TECHNICKÉ PODMÍNKY A BEZPEČNOSTNÍ USTANOVENÍ PRO PROVOZOVÁNÍ PRACOVIŠTĚ AGENTA

Článek 1
Instalační podmínky

(1) Agent musí uzavřít s ČNB dohodu o přístupu přes komunikační bránu ČNB. Informace o kontaktních osobách v ČNB sděluje provozovatel.

(2) Pracovní stanice (článek 2) musí mít LAN konektivitu na router určený pro spojení s ČNB.

(3) Pracovní stanice musí mít přidělenou jedinečnou registrovanou IP adresu ze segmentu IP adres uvedených v dohodě o přístupu přes komunikační bránu ČNB.

(4) Pracoviště agenta (dále jen „pracoviště“) může být umístěno v běžném kancelářském prostředí.

(5) Napojení na ČNB zajistí agent na své náklady.

Článek 2
Technické a programové vybavení

(1) Technické a programové vybavení pracoviště je tvořeno následujícími prostředky

a) Technické prostředky:
   - Pracovní stanice typu PC s parametry umožňujícími bezproblémové provozování programového vybavení v konfiguraci popsané v bodě b)
   - LAN karta min. 10 Mb/s

b) Programové prostředky:
   - Operační systém: podporovaná a aktualizovaná verze Windows 8 nebo 10
   - Prohlížeč MS Internet Explorer verze 11 (do ukončení jeho podpory firmou Microsoft), prohlížeč MS Edge nebo prohlížeč Google Chrome aktuální podporované verze
   - Sun Java Plug-in verze 1.8, konkrétní číslo verze vždy podle informace uvedené na stránkách aplikace SKD v sekci Instalace a technické požadavky

c) Datový spoj minimálně 512 kb/s na jednu pracovní stanici

(2) Agent může po dohodě s ČNB použít jiné technické vybavení s obdobnými parametry.

Článek 3
Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

(1) Agenti při detekci kybernetických bezpečnostních událostí zajistí detekci těchto událostí přiměřeně s ohledem na důležitost aktiv v rámci koncových stanic, mobilních zařízení, serverů, datových uložišť a výměnných datových nosičů aj.[1].

[1] § 23 odst. 2 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)

(2) V případě faktického vzniku kybernetického bezpečnostního incidentu či podezřelého chování informačního systému SKD je agent povinen neprodleně hlásit tuto skutečnost provozovateli SKD[2].

(3) Důležité dokumenty jsou záznamy komunikace s klientem, např. soubory s e-maily, stručný zápis důležitých telefonních hovorů a další informace, které agent považuje za důležité. U všech záznamů musí být uvedeno datum a alespoň přibližný čas, kdy se popisovaná událost uskutečnila. Možné dokumenty, které se týkají podezření na incident, jsou výpis inkriminovaných záznamů z logu nebo výpis podezřelých chování aplikace.

(4) Dokumenty související s kybernetickým incidentem agenti bezodkladně předávají ČNB či dalším orgánům. Po prověření nebo vyřešení kybernetické události či incidentu jsou dokumenty odstraněny, přepsány či fyzicky zlikvidovány dle přílohy č. 4 vyhlášky č. 82/2018[3].

Článek 4
Bezpečnostní ustanovení

(1) Pracoviště mohou obsluhovat pouze osoby, které jsou evidovány v SKD jako pracovníci agenta [Pravidla SKD §6, odst. (1)].

(2) Pokud agent připojí pracovní stanice ke své lokální počítačové síti nebo k jinému systému nebo pokud agent provede na těchto pracovních stanicích instalaci dalších programových produktů, odpovídá za veškeré chyby při provozu programových prostředků.

(3) Povinnosti agenta

a) zabránit přístupu třetích osob k privátním klíčům certifikátů uživatelů systému SKD,

b) zajistit adekvátní úroveň zabezpečení klientských počítačů pracovníků systému SKD, zejména prostředky firewallů, antivirového, antispamového softwaru, systematickým vyhledáváním známých zranitelností, aktualizací operačního systému a instalovaných aplikací a dále omezením přístupu klientských stanic k adresám s nebezpečným obsahem v Internetu,

c) zajistit systémovou a fyzickou ochranu privátních klíčů pracovníků systému SKD, např. pořízením tokenů nebo čipových karet s bezpečným úložištěm pro privátní klíče a certifikáty.

(4) Povinnosti pracovníka agenta

a) důsledně chránit privátní klíč certifikátu pro vytváření elektronického podpisu před přístupem jiné osoby, než které byl certifikační autoritou vydán,

b) zajistit systémovou a fyzickou ochranu privátního klíče certifikátu pro vytváření elektronického podpisu nejlépe technickými prostředky (token, čipová karta) na principu „potřeby mít a znát“ nebo alespoň nastavením vysoké úrovně zabezpečení, tj. s přístupem pouze přes silná hesla, při uložení klíčů do zabezpečeného softwarového úložiště na klientské stanici a v neexportovatelném tvaru,

c) pracovní stanici chránit prostředky antivirové ochrany, firewally a dalšími prostředky pro ochranu před škodlivým softwarem, zejména viry, trojskými koni, spamem, spyware apod.

d) zajistit pravidelné aktualizace a opravy softwaru, především operačního systému, prohlížeče webových stránek a dalších instalovaných aplikací,

[2] § 8 odst. 6 zákon č. 181/2014 Sb., o kybernetické bezpečnosti

[3] Příl. 4 – Likvidace dat - 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)

e) přihlášení pracovníka k operačnímu systému realizovat pomocí standardního uživatelského účtu bez administrátorského oprávnění, a dostatečně složitého hesla, resp. na základě jiného mechanismu s odpovídající nebo vyšší úrovní bezpečnosti,

f) vhodnými prostředky bránit neoprávněným osobám v užívání počítače a zejména aplikace SKD, např. odhlášením nebo alespoň uzamčením počítače v době nepřítomnosti,

g) nereagovat na výzvy k poskytnutí přihlašovacích údajů třetími osobami (spam, phishing), přihlašovací údaje jsou určeny pouze danému uživateli a provozovatel je nikdy po uživatelích za žádných okolností nepožaduje.

h) v případě podezření na zneužití certifikátu bezodkladně zajistit odvolání platnosti kvalifikovaného certifikátu pro elektronický podpis u příslušné certifikační autority, ihned ukončit platnost registrace podpisového certifikátu v systému SKD, a toto neprodleně oznámit provozovateli, sekci řízení rizik a podpory obchodů.

Kontakt: skd@cnb.cz, tel.:+420 224 418 019.

Článek 5
Servisní podmínky

Údržba technického vybavení pracoviště je zajišťována agentem nebo jeho servisní firmou.

Článek 6
Rozšíření pracoviště

Na pracovišti agenta může současně pracovat více pracovních stanic za předpokladu, že každá pracovní stanice má vlastní registrovanou IP adresu.