

5.1.2007



INFORMATIONSSÄKERHETSÖVERSIKT 2006

Under 2006 var syftet med kränkningar av informationssäkerhet fortfarande att få ekonomisk nytta genom att skaffa och utnyttja personuppgifter och uppgifter om betalningsmedel för användare av datorer och elektroniska tjänster.

Ett nytt fenomen där man började sprida spionprogram till angripna datorer blev allt vanligare. Programmen används för att ta reda på www-användarnas uppgifter och att sprida dem vidare till utomstående. Uppgifter om användare samlas alltså under förbindelsen när man använder riktiga webbtjänster och inte genom att skapa liknande bluffsidor. Programmen kan ta över personuppgifter, användarnamn, lösenord och kreditkortnummer mm. Verksamheten var omfattande och organiserad, men CERT-FI fick höra bara om några sådana fall där uppgifter om finländska användare av elektroniska tjänster hade hamnat i orätta händer.

Det centrala skadliga programmet som användes för att få uppgifter om användare var Haxdoor. CERT-FI deltog i analysen av Haxdoors funktion och publicerade ett program som kan ta bort infektionen från datorn.

Med tanke på informationssäkerhet upptäckte man inte några särskilda händelser i samband med Finlands EU-ordförandeskap eller internationella möten i Finland.

Sårbarheter i mjukvara gällde oftast de vanligaste webbläsarna, Windows-operativsystemet och MS Office. Sårbarheter hittades också i andra operativsystem och program.

Spridning och utnyttjande av skadliga program orsakar betydelsefulla ekonomiska hot. Skadliga program spridas och används systematiskt för att få ekonomisk nytta i form av pengar. För att kunna upptäcka sådan verksamhet och för att utreda logiken och utförare bakom verksamheten kräver ofta internationellt samarbete mellan olika myndigheter, företag och aktörer inom informationssäkerheten.

Från bluffsidor till att spionera på telekommunikation

Under årets lopp fick CERT-FI veta om flera webbsidor som liknar äkta elektroniska tjänster men som strävade efter att få uppgifter om användare (phishing). De vanligaste målen var auktionssidor (t.ex. eBay), betalningstjänster (t.ex. PayPal) och olika bankers webbsidor. För finländska webbsidornas del förekom det sidor som liknade Nordea-bankens tjänster. Oftast bluffas dock internationella tjänster som även har en hel del finländska användare.

Utöver dessa phishing-sidor försökte man också lura användare av tjänster att ge sitt användarnamn, lösenord, kreditkortsnummer och andra konfidentiella uppgifter när de matade uppgifterna in i äkta webbtjänster. Det skedde så att man försökte smitta användarens dator med spionprogram som avlyssnar webbförbindelser och tar över användarens uppgifter och förmedlar dem till externa personer för missbruk.

Skillnaden mellan bluffsidor och spionprogram är betydande bland annat därför att phishing-sidorna ofta kan identifieras under förbindelsen, medan ett spionprogram som försöker ta över användarens uppgifter inte alls upptäcks. Programmen använder sk. rootkit-tekniker för att dölja sig från användare och antivirusprogram. Om en dator blir infekterad innan antivirusprogrammet uppdateras för att kunna identifiera det skadliga programmet, kan det vara mycket svårt att upp-



5.1.2007

CERT-FI

täcka infektionen senare. Att skydda WWW-förbindelsen med SSL hindrar inte att spionera, eftersom programmet tar över uppgifterna innan de har blivit enkrypterade för webbförbindelsen.

För första gången blev CERT-FI informerad om spionprogrammet Haxdoor i februari. Haxdoor är ett program som efter att ha smittat en dator gömmer sig från användare och säkerhetsprogram. Därefter samlar det uppgifter som användaren har matat in på olika blanketter på olika webbsidor och förmedlar dessa uppgifter via nätet till en server för sammanställning. Haxdoor är det centrala skadliga programmet som används för att få uppgifter om användare. CERT-FI deltog i analysen av Haxdoors funktion och publicerade ett program som kan ta bort infektionen från datorn i oktober.

Genom sitt internationella samarbetsnätverk blev CERT-FI i juli informerad om att uppgifter om tiotals finländska användare av elektroniska tjänster hade hamnat i obehöriga händer. Ingenting tyder dock på att insamlingen av uppgifterna i synnerhet hade gällt Finland, utan majoriteten av uppgifter som man hade fått med spionprogram gällde andra än finländska användare och tjänster.

Enligt CERT-FI:s iakttagelser finns de webbsidor som sprider skadliga program ofta i samma internet-tjänsteleverantörers nät. Det är väldigt viktigt att utveckla det internationella samarbetet för att avvärja sådan skadlig verksamhet.

Utnyttjande av sårbarheter i programvara

Sårbarheter som beror på fel i programvara kan betyda att en dator blir smittad av ett skadligt program. Sårbarheter söks systematiskt. För sökningen utvecklas också automatiska testmetoder. En teknik som används för att hitta sårbarheter är fuzzing: test av programvarans förmåga att klara av ett oväntat indata genom att systematiskt genomgå stora mängder "trasiga" användningsfall t.ex. så att man manipulerar innehållet i filerna som programvaran använder. CERT-FI har aktivt strävat efter närmare samarbete med sårbarhetsforskare. Syftet med det är att nå en kontrollerad kedja från upptäckt av fel till avhjälpande och ansvarsfull publicering.

Årets mest hotande enskilda fall var ett fel i programvara som hittades vid behandlingen av Windows metafile-filer och gällde alla versioner av Windows-operativsystem. Felet utnyttjades i början av året i omfattande grad innan en rättelse var publicerad och systemen uppdaterade. Det var svårt att skydda sig mot sårbarheten och det var lätt att utnyttja sårbarheten genom www-sidor, e-post, snabbmeddelanden och peer-to-peer nätverk. Effekterna av felet förblev dock mindre än befarat. Samarbetet mellan CERT-aktörerna, teleföretagen, antivirusbolag och Microsoft spelade en avgörande roll vid avvärjande av skadeeffekterna.

Under årets lopp offentliggjordes också flera andra sårbarheter för programvara som används i omfattande grad, t.ex. Windows-operativsystemet, Microsoft Office och webbläsare. En del av dessa sårbarheter utnyttjades aktivt för att sprida skadliga program.

Under året upptäcktes sårbarheter även i sådana utrustningar och tillämpningar som är viktiga för Internets funktion, t.ex. operativsystem för Cisco och Juniper som tillverkar routrar, program för e-postserver Sendmail och BIND som används för namnservrar. CERT-FI samarbetar med tillverkare av maskinvaror och programvaror och med Internet-operatörer vid koordinering av information om sårbarheter. Sårbarheterna utnyttjades inte särskilt mycket innan programmen hade avhjälpats.

Publicering av sårbarheterna politiseras

Det ser ut att några sårbarhetsforskare driver en mer radikal linje i förhållande till den normala



5.1.2007

CERT-FI

publiceringen. Det betyder att sårbarheterna publiceras innan programtillverkaren har hunnit avhjälpa felet. Syftet kan vara att utöva tryck på programtillverkare att avhjälpa felet snabbare än idag.

I juli offentliggjorde H.D. Moore på sin blogg varje dag en ny sårbarhet i en webbläsare med "The Month of Browser Bugs" som tema.

I november drevs ett liknande projekt "The Month of Kernel Bugs" där en sårbarhet i något operativsystem offentliggjordes varje dag. Windows, Linux, MacOS X, FreeBSD, Solaris och olika programvaror och drivrutiner för trådlösa nätverksutrustningar utgjorde mål för projektet.

Cecar Cerrudo hade för avsikt att offentliggöra sårbarheter i Oracles databasprogram med titeln "The Week of Oracle DataBase Bugs". Han ville visa att Oracles program inte var säkra samt kritisera att bolaget avhjälpde programfel för långsamt, men han drog tillbaka försöket.

Riktade attacker

Spridning av skadliga program kan även riktas mot en begränsad grupp av användare, t.ex. mot personalen vid ett visst företag eller mot tjänster som företaget producerar. Syftet med attackerna kan vara att ta reda på hur en organisation fungerar i en exceptionell situation eller att få tag på företagets interna uppgifter, men också personliga motiv kan utgöra grund för riktade attacker.

CERT-FI fick veta om några enskilda attacker som var riktade mot finländska företag eller tjänster. Generellt sett tycks de inte ha vuxit i antal men en del av dem var särskilt svåra att avvärja.

Den typiska angreppsmetoden var ett skadligt program maskerat som bilaga till ett sakligt e-postmeddelande. Antivirusprogrammen kunde inte igenkänna programmet för det hade designats just för denna attack. Programmet utnyttjade en sårbarhet som programtillverkaren inte var medveten om. Attacker riktades även mot organisationers offentliga tjänster, såsom webbsidor eller e-postservrar.

Fel och störningar

De största störningarna i telekommunikationen var avbrott i mobiltelefonnät på glesområden. En del av störningarna hänförde sig till avbrott vid elleverans och en del till problem i telekommunikation. Problemen orsakades av fel i utrustningar eller konfigurationer. Felet avhjälpes relativt snabbt och avbrotten var i allmänhet korta.

Mot slutet av året fick CERT-FI veta att mängden skräppost hade börjat öka kraftigt och att nya skadliga program hade spridits med e-post.

Framtidsutsikter

Kränkningar av informationssäkerhet mot datoranvändare fortsätter. Dataintrång görs fortfarande oftast i vanliga användares datorer i stället för offentliga eller företagets servrar. Man utnyttjar sårbarheter i programvaror och operativsystem genom vilka skadliga program sprids till användarnas datorer. Kanaler för spridning kan fortfarande vara e-post, lämpligt omarbetade bilagor till e-post eller webbplatser som utnyttjar sårbarheter i webbläsare.

Sändare av skräppostmeddelanden försöker utveckla nya sätt att passera genom filter. De försöker utforma sina meddelanden så att de passerar genom de mest allmänna filtreringsprogrammen på teleoperatörernas och företagets e-postservrar eller så att de försöker skada filtrens funktion.



5.1.2007

CERT-FI

Skadliga program och de kommandoservrar och -förbindelser som utnyttjar dem utvecklas vidare och det blir ännu svårare att utreda funktionen av relaterade botnet-nätverk och program. Skadliga program gömmer sig från operativsystemet och antivirusprogram allt bättre.

Inom de närmaste tiderna uppdateras en stor mängd operativsystem när den nyaste Windows-versionen "Vista" publiceras. Övergången till ett nytt system kan medföra en ökad risk för nya sårbarheter och utnyttjande.



5.1.2007

CERT-FI

Ordlista:

Skadligt program = engl. malware, allmän benämning för ett "fiendligt" program med skadlig funktion. Skadliga program kan bl.a. samla uppgifter, sprida skräppost, scanna datanät, attackera mot servrar eller förlora användarens uppgifter.

Phishing = "Nätfiske" av användarens uppgifter genom att lura användaren ge dem i en webbtjänst som liknar en äkta tjänst men som hackaren förfogar över. Användare kan lockas till sådana phishing-sidor t.ex. genom e-postlänkar. Servrarna befinner sig ofta i privatansvärdarens datorer i vilka hackaren har installerat ett serverprogram på distans.

Spionprogram = I användarens dator installerat skadligt program som samlar uppgifter om användare genom att iaktta användarens webbläsning eller telekommunikation. Programmet kapar exempelvis uppgifter som användaren har matat in på olika webbblanketter och förmedlar dessa uppgifter via nätet till en server som hackaren förfogar över.

Rootkit = Allmän benämning för tekniker och programmeringsverktyg som gör att ett skadligt program får största möjliga behörigheter i en dator och som gör att ett skadligt program kan gömma sig från användare, operativsystem och andra program - även antivirusprogram - och passera skyddet vid brandväggen.

Haxdoor = Spionprogram som använder även rootkit-tekniken för att gömma sig från användare och antivirusprogram.

Blockeringsattack = Strävan efter att försvåra eller förhindra serverns eller tjänstens funktion med överbelastning. Angriparen kan ha en stor mängd angripna datorer som deltar i överbelastningen av målet t.ex. så att de orsakar stora volymer trafik eller förbindelseförsök till servern.

Botnet = Nätverk av angripna datorer och kommandoservrar som står i förbindelse med datorer. Angripna datorer kan hanteras på distans och de kan användas för skräppost eller blockeringsattacker utan att användaren vet om det.