Igor Tomeš

19.Března 2013

Informační zdroje, DMZ a jejich ochrana

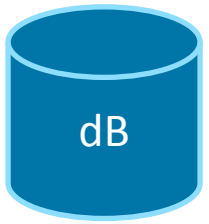
O čem to dnes bude

- Informační bohatství a jeho uživatelé
- Datové centrum a DMZ
- Uživatel a přístup k informacím
- Ochrana Informačního bohatství
- Řízení prostředků ochrany
- Otázky a snad i odpovědi

Informační bohatství a jeho uživatelé

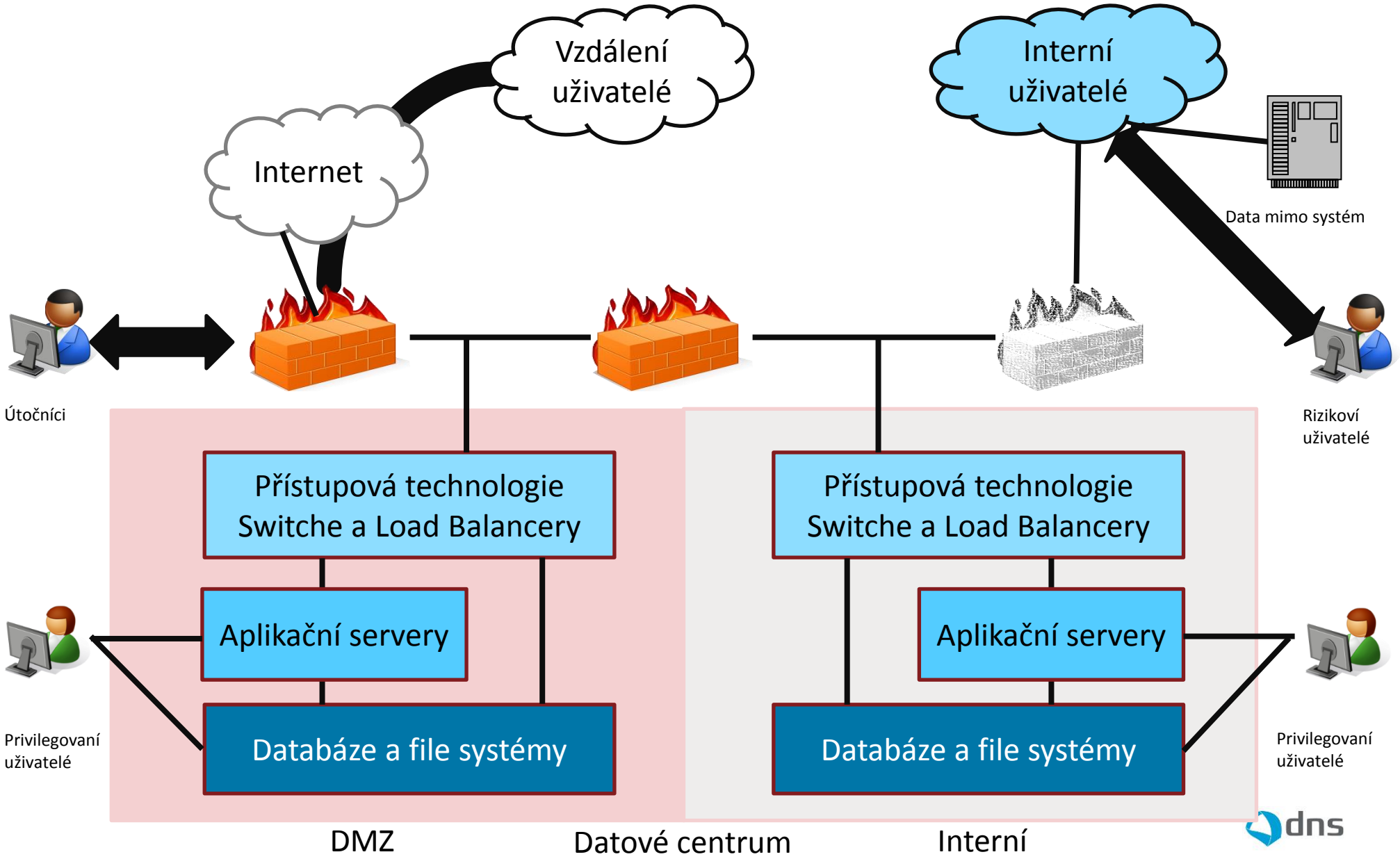
- Informace v elektronické formě
  - Databáze – 30%
    - Strukturované
    - Hierarchie přístupů
    - Snadné vyhledávání
  - Soubory - 70%
    - Nestrukturované
    - Opakující se informace
    - Omezená ochrana
  - Uživatel známý informačnímu systému
  - Uživatel informačnímu systému neznámý

Pepa



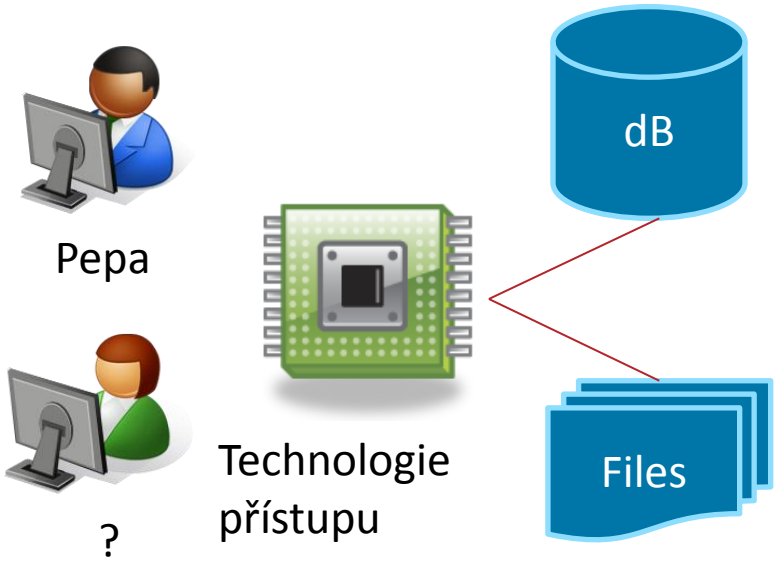
?

Datové centrum a DMZ



Uživatelé a přístup k informacím

- Způsob přístupu uživatele
  - Přímý přístup
  - Terminál server
  - Klient
  - WWW technologie
- Identifikace uživatele
  - Různá síla dle charakteru informací

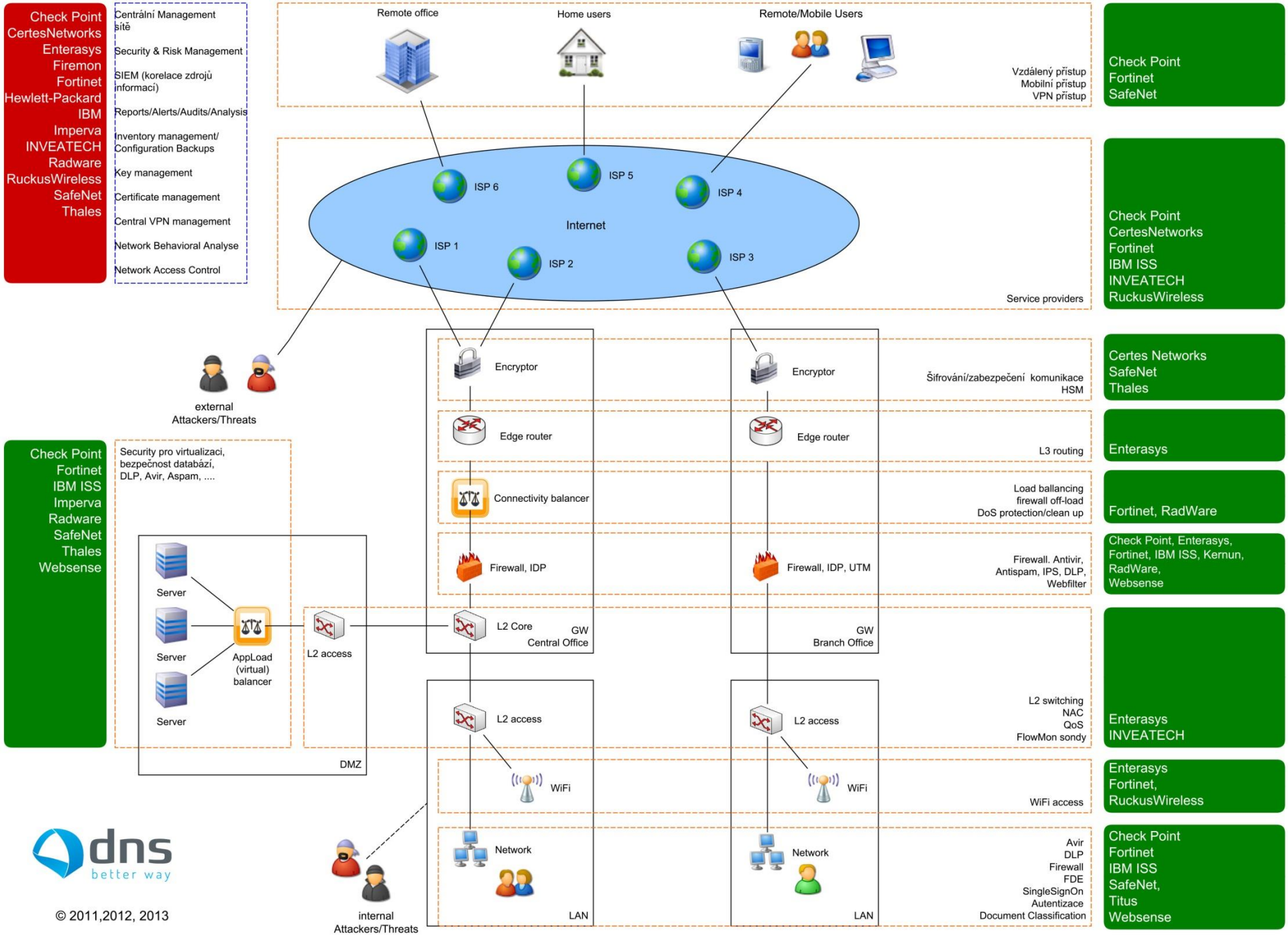


Ochrana informačního bohatství

- Mnohovrstvá dle modelu OSI
  - Typicky pro 3,4, a 7 vrstvu
- Mnoho funkcí
  - Aktivní
    - Zabraňuje v přístupu,
    - Zahazuje data
  - Pasivní
    - Monitoruje činnost
    - Audituje činnost
- Dva principy
  - Předem známé informace (Anti XXX, IPS/IDS, FW, Threat Radar….)
  - Analyzuje chování – posuzuje riziko

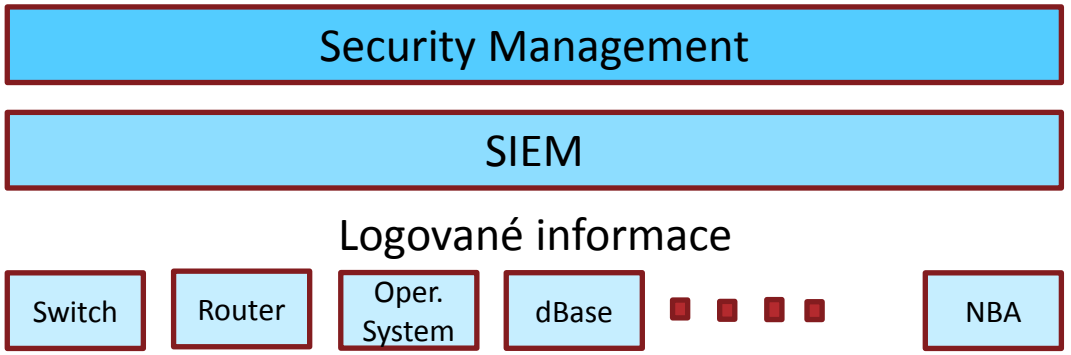
Ochrana informačního bohatství
Technologie ochrany

- 2. vrstva
  - Šifrování provozu
  - VLAN
  - Access Management
- 3. vrstva
  - Šifrování provozu
  - Access Management
  - Firewall
  - DDOS ochrana
  - Ochrana DNS, DHCP …
- 4. vrstva
  - IPS/IDS
  - Nástroje analýzy chování (TCP/IP analýza)
  - VPN, SSL
- 7. Vrstva
  - Ochrana e-mailu
  - Aplikační Firewall (WAF)
  - Databázový Firewall (DBM/DBF)
  - Souborový Firewall (FAM)
  - Anti XXX
  - Autentizace, 2FA, OTP
  - Ochrana proti ztrátě dat – DLP a klasifikace
  - Web Filtering, ochrana přístupu k externím www


Check Point
CertesNetworks
Enterasys
Firemon
Fortinet
Hewlett-Packard
IBM
Imperva
INVEATECH
Radware
RuckusWireless
SafeNet
Thales
Centrální Management sítě
Security & Risk Management
SIEM (korelace zdrojů informací)
Reports/Alerts/Audits/Analysis
Inventory management/ Configuration Backups
Key management
Certificate management
Central VPN management
Network Behavioral Analyse
Network Access Control
Remote office
Home users
Remote/Mobile Users
Vzdálený přístup
Mobilní přístup
VPN přístup
Check Point
Fortinet
SafeNet
ISP 6
ISP 5
ISP 4
Internet
ISP 1
ISP 2
ISP 3
Service providers
Check Point
CertesNetworks
Fortinet
IBM ISS
INVEATECH
RuckusWireless
external
Attackers/Threats
Encryptor
Encryptor
Šifrování/zabezpečení komunikace
HSM
Certes Networks
SafeNet
Thales
Edge router
Edge router
L3 routing
Enterasys
Connectivity balancer
Load ballancing
firewall off-load
DoS protection/clean up
Fortinet, RadWare
Firewall, IDP
Firewall, IDP, UTM
Firewall. Antivir,
Antispam, IPS, DLP,
Webfilter
Check Point, Enterasys,
Fortinet, IBM ISS, Kernun,
RadWare,
Websense
Check Point
Fortinet
IBM ISS
Imperva
Radware
SafeNet
Thales
Websense
Security pro virtualizaci,
bezpečnost databází,
DLP, Avir, Aspam, ...
Server
Server
Server
AppLoad
(virtual)
balancer
L2 access
L2 Core
GW
Central Office
GW
Branch Office
DMZ
L2 access
L2 access
L2 switching
NAC
QoS
FlowMon sondy
Enterasys
INVEATECH
WiFi
WiFi
WiFi access
Enterasys
Fortinet,
RuckusWireless
Network
Network
LAN
LAN
Avir
DLP
Firewall
FDE
SingleSignOn
Autentizace
Document Classification
Check Point
Fortinet
IBM ISS
SafeNet,
Titus
Websense
internal
Attackers/Threats
dns
better way
© 2011,2012, 2013

Řízení prostředků ochrany

- SIEM (Security Information and Event Management)
  - Sběratel logů (ze všeho z čeho to jde)
  - Koreluje události
  - Vyhodnocuje závažnost
  - Trpí nedostatkem inteligence
- Security management
  - Audit a korelace politik
  - Backup konfigurací
  - Auditní nástroje
  - Rizikové analýzy
  - Řízení změn v nastavení bezpečnostních prvků – tiketovací nástroj



Děkuji za pozornost

itomes@dns.cz