Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

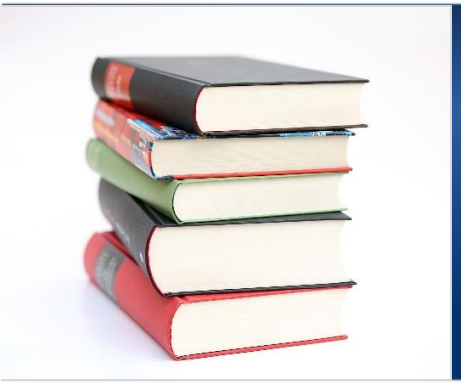
Fyzická bezpečnosť, bezpečnosť prostredia a správa koncových zariadení

Personálne a fyzické opatrenia (Blok III)
Kurz: Manažér kybernetickej bezpečnosti

Ing. Martin Boroš, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Martin.Boros@uniza.sk



Obsah

- Poplachové systémy
- Fyzická a objektová bezpečnosť dátových centier
- Režimové opatrenia
- Požiadavky technických noriem

Poplachové systémy

- Poplachový systém (*angl.: alarm system*) je možné chápať z viacerých pohľadov nakoľko je vo viacerých Slovenských technických normách a predpisoch ako aj odbornej literatúre, s miernou obmenou, definovaný ako elektrická inštalácia reagujúca na manuálnu alebo akustickú detekciu prítomnosti nebezpečia. Mohli by sme preto konštatovať, že poplachovým systémom je každý systém, ktorého primárnym cieľom je vyvolanie poplachu.

- Poplach (*angl.: alarm*), je definovaný v STN EN 50131-1:2007 ako výstraha pri prítomnosti nebezpečia pre život, majetok alebo prostredie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Poplachové systémy

- poplachová aplikácia (angl.: Alarm Application) pod ktorou sa rozumie aplikácia určená na ochranu života, majetku, alebo prostredia. Takouto aplikáciou môže napríklad byť:
  - poplachový zabezpečovací a tiesňový systém,
  - systém privolania pomoci,
  - poplachový systém výťahov,
  - poplachový systém vplyvu prostredia,
  - uzavretý televízny okruh,
  - systém kontroly vstupov,
  - elektrická požiarna signalizácia.

Elektrické zabezpečovacie a tiesňové poplachové systémy

- **Elektrický zabezpečovací systém** (EZS) (angl.: Intruder Alarm System) je poplachový systém na detekciu a indikáciu prítomnosti, vstupu alebo pokusu narušiteľa vstúpiť do chráneného priestoru (STN EN 50131-1).
- **Tiesňový poplachový systém** (TPS) (angl.: Hold-up Alarm System) je poplachový systém, ktorý poskytuje používateľovi prostriedky na zámerné generovanie tiesňového poplachového stavu (STN EN 50131-1).
- **Elektrický zabezpečovací a tiesňový poplachový systém** (EZS/TPS) (angl.: Intrusion and Hold-up Alarm System) je kombinovaný elektrický zabezpečovací systém a tiesňový poplachový systém (STN EN 50131-1). Elektrický zabezpečovací a tiesňový poplachový systém môže pozostávať z viacerých podsystémov. Podsystém je časť EZS/TPS umiestnená v jasne definovanej časti chráneného priestoru schopná samostatnej činnosti (STN EN 50131-1).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Elektrické zabezpečovacie a tiesňové poplachové systémy

- Podľa STN EN 50131-1 musí EZS/TPS minimálne obsahovať nasledujúce komponenty:
  - ústredňu,
  - jeden alebo viac detektorov,
  - jedno alebo viac signalizačných zariadení prípadne poplachových prenosných systémov,
  - jedno alebo viac napájacích zariadení.

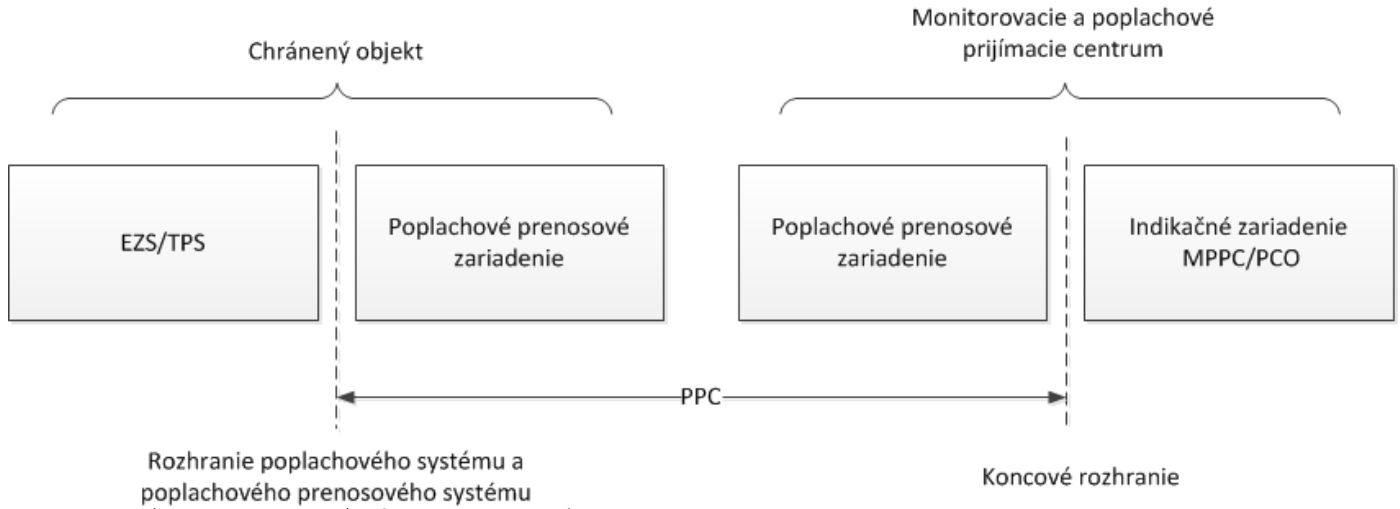
Elektrické zabezpečovacie a tiesňové poplachové systémy

- Stupne zabezpečenia sú nasledujúce:
  - **Stupeň 1: nízke riziko** - narušiteľ má malú znalosť EZS/TPS a má k dispozícii obmedzený sortiment dostupných nástrojov.
  - **Stupeň 2: nízke až stredné riziko** - narušiteľ má určité znalosti o EZS/TPS a má k dispozícii základný sortiment nástrojov a prenosných prístrojov.
  - **Stupeň 3: stredné až vysoké riziko** - narušiteľ je oboznámený s EZS/TPS a má úplný sortiment nástrojov a elektronických zariadení.
  - **Stupeň 4: vysoké riziko** - používa sa vtedy, keď zabezpečenie má prioritu pred ostatnými hľadiskami. Narušiteľ má možnosť spracovať podrobný plán vniknutia, a má kompletný sortiment zariadení vrátane prostriedkov na náhradu komponentov EZS/TPS.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Poplachové prenosové systémy a zariadenia

- **Poplachový prenosový systém** (angl.: Alarm Transmission System) (Obrázok 4-1) je systém použitý na prenos informácií, ktoré sa týkajú stavov jedného alebo viac EZS/TPS, do jedného alebo viac poplachových prijímacích centier. Poplachový prenosový systém zahŕňa:
  - poplachovú prenosovú cestu (PPC),
  - poplachové prenosové zariadenie umiestnené v monitorovacom a poplachovom prijímacom centre (MPPC/PCO),
  - poplachové prenosové zariadenie (PPZ) umiestnené v chránenom objekte (STN EN 50136-1).



Kamerové bezpečnostné systémy

- **CCTV systém** (angl.: Closed Circuit Television System) je systém pozostávajúci z kamerového zariadenia, monitorovacieho a pridruženého zariadenia pre prenosové a riadiace účely, ktoré môžu byť nevyhnutné pre dohľad nad chráneným priestorom. Pod dohľadom nad chráneným priestorom je možné chápať:
  - monitorovanie,
  - detekcia,
  - pozorovanie,
  - rozpoznanie,
  - identifikácia,
  - vyšetrovanie.

Systém kontroly vstupov

- **Systém kontroly vstupov** (angl. *Acces Control Systems*), ďalej len SKV zaraďujeme medzi poplachové systémy a jeho definícia je uvedená v technickej norme EN 60839-11-1, ako : elektronický systém kontroly vstupu, poskytujúci oprávneným osobám alebo entitám vstup alebo opustenie zabezpečeného priestoru a zamietnutie pokusu o vstup alebo opustenie neoprávneným jedincom alebo entitám. Slovíčko entita je doplnením v minulosti dlhodobo používanej definície a označuje akýkoľvek neživý objekt s prideleným oprávnením. V praxi ide hlavne o automobily v rámci smart parkovísk alebo balíkových zásielok. Na základe definície by sme mohli povedať, že SKV nám slúži na zodpovedanie troch základných otázok, ktorými sú kto, kam a kedy má prístup v rámci chráneného objektu. Mohli by sme preto povedať, že SKV plní v rámci objektu dve základné úlohy, a to:
  - riadi pohyb osôb v objekte,
  - monitoruje a zaznamenáva pohyb osôb v objekte.

Systém kontroly vstupov

- Pojem SKV sa pomerne často zamieňa s pojmom prístupový systém, keďže sú tvorené podobnými komponentami. Rozdiel nastáva v podstate daných systémov, zatiaľ čo SKV reálne ovplyvňuje možnosti pohybu osôb po objekte, **prístupové systémy** nezabraňujú voľnému pohybu po objete, a teda je len na dobrovoľnosti používateľa aby ich použil. V prípade SKV však je na konci celého procesu ovládací prvok – turniket, bránky, zámok a podobne, a teda používateľ je nútení použiť čítačku daného systému.

Sociálne inžinierstvo v SKV

- **Slušnosť** – aj obyčajné podržanie dverí, ktoré sa považuje za slušnosť, znemožňuje SKV vykonávať svoje základné funkcie.
- **Zlé počasie** – v prípade nepriaznivého počasie osoby zo solidárnosti pridržia vchodové dvere do objektu aj ďalším osobám a tie sa dostanú do objektu aj bez toho, aby preukázali svoje oprávnenie na vstup.
- **Nevyrovnané/opotrebované dvere** – pri dlhodobom používaní a nedostatočnej kontrole a servise môže dôjsť k neúplnému zatvoreniu alebo pomalému zatvoreniu dverí a vstupu neoprávnených osôb.
- **Ťažkosť/Lenivosť** – ide o úmyselne zablokovanie úplného zatvorenia dverí, zarážkou, kameňmi atď. oprávnenými osobami, aby nemuseli pri každom vstupe žiadať o prístup.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Režimové opatrenia

- Interné smernice

Mechanické zábranné prostriedky

- **Mechanické zábranné prostriedky** (**MZP**) tvoria súbor mechanických a technických prostriedkov, zariadení a komponentov, ktoré svojou konštrukciou znemožňujú ich jednoduché prekonanie. Z hľadiska bezpečnosti majú za úlohu sťažiť alebo celkom znemožniť násilné vniknutie nepovolanej osoby do chráneného priestoru alebo objektu, prípadne zabrániť neoprávnenej manipulácií s chránenými predmetmi v chránenom objekte

Hybridné cylindrické vložky

- Hybridné cylindrické vložky vyžívajú systém štandardného alebo bezpečnostného zámkovým systémom a použitou cylindrickou vložkou ovládanou hybridným (kombinovaným) spôsobom. Tieto cylindrické vložky je možné použiť do zámkov klasických, ale zvyčajne rozvorových, ktoré umožňujú uzamykanie v niekoľkých uzamykacích bodoch, vo vertikálnom i horizontálnom smere. Toto použitie je vhodné aj pre bezpečnostné dvere.
- Výhody magnetických vložiek oproti bežne používaným sú:
  - maximálna ochrana proti napodobeninám kľúčov,
  - každá zámka a každý kľúč sú unikátne,
  - trojnásobná bezpečnosť cez jednu magnetickú a dve mechanické (profil a blokovacie kolíky) kódovacie úrovne,
  - technologická (ochrana proti kopírovaniu), organizačná (bezpečnostná karta) a zákonná ochrana kľúča,
  - modulárna konštrukcia,
  - pri otočení kľúča o 360° sa 2 x nezávisle od seba skontroluje kódovanie,
  - odolnosť proti opotrebeniu vďaka utesneným blokovacím prvkom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hybridné cylindrické vložky

- Ďalšou samostatnou skupinou sú takzvané **biometrické zámky**, tie namiesto kľúčového ovládania využívajú možnosti biometrických údajov používateľov, ktoré na základe oprávneného používateľa otvoria zámok pomocou elektormotora. Takýto spôsob je čoraz častejšie využívaný pri visiacich zámkoch. Pokiaľ sa však zameriame na štandardné dvere je možné rozdeliť ich prevedenia na dve skupiny, a to tie ktoré ovládajú jazýček a uzamykací mechanizmus v dverovom krídle a tie ktoré ovládajú uzamykací systém v zárubni. Pokiaľ sa aplikuje druhá možnosť, využíva sa v dverách hlavne guľa aby sa eliminovala možnosť neoprávneného prekonania.
- V prípade biometrických zámok je možné, a v praxi veľmi často využívané, kombinovanie verifikačných metód. Napríklad biometrická verifikácia s dôkazom vlastníctvom, čipová karta alebo znalosťou zadanie PIN kódu. Kombináciou týchto metód sa zvyšuje odolnosť uzamykacieho systému

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kľúčové systémy

- Kľúčové systémy predstavujú zoskupenie cylindrických vložiek a viacerých kľúčov s priamym definovaným ich hierarchického postavenia. Jedná sa o systému uľahčujúce správu a efektívne využívanie kľúčov v objekte. Z hľadiska používania rozdeľujeme tieto základné skupiny:
  - Systém spoločného kľúča (univerzálny kľúč),
  - Hotelový kľúčový systém,
  - Systém generálneho kľúča

Fyzická a objektová bezpečnosť

Fyzická bezpečnosť a objektová bezpečnosť je systém opatrení na ochranu utajovaných skutočností pred nepovolanými osobami a pred neoprávnenou manipuláciou v objektoch a chránených priestoroch. Ochrana sa zabezpečuje

- mechanickými zábrannými prostriedkami,
- technickými zabezpečovacími prostriedkami,
- fyzickou ochranou,
- režimovými opatreniami a
- ich vzájomnou kombináciou v súlade s bezpečnostným štandardom fyzickej bezpečnosti a objektovej bezpečnosti.

Spôsob, podmienky a rozsah navrhovaných opatrení určuje ich vedúci na základe vyhodnotenia rizík možného ohrozenia objektov a chránených priestorov.

Fyzická a objektová bezpečnosť dátových centier

- V dnešnej informačnej dobe sa stalo nutnosťou starostlivo zabezpečiť uschovávané data. Firewall príliš nepomôže, ak sa k vášmu IT zariadeniu dostane nepovolaná osoba a údaje si z neho skopíruje, alebo vám vaše zariadenie poškodí resp. v extrémnou prípade si ho odnesie.

- Národné aj medzinárodné orgány prijímajú nové a nové nariadenia, ktoré upravujú prácu s informáciami osobách, čo následne ovplyvňuje aj požiadavky na fyzickú bezpečnosť IT infraštruktúry.

- Napriek tomu, že je profesionálne komerčné dátové centrum budovou s veľmi vysokou mierou fyzickej ochrany, niekedy je nutné aktívne zariadenia dodatočne fyzicky oddeliť a zabezpečiť.

- Klietka v dátovom centre dodatočne oddeľuje IT rozvádzače od IT rozvádzačov iných klientov bezpečnostnou mrežou s kontrolovaným vstupom osôb. Môže byť uzamykaná kľúčom, elektromechanicky či biometricky a poskytuje najvyšší štandard fyzickej bezpečnosti pre technológie klienta dátového centra.

- Podobne je možné zabezpečiť aj samotné IT racky. Umiestnia san a ne elektromechanické rukoväte s čítačkami kariet. Tie je možné integrovať do komplexných bezpečnostných systémov. Dostupné sú rôzne miery zabezpečenia, dvojfaktorová autentifikácia, karty s vysokými frekvenciami a podobne.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Fyzická a objektová bezpečnosť dátových centier

Úlohou elektromechanického zabezpečenia IT rozvádzača je kontrola a sledovanie prístupu konkrétnych osôb k citlivým IT zariadeniam. Takáto požiadavka môže často vzniknúť z dôvodu regulácie ochrany citlivých osobných dát.

Existujú rôzne úrovne elektromechanického zabezpečenia IT rovádzačov. Odlišujú sa:

- komfortom použitia (napr. s čítačkami priamo v rukoväti alebo bez, iba s centrálnou správou)
- sofistikovanosťou použitého technického riešenia (čítačky kariet s vysokou alebo nízkou frekvenciou, alebo univezálne)
- mechanickým vyhotovením (dostupné vo viacerých rozmeroch, pre rozvádzače od rôznych výrobcov)
- a samozrejme cenou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Fyzická a objektová bezpečnosť dátových centier

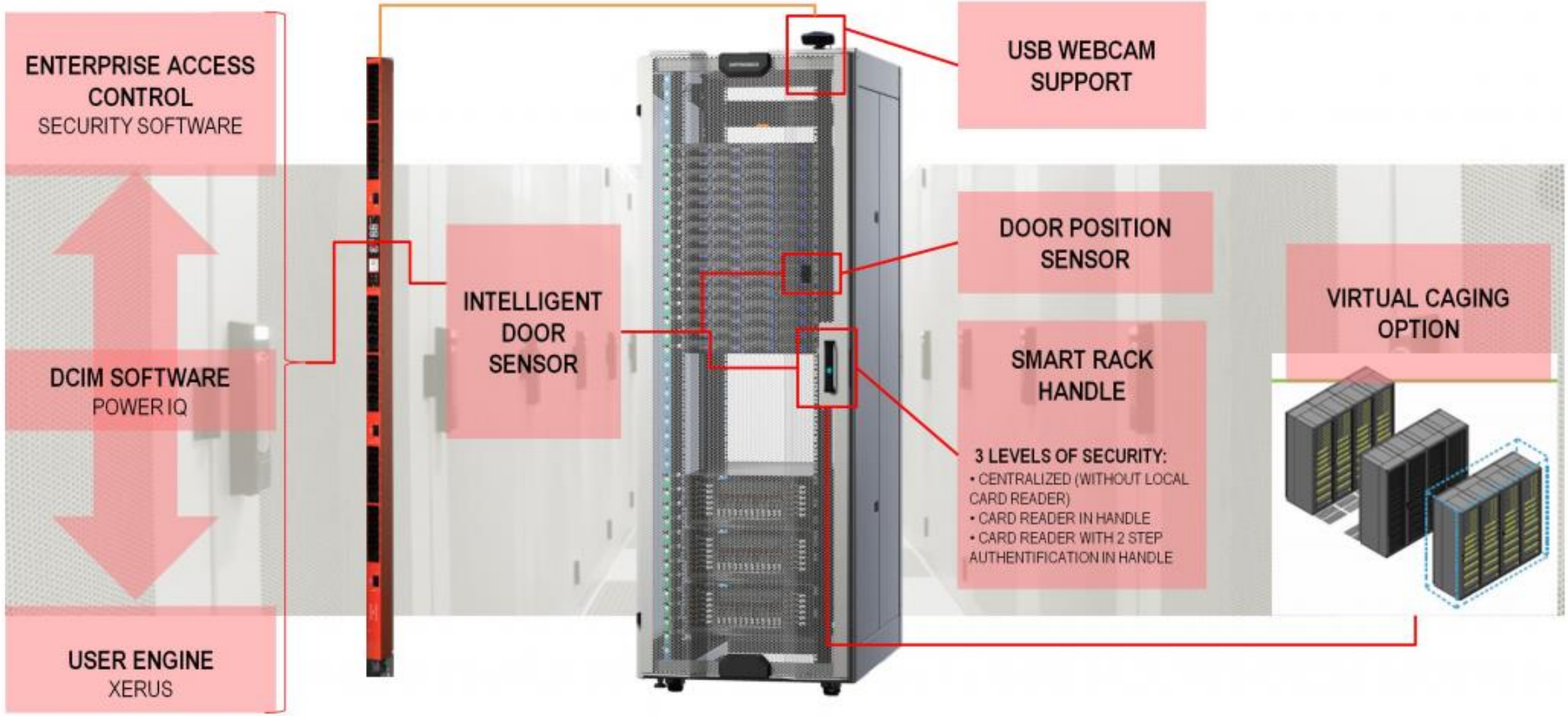
Riešenie je možné implementovať vo viacerých alternatívach:

- Na existujúce IT rozvádzače, iba výmenou zámkou / Uplne nové rozvádzače, dodané komplet vrátane HW a SW
- Ako lokálne stand-alone riešenie / Centralizované zálované multi-site riešenie
- S možnosťou lokálneho ovládania prístupu (čítačky na IT rackoch) / Bez možnosti lokálneho ovládania (administrátor umožní vstup do IT racku na diaľku)
- Ovládanie rukovätí cez inteligentné PDU / Ovládanie cez samostatné riadiace jednotky

Vybrané technické parametri:

- Podpora MIFARE® Classic 4k MIFARE® Plus® 2k MIFARE® DESFire® 4k& iClass® UID, iClass PACS
- Podpora kariet 13,56 MHz a 125 kHz

Príklad logickej schémy zabezpečenia IT racku



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad logickej schémy zabezpečenia IT racku

- Existujú rôzne typy rukovätí – niektoré majú čítačky kariet integrované priamo v rukovätiach, alebo je možné kombinovať elektromechanické rukoväte s externými čítačkami.
- V realizácii nižšie sa jednalo o integrácii čítačky Signo 20 od výrobcu HID Global a rozvádzčov Minkels Nexpand pre podporu vysokej bezpečnosti v štandardoch iClass PACS.

- Realizácia zabezpečenia s čítačkou Signo 20 od HID Global

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Pripájacie káble pre IT zariadenia

Napriek striktným procesom a maximálnej obozretnosti, ľudský faktor zostáva jedným z hlavných faktorov výpadku dostupnosti služieb v dátových centách.

Veľmi často dochádza k nechcenému odpojeniu napájacích káblov pri práci technického personálu v zadnej časti IT racky. Deje sa tak najmä z dôvodov:

- Nedostatočne pevného spoja medzi zásuvkami C13/C14 a C19/C20
- Neprehľadnosti veľkého množstva káblov

V rámci ponuky trhu sú dodávané viacfarebné napácie káble s uzamykateľnými konektormi konektory znižujú pravdepodobnosť náhodného vytrhnutia a odpojenia záťaže.

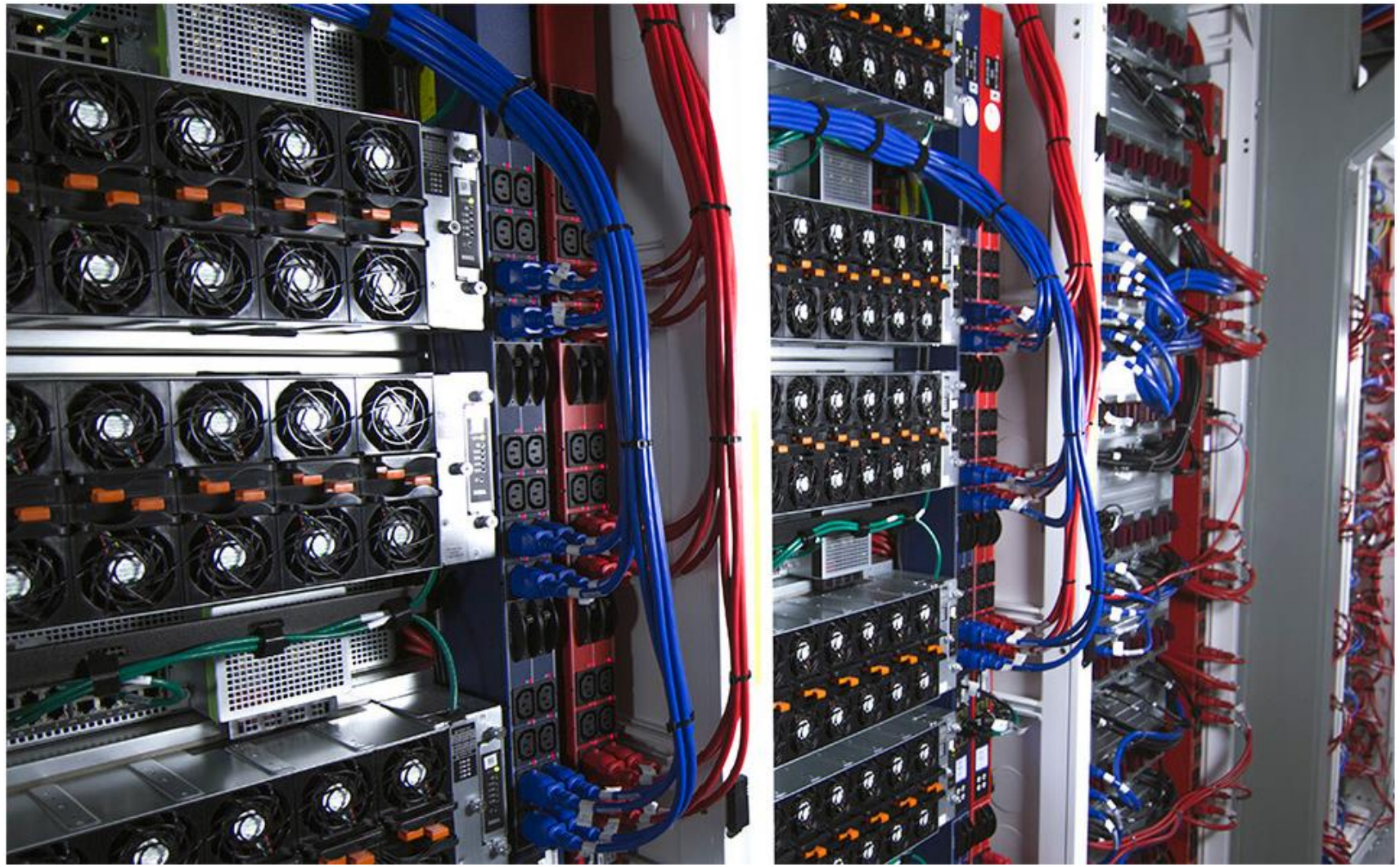
- Káble sú dodávané napríklad v týchto variantoch:
  - Farby: čierna, modrá, zelená, biela, červená
  - DÍžky: 0,5m – 1m – 1,5m – 2m – 2,5m – 3m
  - Pripojenia: IEC C14/IEC C13, IEC C19/20, IEC C14/C15

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad mechanického systému pre pevné uzamknutie kábla v IT zariadení

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklad farebného rozlíšenia napájacích vetiev v IT racku



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Klietky pre dátové centrá

- V prípade legislatívnych požiadaviek na najvyššiu bezpečnosť uschovávaných dát v dátovom centre je nutné dodatočne fyzicky zabezpečiť aj samotné IT racky a zariadeniach v nich. Klietka poskytuje zákazíkovi vlastný fyzicky zabezpečený priestor.
- Klietka je oddelená od ostatných zariadení iných klientov bezpečnostnou mrežou s kontrolovaným vstupom osôb. Môže byť uzamykaná kľúčom, elektromechanicky či biometricky a poskytuje najvyšší štandard fyzickej bezpečnosti pre technológie klienta dátového centra.

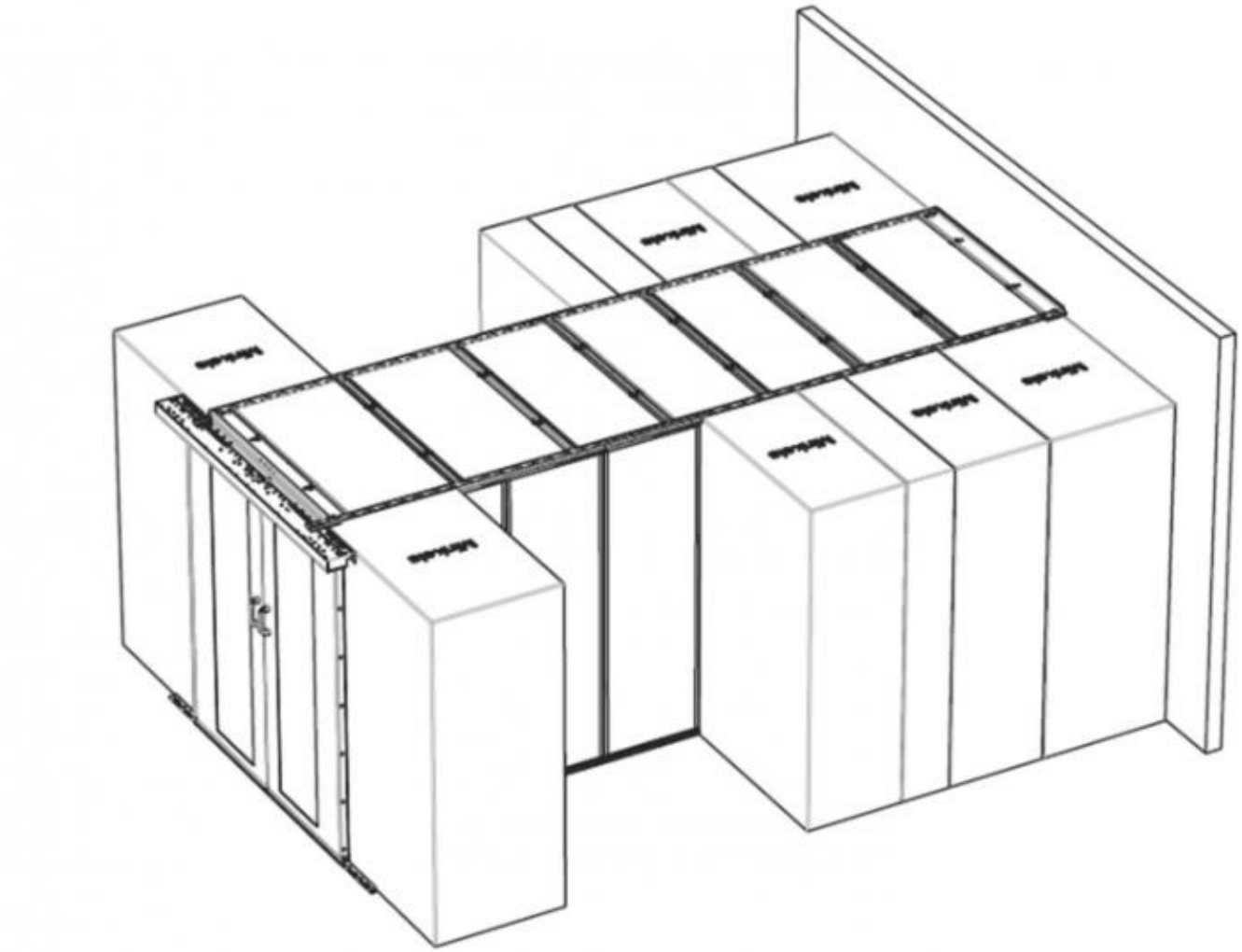
Príklad použitia klietok v dátovom centre

Serverové rozvádzače

- Serverové rozvádzače pre dátové centrá musia spĺňať úplné iné kritériá ako rozvádzače umiestňované v LAN sieťach. Jedným zo základných kritérií je miera vzduchotesnosti rozvádzača (nižšie úniky ochladeného vzduchu = nižší výkon chladiacich jednotiek = nižšia spotreba elektrickej energie = nižšia cena služby pre koncového zákazníka). Nami dodávaná nová generácia 19“ / 21“ / 23“ rozvádzačov pre dátové centrá je riešená vzduchotesne, má vysokú mechanickú pevnosť a kvalitu opracovania. Ponúka široké možnosti príslušenstva pre vedenie kabeláže, integrácie káblových trás a rozvodov energie, ako aj studených, teplých či iných typov uličiek.

Serverové rozvádzače

Serverové rozvádzače



Fyzická a objektová bezpečnosť z pohľadu technických noriem

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Perimetre fyzickej bezpečnosti

Opatrenia
Majú byť definované bezpečnostné perimetre a používané na ochranu oblastí, ktoré obsahujú informácie a ďalšie súvisiace aktíva.

Účel
Zabrániť neoprávnenému fyzickému prístupu, poškodeniu a narušeniu informácií a ďalších súvisiacich aktív organizácie.

Pokyny
Majú sa zvážiť nasledujúce pokyny a v prípade potreby zaviesť pre fyzické bezpečnostné perimetre:
a) definovanie bezpečnostných perimetrov a ich umiestnenie a odolnosť v súlade s požiadavkami informačnej bezpečnosti týkajúcimi sa aktív nachádzajúcich sa v rámci perimetra;
b) zabezpečiť fyzicky spoľahlivé perimetre budov alebo priestorov, v ktorých sa nachádza vybavenie na spracovanie informácií (t. j. perimetr by nemal byť nikde prerušený alebo by v ňom nemali byť miesta, cez ktoré je možné ľahko preniknúť). Vonkajšia strešná konštrukcia, steny a podlahy priestorov majú byť pevnej konštrukcie a všetky vonkajšie dvere majú byť vhodne chránené pred neoprávneným prístupom pomocou kontrolných mechanizmov (napr. mreže, alarmy, zámky). Dvere a okná majú byť počas neprítomnosti uzatvorené, a mala by sa zvážiť vonkajšia ochrana najmä pre okná na prízemí; takisto by sa mali zvážiť ventilačné otvory;
c) zabezpečiť poplašný systém, monitorovanie a testovanie všetkých protipožiarnych dverí v bezpečnostnom perimetri v spojení so stenami tak, aby sa dosiahla požadovaná úroveň odolnosti v súlade s príslušnými normami. To všetko má fungovať bezpečným spôsobom.

Ďalšie informácie
Fyzickú ochranu je možné dosiahnuť vytvorením jednej alebo viacerých fyzických bariér okolo budov organizácie a vybavenia na spracovanie informácií.
Bezpečným priestorom môže byť uzamykateľná kancelária alebo niekoľko miestností obklopených súvislou vnútornou fyzickou bezpečnostnou bariérou. Medzi oblasťami s rôznymi požiadavkami na bezpečnosť v rámci bezpečnostného perimetra môžu byť potrebné dodatočné bariéry a perimetre na riadenie fyzického prístupu. Organizácia má zvážiť, či má k dispozícii fyzické bezpečnostné opatrenia, ktoré je možné v prípade zvýšenej hrozby posilniť.

Fyzický vstup

Opatrenia
Zabezpečené oblasti majú byť na vstupoch a prístupových miestach chránené vhodnými opatreniami.

- **Účel**
  Zabezpečiť, aby k informáciám organizácie a ďalším súvisiacim aktívam mal prístup iba autorizovaný fyzický prístup.

Pokyny
Všeobecne
Prístupové miesta, ako sú miesta doručovania a nakladacie priestory, ako aj iné miesta, ktorými môžu neoprávnené osoby vstúpiť do priestorov, majú byť kontrolované a pokiaľ možno izolované od zariadení na spracovanie informácií, aby sa zabránilo neoprávnenému prístupu.

- Majú sa zvážiť nasledujúce pokyny:
  a) obmedzenie prístupu na pracoviská a do budov len pre oprávnené osoby. Proces správy prístupových práv do fyzických priestorov má zahŕňať udeľovanie, pravidelné prehodnocovanie, aktualizáciu a rušenie oprávnení;
  b) bezpečné vedenie a monitorovanie fyzického denníka alebo elektronickej auditnej stopy o všetkých prístupoch a ochrana všetkých záznamov (pozri bod 5.33) a citlivých autentifikačných údajov.

Fyzický vstup

c) zavedenie a uplatňovanie procesu a technických mechanizmov na riadenie prístupu do oblastí, kde sa spracúvajú alebo uchovávajú informácie. Autentifikačné mechanizmy zahŕňajú používanie prístupových kariet, biometrickej alebo dvojfaktorovej autentifikácie, ako je kombinácia prístupovej karty a tajného PIN kódu. Pre prístup do citlivých oblastí by sa mali zvážiť dvojité bezpečnostné dvere;

d) zriadenie recepcie monitorovanej personálom alebo využitie iných prostriedkov na kontrolu fyzického prístupu do objektu alebo budovy;

e) kontrola a prehliadka osobných vecí zamestnancov a zainteresovaných strán pri vstupe a výstupe;

POZNÁMKA: Môžu existovať miestne právne predpisy a nariadenia týkajúce sa možnosti kontroly osobných vecí.

- f) požiadavka, aby všetci zamestnanci a zainteresované strany nosili viditeľné označenie a aby okamžite informovali bezpečnostný personál, ak sa stretnú s návštevníkmi bez sprievodu alebo s osobami bez viditeľného označenia. Mali by sa zvážiť ľahko rozlíšiteľné preukazy na lepšiu identifikáciu stálych zamestnancov, dodávateľov a návštevníkov.

Fyzický vstup

g) pracovníkom dodávateľov poskytovať obmedzený prístup do zabezpečených oblastí alebo k zariadeniam na spracovanie informácií len v prípade potreby. Tento prístup má byť autorizovaný a monitorovaný;

h) venovať osobitnú pozornosť fyzickej bezpečnosti prístupu v budovách, kde sa nachádzajú aktíva viacerých organizácií;

i) navrhovať opatrenia fyzickej bezpečnosti tak, aby ich bolo možné posilniť v prípade zvýšenej pravdepodobnosti fyzických incidentov;

j) zabezpečiť ďalšie vstupné body, ako sú núdzové východy, pred neoprávneným prístupom;

k) nastaviť proces správy kľúčov tak, aby bol zabezpečený manažment fyzických kľúčov alebo autentifikačných informácií (napr. kódy k zámkom, kombinačné zámky k kanceláriám, miestnostiam a vybaveniu, ako sú skrinky na kľúče), a aby bola vedená kniha záznamov alebo uskutočňovaný každoročný audit kľúčov a zároveň kontrolovaný prístup k fyzickým kľúčom alebo autentifikačným údajom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Fyzický vstup

Návštevníci
Majú sa zvážiť nasledujúce pokyny:
a) overenie totožnosti návštevníkov vhodným spôsobom;
b) zaznamenanie dátumu a času príchodu a odchodu návštevníkov;
c) umožnenie prístupu návštevníkom len na konkrétne, oprávnené účely spolu s poskytnutím pokynov k bezpečnostným požiadavkám daného priestoru a k núdzovým postupom;
d) dohľad nad všetkými návštevníkmi, pokiaľ nie je udelená výslovná výnimka.

Fyzický vstup

Nakladacie a vykladacie priestory a prijímaný materiál
Majú sa zvážiť nasledujúce pokyny:
a) obmedzenie prístupu do priestorov určených na dodávky a nakládku zvonku budovy iba pre identifikovaných a oprávnených pracovníkov;
b) navrhnutie týchto priestorov tak, aby bolo možné vykonávať nakládku a vykládku bez toho, aby doručujúci pracovníci získali neoprávnený prístup do iných častí budovy;
c) zabezpečenie vonkajších dverí nakladacích priestorov, ak sú zároveň otvorené dvere do vyhradených priestorov.

Fyzický vstup

d) kontrola a prehliadka prichádzajúcich dodávok s cieľom zistiť, či neobsahujú výbušniny, chemikálie alebo iné nebezpečné materiály, ešte pred ich premiestnením z priestorov pre dodávky a nakládku;

e) registrácia prichádzajúcich dodávok v súlade s postupmi správy aktív pri ich doručení na miesto;

f) fyzické oddelenie prichádzajúcich a odchádzajúcich zásielok, ak je to možné;

g) kontrola prichádzajúcich zásielok, či s nimi počas doručovania nebolo manipulované. Ak sa zistí manipulácia, má byť okamžite podaná správa bezpečnostnému personálu.

Zabezpečenie kancelárií, miestností a vybavenia

Opatrenia
Majú byť navrhnuté a zavedené opatrenia na fyzickú bezpečnosť kancelárií, miestností a vybavenia.

Účel
Zabrániť neoprávnenému fyzickému prístupu, poškodeniu a narušeniu informácií a ďalších súvisiacich aktív organizácie v kanceláriách, miestnostiach a zariadeniach.

Pokyny
Na zabezpečenie kancelárií, miestností a vybavenia majú byť zvážené nasledujúce pokyny:
a) kritické vybavenie má byť umiestnené tak, aby bol znemožnený prístup verejnosti;
b) ak je to vhodné, budovy by mali byť nenápadné a mali by poskytovať minimálne náznaky o svojom účele, bez zreteľných označení zvonka alebo zvnútra, ktoré by identifikovali prítomnosť aktivít spracovania informácií;
c) vybavenie má byť nakonfigurované tak, aby dôverné informácie alebo činnosti neboli viditeľné ani počuteľné zvonku. Za vhodné sa tiež považuje elektromagnetické tienenie;
d) adresáre, interné telefónne zoznamy a online dostupné mapy identifikujúce umiestnenie zariadení na spracovanie dôverných informácií by nemali byť ľahko prístupné neoprávneným osobám.

Monitorovanie fyzickej bezpečnosti

Opatrenia

Priestory majú byť nepretržite monitorované s cieľom odhaliť neoprávnený fyzický prístup.

Účel

Detegovať a zabrániť neoprávnenému fyzickému prístupu.

Pokyny

Fyzické priestory majú byť monitorované dohľadovými systémami, ktoré môžu zahŕňať bezpečnostnú službu, poplašné systémy proti vniknutiu, video monitorovacie systémy (napr. uzavretý televízny okruh – CCTV) a softvér na správu informácií o fyzickej bezpečnosti, spravovaný interne alebo poskytovateľom monitorovacích služieb.

Monitorovanie fyzickej bezpečnosti

Prístup do budov, v ktorých sú umiestnené kritické systémy, má byť nepretržite monitorovaný s cieľom odhaliť neoprávnený prístup alebo podozrivé správanie, a to prostredníctvom:

a) inštalácie video monitorovacích systémov, ako je CCTV, na sledovanie a záznam prístupu do citlivých oblastí v rámci aj mimo priestorov organizácie;

b) inštalácie a pravidelného testovania kontaktných, zvukových alebo pohybových detektorov v súlade s príslušnými normami s cieľom spustiť poplach v prípade narušenia, napríklad:
1) kontaktné detektory, ktoré spustia poplach pri nadviazaní alebo prerušení kontaktu (napr. na oknách, dverách alebo spodných stranách predmetov);
2) pohybové detektory využívajúce infračervenú technológiu, ktoré spustia poplach pri zaznamenaní pohybu v zornom poli;
3) senzory citlivé na zvuk rozbíjajúceho sa skla, ktoré môžu spustiť poplach a upozorniť bezpečnostný personál;

c) použitie alarmov na pokrytie všetkých vonkajších dverí a prístupných okien. Neobsadené priestory majú byť vždy zabezpečené alarmom; alarmové pokrytie má byť zabezpečené aj pre ostatné priestory (napr. počítačové alebo komunikačné miestnosti).

Monitorovanie fyzickej bezpečnosti

Návrh monitorovacích systémov má zostať dôverný, pretože jeho zverejnenie by mohlo uľahčiť neoprávnené vniknutie.
Monitorovacie systémy majú byť chránené pred neoprávneným prístupom, aby sa zabránilo prístupu k sledovacím informáciám (napr. videozáznamom) alebo vzdialenému vyradeniu systému z prevádzky.

Ovládací panel poplachového systému má byť umiestnený v poplachovej zóne a – v prípade bezpečnostných poplachov – na mieste, ktoré umožňuje jednoducho sa evakuovať osobe, ktorá systém aktivuje. Panel aj detektory majú byť vybavené mechanizmami odolnými voči neoprávnenej manipulácii. Systém má byť pravidelne testovaný, najmä ak jeho komponenty sú napájané z batérií, aby sa overila jeho funkčnosť.

Všetky monitorovacie a záznamové mechanizmy musia byť používané v súlade s miestnymi zákonmi a predpismi, vrátane právnych predpisov o ochrane údajov a osobných údajov (PII), najmä pri monitorovaní zamestnancov a určovaní doby uchovávania videozáznamov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana pred fyzickými a prírodnými hrozbami

Opatrenia

Má byť navrhnutá a zavedená ochrana pred fyzickými a prírodnými hrozbami, ako sú prírodné katastrofy a iné úmyselné alebo neúmyselné fyzické hrozby voči infraštruktúre.

Účel

Predchádzať udalostiam spôsobeným fyzickými a prírodnými hrozbami alebo zmierniť ich následky.

Pokyny

Pred začatím kritických operácií na fyzickom pracovisku a následne v pravidelných intervaloch má byť vykonané hodnotenie rizík na identifikáciu potenciálnych dôsledkov fyzických a prírodných hrozieb.
Majú byť zavedené potrebné ochranné opatrenia a priebežne sledované zmeny v hrozbách.
Je potrebné vyhľadať odborné poradenstvo týkajúce sa riadenia rizík vyplývajúcich z fyzických a prírodných hrozieb, ako sú požiare, povodne, zemetrasenia, výbuchy, občianske nepokoje, toxický odpad, emisie do životného prostredia a iné formy prírodných alebo človekom spôsobených katastrof.

Ochrana pred fyzickými a prírodnými hrozbami

Fyzické umiestnenie a konštrukcia priestorov majú zohľadňovať:

a) miestnu topografiu, ako je vhodná nadmorská výška, vodné plochy a tektonické zlomy;

b) mestské hrozby, ako sú oblasti s vysokým rizikom politických nepokojov, trestnej činnosti alebo teroristických útokov.

Na základe výsledkov posúdenia rizík majú byť identifikované relevantné fyzické a prírodné hrozby a mali by sa zvážiť vhodné opatrenia v nasledovných kontextoch ako príklady:

a) **požiar**: inštalácia a konfigurácia systémov schopných detegovať požiar v ranom štádiu a spustiť poplach alebo automaticky aktivovať hasiace systémy s cieľom zabrániť poškodeniu nosičov dát a systémov spracovania informácií. Hasiace látky majú byť vybrané s ohľadom na okolie (napr. plyn v uzavretých priestoroch);

Ochrana pred fyzickými a prírodnými hrozbami

b) **záplavy**: inštalácia systémov na včasné odhalenie zaplavenia pod podlahami v miestnostiach, kde sa nachádzajú pamäťové médiá alebo systémy na spracovanie informácií. Pre prípad zaplavenia majú byť k dispozícii vodné čerpadlá alebo ekvivalentné vybavenie;
c) **elektrické prepätia**: nasadenie systémov na ochranu serverových aj klientskych informačných systémov pred elektrickými prepätiami alebo podobnými udalosťami, aby sa minimalizovali ich následky;
d) **výbušniny a zbrane**: vykonávanie namátkových kontrol zameraných na odhalenie prítomnosti výbušnín alebo zbraní u zamestnancov, vozidiel alebo tovaru vstupujúcich do priestorov so spracovaním citlivých informácií.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ochrana pred fyzickými a prírodnými hrozbami

Ďalšie informácie

Trezory alebo iné formy bezpečných skladovacích priestorov môžu chrániť uložené informácie pred katastrofami, ako sú požiar, zemetrasenie, povodeň alebo výbuch.

Organizácie môžu pri navrhovaní bezpečnostných opatrení a znižovaní mestských hrozieb zohľadniť koncepciu **prevencie kriminality prostredníctvom environmentálneho dizajnu (CPTED)**. Napríklad namiesto betónových stĺpikov môžu ako fyzické bariéry poslúžiť sochy alebo vodné prvky, ktoré zároveň esteticky zapadajú do prostredia.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Práca v zabezpečených oblastiach

Opatrenia
Majú byť navrhnuté a zavedené bezpečnostné opatrenia pre prácu v zabezpečených oblastiach.

Účel
Chrániť informácie a ďalšie súvisiace aktíva v zabezpečených oblastiach pred poškodením a neoprávneným zásahom zo strany pracovníkov pracujúcich v týchto oblastiach.

Pokyny
Bezpečnostné opatrenia pre prácu v zabezpečených oblastiach by sa mali vzťahovať na všetkých pracovníkov a zahŕňať všetky činnosti vykonávané v zabezpečenej oblasti.

- Majú sa zvážiť nasledujúce pokyny:
  a) informovanie pracovníkov o existencii zabezpečenej oblasti alebo o činnostiach v nej len v nevyhnutne nutnom rozsahu;

Práca v zabezpečených oblastiach

b) vyhýbanie sa práci v zabezpečených oblastiach bez dozoru – z bezpečnostných dôvodov aj na zníženie rizika škodlivých činností;
c) fyzické uzamknutie a pravidelná kontrola prázdnych zabezpečených oblastí;
d) zákaz používania fotografických, obrazových, zvukových alebo iných záznamových zariadení (napr. kamier v koncových zariadeniach používateľa) bez príslušného oprávnenia;
e) primeraná kontrola vnášania a používania koncových zariadení používateľa v zabezpečených oblastiach;
f) zverejnenie núdzových postupov viditeľným a ľahko prístupným spôsobom.

Prázdny stôl a prázdna obrazovka

Opatrenia

Pre zariadenia na spracovanie informácií majú byť stanovené a dôsledne vynucované pravidlá „prázdneho stola“ pre papierové a prenosné pamäťové médiá a pravidlá „prázdnej obrazovky“.

Účel

Znížiť riziko neoprávneného prístupu, straty a poškodenia informácií, ktoré sa nachádzajú na stoloch, obrazovkách a iných dostupných miestach počas pracovnej doby aj mimo nej.

Pokyny

Organizácia má zaviesť a oznámiť všetkým príslušným zainteresovaným stranám tematicky špecifickú politiku týkajúcu sa prázdneho stola a prázdnej obrazovky.

Prázdny stôl a prázdna obrazovka

Majú sa zvážiť nasledujúce pokyny:
a) uzamykanie citlivých alebo kritických informácií (napr. v papierovej forme alebo na elektronických pamäťových médiách) do trezorov, uzamykateľných skríň alebo iného bezpečnostného nábytku, ak nie sú práve používané – najmä pri opustení kancelárie;
b) zabezpečenie koncových zariadení používateľa pomocou zámkov na kľúč alebo iných bezpečnostných mechanizmov, ak sa nepoužívajú alebo sú bez dozoru;
c) odhlasovanie sa z koncových zariadení alebo ich uzamykanie prostredníctvom obrazovkového a klávesnicového zámku, ktorý vyžaduje autentifikáciu používateľa, pri ponechaní zariadenia bez dozoru. Všetky počítače a systémy majú byť nastavené s funkciou časového limitu alebo automatického odhlásenia;

Prázdny stôl a prázdna obrazovka

d) okamžité odoberanie výstupov z tlačiarní alebo multifunkčných zariadení ich pôvodcom. Odporúča sa používanie tlačiarní s funkciou overenia identity, ktoré umožňujú vydanie výtlačkov iba v prítomnosti používateľa;
e) bezpečné uchovávanie dokumentov a výmenných pamäťových médií obsahujúcich citlivé informácie, a ich bezpečné zničenie, ak už nie sú potrebné;
f) zavedenie a komunikácia pravidiel a odporúčaní pre konfiguráciu vyskakovacích okien na obrazovkách (napr. vypnutie e-mailových notifikácií počas prezentácií, zdieľania obrazovky alebo pri práci vo verejných priestoroch);
g) vymazanie citlivých alebo kritických informácií z tabúľ a iných zobrazovacích zariadení, ak už nie sú potrebné.

Organizácia má mať zavedené postupy pre prípady opustenia pracoviska alebo zariadenia vrátane záverečnej kontroly pred odchodom, aby sa zabezpečilo, že žiadne aktíva (napr. dokumenty zapadnuté za zásuvkami alebo nábytkom) nezostanú bez dozoru.

Umiestnenie a ochrana zariadení

Opatrenia
Zariadenie má byť bezpečne umiestnené a chránené.

Účel
Znížiť riziká vyplývajúce z fyzických a prírodných hrozieb, ako aj z neoprávneného prístupu a poškodenia.

Pokyny
Na ochranu zariadení majú byť zvážené nasledujúce pokyny:
a) umiestniť zariadenie tak, aby sa minimalizoval zbytočný pohyb osôb v pracovných priestoroch a zabránilo sa neoprávnenému prístupu;
b) starostlivo rozmiestniť zariadenia na spracovanie informácií, ktoré pracujú s citlivými údajmi, aby sa znížilo riziko ich sledovania neoprávnenými osobami počas používania;

Umiestnenie a ochrana zariadení

c) prijať opatrenia na minimalizáciu rizík fyzických a prírodných hrozieb (napr. krádež, požiar, výbuch, dym, voda alebo jej výpadok, prach, vibrácie, chemické účinky, výpadky napájania, komunikačné rušenie, elektromagnetické žiarenie, vandalizmus);
d) stanoviť pravidlá pre konzumáciu jedál a nápojov a zákaz fajčenia v blízkosti zariadení na spracovanie informácií;
e) monitorovať podmienky prostredia (napr. teplotu a vlhkosť), ktoré môžu nepriaznivo ovplyvniť činnosť zariadení;
f) použiť bleskozvody na všetky budovy a nainštalovať ochranné filtre proti prepätiu na všetky napájacie a komunikačné vedenia;
g) zvážiť použitie špeciálnych ochranných prvkov (napr. ochranné fólie na klávesnice) v priemyselnom prostredí;
h) chrániť zariadenia spracúvajúce dôverné informácie pred únikom údajov v dôsledku elektromagnetického vyžarovania;
i) fyzicky oddeliť zariadenia na spracovanie informácií, ktoré sú spravované organizáciou, od tých, ktoré spravované nie sú.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť aktív mimo priestorov organizácie

Opatrenie
Aktíva mimo priestorov organizácie je potrebné chrániť.

Účel
Zabrániť strate, poškodeniu, krádeži alebo kompromitácii zariadení mimo pracoviska a prerušeniu činnosti organizácie.

- **Pokyny**
  Akékoľvek zariadenie používané mimo priestorov organizácie, ktoré uchováva alebo spracúva informácie (napr. mobilné zariadenia), vrátane zariadení vo vlastníctve organizácie a zariadení vo vlastníctve jednotlivcov, ktoré sa používajú v mene organizácie [prineste si vlastné zariadenie (BYOD)], si vyžaduje ochranu. Používanie týchto zariadení má byť schválené vedením.

Bezpečnosť aktív mimo priestorov organizácie

Na ochranu zariadení, ktoré uchovávajú alebo spracúvajú informácie mimo priestorov organizácie, treba zvážiť nasledujúce pokyny:
a) nenechávať zariadenia a pamäťové médiá vynesené mimo priestorov bez dozoru na verejných a nezabezpečených miestach;
b) neustále dodržiavať pokyny výrobcov na ochranu zariadení (napr. ochrana pred vystavením silným elektromagnetickým poliam, vode, teplu, vlhkosti, prachu);

c) ak je zariadenie mimo priestorov prenášané medzi rôznymi jednotlivcami alebo zainteresovanými stranami, viesť záznam vo forme logu, ktorý definuje reťaz správcov zariadenia a obsahuje aspoň mená a organizácie jednotlivcov, ktorí sú za zariadenie zodpovední. Informácie, ktoré nie je nevyhnutné prenášať spolu s aktívom, majú byť pred prenosom bezpečne vymazané;
d) ak je to potrebné a prakticky realizovateľné, vyžadovať povolenie na vynesenie zariadení a médií z priestorov organizácie a viesť záznamy o takomto vynesení kvôli zachovaniu auditnej stopy (pozri 5.14);
e) ochrana pred pohľadmi na informácie na zariadení (napr. mobilnom telefóne alebo notebooku) vo verejnej doprave a pred rizikami súvisiacimi so sledovaním „cez plece“;
f) zavedenie sledovania polohy a možnosti vzdialeného vymazania zariadenia.

Bezpečnosť aktív mimo priestorov organizácie

- Trvalá inštalácia zariadení mimo priestorov organizácie [ako sú antény a bankomaty (ATM)] môže byť vystavená vyššiemu riziku poškodenia, krádeže alebo odpočúvania. Tieto riziká sa môžu medzi jednotlivými lokalitami výrazne líšiť a mali by byť zohľadnené pri určovaní najvhodnejších opatrení. Pri umiestňovaní týchto zariadení mimo priestorov organizácie by sa mali zvážiť nasledujúce pokyny:
  a) monitorovanie fyzickej bezpečnosti (pozri 7.4);
  b) ochrana pred fyzickými hrozbami a hrozbami prostredia (pozri 7.5);
  c) riadenie fyzického prístupu a neoprávnenej manipulácie;
  d) riadenie logického prístupu.

Pamäťové médiá

Opatrenie

S pamäťovými médiami je potrebné zaobchádzať počas celého ich životného cyklu – od zaobstarania, používania, prepravy až po likvidáciu – v súlade s klasifikačnou schémou organizácie a požiadavkami na ich spracovanie.

Účel

Zabezpečiť, aby k informáciám na pamäťových médiách mali prístup, mohli ich upravovať, odstrániť alebo zničiť iba oprávnené osoby.

- **Pokyny**

  Vymeniteľné pamäťové médiá

  Pri správe vymeniteľných pamäťových médií je potrebné zvážiť nasledujúce odporúčania:

  a) stanoviť tematicky špecifickú politiku pre správu vymeniteľných pamäťových médií a oboznámiť s ňou všetkých, ktorí takéto médiá používajú alebo s nimi pracujú;

Pamäťové médiá

- b) ak je to potrebné a prakticky uskutočniteľné, vyžadovať povolenie na vynesenie pamäťových médií z organizácie a viesť záznamy o takýchto vyneseniach na účely auditnej stopy;
  c) uchovávať všetky pamäťové médiá v chránenom a bezpečnom prostredí podľa klasifikácie obsiahnutých informácií a chrániť ich pred environmentálnymi hrozbami (ako je teplo, vlhkosť, elektromagnetické pole alebo starnutie) v súlade so špecifikáciami výrobcov;
  d) ak je dôvernosť alebo integrita informácií dôležitým aspektom, použiť kryptografické techniky na ochranu informácií na vymeniteľných pamäťových médiách;
  e) na zmiernenie rizika degradácie pamäťových médií v čase, keď sú uložené informácie stále potrebné, preniesť tieto informácie na nové pamäťové médiá ešte predtým, než sa stanú nečitateľnými.

Pamäťové médiá

- **f)** ukladanie viacerých kópií cenných informácií na samostatné pamäťové médiá s cieľom ďalej znížiť riziko náhodného poškodenia alebo straty informácií;
  g) zváženie evidencie vymeniteľných pamäťových médií, aby sa obmedzila možnosť straty informácií;
  h) povolenie portov pre vymeniteľné pamäťové médiá [napr. slotov pre SD karty a USB portov] iba v prípade, že existuje organizačný dôvod na ich používanie;
  i) v prípade potreby používať vymeniteľné pamäťové médiá s možnosťou monitorovania prenosu informácií na tieto pamäťové médiá;
  j) informácie môžu byť počas fyzickej prepravy zraniteľné voči neoprávnenému prístupu, zneužitiu alebo poškodeniu, napríklad pri zasielaní pamäťových médií poštou alebo kuriérskou službou.
  Pri tomto opatrení sa za médiá považujú aj papierové dokumenty. Pri odovzdávaní fyzických pamäťových médií použite bezpečnostné opatrenia uvedené v bode.

Pamäťové médiá

Bezpečné opakované použitie alebo likvidácia

Majú byť stanovené postupy na bezpečné opätovné použitie alebo likvidáciu pamäťových médií, aby sa minimalizovalo riziko úniku dôverných informácií k neoprávneným osobám. Postupy pre bezpečné opätovné použitie alebo likvidáciu pamäťových médií obsahujúcich dôverné informácie by mali byť úmerné citlivosti týchto informácií. Mali by byť zvážené nasledujúce body:

a) ak je potrebné pamäťové médiá obsahujúce dôverné informácie znovu použiť v rámci organizácie, je potrebné bezpečne vymazať dáta alebo pamäťové médiá pred opätovným použitím naformátovať;
b) bezpečná likvidácia pamäťových médií obsahujúcich dôverné informácie, ak už nie sú potrebné (napr. ich zničením, skartovaním alebo bezpečným vymazaním obsahu);
c) zavedenie postupov na identifikáciu položiek, ktoré môžu vyžadovať bezpečnú likvidáciu;
d) mnoho organizácií ponúka služby zberu a likvidácie pamäťových médií. Výber vhodného externého dodávateľa s primeranými opatreniami a skúsenosťami si vyžaduje osobitnú pozornosť;
e) vedenie záznamov o likvidácii citlivých položiek na zabezpečenie auditnej stopy;
f) pri zhromažďovaní pamäťových médií určených na likvidáciu treba brať do úvahy efekt agregácie, ktorý môže spôsobiť, že veľké množstvo necitlivých informácií sa v súhrne stane citlivými informáciami.

- V prípade poškodených zariadení obsahujúcich citlivé údaje by malo byť vykonané posúdenie rizík, aby sa určilo, či by zariadenia mali byť fyzicky zničené namiesto toho, aby boli odoslané na opravu alebo vyradené.

Podporné služby

Opatrenie
Zariadenia na spracovanie informácií majú byť chránené pred výpadkami napájania a inými poruchami spôsobenými zlyhaním podporných služieb.

Účel
Zabrániť strate, poškodeniu alebo ohrozeniu informácií a ďalších súvisiacich aktív, ako aj prerušeniu činnosti organizácie v dôsledku zlyhania a narušenia podporných služieb.

- **Pokyny**
  Organizácie sú závislé od verejných služieb (napr. elektrina, telekomunikácie, dodávky vody, plyn, kanalizácia, vetranie a klimatizácia), ktoré podporujú ich vybavenie na spracovanie informácií. Organizácia by preto mala:
  a) zabezpečiť, aby zariadenia podporujúce verejné služby boli konfigurované, prevádzkované a udržiavané v súlade s príslušnými špecifikáciami výrobcu;
  b) zabezpečiť, aby verejné služby boli pravidelne hodnotené z hľadiska ich kapacity pre potreby obchodného rastu a vzájomnej prepojenosti s inými podpornými verejnými službami.

Podporné služby

c) zabezpečiť, aby zariadenia podporujúce verejné služby boli pravidelne kontrolované a testované na zabezpečenie ich správneho fungovania;
d) v prípade potreby spúšťať poplachy na odhalenie porúch vo fungovaní verejných služieb;
e) v prípade potreby zabezpečiť existenciu viacerých zdrojov verejnej služby s odlišným fyzickým smerovaním;
f) zabezpečiť, aby zariadenia podporujúce verejné služby, ak sú pripojené do siete, boli v sieti oddelené od zariadení na spracovanie informácií;
g) zabezpečiť, aby zariadenia podporujúce verejné služby boli pripojené na internet iba v prípade potreby a len bezpečným spôsobom.

Je potrebné zabezpečiť núdzové osvetlenie a komunikačné prostriedky. Núdzové vypínače a ventily na odpojenie elektriny, vody, plynu alebo iných médií by mali byť umiestnené v blízkosti núdzových východov alebo miestností s vybavením. Kontaktné údaje pre prípad núdze majú byť zaznamenané a dostupné pracovníkom v prípade výpadku.

Bezpečnosť káblových rozvodov

Opatrenie

Káble prenášajúce napájanie, dáta alebo podporné informačné služby musia byť chránené pred odpočúvaním, rušením alebo poškodením.

Účel

Zabrániť strate, poškodeniu, krádeži alebo kompromitácii informácií a ďalších súvisiacich aktív, ako aj prerušeniu činností organizácie v súvislosti s napájacou a komunikačnou kabelážou.

Pokyny

Na zabezpečenie kabeláže by mali byť zvážené nasledujúce odporúčania:

- **a)** napájacie a telekomunikačné linky pripojené k zariadeniam na spracovanie informácií by mali byť, ak je to možné, vedené pod zemou alebo inak primerane chránené, napr. pomocou podlahových káblových chráničiek a inžinierskych stĺpikov; ak sú káble vedené pod zemou, treba ich chrániť pred náhodným prerezaním (napr. pancierovými rúrami alebo signalizáciou ich prítomnosti);

Bezpečnosť káblových rozvodov

b) oddelenie silových káblov od komunikačných káblov, aby sa predišlo rušeniu;
c) pri citlivých alebo kritických systémoch treba zvážiť ďalšie opatrenia vrátane:

1. inštalácie pancierových káblových rozvodov, uzamknutých miestností alebo skríň a poplašných zariadení na kontrolných a ukončovacích miestach;
2. použitia elektromagnetického tienenia na ochranu káblov;
3. pravidelných technických kontrol a fyzických prehliadok na detekciu neoprávnených zariadení pripojených ku káblom;
4. riadeného prístupu k prepojovacím panelom a rozvodným miestnostiam (napr. pomocou mechanických kľúčov alebo PIN kódov);
5. používania optických káblov;
   d) označovanie káblov na každom konci dostatočnými údajmi o ich zdroji a cieli, ktoré umožnia fyzickú identifikáciu a kontrolu káblov.

Je vhodné vyžiadať si odborné poradenstvo o tom, ako riadiť riziká vyplývajúce z incidentov alebo porúch kabeláže.

Údržba zariadení

Opatrenie
Zariadenie má byť správne udržiavané, aby bola zabezpečená dostupnosť, integrita a dôvernosť informácií.

Účel
Zabrániť strate, poškodeniu, krádeži alebo kompromitácii informácií a ďalších súvisiacich aktív, ako aj prerušeniu činnosti organizácie v dôsledku nedostatočnej údržby.

Pokyny
Na údržbu zariadení by mali byť zvážené nasledujúce odporúčania:

- **a)** vykonávať údržbu zariadení v súlade s odporúčanou servisnou periódou a špecifikáciami výrobcu;
  b) zaviesť a monitorovať program údržby v rámci organizácie;
  c) opravy a údržbu zariadení vykonávať len autorizovanými pracovníkmi údržby;
  d) viesť záznamy o všetkých predpokladaných alebo skutočných poruchách a o všetkých preventívnych a nápravných údržbách;

Údržba zariadení

- **e)** pri plánovaní údržby zariadení prijať vhodné opatrenia s ohľadom na to, či údržbu vykonávajú pracovníci na mieste alebo mimo organizácie; zabezpečiť, aby boli pracovníci údržby viazaní dohodou o mlčanlivosti;
  f) dohliadať na pracovníkov údržby pri výkone údržby priamo v priestoroch organizácie;
  g) autorizovať a riadiť prístup v prípade vzdialenej údržby;
  h) uplatniť bezpečnostné opatrenia pre aktíva mimo priestorov organizácie (pozri 7.9), ak je zariadenie obsahujúce informácie dočasne premiestnené mimo organizáciu za účelom údržby;
  i) dodržiavať všetky požiadavky na údržbu stanovené poisťovňou;
  j) pred opätovným uvedením zariadenia do prevádzky po údržbe vykonať kontrolu, aby sa zabezpečilo, že so zariadením nebolo manipulované a že správne funguje;
  k) uplatniť opatrenia na bezpečnú likvidáciu alebo opätovné použitie zariadenia, ak bolo rozhodnuté o jeho vyradení.

Bezpečná likvidácia alebo opätovné použitie zariadenia

- **Opatrenie**
  Časti zariadení obsahujúce pamäťové médiá majú byť skontrolované s cieľom zabezpečiť, aby všetky citlivé údaje a licencovaný softvér boli pred likvidáciou alebo opätovným použitím odstránené alebo bezpečne prepísané.

Účel
Zabrániť úniku informácií zo zariadení, ktoré majú byť zlikvidované alebo opätovne použité.

- **Pokyny**
  Pred likvidáciou alebo opätovným použitím je potrebné overiť, či zariadenie obsahuje pamäťové médiá.
  Pamäťové médiá obsahujúce dôverné informácie alebo informácie chránené autorským právom majú byť fyzicky zničené, alebo informácie na nich musia byť zničené, vymazané alebo prepísané pomocou techník, ktoré znemožňujú obnovu pôvodných dát – nie len pomocou štandardnej funkcie vymazania.
  Podrobné pokyny k bezpečnej likvidácii pamäťových médií, a k vymazávaniu informácií.

Bezpečná likvidácia alebo opätovné použitie zariadenia

Štítky a označenia identifikujúce organizáciu alebo klasifikáciu, vlastníka, systém či sieť majú byť pred likvidáciou odstránené – vrátane prípadov ďalšieho predaja alebo darovania na charitatívne účely.

- Organizácia má zvážiť odstránenie bezpečnostných opatrení, ako je riadenie prístupu alebo monitorovacie zariadenia, na konci nájomného vzťahu alebo pri sťahovaní z priestorov. Toto závisí od faktorov, ako sú:
  a) nájomná zmluva vyžadujúca uvedenie zariadení do pôvodného stavu;
  b) potreba minimalizovať riziko, že citlivé systémy (napr. zoznamy prístupov, videá alebo obrazové súbory) zostanú ďalšiemu nájomcovi;
  c) možnosť opätovného využitia týchto opatrení v nových priestoroch.

Bezpečná likvidácia alebo opätovné použitie zariadenia

Ďalšie informácie

Poškodené zariadenia s pamäťovými médiami môžu vyžadovať posúdenie rizika, aby sa určilo, či by ich časti mali byť fyzicky zničené, namiesto toho, aby boli posielané na opravu alebo štandardné vyradenie.
Informácie môžu byť kompromitované v dôsledku neopatrnej likvidácie alebo opätovného použitia zariadenia.

Okrem bezpečného vymazania disku sa riziko úniku dôverných údajov znižuje aj šifrovaním celého disku v prípade likvidácie alebo opätovného použitia zariadenia, za predpokladu, že:
a) šifrovací proces je dostatočne silný a zahŕňa celý disk (vrátane nevyužitého priestoru a dočasných súborov);
b) kryptografické kľúče sú dostatočne dlhé na odolanie útokom hrubou silou;
c) kryptografické kľúče sa považujú za dôverné (napr. nikdy nie sú uložené na tom istom disku).

Ďalšie odporúčania k šifrovaniu.

- Techniky bezpečného prepisu pamäťových médií sa líšia v závislosti od technológie pamäťového média a úrovne klasifikácie údajov. Používané nástroje na prepis majú byť overené, aby sa zabezpečilo, že sú vhodné pre daný typ pamäťového média.

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť!

Fyzická bezpečnosť, bezpečnosť prostredia a správa koncových zariadení

Personálne a fyzické opatrenia (Blok III)
Kurz: Manažér kybernetickej bezpečnosti

Ing. Martin Boroš, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Martin.boros@uniza.sk