Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Fyzická bezpečnosť

Jozef Stanko

Jún 2013

KPMG
cutting through complexity™

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Motivácia

Čo vlastne chránime?

- Fyzické aktíva (hardvér, komunikačné prostriedky, výrobné prostriedky, budovy,..)
- Informácie/dáta (Know-how)
- Softvér
- Ľudia
- Reputácia

Prečo to chránime?

- Predstavujú pre nás hodnotu, ich zneužitie, odcudzenie, alebo znehodnotenie je kritickým incidentom a stratou tejto našej hodnoty.
- To čo dnes vyzerá ako nevinný incident, môže v spojení s inými drobnými incidentmi spôsobiť stratu zisku/reputácie/know-how

Ako to chránime?

- Riadením IB vo všetkých jej oblastiach, pre účely tejto prezentácie najmä použitím prostriedkov fyzickej ochrany v rámci chráneného objektu a priestoru

KPMG
cutting through complexity™

Riadenie bezpečnosti

Ochrana prístupu – identifikácia a autentifikácia a kontrola prístupu používateľa ku zdrojom

- Čo osoba vie,
- Čo osoba má,
- Čo osoba je.

Ciele fyzickej ochrany IKT

- Zabezpečenie prístupu do priestorov kde sa nachádzajú IKT len oprávneným osobám
- Zabezpečenie voči neoprávnenej činnosti
- Minimalizácia rizika nepredvídaného útoku
- Minimalizácia strát a obnova v prípade, že dôjde k incidentu

Základné požiadavky na prostredie

- Ľudia potrebujú pracovné podmienky nezlučiteľné s tými, ktoré sú vhodné pre IKT
- Ochrana najmä voči nasledovným typom hrozieb:
    - prírodné vplyvy, poruchy infraštruktúry, zemetrasenie, technické poruchy, úder bleskom/anomálie v prísune elektrickej energie, sabotáž, úmyselné poškodenie, krádež

Prehľad základných prvkov fyzickej bezpečnosti

Súhrn opatrení na priame zabezpečenie objektu vytvorením systému zábran, prekonanie ktorých vyžaduje určitý čas, použitie nástrojov a prostriedkov, zručnosť páchateľa a pod.

Mechanické zábranné prostriedky (MZP)

- „klasická ochrana“ -„pasívna bezpečnosť“
- Ploty, brány, bariéry, steny, dvere, okná, trezory (úschovné objekty), zámky, bezpečnostné osvetlenie
- Bezpečnostné triedy odolnosti MZP, kategória náradia, odporový čas
- Celok je len tak bezpečný, ako bezpečný je jeho najslabší článok

Technické zabezpečovacie prostriedky (TZP)

- monitory pohybu, monitory požiaru, protipožiarne zariadenia, bezpečnostné kamery, detekčné systémy, EPS

Podporná infraštruktúra

- Dvojité podlahy , klimatizácia, UPS, dvojité napájanie , chladenie a konektivita

Chránený objekt a chránený priestor

Bezpečnostný perimeter

- je ohraničený mechanickými zábrannými prostriedkami pod kontrolou snímačov (detektorov) elektrického zabezpečovacieho systému (EZS)

Chránený objekt

- budova alebo iný stavebne alebo inak ohraničený priestor, ktorý je záujmom ochrany

Chránený priestor

- je stavebne alebo inak ohraničený priestor vo vnútri objektu, ktorý je záujmom ochrany

Umiestňovanie a prístup k IKT

Umiestňovanie IKT

- V priestore ohraničenom bezpečnostným perimetrom
- Zóny a úrovne
  - Zóna je plošné rozdeľovanie chránených priestorov

Prístup k IKT

- Akcia vstupu dovnútra alebo výstupu von zo zabezpečovaného a ovládaného priestoru
- Prístup verejnosti limitovaný tak, aby nedošlo k narušeniu chránenej zóny
- Prístup údržby a zodpovedných osôb, ktoré majú zodpovednosť za službu v strážených objektoch a po vyhlásení poplachu za prijatie príslušných opatrení
- Prístup externých špecialistov - ich prístup kontroluje a je časovo a zónovo limitovaný v rámci opatrení režimovej ochrany

Všeobecné opatrenia

Všeobecné opatrenia na ochranu dôvernosti informácií

- Fyzické riadenie prístupu
- „Čistý stôl“ a „Čistá obrazovka“

Práca mimo priestorov organizácie, bezpečnosť zariadení mimo priestorov organizácie

- Notebook v exponovanom prostredí pripevnený o pevný predmet káblovým zámkom
- Šifrovanie dát na pevnom disku a prenosných médiach
- Ochrana a zabezpečenie „chytrých“ telefónov

Elektromagnetické vyžarovanie (EMV)

- kompromitujúce vyžarovanie, ktoré ak je zachytené a analyzované, prezradí vysielanú, prijímanú alebo iným spôsobom spracovávanú informáciu
- väčší kontrolovateľný priestor, priestor v podzemných podlažiach, obklopený ďalšími stenami, bez stavebných otvorov, steny väčšej hrúbky, resp. viacero stien za sebou z kari rohože s menšími okami

Bezpečnostné osvetlenie

- s odradzujúcim účinkom proti potenciálnemu narušiteľovi, najmä ochrana perimetra

Fyzická bezpečnosť dátových centier (1/2)

Tier 1 - Základný: dostupnosť 99.671%

- Náchylné na poruchy pri plánovanej aj neplánovanej aktivite
- Jednocestné napájanie elektrickou energiou a jeden prívod chladenia, žiadna redundancia
- Môže, ale nemusí mať dvojitú podlahu, UPS, alebo diesel generátor
- Implementácia trvá tri mesiace
- Súhrnný ročný výpadok 28.8 hodiny
- Musí byť úplne vypnutý pri preventívnej údržbe

Tier 2 - Redundantné časti: dostupnosť 99.741%

- Menej náchylné na poruchy pri plánovanej a neplánovanej aktivite
- Jednocestné napájanie elektrickou energiou a jeden prívod chladenia, obsahuje redundantné komponenty
- Zahŕňa dvojitú podlahu, UPS aj diesel generátor
- Implementácia trvá 3-6 mesiacov
- Súhrnný ročný výpadok 22 hodín
- Údržba prívodu elektrickej energie a ostatných častí infraštruktúry vyžaduje vypnutie

Fyzická bezpečnosť dátových centier (2/2)

Tier 3 - Paralelne servisovateľný: dostupnosť 99.982%

- Plánované aktivity bez prerušenia služby. Neplánované aktivity stále spôsobujú výpadok
- Viaccestné napájanie elektrickou energiou a viaccestný prívod chladenia, obsahuje redundantné komponenty,
- Implementácia trvá 15-20 mesiacov
- Súhrnný ročný výpadok 1.6 hodiny
- Zahŕňa dvojitú podlahu, redundanciu dostatočnú na to, aby bolo možné prepnúť prevádzku na jednu časť, kým sa realizuje údržba na druhej časti

Tier 4 - Tolerancia voči poruchám: dostupnosť 99.995%

- Plánované aktivity bez prerušenia služby a dátové centrum dokáže prekonať najmenej jeden kritický incident
- Viaccestné aktívne napájanie elektrickou energiou a viaccestný prívod chladenia, obsahuje redundantné komponenty
- Implementácia trvá 15-20 mesiacov
- Súhrnný ročný výpadok 0.4 hodiny

Legislatíva z oblasti fyzickej bezpečnosti

Zákon o ISVS

- zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov

Štandardy minimálneho technického zabezpečenia pre ISVS

- Výnos MFSR č. 312/2010 o štandardoch pre ISVS - *§34 Fyzická bezpečnosť a bezpečnosť prostredia*

Pre oblasť ochrany utajovaných skutočností:

- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov
- Vyhláška NBÚ č. 336/2004 Z.z. o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ č. 337/2004 Z.z. podrobnosti o certifikácii mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov
- Vyhláška NBÚ č. 314/2006 Z.z. ktorou sa mení a dopĺňa predošlý 337/2004 Z.z.
- Vyhláška NBÚ č. 315/2006 Z.z. ktorou sa mení a dopĺňa vyhláška Vyhláška NBÚ č. 336/2004
- Vyhláška NBÚ č. 479/2011 Z.z. ktorou sa mení a dopĺňa 337/2004 Z. z.

Čo povedať na záver?

Čo zostáva povedať?

- FOB operuje s ochranou pred nepredvídateľnými rizikami súvisiacimi s prírodnými vplyvmi ako sú zemetrasenie a záplava až po krádež hmotného majetku a vážne kriminálne činy
- S širokou paletou hrozieb sa musí rátať pri aplikovaní princípov riadenia fyzickej bezpečnosti podľa platných štandardov, noriem a metodických usmernení
- Dopady pri nedostatočnej implementácii opatrení fyzickej bezpečnosti sa môžu týkať poškodenia renomé organizácie a môžu sa násobiť s nemenej významnými stratami ako je finančná strata súvisiaca s narušením integrity objektu
- Chránime predovšetkým dôležité aktíva organizácie a bránime sa ňou proti hrozbe potenciálneho zneužitia citlivých informácií, informačných a fyzických aktív

Priestor na otázky:

- Aké sú vaše skúsenosti s aplikovaním bezpečnostných opatrení v podmienkach MFSR?
- Čo by ste vyzdvihli ako pozitívum a čo naopak zmenili?
- Iné???