

Content Security

Spam e nuove minacce

Alessio L.R. Pennasilico - apennasilico@clusit.it
Antonio Ieranò - antonio.ieranò@cisco.com



Security Summit
16 Marzo 2010
ATA Hotel Executive, Milano

Clusit
Education

Alessio L.R. Pennasilico

Security Evangelist @  Albast

Board of Directors:

Associazione Informatici Professionisti

Associazione Italiana Professionisti Sicurezza Informatica

CLUSIT

Italian Linux Society, LUGVR, Metro Olografix, Sikurezza.org

Hacker's Profiling Project, CrISTAL

Antonio Ieranò

Content Security Engineer @



Firewall

“Ho il firewall”...

Firewall

“Ho il firewall”...

Non si tratta della panacea ad ogni male

SPAM

Vecchio il concetto
(volantini, piazzisti, etc etc)

Cambia solo il vettore

Phishing

Dal vendere il prodotto
alla truffa, passando per il via

Phishing

Dal vendere il prodotto
alla truffa, passando per il via

ovvero

come prendere le 20.000 lire e non andare in prigione

SPIT / Vishing

“Nuove Minacce”

SPIT / Vishing

“Nuove Minacce”

ovvero

*andare in ferie nello stesso posto ogni anno,
facendo una strada diversa per arrivarci...*

Malware

Virus
Worm
Keylogger
Trojan
Dialer?
Spyware
Backdoor

Navigazione

Le stesse minacce possono essere inconsapevolmente scaricate in maniera attiva dagli utenti

Oppure possono essere infettati i client utilizzando vulnerabilità note (trend di crescita)

Botnet

Lo scopo è avere una grande rete di computer casalinghi da comandare per svolgere compiti remunerativi (es. SPAM)

DoS/DDoS

Gli stessi PC possono essere utilizzati per attaccare altre reti, magari dietro compenso...

Chat

Traffico de-centralizzato
Protocolli esotici / criptati

Tunnel

E' possibile installare fuori dall'azienda (anche a casa) un proxy/server VPN per far passare in una connessione autorizzata (es. navigazione) tutto il traffico non permesso...

Social Network

Problemi di contenuti ricevuti
contenuti pubblicati
chat
scambio file
bug / worm / virus

Social Engineering

Non importa il vettore
(mail, chat, social network)

Basta convincere l'utente a rilasciare alcune
informazioni riservate

Data Loss Prevention

Perdita di dati dovuta ad infezione / intrusione accidentale o pilotata (competitor/disgruntled)

E' solo la non disponibilità il problema?

Conclusioni

Le minacce da affrontare sono molte e spesso non banali da gestire

La tecnologia supporta il lavoro del CSO

Purtroppo si rende sempre necessario fare “hardening” del personale oltre che delle macchine

Web-o-Grafia

<http://www.cisco.com/go/securityreport>

<http://portadiferro.blogspot.com/>

<http://www.alba.st/presentazioni.php>



Grazie dell'attenzione!

Domande?

Alessio L.R. Pennasilico - apennasilico@clusit.it
Antonio Ieranò - antonio.ieranò@cisco.com



Security Summit
16 Marzo 2010
ATA Hotel Executive, Milano

Clusit
Education