Metody fyzické ochrany

fyzická ochrana se snaží eliminovat případnou hrozbu ještě dříve, než přijde do přímého kontaktu s vlastním výpočetním systémem
primární nebezpečí která fyz. ochrana pokrývá můžeme rozdělit:

- přírodní katastrofy
- vandalové
- nehody
- ostatní vnější vlivy
- cílevědomí pachatelé

a dále vytváří předpoklady pro aplikaci dalších protiopatření

… smyslem je vytvořit uzavřené prostředí (TCB), ve které jsme schopni zajistit požadované vlastnosti prostředí odpovídající bezpečnostní politice

Přírodní katastrofy

není jim možné předcházet, je třeba se soustředit na omezení možného odpadu a na odstranění případných následků

Záplavy

v podstatě dvou druhů
stoupající voda - většinou bývá dost času odstavit systém a přinejmenším datové nosiče přesunout do bezpečí. Pro tyto účely by každá komponenta systému měla být jasně vyznačen stupeň důležitosti, aby s odsunem mohli efektivně pomáhat i nekvalifikovaní pracovníci.
padající voda - např. poruchy potrubí, izolací apod. Tyto záplavy bývají velmi rychlé, v první fázi stačí vhodný nepromokavý kryt a následný odsun zařízení. Opět vhodné vyznačení stupňů důležitosti komponent.

Požáry

představuje často nebezpečí nejen pro techniku, ale i pro obsluhující personál
je vhodné mít vyzkoušen postup zahrnující bezodkladné odstavení systému a evakuaci personálu a životně důležitých komponent systému
je třeba vhodně volit automatické protipožární systémy chránící prostory výpočetního systému, vhodné je umístit nejdůležitější části systému v prostorách s vysokou pasivní požární bezpečností

Ztráty napájení

pro nejdůležitější části systému je nutné zajistit náhradní zdroje energie, které jsou v případě výpadku hlavního napájení schopny dostatečně rychle zajistit dodávky elektřiny
na kratší dobu jsou to různé akumulátory a UPS zdroje, v případě potřeby překonávat delší výpadky pak agregáty na výrobu el.energie
důležité jsou rovněž filtry a přepěťové ochrany chránící zařízení před výkyvy napětí, blesky apod.

Chlazení

některé komponenty jsou citlivé na teplo, při ztrátě chlazení může dojít k jejich zničení
větší systémy nelze bez odpovídajícího chlazení provozovat ani krátkodobě, příslušná technologie se tak může stát klíčovou komponentou

Hmotnost

serverová technologie může vyžadovat speciální podlahy se zvýšenou nosností, může se stát problémem zejména při zařizování záložního centra po havárii
jindy lze hmotnost využít jako bezpečnostního mechanismu

Prašnost, vibrace, další vlivy

... mohou i výrazným způsobem omezovat životnost komponent, případně zvyšovat poruchovost

Prostorová ochrana

prostředky umožňující zabránit potenciálním útočníkům ve vstupu do prostor, kde jsou instalovány důležité komponenty systému, nebo vnesení potenciálně nebezpečných předmětů či detekci takové skutečnosti, případně může být cílem zabránění opuštění prostoru, respektivě vynesení komponent
předmětem útoku můžou být:

- vlastní počítače
- výměnná záznamová media
- části počítačů (myši, světelná pera, …)
- vytištěné senzitivní materiály
- části síťové technologie,
- klíčoví pracovníci

metody ochrany:

Stráže

měly by být k dispozici nepřetržitě, musí osobně znát všechny pracovníky, nebo musí umět rozpoznat oprávněnou osobu jiným způsobem - např. dle tokenu
stráž musí provádět záznam o pohybu všech osob
problémem jsou zaměstnanci, se kterými byl nedávno rozvázán pracovní poměr a celková míra spolehlivosti stráží

náhradou nebo doplňkem stráží mohou být různé turnikety a přechodové komory vybavené zařízeními pro identifikaci osob nebo tokenů

Elektronická prostorová ochrana

- dveřní a okenní kontakty - detekují otevření
- otřesové hlásiče - detekují rozbití nebo proražení střežené plochy - skla, příčky, přepážky, …
- vodičové desky, drátěné sítě - slouží k detekci průrazů ve stěnách, podlahách apod.
- kontaktní matice - při instalaci pod podlahové krytiny slouží k detekci vstupu osob do chráněného prostoru
- Mikrovlnné, ultrazvukové, infračervené detektory - reagují na změnu rep. přerušení svazku příslušného záření
- zvukové hlásiče - reagují na specifické zvuky jako řezání, vrtání, šroubování, …
- kyvadlové hlásiče - reagují na otřesy a vychýlení z původní roviny

k ochraně jednotlivých předmětů lze použít obrazových vah, závěsů apod.
vhodným prostředkem v mnoha případech je průmyslová televize, zejména v kombinaci se záznamem snímaného obrazu

Detekce výstupu

vhodnou metodou je pokoušet se odhalit člověka odnášejícího část vybavení
prostředky jsou obdobné, jaké se používají v obchodních domech - různé nálepky či přívěsky, které lze snadno detekovat

Likvidace medií se senzitivními informacemi

je nutné mít k dispozici prostředky ke zničení nebo znehodnocení medií před jejich exportem z chráněného perimetru, nikdy není jasné, kam se dostanou

Zkartovače

existují v mnoha verzích pro nasazení v různých stupních zabezpečení, navzájem se liší jemností a způsobem provádění skartování

slouží především k ničení papírových dokumentů, dále disket pásek ze streamerů, kazet, barvicích pásek z úderových tiskáren

Přepisování magnetických medií

prosté smazání souboru většinou vede pouze k odstranění záznamu o jeho existenci, proto je nutné zajistit skutečné fyzické přepsání původních dat, pro větší stupeň bezpečnosti několikanásobné
metoda je zdlouhavá a ne úplně bezpečná

Degaussery

přístroj vygenerováním silného elektromagnetického pulsu dokáže zničit původní magnetické pole
ani v tomto případě nejde o zcela spolehlivou metodu vhodnou pro nasazení v nejvyšších stupních utajení

Odpovědnost za zabezpečení

celkovou odpovědnost má vedení organizace, lze ji rozdělit na odpovědnost za návrh bezpečnostní strategie a na odpovědnost za dodržování bezp. opatření
důležitou součástí bezpečnosti jsou opakované namátkové kontroly

Elektromagnetické vyzařování

… je způsobeno změnou proudu ve vodiči
problémem je vyzařování nejrůznějších částí počítačů, zejména monitorů a přenosových linek, důležité informace mohou unikat i naindukováním do napájecích obvodů zařízení
odposlech elmg. záření začasté není možné kriminalizovat a je nutno se vyrovnat s faktem, že jej útočník provádí
metody ochrany:

- Vzdálenost - intenzita vyzařování klesá se čtvercem vzdálenosti
- Zmatení - množství podobných signálů ztěžuje odposlech, je možno generovat záření podobných vlastností jako vyzařování výpočetního zařízení, nebo umístit více vyzařujících zařízení blízko sebe
- Speciální vybavení - je možné zakoupit součásti vyvinuté tak, aby jejich vyzařování nepřekračovalo jistou únosnou mez
- Vhodné umístění - alternativou nákupu nevyzařujících zařízení je umístění standardních zařízení v prostorách, které zamezují šíření záření - jde o různé schránky, skříně případně celé stíněné místnosti

Obnova provozu - dostupnost

pří ztrátě či poškození celého, nebo části IS je nezbytné co nejdříve nahradit (je-li to možné) ztracené informace a služby a obnovit činnost v -pokud možno- původním rozsahu
není možné mít stále zálohy všech částí výpočetního systému, je třeba hledat kompromis mezi proveditelností záloh a jejich aktuálností a úplností
účinné zálohování musí být součástí globální bezpečnostní strategie, musí vycházet z celkového hodnocení bezpečnostní situace
kromě prvotní funkce zotavení z chyb poskytuje dobře navržený systém záloh též prostředky k vytvářená archivních kopií různých stadií zpracovávaného projektu (viz. zpráva konfigurací)
obecným řešením jsou „zálohy“

Uživatelé

v běžném případě nejsou zálohy pro chod systému potřebné, pouze zdržují, nejsou konstruktivní
většina uživatelů nechápe jejich důležitost, často jsou dlouhodobými zkušenostmi utvrzováni v přesvědčení, že havárie nenastávají

Mechanismus pro vytváření záloh

- musí být schopen provádět zálohy na co možná nejrůznější zařízení
- vlastní zálohy by měly být uloženy v nějakém standardním formátu
- je nezbytná verifikace vytvořené záložní kopie
- žádoucí je komprese, deduplikace ukládaných dat - přináší zrychlení a menší objem záložních dat
- důležitá je kryptografická ochrana záloh, aby mohly být ukládány mimo chráněné prostory
- zálohovací SW by měl používat mechanismus pro korekci chyb - vede ke zvýšení pravděpodobnosti, že zálohu se podaří přečíst a obnovit původní data
- mělo by být možno specifikovat, která data mají být (kdy) zálohována
- SW by měl vytvářet podrobný audit o své činnosti
- vlastní SW by měl být schopen běžet na co největším počtu HW platforem
- zálohovací SW by měl být před ostrým nasazením důkladně otestován, je vhodné znát názor uživatelů
- nejčastější použití záloh spočívá v přenesení a obnově dat na jiný funkční stroj
- úspěšný přístup k zálohám by měl být vázán na zadání hesla

Záložní media

výměnná media

- USB disky - snadno dostupné levné řešení, nevýhodnou mizivá kapacita
- pásky - dodávají se v kapacitách od stovek GB až jednotky TB, patrně nejrozšířenější záložní medium, nutno používat skutečně kvalitní materiál
- WORM disky – dnes diskutabilní pro dlouhodobé zálohy a pořizování archivních kopií, velmi dobrá cena za byte, relativně nejistá spolehlivost, malá kapacita
- hard copy - může být za jistých podmínek vhodná pojistka, jistě lepší, než nemít data vůbec ☺

Nevýměnná media

- další disk - důležitá data jsou kopírována na další disk, jednoduché, rychlé, nechrání před zničením celého počítače, nebo jeho odcizením atp.
- disk mirroring - zápisy na jednom disku jsou automaticky prováděny i na druhém disku - opět chrání pouze před chybami disku, výhodou je transparentnost a on-line zotavení z chyby
- duplexing - dva stroje si udržují přesně stejný obsah paměti a synchronně provádějí veškeré operace, při výpadku prvního stroje automaticky přebírá jeho funkci záložní počítač - velmi drahé řešení, opět plně transparentní
- síť - zálohování lze provádět kopírováním dat na jiný počítač zapojený v síti

Vzdálená úložiště

- různé formy remote kopií dat – nutno zvážit, proti jakému druhu incidentu jsou relevantní, diskutabilní doba zotavení

Zálohy hardware

je nutné být schopen vyrovnat se dostatečně rychle s chybou technického vybavení - tedy buď mít k dispozici záložní systém, nebo alespoň kritické součástky, případně mít možnost vadnou součástku nahradit částí jiného stroje
řešením též smlouva o servisních zásazích s dodavatelem technologie
existují firmy, provádějící záchranu dat z havarovaných zařízení - tyto výkony však bývají drahé

Software

- ze všech medií s instalacemi nového sw. by měla být neprodleně pořízena alespoň jedna kopie
- originální instalace by měla být po celou dobu chráněna proti zápisu a ihned po pořízení kopií uložena na bezpečném místě
- vlastní instalace probíhá z pořízených kopií

tyto zásady ztrácejí naléhavost v souvislosti s rozšiřováním instalací na CDROM

Zásady pro pořizování záloh

pravidla pro pořizování záloh závisí na konkrétní situaci - jak často dochází k změnám dat, denní objem nových dat, důsledky případné ztráty dat, atd.

Data nebo programy

ztráta dat je vždy velmi problematické, znovupořízení dat může být obtížné, nebo dokonce nemožné
naproti tomu software je zpravidla možno znovu nainstalovat, což však zabere nějaký čas, navíc vytvoření dobré konfigurace může trvat velmi dlouho
konfigurační soubory by tedy měly být zálohovány společně s daty

Typy záloh

pokud máme k dispozici dostatek místa, je vhodné provádět zálohu komplet všech dat a programů
dříve častý model Grandfather-Father-Son - tři cyklicky používané archivní kopie, nejnovější kopie vždy vytvořena na mediích po nejstarší kopii, případně nejstarší kopie je uložena na bezpečném místě
alternativou je provádění kompletní zálohy vždy po určitém čase a v mezidobí pořizovat pouze zálohy změněných souborů
v současné době se zálohování soustřeďuje na objekty příslušné úrovně IS (OS, DB, aplikační server), systémy řízení zálohovacího mechanismu umožňují sofistikovaná schémata zálohování pracující s jednotlivými zálohovanými objekty namísto celých setů záloh
četnost těchto částečných záloh může být závislá na důležitosti zálohovaných dat

Uložení záložních kopií

význačné záložní kopie (např. záloha z konce týdne, záloha při ukončení fáze projektu, …) by měly být uloženy na bezpečném místě vzdáleném od místa, kde je instalován výpočetní systém
oddělené uložení kopií chrání proti následkům přírodních katastrof, zlodějům, teroristům apod.

přivezení kopií ze vzdáleného místa uložení poskytne personálu čas pro překonání prvotního stresu a provedení racionálního rozboru situace

místo uložení záložních kopií by mělo být zajištěno proti přírodním katastrofám, mělo by pro uložené materiály zajišťovat stabilní prostředí, je vhodné aby bylo chráněno proti vniknutí neoprávněných osob
každý vstup do tohoto zařízení musí být zaznamenám, stejně jako všechny zde prováděné operace

Plány kontinuity – bus. continuity planning

Organizace musí mít připravené postupy, jak v případě havárie po určitou dobu postupovat bez:

- podpory informačního systému
- vlastního zaškoleného personálu
- komunikace
- provozních prostor
- …

Součástí plánů požadavky na dobu a rozsah návratu původních služeb.

čím déle vydrží, tím snazší je připravit a provozovat odpovídající prostředky pro obnovu

Plány obnovy

pro případ poruchy by měly být vypracovány podobné procedury, co je třeba učinit za účelem rychlého odstranění následků
tyto plány musí být důkladně prověřeny a otestovány, musí být stále k dispozici (nejlépe v tištěné podobě) pro případ poruchy

Obnova provozu

často může být životně důležité obnovit dostatečně rychle činnost výpočetního systému (na druhou stranu – nepřeceňovat)
většina výrobců počítačů je schopna v kritickém případě dodat během jediného dne náhradní technické vybavení stejné, nebo dostatečně podobné původnímu

- *cold site* je zařízení vybavené zdroji elektrické energie, klimatizací, komunikačními linkami atd., kde může být výpočetní systém velmi rychle nainstalován a uveden do provozu

- *hot site* je zařízení navíc vybavené též výpočetním systémem, který je připraven ke spuštění, stačí pouze přinést zálohu dat a programů, pomocí hot site lze obnovit provoz zcela zničeného výpočetního systému během několika hodin
- clustery – redundance na úrovni funkčních jednotek (serverů, systémů) zajišťující automatické přenesení výpočetních operací na zbylé kapacity
- mirroring – on-line redundance na úrovni datových úložišť
- zálohy