10.3 Bezpečné používání mobilních zařízení

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

- **Požadavky na zabezpečení mobilních zařízení.**
- **Pravidla a postupy používání mobilních zařízení.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti (VKB) – Řízení přístupu (§ 12), Ochrana před škodlivým kódem (§ 21), Detekce kybernetických bezpečnostních událostí (§ 23).

1 Pravidla a postupy pro bezpečné používání mobilních zařízení

Cíl: Zajistit bezpečnost mobilních zařízení společnosti, která jsou využívána mimo pracoviště.

1.1 Požadavky na mobilní zařízení

Provozní postupy MUSÍ stanovit pravidla pro používání mobilních zařízení na základě analýzy rizik (AR) pro jednotlivá aktiva, u který je předpoklad práce na dálku.

Implementační pokyny:

1.1.1 U každého mobilního zařízení se MUSÍ dodržovat postupy pro zabezpečení dat (viz SM-7 Řízení přístupu, SM-8 Bezpečné chovaní uživatelů).

1.1.2 Na základě směrnice SM-7 Řízení přístupu se MUSÍ aplikovat definovaná 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.

1.1.3 Společnost MUSÍ stanovit jasnou strategii práce na dálku, která BY MĚLA zahrnovat jasné pokyny pro přístup k podnikovým zdrojům.

1.1.4 Společnost MUSÍ stanovit způsob, kterým budou zaměstnanci hlásit problémy s mobilními zařízeními.

1.1.5 Při používání mobilních zařízení BY MĚLA být věnována zvláštní pozornost tomu, aby nebyly kompromitovány informace týkající se činnosti společnosti, provozní postupy MUSÍ brát v úvahu rizika práce v nechráněných prostředích.

1.1.6 Každé mobilní zařízení (mobilní telefon, notebook, tablet…) MUSÍ být registrováno.

1.1.7 Na mobilním zařízení MUSÍ být nastaveno:

1.1.8 šifrování disku

1.1.9 vypínání/odhlašování se při nečinnosti (zámek obrazovky)

1.1.10 MUSÍ být nastaven pravidla využívání vyměnitelných médií (např. USB disk). Mobilní zařízení MUSÍ disponovat nástroji pro ověřování, řízení a šifrování vyměnitelných médií.

1.1.11 Mobilní zařízení MUSÍ být fyzicky chráněno proti krádeži.

1.1.12 U počítačových systému MUSÍ být zajištěno zálohování, využíván firewall a MUSÍ být omezena instalace softwaru.

1.1.13 MUSÍ být zajištěno použití nástroje pro nepřetržitou automatickou ochranu před škodlivým kódem s ohledem na důležitost aktiv. Nástroj MUSÍ být pravidelně aktualizován.

1.1.14 MUSÍ být zajištěna detekce kybernetického bezpečnostního incidentu přiměřeně s ohledem na důležitost aktiv. Společnost MUSÍ stanovit, jak postupovat vyskytne-li se bezpečnostní událost.

1.1.15 MĚLO BY být zajištěno komplexní zabezpečení mobilních koncových zařízení (Endpoint security).

1.1.16 Do podnikové sítě se zaměstnanci MUSÍ připojovat pouze s využitím podnikové VPN. K připojení MUSÍ být využito dvoufaktorové ověření. MUSÍ být stanovena doba nečinnosti, po které se VPN připojení přeruší.

1.1.17 Operační systém a všechny aplikace na mobilních zařízeních MUSÍ být pravidelně aktualizovány.

1.1.18 Přístup k podnikové elektronické poště MUSÍ být povolen pouze při použití dvoufaktorového ověření.

1.1.19 Společnost MUSÍ pravidelně informovat zaměstnance o rizicích práce na dálku zejména pak o kybernetických hrozbách jako je sociální inženýrství a phishing.

1.1.20 Na mobilních zařízeních MUSÍ být nastaveny silná hesla. MĚL BY být využit nástroj na správu hesel.

1.1.21 Mobilní zařízení určené k práci na dálku NESMÍ být využívána k osobním účelům.

1.1.22 MUSÍ být nastaven proces pro znemožnění přístupu k zařízení, které se ztratilo nebo bylo odcizeno. Tam, kde je to možné BY MĚL být nainstalován software, který v případě ztráty či zcizení, umožní mobilní zařízení nalézt, popřípadě z něj alespoň vymazat citlivá data společnosti, která by mohla být kompromitována.

2 Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě

Cíl: Zajištění bezpečnosti soukromých mobilních zařízení, kterými se zaměstnanci připojují do počítačové sítě společnosti.

2.1 Požadavky na mobilní zařízení

2.1.1 Umožňuje-li společnost využívat počítačovou síť k přístupu na Internet zařízením, které nemá ve své správě (ve správě zaměstnanců nebo návštěvníků) MUSÍ být oddělena od zbytku počítačové sítě.

2.1.2 Umožňuje-li společnost zaměstnancům používat zařízení v režimu BYOD (Bring Your Own Device), tedy vlastní zařízení zaměstnanců využívaná k plnění pracovních povinností (např. vyřizování pošty na mobilním telefonu), pak platí následující postupy:

2.1.3 Společnost MUSÍ jasně stanovit pravidla a postupy pro zaměstnance využívající BYOD.

2.1.4 Na zařízení BYOD BY MĚL být nastaven zámek obrazovky.

2.1.5 Na základě směrnice řízení přístupu (viz SM-7 Řízení přístupu) se MUSÍ aplikovat definovaná 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.

2.1.6 Umožňuje-li to zařízení, MUSÍ být zajištěno použití nástroje pro nepřetržitou automatickou ochranu před škodlivým kódem s ohledem na důležitost aktiv. Nástroj MUSÍ být pravidelně aktualizován.

2.1.7 Do podnikové sítě se zaměstnanci MUSÍ připojovat pouze přes zabezpečený VPN server schválený společností.

2.1.8 Operační systém a aplikace na mobilních zařízeních ýt pravidelně aktualizovány.

2.1.9 MĚL BY být definován seznam aplikací a dat, ke kterým mohou zaměstnanci ze soukromých zařízení v rámci podnikové sítě přistupovat.

2.1.10 Společnost MŮŽE stanovit povinnost instalace softwaru, který umožní vymáhání pravidel a politik na BYOD zařízení.

2.1.11 Společnost MŮŽE využít na BYOD zařízení kontejnerizaci oddělující osobní data od podnikových.

2.1.12 Tam, kde je to možné BY MĚL být nainstalován software, který v případě ztráty či zcizení umožní mobilní zařízení nalézt, popřípadě z něj alespoň vymazat citlivá data společnosti, která by mohla být kompromitována.

2.1.13 Zaměstnancům MUSÍ být stanovena povinnost smazat veškerá data společnosti po ukončení pracovního poměru.

2.1.14 Společnost MŮŽE pro spravování firemních i osobních zařízení využít nástroje Mobile Device Management (MDM), který MŮŽE obsahovat například tyto funkcionality: konfiguraci mobilních zařízení, zálohu dat, obnovu dat, distribuci aktualizací operačního systému a aplikací, monitoring zařízení apod.

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

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)