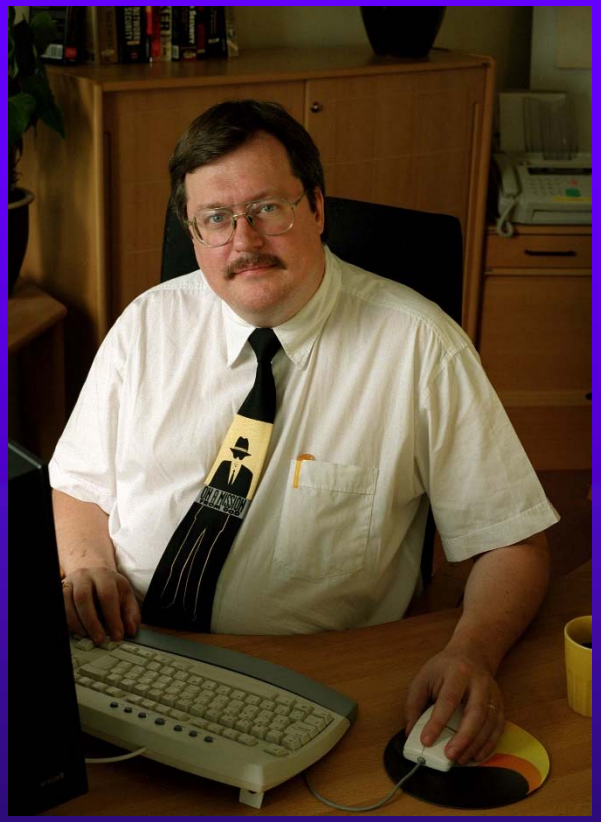
Grundläggande säkerhet för PC, mobil och läsplatta

Joakim von Braun
Säkerhetsrådgivare
von Braun Security Consultants
Senior Net Danderyd 2014-10-13

Joakim von Braun

- Född 1955
- Fil kand
- Professionellt säkerhetsarbete i över 35 år
- Extern rådgivare och konsult åt SÄPO i 25 år
- Arbete för den militära underrättelsetjänsten
- Timbro 1979 - 1988
- Egen företagare i 16 år
- Säkerhetsrådgivare Symantec 2001-2005
- Säkerhetsrådgivare HPS 2007-2009
- Säkerhetssamordnare Sv Radio 2011-2012
- Konsult och rådgivare
- Föredragshållare och lärare
- Journalist och författare
- Historieforskare
- Författare till ”Ryska elitförband”



En helt ny slags säkerhet

- PC-datorn knappt 30 år gammal
- Internet cirka 20 år gammalt
- Från enskild burk till jättenätverk
- Utvecklingen går mycket snabbt
- Olika slags kommunikation – telefoni, TV, larm, hälsodiagnostik (t.ex. blodtryck, blodsocker)
- Aktivitet dygnet runt, 365 dygn/år
- Säkerhet mycket komplext o stort område

Revolution underifrån

- Den teknologiska utvecklingen på arbetsplatsen drivs fram av enskilda intresserade underifrån
- Teknik, inte verksamhet driver utvecklingen framåt

Många jobbiga problem

- Datavirus, trojanska hästar, maskar
- Stöld av teknisk utrustning
- Försvunnen information
- Ändrad information
- Identitetsstölder
- Bedrägerier
- Dåliga lösenord
- Problem med elektriciteten

Säkerhet för vad då?

- Säkerhet på hemmaplan bör knytas samman med säkerheten på jobbet
- ”Bring your own device”
- Att arbeta hemifrån
- I hemmet finns varken säkerhets- eller data-avdelning

Nätverk av nätverk

- Enskild dator
- Skrivardelning
- E-post
- LAN
- WAN
- Internet

Snabb utveckling

Verksamhet dygnet runt

- Drift igång 24 x 365
- Medarbetarna och kunderna
- Leverantörerna
- ... men säkerheten arbetar endast mellan 8.00 och 17.00 vardagar!!!
- Sprids det inga virus på nätterna???
- Tar hackers lov under helgen???
- Dygnetruntverksamheten drabbar också hemanvändarna

Skydd mot fientlig kod

- AV-program på PCn (gäller även Mac) +
- Personlig brandvägg
- Återkommande uppdateringar av program
- Brandvägg som skyddar nätverket
- Sök ny information
- Problemen tycks aldrig ta slut!

- Gäller även Mac-datorer och andra datorer

AV-programmens begränsningar

- Basen är reaktiv – först kommer viruset, sedan kommeer skyddet
- Svårt att hänga med – 5 timmar som bäst
- Vita och svarta listor
- Vem tar ansvar?
- Detta kan ta mycket tid och kosta pengar

Firewalls

- En brandvägg är ett trafik-filter för utgående och inkommande trafik
- Grunden är att allt ska vara stängt
- Personliga brandväggar annorlunda – de tittar på enskilda dataprogram
- Filtreringens bas beror på dig
- Allt på port 80

Fysisk säkerhet

- Hacking kan ersättas av en stöld
- Remote access kan ersättas av fysisk tillgång av datorn
- Lösenord kan enkelt passeras på plats

Glöm inte personalens hemmiljö och anhöriga

- Ditt nätverk finns där personalen är
- Arbete och fritid flyter ihop
- Arbetsgivaren behöver goodwill
- Ökat intresse för säkerhet
- Familjen viktiga stödtrupper

Lösenord (1)

- Statiska lösenord är obsoleta
- 8-12 tecken är ett minimum
- Val på 26 eller 256 tecken?
- Aldrig mer än ett password per ställe
- Glöm inte att lösenord kan passeras
- Lösenord kan avlyssnas
- Kryptering viktigt komplement

Lösenord (2)

- Använd aldrig riktiga ord
- Att lägga till ett tecken räcker inte långt
- Kom-ihåg ramsor bra trick
- Skräpinformation från barndomen
- Byt bokstäver mot siffror: i = 1, o = 0, s = 5
- För mycket krångel är farligt
- Hjälp inte till för mycket
- Skriv helst inte upp dina lösenord (fast det gör jag)

Digitala signaturer

- Garanterar avsändarens legitimitet – talar om att du är du
- Skyddar innehållet mot förändring – ändras innehållet ändras signaturen!
- Kan användas utan kryptering

Brister med dagens kryptering (1)

- Filkryptering lämnar hårddisken öppen för attacker
- Diskkryptering lämnar allt okrypterat efter påloggning
- VPN (krypterad tunnel över Internet) skyddar inte mot interna attacker

Brister med dagens kryptering (2)

- Den är inte tillverkad för människor – krånglig att installera, krånglig att använda
- Den medför extraarbete
- Den skapar för många problem
- Den lämnar blottor
- Den skyddar inte fram till mottagaren
- Den är inte heltäckande

VPN

- Virtuella Privata Nätverk, VPN
- Krypterade tunnlar
- Säkerhet över Internet
- Bra skydd mot avlyssning
- VPN gör dig anonym
- Ingen garanti att trafiken kommer fram
- VPN utan kryptering
- Anonym surfning (t.ex. Tor)

Skydd mot Identitets- och CC-stölder

- Kolla alltid att Web-sajten är legitim
- Jämför kontoutdrag med gjorda inköp
- Riv sönder kontoutdrag och kvitton med kreditkorts-nummer
- Lämna inte ut personliga information i onödan
- Lämna inte ut kreditkorts-information på någon annans uppmaning (t.ex. mail)
- Röj aldrig dina lösenord eller CCV-kod
- Begär ut datalagrad information en gång/år
- Rapportera underligheter till bank och polis

Håll hårt i prylarna

British MoD Stunned By Massive Data Loss

Posted by timothy on Saturday October 11, @04:41AM
from the **austin-powers-meets-the-peter-principle** dept.

Master of Transhuman writes

> "Seems like nobody can keep their data under wraps these days. On the heels of the World Bank piece about massive penetrations of their servers, the British Ministry of Defense has lost a hard drive with the personal details of 100,000 serving personnel in the British armed forces, and perhaps another 600,000 applicants. This comes on the heels of the MoD losing 658 of its laptops over the past four years and 26 flash drives holding confidential information. Apparently the MoD outsources this stuff to EDS, which is under fire for not being able to confirm that the data was or was not encrypted."

Säkerhetskopiering

- Ofta och mycket beroende på verksamheten
- Svårt med databaser
- Glöm inte klienterna – klar policy!
- Image-kopior
- Band, DVD eller hårddisk
- Förvara backupen på annan plats!
- Bevisa att säkerhetskopian tagits

Säker ström i sladden

- Drar ur sladdarna när åskan går!
- Skaffa åskkydd till elkontakten
- Åskskydd till andra sladdar
- Skydda hela huset?
- Vad är en UPS? (Uninterruptabel Power Supply = avbrottsfri elkraft)
- Ju fler problem med strömmen desto oftare måste man ta backup!!!

Prata svenska!

- Vad är ett ”passord”? - Lösenord
- Vad är att ”monitorera”? - Övervaka

- Swenglish gör dig löjlig
- Swenglish ökar distansen

Frågor? Synpunkter?

Joakim von Braun
von Braun Security Consultants

joakim.von_braun@bredband.net
0709-56 16 42
08-659 54 78