ADVANCED PERSISTENT THREAT

Viktorija Almazova

If P&C Insurance AS Latvijas filiāle

ADVANCED PERSISTENT THREAT

uzlabotie pastāvīgie draudi

- Uzlabotie (advanced) – nozīmē, ka pretinieks ir spējīgs izmantot uzbrukuma pilno spektru. Tie var izmantot plaši pieejamos eksploitus pret labi zināmām ievainojamībām vai arī veikt pētījumus, lai atklātu un izveidotu jaunus eksploitus atkarībā no mērķa pozīcijas
- Pastāvīgie (persistent) – nozīmē, ka pretiniekam ir "oficiāli" uzdots paveikt šo misiju. Savukārt, jēdziens "pastāvīgie" nenozīmē, ka nepārtraukti tiek izpildīts ļaunprātīgs kods uz "upura" datorsistēmām. Drīzāk tie uztur mijiedarbības līmeni, kas ir nepieciešams nostādīto mērķu izpildei.
- Draudi (threat) – nozīmē, ka pretinieks nav bezjēdzīga koda daļa. Šim momentam ir izšķirošā nozīme. Daudzi cilvēki ar terminu "threat"/"drauds" apzīmē ļaunprātīgās programmas - malware. Ja aiz ļaunprātīgās programmas nav cilvēka (kas kontrolē upuri, lasa nozagto informāciju un tml), vairums ļaunprātīgo programmu neizraisītu uztraukumu (ja tie neizdzēš datus). Drīzāk pretinieks ir "drauds", jo ir organizēts, finansēts un motivēts.

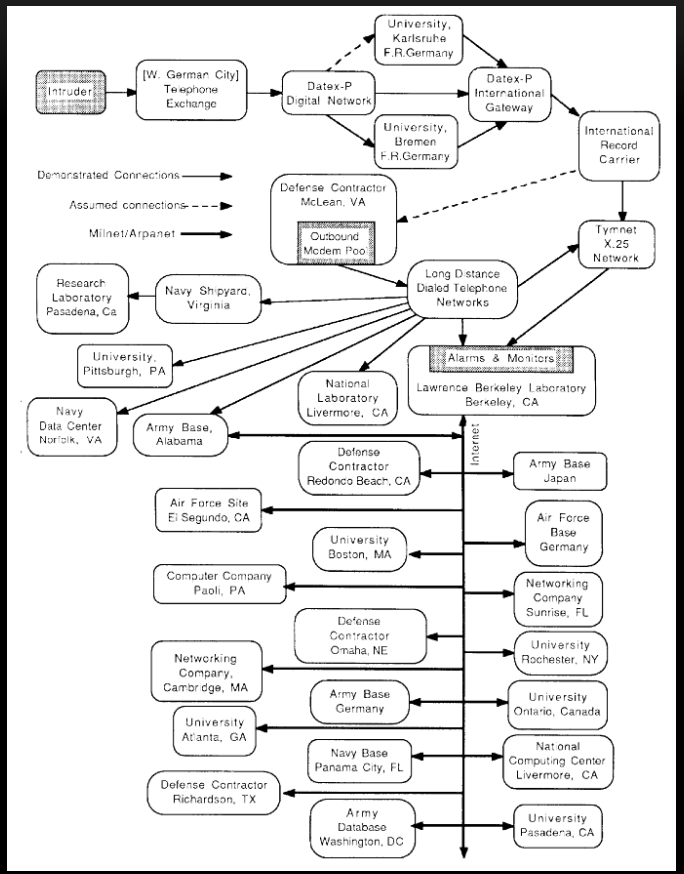
Richard Bejtlich, TaoSecurity, 2010

MALWARE
uzbrukuma metode

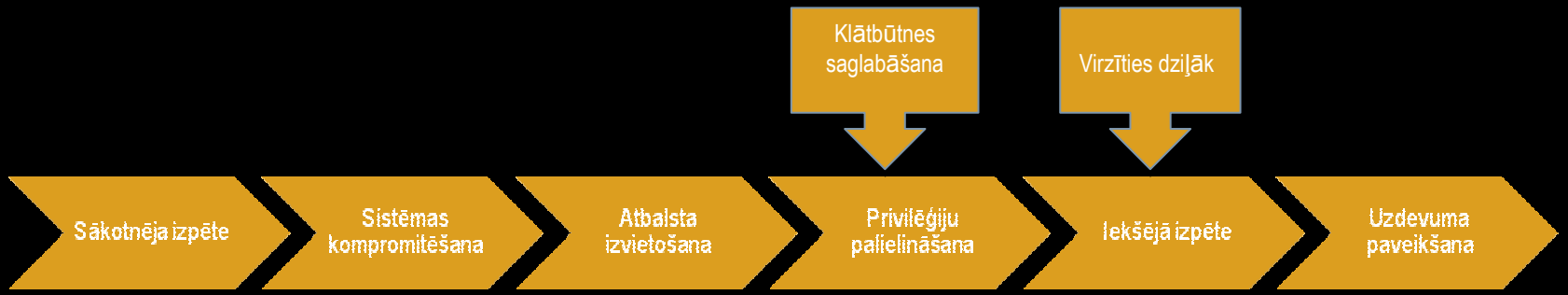
	Stuxnet	Duqu	Flame	Gauss
Atklāšanas datums	2010. jūlijs	2011. jūlijs	2012. jūlijs	2012. augusts
Inficēto skaits	180 000	20	700	2500
Izplatīšanas valsts	Indija, Indonēzija, Irāna	Irāna, Indija, Sudāna, Vietnama, Francija, Nīderlande, Šveice, Ukraina, Austrija, Ungārija, Indonēzija, Lielbritānija	Irāna, Izraēla	Izraēla, Palestīna, Līvāna
Sākotnējās inficēšanas veids	Nav zināms – iespējams flash drive	Caur Word dokumentu, kas tika izsūtīts atslēgas cilvēkiem	Nav zināms – ir iespēja instalēt caur viltoto Windows atjaunošanas mehānismu	Nav zināms
Izstrādes vide	Visual Studio	Visual Studio, C	C++, Lua	C++
Funkcionāls	Failu meklēšana un implementēšana Siemens WinCC SCADA	Failu meklēšana un nodošana, klaviatūras ievades izsekošana un informācijas ievākšana par tīkla konfigurāciju	Failu meklēšana un nodošana, balss informācijas ierakstīšana, Bluetooth pārtveršana	Failu meklēšana un nodošana, balss informācijas ierakstīšana, Paroļu pārtveršana
Mērķis	SCADA funkcionalitātes traucēšana	Spiegošana un datu sagatave vēlākai integrēšanai tīklā	Spiegošana	Ietekme uz sociāliem apstākļiem
Iespējamais izstrādes gads	2009	2008	2006	2011

1980 APT

"STALKING THE WILY HACKER", CLIFFORD STOLL, MAY 1988 VOL. 31. NO. 5



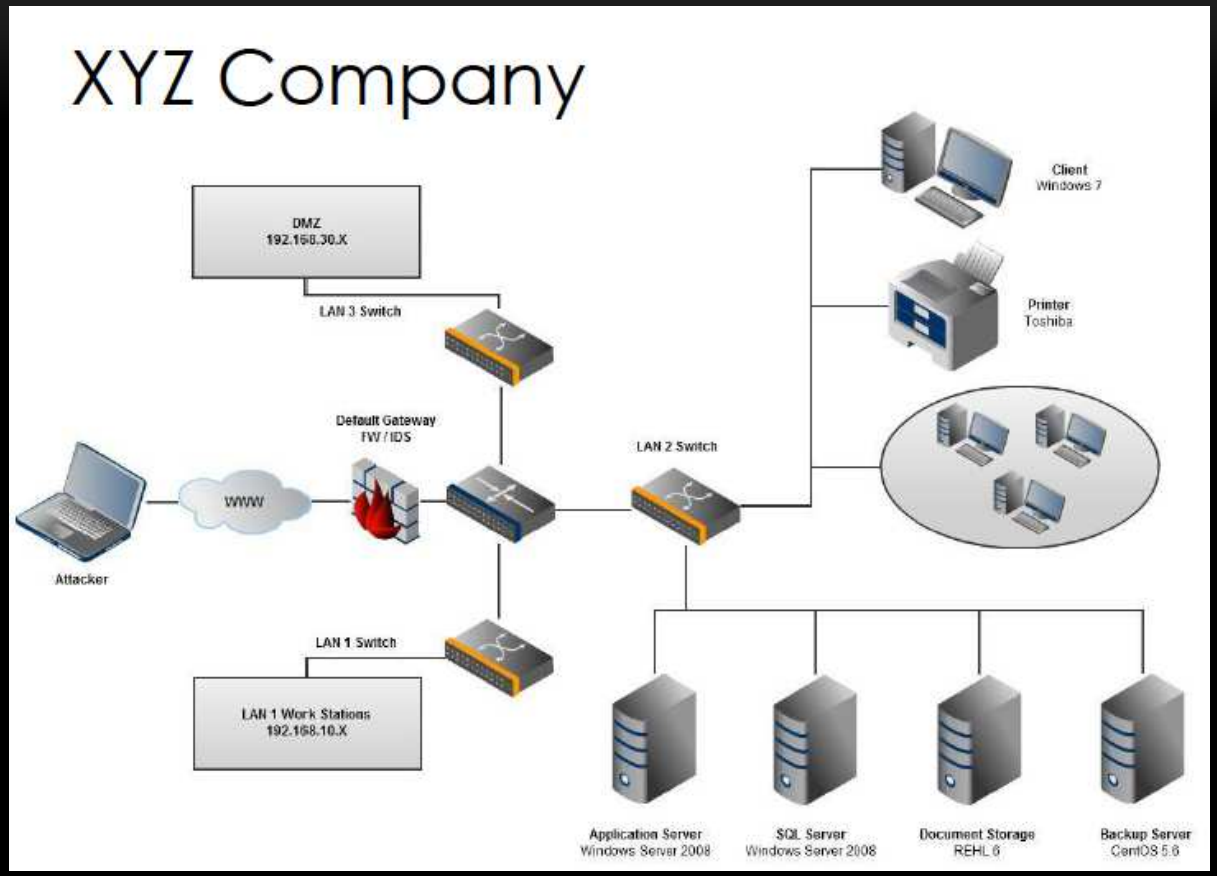
MĒRĶĒTĀ UZBRUKUMA DZĪVES CIKLS



NEOFICIĀLĀ METODOLOĢIJA

- ✓ ielauzties tīklā
- ✓ atrast informāciju
- ✓ nokopēt/saglabāt visu
- ✓ atstāt tīklu
- ✓ kļūt par bagātu vai noķertu

KĀDA UZŅĒMUMA “VEIKSMES” STĀSTS



Gianni Gnesa, Šveice

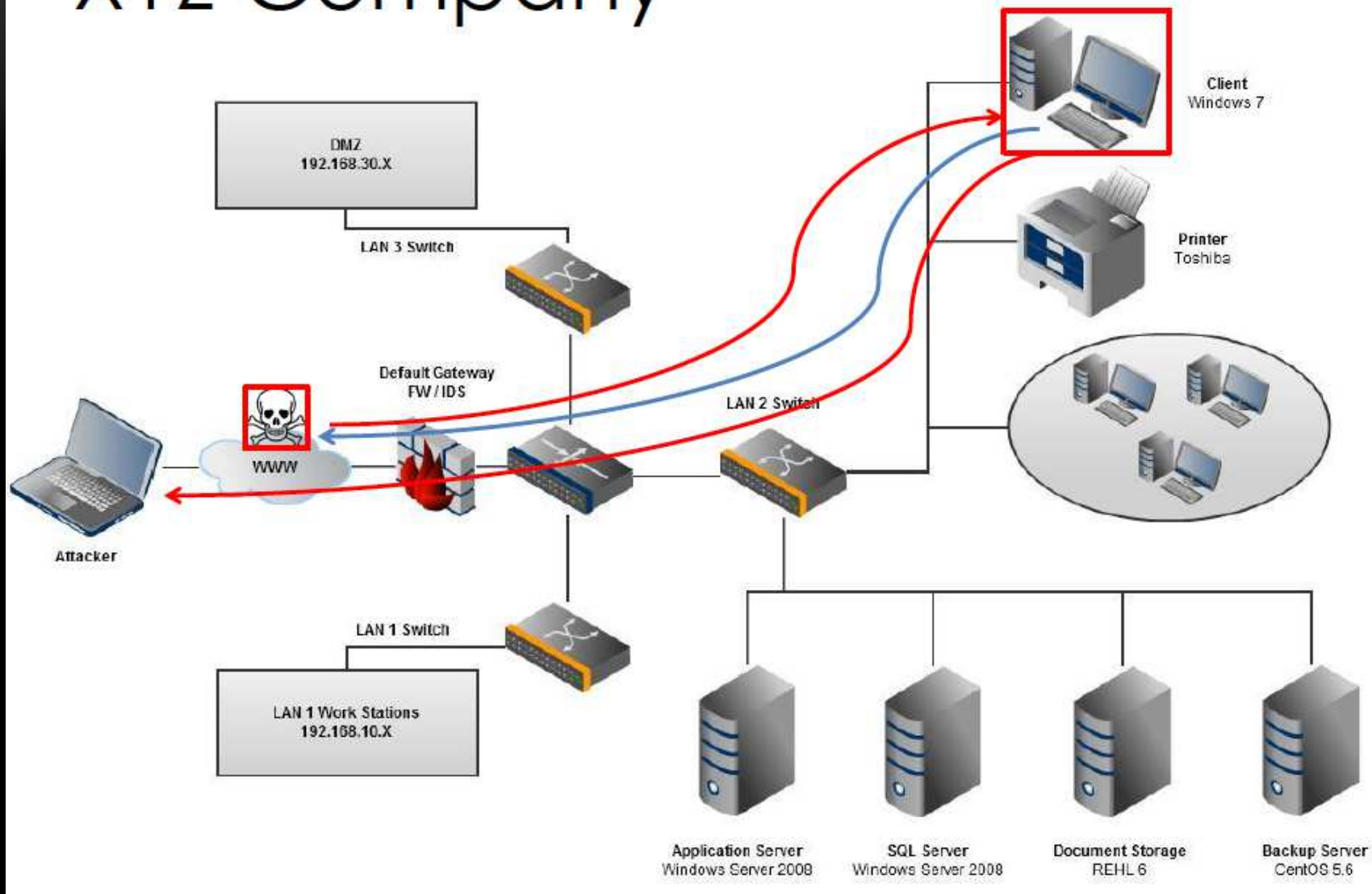
SĀKOTNĒJA IZPĒTE

- ✓ tīkla perimetrs ir drošs
  - drošības auditi tiek veikti regulāri
- ✓ mājas lapa atradās DMZ zonā un nebija ievainojama
- ✓ darbinieki bija apmācīti atpazīt sociālās inženierijas (social engineering) uzbrukumus

SISTĒMAS KOMPROMITĒŠANA

- ✓ svaiga eksploita/0day izmantošana e-pasta nosūtīšanā
- ✓ šajā gadījumā, uzbrucējs izveidoja atsevišķu mājas lapu ar vairākiem eksplotiem, ieskaitot vienu MS12-037 Internet Explorer Same ID Property Deleted Object Handling Memory ievainojamību

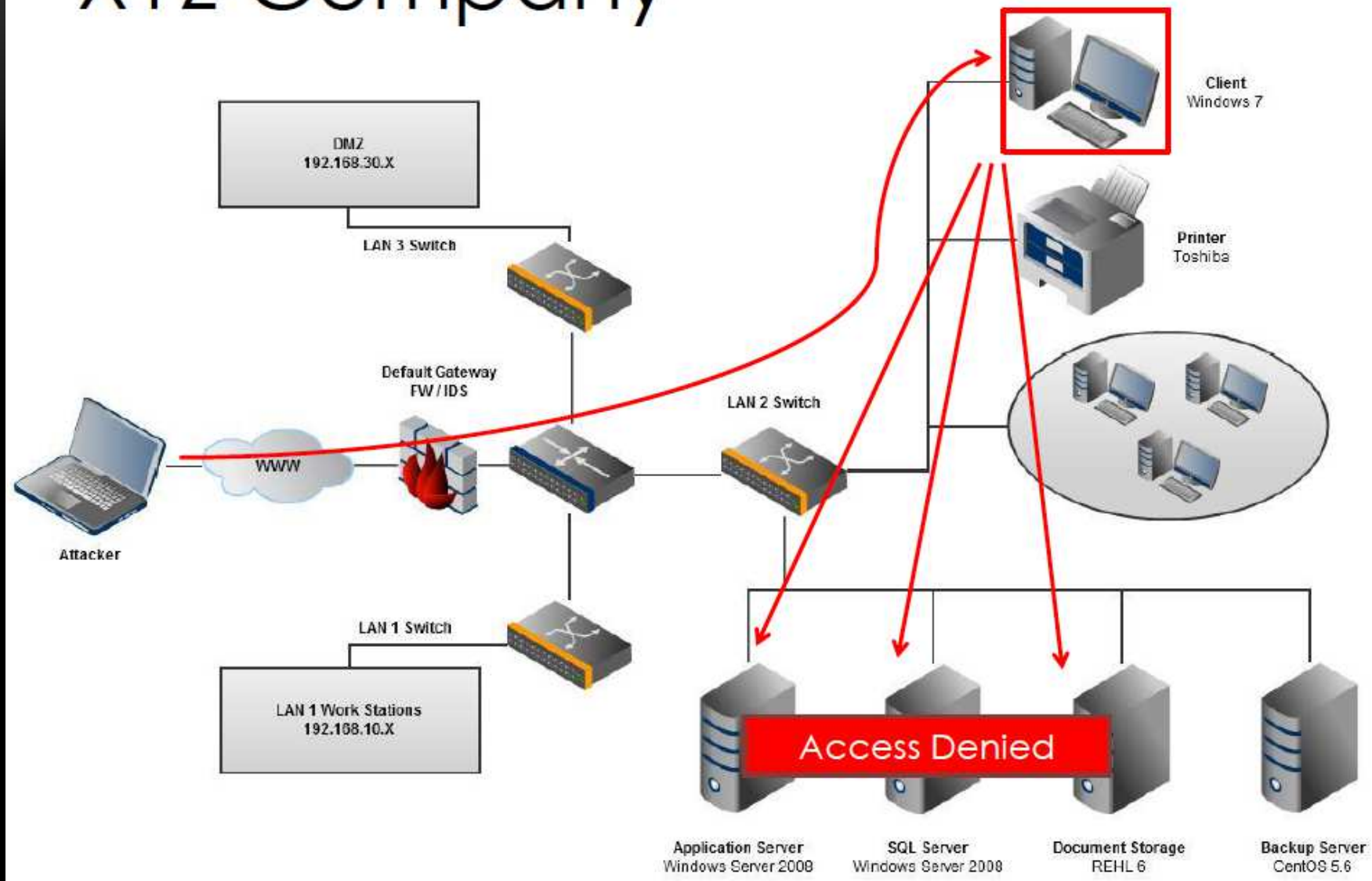
XYZ Company


DMZ
192.168.30.X
LAN 3 Switch
Client
Windows 7
Printer
Toshiba
Default Gateway
FW / IDS
LAN 2 Switch
WWW
Attacker
LAN 1 Switch
LAN 1 Work Stations
192.168.10.X
Application Server
Windows Server 2008
SQL Server
Windows Server 2008
Document Storage
REHL 6
Backup Server
CentOS 5.6

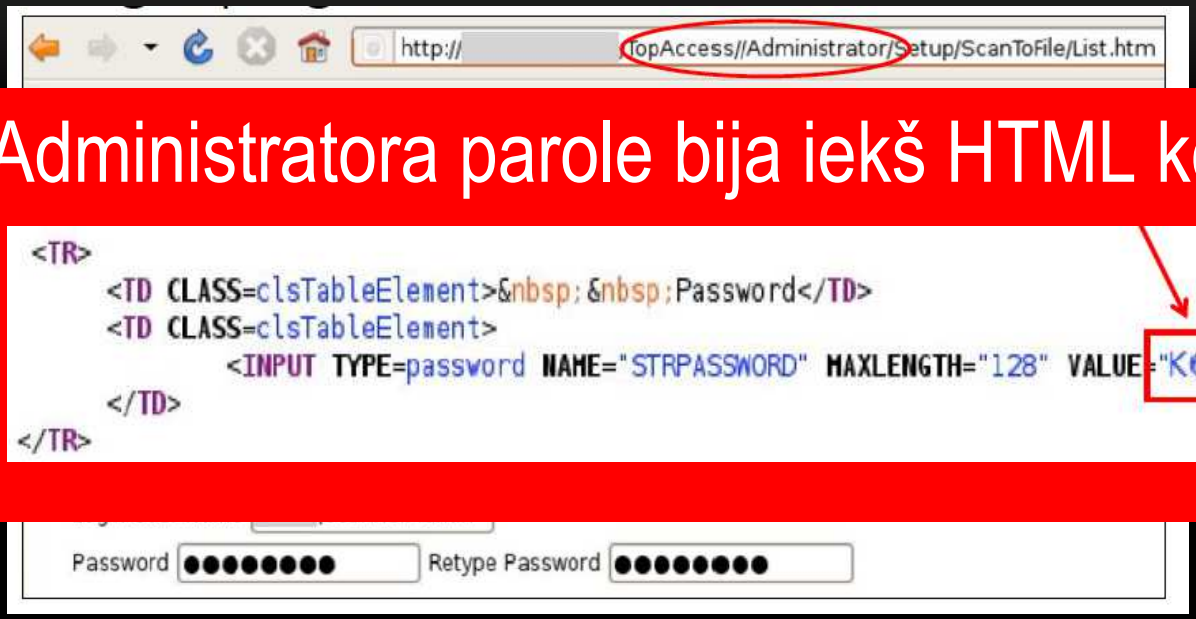
INFORMĀCIJAS IEVĀKŠANA

- ✓ izvietoja nepieciešamās ļaunprātīgās programmas (malware) patstāvīgai savienojuma izveidei
- ✓ tiklīdz iebrucējs bija iekļuvis, izmantojot kompromentēto datoru, noteica svarīgās informācijas atrašanās vietu
- ✓ izmantojot sniferus un citus rīkus, noteica galvenos serverus: aplikācijas serveri, sql serveri un dokumentu glabāšanas serveri
- ✓ uzbrucējam neizdevās iegūt pieeju ne pie viena servera
- ✓ katram serverim bija sava parole
- ✓ ievainojamības netika atrastas
- ✓ vienīgā iespēja - brute forcing

XYZ Company


DMZ
192.168.30.X
LAN 3 Switch
Client
Windows 7
Printer
Toshiba
Default Gateway
FW / IDS
LAN 2 Switch
WWW
Attacker
LAN 1 Switch
LAN 1 Work Stations
192.168.10.X
Access Denied
Application Server
Windows Server 2008
SQL Server
Windows Server 2008
Document Storage
REHL 6
Backup Server
CentOS 5.6

Uzbrucējs izmantoja “/”, lai apietu autentificēšanas lapu



Uzbrucējs pamēģināja atvērt lapu
/Setup/Network/setting/smb.htm

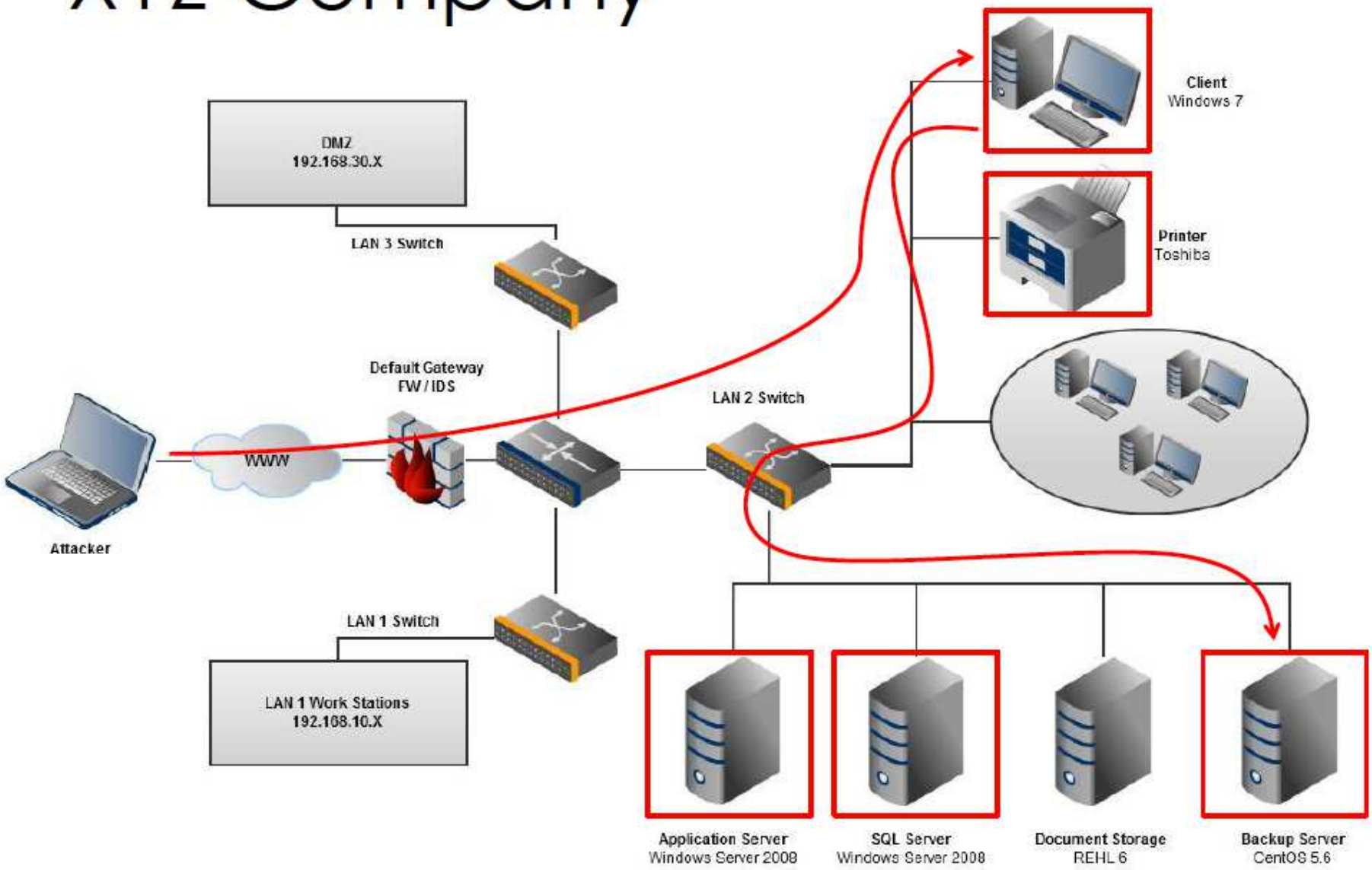
INFORMĀCIJAS IEVĀKŠANA

- ✓ par nelaimi, iegūtā parole tika izmantota arī aplikācijas serverī
- ✓ aplikācijas serverī iebrucējs atrada nepieciešamos datus pieejai SQL serverī
- ✓ tomēr vērtīga informācija netika glabāta SQL serverī
- ✓ dokumenti, diagramas, projekti – bija glabāti Linux failu serverī
- ✓ linux serveris RHEL6 nebija ievainojams
- ✓ atrasts arhīvu serveris (iespējams - administratora piezīmēs)

PRIVILĒĢIJU IEGŪŠANA

- ✓ Arhīvu serverim bija instalēti vairāki servisi
- ✓ Uzbrucējs izmantoja phpMyAdmin 3.4.1 Swekey RCE eksploitu, lai iegūtu attālināto pieeju pie konsoles
- ✓ Pēc tam izmantoja Linux 2.6.x umount eksploitu, lai iegūtu root (administratora) tiesības

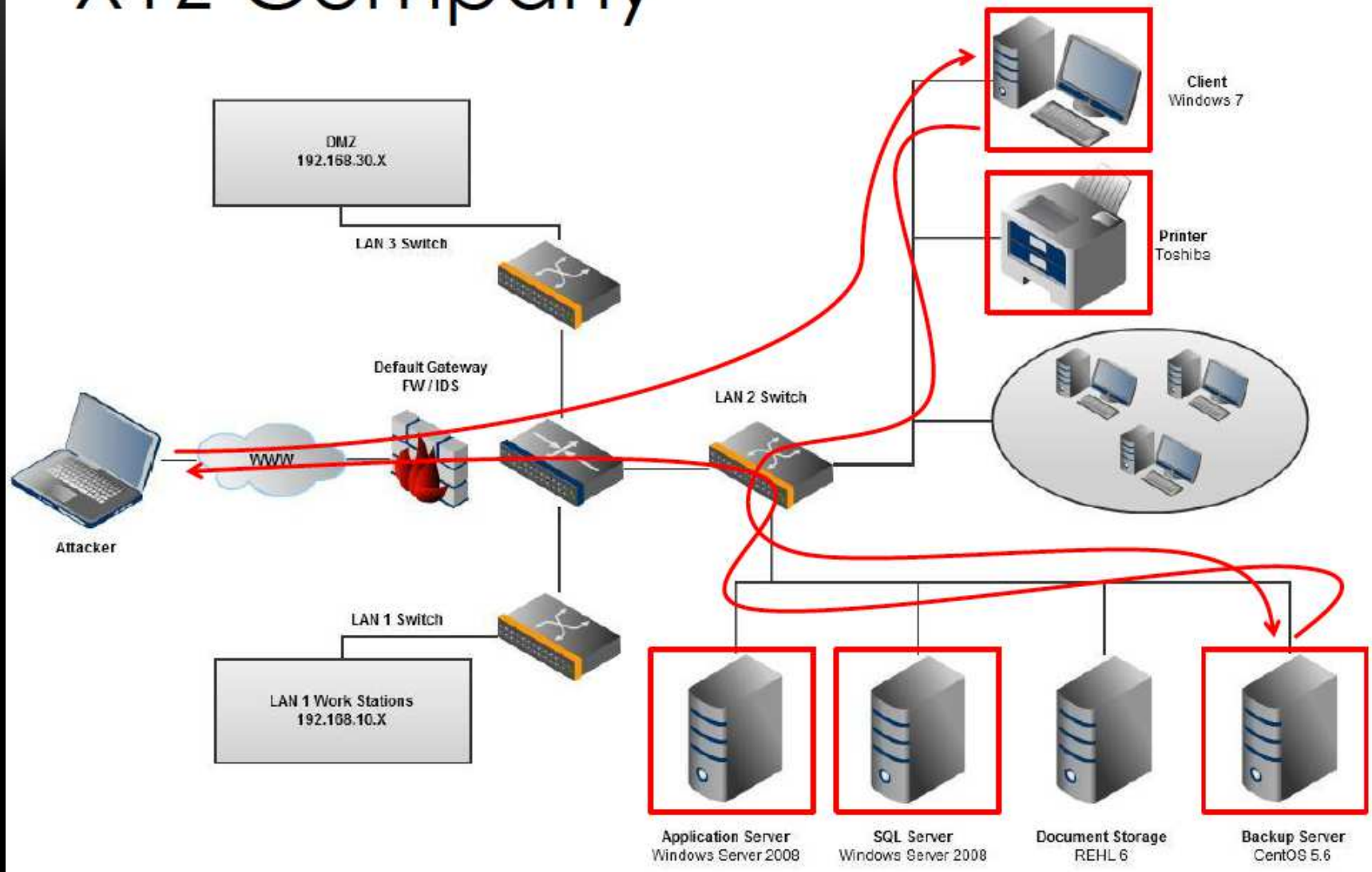
XYZ Company


DMZ
192.168.30.X
LAN 3 Switch
Default Gateway
FW / IDS
LAN 2 Switch
Client
Windows 7
Printer
Toshiba
WWW
Attacker
LAN 1 Switch
LAN 1 Work Stations
192.168.10.X
Application Server
Windows Server 2008
SQL Server
Windows Server 2008
Document Storage
REHL 6
Backup Server
CentOS 5.6

UZDEVUMA PAVEIKŠANA

- ✓ kā root lietotājam - uzbrucējam bija pieeja pie visiem failiem un direktorijām sistēmā
- ✓ vērtīgākie dokumenti tika saarhivēti vairākos tar.gz failos
- ✓ un tad nosūtīti caur https uz Malaizīju

XYZ Company


DMZ
192.168.30.X
LAN 3 Switch
Default Gateway
FW / IDS
WWW
Attacker
LAN 2 Switch
Client
Windows 7
Printer
Toshiba
LAN 1 Switch
LAN 1 Work Stations
192.168.10.X
Application Server
Windows Server 2008
SQL Server
Windows Server 2008
Document Storage
REHL 6
Backup Server
CentOS 5.6

KOPSAVILKUMS

- ✓ vairums svarīgo dokumentu: līgumi, diagrammas, bildes, ieskaitot elektroniskos parakstus, tika nozagti
- ✓ dažas nedēļas vēlāk uzbrucējs mēģināja iegūt naudu, izmantojot nozagtos elektroniskos parakstus
- ✓ bankai dotais darījums šķita aizdomīgs un tie atcēla transakciju
- ✓ vēl joprojām nav zināms, kurš uzlauza tīklu un kādi ir zaudējumi

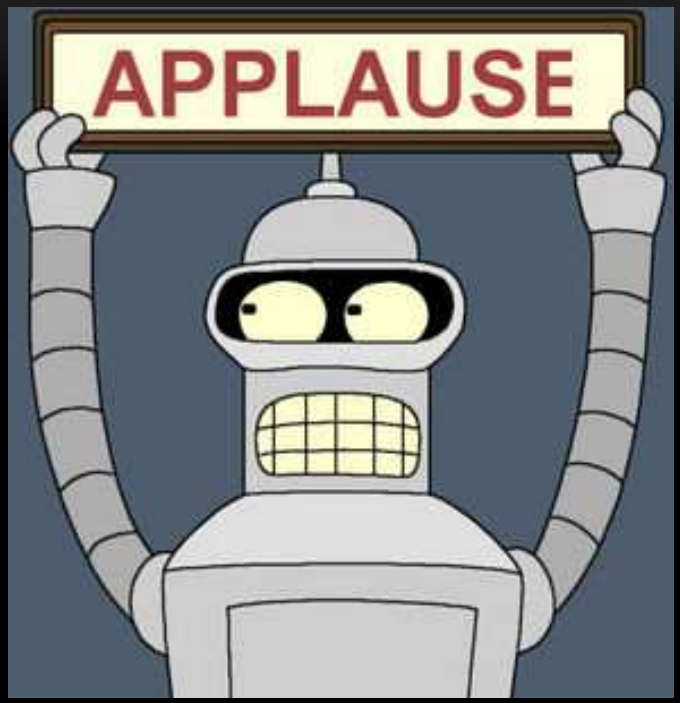
STĀSTA BEIGAS

- ✓ ja uzbrucējs vēlās iekļūt jūsu tīklā, viņš iekļūs, un jūs tur neko nevarat darīt

- ✓ vienīgais ko jūs varat paveikt – sarežģīt to

APT PAZĪMES

- APT pazīme #1: palielinās *logon* ierakstu skaits
- APT pazīme #2: vairāki trojāni tīklā
- APT pazīme #3: netipiskās informācijas plūsmas
- APT pazīme #4: datu atrašanās neraksturīgā vietā
- APT pazīme #5: atrodas PTH (pass-the-hash) uzlaušanas rīki


APPLAUSE