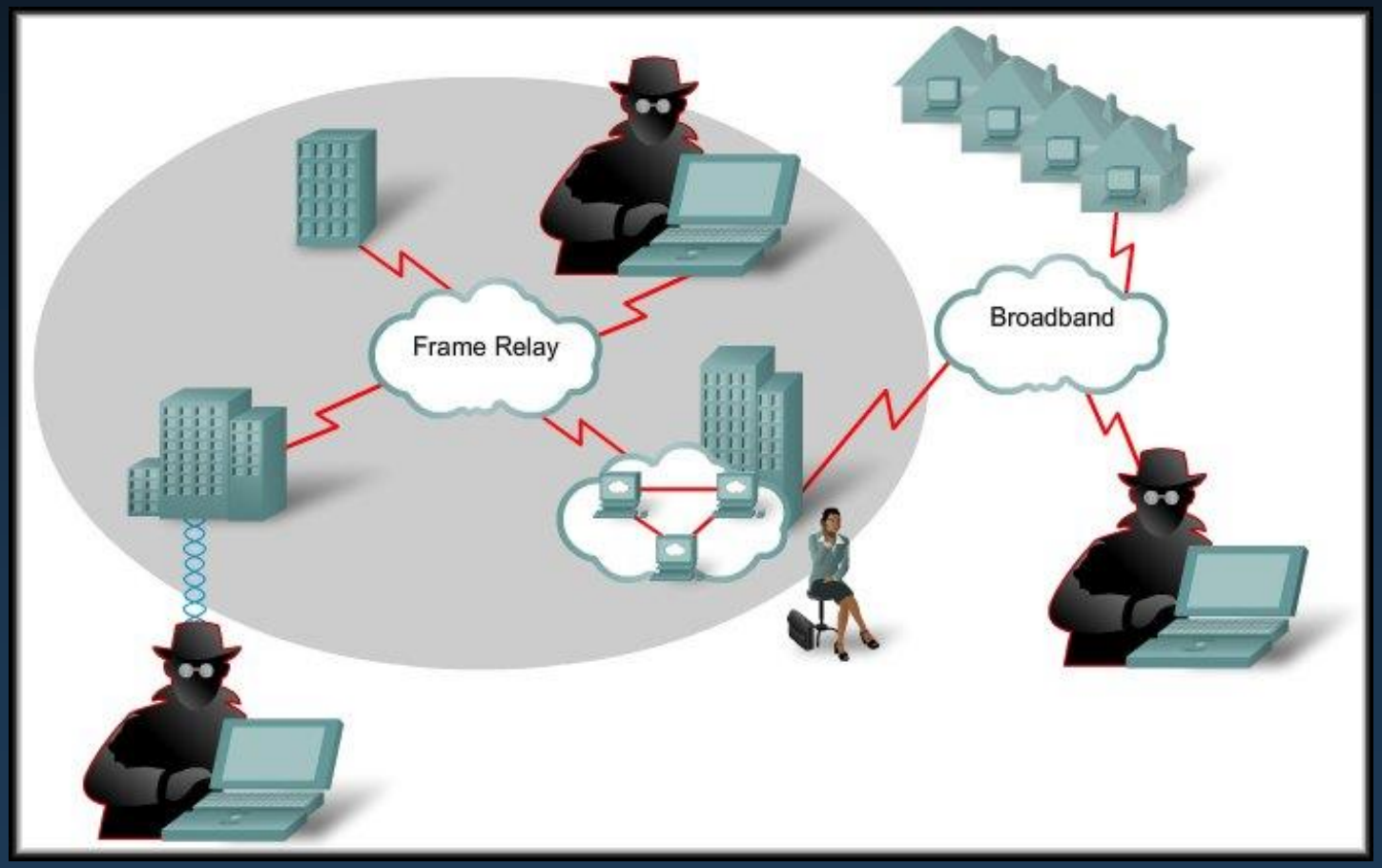
Sieťová bezpečnosť

I.

Základy sieťovej bezpečnosti



Základy sieťovej bezpečnosti

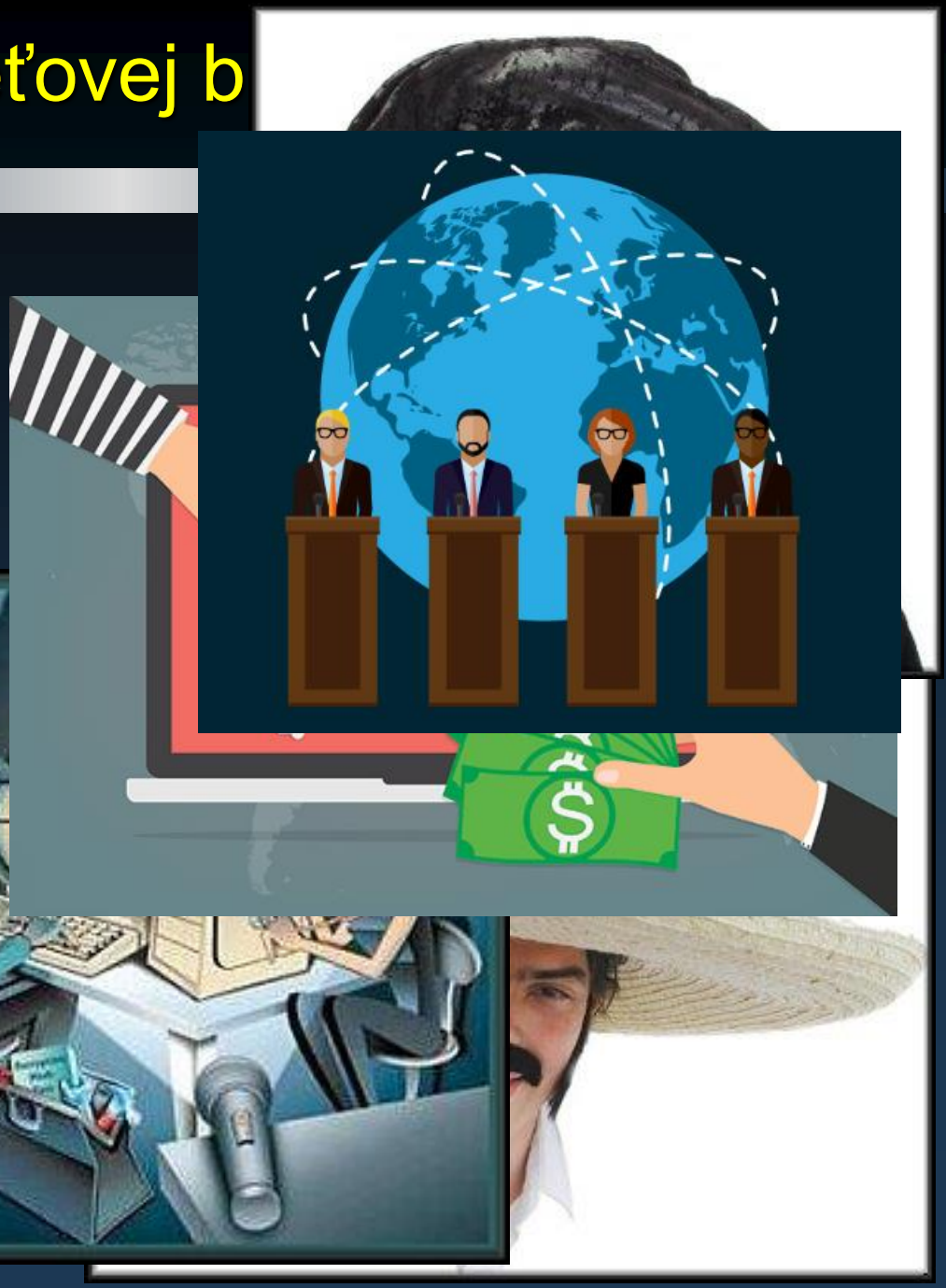
- Cisco Security kurz
  - Intro to Cybersecurity
  - Cybersecurity Essentials
  - Cybersecurity Operations
  - CCNA Security
- Informácie o zabezpečení
  - Web preventista.sk
  - http://preventista.sk/info/desatoro-bezpecneho-pocitaca/
  - http://preventista.sk/info/dvanastoro-bezpecneho-spravania/
  - A iné

Základy sieťovej bezpečnosti

- Význam bezpečnosti
  - V súčasnosti rastie význam bezpečnosti v IT
  - Hlavné dôsledky problémov s bezpečnosťou:
    - Strata súkromia - záznamy
      - Lekárske
      - Vzdelávacie
      - Finančné
      - Identifikačné
    - Krádež informácií
    - Právna zodpovednosť

Základy sieťovej b

- Pojmy:
  - White Hat
  - Black Hat (Grey Hat)
  - Hacker, Hactivists
  - Financial Gain
  - Politické ciele

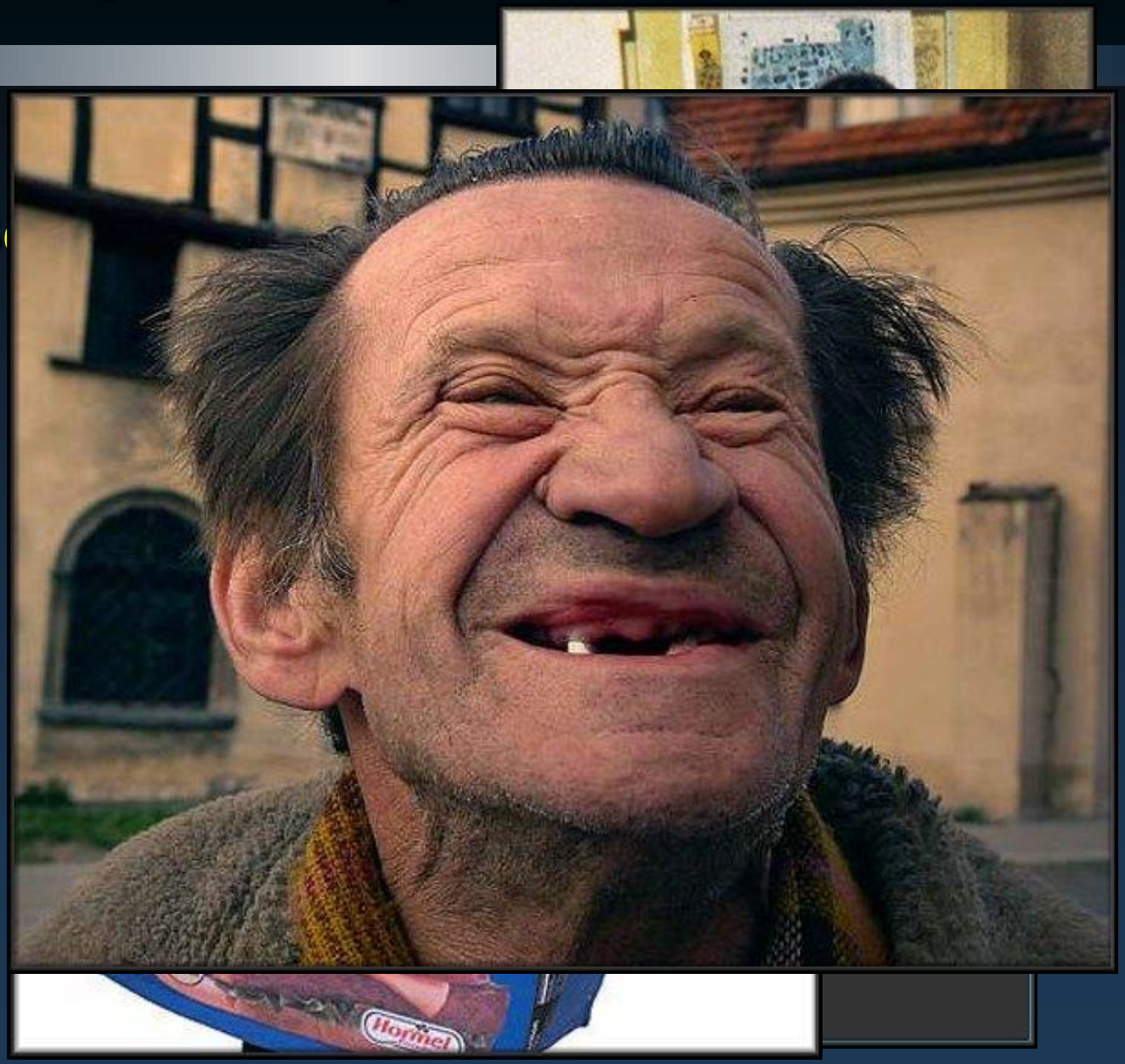


Zabezpečenie Internet of Things

- Internet of Things (IoT)
  - Zlepšuje kvalitu života
  - Napr. snímače životných funkcií
- Ako zabezpečiť?
  - Firmware
  - Bezpečnostné chyby
  - Aktualizácie
- DDoS útoky
  - Took down many websites.
  - Napadnuté zariadenia - webcams, routers, a iné IoT zariadenia slúžia ako botnet.
  - Zneužiteľné na DDoS.

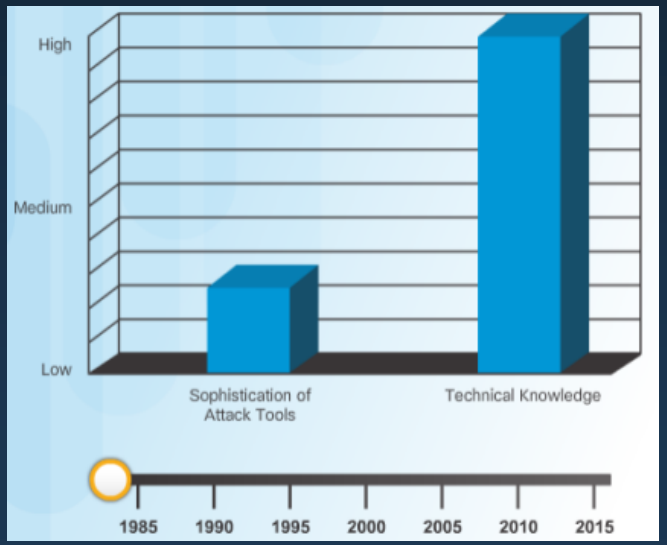
Základy sieťovej bezpečnosti

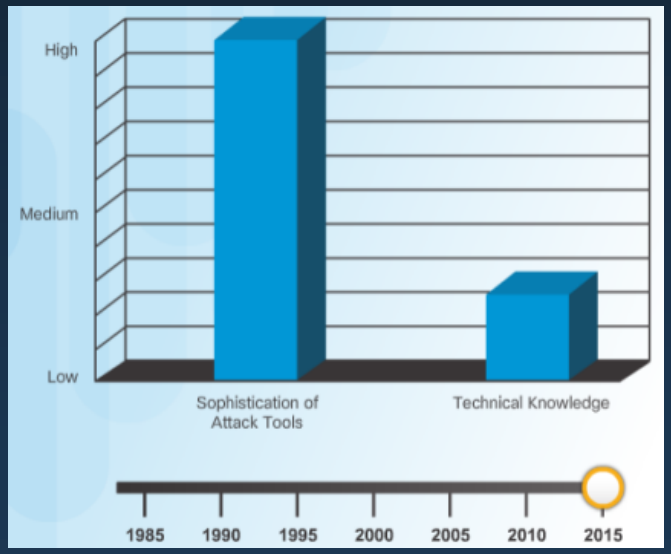
- Pojmy:
  - Cracker - S
  - Phreaker:
  - Spammer:
  - Phisher:



Základy sieťovej bezpečnosti

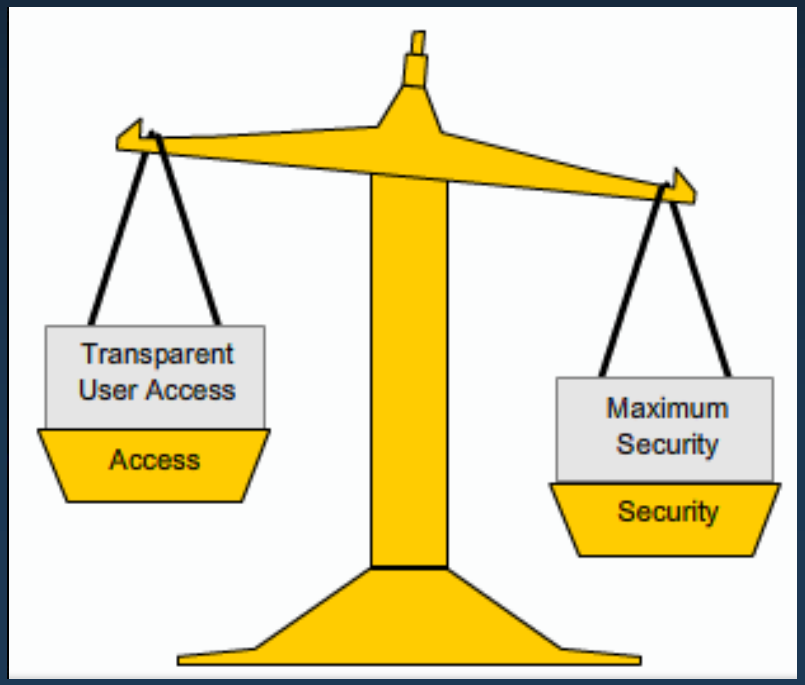
- Nárast počtu útokov:
  - V priebehu rokov rastie počet a dostupnosť útočných nástrojov - programov.
  - Klesá potreba vysokej technickej úrovne útočníka.





Základy sieťovej bezpečnosti

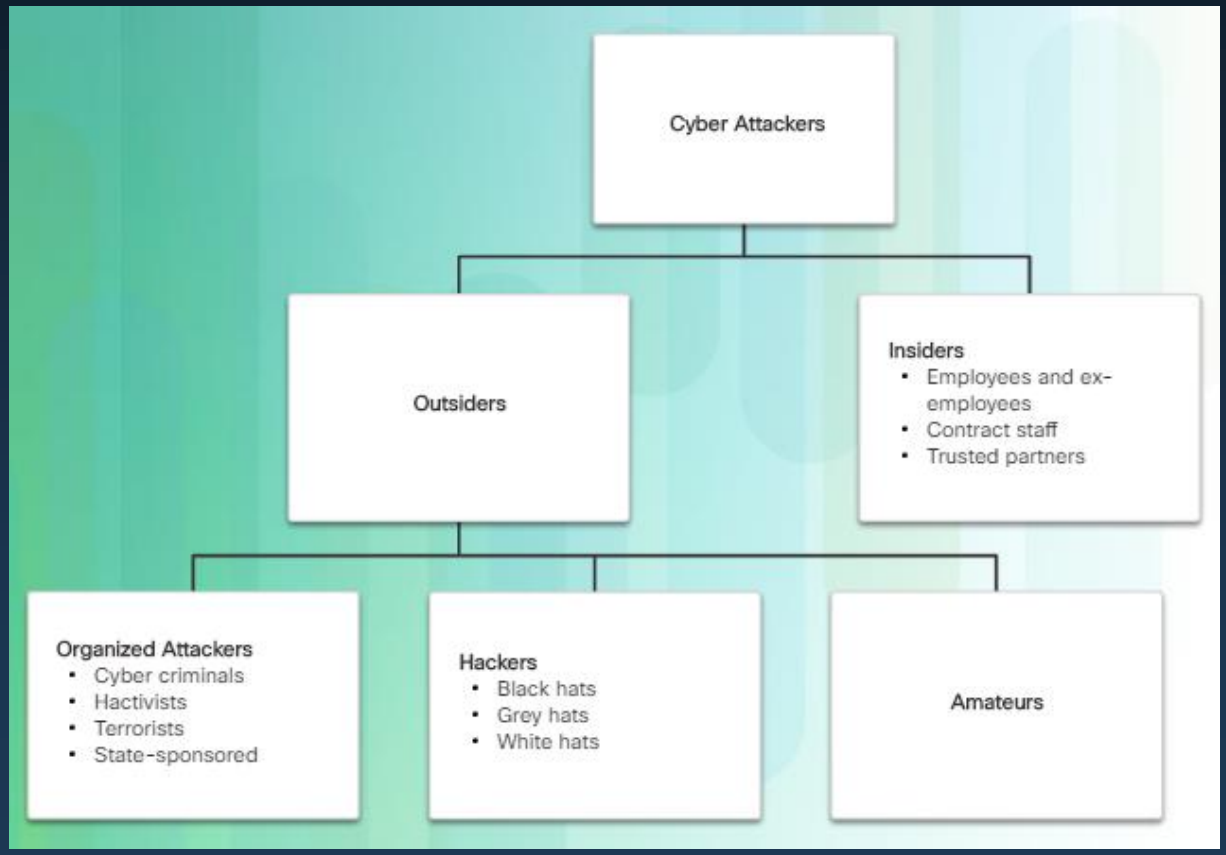
- Otvorené a uzavreté siete:
  - Úloha – nájsť optimálnu cestu.
    - Prístupnosť siete.
    - Zabezpečenie dát.



Spôsoby ohrozenia

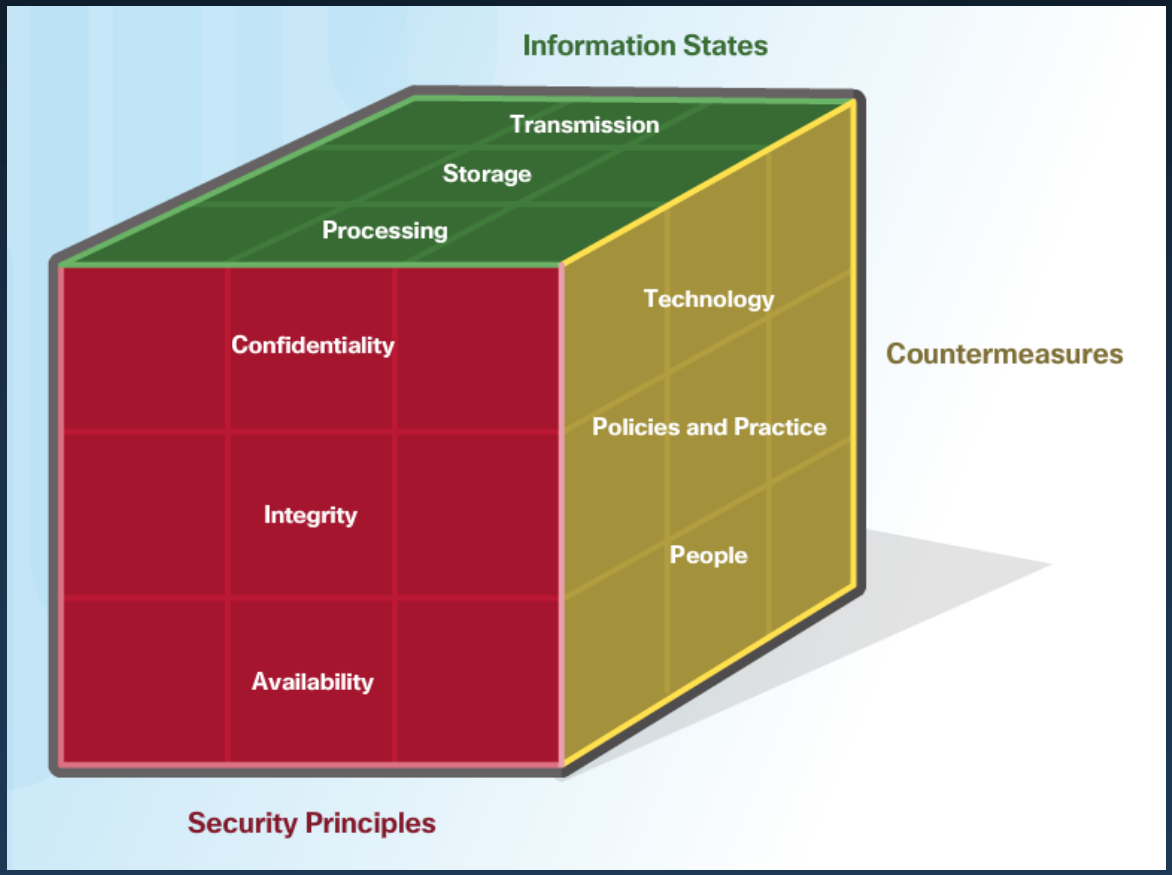
- Interné
  - Zamestnanci
  - Návštevy
  - Partneri
- Externé

- Mobilné zariadenia
  - BYOD



Bezpečnostná kocka

- John McCumber – autor
- 1. Zásady bezpečnosti – CIA
- 2. Stav informácií
- 3. Obranné prostriedky

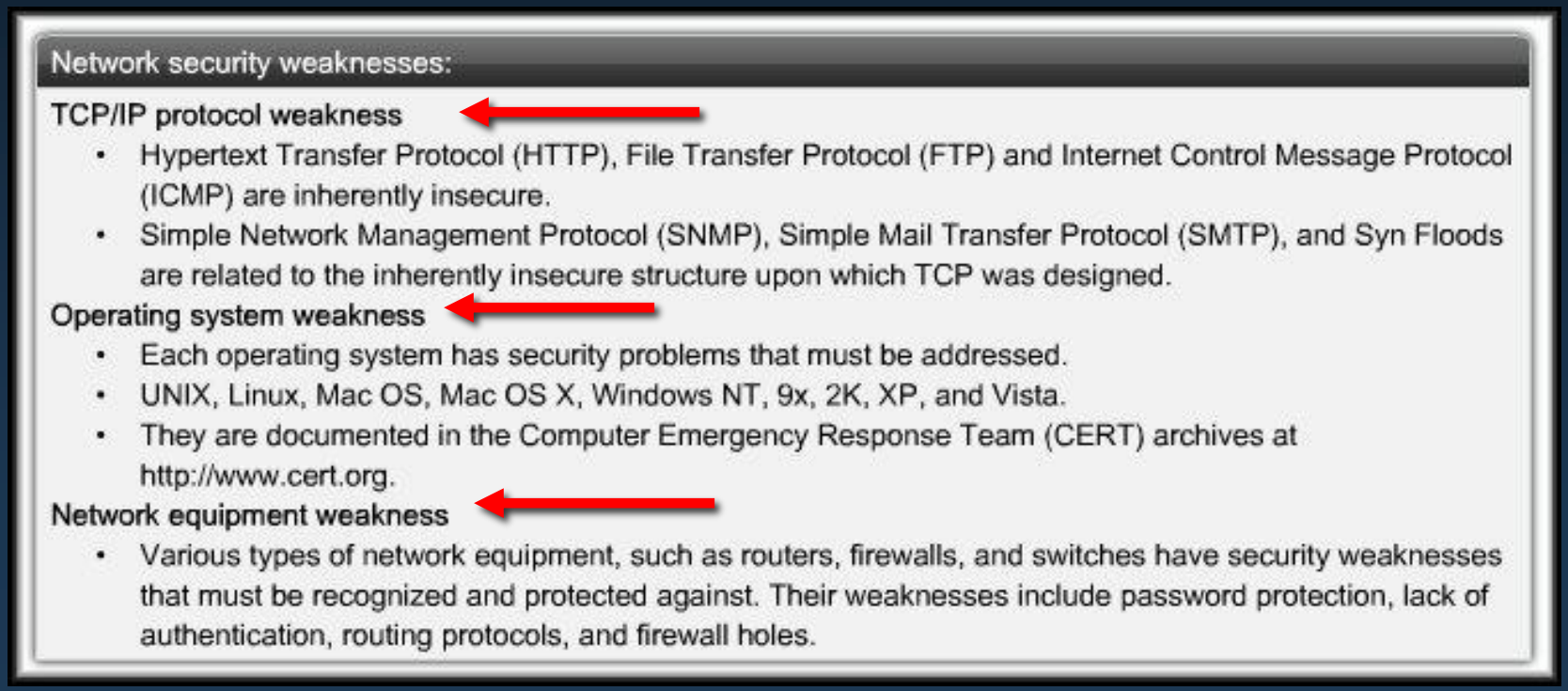


Kategórie bezpečnostných hrozieb

- Zraniteľnosť, ohrozenie:
  - Hardvérové
    - Úroveň problémov, ktoré vnášajú do siete zariadenia Router, switch, desktop, server a iné.
  - Softvér
- Hrozba:
  - Predstavuje osoby zaoberajúce sa vyhľadávaním chýb.
- Útok:
  - Rôzne nástroje a programy na útok proti sieti.

Ohrozenia

- 3 základné ohrozenia:
  - Technologické chyby.
    - Počítačové a sieťové technológie – základná úroveň ohrozenia.



Softvérové zraniteľnosti

- Pretečenie vyrovnávacej pamäte
- Nevalidovaný vstup
- Hazardné poradie vstupov
- Nedostatky v bezpečnostných postupoch
- Problémy s riadením prístupu

Typy škodlivého softvéru

- Spyware – sledovanie
- Adware – reklama
- Bot – vykonávanie operácií
- Ransomware – šifrovanie
- Scareware – strašenie
- Rootkit – úprava OS
- Vírus – vyžaduje spustiteľný súbor
- Trójsky kôň
- Červ – samostaný škodlivý softvér, samošíriteľný

Symptómy

- Zvyšuje sa využitie procesora.
- Rýchlosť počítača klesá.
- Počítač často zamrzne alebo havaruje.
- Rýchlosť prehliadania webových stránok klesá.
- Vyskytujú sa nevysvetliteľné problémy so sieťovými pripojeniami.
- Súbory sú upravené, alebo sa odstránia.
- Vyskytujú sa neznáme súbory, programy alebo ikony na pracovnej ploche.
- Existujú neznáme spustené procesy.
- Programy sa vypínajú alebo sa znovu konfigurujú.
- E-mail sa odosiela bez vedomia alebo súhlasu používateľa.

Ohrozenia

- 3 základné ohrozenia :
  - Konfiguračné chyby.
    - Chyby vytvorené administrátormi a inžiniermi, ktoré sa dajú opraviť dôkladným poznaním zariadenia.

Configuration Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.

Ohrozenia

- 3 základné ohrozenia :
  - Chyby bezpečnostnej politiky.
    - Ak užívateľ nerešpektuje zásady bezpečnostnej politiky.

Policy Weakness	How the weakness is exploited
Lack of written security policy	An unwritten policy cannot be consistently applied or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved applications create security holes.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise.

Sociálne inžinierstvo

- Nevyžaduje technické znalosti.
  - Útočník oklame zamestnanca s cieľom získať prístupové údaje.
- Phishing:
  - Jeden z typov SI s cieľom získať prístup k bankovým údajom, kreditným kartám.
  - Mail, web alebo osobne.
  - Najlepšia prevencia je vzdelávanie užívateľov a upozornenie na problematické maily, správanie.