10.5 Fyzická bezpečnost

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

- **Ochranu objektů společnosti.**
- **Prevenci neoprávněného fyzického přístupu k informacím společnosti.**
- **Prevenci neoprávněného fyzického přístupu poškození a ovlivnění zařízení pro zpracování informací.**
- **Zabránění ztrátě, poškození, krádeže nebo narušení IT/OT aktiv a souvisejícímu přerušení provozu společnosti.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Fyzická bezpečnost (§ 17).

1 Pravidla pro ochranu objektů

CÍL: Zajištění ochrany pro zajištění ochrany na úrovni objektů a v rámci objektů společnosti. Předcházení poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému.

1.1 Fyzický bezpečnostní perimetr

Společnost MUSÍ stanovit fyzický bezpečnostní perimetr ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému. Tuto oblast je nutné chránit a zabezpečit před neoprávněným vstupem a poškozením, krádeží či zneužitím. MUSÍ být zajištěna ochrana kritických míst v rámci objektů (např. serverovny, kanceláře zaměstnanců, technologické místnosti), ale také objektů samotných. Pro přehlednost bude pro tato kritická místa zaveden pojem tzv. bezpečné oblasti.

Implementační pokyny:

1.1.1 Úroveň zabezpečení každého definovaného perimetru BY MĚLA být závislá na bezpečnostních požadavcích aktiv v rámci perimetru a na výsledcích posouzení rizik.

1.1.2 MUSÍ být uplatněny prostředky fyzické bezpečnosti pro zajištění zvýšené bezpečnosti vymezených prostor (bezpečné oblasti), ve kterých jsou umístěna technická aktiva informačního systému kritické informační infrastruktury.

1.1.3 Součásti ochrany fyzického bezpečnostního perimetru MUSÍ být opatření obsahující:

a) vymezení vnější hranice, například plotů a/nebo zdí,

b) zabezpečení otevřených prostor, například: monitorování celého prostoru kamerovým systémem, bezpečnostními pracovníky, systémy detekce vniknutí,

c) identifikaci osob a/nebo vozidel, vstup a pohyb v rámci objektu pouze po předchozí identifikaci např. pomocí čipové karty, resp. možnost nastavení různých oblastí, do kterých mají přístup pouze omezené skupiny zaměstnanců, zamykání dveří a prostor

1.1.4 Perimetr budovy nebo místa s vybavením pro zapracování informací BY MĚLY být fyzicky v pořádku (tj. perimetr by neměl být nikde přerušen nebo by v něm neměla být místa, kudy lze snadno

proniknout),

1.1.5 Všechny požární dveře v bezpečnostním perimetru BY MĚLY být chráněny alarmem, monitorovány a testovány. MUSÍ fungovat v souladu s místními požárními předpisy způsobem zabezpečeným proti selhání.

1.1.6 Vybavení pro zpracování informací spravované společností BY MĚLO být odděleno od vybavení spravované externími stranami.

1.1.7 Kancelářské budovy a provozní prostory BY MĚLY být rozděleny do zón s odlišnými úrovněmi zabezpečení (princip „cibule“, tzn. vnější prostor, kontrolovaná vstupní oblast, vnitřní oblast a bezpečná oblast) dle normy *ČSN P 734450-1 Fyzická ochrana prvku KI – část 1: Obecné požadavky* (1).

1.1.8 Zóny pohybu návštěvníků BY MĚLY být fyzicky oddělené od vnitřních oblastí a bezpečných oblastí.

1.1.9 Přechod do zóny s vyšší úrovní zabezpečení BY MĚL být zabezpečen prvky fyzické kontroly vstupu (viz. bod 2).

1.1.10 Informace o umístění a využití bezpečných oblastí BY NEMĚLY být veřejně dostupné.

2 Pravidla pro kontrolu vstupu osob

Fyzický přístup do bezpečných oblastí MUSÍ být omezen pouze na oprávněné osoby.

Implementační pokyny:

2.1.1 Vstup do bezpečných oblastí MUSÍ být kontrolován a povolen pouze oprávněným osobám.

2.1.2 Pro fyzické bezpečnostní perimetry platí následující pravidla a postupy:

a) MUSÍ být stanoveny postupy pro zaměstnance na základě kterých jsou oprávněni k přístupu do bezpečných oblastí,

b) MUSÍ být jasně definována pravidla pro návštěvy a třetí strany, jako je např.: vstup pouze s doprovodem, identifikace návštěvy při vstupu do objektu apod.

b) MUSÍ být stanoveny autorizační postupy platné pro osoby s přístupem do bezpečných oblastí a pokud to je možné, omezen fyzický přístup do bezpečných oblastí na základě pravidel „potřeba vědět“ (Need-to-know) a „oprávněná potřeba“ (Need-to-use),

c) MĚLA BY být pravidelně přezkoumávána práva pro fyzický přístup přidělený bezpečným oblastem, a v případě potřeby je okamžitě aktualizovat či odebrat,

d) identity osob MUSÍ být prověřeny předtím, než je jim povolen přístup do bezpečných oblastí,

e) MĚL BY být udržován a monitorován auditní záznam, dokumentující dobu, kdy osoba do bezpečných oblastí vstupuje a kdy je opouští

f) MĚLO BY být zavedeno nošení nějaké formy viditelné identifikace před vstupem do bezpečných oblastí,

g) MUSÍ být odebrány klíče, přístupové karty nebo podobné prostředky po ukončení činnosti v bezpečných oblastí.

2.1.3 Postupy kontroly vstupu do bezpečných oblastí MUSÍ být pravidelně kontrolovány pro ověření jejich efektivity.

2.2 Zabezpečení kanceláří, místností a zařízení

MUSÍ být navržena a zavedena fyzická bezpečnost pro kanceláře, místnosti a zařízení, které jsou součástí bezpečných oblasti.

Implementační pokyny:

2.2.1 MĚLY BY být navržena a zavedena fyzická bezpečnost na základě plánovaného nebo aktuálního využití kancelářských budov, místností a provozních zařízení za účelem ochrany osob zde pracujících a zařízení zde umístěného, což zahrnuje přinejmenším požadavky týkající se:

a) architektonické/stavební bezpečnosti,
b) kabeláže,
c) elektřiny/zdrojů energií,
d) ochrany před požárem/bleskem,
e) topení, větrání a klimatizace (HVAC),
f) detekce vniknutí,
g) kontrol fyzického přístupu.

2.3 Ochrana před vnějšími a přírodními hrozbami

Pro budovy, v nichž se nacházejí bezpečné oblasti, BY MĚLA být navržena, aplikována a udržována opatření na ochranu před přírodními hrozbami (např. bouře, povodně, zemětřesení) a před hrozbami lidského původu (např. požár, výbuch, škody způsobené událostmi v blízkém okolí).

Implementační pokyny:

2.3.1 Potenciální události ohrožení budovy/majetku BY MĚLY být identifikovány, dokumentovány a přezkoumány/aktualizovány.

2.3.2 Rizikové scénáře, vyplývající z identifikovaných událostí ohrožení BY MĚLY být určeny a zdokumentovány, a rizika BY MĚLA být posouzena, ohodnocena, adekvátně spravována, komunikována, monitorována a přezkoumávána.

2.3.3 Dopad vyplývající z přírodních nebo člověkem způsobených hrozeb BY MĚL být minimalizován v ekonomicky přijatelném rozsahu.

2.3.4 Návrh a provozní efektivita kontrol/opatření na ochranu před přírodními a člověkem způsobenými hrozbami BY MĚLY být pravidelně testovány.

2.4 Práce v bezpečných oblastech

Postupy pro práci v bezpečných oblastech MUSÍ být zavedeny a školeny.

Implementační pokyny:

2.4.1 Bezpečné oblasti BY MĚLY být identifikovatelné jen zevnitř.

2.4.2 Pravidla chování při práci v bezpečných oblastech (zahrnující všechny činnosti, které jsou v

bezpečné oblasti vykonávány) MUSÍ být definovány, zdokumentovány a komunikovány pravidelně a srozumitelně všem osobám, pracujících v bezpečných oblastech.

2.4.3 Pokud není stanoveno jinak, použití nahrávacích zařízení (fotoaparátů, video, audio) BY MĚLO být zakázáno.

2.4.4 Práci bez dozoru v bezpečných oblastech BY MĚLO být předcházeno z bezpečnostních důvodů a také za účelem předcházení příležitostem ke škodlivým činnostem.

2.4.5 Třetí strany a návštěvníci BY MĚLI být v bezpečných oblastech nepřetržitě doprovázeni interními zaměstnanci.

2.5 Oblasti pro nakládku a vykládku

Oblasti pro nakládku a vykládku a další veřejné přístupové body, kde by mohly do prostoru/budovy vstoupit neoprávněné osoby, BY MĚLY být odděleny od bezpečných oblastí pro zamezení neoprávněného přístupu.

Implementační pokyny:

2.5.1 Oblasti pro nakládku a vykládku BY MĚLY být takto označené.

2.5.2 Oblasti pro nakládku a vykládku BY MĚLY být navrženy tak, aby bylo možno materiál nakládat a/nebo vykládat bez možného nebo nezbytného přístupu do dalších částí budovy nebo oblastí.

2.5.3 Fyzický přístup do oblasti nakládky a vykládky zvenčí MUSÍ být omezený pouze na identifikované a oprávněné osoby.

2.5.4 Oblasti pro nakládku a vykládku BY MĚLY být nepřetržitě pod dohledem.

3 Pravidla pro ochranu zařízení

Zařízení informačního a komunikačního systému MUSÍ být umístěno tak, aby bylo chráněno před riziky přirozených hrozeb a proti neoprávněnému přístupu, ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace.

Implementační pokyny:

3.1.1 Komponenty IT infrastruktury (např. servery, síťové komponenty) BY MĚLY být provozovány v datových centrech, počítačových místnostech a/nebo uzamykatelných serverových skříních, do kterých mají přístup pouze oprávněné osoby a na které se vztahují (pokud je to relevantní) požadavky definované v oddílech 2.3, 2.4, 2.5, aby byla zajištěna odpovídající ochrana proti hrozbám prostředí a krádeží, zničení a manipulaci.

3.1.2 Komponenty IT infrastruktury BY MĚLY být odpovídajícím způsobem prostorově odděleny od systémů či komponent používaných pro zálohování jejich dat (např. záložní servery v oddělených protipožárních skříních).

3.1.3 Komponenty IT infrastruktury BY MĚLY být schopny pracovat v zamýšleném prostředí v souladu se specifikacemi výrobce (např. splnit požadavky na vlhkost, teplotu, prašnost, elektromagnetické záření, napájení, přepěťovou ochranu, zabránění zbytečným rizikům požárů atd.).

3.1.4 Pro komponenty průmyslových, řídicích a obdobných specifických systémů MUSÍ být použity nástroje a opatření, které zajistí omezení fyzického přístupu k zařízením těchto systémů a ke komunikační síti. Komunikační sít určená pro tyto systémy MUSÍ být vyčleněna od ostatní

infrastruktury.

3.2 Podpůrné služby

Komponenty IT infrastruktury s (velmi) vysokými nároky na dostupnost MUSÍ být chráněny před výpadky napájení a dalšími narušeními, které by mohly být způsobeny selháním podpůrných služeb.

Implementační pokyny:

3.2.1 Podpůrné služby MUSÍ být automaticky monitorovány a v případě poruchy musí být okamžitě upozorněn zodpovědný personál.

3.2.2 Podpůrné služby včetně případných existujících systémů záložních zdrojů energie (UPS) MUSÍ být pravidelně udržovány a testovány v intervalech údržby stanovených výrobcem. Kontroly a údržba MUSÍ být zaznamenávány.

3.2.3 V případě komponent infrastruktury nutných pro dosažení kritických cílů BY MĚL být zvážen záložní zdroj napájení (UPS, DG) s dostatečnými parametry, aby byla zajištěna dodávka energie všem připojeným komponentám i v případě výpadku napájení, a to na tak dlouho, aby nedošlo ke ztrátě dat.

3.2.4 IT infrastruktura s (velmi) vysokými požadavky na dostupnost BY MĚLA být napájena ze dvou nezávislých elektrických okruhů.

3.2.5 Ochrana a návrh obvodů BY MĚLY být pravidelně revidovány.

3.2.6 Nouzové vypínače napájení BY MĚLY být chráněny nebo instalovány tak, aby nemohly být aktivovány neúmyslně.

3.2.7 Inženýrské sítě (např. vodovod, plynovod, odpady) BY SE NEMĚLY nalézat v blízkosti komponent IT a infrastruktury s vysokými požadavky na ochranu. Pokud se tomu nelze vyhnout, MUSÍ být inženýrské sítě v kritických místech pravidelně kontrolovány na netěsnosti.

3.2.8 Aktuální plány umístění všech rozvodů inženýrských sítí BY MĚLY být k dispozici a uloženy tak, aby k nim mohly v případě potřeby rychle přistupovat pouze oprávněné osoby.

3.3 Bezpečnost kabelových rozvodů

Napájecí a telekomunikační kabely používané pro přenos dat nebo podpůrných informačních služeb BY MĚLY být chráněny před odposlechem, rušením či poškozením.

Implementační pokyny:

3.3.1 Pro ochranu před odposlechem MUSÍ být, pokud je to relevantní, implementovány požadavky definované ve směrnici SM-20 Bezpečné používání kryptografické ochrany, týkající se použití odpovídajících šifrovacích algoritmů s dostatečnou délkou klíče a kryptografickou silou.

3.3.2 Výběr, instalace a údržba napájecích a telekomunikačních kabelů BY MĚLA odpovídat standardům a nařízením.

3.3.3 Při instalaci napájecích a telekomunikačních kabelů BY MĚLY být zváženy přirozené faktory prostředí (např. teplota, kabelové schránky, možné zdroje rušení či poškození).

3.3.4 Napájecí kabely BY MĚLY být vedeny odděleně od telekomunikačních za účelem zabránění rušení. V případě, že jsou napájecí a telekomunikační kabely vedeny společně, MĚLA BY být

implementována odpovídající opatření, aby se zabránilo rušení.

3.3.5 Kabeláž BY MĚLA být pravidelně kontrolována a/nebo odborně prověřena. Zjištěné nesrovnalosti BY MĚLY být zdokumentovány, přezkoumány a napraveny.

3.3.6 V případě kabelových místností BY MĚLY být implementovány požadavky na kontrolu vstupu definované v oddílu 2.

3.3.7 Síťová infrastruktura OT BY MĚLA být navržena pro třídu MCN (síť s maximální dostupností).

3.4 Údržba zařízení

Zařízení BY MĚLO být profesionálně udržováno k zajištění trvalé dostupnosti a integrity.

Implementační pokyny:

3.4.1 Činnosti údržby MUSÍ být oznámeny, koordinovány, zdokumentovány a sdělené v souladu s odpovídajícími postupy řízení změn.

3.4.2 Zařízení BY MĚLO být udržováno v souladu se specifikacemi výrobce v doporučených intervalech údržby.

3.4.3 Činnosti údržby BY MĚLY být prováděny pouze autorizovaným technickým personálem.

3.4.4 Činnosti údržby (na místě nebo vzdáleně) BY MĚLY být prováděny pod dohledem/monitorovány, aby bylo zajištěno, že se zařízením nebylo neodborně zacházeno a že pracuje dle očekávání.

3.4.5 Záznamy o všech podezřeních na závady nebo skutečných závadách týkajících se komponent/zařízení, a o všech nápravných aktivitách údržby komponentu/zařízení BY MĚLY být trvale udržovány.

3.5 Odstranění aktiv

Trvalé odstranění aktiv z prostor společnosti NESMÍ být prováděno bez předchozího schválení.

Implementační pokyny:

3.5.1 Aktiva NESMÍ být trvale odstraněna z prostor společnosti bez předchozího schválení a bez důvodu a potřeb společnosti.

3.5.2 Koncová zařízení a dokumenty MOHOU být dočasně odebrány bez předchozího schválení a pouze pro obchodní účely (např. služební cesta), pokud to není výslovně omezeno/zakázáno.

3.5.3 Jakékoliv zákazy či omezení dočasného odebrání aktiv z prostor organizace MUSÍ být zdokumentovány a patřičně sděleny příslušným zúčastněným stranám.

3.5.4 Jakékoliv zákazy či omezení dočasného odebrání aktiv z prostor organizace BY MĚLY být podpořeny odpovídajícími technickými a/nebo organizačními opatřeními, například:

a) dokumentací identity osoby a ID aktiv,
b) dokumentací důvodů pro odebrání a plánovaného data navrácení,
c) zaznamenáním data/času odebrání a návratu,
d) kontrolou platnosti a/nebo ověřením schválení.

3.6 Neobsluhovaná uživatelská zařízení

Uživatelé MUSÍ být instruováni, aby za všech okolností koncová zařízení, ponechaná bez dohledu, vždy přiměřeně zabezpečili.

Implementační pokyny:

3.6.1 Uživatelské zařízení bez dohledu MUSÍ být při práci na veřejnosti nebo v oblastech s pohybem návštěvníků zabezpečeno proti krádeži.

3.6.2 Obrazovky uživatelského zařízení bez dohledu MUSÍ být při práci na veřejnosti, nebo v oblastech s pohybem návštěvníků, uzamčena, nebo MUSÍ být zařízení zcela vypnuto za účelem zabránění neoprávněného přístupu k informacím.

4 Detekce narušení fyzické bezpečnosti

Společnost MUSÍ k zamezení poškození a neoprávněným zásahům do fyzické bezpečnosti využít detekci narušení fyzické bezpečnosti.

Implementační pokyny:

4.1.1 Společnost MUSÍ využívat detekci narušení fyzické bezpečnosti například ve formě elektronických zabezpečovacích systémů, poplašných systémů a senzorů.

Použité zdroje

(1) *ČSN P 73 4450-1 (734450) Fyzická ochrana prvku kritické infrastruktury - Část 1: Obecné požadavky*. CTN Česká asociace bezpečnostních manažerů, 2013.

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

(3) *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)