10.10 Řízení provozu a komunikací

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

- **Pravomoci a odpovědnosti spojené s bezpečným provozem**
- **Postupy bezpečného provozu.**
- **Požadavky a standardy bezpečného provozu.**
- **Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Řízení provozu a komunikací (§ 10).

---

1 Pravomoci a odpovědnosti spojené s bezpečným provozem

Cíl: Zajistit bezpečný provoz a komunikaci informačního a komunikačního systému, minimalizovat riziko selhání systému, ochrana integrity a dostupnosti softwarového vybavení, ochrana důvěrnosti informací a zajištění ochrany počítačových sítí.

1.1 Práva a povinnosti administrátorů, uživatelů a osob zastávajících bezpečnostní role

Společnost MUSÍ delegovat práva a povinnosti dotčených osob.

Implementační pokyny:

1.1.1 Za řízení bezpečného provozu odpovídá vedoucí ustavených útvarů IT.

1.1.2 Za bezpečnost provozu a za řízení kybernetické bezpečnosti odpovídá manažer kybernetické bezpečnosti (MKB).

1.1.3 Práva a povinnosti administrátorů:

- Administrátoři BY MĚLI mít uzavřenou dohodu o zachování mlčenlivosti buď přímo ve formě smlouvy (NDA) nebo doložky k pracovní smlouvě.
- Administrátoři MUSÍ být poučeni o jejich povinnostech a seznámeni s platnými bezpečnostními politikami.
- Viz SM-5 Bezpečnost lidských zdrojů.

1.1.4 Práva a povinnosti uživatelů:

- Uživatelé MUSÍ být poučeni o jejich povinnostech a seznámeni s platnými bezpečnostními politikami včetně kontroly jejich dodržování.
- Uživatelé 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 by měli být seznámeni se způsobem, jak tyto neobvyklé situace hlásit
- Viz Bezpečné chování uživatelů.

1.1.5 Práva a povinnosti osob zastávajících bezpečnostní role:

- Osoby zastávající bezpečnostní role BY MĚLY mít uzavřenou dohodu o zachování mlčenlivosti buď přímo ve formě smlouvy (NDA) nebo doložky k pracovní smlouvě.
- Osoby 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
- Viz Bezpečnost lidských zdrojů.

2 Postupy bezpečného provozu

MUSÍ být nastaveny adekvátní postupy, které by neměly za následek negativní dopad na řízení provozu a komunikací.

Implementační pokyny:

2.1.1 Pracovní postupy MUSÍ být dostupné všem dotčeným osobám.

2.1.2 Spuštění chodu systému:

- Za stanovení postupu je odpovědný garant aktiva
- Při posuzování dopadu změny MUSÍ být zvažována všechna rizika související se zranitelnostmi systému (Zero Day zranitelnost) a možnými kybernetickými útoky.

2.1.3 Ukončení chodu systému:

- Za stanovení postupu je odpovědný garant aktiva, které je dotčeno iniciačním požadavkem na ukončení chodu.

2.1.4 Restart nebo obnovení chodu systému po selhání:

- Při restartu nebo obnovení chodu systému MUSÍ být ošetřeny chybové stavy nebo mimořádné jevy.
- Viz Řízení kontinuity činnosti.

2.1.5 Postupy pro sledování kybernetických bezpečnostních událostí:

- MUSÍ být zavedena opatření pro ochranu přístupu k záznamům o událostech (ochrana logů).
- Viz Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.

2.1.6 Pravidla a postupy pro ochranu před škodlivým kódem:

- Viz Bezpečné chování uživatelů
- Viz Ochrana před škodlivým kódem

2.1.7 Řízení technických zranitelností

- Viz Řízení technických zranitelností

2.1.8 Spojení na kontaktní osoby, které jsou pověřeny výkonem systémové a technické podpory:

- MUSÍ být zaveden systém kontaktů na pověřené osoby
- MUSÍ být zajištěno řádné seznámení uživatelů s tímto systémem

2.1.9 Postupy řízení a schvalování provozních změn:

- Viz Řízení změn

2.1.10 Postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů:

- Viz Bezpečnost lidských zdrojů.
- Technické zdroje se řídí dokumenty pro oblast ICT nebo ICS (Industrial Control System, průmyslové řídící systémy) v souladu s bezpečnostní strategií společnosti.

2.1.11 Pravidla a postupy pro ochranu informací a dat v průběhu celého životního cyklu:

- Viz Ochrana osobních údajů.

2.1.12 Pravidla a postupy pro instalaci technických aktiv:

- MUSÍ být zavedeny pravidla pro nasazení technických aktiv včetně způsobu pořízení a vyhodnocování provozních záznamů během celého životního cyklu aktiva.

2.1.13 Provádění pravidelného zálohování a kontroly použitelnosti provedených záloh:

- Viz Zálohování a archivace.

2.1.14 Pravidla a postupy pro zajištění bezpečnosti síťových služeb:

- Používané síťové služby MUSÍ být zdokumentovány a schváleny
- Za správné používání síťových služeb je odpovědný příslušný správce sítě a MKB.

2.2 Aktualizace provozních pravidel

Uživatelé MUSÍ být seznámeni se změnami pracovních postupů a s možnými dopady. Společnost BY MĚLA vhodnou formou vysvětlit výsledky přezkoumání možných dopadů případných změn.

Implementační pokyny:

2.2.1 Pracovní postupy MUSÍ podléhat pravidelným revizím a jejich změna MUSÍ probíhat prostřednictvím změnového řízení.

2.3 Zajištění oddělení vývojového, testovacího a provozního prostředí

Společnost MUSÍ zajistit oddělení prostředí s rozdílnou úrovní požadavků na kybernetickou bezpečnost.

Implementační pokyny:

2.3.1 Společnost MUSÍ zabezpečit, aby nedošlo k instalaci a provozu softwarového vybavení, které nebylo schváleno k provozu v produkčním systému.

2.3.2 Veškeré zkoušení a testování softwarové vybavení, včetně provozního firmwaru zařízení MUSÍ probíhat pouze na testovacím systému.

3 Požadavky a standardy bezpečného provozu

Společnost MUSÍ zajistit plnění všech patných legislativních i smluvních požadavků na zajištění kybernetické bezpečnosti.

Implementační pokyny:

3.1.1 Společnost MUSÍ zabezpečit, aby všechny platné legislativní i smluvní požadavky na zajištění bezpečnosti informací byly dokumentovány a aktivně využívány při tvorbě interních předpisů, souvisejících s provozem informačního systému.

3.1.2 Všechny řídicí dokumenty v oblasti bezpečnosti provozu MUSÍ být podřízeny jednotné formě řízení dokumentace.

3.1.3 Řízení dokumentace MUSÍ jednoznačně určit správce každého dokumentu (platnost dokumentu, strukturu dokumentu, osoby a útvary, podílející se na schválení dokumentu a pravidla pro manipulaci s dokumentem).

4 Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů

Společnost MUSÍ zajistit pravidla pro provádění auditů kybernetické bezpečnosti.

Implementační pokyny:

4.1.1 Společnost MUSÍ v souladu se směrnicí SM-3 Organizační bezpečnost určit osobu auditora kybernetické bezpečnosti.

4.1.2 Audity a bezpečnostní testy MUSÍ být plánovány v souladu s provozními možnostmi všech dotčených systémů tak, aby nedošlo, je-li to možné, k ohrožení provozu jak z pohledu jeho kontinuity a stanovených SLA (Service-Level Agreement), tak z pohledu bezpečnosti.

4.1.3 O provádění auditu MUSÍ být informováni s dostatečným předstihem všichni dotčení pracovníci zajišťující provozní podporu dotčených systémů a s prováděním auditu musí vyslovit souhlas MKB.

4.1.4 Audit kybernetické bezpečnosti a provozní testy NESMÍ být prováděny v době, kdy probíhá bezpečnostní incident, případně kdy jsou aplikována neodkladná opatření ke zmírnění dopadů technických zranitelností

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 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)