Az informatikai biztonság alapjai

Pintér-Huszti Andrea

2020. szeptember 6.

Tartalom

Fizikai védelem

Fizikai védelem

- A fizikai védelem feladata azon **fizikai erőforrások védelme**, melyek az adatok tárolását, feldolgozását, továbbítását biztosítják. A védelmi intézkedések többsége *preventív vagy detektív*.
- Fizikai infrastruktúra (általános fogalom):
  - **Informatikai rendszer hardver elemei**: Adatfeldolgozó és tároló eszközök, adatátviteli és hálózati elemek és offline tároló eszközök. Ide soroljuk az informatikai rendszer dokumentációit is.
  - **Épületek**: Épületek, ahol az informatikai rendszer fizikai elemei megtalálhatóak.
  - **Kiszolgáló rendszerek**: Elektromos vezetékek, kommunikációs hálózatok,víz- és gázvezetékek.
  - **Személyzet**: Azon személyek, melyek az informatikai rendszer használói, fenntartói vagy működtetői.

Fizikai fenyegetések kategóriái

- Környezeti fenyegetések, természeti csapások
- Technikai fenyegetések
- Emberi fenyegetések

Természeti csapások

Tornádó forgószél

- szerkezeti kár, épületek tetejét veszélyezteti, kültéri berendezések sérülése, elvesztése
- a szél és repülő tárgyak okozhatnak kárt
- helyi közmű, és kommunikáció ideiglenes elvesztése
- a közmű szolgáltatások gyors helyreállítása követi

Trópusi ciklonok hurrikánok, trópusi viharok, tájfunok

- jelentős szerkezeti károk és kültéri berendezések sérülése
- közmű szolgáltatások, kommunikáció sérülése
- személyzet vészhelyzeti ellátása szükséges, generátor szükséges

Table 16.2 **Fujita Tornado Intensity Scale**

Category	Wind Speed Range	Description of Damage
F0	40–72 mph 64–116 km/hr	Light damage. Some damage to chimneys; tree branches broken off; shallow-rooted trees pushed over; sign boards damaged.
F1	73–112 mph 117–180 km/hr	Moderate damage. The lower limit is the beginning of hurricane wind speed; roof surfaces peeled off; mobile homes pushed off foundations or overturned; moving autos pushed off the roads.
F2	113–157 mph 181–252 km/hr	Considerable damage. Roofs torn off houses; mobile homes demolished; boxcars pushed over; large trees snapped or uprooted; light-object missiles generated.
F3	158–206 mph 253–332 km/hr	Severe damage. Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off ground and thrown.
F4	207–260 mph 333–418 km/hr	Devastating damage. Well-constructed houses leveled; structures with weak foundation blown off some distance; cars thrown and large missiles generated.
F5	261–318 mph 419–512 km/hr	Incredible damage. Strong frame houses lifted off foundations and carried considerable distance to disintegrate; automobile-sized missiles fly through the air in excess of 100 yards; trees debarked.

Table 16.3 **Saffir/Simpson Hurricane Scale**

Category	Wind Speed Range	Storm Surge	Potential Damage
1	74–95 mph 119–153 km/hr	4–5 ft 1–2 m	Minimal
2	96–110 mph 154–177 km/hr	6–8 ft 2–3 m	Moderate
3	111–130 mph 178–209 km/hr	9–12 ft 3–4 m	Extensive
4	131–155 mph 210–249 km/hr	13–18 ft –5 m	Extreme
5	>155 mph >249 km/hr	>18 ft >5 m	Catastrophic

Természeti csapások

Földrengés

- teljes rombolás, jelentős, hosszú ideig fennálló kár informatikai renszer épületeiben
- hardver, közmű, infrastruktúra megsemmisülése, megemelt padlók összeomlása
- személyzetet veszélyeztetik a törött üvegek, repülő tárgyak

Jégvihar

- Informatikai rendszer épületeinek megrongálódása
- közmű és kommunikáció megsérülése

Természeti csapások

Villám „Felhős nap volt, a szomszéd faluban villámlott. Mivel én közel lakom , ezért a telefonvonalaim a szomszéd faluba csatlakoznak. Elektromos lökéshullám érkezett. . . a modemem lángra kapott.” (www.pcszerviz.com)

- egyszerű becsapódástól a katasztrófáig terjedhet
- elektromos vezetékek megsérülése, tűz keletkezhet

Árvíz

- árterületen, illetve alacsony szinten levő berendezések veszélyeztetettek
- hosszú ideig tartó sérülés, komoly takarítás szükséges

Környezeti fenyegetések - Nem megfelelő hőmérséklet

Olyan környezeti feltételek, melyek korlátozzák vagy megszakítják az informatikai rendszer szolgáltatását, vagy a tárolt adatokat

Nem megfelelő hőmérséklet

- A legtöbb számítógépes rendszert 10 és 32 fok közötti hőmérsékleten kell tárolni.
- Ezen az intervallumon kívül az erőforrás továbbra működőképes, de lehet, hogy nem megfelelő eredményeket ad.
- Ha a környezet hőmérséklete nagyon magas lesz, a számítógép nem lesz képes megfelelően hűteni magát és a belső komponensek sérülhetnek.
- Ha a hőmérséklet túl alacsony, bekapcsolásnál a rendszer hőtani sokkon esik át, mely integrált áramkörök sérüléséhez vezethet.
- Okostelefonok, digitális kamerák, táblagépek és laptopok stb. akkumulátorainak kapacitása is csökken, ha túl meleg vagy túl hideg van.

Table 16.4 **Temperature Thresholds for Damage to Computing Resources**

Component or Medium	Sustained Ambient Temperature at which Damage May Begin
Flexible disks, magnetic tapes, etc.	38 °C (100 °F)
Optical media	49 °C (120 °F)
Hard disk media	66 °C (150 °F)
Computer equipment	79 °C (175 °F)
Thermoplastic insulation on wires carrying hazardous voltage	125 °C (257 °F)
Paper products	177 °C (350 °F)

Source: Data taken from National Fire Protection Association.

Környezeti fenyegetések - Nem megfelelő hőmérséklet és páratartalom

- Az eszköz belső hőmérséklete
  - A belső hőmérséklet jelentősen nagyobb, mint a szoba hőmérséklete.
  - Saját hűtésük külső feltételektől is függ: pl. külső hűtés léte
- Magas páratartalom
  - A hidegből a meleg épületbe érve sincsenek azonnal biztonságban az eszközök, ekkor ugyanis pára csapódhat le a belsejükben.
  - Magas pára korróziót okozhat.
  - A vízcsepp a mágneses és optikai tárolókat is veszélyezteti.
  - A vízcseppek zárlatot okozhatnak az alkatrészekben. (vízálló táblagépek és okostelefonok)

Környezeti fenyegetések - Sztatikus elektromosság

„Összesen annyit csináltam, hogy leültem az éppen működő gépem mellé, és hoppá!. Amikor rátettem a kezemet az egérre, akkor az egér sztatikusan feltöltődött, miközben egy kicsit engem is megrázott. Az egér és a billentyűzet nem működtek tovább és észrevettem, hogy az egér elkezdett felmelegedni. Újraindítottam a PC-t, de amikor újrabootolt, nem működött sem, az egér sem a billentyűzet. Ezután, az egér annyira felmelegedett, hogy nem lehetett hozzányúlni!" (http://www.pcszerviz.com)

- Sztatikus elektromosság
  - A sztatikusan feltöltött személyek, tárgyak kárt okozhatnak az elektromos eszközökben.
  - Már a 10 voltos kisülések is kárt okozhatnak az áramkörökben.
  - Több száz voltos kisülések jelentős kárt okozhatnak.
  - Az emberi test jóval több elektromos ellenállás tárolására alkalmas, mint egy átlagos IC. Az emberi sztatikus kisülések több ezer voltot is elérhetik.

Környezeti fenyegetések - Tűz-, füst- és vízkárok

Tűz, füst

- emberi életre és a berendezésekre is vonatkozó fenyegetés
- a közvetlen láng és a hő is veszélyforrás
- mérgező gázok felszabadulása veszélyes az emberekre nézve
- tűzoltásból keletkező vízkár
- füstkár

Víz

- a számítógépes eszközöket, papírokat, elektromos tároló eszközöket veszélyezteti
- elektromos rövidzárlat keletkezhet
- mozgó vizek: vízvezetékek, eső, hó, jég okozta víz
- ha vízhálózat két szinttel van feljebb, akkor már nem annyira kockázatos
- árvíz sárt hagy maga után, nagyon nehéz a kitakarítása

Környezeti fenyegetések - Por

Por

- Általában ezzel a fenyegetéssel kevésbé foglalkozunk.
- A por és kosz mindenütt megtelepszik.
- Nagyobb a fenyegetés, ha környezetünkben kontrolált épület rombolások, vagy vihar van.
- Szellőzőréseken át bejutó por eltömíti a levegő szabad áramlásának útját, ezért a belső ventilátor nem tudja kellő hatékonysággal hűteni a működése során forróvá váló processzort.
- Megjegyzés: Laptopokat állandó hordozása miatt évente egyszer ki kell takaríttatni.

Rovarfertőzés

- élő organizmusok is fenyegetések: rovarok, penész, rágcsálók
- A penész mind a személyzetre, mind a berendezésekre is vonatkozó veszélyforrás.

Technikai fenyegetések - Elektromos teljesítmény

Feszültséghiány

- A berendezés kevesebb feszültséget kap, mint amennyire szüksége van a normál működéshez.
- A legtöbb számítógép ellenáll a kb. 20%-os feszültséghiánynak, még nem áll le, nem történik működésbeli hiba.
- Nagyobb feszütséghiány leállítja a rendszert.
- Komolyabb kár sérülés nem keletkezik, csak a szolgáltatás szakad meg.

Túlfeszültség

- áramszolgáltatási anomáliák, villámcsapás okozhatja
- processzorokban, memóriákban okozhat kárt

Technikai fenyegetések - Elektromágneses Interferencia

Elektromágneses Interferencia

- Elektromos eszközök, más számítógépek elektromos zajt generálnak, mely kárt okozhat a saját számítógépünkben.
- Ez a zaj a térben és elektromos vezetékeken is továbbítódik.
- Zaj eredhet a közeli mikrohullámú antenna, vagy akár mobiltelefon révén is.

Emberi fizikai fenyegetések

Az emberi fizikai fenyegetések kevésbé kiszámíthatóak, mint más fizikai fenyegetések. Az emberek a rendszer leggyengébb pontjait keresik.

Jogosulatlan fizikai hozzáférés
- Szerverek általában lezárt területen vannak, ahova való bejutás korlátozott. Néhány alkalmazottnak van jogosultsága.
- Jogosulatlan fizikai hozzáférés lopáshoz, vandalizmushoz és visszaéléshez vezethet.

Lopás
- berendezések eltulajdonítása, adatok megszerzése
- csatorna lehallgatása is ide tarozik

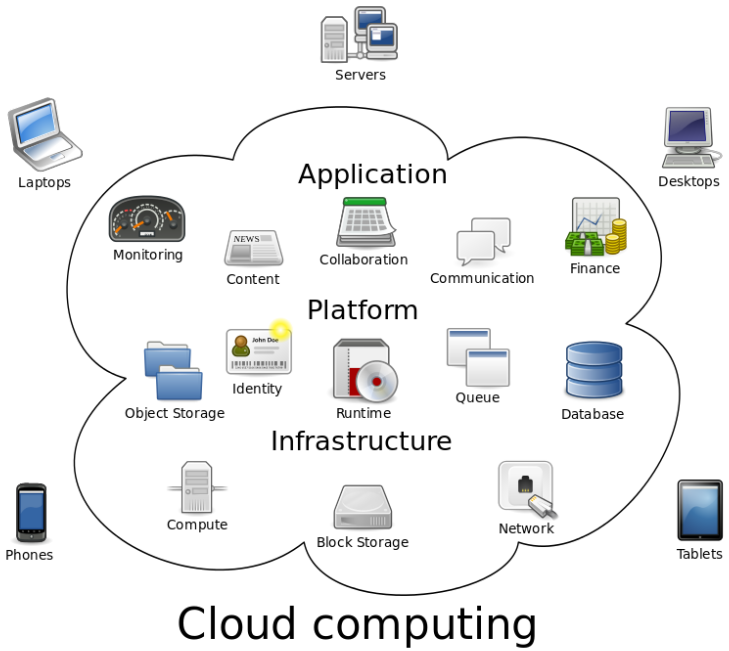
Vandalizmus
- berendezések tönkretevése

Visszaélés
- az erőforrások jogosulatlan használata

Fizikai preventív kontrollok

Általános preventív védekezés: *felhők használata*

- lokálisan lényegesen kevesebb erőforrásra van szükség
- a nagy mennyiségű adatok lokálisan nincsennek fizikai fenyegetéseknek kitéve



Fizikai preventív, detektív kontrollok - Környezeti fenyegetések

Nem megfelelő hőmérséklet és páratartalom
- Mérőeszközök segítségével a megfelelő környezetet el lehet érni. Ha az érték túllép a megengedett határon, akkor jelez is.

Vízkár
- Vízérzékelők elhelyezése a padlón és az emelt padlók alatt.
- Víz esetén automatikusan le kell, hogy kapcsolódjon az áram.

Por
- Ventillátor szűrő karbantartása és a helyiség tisztán tartása.

Fizikai preventív, detektív kontrollok - Környezeti fenyegetések

Tűz, füst Tűzjelzők, megelőző intézkedések, tűz oltása
Ritkán keletkezik katasztrófális tűz egy jól védett számítógépes helyiségben. Úgy kell a helyiséget kiválasztani, hogy minimális legyen a környezetében keletkező tűz, víz, füst kockázata. Védelmi intézkedések:

- Közös falak legalább egy óra hosszat tűzálló legyenek.
- Légkondicionállók úgy legyenek megtervezve, hogy a tüzet ne terjesszék.
- Gyúlékony anyagokat ne tároljunk a helyiségben.
- Kézi tűzoltókészülék legyen elérhető, egyértelműen jelezve, és rendszeresen tesztelt.
- Automata tűzoltó rendszer is legyen telepítve.

Fizikai preventív, detektív kontrollok - Környezeti fenyegetések

Tűz, füst További intézkedések:

- Tűzjelzők vészjelet adjanak le a helyiségben és külső felügyeletnek is.
- Főkapcsoló szükséges és egyértelműen jelezve legyen.
- Menekülési útvonalak ki legyen függesztve.
- Fontos adatok, dokumentumok tűzálló kabinetben legyenek.
- Az adatok, programok up-to-date másolata más helyiségben legyen.
- Biztosítási cégek, tűzoltóság vizsgálja át az épületet.

Fizikai preventív, detektív kontrollok - Technikai fenyegetések

Elektromos teljesítmény, Elektromágneses interferencia

- Szünetmentes tápegység kapcsolása minden egyes kritikus berendezéshez.
- Szünetmentes tápegység elektromos áramot biztosít, ha megszűnik a hálózati áramforrás, áramingadozás van, vagy áramszünet lép föl.
- A szünetmentes tápegység áthidalási ideje néhány perctől pár óráig terjed. Hosszabb kimaradások esetén generátor szükséges.

Fizikai preventív, detektív kontrollok - Emberi fenyegetések

- Csak az arra jogosult léphet be az **épületbe**. Nem vonatkozik az alkalmazottakra, jogosulatlan belső támadókra.
- Erőforrásokat tegyük zárható tárolókba, szétekbe, szobákba.
- Berendezéseket rögzítsük olyan tárgyakhoz, melyeket nem lehet elmozdítani.
- Mozdítható berendezéseket nyomkövetővel láthatunk el, mely jelzi, ha elhagyja a területet.
- Hordozható eszközök nyomkövetővel való ellátása, mely állandó monitorozást tesz lehetővé.
- A megfigyelő rendszer része az épületnek. Ezek a rendszerek valós idejű távoli megfigyelést és rögzítést jelent.

Fizikai helyreállító kontroll

Helyreállító kontroll A helyreállító kontroll hasonlít a *korrektív* kontrollhoz, csak komolyabb helyzetekben alkalmazzuk.

- A legfontosabb helyreállító intézkedés a másolatok készítése: **Backups**.
- A másolatok *nem védenek az esetleges bizalmassági sérülésekkel szemben*, de az adatok visszaállíthatóak.
- **Hot site**: Közel valós idejű szinkronizálással készített másolat, mely képes egyből átvenni a szolgáltatást.
- A víz, a füst, a tűz maga után hagy maradványokat, melyeket el kell takarítani. Speciális tisztítókat kell hívni.