PERSECUTOR

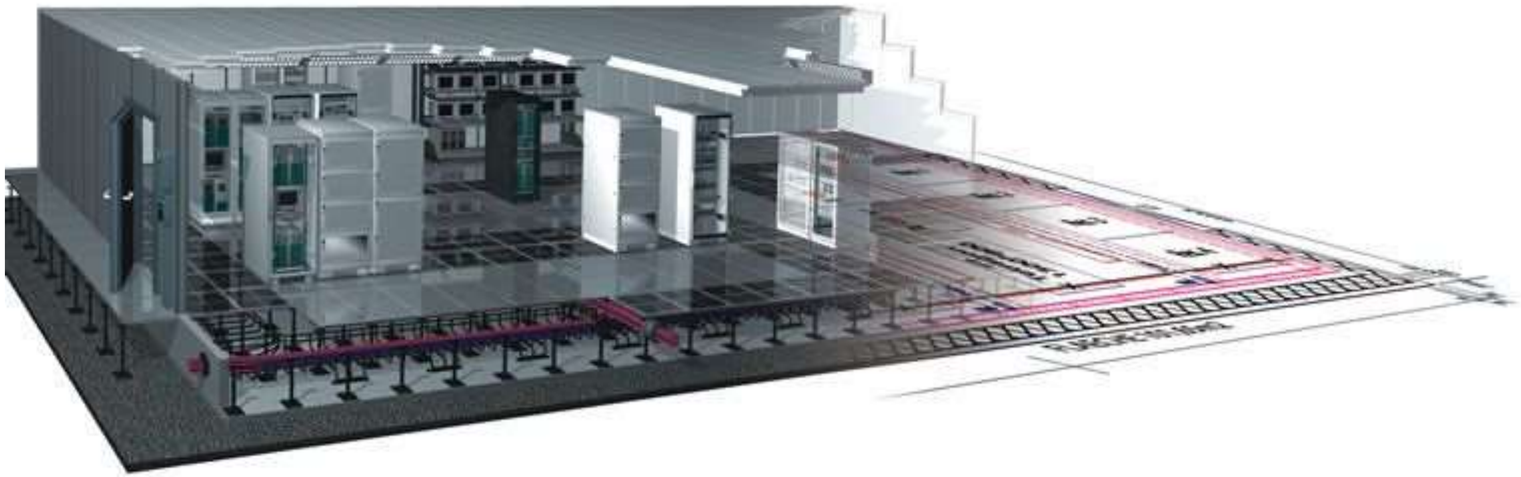
With the technology of tomorrow
for the safety of today.

www.persecutor.hu

# IT biztonság - 2014/2015 tanév

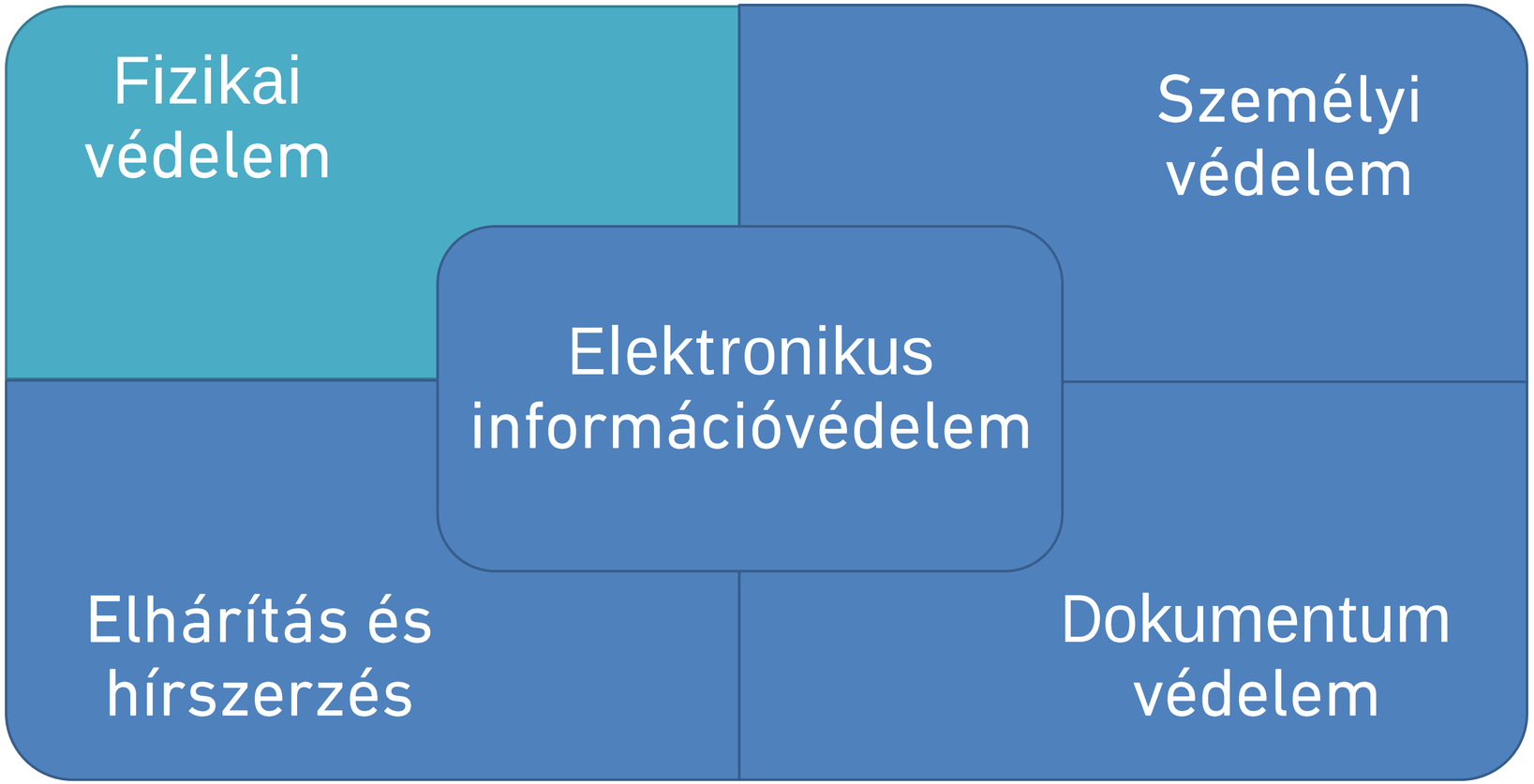
# Fizikai biztonság

# Tematika



- IT fizikai biztonság módszertana
- Fizikai biztonsági fenyegetettségek
- Szabványok, ajánlások
- Kockázatcsökkentés
- Gyakorlati példák

# Információvédelem egy lehetséges módszertana



# Megközelítés

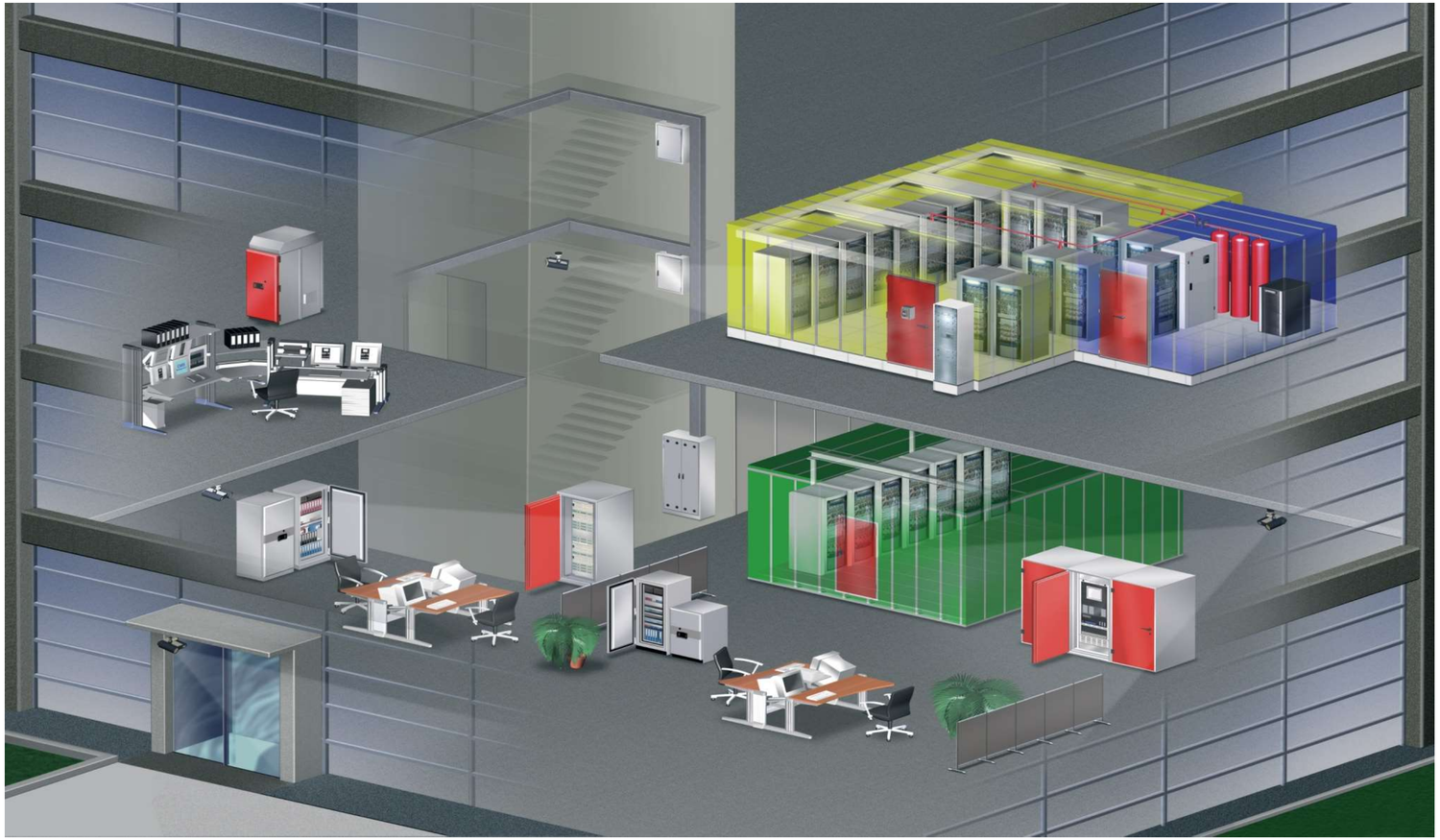
**Bizalmasság**
**Sértetlenség**
**Rendelkezésre állás**

... a fizikai **biztonság vonatkozásában.**

# IT fizikai biztonság területei

1. Adatfeldolgozás helyszínei és kapcsolódó létesítmények, úgy mint:
    - IT gépterem
    - Géptermi kiszolgáló területek (áramellátó, ups, akkumulátor helyiség, NOC, OC, klíma gépház stb.)
    - Co-location helyszínek
2. Adat továbbítás helyszínei és kapcsolódó létesítmények, úgy mint:
    - Kommunikációs gépterem
    - WAN/ LAN központok / eszközök
    - WAN / LAN kábelezés
    - További telco eszközök
3. Adattárolás helyszínei
    - SAN környezet és egyéb online mentőegységek (havária back-up stb)
    - Mentési média tárolók (tűzálló széfek, termek stb)
    - Mentési médiák szállítása
4. Felhasználói környezet
    - Kliens oldal
    - Távoli elérés

# Fizikai biztonság helyszínei



# Informatikai fizikai biztonság

## Fizikai biztonság

- passzív tűzvédelem
- páratartalom szabályozás
- vízbetörés elleni védelem
- betörés/illetéktelen hozzáférés elleni védelem
- vandalizmus elleni védelem
- EMC védelem
- porvédelem
- robbanás, terrorveszély elleni védelem

## Technikai biztonság

- biztonságos energiaellátás és elosztás
- géptermi és technikai területek hűtése, extrém hűtése
- automatikus üzemfelügyelet
- aktív tűzvédelem
- kábelmenedzsment
- kommunikációs hálózat fizikai biztonsága

## Logikai biztonság

- hozzáférés szabályozás
- integrált elektronikus védelmi (behatolás, beléptető és CCTV) rendszerek
- védelmi rendszerek log elemzése
- fizikai és IT környezet változáskezelés
- karbantartás és hibaelhárítás menedzsment

# A „támadó”...

Emberi, szándékolt

- Külső magánszemély vagy bűnszervezet (mindenképp szándékolt)
- Saját dolgozó (sértett dolgozó, bosszú, naivitás stb)
- Bizonyos esetekben kormányok, egyéb politikai szervezetek

Nem emberi, nem szándékolt

- Természeti csapás
- Üzemzavar
- Emberi mulasztás

# A „támadó” kockázatelemzése

A „Támadó”, céljai ismeretében ugyanúgy végez kockázatelemzést, mint a védekező fél.

A hagyományos (fizikai) támadás azonosítási kockázata ugyan jellemzően magasabb, mint a „szoftveres” támadásé, azonban a szükséges felkészültség, illetve a potenciálisan okozható kár figyelembe vételével lehet csak megfelelő kockázatértékelést végezni.

Ugyanis:

- a legtöbb számítógépterem közterületről akár célzottan is támadható viszonylag kevés információ birtokában,
- a támadást sok esetben már kézi szerszámokkal, eszközökkel is végre lehet hajtani,
- a számítógéptermi fizikai kiszolgáló infrastruktúra (pl.: transzformátor, klíma kültéri egységek, diesel, stb.) pótlási és javítási ideje akár heteket is igénybe vehet!

# Közvetlen fizikai fenyegetések

# Közvetlen fizikai fenyegetések

**Tűzvédelem** IT **környezet számára**

**Vízbetörés és oltóvíz** elleni **védelem**

**Égési gázok** elleni **védelem**

**Törmelékhullás** elleni **védelem**

**Porlerakódás** elleni **védelem**

**Illetéktelen hozzáférés** elleni **védelem**

Vandalizmus **és szabotázs** elleni **védelem**

**Elektromágneses sugárzás**

**Katasztrófa esetén** a fenti **veszélyforrások** nagy **része** egyszerre jelenik meg.

# Fizikai biztonsági elvárások meghatározása

A fizikai biztonsági kockázatokat befolyásoló főbb külső (sokszor nem változtatható) tényezők:

- Objektum elhelyezkedése
- Épület elhelyezkedése az objektumon belül, környező épületek
- Épület egyéb funkcióinak hatásai
- Épület építészeti, statikai, védelmi kialakításai
- Gépterem épületen belüli elhelyezkedése
- Gépterem közvetlen környezete
- Géptermen kívüli infrastruktúra védelme
- Épületen kívüli infrastruktúra védelme
- Reagáló erők jelenléte és felkészültsége
- Törvényi, hatósági, vevői elvárások
- Elvárt rendelkezésre állás

Georedundancia?

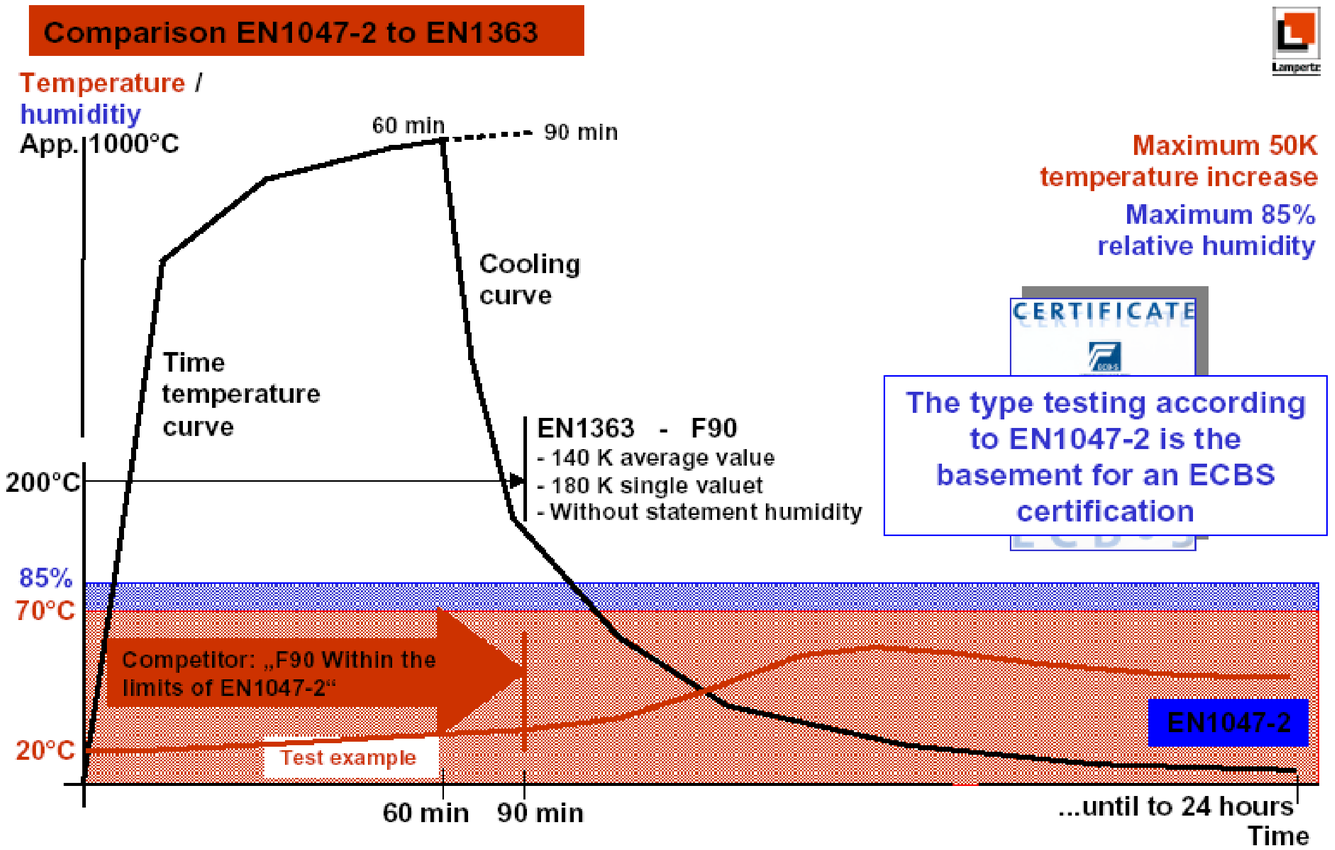
# Informatikai eszközök érzékenysége – elvárt védelmi értékek

| Adathordozók | Hőmérséklet maximum | Páratartalom maximum |
|---|---|---|
| Papír | 170 °C | 100% |
| Adathordozó (Cd, DLT...) | 50 °C | 85% |
| Hardware tárolás | -15...70 °C | 85% |
| Hardware üzem | 15...35 °C | 85% |

A **veszteséget okozó katasztrófa események** csak 20%-a keletkezik **közvetlenül** a **gépteremben**!

Az IT **infrastruktúra fizikai sérülését** a **vállalatoknak** csak 20%-a **éli túl**!

# MSZ EN 1047-2 – IT gépterem tűzterhelésére vonatkozó szabvány




Maximum 50K temperature increase

Maximum 85% relative humidity




The type testing according to EN1047-2 is the basement for an ECBS certification

Materialprüfungsanstalt für das Bauwesen Dresden (MPA Dresden)

**Prüfungsbericht**

**Nr. 99-23-0938**

- Kurzfassung -

**Art der Untersuchung**

Durchführung einer Brandprüfung am IT-Modulsafe Version Lampertz der Otto Lampertz GmbH & Co. KG zum Nachweis des Brandverhaltens bei allseitiger Befammung gemäß Einheitstemperaturkurve nach DIN 4102 Teil 2 (09/77) bezüglich der Einhaltung der Grenzwerte nach EN 1047-2 (max. 50 K Temperaturanstieg und 85 % relative Luftfeuchte).

**Bewertung der Ergebnisse**

Die im Innenraum gemessene maximale Absolutemperatur betrug zum Versuchsende nach 30 Minuten an den Oberflächenmeßstellen 48 °C und an den Luftmeßstellen 72 °C. Das entspricht einer Erhöhung gegenüber der Anfangstemperatur um 25 K an den Oberflächen bzw. 50 K in der Luft.
Die relative Luftfeuchte betrug maximal 62,7 %.
Die Grenzwerte nach EN 1047-2 bezüglich der maximal zulässigen Temperaturerhöhung von 50 K bzw. der maximalen Luftfeuchte von 85 % sind während der Befammung nach Einheitstemperaturkurve über 30 Minuten eingehalten worden.

**Besondere Hinweise**

Diese Kurzfassung zum Prüfungsbericht Nr. 99-23-0938 besitzt nur informellen Charakter und ist ohne diesen unverbindlich.
Der Prüfungsbericht Nr. 99-23-0938 gilt nur für den IT-Modulsafe Version Lampertz, der in der Ausführung und den Abmessungen den Angaben des Abschnittes 2 und der Anlage 1 des vorgenannten Prüfungsberichtes entsprechen.

Auf Grund der EN 1047 Anhang A (Übertragbarkeit der Prüfergebnisse) kann das Prüfergebnis auf das in der Anlage 1 dargestellte und bis auf die geringfügig kleinere Höhe baugleiche zweite Modell des IT-Modulsafe Version Lampertz übertragen werden.

Der Prüfungsbericht Nr. 99-23-0938 gilt nur bis zum 16. August 2002 und kann danach auf Antrag verlängert werden.

Freiberg, den 99-08-18

Materialprüfungsanstalt für das Bauwesen Dresden (MPA Dresden)
Referat Freiberbau
Petersstraße 22
09599 Freiberg

BOR Hübler
Referatsleiter

# Gépterem tesztelése

**Type testing norm EN 1047-2**

**Before testing**

**Test**

**After testing...**

# Egy tanulságos vizsgálat

**Betonverhalten Prüfinstitut Braunschweig am 27.08.1985**

| | |
|---|---|
| **Prüfobjekt:** | Betonwand F 90<br>trocken vorgelagert<br>100 mm stark |
| **Beflammung:** | nach DIN 4102 |
| **max. Temperatur:** | 960 °C |

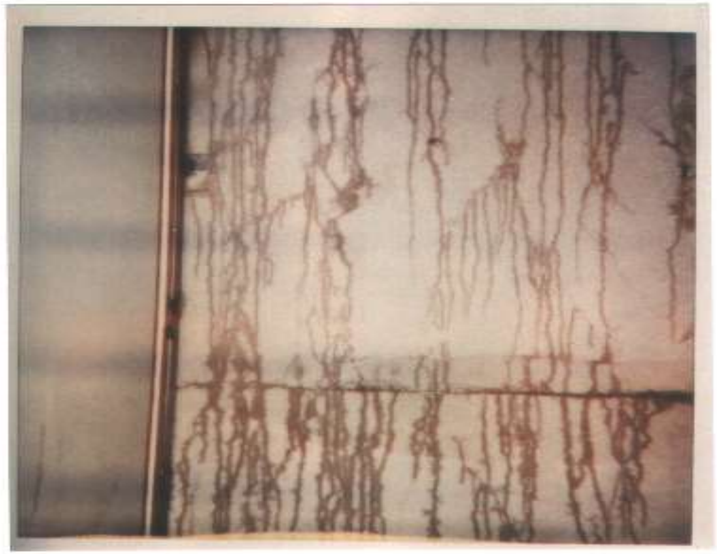


**Bild 1**
ca. 15 Minuten nach Beflammungsbeginn
Ofentemperatur: ca. 700°C
Wasserabfluß Innenseite

**Bild 2**
ca. 20 Minuten nach Beflammungsbeginn
Ofentemperatur: ca. 750°C
Stärkerer Wasseraustritt, in Dampf übergehend

# Önbizalom…

# Példa egy épített gépterem mennyezeti rétegrendjére irodaházi környezetben

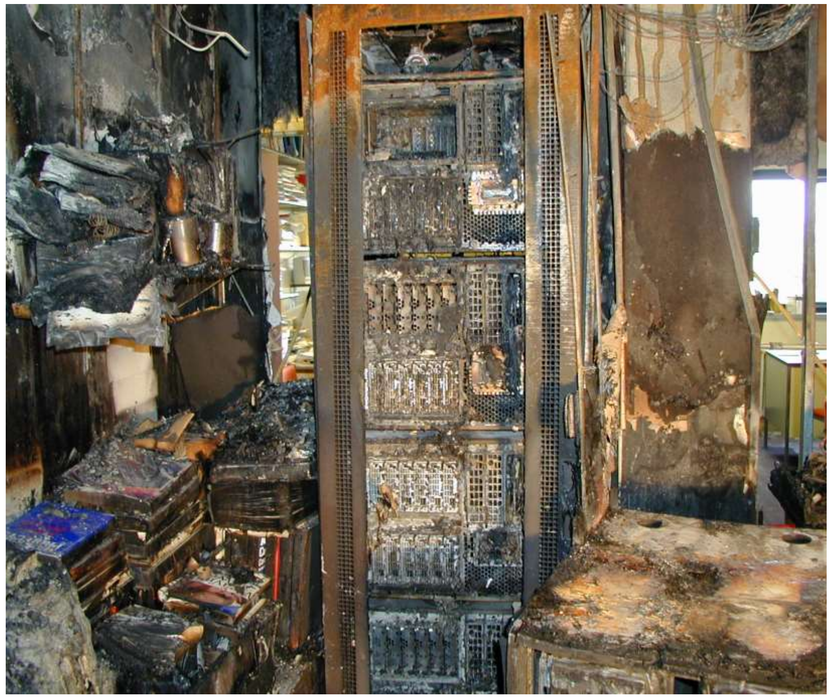
- Felső burkolat (szőnyegpadló / pvc)
- Fogadó aljzatbeton
- Elválasztó és tűzgátló réteg
- Nagy rugalmasságú felső vízszigetelés (géptermen túlnyúlva)
- 18-25cm vasbeton födémszerkezet (~F90 tűzállóság)
- Rugalmas elválasztó réteg (tapéta, rugalmas szigetelés)
- Egybefüggő horganyzott fémlemez (légréssel), egyedi, vízzáró rögzítéssel
- Gipszkarton /OSB védőburkolat
- További opció: emc védelem és emc védelmet védő gipszkarton burkolat, vagy egyedi mennyezeti függesztő-szerkezet

+ minden egyes pillért és egyéb csomópontot egyedi tervezésű védelemmel kell ellátni

+ oldalfalak, aljzat, kábel- és csőátvezetések, ajtó- és légtechnikai átvezetések

# Néhány informatikai fizikai biztonsági esemény felvételről...

# Amikor a lehetetlennek vélt esemény mégis megtörténik…



A nem megfelelően méretezett és megvalósított géptermi határoló szerkezetre fordított összeg ablakon kidobott pénz, mivel valójában nem csökkenti a kockázatokat.

# Cloud computing...

# Vízbetörés...

# Még egy kis víz...

# Fizikai biztonság és cloud computing

- Cloud computing, outsourcing, colocation esetén a fizikai biztonsági kérdések egy része is „kiszervezésre kerül” a szolgáltatóhoz.
- Ez esetben alapvetően jogi és garanciális (SLA) kérdés a kiszervezett terjedelem fizikai biztonsága,DE:
- Minden esetben marad a szervezetnél fizikai biztonsági feladat:
  - mentés
  - Back-up
  - WAN eszközök
  - kliens oldal
- Cloud / virtualizált szolgáltatás esetén is vizsgálni szükséges, hogy hol van a cloud, mennyire adott a georedundancia.

# Fizikai biztonsági események

- jellemzően alacsony valószínűségű események
- jellemzően magas potenciális kárérték jellemzi
- nehezen szimulálhatóak
- magas a „heves reakció” esélye és addicionális kárértéke
- potenciálisan veszélybe kerülhet a szimulációt végző személy – „fizikai etikus hacking”
- jogilag könnyen értelmezhető, viszont a szimuláció viszont még nehezebben kezelhető, mivel a fizikai biztonsági események közelebb állnak a törvénykezés értelmezéséhez.

# Nemzetközi és hazai számítógéptermi ajánlások

**Hazai ajánlások**

KIB 28 Követelménytár – Tervezés IT Biztonsági Szempontból *(ez tartalmazza viszonylag **részletesen a fizikai biztonsági követelményeket**)*

**Nemzetközi ajánlások**

ANSI TIA/EIA 942 (amerikai ajánlás)

BITKOM (német BSI ajánlás)

TÜV IT (kész géptermek osztályozása)

Tudástár

www.datacenterknowledge.com

www.uptimeinstitute.com

BME IK

Informatikai Központ

BITKOM

**ANSI TIA/EIA 942**

# Ajánlások használhatósága

- A nemzetközi ajánlások alapvetően a rendelkezésre állási elvárások (technikai biztonság) mentén sorolják osztályba a védelmi követelményeket, ami azonban sosem lehet teljes körű (bizalmasság, sértetlenség osztályozott figyelembe vétele hiányzik).
- A géptermi ajánlások nem követik le az új informatikai architektúrák (virtuális szerver, private cloud stb.) megjelenésének hatását.
- Az ajánlások nem adnak útmutatást a különböző IT biztonsági területek kockázat alapú súlyozására (erre vonatkozóan a best practice is erősen hiányzik)
- Nincs egyértelmű útmutatás arra vonatkozóan, hogy az informatikai fizikai biztonság melyik szervezeti egységhez tartozik (kockázatkezelés, budget stb. oldalról)
- A magyar adoptáció adós marad a biztonsági osztály szerinti részletes differenciálással.

BITKOM

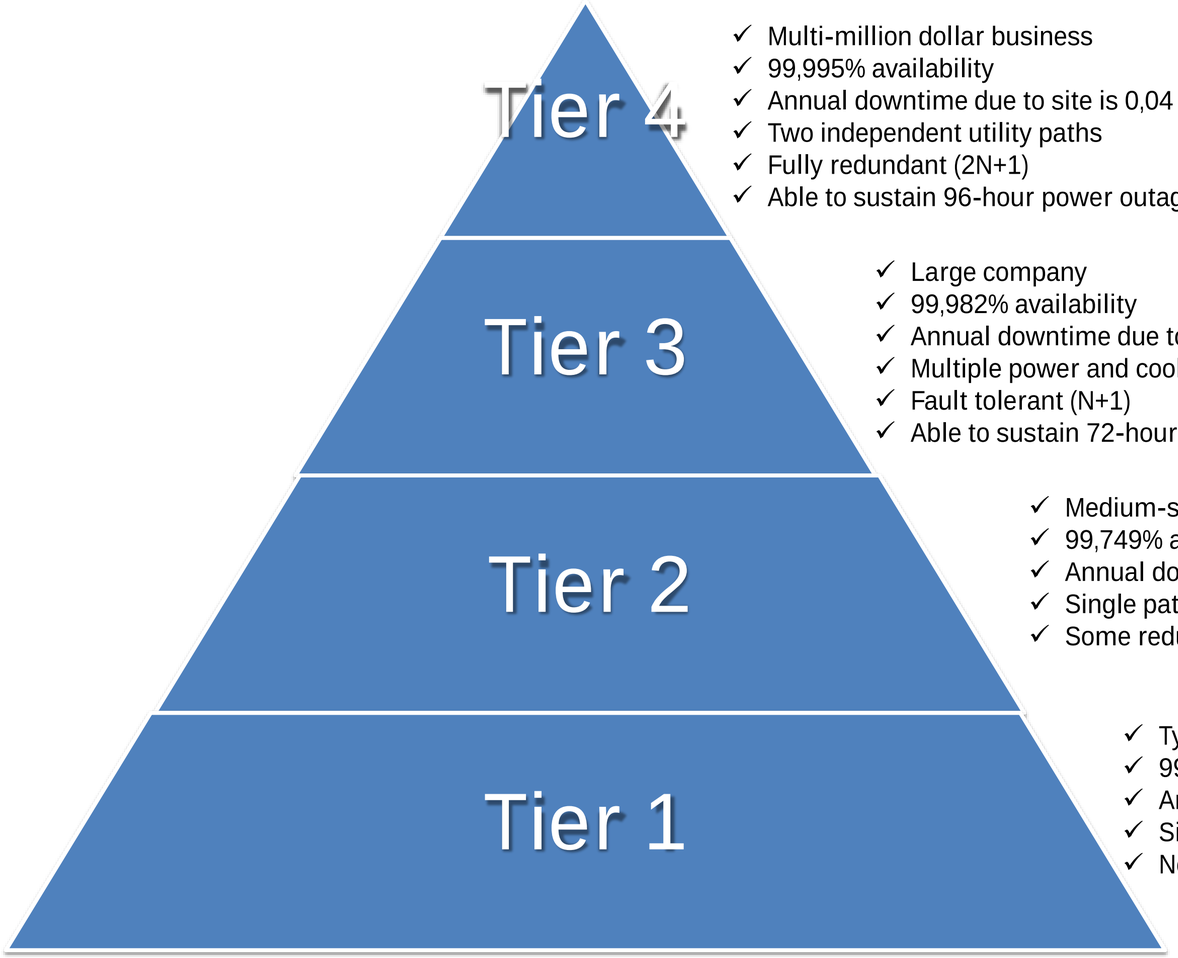
**Egy tipikus példa:**

**Bitkom „C” kategória** (~Tier 3)

- **Évenkénti maximális kiesési idő: 1 óra**
- **Üzem közben karbantartható rendszerek**

(Bitkom **rendszerben A, B, C, D, E kategóriát különböztetnek meg**)

# Data Center Tiers




- ✓ Multi-million dollar business
- ✓ 99,995% availability
- ✓ Annual downtime due to site is 0,04 hours
- ✓ Two independent utility paths
- ✓ Fully redundant (2N+1)
- ✓ Able to sustain 96-hour power outage

- ✓ Large company
- ✓ 99,982% availability
- ✓ Annual downtime due to site is 1,6 hours
- ✓ Multiple power and cooling paths
- ✓ Fault tolerant (N+1)
- ✓ Able to sustain 72-hour power outage

- ✓ Medium-size business
- ✓ 99,749% availability
- ✓ Annual downtime due to site is 22,0 hours
- ✓ Single path of power and cooling
- ✓ Some redundancy in power and cooling

- ✓ Typically small business
- ✓ 99,641% availability
- ✓ Annual downtime due to site is 28,8 hours
- ✓ Single path of power and cooling
- ✓ No redundant components

# Ajánlások és fizikai biztonság a lokáció vonatkozásában

Adatközpont lokáció kiválasztása

- Elmúlt 100 évben nem lehet árvíz
- Folyó és állóvíztől mért minimum magassági előírás (minimum 4-6 méter)
- Megközelíthetőség
- Közművek biztonsága
- Tengerszint feletti magasság
- Extrém időjárási körülmények (vihar, hó magasság stb.)
- Földrengési gyakoriság és intenzitás

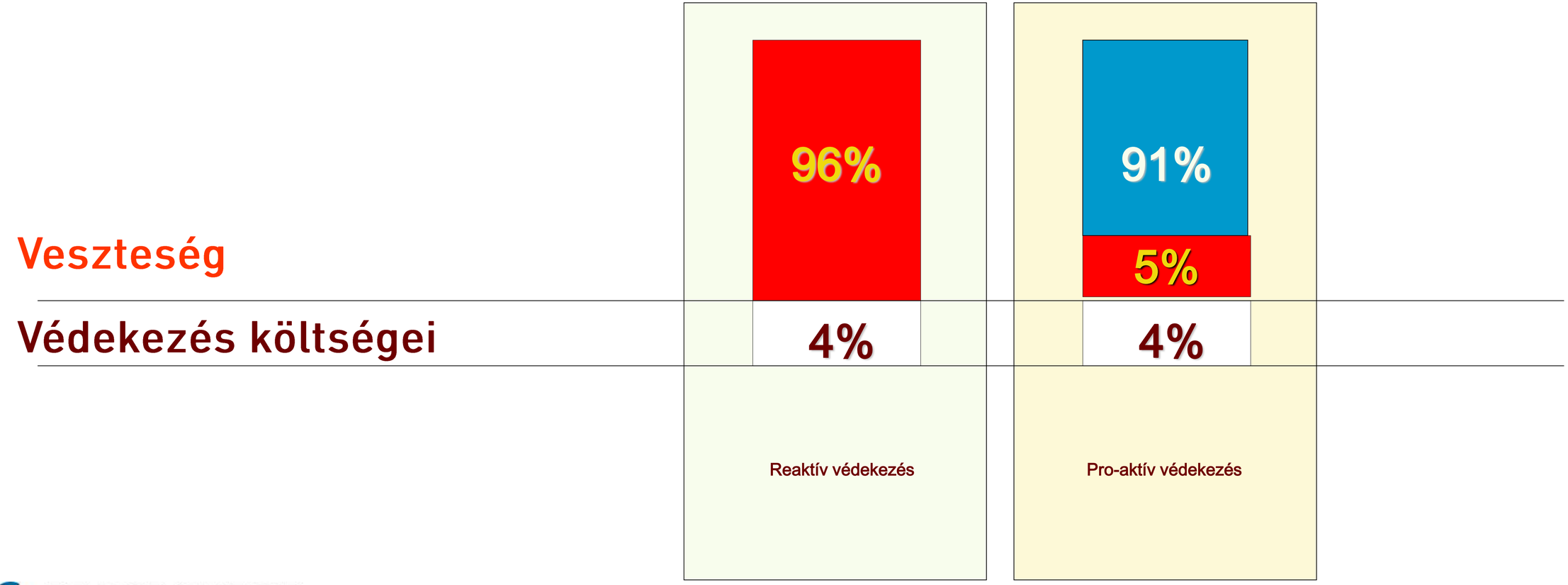
BITKOM

| Kategória | | Követelmény |
|---|---|---|
| Áramellátás | Szolgáltatói hálózat | Redundáns betáp |
| | UPS | Legalább N+1 redundáns, mentéshez igazodó áthidalás |
| | Szükség energia | Nem redundáns. 15mp belül terhelhető, 24 óra üzemanyag |
| | Áramelosztás | Redundáns (teljes elosztási hálózaton) |
| | Légkondicionálás | Legalább N+1 redundáns, min. precíziós hűtés |
| Tűzvédelem | Aktív tűzvédelem | Legalább korai tűzjelző rendszer, automatikus tűzoltórendszer |
| | Passzív tűzvédelem | Teljes határoló felület EN 1047-2 szerint minősített, védelem a vízzel és a füstgázzal szemben |
| Kockázatmenedzsment | | Automatikus meghibásodás jelző rendszer |
| Szerviz | | 7/24/365 szerződésállomány minden alkotóelemre, helyszíni vagy szerződéses pótalkatrész |

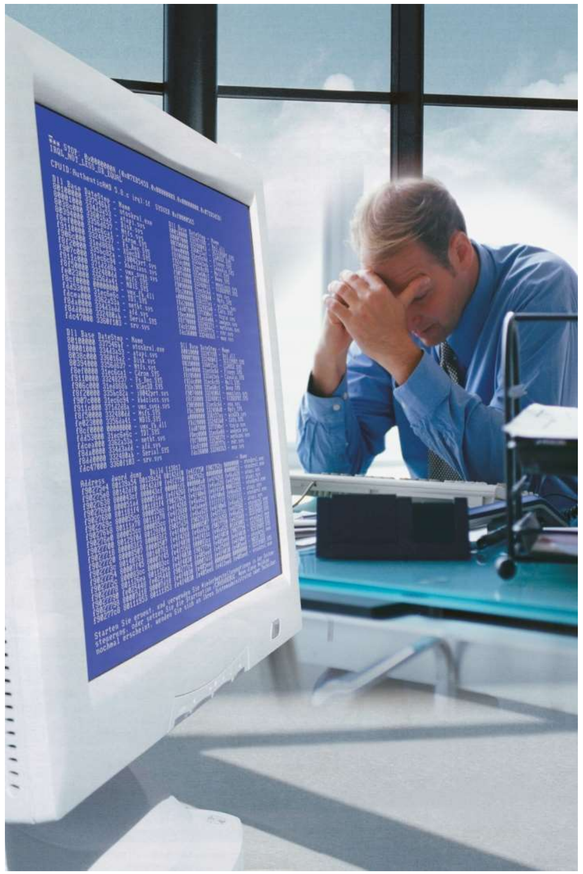
# Kockázatcsökkentés

- szabványosság, ajánlási megfelelőség érvényesítése beszerzéseknél, fejlesztéseknél, működési kockázatelemzésnél
- rendszeres és szabályozott éles havária tesztelés a kritikus rendszerelemekre nézve
- az informatikai rendszer módosításával automatikusan és szabályozottan együtt végzett fizikai kiszolgáló infrastruktúrára vonatkozó változáskezelés
- átfogó, biztonsági szempontú audit.

# A potenciális veszteség és a védekezési költség aránya fizikai biztonsági kérdések esetében



# Egy gyors **helyzetértékelés**



Tegyük fel magunknak az alábbi kérdéseket:

1. Rendelkezik az adott szervezet elfogadott és dokumentált rendelkezésre állási elvárásokkal az IT szolgáltatások irányában?
2. Ezen rendelkezésre állási elvárások megfeleltetésre kerültek a géptermi fizikai és technikai környezetével?
3. Rendelkezik az adott szervezet rendszerszintű (végrehajtható) katasztrófatervvel?
4. Rendelkezésre áll naprakész átfogó kockázatelemzés a szerverterem és az azt kiszolgáló infrastruktúra fizikai biztonsági fenyegetettségeiről?
5. Ki lenne a felelős amennyiben az IT szolgáltatás katasztrófaesemény következtében hosszabb ideig szünetel?

# Néhány alkalmazott technológia…

- Épített géptermi környezet (minden esetben speciális kialakítás
- Előre gyártott, ún. moduláris géptermi technológia
- Konténeres, kültéri kompakt géptermi kivitelek

# Aktív tűvédelem

**Nagyon korai tűzjelző rendszerek:**

- Pontszerű
- Aspirációs

**Géptermi, technológiai oltórendszerek:**

- Gázzal oltó rendszerek
- Oxigén szint elnyomás

# Géptermi áramellátás és hűtés

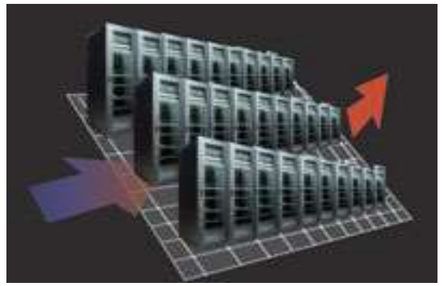
avagy

# Biztonság kontra „zöldség”?

# PUE

$$PUE = \frac{Total\ \ Facility\ \ Power}{IT\ \ Equipment\ \ Power}$$

# Géptermi hűtés



1. Perimetrikus hűtés (terem orientált hűtés)

Érezhető hűtési teljesítmény 500-1000 (1500W) / nm (2-5kw/rack)

Függőleges légáramlás

Páratartalom szabályozás, redundancia, szabadhűtés, megbízhatóság

2. Extrém hűtés (rack sor vagy rack orientált hűtés)

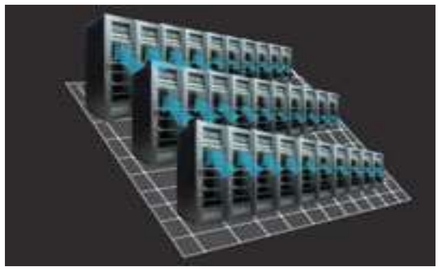
Érezhető hűtési teljesítmény akár 15-30kW/rack (LCP)

Vízszintes, egyenletes légáramoltatás

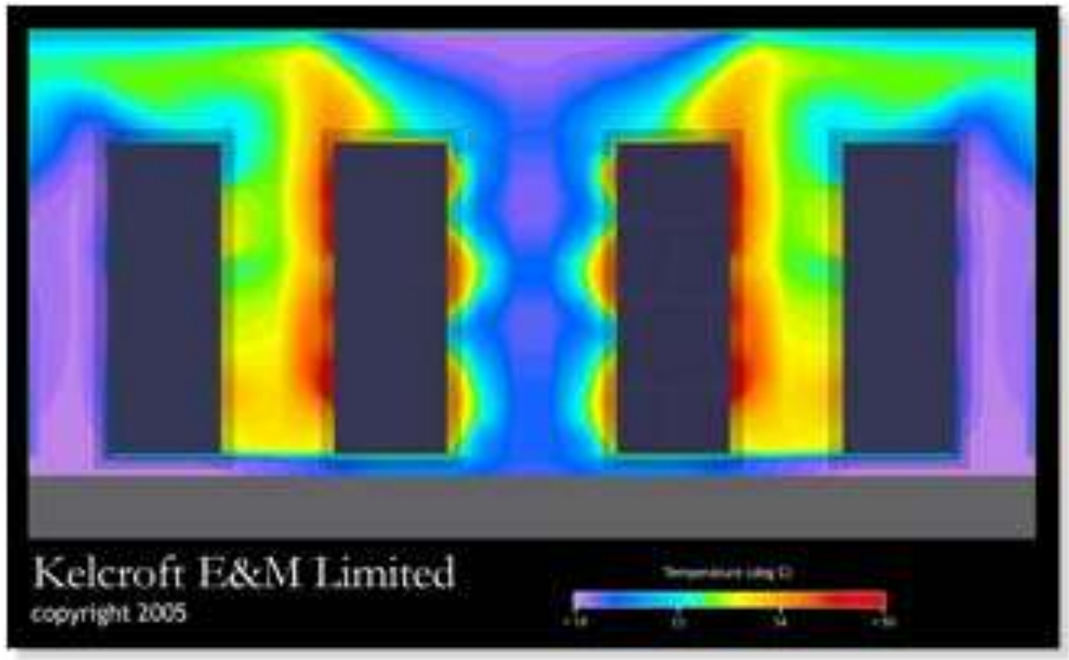
Páratartalom szabályozás kritikus, helyi redundancia

Kritikus tényezők:

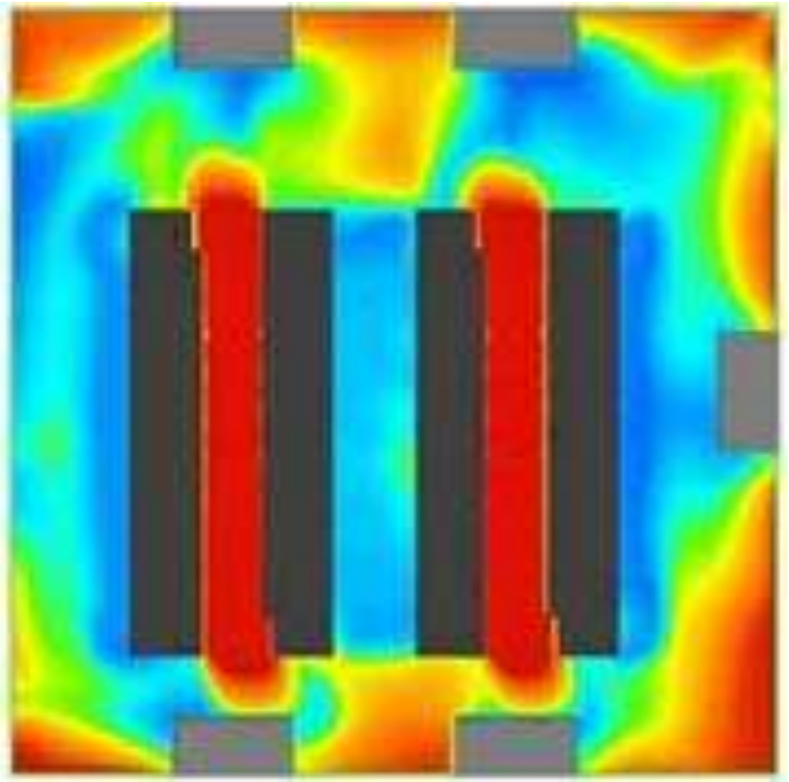
- Hosszú időre nem lehet meghatározni az extrém hőterhelés géptermen belüli eloszlását és helyét
- Utólagos géptermi hűtőköri csövezés
- Géptermen kívüli egységek fizikai biztonsága

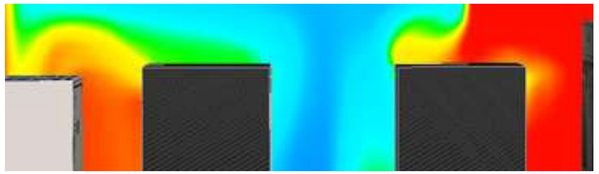


# Technikai biztonsági kérdések - hűtés




2. Hideg-meleg folyosó





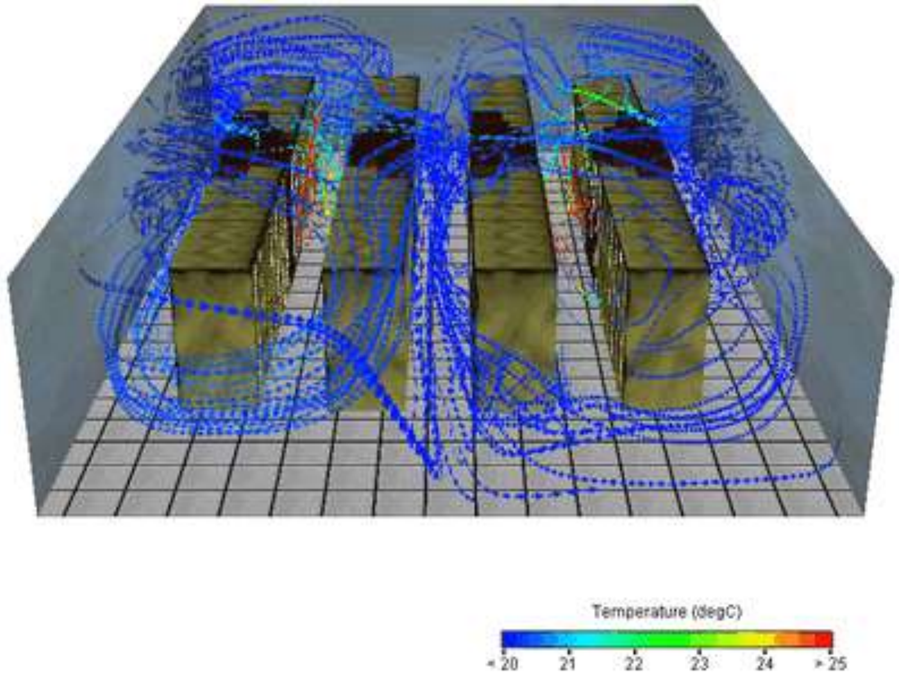
1. Hot spot

Server air in: up to 27C°

Server air out: up to 40-45C°

# Technikai biztonsági kérdések - hűtés

3. Levegő mennyiség (Air in = Air out)




4. Páratartalom (40-70%)

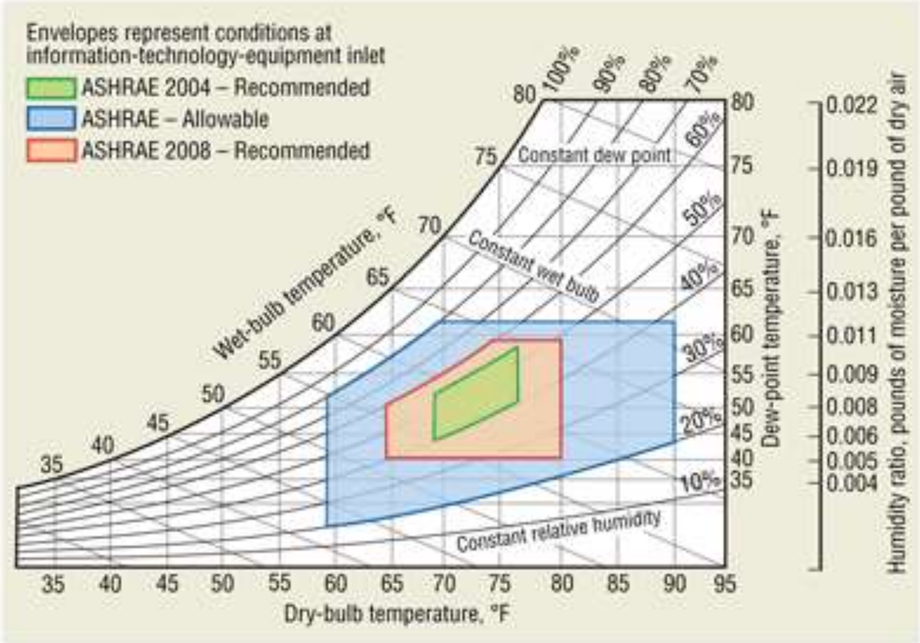
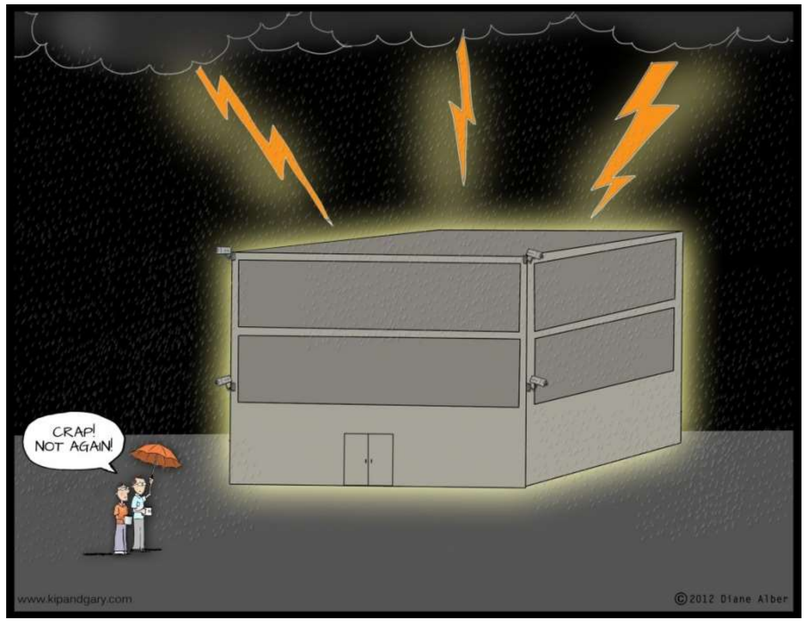



**FIGURE 1. ASHRAE environmental specifications.**

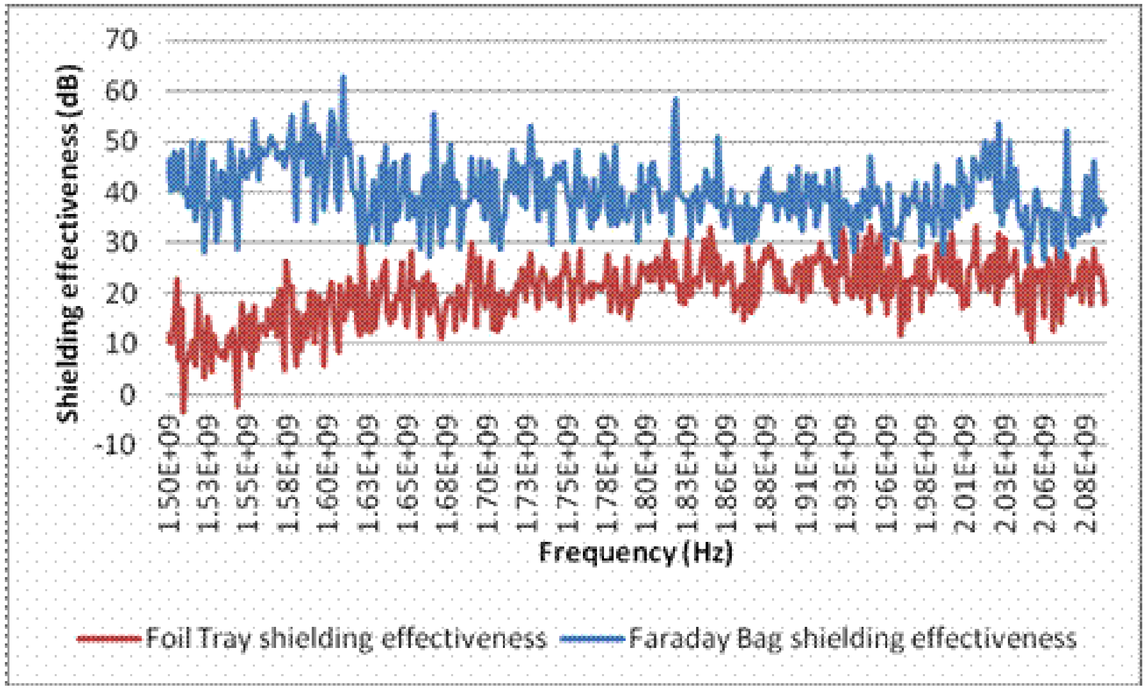
# Technikai biztonsági kérdések - áramellátás

1. Szolgáltatói hiba 10/20/120kV – középfeszültségi függetlenség

2. Villám és túlfeszültség védelem
- EM hatások
- Külső fémes kapcsolatok
- Árnyékolás, Faraday



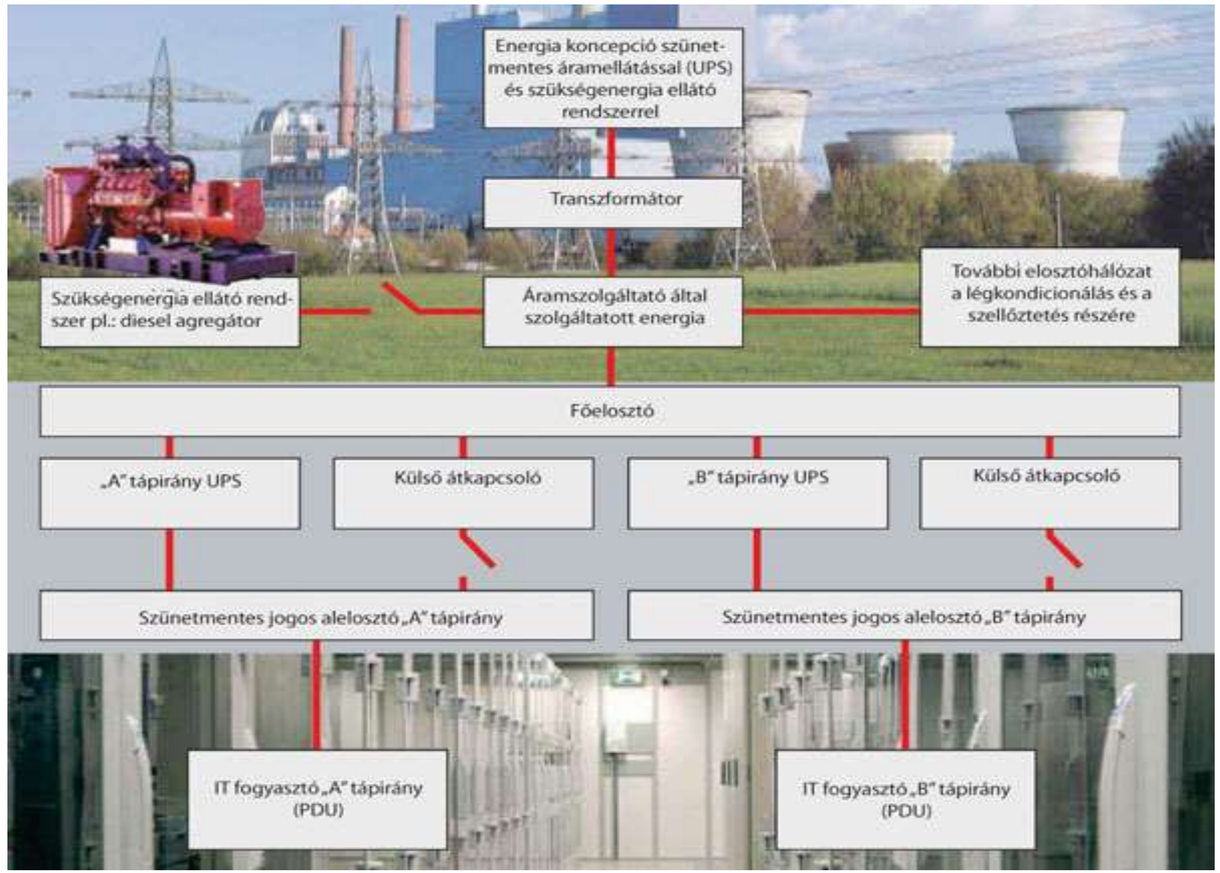
# Technikai biztonsági kérdések - áramellátás




3. EMC árnyékolás

- Milyen frekvencián? (jellemzően 100Mhz-3Ghz)
- Milyen csillapítás? (jellemzően 40-60dB, katonai környezetben 100dB)
- Másodlagos villámvédelem
- EM bomba?
- EM és RF támadás?
- Lehallgatás?

# 99,98% rendelkezésre állás energiaellátási modellje




0,4kV-os hálózati redundancia
(avagy hogyan legyünk 10ms alatt)

# Technikai biztonsági kérdések - biztonságtechnika

**Ellenőrzés:**

- Csomagellenőrzés
- Gépjármű ellenőrzés

**Megfigyelés:**

- Mozgásérzékelés, nyitásérzékelés
- CCTV

**Hozzáférés kezelés:**

- Beléptetési szintek, jogosultságok
- Zsiliprendszerek, biometrikus, proximity

**Biztonsági rend fenntartása:**

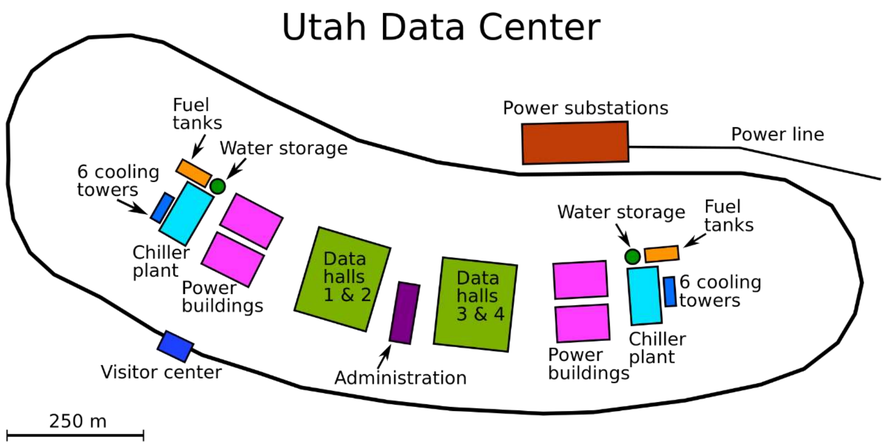
- Az egyes védett eszközökhöz történő fizikai hozzáférés szabályozása
- Számkombinációs védőeszközök, jelszó kezelés és érvényesítés,
- Rejtett szabotázs-védelmi kapcsolók, egyéb biztonsági elemek és

**INTEGRÁCIÓ**!

# Nagy nemzetközi adatközpontok

# Yahoo – PUE!

# NSA – Utah Data Center



# Apple – Under construction

**1 THE DATA CENTER THAT POWERS THE iCLOUD:** Apple's 500,000 square foot Maiden, NC, facility was completed last year.

**2 THE QUESTION MARK:** Apple is building a 4.8 megawatt biogas-powered power generator right next to the data center. This looks like the spot it will go.

**3 THE SOLAR ARRAY:** This 100 acre solar power farm will generate 20 megawatts of power.

# És a hazai gyakorlat…

# Köszönöm a figyelmet!

PERSECUTOR

www.persecutor.hu