



30.1.2006

CERT-FI

ÅRSRAPPORT 2005

Syftet med kränkningarna av informationssäkerheten år 2005 var ofta ekonomisk vinning. Kränkningarna riktade sig mot informationssäkerhetens svagaste länk, nämligen den datoranvändande människan. *Phishing-bedrägerierna*, som varit mer eller mindre okända inom de finska och svenska språkområdena, nådde Finland i oktober. Med phishing avses olagligt inhämtande av uppgifter för ekonomisk vinning, såsom personuppgifter och uppgifter om betalningsmedel. Vid phishing-bedrägerier är målet i allmänhet att få användaren att själv lämna ut uppgifterna.

De skadliga programmen fortsatte att infektera oskyddade internetuppkopplade datasystem. Dagens skadliga program möjliggör fjärradministration och -uppdatering. Enligt CERT-FI:s undersökningar är upp till tusentals finländska datorer ständigt infekterade av *skadliga bot-program* med fjärråtkomst. Uppgifterna i och kommunikationen från de kapade datorerna utsätts för skadlig verksamhet som delar av bot- eller robotnätverk. Globalt är antalet kapade datorer flera miljoner.

Ifråga om servrar finns den flitigast utnyttjade sårbarheten hos PHP-tekniken i www-tjänster eller hos serverapplikationer som bygger på denna teknik. CERT-FI får fortlöpande rapporter om automatiska lösenordsgissningar i terminalservrar och om fall där lösenord har inhämtats med hjälp av trojanprogram som har installerats i servrar. I slutet av året användes flera finländska organisationers oskyddade namnservrar för realiseringen av en global denial of service-attack.

Framförallt i slutet av året kunde man konstatera att informationssäkerheten intresserar media och allmänheten. Bredbandsförbindelserna har gjort Internet till en allemansteknik. Informationsverksamheten har avgörande betydelse för medborgarnas färdigheter att använda informationsnäten tryggt och säkert.

Utnyttjad sårbarhet

Sårbarheten hos operativsystemet Windows undersystem *Universal Plug and Play (uPnP)*, som gavs ut i augusti, visade sig vara den mest utnyttjade under hela året. Tusentals finländska hemdatorer infekterades av nätmaskar, som enbart genom sin spridning åstadkom olika funktionsstörningar i flera företagsnät.

En annan utnyttjad sårbarhet hos Windows utgjordes av ett planeringsfel i bildformatet *Windows Metafile (WMF)*. De första skadliga programmen som utnyttjade sårbarheten spreds innan programtillverkaren hade hunnit publicera sin felkorrigering. Sårbarheten utsatte användarnas datorer för angrepp av skadliga program via bland annat www, e-post, snabbkommunikationsprogram och P2P-nät. Felet gällde alla Windows-versioner, vilket visar att det handlade om ett omfattande problem. Trots att utnyttjandet av sårbarheten är utbredd, är det tillsvidare mindre omfattande än beräknat.

Många välbekanta kundprogram, såsom webbläddrare, program för snabbkommunikation, program för Internet-telefoni och multimedieprogram, var behäftade med informationssäkerhetsproblem. Enbart för bläddrarprogrammen publicerades tiotals informationssäkerhetsrelaterade korrigeringar. Bläddrarprogrammets svagheter ifråga om filtrering och genomsläpplighet har använts flera år som attackkanaler. Av samma orsak är programmen för snabbkommunikation och P2P-nätsapplikationerna intressanta områden för dem som skapar och sprider skadliga program.



30.1.2006

CERT-FI

CERT-FI utfärdade sammanlagt 12 bulletiner under året, i vilka varnades för sårbarhet i de viktigaste antivirusprogrammen. De flesta bristerna gällde hanteringen av filbilagor. CERT-FI känner dock inte till att sårbarheten skulle ha använts för att kringgå datorskyddet. Utnyttjandet av sårbarheten försvårades förmodligen av att antivirusprogrammen i allmänhet uppdateras automatiskt utan aktiva åtgärder av användaren.

Kränkningarna av informations säkerheten via webbaserade diskussionsspalter och *bloggar* ökar i takt med spaltarnas och bloggarnas popularitet. Sårbarheten hos system som baserar sig på *PHP-teknik* utnyttjades flitigt. CERT-FI utfärdade i början av året varningar avseende det populära programmet *phpBB* och följde med försöken att utnyttja sårbarheten hos *XML-RPC*.

I november utfärdade CERT-FI en varning avseende flera sårbarheter hos protokollrealiseringen *ISAKMP*. Sårbarhetsundersökningen och korrigeringsarna koordinerades konfidentiellt från början av året av tiotals programtillverkare, OUSPG-gruppen vid Uleåborgs universitet som hade utvecklat det testsystem som användes för sårbarhetsundersökningen, CERT-FI och engelska NISCC. Förteckningen över sårbara program och apparater har uppdaterats flera gånger efter att tillverkarna har publicerat sina korrigeringsuppdateringar. CERT-FI känner inte till något lyckat utnyttjande av publicerade sårbarheter.

Den sårbarhet som man fann i programmen i IP-nätens nätrouterar i januari 2005 kunde åtgärdas och programmen uppdateras innan någon attack gjordes. Det konfidentiella samarbetet mellan programtillverkarna, de viktigaste säkerhetsaktörerna och teleföretagen betraktades som värdefullt och gav önskat resultat.

Utvecklingen av skadliga program

Tyngdpunkten hos utvecklingen av skadliga program har förskjutits från konventionella virus- och nätmaskprogram mot mångsidigare bot-program med fjärråtkomst. De skadliga bot-programmen skrivs nästan uteslutande för Windows-plattformar, förmodligen på grund av att dessa är så allmänna. Bakom phishing-bedrägerier, skräppost, spionprogram och denial of service-attacker finns nästan alltid skadliga bot-program.

Ett gott exempel på fenomenets omfattning är arresteringen av tre personer i Holland i oktober. Personerna hade kontroll över, försiktigt uppskattat, ett nätverk om 1,5 miljoner datorer som hade infekterats med det skadliga programmet *Toxbot*. Utnyttjandet av skadliga program, som har en professionell prägel, visar tydliga tecken på organiserad verksamhet. I verksamheten deltar personer som har specialiserat sig på olika områden: sårbarhetsundersökning, skrivning av skadliga program, upprätthållande av bot-nät och förmedling av den olagliga ekonomiska nyttan.

Det finns bevis på att de skadliga programmens standardegenskaper allt oftare omfattar förmågan att gömma sig för datoranvändarna och virusprogrammen. Under året upptäcktes flera vitt spridda skadliga program, som i vissa fall uppdaterades flera gånger per dygn. Syftet med versionsuppdateringen är att ständigt vara steget före användarnas säkerhetsprogram. De skadliga programmen kan även göra säkerhetsprogrammen funktionsodugliga och gömma sig med hjälp av s.k. rootkit-teknik.

De skadliga mobilprogrammen ledde inte till några allvarigare informations säkerhetsproblem år 2005. De skadliga programmen kan sprida sig med hjälp av *bluetooth-radiovågor*, som har kort räckvidd, och via *multimediameddelanden*. Den epidemiska spridningen av skadliga mobilprogram stävjas dock av att installationen fordrar att telefonanvändaren godkänner en installationsförfrågan. Spridningen med hjälp av Bluetooth är effektivast i folksamlingar, vilket framkom bland annat



30.1.2006

CERT-FI

under friidrotts-VM i Helsingfors i augusti. CERT-FI fick information om ett tjugotal infektioner under evenemanget.

Phishing-bedrägerierna till Finland

Utbredningen av phishing-fenomenet från den engelskspråkiga världen till de mindre språkområdena förutspåddes i CERT-FI:s rapport 3/2005, efter att bedrägerierna hade spritt sig till det tyska språkområdet. Under det sista kvartalet år 2005 spred sig fenomenet till de nordiska länderna.

Den första phishing-attacken mot finländska nätbankskunder gjordes i slutet av oktober. Under perioden november-december gjordes ytterligare tre liknande attacker. I den första attacken användes engelskspråkiga skräppostmeddelanden, men språket övergick senare till stel finska. Antalet meddelanden per attack har uppskattats till minst 500 000. De sidor som användes för insamling av användarnamn var fördelade på angripna www-servrar runt om i världen. Hittills har finländska banker och företag som hanterar uppgifter om betalningsmedel via Internet inte blivit utsatta för phishing i någon större omfattning.

Riktade attacker

Antalet till CERT-FI rapporterade dataintrång hos finländska företag ökade inte ifjol. Vid informationsinhämtningen användes oftare skadliga program som skraddarsyttts för objektet än under tidigare år. Programmen skickades till målorganisationerna som filbilagor till e-postmeddelanden. Ett annat sätt att få tillgång till terminaler i en enskild organisations interna nät var att locka användaren att besöka en viss webbsida. Det skadliga programmet, som installerades i måldatorn från webbsidan, utnyttjade terminalens sårbarhet.

Runt om i världen rapporterades, liksom under tidigare år, många dataintrång, vid vilka bedragarna kom över ett stort antal kreditkortsnummer, användarnamn och andra personliga uppgifter, däribland finländska. Uppgifterna inhämtades genom att lura användarna att uppge dem, stjäla dem med hjälp av spionprogram och genom att göra intrång i näthandlars och betalningsförmedlars databaser.

De denial of service-attacker som riktade sig mot finländska organisationer och som CERT-FI fick kännedom om, gällde främst www- och irc-tjänster. I jämförelse med den globala situationen, har antalet attacker och problemets omfattningen samt de därmed förbundna skadorna varit relativt ringa i Finland.

I slutet av året observerade man tecken på en global denial of service-attack, som utnyttjade öppenheten i DNS-servrar för namnutredning samt det bristande skyddet hos bredbandsnät ifråga om falska adresser. Trots att attacken inte primärt riktade sig mot Finland, användes flera finländska namnservrar för förstärkning av attacken. Vid attacken utnyttjades den sårbarhet hos DNS-system som rapporterades redan för fem år sedan, men fortfarande är aktuell. CERT-FI och teleföretagen gav information och skyddsanvisningar till upprätthållarna av namnservrar.

Fel och störningar

De viktigaste felsituationerna i kommunikationsnät avsedda för förmedling av tal gällde kommunikationsavbrott i glesbygdens osäkrade stamnät och avbrott till följd av lokala, väderrelaterade längre strömvabrott.

30.1.2006

CERT-FI

Störningarna i IP-baserade stamnät med hög kapacitet ledde speciellt i januari och februari till kommunikationsavbrott med stor geografisk spridning. Effekterna gällde framförallt datatrafiken. Störningarna berodde i allmänhet på felaktig nätspecifikation, programfel eller samverkan mellan dessa till följd av ändringsarbeten. Allvarliga störningar i datatrafiken till följd av apparatfel rapporterades också.

Framtidsutsikter

De kränkningar av informationssäkerheten som riktar sig mot användaren snarare än datorn, har fortgått under innevarande år. Bedragarnas meddelanden blir allt mer övertygande. Bedrägerierna har inte hittills förutsatt någon speciellt avancerad teknik. Den för snabbade internationella betalningstrafiken och den ökade användningen av elektroniska fakturor uppmuntrar till missbruk av datateknisk natur. Vid sidan av banktjänsterna är även andra elektroniska kundtjänster, som omfattar hantering av betalningsmedelsuppgifter och annan ekonomiskt användbar information, bedrägerikänsliga.

För att försvåra brottsutredningen kommer de systematiska attackerna även framöver främst att göras via datasystem utanför Finlands gränser. CERT-FI fortsätter att utvidga sina redan omfattande nationella och internationella samarbetsnätverk.

Den kraftiga ökningen av antalet bredbandsförbindelser accentuerar betydelsen av automatiserade informationssäkerhetsprocesser i nätadministrationen. Eftersom dagens informationssäkerhetsrisker allt oftare gäller slutanvändaren, är det viktigt att informera kunden om skyddsåtgärderna redan innan datatjänsten levereras.

De nya operativsystemens begränsningar av användarrätten och deras övriga, färdigt installerade informationssäkerhetsegenskaper gör dem tryggare att använda. De skadliga programmen kommer förmodligen att vara inriktade på att lura användarna och att utnyttja programsårbarheter i datatrafikskyddet. Bland annat serverprogram, program för snabbkommunikation, fildelningsprogram och P2P-program är applikationer som kan utnyttjas. För att försvåra användningen av skadliga bot-program, borde den utgående trafiken från datasystem begränsas. Detta skulle även öka möjligheterna att upptäcka skadliga program.

I slutet av året utfärdade Kommunikationsverket en föreskrift om Internet-förbindelsetjänsternas informationssäkerhet och funktionsduglighet (13/2005). Föreskriften och den därmed förbundna rekommendationen förtydligar Internet-tjänsteleverantörernas rättigheter och skyldigheter ifråga om informationssäkerheten hos de levererade tjänsterna. Föreskriften, som omfattar den bästa praxisen ifråga om nättrygghet, fäster särskild uppmärksamhet vid informationssäkerheten i samband med anslutningsleveranser. Föreskriften kompletterar den tidigare utfärdade föreskriften om e-posttjänsternas informationssäkerhet och funktionsduglighet (11/2004). Syftet med regleringen är att säkra att informationssäkerheten hos de finländska kommunikationstjänsterna även framöver är av högsta internationella klass.