

2.10.2006

CERT-FI

LÄGESRAPPORT 3/2006

Under årets tredje kvartal reagerade CERT-FI på informationssäkerhetsändelserna genom att publicera 36 aktuella artiklar och genom att skicka några särskilt riktade meddelanden. Antalet fall är ganska normalt, men några nya företeelser upptäcktes också.

CERT-FI fick veta om ett fall där data om flera tiotal finländska internet-användare hade kommit i obehöriga händer. Data hade skaffats med ett Haxdoor spionprogram som hade infekterat arbetsstationerna. Globalt omfattade fallet tiotusentals eller till och med hundra tusentals offer.

Sedan juli har flera aktörer publicerat sårbarheter i arbetsstationstillämpningar, för vilka det inte fanns någon korrigerings vid publiceringstiden. Många sårbarheter utnyttjades för att sprida skadliga program. De webbsidor där skadliga program distribuerades, fanns oftast i samma tjänsteleverantörens nät.

Under ASEM-toppmötet som arrangerades i september i Helsingfors rapporterades inte några betydande fall som skulle ha äventyrat informationssäkerheten.

Internetbedrägerier

Nordea-bankens svenska kunder var föremål för phishing, dvs. att man försökte stjäla kundernas data med hjälp av webbplatser som liknade nätbankens sidor. Phishing riktades inte mot finländska nätbankskunder. Med skräppost kommer dock hela tiden länkar till bluffsidor, vilka också gäller finländska internetanvändare. Exempelvis eBay- och PayPal-tjänsterna har många finländska kunder.

Data kan också stjälas genom att spionera användarens nättrafik till äkta servicesidor. Haxdoor-spionprogram stjälar uppgifter som användaren matat in på olika blanketter på webbsidorna, såsom användaridentifikationer och kreditkortsuppgifter, och skickar dem vidare till en insamlingsserver som angriparen upprätthåller. Globalt har man rapporterat att så gott som hundra tusen datorer har drabbats av dataintrång med Haxdoor. CERT-FI fick också veta om några fall där finländska användares data hade avslöjats under våren och sommaren. Ingenting tyder dock på att syftet med bedrägeriet uttryckligen skulle ha varit att sträva efter data om finländska användare eller elektroniska tjänster. Tjänsteleverantörerna och dataombudsmannen har blivit informerade om saken.

Haxdoor, samt Torpig och BZub som betar sig på samma sätt, är exempel på dataintrång vars syfte är att samla data som angriparen önskar utnyttja ekonomiskt. Det är ganska svårt att upptäcka om en dator redan har drabbats av Haxdoor, men de allmänna och uppdaterade antivirusprogrammen hindrar datorn från att bli infekterad.

Sårbarheter i arbetsstationer

H. D. Moore, som blev känd av Metasploit-projektet, meddelade i sin blogg att han kommer att släppa en ny bug i olika webbläsare varje dag under juli månad. Han kallade det "The Month of Browser Bugs". Också många andra aktörer publicerade sårbarheter av vilka en del ännu inte har korrigerats.

Sårbarheter som påverkar arbetsstationsanvändarnas säkerhet upptäcktes både i Windows och i Microsoft Office. Några av dem möjliggjorde körning av den programkod som angriparen valt i

2.10.2006

CERT-FI

användarens dator. Tillverkaren har publicerat programuppdateringar för att laga sårbarheterna. Enligt den information som CERT-FI har fått, har vissa sårbarheter utnyttjats aktivt.

Mot slutet av kvartalet upptäcktes två sårbarheter i Windows-operativsystem. De utnyttjas så att användaren av Internet Explorer lockas till attack mot den webbsida som används. Den ena sårbarheten korrigerades exceptionellt snabbt, men det är fortfarande möjligt att utnyttja den mot arbetsstationer som inte har uppdaterats. Än så länge finns det ingen korrigering för den andra sårbarheten, som utnyttjas för att sprida skadliga program. Man kan skydda sig mot den genom att ändra datorns Windows-inställningar.

I McAfee Security Center antivirusprogram upptäcktes en sårbarhet som kan utnyttjas genom webbsidor som bearbetats på ett visst sätt. Fel i informationssäkerhetsprogram kan göra att skadliga program eller intrångsförsök inte upptäcks.

Sårbarheter upptäcktes också i drivrutiner till trådlösa nätkort (WLAN) för bärbara datorer. Dessa sårbarheter möjliggör körning av angriparens egen programkod i datorn. Attackerna är möjliga endast inom WLAN-kortets täckningsområde, vilket begränsar utnyttjandet av sårbarheterna. Korrigerade drivrutiner har publicerats för system som är utsatta för sårbarheter.

Sårbarheter i servrar och nätanläggningar

Under kvartalet upptäcktes också sådana sårbarheter som hade inverkan på leverantörer av internetförbindelser och nättjänster. Ett fel i JunOS-operativsystemet för Juniper-routningsanläggningar möjliggjorde en blockeringsattack vars ursprung var ett fel i behandlingen av IPv6-paket. Förvalda inställningar för vissa versioner av IOS-operativsystemet för Cisco-routrar tillåter ändring av routerns inställningar med administratörens rättigheter. En sårbarhet som möjliggjorde en blockeringsattack upptäcktes i Ciscos system för förhindrande av intrång. Två sårbarheter som möjliggjorde en blockeringsattack upptäcktes i BIND som är den mest använda serverprogramvaran för Internets namntjänst (DNS). Det finns korrigerande programuppdateringar för alla ovannämnda sårbarheter. För Oracle-databasprogrammet publicerades korrigeringar för en mängd sårbarheter.

Det finns brister i informationssäkerheten i en hel del programvaror som är avsedda för att producera innehåll på webbsidorna och för att publicera sidorna; en del av bristerna kan bero på att de förvalda inställningarna är osäkra. Angriparen kan utnyttja sårbarheterna exempelvis med tanke på att ändra sidornas innehåll, men det kan också vara möjligt att köra angriparens programkod på webbservern. Offentligt tillgängliga publiceringssystem, såsom Joomla och Mambo, har blivit allt vanligare också bland privatpersoner när de söker hjälpmedel för att upprätthålla sina webbsidor.

Riktade attacker

Från utlandet rapporterades ett riktat utnyttjande av en sårbarhet i Microsoft PowerPoint. CERT-FI fick veta att finländska företag också har varit föremål för riktade attacker och att en läroanstalt har varit föremål för dataintrång.

Framtidsutsikter

Fientligt agerande gäller mest att skaffa användares data. Tröskeln för att göra skadliga program har blivit lägre och kräver mindre erfarenhet och programmeringskunskap än tidigare. Program och tjänster som erbjuds för att sprida dem kan köpas på internet till ett relativt förmånligt pris.



2.10.2006

CERT-FI

Några nätoperatörer erbjuder förbindelser och registrering av domännamn för spridning och försäljning av skadliga program eller för att göra bluffsidor. De svarar inte på anmälningar om missbruk. Sådana operatörer finns till exempel i Förenta Staterna, Ryssland och Kina.

E-postförmedlingen försvåras på grund av spärllistor som omfattar postserverar som sprider skräppost. De som upprätthåller serverna använder listorna för att hindra skräppost från serverar som finns på listan. Om en server utan skäl har hamnat på listan har e-post kanske inte alltid nått fram. Kommunikationsverket har en lista där tillförlitliga finländska e-postserverar samlas in. De som upprätthåller serverna kan tillåta att meddelanden förmedlas från serverna oberoende av om de hamnat på spärllistan. Det finns också motsvarande internationella projekt på gång.

Namn som liknar domännamn som registreras för stora internationella evenemang registreras ofta i syfte att skämta eller bedraga, i syfte att göra ofog eller propaganda, eller för att komplettera innehållet på de offentliga sidorna, och de upprätthålls av sakintresserade. Det är omöjligt att registrera alla sådana domännamn som kan användas för olika ändamål parallellt med det egentliga domännamnet.