

# Pokročilé bezpečnostné riešenia

Marek Kl'oc, CCSP, CCSE, CCDA  
Advanced Security Department, Lynx

# Legenda

- Pohľad do „kuchyne“ Lynx - kompetenčného centra pre Cisco bezpečnostné technológie
- Bezpečnostné hrozby – prehľad a príklady
- Bezpečnostné hrozby - riešenia
- Pokročilé bezpečnostné riešenia

**Pohľad do „kuchyne“ Lynx -  
kompetenčného centra pre Cisco  
bezpečnostné technológie**

# LYNX, vzťah k Cisco

- odd. Sieťová a komunikačná infraštruktúra
- odd. Pokročilé bezpečnostné riešenia - Cisco kompetenčné centrum pre bezpečnosť

# LYNX, odd. SKI

- Návrh a realizácia pokročilých projektov v technologickej oblasti Routing a Switching, Wireless, IP telefónie a IPT v Enterprise
- Advance Routing a Switching špecializácia
- Technologický Lab v oblasti Routing a Switching, Wireless so širokou množinou zariadení

# LYNX, odd. PBR

- **Realizácia typických projektov v oblasti technologickej bezpečnosti**
  - Budovanie bezpečnostných zón
  - Implementácia systémov detekcie prienikov
  - Implementácia centrálného monitorovania bezpečnosti
    - Implementácia endpoint security
    - Hardening serverov, staníc a databáz
- **PBR ako kompetenčné centrum pre Cisco bezpečnostné technológie**
  - Lab PBR – simulácia problémov zákazníka, simulácie útokov, prezentácie použitia Cisco bezpečnostných technológií

# LYNX, odd. PBR – Cisco Lab

## Cisco zariadenia

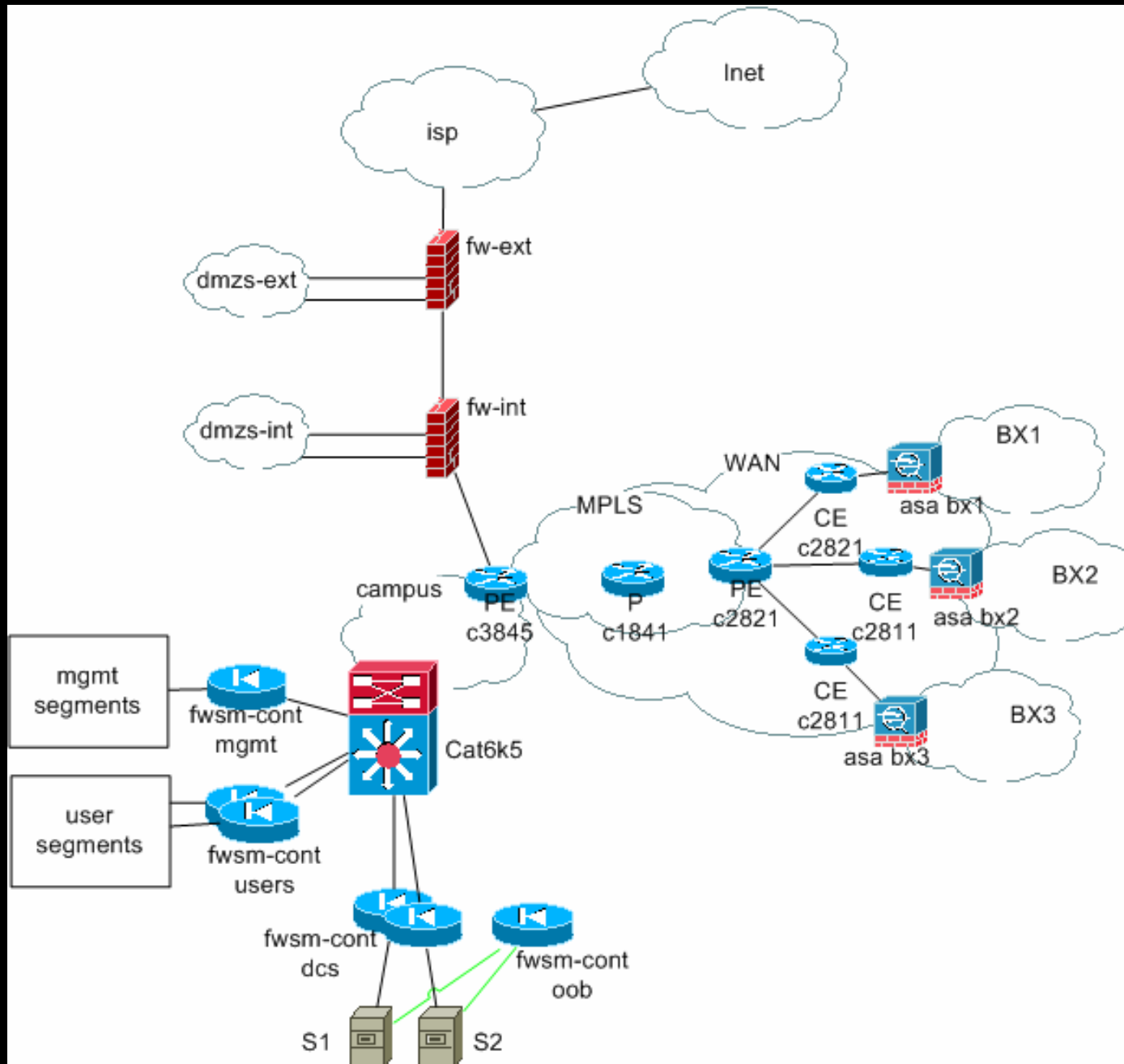
- Bezpečnostné zariadenia – FWSM(modul do 65k), ASA, PIX
- Log Manažment infraštruktúra – SIMS a MARS
- VPN koncentrátoary
- Network Intrusion Prevention (Standalone resp. servisný modul)
- Smerovače radu 18xx až 38xx
- Prepínače radu 29xx, 37xx, 49xx, 65xx
- Voice infraštruktúra
- Wireless - autonómny a lightweight
- Content engine
- NAC appliance a NAC Framework
- Secure Access Control server
- Security management server
- Security Agent infraštruktúra

# LYNX, odd. PBR – Cisco Lab

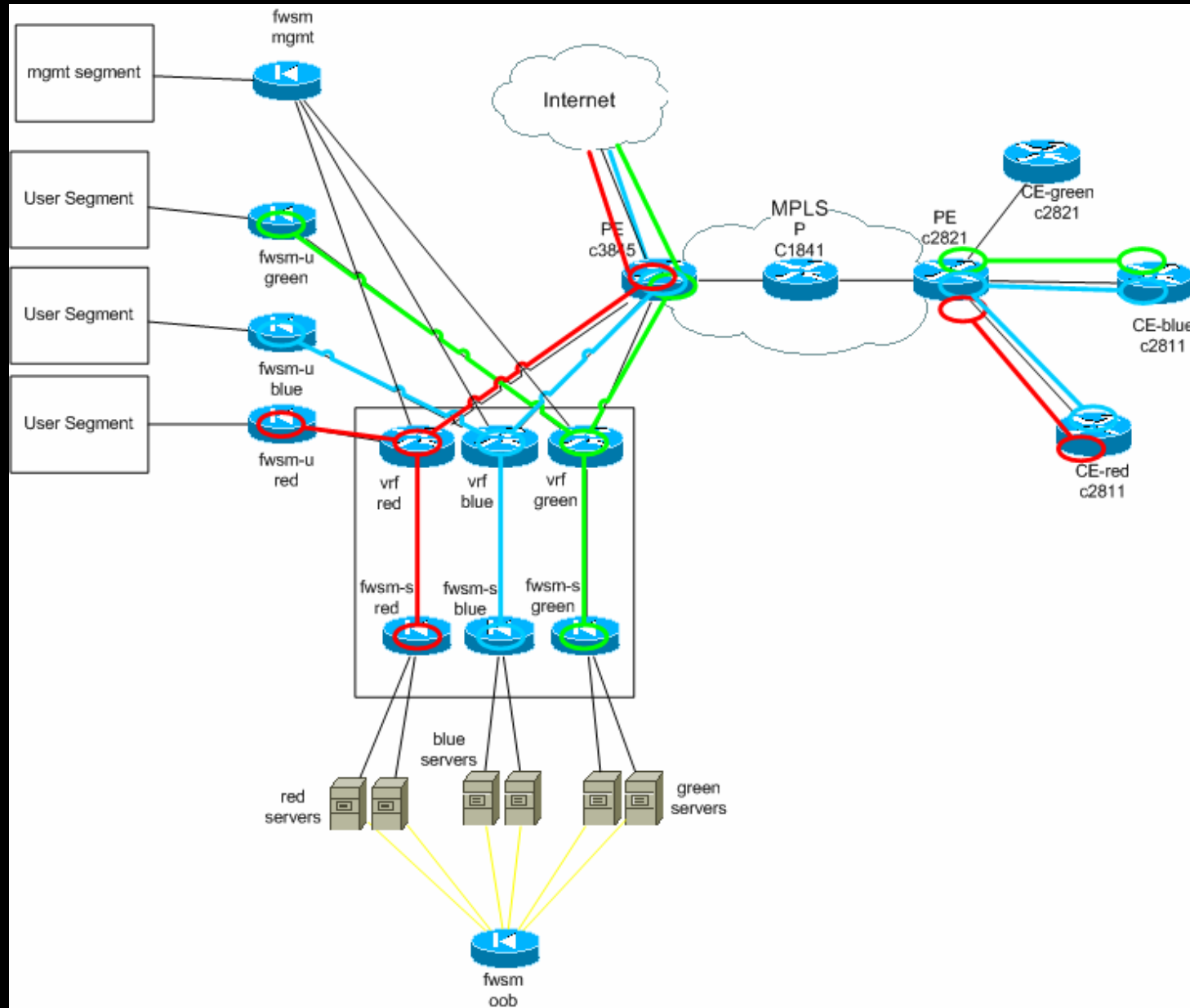
## Cisco technológie

- Filtrovanie paketov, obsahu, URL
- VPN (MPLS, RA-VPN, L2L-VPN, DMVPN, TEDVPN, EZVPN, PPTP, L2TP, GRE, SSLVPN)
- Smerovanie (BGP, OSPF, EIGRP, RIP) – autentizácia, filtrovanie smerovania, filtrovanie smerovacích protokolov
- Prepínanie (VTP, STP, VLAN, PVLAN, VLAN-ACL, DTP, Span) - hardening
- Autentizácia, Autorizácia a účtovanie AAA – protokoly RADIUS, TACACS+
- Rozšírené autentizačné protokoly - EAP – PEAP, FAST, TLS, MD5
- IOS Firewall a IOS PKI
- Netflow
- L2 security – DAI, IP Source Guard, DHCP Snooping, Port security

# LYNX, odd. PBR – Cisco Lab



# LYNX, odd. PBR – Cisco Lab



# Bezpečnostné hrozby

# Bezpečnostné hrozby - prehľad

- Buffer Overflow
- Neautorizovaný prístup
- Nesprávne použité bezpečnostné riešenia
- Chyby implementácie
- Prezradenie informácií
- Virus
- Trojan Horse
- Spoofing
- Backdoor Trojan
- Directory Traversal
- Multiple Vulnerabilities
- Format String
- Worm
- Cross-Site Scripting
- Privilege Escalation
- Arbitrary Code Execution
- Denial of Service
- „Day-Zero“ zraniteľnosti

# Bezpečnostné hrozby - prehľad

## Kritický malware v roku 2007

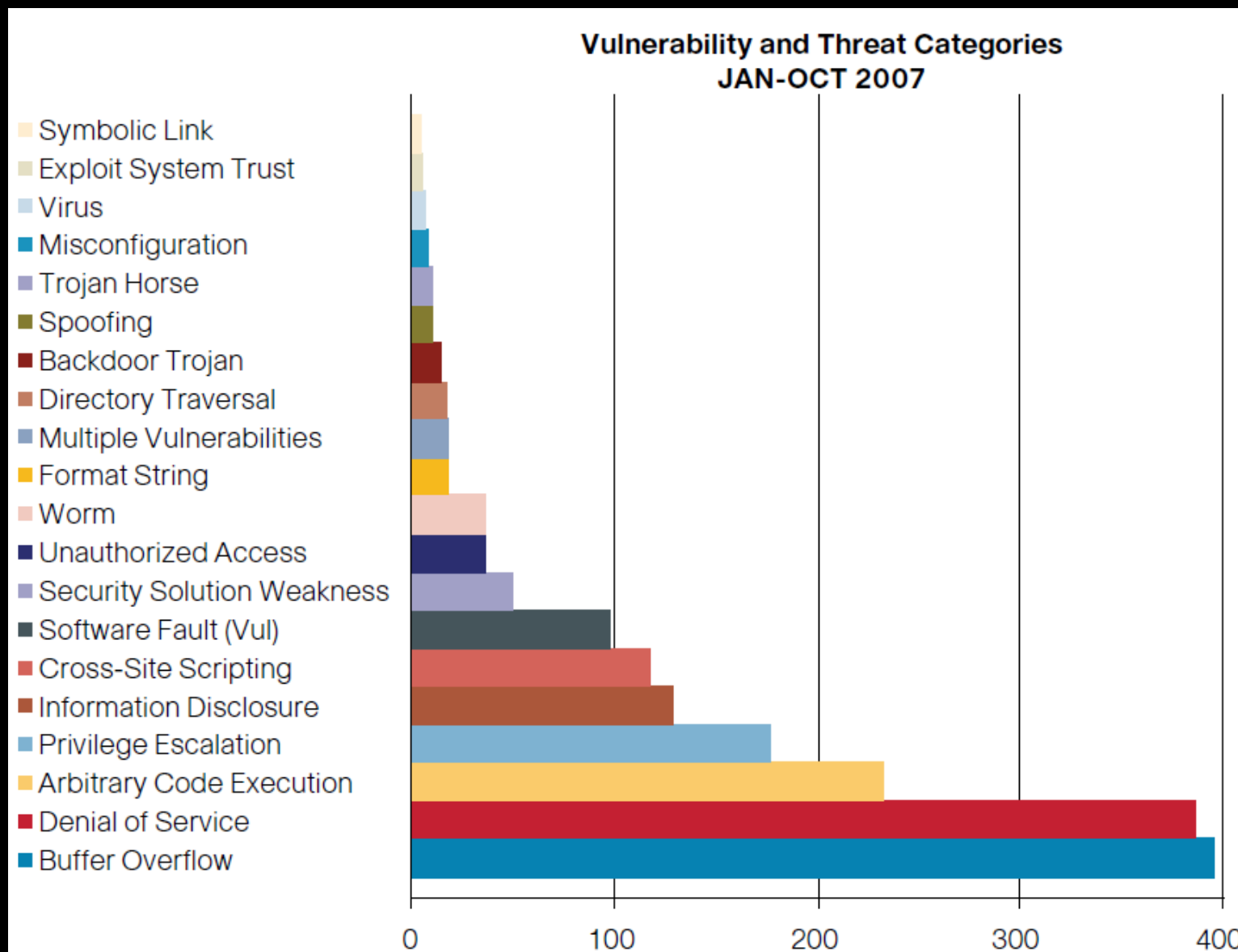
### STORM červ (tiež Peacomm, Nuwar, Zhelatin)

- Infiltrácia mnohými cestami (buffer/overflow, dokumenty, mail, url, mp3)
- Samostatne vyvíjajúci sa – prispôsobuje sa sieťovému prostrediu
- Môže stráviť čakaním i mesiace, po príkaze sa zmení (iné správanie)
- Po infiltrácii pripojí obeť k bootnetu s následným použitím obeť ako zdroj Spam-u resp. DDoS
- Veľmi sofistikovaný
- Predpokladaný počet obetí pripojených v bootnete – 10 mil.
- v2 = MAYDAY ?

### ANICMOO trójsky kôň

- využíva zraniteľnosť Microsoft Windows ANI, vykonaním ľubovoľného kódu
- exploit pre Microsoft Windows, zraniteľné sú mnohé Windows platformy vrátane Vista
- Po malej zmene kódu, je možné „oklamať“ existujúce signatúry antivírových programov

# Bezpečnostné hrozby - prehľad



# Bezpečnostné hrozby - prehľad

Threat Category	Alert Count	% Change from 2006
Arbitrary Code Execution	232	-24%
Backdoor Trojan	15	-72%
Buffer Overflow	395	23%
Directory Traversal	17	-52%
Misconfiguration	8	-57%
Software Fault (Vul)	98	53%
Symbolic Link	5	-64%
Worm	37	-28%

# Bezpečnostné hrozby - príklady

- Manipulácia so „Spanning Tree Protokolom“
- Private VLAN proxy útok

# Bezpečnostné hrozby - príklady

## Manipulácia so „spanning tree protokolom“

### Predpoklady:

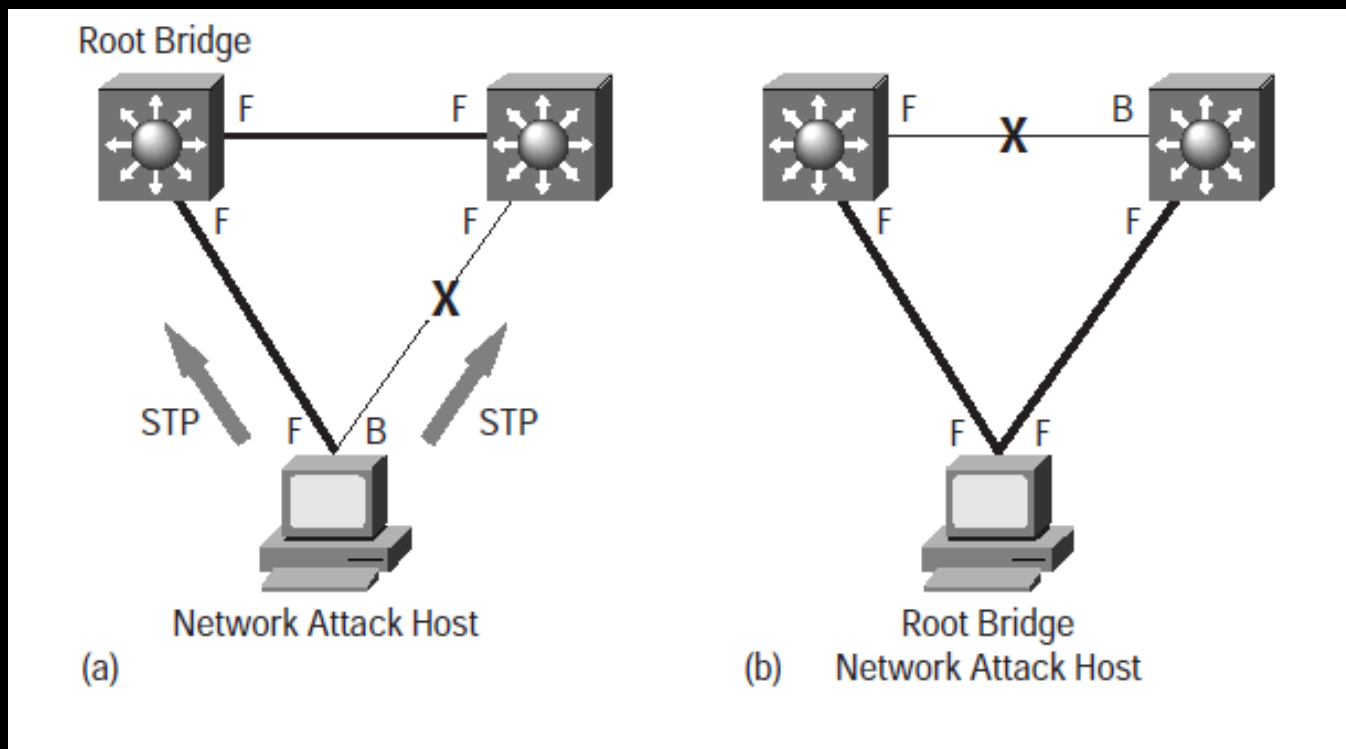
- PC s 1NIC resp. 2NIC
- OS s podporou Spanning tree protokolu
- Pripojenie do LAN resp. pripojenie na 2 rôzne prepínače

### Dopad:

- Presmerovanie sieťovej prevádzky cez útočníka
- Zahľtenie siete - DoS

# Bezpečnostné hrozby - príklady

## Manipulácia so „spanning tree protokolom„



# Bezpečnostné hrozby - príklady

## Manipulácia so „spanning tree protokolom“

```
Switch(config)# interface Gi1/11
Switch(config-if)# spanning-tree guard root
Switch(config-if)# end
Switch#
```

# Bezpečnostné hrozby - príklady

## Manipulácia so „spanning tree protokolom“

Príklad DoS:

1. Posielanie BPDU s ID = 1
2. Nastavenie minimálnej hodnoty časovača *max-age* (6 sec.)
3. Neposielanie BPDU spôsobu opakované „voľbu“ root prepínača
4. Opakovaním týchto krokov bude sieť „perzistentnom“ v stave „voľba root prepínača“ – otázka ako to využiť?

# Bezpečnostné hrozby - príklady

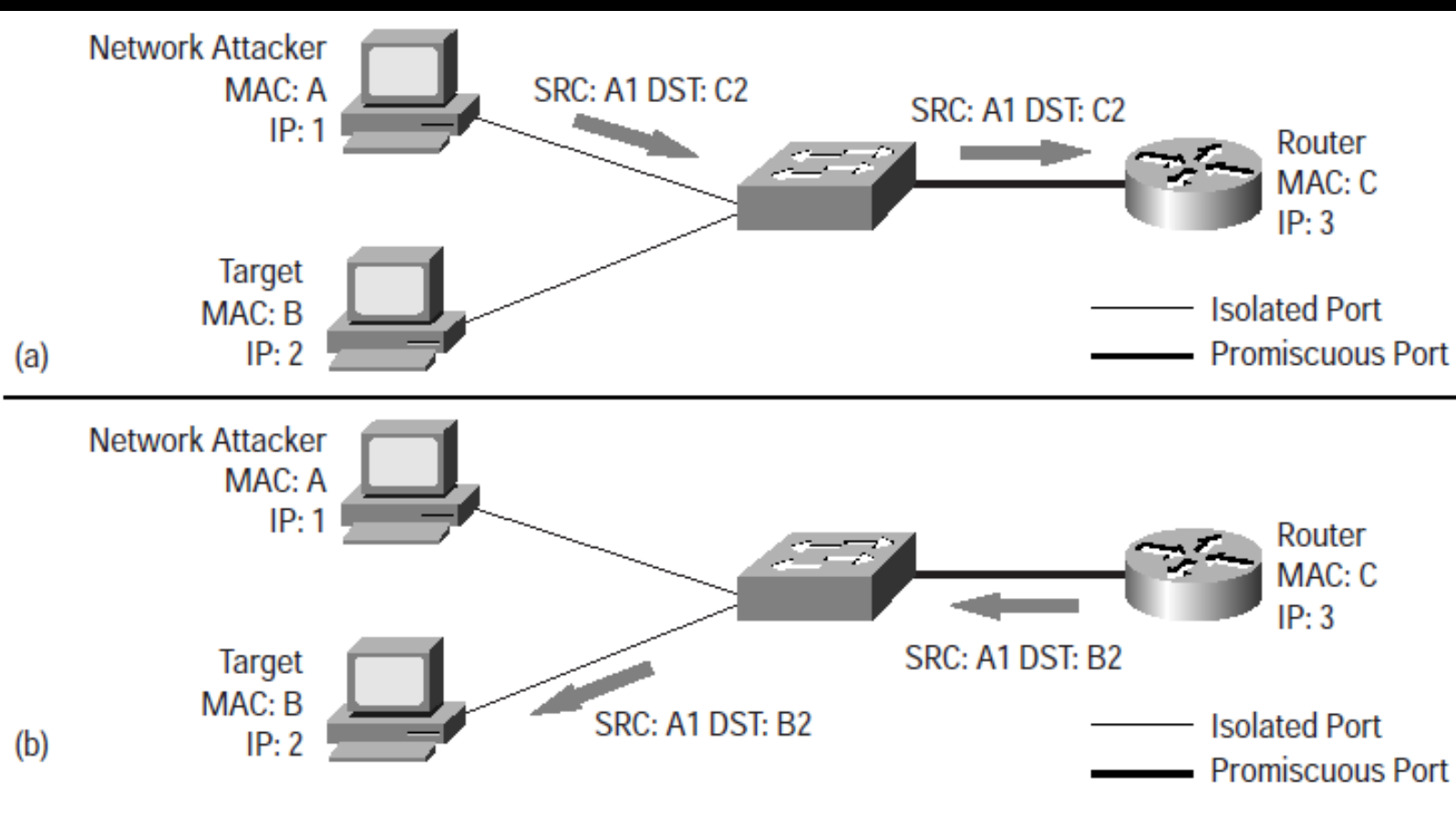
## PVLAN proxy útok

### Predpoklady:

- OS s možnosťou manipulácie paketov - Linux
- ACL na smerovači s default permit any – white list

# Bezpečnostné hrozby - príklady

## PVLAN proxy útok



# Bezpečnostné hrozby - príklady

## PVLAN proxy útok - riešenie

- ? Unicast Reverse Path Forwarding
- ? Dynamic ARP Inspection
- ? Source guard
- Input ACL na smerovači – deny ip ip\_net ip\_net-mask ip\_net ip\_net-mask
- VLAN ACL

# Bezpečnostné hrozby

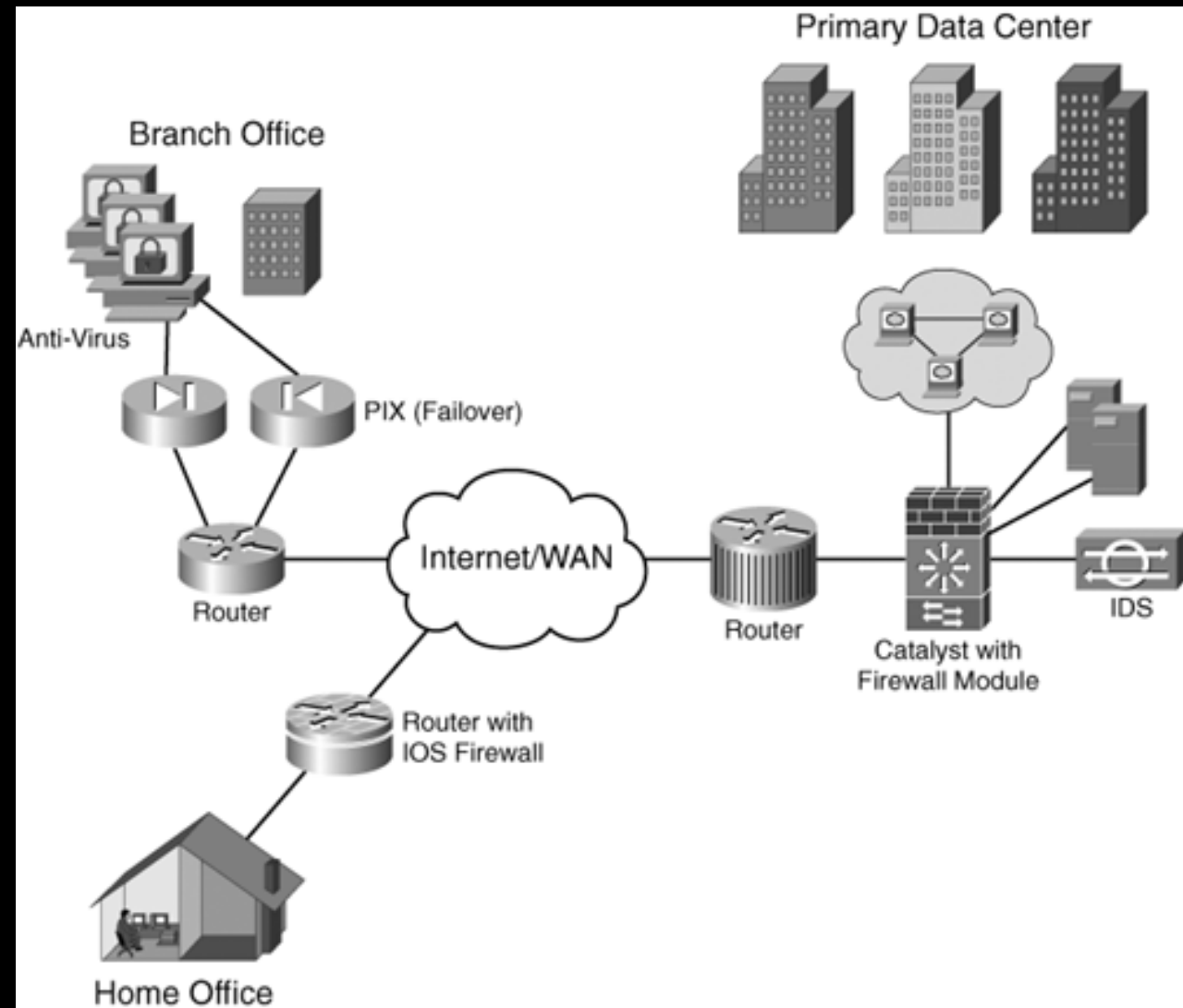
- **Dôležité odporúčania**
  - Patch management
  - Použiť HIPS s ochranou proti Day-zero útokom
  - Pravidelne sledovať trendy útokov a prispôbovať tomu korporátnu infraštruktúru
  - Bezpečné programovanie web aplikácií
  - Monitorovanie a logging

# Pokročilé bezpečnostné riešenia

# Pokročilé bezpečnostné riešenia

## Klasická bezpečnostná infraštruktúra

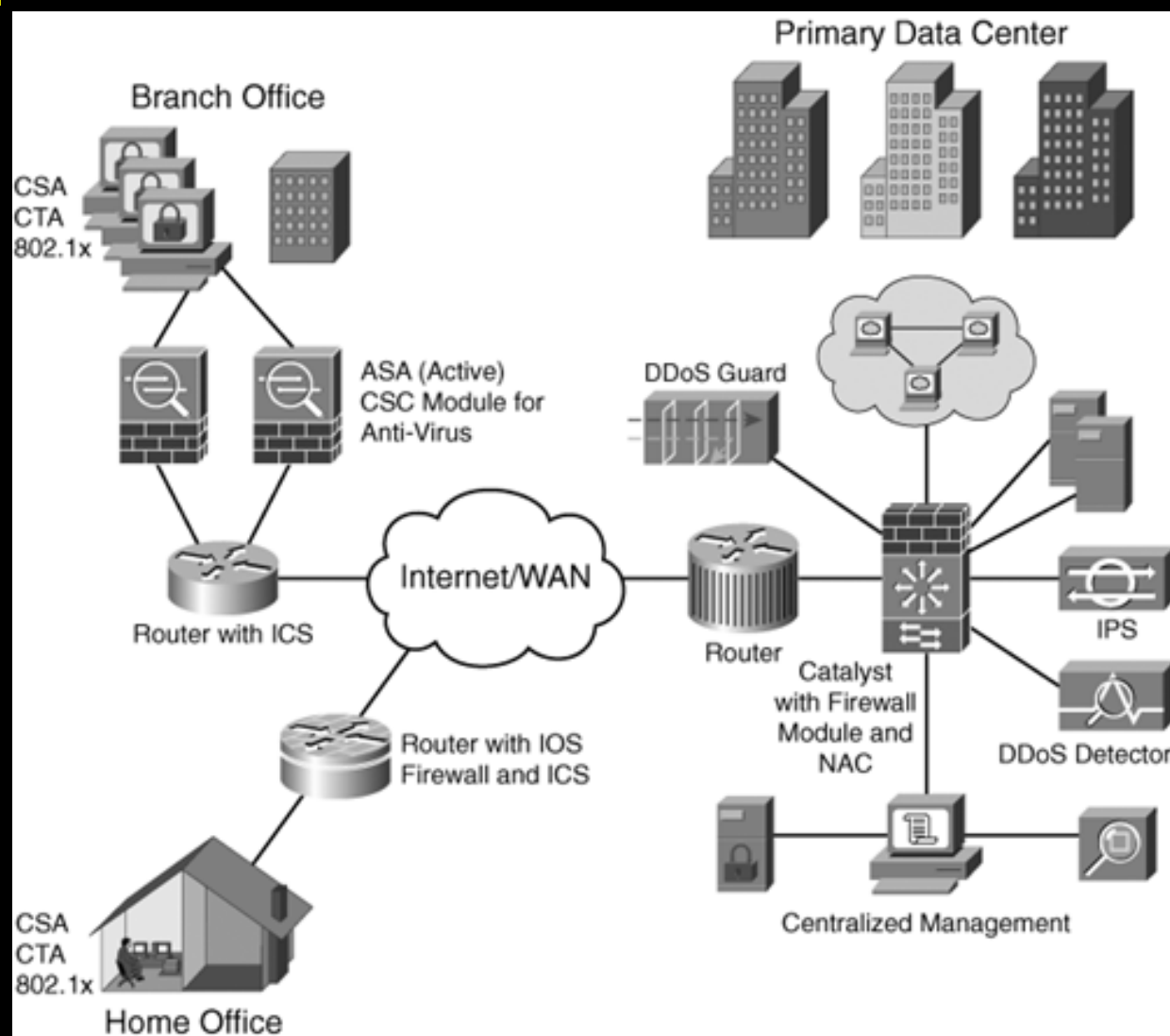
- Access lists
- Firewalls
- IDS
- VPN
- Antivírus



# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

- Security Information Management (SIM)
- Cisco DDoS guard a Cisco DDoS traffic anomaly detector
- Network Admission Control (NAC)
- Identity Based Network Services (IBNS)
- Host Intrusion Prevention (CSA)
- Adaptive Security Appliance (ASA)



# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Security Information Management (SIM)

- Import Netflow dát pre detekciu anomálií
  - Base line pre štandardnú sieťovú prevádzku
- Sofistikované rozpoznávanie dátových tokov (napr. NAT)
  - Rozpoznávanie konfigurácií zariadení
- Korelácia udalostí
- Redukovanie false positive
- Zobrazovanie vektoru útoku
- Vykonávanie aktívnej odozvy

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Cisco Adaptive Security Appliance (ASA)

- Antispoofing (uRPF)
- Možnosť integrácie s IPS resp. Content a Control Security (Antivírus, Antispam, Antiphishing, Antispyware, URL filtering, Content Security, File blocking)
- Aplikačná inšpekcia (DNS, HTTP, Voice, Netbios, PPTP, SQL, RPC)
- QoS
- VPN - L2L, RA-VPN, L2TP, PPTP

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### IEEE802.1x a IBNS

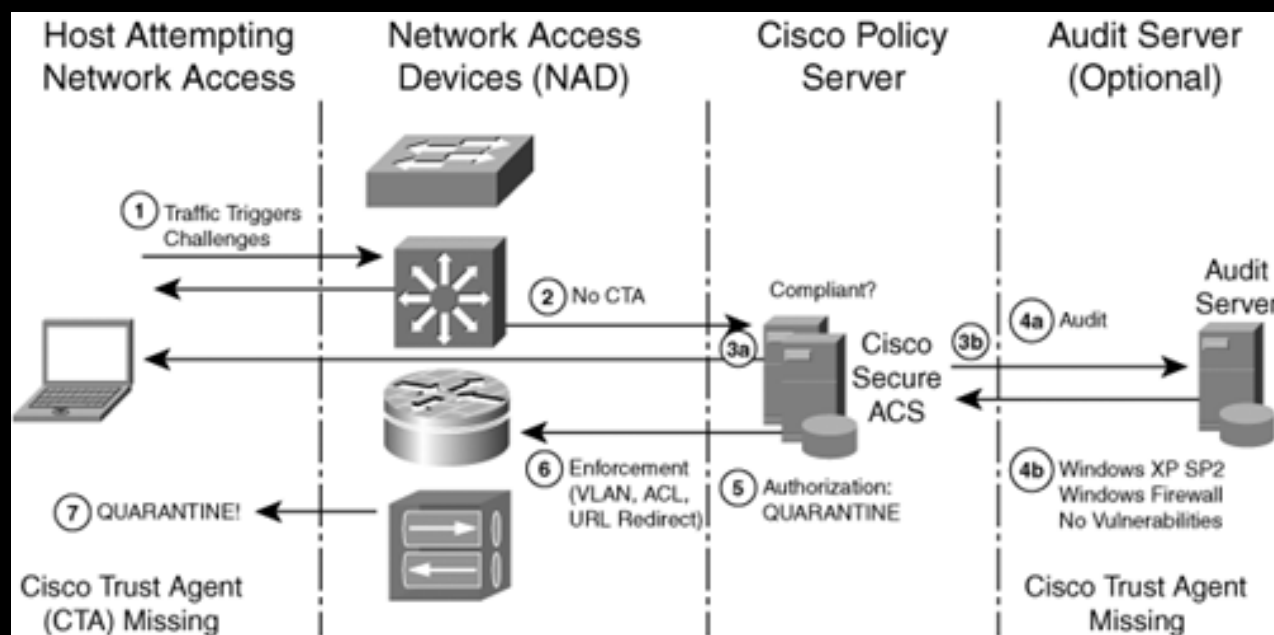
- Autentizácia na II. vrstve TCP/IP
- Autentizácia užívateľa a zariadenia
- Autentizácia voice infraštruktúry
- Flexibilita – priradenie do VLAN(aj PVLAN), MAC Bypass, Critical port, Guest, WoL, dACL,

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Network Admission Control (NAC)

- NAC Framework a NAC Appliance
- Autentizácia a Autorizácia
- Integrácia s 802.1x
- Podpora a zariadení bez agenta
- Neautorizované zariadenia sú umiestnené do karantény
  - vlan, pvlan, vrf, acl
- Remediation



# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Host Intrusion Prevention (CSA)

- Ochrana pred *Day-zero* útokmi (?)
- Host intrusion prevention
- Ochrana pred buffer overflows
- Detekcia Port scan
- Distribuovaný personal firewall
- Ochrana pred spyware/adware
- Inventarizácia softvéru
- *Location-based* politiky – vykonávanie politiky v závislosti od toho či je pracovná stanica pripojená do podnikovej siete alebo niekde inde
- Politika pre obmedzenie prístupu na odnímateľné média, vrátane USB zariadení

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Host Intrusion Prevention (CSA)

- Kontrola Hot fix-ov and Service Pack-ov (SP)
- Ochrana súborov a adresárov
- Ochrana dát v Clipboard-e
- Kontrola Antivirus DAT súborov
- Integrácia s Cisco Trust Agent pre NAC
- „*Tagovanie*“ trafiku aplikácií pre QoS
- Podpora pre VMWare
- Podpora pre Tablet PC
- Podpora pre Solaris 9

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Host Intrusion Prevention (CSA) – *buffer overflow – BO*

- Prečo BO funguje:
  1. Programátor predpokladá, že na vstupe bude mať požadované množstvo dát ;-)
  2. Program spracuje toľko dát koľko dostane
- Dopad:
  - Spustenie akéhokoľvek programu
    - *Call register* – napr. Volanie niektorej funkcie z *Kernel32.dll*
    - *Push, Pop, Blind return* – volanie podvrhnutého programu/funkcie

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Host Intrusion Prevention (CSA) – Ochrana pred *buffer overflow*

#### Riešením je sledovanie správania sa aplikácie

- Klasifikácia aplikácie
- Sledovanie vykonávania nasledovných operácií (uvedené sú len niektoré)
  - Prístup k systémovým funkciám volaných z heap-u resp. stack-u
  - Čítanie systémových registrov
  - Priamy prístup do pamäte – obchádzanie reštrikcií virtuálnej pamäte
  - Zapísanie kódu (napr. dll) do pamäte rezervovanej inej aplikácii

# Pokročilé bezpečnostné riešenia

## Rozšírená bezpečnostná infraštruktúra

### Cisco DDoS guard a Cisco DDoS traffic anomaly detector

- Generuje „Base line“ štandardnej sieťovej prevádzky
- Presmerovanie DoS trafiku mimo cieľového zariadenia
- Rôzne techniky pre presmerovanie trafiku – policy routing, VRF, VLAN, GRE
- „Vyčistený“ trafik je presmerovaný späť cieľovému zariadeniu

# Otázky