Pressmeddelande
2 juni 2009

CISCO IRONPORT SECURITY INDEX – JUNI 2009

LISTA – Nätets 8 vanligaste fällor

Nya metoder att lura användare att ladda ner virus och skadlig kod till sina datorer utvecklas kontinuerligt. Målet är att ta kontroll över användares datorer och få tillgång till koder och lösenord samt att göra datorn till en zombie, det vill säga att använda datorns kapacitet till att skicka skräppost. Utvecklingen är blixtsnabb. Här är de främsta fällorna!

1. **Falska chatvänner**
   Infekterade snabbmeddelanden från vänner i chatprogram till exempel MSN. Snabbmeddelandet länkar vidare till en webbsida med skadlig kod. Mottagaren lockas att klicka på länken genom en intresseväckande hälsningsfras som till exempel *”Visst är det här du?!?!”*.

2. **Elakt Twitterflöde**
   Twitterkonton med syfte att länka vidare till infekterade webbsidor. En oaktsam användare kan av misstag följa konton som administreras av spammare som använder Twitter som kanal att sprida virus och skadlig kod.

3. **Vilseledande webbadresser (Tiny URL)**
   Förkortade webbadresser. Att korta ner webbadresser för att lättare kunna dela med sig av dem genom mikrobloggar är vanligt förekommande. Tyvärr blir det då svårt för användaren att på förhand veta vad länken leder till, något som kan utnyttjas av spammare.

4. **Elaka vykort**
   E-vykort med skadlig kod. Mottagaren får ett e-postmeddelande med länk till ett e-vykort eller påstådd semesterbild. När användaren klickar på länken laddas skadlig kod ner till datorn.

5. **Falska Anti-virusprogram**
   Webbsidor som lockar med gratis skanning av användarens dator. Istället för att hitta infekterade filer installeras virus och spyware på datorn. Det förekommer också att användaren betalar för anti-virusprogrammet, vars syfte i själva verket är att ta kontroll över datorn.

6. **Oäkta Blogg-kommentarer**
   Länkar i bloggars kommentarer som leder till infekterade webbsidor. Läsaren lockas att klicka på länken eftersom bloggen hanterar ett ämne som är av intresse.

7. **Läkemedelsspam**
   Skräppost som gör reklam för läkemedel. Den länkar vidare till en ofta väldesignad och trovärdig sida där läsaren kan köpa billiga läkemedel (oftast Viagra).

8. **”Tjäna pengar”- spam**
   Skräppost som meddelar mottagaren att hon eller han har vunnit på lotto, ska få tillbaka pengar på skatten eller om någon annan ekonomisk möjlighet.

– Det är viktigt att vara medveten om de fällor och fallgropar som finns på internet idag. För bara några månader sedan såg hotbilden annorlunda ut, vilket gör det svårt att hänga med. Därför är det viktigt att ha ett bra IT-skydd, samtidigt som man ska använda sitt sunda förnuft, säger Henrik Davidsson, Nordenchef på Cisco IronPort.

För mer information:
Henrik Davidsson, Nordenchef, Cisco IronPort
Tel: 0701-90 11 00
E-post: hdavidsson@ironport.com

Jonathan Stara, Spotlight PR
Tel: 076-545 40 14
E-post: jonathan.stara@spotlightpr.se

Om Cisco IronPort:
Cisco IronPort är marknadsledande inom anti-spam, anti-virus & anti-spywarelösningar för företag. Cisco IronPorts lösningar baseras på SenderBase®, världens största epost- & webbövervakningsnätverk som bevakar mer än 30 procent av världens webb- och e-posttrafik. Företaget är en del av Cisco Systems och finns över hela Norden. Några av kunderna i Sverige är Volvo, Bredbandsbolaget/Telenor, ICA och Krisberedskapsmyndigheten.

För mer information om Cisco IronPorts produkter och tjänster, vänligen besök www.ironport.com.