



# Hálózatbiztonsági alapismeretek I.



**Hirsch Gábor, Cisco Systems Magyarország**

# Alapfogalmak



# Információ

- Információ: objektumok állapotáról szóló megállapítás
- Térben és időben értéket képvisel
- Hozzáférhetőség->Kommunikáció  
Eltitkolás->Védelem

# Kommunikáció

- Kommunikációs Csatorna:

küldő->üzenet->fogadó

- Kódolás folyamata->az információból adat keletkezik  
Dekódolás folyamata->az adatból információ keletkezik
- Az adat az információ tárgyiasult formája

# Kommunikáció formái

- Közvetlen kommunikáció (pl: beszéd)
- Közvetett kommunikáció (pl: levél)  
rögzítés->adathordozó megjelenése

információ=adat=tárolt adat=megjelenített adat=információ

Adatvédelem: védelem az adathordozók megsemmisülése ellen és az adat illetéktelen kezekbe jutásának megakadályozása.

# Napjaink elvárásai

- Az adathordozók állapota nem észlelhető emberi érzékszervekkel
- Az adatvédelem magasabb szintje szükséges.
- Adatbiztonság: az adatok manipulálhatóságának védelme.

# Adatbiztonság, Adatvédelem



# Védelem területei

Humán

Fizikai

Algoritmikus

Adminisztratív

# Fenyegetettségek

Bizalmasság

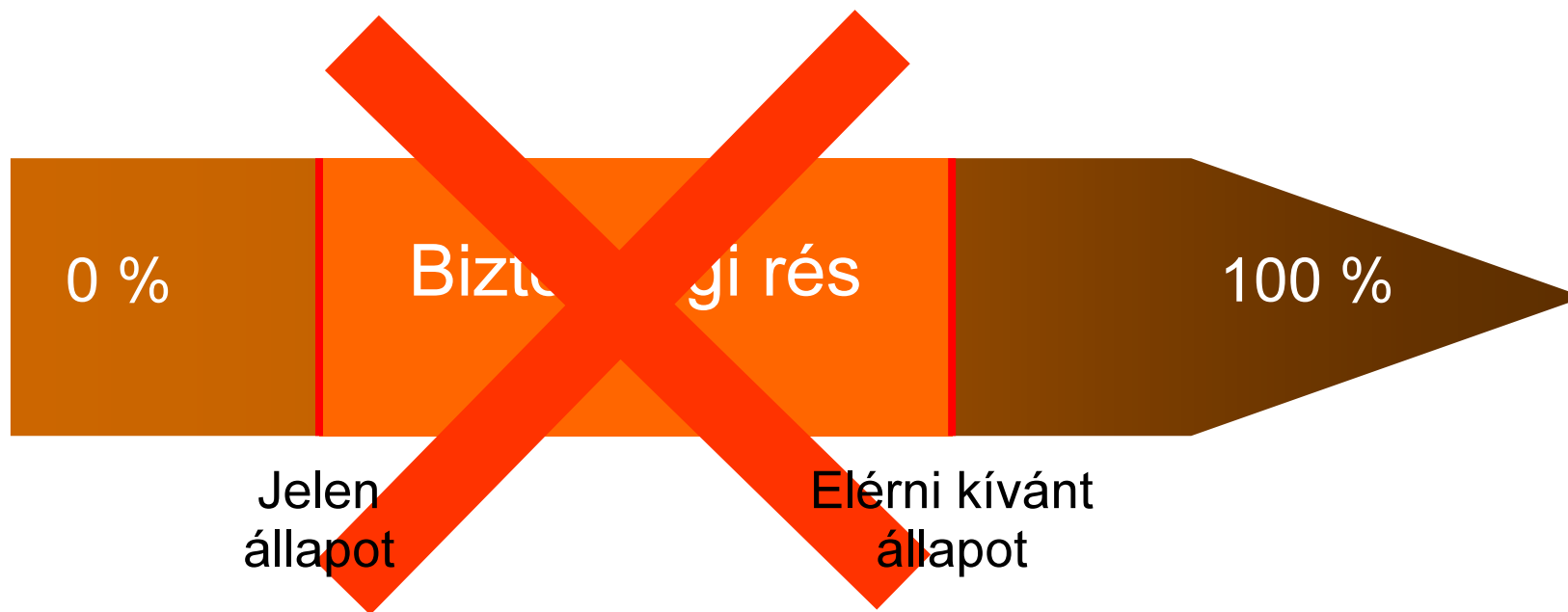
Hitelesség

Sértetlenség

Rendelkezésre állás

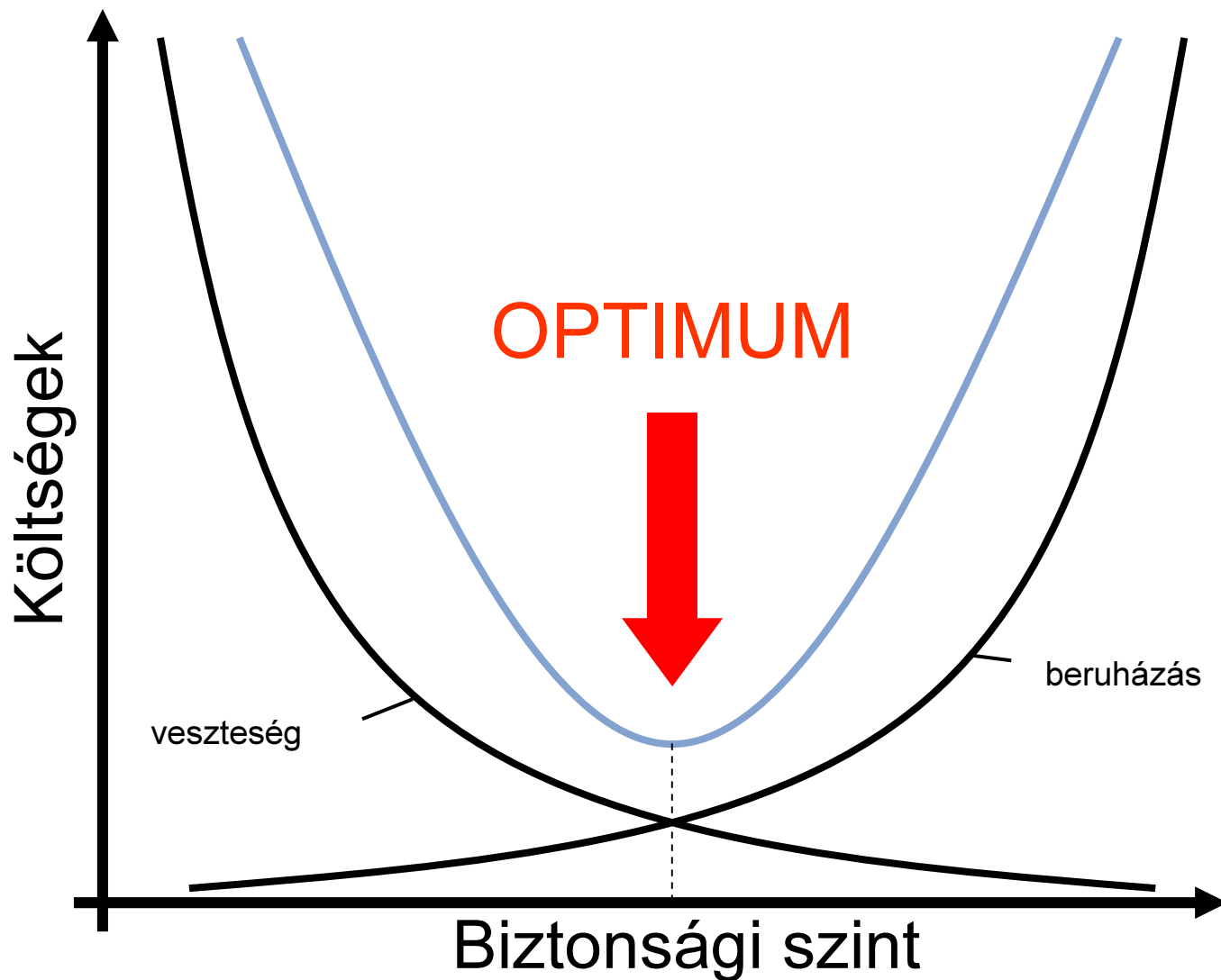
Időbeni letagadhatatlanság

## Mi a cél?



## A biztonsági rés megszüntetése

# Mennyibe kerül?



# Speciális területek

- Pénzügyi szektor
  - Tranzakció biztonsága
  - Tranzakció letagadhatatlansága
  - Banki adatok bizalmasága
- Telekommunikációs szektor
  - Üzletmenet folytonosság
  - Előfizetői adatok bizalmassága

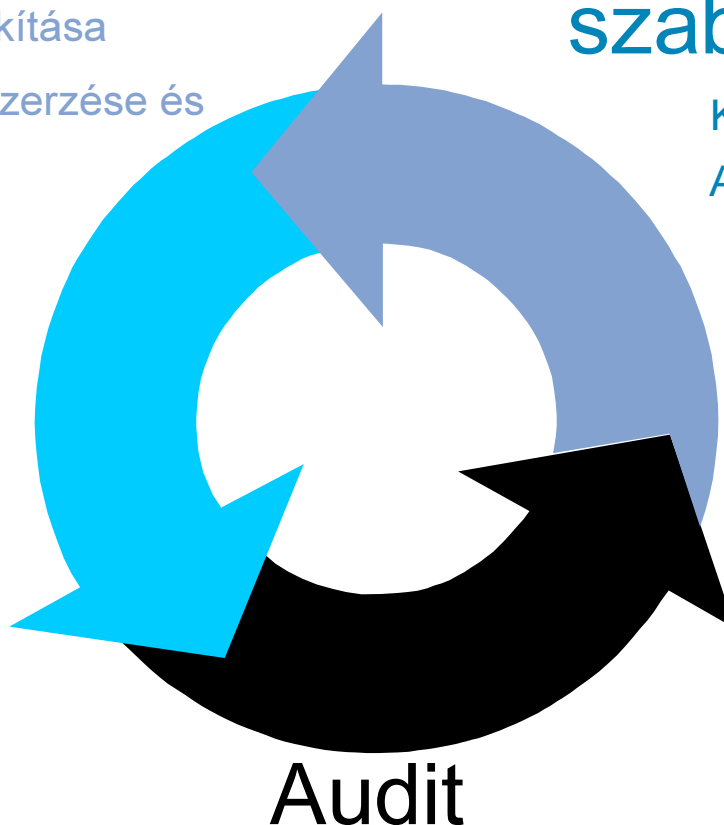
# A biztonság, mint folyamat

## Megvalósítás

Biztonsági folyamatok kialakítása  
Eszközök kiválasztása, beszerzése és telepítése  
Bevezetés, oktatás

## Adminisztratív szabályzás

Kockázat elemzés  
Adminisztratív rendszer  
Biztonsági politika  
Biztonsági házirend  
Biztonsági szabályzatok



Mennyire valósul meg az elérni kívánt biztonsági szint

# Algoritmikus védelem



# Miért?

- Adatlopás-Adatmanipuláció  
anyagi vagy más természetű haszon reményében
- Figyelemfelkeltés  
politika, világnézeti különbségek  
kivételes esemény  
stb.
- Kedvtelés

# Hol?

- Szempontok:
  - Leggyengébb láncszem ellen
  - Tárolt információ értékének arányában
- Támadás helyszínei:
  - Kívülről
  - Belülről

# Hogyan?

- Fizikai támadás
- Technológiai támadás
- Social Engineering

# Kevin Mitnick trófeái

## 1993-1994

Sun, USA; Solaris forráskód: **\$80M**

NEC, Japán; mobiltelefon források: **\$1.75M**

Nokia, Finnország; HD760 projekt: **FIM 2.5M**

Nokia, UK; "Mobile software": **\$135M**

Novell, USA; Netware források: **\$75M**

Fujitsu, USA; PCX telefon-források: **\$2.1M**

Source: <http://www.hackernews.com/orig/letters.html>



NBC News

## Kevin Mitnick ítélete

- Elítélve: 1999 augusztus 9.
- Összérték: \$296,000,000
- Mitnick büntetése: \$4,125
- És 46 hónapi szabadságvesztés
- 2000 januárjában kiszabadult

# Technológiai támadások

- Verzió és alkalmazás hibák kihasználása
- Emberi mulasztás kihasználása
- Elárasztásos (DoS, DDoS) támadás
- Lehallgatás
- Gyenge titkosítás alkalmazása
- Nem biztonságos hálózatok
- Nem biztonságos adattárolás
- Rossz felhasználó-azonosítás

# Felhasználói elvárások



# A felhasználók három fontos elvárása



## EGYSZERŰSÍTÉS

- Scale
- Cost
- Staffing
- Integration and systems management



## ALKALMAZÁSOK OPTIMALIZÁLÁSA

- Enablers
- Awareness
- App management
- Performance/optimization
- Resilience



## HÁLÓZATBIZTONSÁG FOKOZÁSA

- Threats
- Theft
- Loss
- Response time

# Security = Still a Top Business Issue

## Top Business Trends

	Ranking
<b>Security breaches/business disruptions</b>	<b>1</b>
<b>Operating costs/budgets</b>	<b>2</b>
<b>Data protection and privacy</b>	<b>3</b>
Need for revenue growth	4
Use of information in products/services	5
Economic recovery	6
Single view of customer	7
Faster innovation	8
Greater transparency in reporting	9
Enterprise risk management	10

Source: Gartner Group, 2004

## Top Security Challenges

	Ranking
<b>Limited budget</b>	<b>1</b>
<b>Regulatory compliance</b>	<b>2</b>
<b>Educating executives on risks</b>	<b>3</b>
<b>Scope, volume and proliferation of data/devices</b>	<b>4</b>
<b>Not enough security staff</b>	<b>5</b>
Wireless LANs	6
Mobile clients	7
Company growth	8
Volume and complexity of network traffic	9
Lack of key security skills	10

Source: CSO/Cisco Proprietary Research, April 2006

# A biztonsági kihívások evolúciója

A károkozás célja és mértéke

Egyre gyorsabban terjedő veszély

**TELJES**  
Infrastruktúra

**Másodpercek**

**REGIONÁLIS**  
hálózatok

**Percek**

**ÖSSZETETT**  
hálózatok

**Napok**

**EGYES**  
hálózatok

**Hetek**

**First Gen**  
• Boot viruses

**Second Gen**  
• Macro viruses  
• Denial of Service

**Third Gen**  
• Distributed Denial of Service  
• Blended threats

**Next Gen**  
• Flash threats  
• Massive “bot” driven DDoS  
• Damaging payload worms

**EGYES**  
számítógépek

**1980-as**

**1990-es**

**Napjainkban**

**A jövőben**

# Konvergencia ... D / V / V / M

## Integrált és Átfogó Biztonság



# Q and A

