10.2 Bezpečné chování uživatelů

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

- **Bezpečné nakládání s aktivy.**
- **Bezpečné použití přístupových hesel.**
- **Bezpečné použití elektronické pošty a přístupu na internet**
- **Bezpečný vzdálený přístup**
- **Bezpečné chování na sociálních sítích**
- **Bezpečnost ve vztahu k mobilním zařízením**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Bezpečnost lidských zdrojů (§ 9), Řízení přístupu (§ 12).

1 Pravidla pro bezpečné nakládání s aktivy

Cíl: Zajistit ochranu aktiv společnosti přístupných uživatelům.

1.1 Politika bezpečnosti informací pro nakládání s aktivy

Uživatelé MUSÍ být seznámeni s aktivy, s kterými přicházejí do styku.

Implementační pokyny:

1.1.1 Garanti jednotlivých aktiv MUSÍ zajistit informovanost uživatelů o daném aktivu, vysvětlit proces pořizování, zpracování a předávání dat v rámci daného aktiva. Uživatelé MUSÍ sdílet odpovídající povědomí o aktuálních rizicích daného/relevantního aktiva.

1.1.2 Uživatelé jednotlivých aktiv MUSÍ nahlásit garantovi aktiva případné technické neshody aktiva.

2 Bezpečné použití přístupového hesla

Cíl: Zajistit jednoznačnou identifikaci uživatelů v rámci daného aktiva – systému, tj. povolení a logování přístupu přes jednoznačnou autorizaci a autentizaci

2.1 Používání a monitorování a přístupových hesel

Společnost MUSÍ stanovit pravidla pro nastavení formálních požadavků na sílu hesla a délce platnosti v návaznosti na specifika daného aktiva (zejména požadavků na důvěrnost). Detailněji jsou pravidla a postupy definovány ve směrnici SM-7 Řízení přístupů.

Implementační pokyny:

2.1.1 Společnost MUSÍ vysvětlit a vynucovat používání adekvátní formu hesel pro:
   a) Uživatelský přístup,
   b) Privilegovaný přístup (role jako admin, root, sys).

2.1.2 Společnost MUSÍ v návaznosti na posouzení rizik, používat vícefaktorovou autentizaci. Například dvoufázové ověření, kdy se uživatel MUSÍ prokázat pomocí dvou faktorů (prvním je obvykle uživatelské jméno a heslo, druhým pak například PIN, otisk prstu, snímek sítnice oka, elektronický token a podobně).

2.1.3 Uživatel NESMÍ přihlašovací údaje, tokeny, PIN, certifikáty sdělovat ani umožňovat využívat jiným osobám.

2.1.4 Jakékoliv incidenty v souvislosti s vyzrazením nebo zneužitím hesel MUSÍ být neprodleně řešeny.

3 Bezpečné použití elektronické pošty a přístupu na internet

Společnost MUSÍ definovat pravidla pro užívání elektronické pošty a internetu.

3.1 Pravidla pro uživatele

3.1.1 Uživatel NESMÍ používat protokoly POP3 nebo IMAP.

3.1.2 Uživatel BY NEMĚL ke svým soukromým schránkám přistupovat za využití prostředků společnosti popřípadě pouze v rozumné míře.

3.1.3 Uživatel ke své schránce na serveru společnosti MŮŽE z Internetu přistupovat jen přes zabezpečené https spojení.

3.1.4 Uživatel při obdržení mailu z nedůvěryhodného zdroje NESMÍ otevírat email. MUSÍ jej zahodit nebo v případě pochybností požádat přes HelpDesk o kontrolu.

3.1.5 Uživatel NESMÍ používat tunelování jiných protokolů přes http protokol (Pozn. síťové tunelování je technika používaná v počítačových sítích, která pro přenos jednoho nebo více síťových spojení používá jiné síťové spojení. Umožňuje tak přenášet data přes nekompatibilní sítě, obcházet administrativní omezení určité sítě, poskytovat zabezpečenou komunikaci přes nezabezpečenou, resp. nedůvěryhodnou síť).

3.1.6 Uživatel BY MĚL, zejména při prvotní komunikaci, ověřovat identitu protistrany, tedy že osoba je skutečně tou, za kterou se vydává.

4 Bezpečný vzdálený přístup

Společnost MUSÍ definovat pravidla pro vzdálené připojení. Detailnější pravidla a postupy jsou definovány ve směrnici SM-12 Bezpečné používání mobilních zařízení.

4.1 Pravidla pro uživatele

4.1.1 Uživatel se MŮŽE vzdáleně připojit pomocí SSH při použití autentifikačních a autorizačních údajů.

4.1.2 Uživatel se MŮŽE vzdáleně připojit pomocí VPN při použití osobního certifikátu a hesla.

5 Bezpečnost ve vztahu k mobilním zařízením

Společnost MUSÍ definovat pravidla a postupy pro používání mobilních zařízení a dalších elektronických zařízení. Detailnější pravidla a postupy jsou definovány ve směrnici SM-12 Bezpečné používání mobilních zařízení.

5.1 Pravidla pro uživatele

5.1.1 Uživatel MUSÍ zadávat přístupové údaje tak, aby je okolí nemohlo zjistit/vysledovat, preferovaný způsob může být použití otisku prstu nebo skenu obličeje.

5.1.2 Uživatel MUSÍ provádět/umožnit provedení aktualizací zařízení a programů.

5.1.3 Uživatel BY MĚL používat šifrování dat na interních i externích zařízeních.

5.1.4 Uživatel BY NEMĚL používat veřejné Wifi přístupové body.

5.1.5 Uživatel BY MĚL věnovat zvýšenou pozornost při použití i jiných bezdrátových technologií jako Bluetooth, NFC. Zapínat tyto technologie jen pokud je potřeba.

6 Bezpečné chování na sociálních sítích

Společnost MUSÍ definovat pravidla a postupy pro chování na sociálních sítích, pokud je využívá.

5.2 Pravidla pro uživatele

5.2.1 Uživatel BY MĚL mít nastavené silné heslo.

5.2.2 Uživatel BY MĚL nastavit a používat dvoufázové ověření.

5.2.3 Uživatel BY NEMĚL veřejně uvádět své telefonní číslo a adresu.

5.2.4 Uživatel BY MĚL ověřovat důvěryhodnost informací na sociálních sítích.

5.2.5 Uživatel NESMÍ sdílet jiné interní informace, než ty označené jako „veřejné“.

5.2.6 Uživatel BY NEMĚL sdílet citlivé informace, fotografie,..

5.2.7 Uživatel BY MĚL využívat možnosti v nastavení „soukromí“.

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) ČSN EN ISO/IEC 27002 (369798) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací. Technická normalizační komise, 2014.

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)