost ZKB a VKB.

1.5.11 MUSÍ mít znalosti potřebné k provádění auditu kybernetické bezpečnosti.

1.5.12 Školení auditor kybernetické bezpečnosti BY MĚLO:

- Připravit účastníky na efektivní provádění auditů kybernetické bezpečnosti na úrovni certifikovaných auditorů.

1.5.13 V rámci zvyšování bezpečnostního povědomí vytvořil NÚKIB vzdělávacím portálu https://osveta.nukib.cz/. E-learningové kurzy, které MOHOU být využity pro školení zaměstnanců:

- Kurz pro manažery kybernetické bezpečnosti (e-learning).
- Základy kybernetické bezpečnosti (vhodné pro běžné uživatele).
- Doporučení pro bezpečný pohyb v kybersvětě.

1.5.14 MĚLA BY být využita doporučení vydávaná NÚKIB (https://www.nukib.cz/cs/infoservis/doporuceni).

2 Bezpečnostní školení nových zaměstnanců

2.1.1 Noví zaměstnanci MUSÍ být dostatečně bezpečnostně proškoleni před tím, než je jim umožněn přístup do systému společnosti.

2.1.2 Školení MUSÍ absolvovat při nástupu včetně specifických školení souvisejících s kybernetickou bezpečností určených pro konkrétní pracovní pozice.

2.1.3 Povinné základní školení BY MĚLO být absolvováno v prezenční formě a povinnost jej absolvovat BY MĚLA být zabudována do pracovní smlouvy

2.1.4 Následně se zaměstnanci MUSÍ pravidelně účastnit školení. Školení BY MĚLO probíhat jednou ročně v prezenční formě nebo v případě potřeby (při změně či bezpečnostním incidentu).

3 Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací

3.1.1 Uživatelé MUSÍ být obeznámeni o rizicích porušení bezpečnostní politiky a případné narušení bezpečnosti (incidenty) MUSÍ hlásit odpovědným osobám (viz SM-22_Zvládání kybernetických bezpečnostních incidentů).

3.1.2 Uživatelé MUSÍ být seznámeni s přístupnou bezpečnostní dokumentací včetně disciplinárních kroků za porušení bezpečnostních pravidel (porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů).

3.1.3 Nedodržení bezpečnostní politiky MŮŽE být kvalifikováno jako porušení povinností zaměstnance případně porušení pracovní kázně s příslušnými důsledky. Případy porušení bezpečnostní politiky se řeší podle pracovního řádu s návazností na pracovní smlouvy.

3.1.4 Šetření závažných bezpečnostních incidentů provádí vedoucí technik informačních řídicích systémů včetně zpracování protokolů o bezpečnostních incidentech, jejich evidence a předložení návrhů řediteli společnosti k zajištění bezpečnosti.

4 Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

4.1 Vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu

4.1.1 MUSÍ být zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.

4.1.2 V případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role MUSÍ být zajištěno předání odpovědností. ¨

4.1.3 MUSÍ být odevzdána všechna používaná aktiva společnosti včetně dat na mobilních zařízeních.

4.2 Změna přístupových oprávnění při změně pracovní pozice

4.2.1 MUSÍ být zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

4.2.2 Pokud u zaměstnance dojde ke změně pracovního místa a vzniku potřeby proškolení na kybernetickou bezpečnost ve větším rozsahu MUSÍ absolvovat odpovídající školení.

Použité zdroje

(1) *NIST Special Publication 800-16: A Role-Based Model for Federal Information Technology/ Cybersecurity Training*. Revision 1 (3rd Draft). Gaithersburg: National Institute of Standards and Technology, 2014. Dostupné také z: https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf

(2) CABALLERO, Albert. Security Education, Training, and Awareness. *Computer and Information Security Handbook (Third Edition)* [online]. [cit. 2022-04-11]. Dostupné z: https://www.sciencedirect.com/science/article/pii/B9780128038437000338

(3) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(4) Podpůrné materiály: Pomůcka k auditu bezpečnostních opatření. In: *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2019-03-11]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/

(5) Doporučení NÚKIB pro administrátory, verze 4.0. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. NÚKIB [cit. 2022-04-11]. Dostupné z: https://www.nukib.cz/cs/infoservis/doporuceni/1511-doporuceni-nukib-pro-administratory-verze-4-0/

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)

Příloha B – Checklist k auditu (Zdroj: (4))

3.1.7. Bezpečnost lidských zdrojů (VKB § 9)

KII	VIS			N	P	Z	NA
X	X	odst. 1 a)	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.				
X	X	odst. 1 b)	V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.				
X	X	odst. 1 c)	Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.				
X	X	odst. 1 d)	Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.				
X	X	odst. 2	O školení podle odstavce 1 jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.				
X		odst. 3 a)	Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.				
X		odst. 3 b)	Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.				
X		odst. 3 c)	Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.				
X		odst. 3 d)	Zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.				

Příloha C: Bezpečnostní doporučení NÚKIB pro administrátory (Zdroj: (5))

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ
tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

SPRÁVA ÚČTŮ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY
Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET
pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.
Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.
V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE / CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

NASAĎTE ANTI-DDoS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

STANICE A SERVERY

UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM
pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE,
pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,
používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ
a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
– povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,
které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH
detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH
– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

POUŽÍVEJTE ANTIVIROVÝ A BEZPEČNOSTNÍ SOFTWARE
a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

ŠIFRUJTE DISKY
– zejména u přenosných počítačů – včetně centrální evidence klíčů.

VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),
tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

NASTAVTE HESLO UEFI/BIOS
unikátní pro každou stanici s centrální správou hesel.

VYNUCUJTE SECURE BOOT
a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

CHRAŇTE SE PŘED ÚTOKY NA HESLA
u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

PRO SPRÁVU SERVERŮ POMOCÍ SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA
Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.