

Joakim von Braun på Security Advisory Boardmöte:

”Målet måste vara att skydda verksamheten”

– *Vi har inte två sorters säkerhet i företagen, utan allting är samma sorts säkerhet. Det underströk säkerhetsrådgivaren Joakim von Braun vid High Performance Systems, HPS, när han träffade Security Advisory Board i maj.*

Text: Lotta Eriksson

– De flesta företag har fortfarande en traditionell säkerhetsavdelning och en IT-säkerhetsavdelning. Det är den största anledningen till att vi inte kommer tillräta med dagens säkerhetsproblem, var *Joakim von Brauns* budskap till Security Advisory Board vid ett möte i maj.

– Tyvärr är det nästan enbart tekniker som jobbar med IT-säkerhet och det är särskilt farligt för företag, eftersom det är den vinstgivande verksamheten som man ska skydda. Huvudmålet måste vara att skydda verksamheten och där sammanfaller intresset för traditionell säkerhet och IT-säkerhet, poängterade han bland annat.

Joakim von Braun ville med detta belysa att IT-brottslingar, precis som kriminella i traditionell mening, är ute efter pengar och att bedrägerier eller utpressning i dag kan ske i allt mer sofistikerade former, från att hacka sig in i en dator till att fysiskt stjälja datorn.

Framtida hot och hinder

Vid mötet informerade han om hur de framtida IT-säkerhetshoten ser ut och vad man kan, eller snarare bör, göra för att undvika dem.

– Den aktuella hotbilden är att pengar betyder allt och att information är vägen till pengar. Vi kommer att se en fortsatt ökning av trojaner och maskar, botnets, nätfiskeattacker och hacking med inriktning på att tjäna pengar. De riktade attacker ökar och vi måste arbeta mer aktivt mot den ökande insiderproblematiken, konstaterade han.

Som Aktuell Säkerhet tidigare har berättat (nr 4/07) ägnar sig internetbrottslingarna åt social ingenjörskonst och söker information genom att rikta sig mot personer i företagen för att övertyga, lura eller muta dem. Informationslämning sker både av misstag och av illojalitet.

– Man ska ha klart för sig att lojaliteten mot arbetsgivarna är lägre numera och att det inte bara handlar om att anställda kan utsättas, utan även konsulter, anhängiga, stödare, väktare och andra som rör sig i lokalerna, förtydligade han.

Andra hot är USB-minnen, som kan fungera som ypperliga hackingverktyg, genom att de prepareras för att samla in information eller sprida smitta, att skrivarna inte längre bara är skrivare utan nu för tiden har hårddiskar som fungerar som servrar och innehåller sparad företagsinformation och att nyttillverkade, okända trojaner kan köpas för en tusenlapp.

– De flesta verktyg går att ladda ner eller köpa på nätet och finns inte just det som någon efterfrågar, dyker det alltid upp personer som är beredda att skraddarsy en trojan för ett specifikt företag och som garanterar att inget antivirusprogram hittar den.

Brottslighet på Internet kan också handla om spionage av olika slag, både med vetenskapligt, ekonomiskt, tekniskt eller kommersiellt syfte.

Möt hoten på bästa sätt

Joakim von Braun gav också Security Advisory Boards medlemmar tips på hur man kan svara upp mot de framtida hoten.

– Man måste ha säkerhet 24 timmar om dygnet, 365 dagar om året, oavsett om det handlar om att någon fysiskt är på plats, har beredskap eller man hyr in tjänsten. Man måste också ha en enda säkerhetsfunktion där man samlar all säkerhet, en aktiv säkerhetsunderrättelsetjänst och utveckla samarbete mellan företag, Internetleverantörer och myndigheter.

– Dessutom är det viktigt med en bra intern utbildning och personalhantering, sade han och avslutade med:



All brottslighet handlar till syvende och sist om att tjäna pengar, även nätkriminalitet. Foto: FIB

– Alla som har kundrelationer på nätet är utsatta, så var ödmjuka inför allt ert behov av säkerhet!

Security Advisory Board, som initierats av Aktuell Säkerhet och leds av *Tommy Svensson* från Näringslivets Säkerhetsdelegation, träffas fyra gånger om året. På majmötet deltog bland andra *Peter Köhler* från Securitas, *Janne Rastas* från Addici Security, *John Hedesand* från Assa, *Sven Boëthius* från Gunnebo och *Anders Leide-man* från Multicom Security.

De som ingår i rådet är dessutom Coromatic, Svensk Krisledning, G4S, Clavister, Grontmij och SOS Alarm. □

Läs mer om Joakim von Braun och hans krönika om IT-säkerhet på sidan 14.

Välkomna!

Nya medlemmar i Security Advisory Board: Bravida Säkerhet och Niscayah. Läs mer om Bravida Säkerhet och flaggskeppet Integra i Aktuell Säkerhet nr 2/08 och om Niscayah på sidorna 28-29 i denna tidning.