Velkommen til

Internet sikkerhedstendenser i 2009

Content Security Seminar

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

Slides er tilgængelige som PDF

© copyright 2009 Security6.net, Henrik Lund Kramshøj

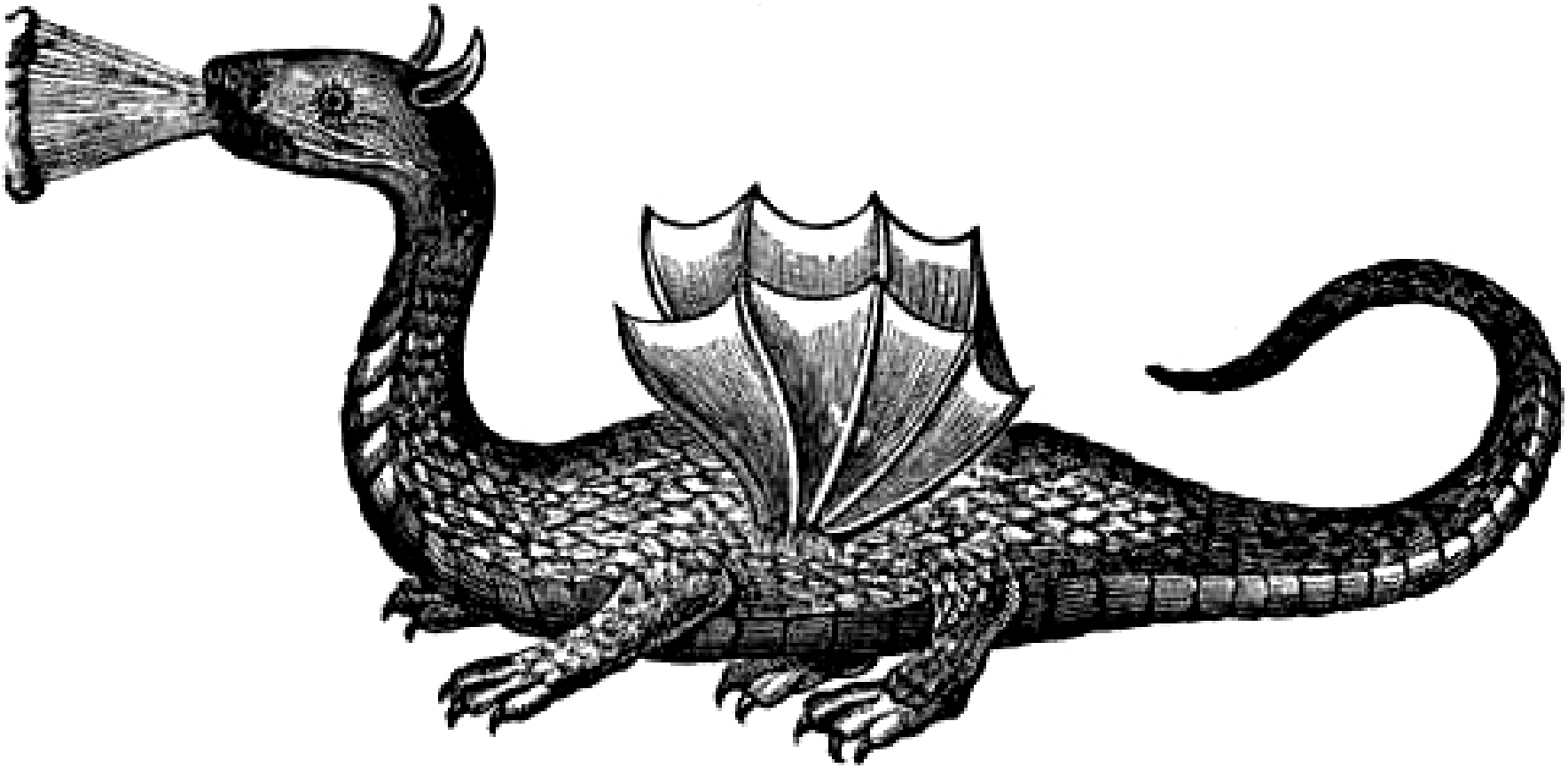
Formål

Give overblik over hvad internetsikkerhed betyder i år 2009

Hvad er almindeligt forekommende hændelser

Hvad kan vi forvente os af 2009

Internet - Here be dragons



Himlen falder ned

... igen

Rinse repeat

Kendte sårbarheder udnyttes stadig

Kendte angrebsmetoder udvides - social engineering

Stadig misbrug af kreditkort, selv med Verified by VISA på plads osv.

Gider I høre de samme råd igen

2008 hvad skete der

Botnets fortsætter med at vokse - millionvis af computere

Botnets bliver sværere at udrydde

Sikkerhed for botnets er blevet populært

Botnets er blevet en hyldevare

Botnets er grundlaget for mange nye angreb

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Moderne botnets

Botnets spreder sig ved at inficere så mange systemer som muligt

Botnets idag vokser gerne langsommere - ingen ny Code Red hastighedsrekord

Spreder sig via SMTP, HTTP, SMB, ... alle protokoller der kan overføre data

Bannerkampagner og 3. parts kilder til elementer på din side?!

Når først der er kommet malware på systemet udvides med moduler

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Malware idag

Malware idag er sofistikeret

Modulært opbygget

Benytter stærk kryptering til at sikre administrationen af inficerede computere

Benytter seneste sikkerhedshuller - 0 days til at sprede sig

Benytter de seneste rootkit metoder til at holde sig skjult

Muterer efter alle kendte metoder for at undgå opdagelse

Larmer mindre end tidligere

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Botnets og malware sælges med support

Dagens tilbud

trojanere

Køb 2 betal for 1

Friske botnets

Friske phish
inficeret indenfor den seneste uge

Supportaftale

trojanersupport
email, IRC, IM
Betal med kreditkort

Malware programmører har lært kundepleje

”Køb denne version og få gratis opdateringer”

Lej vores botnet med 100.000 computere

© copyright 2009 Security6.net, Henrik Lund Kramshøj

milw0rm - dagens buffer overflow

[home] [contents] [platforms] [shellcode] [search] [cracker] [links] [rss] [archive]

MILW0RM

[highlighted]

-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-03-05	Winamp <= 5.541 Skin Universal Buffer Overflow Exploit	3128	R		D		SkD
2009-02-26	Coppermine Photo Gallery <= 1.4.20 (BBCode IMG) Privilege Escalation	7338	R		D		StAkeR
2009-02-25	Apple MACOS X xnu <= 1228.x Local Kernel Memory Disclosure Exploit	4111	R		D		mu-b
2009-02-23	Adobe Acrobat Reader JBIG2 Local Buffer Overflow PoC #2 0day	17652	R		D		Guido Landi
2009-02-23	MLdonkey <= 2.9.7 HTTP DOUBLE SLASH Arbitrary File Disclosure Vuln	4225	R		D		Michael Peselnik
2009-02-23	Multiple PDF Readers JBIG2 Local Buffer Overflow PoC	7781	R		D		webDEVIL

[remote]

-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-03-05	SupportSoft DNA Editor Module (dnaedit.dll) Code Execution Exploit	1093	R		D	X	Nine:Situations:Group
2009-03-04	Easy File Sharing Web Server 4.8 File Disclosure Vulnerability	1424	R		D		Stack
2009-03-04	EFS Easy Chat Server Authentication Request Buffer Overflow Exploit (pl)	969	R		D		Dr4sH
2009-03-04	MS Internet Explorer 7 Memory Corruption Exploit (MS09-002) (fast)	3965	R		D		Ahmed Obied
2009-03-03	EFS Easy Chat Server (XSRF) Change Admin Pass Vulnerability	1215	R		D		Stack
2009-03-03	Imera ImeraIEPlugin ActiveX Control Remote Code Execution Exploit	1020	R		D		Elazar

[local]

-::DATE	-::DESCRIPTION	-::HITS					-::AUTHOR
2009-03-05	Media Commands (m3u File) Universal SEH Overwrite Exploit	669	R		D		His0k4
2009-03-05	Media Commands .m3l File Local Buffer Overflow Exploit	621	R		D		Stack

http://milw0rm.com/

Metasploit

What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

Idag findes der samlinger af exploits som milw0rm

Udviklingsværktøjerne til exploits er idag meget raffinerede!

Exploits sælges på både åbne og lukkede ”exploitbørser”

http://www.metasploit.com/

Spamming as a service

BBC programmet Click undersøgte mulighederne for at købe sig adgang til et botnet

Lejede 22.000 computere og afprøvede skadevirkninger

Det virkede (desværre) som forventet

Kilde: Marts 2009 BBC
http://news.bbc.co.uk/1/hi/programmes/click_online/7932816.stm

Hvad vil der ske på serverne i 2009

Problemerne med sikkerhed bliver ikke løst endeligt

Mange angreb vil fortsætte - status quo

Organiseret kriminalitet vil fortsætte med at udnytte mulighederne

Målgruppen for angreb vokser - flere vil blive ramt

Serveroperativsystemerne er dog i mange tilfælde mere resistente idag

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Gode operativsystemer

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

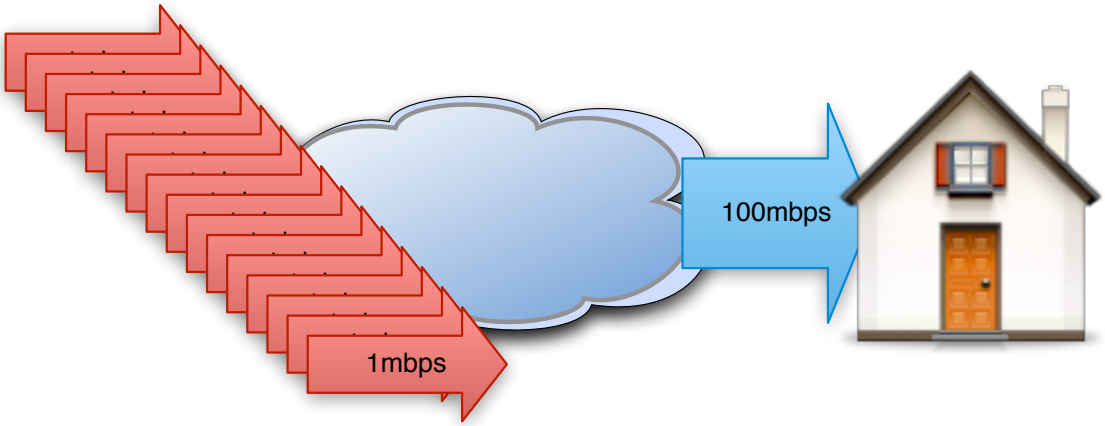
Windows 2008 er klart at foretrække fremfor Windows 2000 servere ;-)

OpenBSD er nok nået længst og et godt eksempel
http://www.openbsd.org/papers/

... og husk alle de sædvanlige råd, opdateringer, firewalls, backup, UPS osv.

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Dør din infrastruktur i 2009



Selvom dine servere er iorden skal du være klar til at modtage angreb

Hvor mange ressourcer bruger du på din infrastruktur

Kan du stadig supportere den og køre din forretning?

Hvad er *din* kerneforretning

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Nyeste botnets

Det amerikanske sikkerhedsfirma Finjan har optrevlet et botnet med 1,9 millioner inficerede computere.

Finjan har offentliggjort fundet på RSA-konferencen og betegner botnettet som et af de største, som er kontrolleret af en enkelt, kriminel bande, skriver CNet.

Botnettet har været aktivt siden februar og hostes i Ukraine, hvorfra det styres af seks personer. Den kriminelle bande styrer de indlemmede Windows XP-maskiner til at kopiere filer, registrere tastetryk, sende spam og tage screenshots.

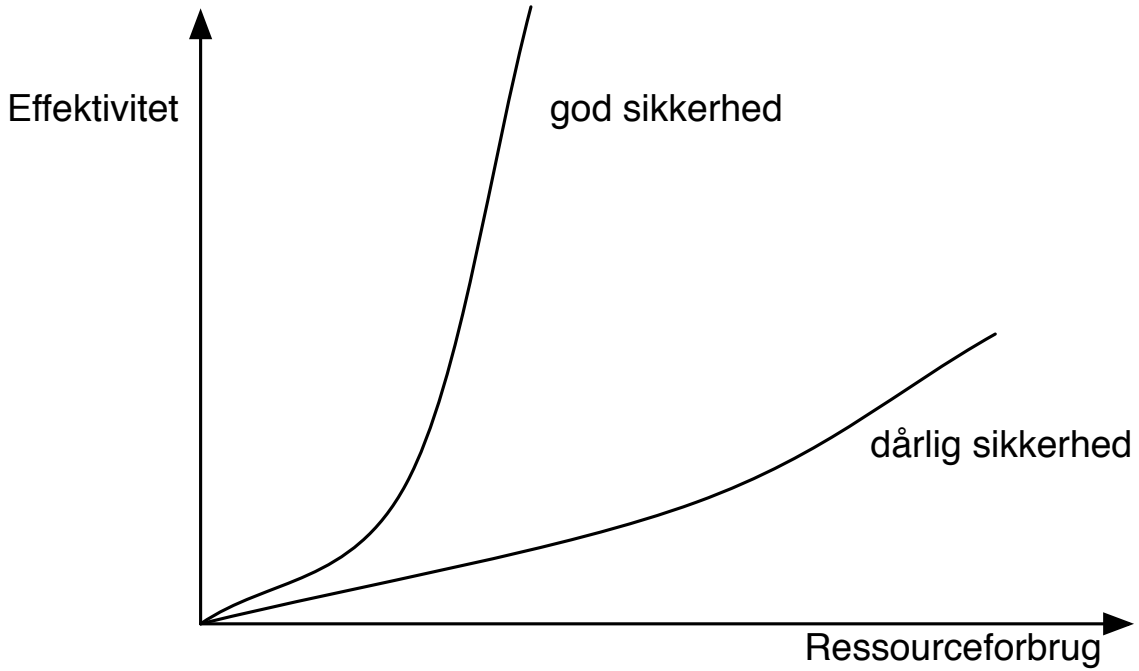
Ifølge det engelske it-medie Computer Weekly har banden solgt kontrollen over de inficerede computere i bundter af 1.000 computere for omkring 250-600 kroner, og ifølge CNet har banden kunnet tjene op til 1,1 millioner kroner om dagen ved at udleje zombierne til andre.

Hver uge har historier om botnets - denne artikel på version2.dk er fra 22. april

Kilde:

http://www.version2.dk/artikel/10679-sikkerhedsfirma-finder-botnet-med-19-mio-zombier

Gode sikkerhedsforanstaltninger



Du har begrænsede ressourcer - udnyt dem bedst muligt - det er din pligt

- **Din indsats skal stå mål med effektiviteten**

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Hvad rammer dine brugere i 2009

Drive by hacking, følg et link til en server

- sekundet efter er din maskine inficeret - *booom*

Phishing - Receipt for Your Payment to mark561@bt....com

Security .net

Mark Willson
145 Church Lane East
Aldershot, Hampshire, GU11 3ST
United Kingdom

Important Note: Mark Willson has provided an Unconfirmed Address. If you are planning on shipping items to Mark Willson, please check the Transaction Details page of this payment to find out whether you will be covered by the PayPal Seller Protection Policy.

Note:

If you haven't authorized this charge ,click the link below to cancel transaction

Cancel Transaction:

https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

*SSL connection:
PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)
---

http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

Kan du selv genkende Phishing kan dine brugere

Fast flux

Tidligere var malware sites på få hackede servere

Idag er malware sites placeret på mange computere

Med lav DNS Time to Live (TTL) ”sikres oppetiden bedre”

Svært at finde alle IP-adresserne og rapportere dem

Fast flux netværk indgår idag i angreb mod danske firmaer

Know Your Enemy: Fast-Flux Service Networks
http://www.honeynet.org/book/export/html/130

Hvordan bliver dine brugere mere sikre

Lad være med at bruge computere ☺

Lad være med at bruge een computer til alt

Firmacomputeren er ikke en privat bærbar, lås den - alle har råd til en privat netbook

Forskellige systemer til forskellige formål

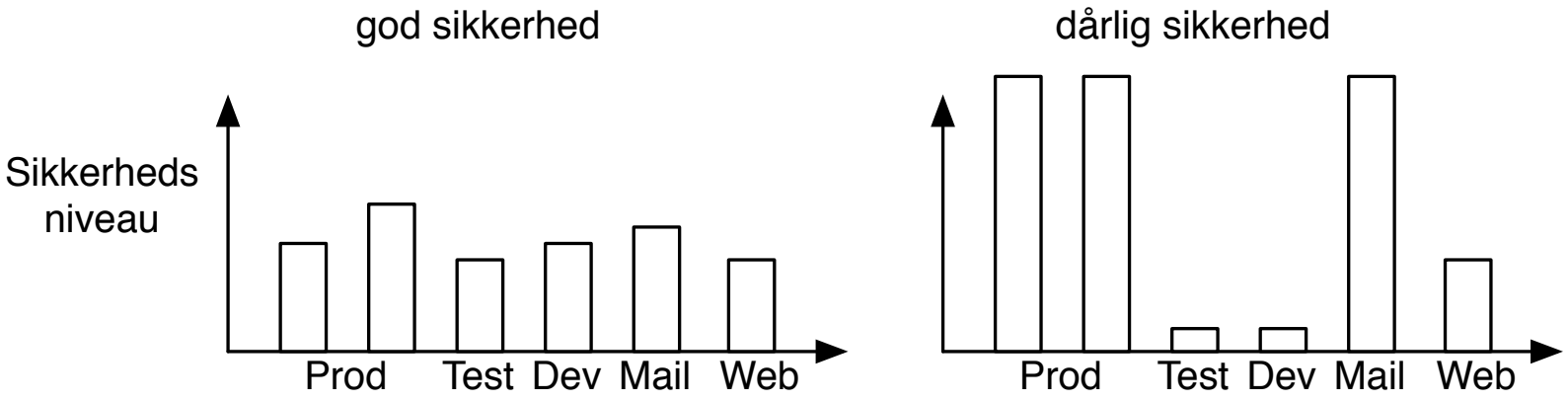
Brug en sikker konfiguration, minimumskonfiguration alle steder

Opsætning af netværk, hvordan? Security Configuration Guides + paranoia

- http://csrc.nist.gov/publications/PubsSPs.html
- http://www.nsa.gov/research/publications/index.shtml
- http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Afbalanceret sikkerhed



Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vælger ikke med vilje den sværeste vej ind

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Forslag til aktiviteter

Accepter at der ikke findes 100% sikkerhed

Vælg dit sikkerhedsniveau

Vælg dine kampe med omhu
- lad andre kæmpe mod spam hvis det ikke er din kerneforretning

For lidt samarbejde

Team up!

Snak med din sidemand/dame - I har sikkert mange af de samme udfordringer.

Informationssikkerhed

Husk følgende: Sikkerhed kommer fra langsigtede intiativer

Informationssikkerhed er en proces

© copyright 2009 Security6.net, Henrik Lund Kramshøj

Spørgsmål?

Henrik Lund Kramshøj
hlk@security6.net

http://www.security6.net

I er altid velkomne til at sende spørgsmål på e-mail

FreeScan.dk - gratis portscanning

FreeScan.dk - free portscanning

Home Miniscan List

On this page you can configure and start a portscan of your IP-address from this server.
Your IP-address is: **85.82.28.68**

Configure and start a scan of the IP-adress

Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.

http://www.freescan.dk

Reklamer: kursusafholdelse

Security6.net

Følgende kurser afholdes med mig som underviser

- IPv6 workshop - 1 dag
  Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk.
- Wireless teknologier og sikkerhed workshop - 2 dage
  En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk, samt integration med hjemmepc og wirksomhedsnetværk.
- Hacker workshop 2 dage
  Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus m.fl.
- TCP/IP workshop 2 dage
  Med fokus på almindelige protokoller i TCP/IP gennemgås grundlaget for internet gennem 5 dage med teori og opgaver på en skalmodel af internet
- Moderne Firewalls og Internetsikkerhed 2 dage
  Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.

Se mere på `http://www.security6.net/courses.html`

© copyright 2009 Security6.net, Henrik Lund Kramshøj