MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 6
SOUBOR POSTUPŮ PRO MANAGEMENT BEZPEČNOSTI INFORMACÍ – FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)

esf evropský sociální fond v ČR | EVROPSKÁ UNIE | MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY | OP Vzdělávání pro konkurenceschopnost | UNIVERZITA OBRANY

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OBSAH

- ✓Zabezpečené oblasti.
  - ✓Fyzický bezpečnostní perimetr.
  - ✓Fyzické kontroly vstupu osob.
  - ✓Zabezpečení kanceláří, místností a prostředků.
  - ✓Veřejný přístup, prostory pro nakládku a vykládku.
- ✓Bezpečnost zařízení.
  - ✓Umístění zařízení a jeho ochrana.
  - ✓Podpůrná zařízení.
  - ✓Bezpečnost kabelových rozvodů.
  - ✓Údržba zařízení.
  - ✓Bezpečnost zařízení mimo prostory organizace.
- ✓Závěr

Literatura

ČSN ISO/IEC 27000 Datum vydání : 1.5.2010

Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

ČSN ISO/IEC 27001 Datum vydání : 1.10.2006

Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 / 17799 Datum vydání : 1.8.2006

Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.

1. Zabezpečené oblasti

Cílem je předcházet neautorizovanému fyzického přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.

Prostředky zpracovávající kritické nebo citlivé informace organizace, by měly být umístěny v zabezpečených zónách chráněných vymezeným bezpečnostním perimetrem s odpovídajícími bezpečnostními bariérami a vstupními kontrolami.

Tato zařízení by měla být fyzicky chráněna proti neautorizovanému přístupu, poškození a narušení.

Jejich ochrana by měla odpovídat zjištěným rizikům.

Zabezpečené oblasti

Při ochraně prostor by měly být používány bezpečnostní perimetry. **Nejdůležitější doporučení a opatření**:

a) měl by být jasně vymezen bezpečnostní perimetr;

b) perimetr budovy nebo oblasti obsahující prostředky pro zpracování informací by měl být v řádném stavu;

c) pro kontrolu fyzického přístupu do objektu nebo budovy by mělo být využíváno recepce či jiných prostředků;

d) fyzické bariéry by měly být tam, kde je to účelné;

e) požární dveře v bezpečnostním perimetru by měly být opatřeny elektronickým zabezpečovacím systémem a měly by být monitorovány;

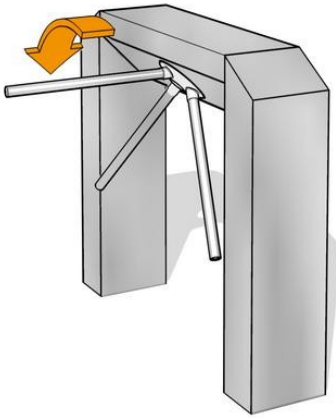
f) vnější dveře a dosažitelná okna by měla být chráněna vhodným detekčním systémem;

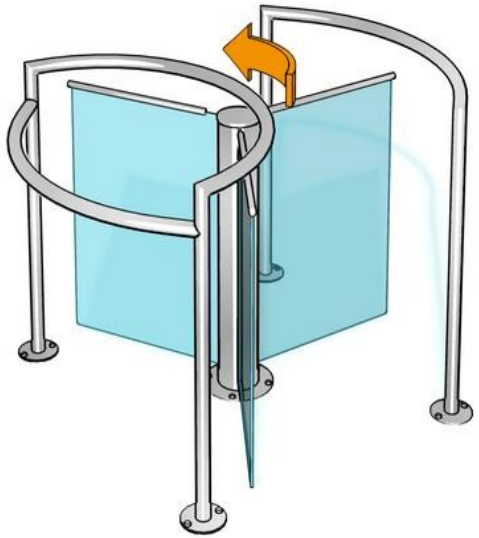
g) prostředky pro zpracování informací spravované organizací by měly být fyzicky odděleny od prostředků třetích stran.

Bezpečnostní perimetry

Při ochraně prostor by měly být používány bezpečnostní perimetry - bariéry jako například zdi, vstupní turniket na karty nebo recepce.

Turnikety jsou speciálním typem brány, který umožňuje, aby přes něj v jeden moment prošel vždy jen jeden člověk



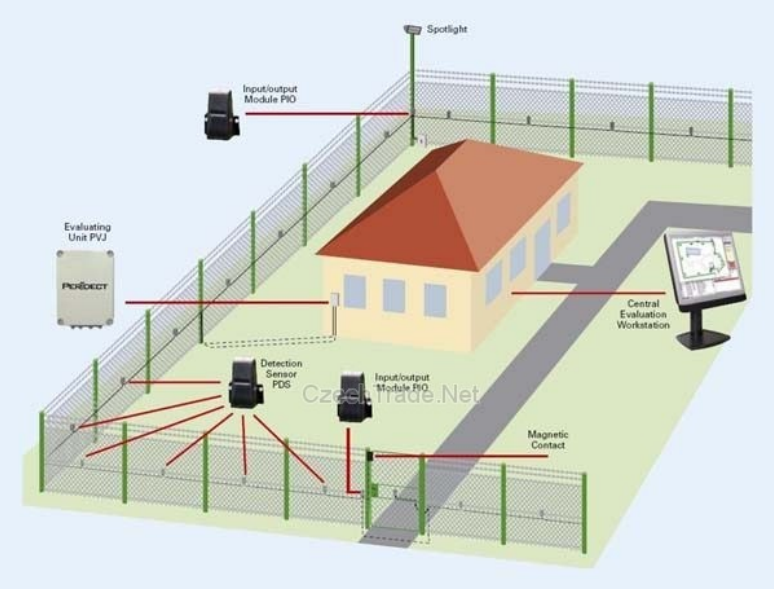


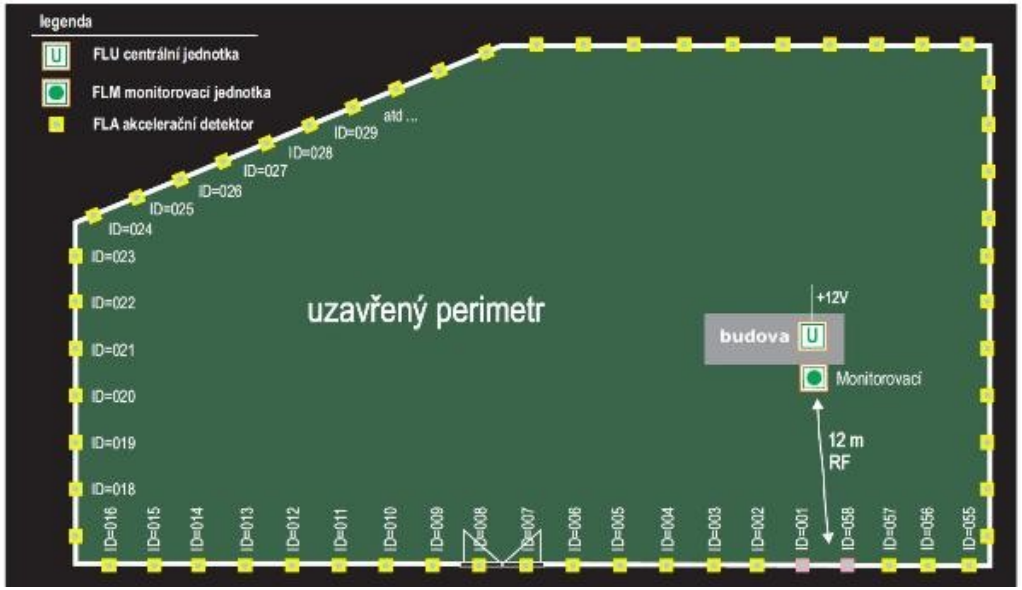
Bezpečnostní perimetry

Turnikety jsou speciálním typem brány, který umožňuje, aby přes něj v jeden moment prošel vždy jen jeden člověk

Perimetrický detekční systém

Perimetrický detekční systém pro ochranu objektů a oblastí před neoprávněným průnikem. Montáž na běžné oplocení - pletivové ploty, svařované dílce a další. Perimetrický detekční systém je vhodný pro rozsáhlé integrované bezpečnostní systémy umožňující střežení obvodového oplocení pomocí speciálních akceleračních tagů připevněných na pletivu či vstupních a vjezdových branách.





Fyzické kontroly vstupu osob

Měla by být zvážena následující opatření:

a) datum a čas příchodu a odchodu návštěvníků by měl být zaznamenán a návštěvníci by měli být pod stálým dohledem;

b) přístup do oblastí, kde se zpracovávají nebo jsou uloženy citlivé informace, by měl být kontrolován a umožněn pouze oprávněným osobám;

c) po všech zaměstnancích, smluvních a třetích stranách a návštěvnících by mělo být požadováno používat nějakou formu viditelné identifikace;

d) přístupová práva do zabezpečených oblastí by měla být pravidelně přezkoumávána a aktualizována a v případě potřeby zrušena.

Kamerový systém

Kamerový systém je určen pro monitorování vybraných venkovních nebo vnitřních prostor. Obraz z kamer je přenášen na monitor obsluhy nebo je ukládán pro budoucí využití, jako je dohledání záznamu kritické události. Záznam z kamerového systému může sloužit jako klíčový důkaz při dokazování trestné činnosti.

- Analogový kamerový systém
- IP kamerový systém

Analogový kamerový systém

Kamery s nízkým rozlišením přenášejí signál do záznamového zařízení analogově. Tam je signál digitalizován a ukládán na pevný disk. K záznamu a obrazu z kamer lze přistupovat případně i přes síť nebo internet. Většina systémů umožňuje i připojení pomocí chytrého mobilního telefonu. Existuje velmi široká škála kamer i záznamových zařízení. Tyto systémy jsou většinou levné, ale nevýhodou je nízké rozlišení obrazu.

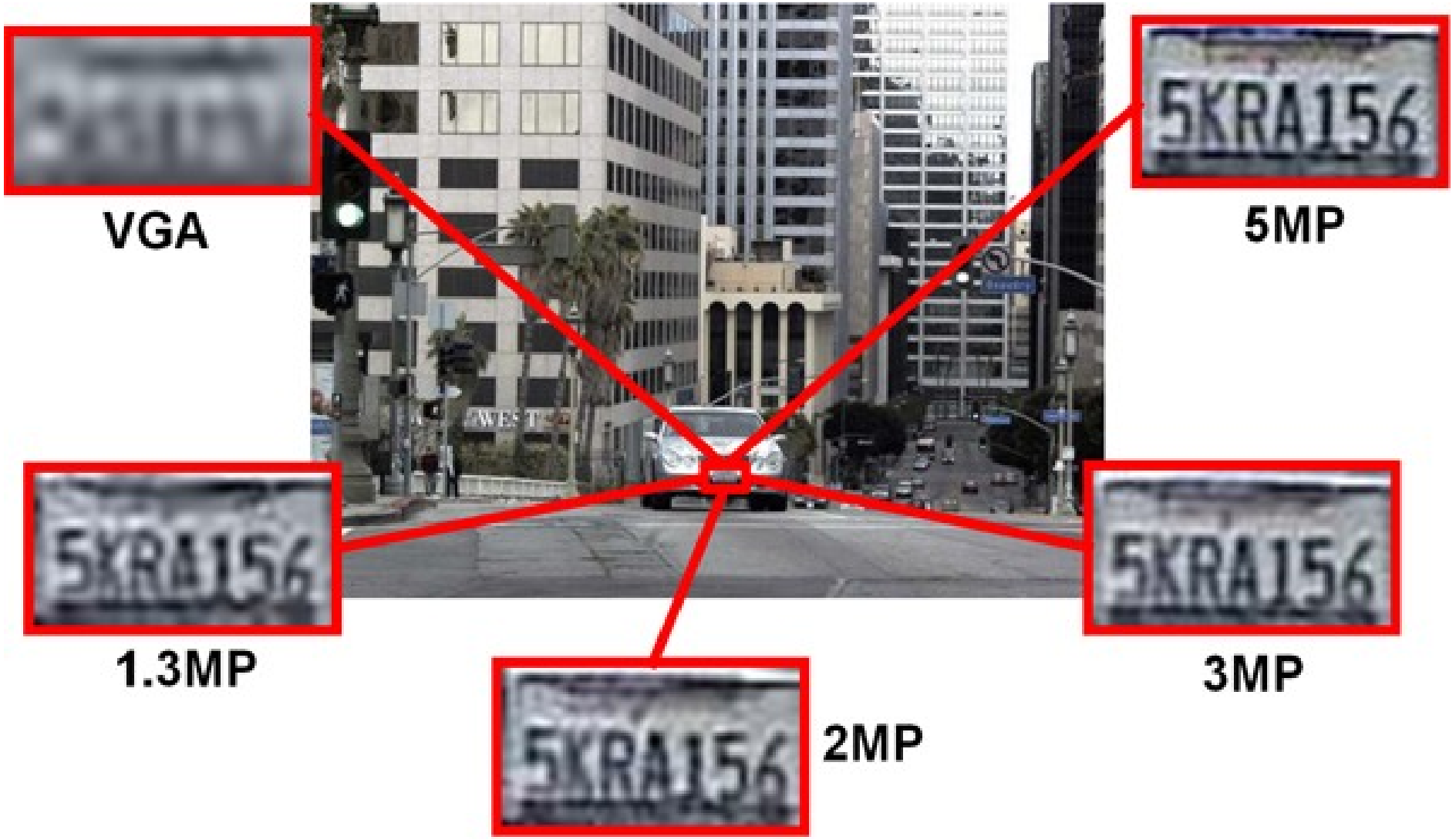
IP kamerový systém

Kamery s vysokým rozlišením v řádu několika megapixelů jsou k záznamovému zařízení připojeny přes síť ethernet. Záznam je prováděn na místní pevný disk nebo na vzdálené úložiště. K obrazu z kamer a k záznamu lze přistupovat přes síť nebo chytrý mobilní telefon. I zde existuje velmi široká škála kamer i záznamových zařízení. Tyto systémy jsou většinou dražší než analogový systém, ale poskytují nesrovnatelně větší možnosti. Nevýhodou těchto systémů jsou vyšší nároky na přenosovou rychlost sítě, do níž jsou kamery připojeny.

Vlastnost	Analogový systém kamer	IP systém kamer
Rozlišení kamer	0,4 MPix	**Standardně 1,3 - 2 MPix**
Citlivost kamer	**Vyšší**	Nižší
Snímková frekvence	25 FPS	**6 - 60 FPS**
Detekce pohybu v obraze	Ano (často jen při použití záznamového zařízení)	**Ano**
Inteligentní analýza	Ne	**Ano**
Lze sledovat přes internet a na mobilních zařízení	Většinou ano (jen při použití záznamového zařízení)	**Ano**
Nároky na diskovou kapacitu	**Nižší** Jedna kamera při plné snímkové frekvenci spotřebuje cca 20GB denně	Vyšší Jedna kamera v rozlišení 2MPix při plné snímkové frekvenci vyžaduje cca 100GB denně
Kabeláž	**Vyhrazená** Kabely již nelze využít k přenosu jiných informací, k jedné kameře někdy musí vést několik kabelů	**Sdílená** Kabely lze ji využít i k jiným účelům (např. pro připojení počítačů). Jeden kabel často přenáší několik různých typů dat a může sloužit i k přenosu napájení (PoE)
Úroveň zabezpečení	Nižší	**Vyšší**
Standardizace	**Vyšší**	Nižší
Finanční nároky	**Nižší**	Vyšší

Rozlišení

Určuje, kolika obrazovými body (pixely) je tvořen výsledný obraz, obvykle se udává v tzv. mega-pixelech - tzn. počet miliónů pixelů; zkratka je MPix.



Rozlišení

Určuje, kolika obrazovými body (pixely) je tvořen výsledný obraz, obvykle se udává v tzv. mega-pixelech - tzn. počet miliónů pixelů; zkratka je MPix.

Zabezpečení kanceláří a prostředků

Pro zabezpečení kanceláří, místností a zařízení by měla být zvážena následující doporučení:

a) v úvahu by měly být vzaty odpovídající předpisy a normy pro bezpečnost a ochranu zdraví při práci;

b) důležitá zařízení by měla být situována tak, aby nebyla veřejně přístupná;

c) tam, kde je to použitelné by měly budovy být nenápadné, aby co nejméně naznačovaly jejich účel;

d) adresáře a interní telefonní seznamy by neměly být přímo přístupné veřejností.

Veřejný přístup, prostory pro nakládku a vykládku

Prostory pro nakládku a vykládku a další místa kudy se mohou neoprávněné osoby dostat do prostor organizace, by měly být **kontrolovány** a pokud možno by měla být **izolovány** od prostředků pro zpracování informací tak, aby se zabránilo neoprávněnému přístupu k nim.

Přístup do prostor pro nakládku a vykládku by měl být umožněn pouze osobám již **známým a oprávněným zaměstnancům**.

Došlý materiál by měl být vždy **prozkoumán** a při převzetí zaevidován.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Práce v zabezpečené oblasti

Zaměstnanci jsou obeznámeni v nutném rozsahu o zpracovávání citlivých dat na pracovišti, a však bez dalších podrobností.

Zamezit vnášení a využívání externích nahrávacích audio vizuálních prostředků bez povolení.

Projekt fyzické bezpečnosti

Pro přístupu k utajovaným informacím dle § 20 písm. a) i b) zákona č. 412/2005 Sb., tj. i pro poskytování, ukládání a vznik utajovaných informací, musí být pro zabezpečenou oblast (objekt) zpracován i **projekt fyzické bezpečnosti**,

Obsah projektu fyzické bezpečnosti specifikuje § 32 zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění a podrobnosti stanoví Vyhláška NBÚ č. 528/2005 Sb. o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011Sb.

Projekt fyzické bezpečnosti

Pro nejnižší **stupeň utajení "Vyhrazené"** projekt fyzické bezpečnosti obsahuje:

- určení objektů, zabezpečených oblastí, včetně jejich hranic a tříd zabezpečených oblastí,
- způsob použití opatření fyzické bezpečnosti,
- technickou dokumentaci fyzické bezpečnosti (výkresová dokumentace, dokumentace certifikovaných i necertifikovaných technických prostředků).

Pro **vyšší stupně utajení** je obsah projektu fyzické bezpečnosti následující:

- vyhodnocení rizik,
- určení kategorií objektů, zabezpečených oblastí a jednacích oblastí včetně jejich hranic a určení tříd zabezpečených oblastí a jednacích oblastí,
- způsob použití opatření fyzické bezpečnosti,
- provozní řád,
- plán zabezpečení objektů, zabezpečených oblastí a jednací oblasti v krizových situacích.

2. Bezpečnost zařízení

Cílem je předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiva přerušení činností organizace. Zařízení by měla být fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů.

Ochrana zařízení je nezbytná jak pro snížení rizika neautorizovaného přístupu k datům, tak k zajištění ochrany proti ztrátě nebo poškození. Pozornost by měla být věnována také jejich umístění a likvidaci.

Na ochranu proti možnému ohrožení nebo neautorizovanému přístupu a na ochranu podpůrných prostředků, například dodávky elektrické energie a infrastruktury kabelových rozvodů, mohou být požadována zvláštní opatření.

Umístění zařízení a jeho ochrana

Zařízení by měla být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup:

- zařízení by měla být umístěna tak, aby byl minimalizován nadbytečný přístup do pracovních prostor,
- prostředky pro zpracování a ukládání citlivých dat by měly být umístěny tak, aby bylo sníženo riziko možného odezírání informací,
- ve všech budovách by měla být nasazena ochrana proti blesku,
- pro zařízení ve výrobním prostředí by mělo být zváženo používání zvláštních ochran.

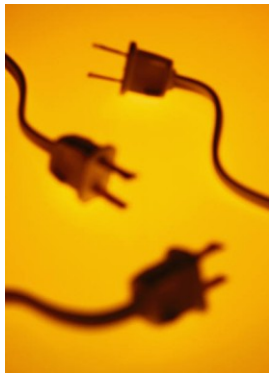
Podpůrná zařízení

Zařízení by mělo být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

Veškeré podpůrné služby jako elektřina, dodávky vody, kanalizace, topení/ventilace a klimatizace by měly být přiměřené systému, který podporují.

Pro elektrická zařízení zajišťující kritické operace organizace je doporučeno použití záložních zdrojů UPS.

Telekomunikační zařízení by mělo být k poskytovateli služby připojeno nejméně dvěma různými cestami.



esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

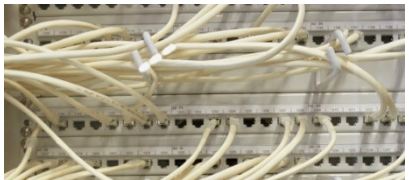
Bezpečnost kabelových rozvodů

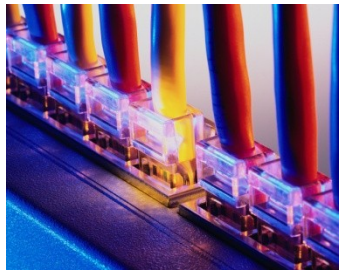
Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, by měly být chráněny před odposlechem či poškozením.

Napájecí a telekomunikační linky připojené k prostředkům IT by měly vést v podzemí nebo by měly být chráněny jiným vhodným způsobem.

Kabely a zařízení by měly být zřetelně označeny, aby se zabránilo možnosti záměny v případech provádění oprav poškozených kabelů.

Pro snížení pravděpodobnosti vzniku chyb by měl být udržován seznam propojení.





esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Údržba zařízení

Zařízení by mělo být správně udržováno pro zajištění jeho stálé dostupnosti a integrity:

a) zařízení by měla být udržována a provozována v souladu s doporučeními dodavatele;
b) opravy a servis zařízení by měly provádět pouze oprávněné osoby;
c) o všech závadách nebo podezřelých chybách by měly být pořízeny záznamy, stejně tak o preventivních prohlídkách a opravách;
d) v případech, kdy údržbu zařízení neprovádí prověřené osoby, by z něj měly být odstraněny veškeré citlivé informace.

Bezpečná likvidace a znovu využití vybavení

Všechno vybavení obsahující paměťové médium musí být zkontrolováno, že neobsahuje citlivá data ani licencovaný software.

Všechna zařízení, která obsahují citlivou informaci, by měla být fyzicky zničena nebo informace musí zničena, smazána nebo přepsána takovým způsobem, že původní informace bude nadále nečitelná.

Bezpečnost zařízení mimo prostory organizace

Použití prostředků pro zpracování informací, bez ohledu na jejich vlastníka, mimo budovy organizace by mělo podléhat schválení vedením organizace. Při práci mimo prostory organizace by měla být zvážena následující doporučení:

a) při cestách mimo organizaci by zařízení a média ve veřejných prostorách neměla být ponechána bez dozoru. Přenosný počítač by měl být přepravován jako příruční zavazadlo a v rámci možností ukrýván;

b) měly by se dodržovat pokyny výrobce týkající se ochrany zařízení;

c) pro práci doma by měla být určena vhodná opatření na základě hodnocení rizik, například uzamykatelné skříňky, pravidlo prázdného stolu, kontrola přístupu k počítači a zabezpečení spojení s kanceláří;

d) zařízení používané mimo prostory organizace by mělo být pojištěno.

ZÁVĚR

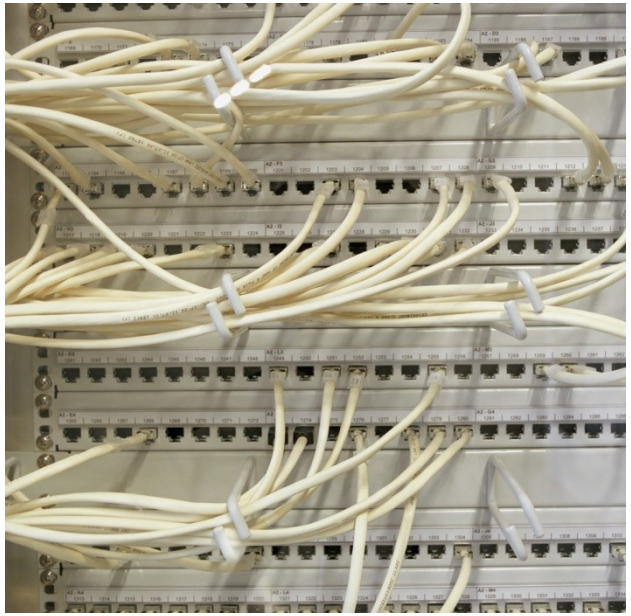
Prostředky zpracovávající kritické nebo citlivé informace organizace, by měly být umístěny v zabezpečených zónách chráněných vymezeným bezpečnostním perimetrem s odpovídajícími bezpečnostními bariérami a vstupními kontrolami.

Tato zařízení by měla být fyzicky chráněna proti neautorizovanému přístupu, poškození a narušení.

Jejich ochrana by měla odpovídat zjištěným rizikům.

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ