10.8 Řízení přístupu

Tento dokument popisuje opatření, která MUSÍ nebo BY MĚLA být implementováno pro:

- **Omezení přístupu k informacím a prostředkům pro zpracování informací společnosti.**
- **Zajištění oprávněného uživatelského přístupu.**
- **Prevenci neoprávněného přístupu k systémům a aplikacím.**
- **Řízení přístupů na základě rolí a evidence přidělování nebo odebírání přístupových oprávnění.**
- **Specifikace parametrů pro hesla a využívání vícefaktorové autentizace.**

Dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Řízení přístupu (§ 12), Správa a ověřování identit (§ 19), Řízení přístupových oprávnění (§ 20).

Vztahuje se na zaměstnance a dodavatele společnosti, také na uživatele obchodních partnerů a dodavatelů v prostředích informačních (IT) technologií společnosti.

---

1 Princip minimálních oprávnění/potřeba znát (need to know)

Cíl: Omezit přístup k informacím a prostředkům pro zpracování informací. Pro všechny typy účtů MUSÍ být uplatněn princip need-to-know. To znamená, že každý účet má nastavena pouze taková oprávnění, která jsou nezbytná pro provádění činností odpovídajících pracovní pozici a náplni práce uživatele. Vedení organizace by nemělo být výjimkou a mělo by využívat běžné uživatelské účty.

1.1 Politika správy přístupu

Společnost MUSÍ na základě provozních a bezpečnostních potřeb řídit přístup k informačnímu a komunikačnímu systému a přijímat opatření, která slouží k zajištění ochrany údajů používaných pro přihlášení a která brání ve zneužití těchto údajů neoprávněnou osobou.

Při určování úrovně podrobností a síly opatření pro přístup, přístupová práva a omezení pro specifické uživatelské role ve vztahu k jejich aktivům MUSÍ být zohledněny požadavky na důvěrnost a integritu ochraňovaných informací.

Typy aktiv a vlastnictví aktiv jsou popsány v SM-2 Řízení aktiv, odpovídající oddíly MUSÍ být zohledněny. Opatření fyzického přístupu viz SM-15 Fyzická bezpečnost MUSÍ být také zvažovány v souvislosti s opatřeními logického přístupu.

Implementační pokyny:

1.1.1 Způsob autorizace MUSÍ být zdokumentován v rámci provozně/bezpečnostní dokumentace k informačnímu nebo komunikačnímu systému.

1.1.2 Pro informační nebo komunikační systém MUSÍ být definovány samostatné uživatelské role, které se dále člení dle aplikačních požadavků. Informační nebo komunikační systém MUSÍ zajišťovat tzv. AAA (Autentizaci, Autorizaci, Audit) v potřebné úrovni dle jeho konkrétní specifikace.

1.1.3 Dokumentace řízení přístupu MUSÍ obsahovat koncept rolí a oprávnění, který zahrnuje definice toho, jaká oprávnění mají přiřazenou danou roli pro definovanou akci na definovaném zdroji za definovaných podmínek (např.: *role A* má oprávnění vykonat *akci B* [např. číst, psát, spouštět] na *zdroji C* [např. objekt], pokud platí *podmínka D* [např. úspěšná identifikace a ověření], viz 4.2, 2.3).

1.1.4 Dokumentace řízení přístupu MUSÍ zahrnovat formální postupy pro schvalování požadavků uživatelského přístupu oprávněnou osobou po zvážení principu „potřeba vědět“/ „potřeba využívat“ („**need-to-know principle“/„need-to-use principle**“).

1.1.5 Přístupová oprávnění se MUSÍ pravidelně přezkoumávat a případně upravit podle výše zmíněného principu.

1.1.6 Dokumentace řízení přístupu MUSÍ definovat oddělení rolí za účelem zajištění toho, že konfliktní role a oblasti zodpovědností jsou od sebe oddělené, aby se snížily možnosti neoprávněného zneužití (Rozdělení povinností/segregation of duties, SoD). Vždy, když nelze dosáhnout oddělení rolí, BY MĚLA být zvážena další opatření, např. monitorování aktivit, hodnocení auditních stop a dohled na řízení.

1.1.7 Kdykoliv je vyžadováno přiřadit přístupová práva k účtům, které jsou používány postupně různými uživateli, MUSÍ být tato skutečnost zdokumentována, včetně

a) identifikace a posouzení rizik snižujících nedostatek možností zpětného dohledání, které mohou být s takovou situací spojené, a
b) snížení těchto rizik na přijatelnou úroveň zavedením dodatečných a/nebo pokročilých kontrolních prvků, a
c) přijetí zbytkového rizika vlastníkem aktiva.

2 Požadavky na řízení přístupu

Cíl: Zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systémům a službám.

2.1 Základní požadavky řízení přístupu

Přístup MUSÍ být řízen na základě rolí a MUSÍ být evidováno přidělování nebo odebírání přístupových oprávnění.

Implementační pokyny:

2.1.1 Společnost MUSÍ řídit přístup na základě skupin a rolí.

2.1.2 Každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému MUSÍ být přidělena přístupová práva a oprávnění a jedinečný identifikátor.

2.1.3 Společnost MUSÍ řídit identifikátory, přístupová práva a oprávnění aplikací a technických účtů.

2.1.4 Společnost MUSÍ zavést bezpečnostní opatření pro řízení přístupu zařízení k prostředkům informačního a komunikačního systému.

2.1.5 Společnost MUSÍ zavést bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení a jiných technických zařízení, popřípadě i bezpečnostní opatření spojená s využitím technických zařízení, která společnost nemá ve své správě (viz SM-12 Bezpečné používání mobilních zařízení).

2.1.6 Společnost MUSÍ definovat pravidla a postupy potřebné pro omezení a kontrolu používaného softwaru a hardwaru, který by mohl narušit systémovou a aplikační bezpečnost. Jedná se např. o kontrolu připojovaných USB, antivir apod. (SM-12 Bezpečné používání mobilních zařízení, SM-17_Ochrana před škodlivým kódem).

2.2 Přístup k sítím a síťovým službám

Uživatelé MUSÍ mít k dispozici pouze přístup k sítím a síťovým službám, pro jejichž použití byli výhradně autorizováni.

Implementační pokyny:

2.2.1 Uživatelský přístup k sítím společnosti BY MĚL být chráněn opatřeními fyzického přístupu (např. fyzické vstupní prvky a/nebo fyzické bezpečnostní oblasti, viz SM-15 Fyzická bezpečnost a/nebo technickými opatřeními logického přístupu (např. IEEE 802.1X nebo ověření certifikátem zařízení). Síla ochrany fyzického přístupu a/nebo technických opatření logického přístupu BY MĚLA brát v potaz související požadavky na důvěrnost a integritu ochraňovaných informací.

2.2.2 Uživatelský přístup k síťovým službám společnosti MUSÍ být chráněn ověřením uživatele. Síla ověření uživatele BY MĚLA brát v potaz související požadavky důvěrnosti a integrity. Příklad síťových služeb společnosti zahrnuje:

a) služby doménové či síťové infrastruktury,
b) vzdálený síťový přístup.

2.2.3 Postupy MUSÍ být zdokumentovány a udržovány, aby popsaly, jak je chráněn přístup k povoleným sítím a síťovým službám, včetně popisu použitých prostředků a odpovědností dané prostředky provozovat a udržovat.

2.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu svých autentizačních informací.

Uživatelé MUSÍ dodržovat interní nařízení společnosti o používání privátních autentizačních informací (větší míra zabezpečení).

Implementační pokyny:

2.3.1 Požadavky týkající se použití privátních autentizačních informací jsou zahrnuty ve SM Bezpečné předávání a výměny informací a MUSÍ být dodržovány.

2.3.2 Dodatečné požadavky na použití privátních autentizačních informací MUSÍ být zdokumentovány a jasně sděleny příslušným zúčastněným stranám.

2.3.3 Odpovědnosti zaměstnanců a dodavatelů v rámci bezpečnosti informací jsou popsány v SM Bezpečnost lidských zdrojů, podmínky zaměstnaneckého poměru MUSÍ být dodrženy.

3 Řízení přístupu k systémům a aplikacím

Cíl: Zabránit neoprávněnému přístupu k systémům a aplikacím.

3.1 Omezení přístupu k informacím

Přístup k informacím a aplikačním systémovým funkcím BY MĚL být omezen v souladu s politikou správy přístupu.

Implementační pokyny:

3.1.1 Při omezování přístupu k informacím BY MĚLA být zvážena (s ohledem na související požadavky pro důvěrnost a integritu) následující neúplný seznam aspektů, zejména:

a) omezení systémových funkcí, ke kterým je umožněn přístup (např. poskytováním nabídek a souvisejícího řízení přístupu, které umožňují přístup pouze ke specifickým funkcím potřebným k plnění určené role),

b) omezení toho, ke kterým informacím může přistupovat konkrétní uživatel (tj. použití principu výchozího odepření přístupu),

c) omezení rozsahu, jakým může být k informacím přistupováno (např. čtení, zápis, mazání a spouštění),

d) minimalizaci potřeby silných či rozsáhlých přístupových práv/schopností na naprosté minimum,

e) omezení výstupů informací z aplikací či systémů na naprosté minimum,

f) poskytování dostatečných fyzických a logických přístupových opatření za účelem oddělení citlivých informací a aplikačních systémových funkcí.

3.2 Bezpečné postupy přihlášení

Přístup k systémům a aplikacím MUSÍ být řízen bezpečným přihlašovacím postupem využívajícím odpovídající autentizační metody pro doložení udávané identity uživatele.

Implementační pokyny:

3.2.1 MUSÍ být využíván nástroj pro správu a ověřování identity a nástroj pro řízení přístupových oprávnění.

3.2.2 Postupy bezpečného přihlášení BY MĚLY být nastaveny tak, aby:

a) ověřily přihlašovací data pouze tehdy, pokud byla zadána úplně,

b) nezobrazovaly trvale zadávané znaky hesla,
c) nenaznačovaly, která část zadávaných dat (uživatelské jméno nebo heslo) je správná či nesprávná,
d) nezobrazovaly legitimní ID uživatele (identifikátor, viz ACL – access control list,), dokud nebude přihlašovací postup úspěšně dokončený,
e) neposkytovaly během přihlašovacího postupu nápovědné zprávy, které by mohly pomoci neoprávněnému uživateli,
f) omezovaly počet neúspěšných pokusů o přihlášení, které jsou povolené (viz příloha 7),

3.2.3 Postupy bezpečného přihlašování BY MĚLY být nastaveny tak, aby:
a) zaznamenávaly úspěšné a neúspěšné pokusy o přihlášení,
b) chránily autentizační data před neoprávněným prozrazením použitím schválených
i. kryptografických hašovacích algoritmů pro skrytí hesel v čitelné textové podobě a ochraně před útoky hrubou silou (brute force attack),
ii. metod solení (salting) pro zajištění jedinečnosti hesla a zabezpečení proti útokům pomocí duhových tabulek (rainbow table).

3.3 Systém správy hesel

Systémy správy hesel MUSÍ zajišťovat kvalitní hesla.

Implementační pokyny:

3.3.1 Systém správy hesel MUSÍ:
a) ověřit identitu uživatele,
b) umožnit uživateli nastavit (zvolit a změnit) své vlastní heslo,
c) vynutit ověření hesel před přijetím jejich změn,
d) přimět uživatele změnit dočasná hesla při jejich prvním použití (pokud je to relevantní),
e) zajistit, že se hesla nezobrazují na obrazovkách nebo na výtiscích,
f) ukládat hesla odděleně od dat aplikací.

3.3.2 Kvalita hesla vynucená systémy správy hesel MUSÍ být v souladu s politikou hesel společnosti (viz příloha C).

3.3.3 Změny hesel MUSÍ být v souladu s požadavky na obnovení hesel, které jsou popsány v politice hesel společnosti (viz přílohu C).

3.4 Řízení přístupu ke zdrojovému kódu programů

Přístup ke zdrojovému kódu programů BY MĚL být omezený za účelem zabránění neoprávněnému přístupu a manipulaci (viz SM-13 Akvizice vývoj a údržba).

Implementační pokyny:

3.4.1 Zdrojový kód BY MĚL být ukládán prostřednictvím řešení pro správu zdrojového kódu.

3.4.2 Přístup ke zdrojovému kódu BY MĚL být omezený na omezený počet oprávněných osob.

3.4.3 Se zdrojovým kódem BY MĚLO být nakládáno jako s „citlivými“ informacemi.

3.5 Nástroj pro správu a ověřování identit

Společnost MUSÍ používat nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.

Implementační pokyny:

3.5.1 Nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací MUSÍ zajišťovat:
- a) ověření identity před zahájením aktivit v informačním a komunikačním systému,
- b) řízení počtu možných neúspěšných pokusů o přihlášení,
- c) odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití,
- d) ukládání autentizačních údajů ve formě odolné proti offline útokům,
- e) opětovné ověření identity po určené době nečinnosti,
- f) dodržení důvěrnosti autentizačních údajů při obnově přístupu a
- g) centralizovanou správu identit.

3.5.2 Společnost MUSÍ využívat autentizační mechanizmus, který není založený pouze na použití identifikátoru účtu a hesla, nýbrž na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů. Do doby splnění tohoto požadavku MUSÍ nástroj používat autentizaci pomocí kryptografických klíčů a zaručit obdobnou úroveň bezpečnosti.

3.5.3 Do doby splnění požadavků podle odstavce 3.5.1 nebo 3.5.2 musí nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k autentizaci identifikátor účtu a heslo, vynucovat pravidla viz příloha C.

3.6 Řízení přístupových oprávnění

Společnost MUSÍ používat centralizovaný nástroj pro řízení přístupových oprávnění.

Implementační pokyny:

3.6.1 Nástroj MUSÍ zajišťovat řízení oprávnění:
- a) pro přístup k jednotlivým aktivům informačního a komunikačního systému,
- b) pro čtení dat, zápis dat a změnu oprávnění.

4 Životní cyklus řízení přístupu

4.1 Registrace a zrušení registrace uživatelů

MUSÍ být implementovány a udržovány formální postupy pro vytváření a deaktivaci účtů.

Implementační pokyny:

4.1.1 Názvy účtů MUSÍ být jedinečné.

4.1.2 Účty MUSÍ být vytvořeny a přiděleny pouze fyzickým osobám (jednotlivcům) pracujícím pro společnost nebo v jejím zastoupení.

4.1.3 Systémy a služby NESMÍ být používaný anonymně. Sdílené účty NESMÍ být provozovány. Vyjma zdůvodněných výjimek.

4.1.4 Jednotlivci BY MĚLI mít pro svou každodenní práci pouze jeden „primární“ účet.

4.1.5 Jednotlivci MOHOU požadovat dodatečné sekundární účty odlišného typu pro různé účely.

4.1.6 Některé typy sekundárních účtů MOHOU být převedeny na jinou osobu prostřednictvím zdokumentovaného a ověřitelného postupu.

4.1.7 Počet sekundárních účtů přidělených jednotlivci BY MĚL být minimální. To je vhodné nejen po stránce bezpečnosti, ale také po stránce použitelnosti.

4.1.8 Jednotlivci MUSÍ být registrováni pomocí zdokumentovaných a ověřitelných postupů kontroly totožnosti.

4.1.9 Společnost MUSÍ zajistit odebrání nebo změnu přístupových oprávnění při změně pozice nebo zařazení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

4.1.10 Společnost MUSÍ zajistit odebrání nebo změnu přístupových oprávnění při ukončení nebo změně smluvního vztahu.

4.1.11 Účty pro zrušené osoby BY MĚLY být okamžitě deaktivovány a jejich přihlašovací údaje zrušeny. V případě některých typů/účelů účtů MOHOU být povoleny výjimky z důvodů zajištění kontinuity provozu. Po zdokumentovaném období odkladu MUSÍ být účty zrušených uživatelů smazány.

4.1.12 Vytvoření účtu MUSÍ být nezměnitelně zaznamenáno (logged) nebo jiným způsobem zdokumentováno pro pravidelnou kontrolu.

4.1.13 Jednotlivci BY MĚLI být registrováni v centrálních a důvěryhodných zdrojích dat, například systémech personálního oddělení, namísto lokálních (proprietárních) postupech registrace uživatelů.

4.1.14 Aplikace BY MĚLY používat Identity & Access Management infrastrukturu.

4.2 Zajištění přístupu uživatele

Formální postupy pro poskytování přístupu uživatelů MUSÍ být implementovány, aby bylo možno přiřadit požadovaná přístupová práva k účtům a odebrat přístupová práva účtům v případě, že již nejsou déle potřeba.

Implementační pokyny:

4.2.1 Aplikace BY MĚLY přiřazovat vyžadovaná přístupová práva účtům pouze na základě rolí v souladu s procesy definovanými v jejich konceptu rolí a oprávnění (viz 1.1.1).

4.2.2 Aplikace MUSÍ přidělovat účtům vyžadovaná přístupová práva pouze na základě potřeb společnosti.

4.2.3 Aplikace MUSÍ odebrat přístupová práva účtům, jakmile potřeby společnosti pro přístup pominou.

4.2.4 Jestliže existují v rámci informačního nebo komunikačního systému lokální účty, MUSÍ se řídit politikou hesel pro privilegované účty, nebo je nutné umožnit integraci s informačním nebo komunikačním systémem pro správu privilegovaných účtů.

4.2.5 Poskytnutí přístupových práv/rolí k účtům MUSÍ být nezměnitelně zaznamenáno (logged), nebo jiným způsobem zdokumentováno k pravidelnému přezkoumání.

4.3 Odebrání nebo úprava přístupových práv

Přístupová práva všech interních i externích uživatelů k informacím a zařízením zpracovávající informace MUSÍ být odebrána nebo pozastavena po skončení jejich zaměstnaneckého poměru, smlouvy nebo dohody, a upravena po provedení změn (např. změna útvaru).

Implementační pokyny:

4.3.1 Postupy pro zrušení či pozastavení přístupových práv uživatelů po skončení jejich zaměstnaneckého poměru, smlouvy či dohody MUSÍ být zavedeny, aby bylo zajištěno, pokud je to možné:

a) přístupová práva zařízením zpracovávající informace a službám jsou odebrána okamžitě,
b) přihlašovací údaje (např. ID uživatele, heslo, token či digitální certifikát) jsou okamžitě zablokovány,
c) komponenty určené k poskytování přístupu, například tokeny nebo průkazy totožnosti zaměstnanců s čipovými kartami jsou okamžitě deaktivovány nebo odstraněny,
d) účty ve všech systémech, ke kterým měl uživatel přístup, jsou okamžitě uzamčeny.

4.3.2 Postupy pro změnu přístupových práv při změně zaměstnaneckého poměru BY MĚLY být zavedeny pro:

a) zajištění, že jsou přiřazená přístupová práva stále přiměřená pro nové zaměstnání/pozici při zvážení principů „potřeby vědět“/“potřeby využívat“ („need-to-know principle“/„need-to-use principle“),
b) ověření, zda mohou být nadbytečná přístupová práva zrušena.

4.3.3 Jakékoliv odebrání nebo změny přístupových práv BY MĚLY:

a) brát v úvahu a zahrnout, jak fyzický, tak logický přístup,
b) být nezměnitelně zaznamenány (logged), nebo jiným způsobem zdokumentovány pro pravidelnou kontrolu.

4.4 Řízení privátních autentizačních informací uživatelů

Přidělení privátních autentizačních informací MUSÍ být řízeno formální řídícím procesem.

Implementační pokyny:

4.4.1 Počáteční přidělení privátních autentizačních informací (hesel a PINů) a jakékoliv požadavky na obnovení hesel či PINů MUSÍ přímo zahrnovat osobu, které je dané heslo nebo PIN, jednoznačně přiřazeno, a to při zajištění:

a) ověření identity uživatele před poskytnutím nového (dočasného) nebo znovu nastaveného hesla či PINů,
b) zajištění, že hesla nebo PINy nejsou přenášeny/ukládány v čitelném formátu (clear text).

4.4.2 Dočasná hesla a PINy, které byly uživateli přiděleny, MUSÍ být při prvním použití změněny.

4.4.3 Dočasná hesla a PINy BY MĚLY být jedinečné pro každého uživatele a NEMĚLY BY být uhodnutelné.

4.4.4 Uživatelé BY MĚLI potvrdit příjem privátních autentizačních informací NEBO by měli být informováni o přidělení privátních autentizačních informací pro svůj účet.

4.4.5 Více viz příloha B.

5 Řízení privilegovaných oprávnění

Privilegované účty se silnými oprávněními (administrátorské účty) MUSÍ být dostatečně zabezpečeny.

Implementační pokyny:

5.1.1 Privilegované účty MUSÍ mít přiděleny samostatné přihlašovací údaje.

5.1.2 Jednotliví administrátoři MUSÍ mít vedle privilegovaného účtu i účet běžného uživatele pro činnosti, které nevyžadují privilegovaná oprávnění.

5.1.3 Přidělování a použití privilegovaných přístupových práv MUSÍ být omezováno a kontrolováno.

5.1.4 Přidělování privilegovaných oprávnění MUSÍ být omezeno na úroveň nezbytně nutnou k výkonu náplně práce.

5.1.5 Privilegovaná přístupová práva MOHOU být přidělena na aplikační úrovni, jakožto i na dalších úrovních, např. operačního systému, systému řízení databází a zahrnují:

a) *Účty lokálních administrátorů*, které poskytují administrátorský přístup k operačnímu systému na lokálním hostiteli.

b) *Privilegované uživatelské účty,* které poskytují administrační přístup k jednomu nebo více systémům (např. k operačnímu systému a/nebo databázi).

c) *Účty doménových administrátorů,* které mají úplnou kontrolu nad všemi řadiči domény a schopnost modifikovat členství každého administrátorského účtu v doméně Windows.

d) *Nouzové účty,* které poskytují neprivilegovaným uživatelům administrační přístup k systémům v případě nouze.

e) *Servisní účty,* tj. privilegované lokální nebo doménové účty, které jsou používány aplikací nebo službou k interakci s operačním systémem.

f) *Aplikační účty*, které jsou používány pro přístup k databázím a poskytují přístup k dalším aplikacím.

5.1.6 Privilegovaná přístupová práva MUSÍ být přidělena pouze za následujících podmínek:

a) daná osoba pracuje pro společnost nebo v jejím zastoupení,

b) existuje oprávněná potřeba k jejich přidělení nebo je nezbytné na základě události (event-by-event necessary),

c) rozsah privilegovaných přístupových práv je omezen na nezbytné minimum (nejméně privilegované),

d) dočasně omezené, pokud možno.

5.1.7 Privilegovaná přístupová práva NESMÍ být přidělena anonymním účtům nebo skupinám účtů.

5.1.8 Běžné pracovní aktivity BY NEMĚLY být vykonávány z účtu s přiřazenými privilegovanými přístupovými právy.

5.1.9 Privilegovaná přístupová práva MUSÍ být přiřazena prostřednictvím dokumentovaných a ověřitelných postupů. Změny privilegovaných přístupových práv MUSÍ být zaznamenávány (logged) pro pravidelnou kontrolu.

5.1.10 Privilegovaná přístupová práva BY MĚLA automaticky vypršet po definované lhůtě.

5.1.11 Pro přístup privilegovaných rolí MUSÍ být využita vícefaktorová autentizace.

5.1.12 Servisní nebo technické účty, pod kterými běží informační nebo komunikační systém nebo jeho jednotlivé komponenty, nebo prostřednictvím kterých informační nebo komunikační systém přistupuje k ostatním komponentám nebo externím informačním nebo komunikačním systémům, MUSÍ být uvedeny v dokumentaci k informačnímu nebo komunikačnímu systému. U každého účtu

MUSÍ být uveden jeho účel a způsob jakým je možné účtu změnit heslo či obnovit certifikát, včetně identifikace všech míst, kde je takové heslo či certifikát bezpečně uložen/o.

5.2 Použití privilegovaných obslužných programů

Použití privilegovaných obslužných programů, které mohou být schopné potlačit systémové a aplikační opatření MUSÍ být omezeno a důsledně kontrolováno.

Implementační pokyny:

5.2.1 Použití privilegovaných obslužných programů MUSÍ být omezené na úzce vymezené okolnosti (např. upřesnění účelu, požadavek schválení, časového omezení).

5.2.2 Použití privilegovaných obslužných programů MUSÍ být omezené na omezený počet oprávněných osob.

5.2.3 Použití privilegovaných obslužných programů MUSÍ být zaznamenáno (logged). Záznamy BY MĚLY být pravidelně kontrolovány v krátkých intervalech, zda neobsahují podezřelé činnosti.

6 Řízení přístupu pro mimořádné situace

V mimořádných situacích (např. v případě havárie) MUSÍ být zajištěn nouzový administrační přístup.

Implementační pokyny:

6.1.1 Hesla k administrátorským účtům MOHOU být uschována v trezoru pro potřeby zastupitelnosti při havárii. Využití hesla MUSÍ být zaznamenáno.

6.1.2 Nouzové účty MOHOU být zřízeny pro přístup neprivilegovaných pověřených uživatelů k administrátorským účtům.

7 Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

7.1 Přezkoumání přístupových práv uživatelů

Dokumentace řízení přístupu MUSÍ podrobně analyzovat postupy v rámci pravidelných přezkoumání a pokud je to relevantní, tak i odstranění či úpravu přístupových práv (viz 4.3).

Implementační pokyny:

7.1.1 Pravidla kontroly přístupu MUSÍ zohledňovat příslušné právní, regulační a smluvní závazky.

7.1.2 Postupy využívané pro řízení přístupu MUSÍ být pravidelně přezkoumávány a upravovány v reakci na nové a rozvíjející se hrozby, možnosti, zranitelnosti, požadavky společnosti nebo zkušenosti s incidenty bezpečnosti informací.

7.1.3 MUSÍ být pravidelně přezkoumáno nastavení veškerých přístupových oprávnění včetně rozdělení do přístupových skupin a rolí.

7.1.4 Kontrola přístupových práv BY MĚLA být prováděna pro:

a) zajištění, že jsou přiřazená přístupová práva stále přiměřená při zvážení principů „potřeby vědět“/“potřeby využívat“ („need-to-know principle“/„need-to-use principle“),
b) kontrolu, zda mohou být nadbytečná přístupová práva odebrána.

7.1.5 Přiřazená přístupová práva, která již nejsou dále odpovídající potřebám společnosti, nebo jsou nadbytečná, MUSÍ být odebrána nebo upravena (viz 4.3).

7.1.6 Kontroly přístupových práv MOHOU být vykonány jednou nebo více osobami pověřenými vlastníkem aktiva.

Použité zdroje

(1) 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

(2) *MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD* [online]. Verze 1.0. NÚKIB, 2020 [cit. 2022-04-20]. Dostupné z: https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

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 při zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné při zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)

Příloha B: Politika hesel a PINů

Politika hesel

Požadavky na složitost	Uživatelské účty	Privilegované účty
Délka	Min 12 znaků	Min. 17 znaků
Požadavky na heslo	umožněno zadat heslo o délce alespoň 64 znaků, neomezeno použití malých a velkých písmen, číslic a speciálních znaků, heslo unikátní, dostatečně dlouhé a nedá se snadno uhodnout.	umožněno zadat heslo o délce alespoň 64 znaků, neomezeno použití malých a velkých písmen, číslic a speciálních znaků, a speciální znak heslo unikátní, dostatečně dlouhé a nedá se snadno uhodnout.
Dočasné heslo	bezodkladná změna výchozího hesla po jeho prvním použití	bezodkladná změna výchozího hesla po jeho prvním použití
Maximální doba platnosti	18 měsíců (nevztahuje se na účty sloužící k obnově systému v případě havárie) nebo v případě důvodného podezření na únik citlivých informací nebo v případě, že chce uživatel své původní heslo nahradit silnějším heslem	18 měsíců (nevztahuje se na účty sloužící k obnově systému v případě havárie) nebo v případě důvodného podezření na únik citlivých informací nebo v případě, že chce uživatel své původní heslo nahradit silnějším heslem
Minimální platnost hesla	30 minut	30 minut
Historie hesel	zákaz používaní stejného hesla (posledních 12 hesel)	zákaz používaní stejného hesla (posledních 12 hesel),
Uzamčení účtu uživatele	po 5 neplatných pokusech zadání hesla v řadě,	po 5 neúspěšných pokusech
Omezení	Hesla NESMÍ obsahovat: • nejčastěji používaná hesla, • přihlašovací jméno, e-mail, název systému a obdobně • opakované či sekvenční sady (třeba zzzz nebo abc456 • jména a/nebo data narození uživatele, jeho přátel či příbuzných; • kombinace obsahující aktuální rok, měsíc nebo roční období (např. Summer2018);	

V případě použití autentizace pouze účtem a heslem MUSÍ být zajištěno:

- bezodkladná změna výchozího hesla po jeho prvním použití,
- bezodkladné zneplatnění hesla sloužícího k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření a

Pravidla uvedená v tabulce je nutné chápat jako minimální doporučení a jejich implementace MŮŽE být přísnější

Nejvhodnějším heslem je náhodná zmodifikovaná fráze nebo náhodné seskupení slov, které si uživatel zapamatuje. Náhodné seskupení krátkých slov má vyšší entropii než slovo jediné.

Hesla MUSÍ být v takové formě, aby co nejvíce ztížila případný útok. Databáze případných získaných hesel BY MĚLA být správně zahešovaná.

Politika pro PINy

	jako jednofázové	**jako 2. fáze**
Minimální délka PINu	osm číslic	šest číslic
Maximální životnost PINu	v případě důvodného podezření na únik citlivých informací nebo v případě, že chce uživatel své původní heslo nahradit silnějším heslem	v případě důvodného podezření na únik citlivých informací nebo v případě, že chce uživatel své původní heslo nahradit silnějším heslem
Historie PINů	5	není k dispozici
Žádné jednoduché PINy	PINy BY NEMĚLY obsahovat: • Po sobě jdoucí číslice (např. 123456); • Opakující se číslice (např. 000000); • Data narození uživatele, jeho přátel či příbuzných.	
Počáteční PINy	Změna při prvním přihlášení (pokud je to technicky možné)	
Uzamčení uživatele	Po 5 neúspěšných pokusech	Po 3 neúspěšných pokusech

*Není definováno vyhláškou – možno upravit dle potřeb