



4.7.2006



Lägesrapport 2/2006

De sårbarheter i webbläsarprogramvaror som upptäcktes i slutet av förra kvartalet utnyttjades även under andra kvartalet. Korrigeringar för sårbarheterna i Internet Explorer-webbläsaren publicerades i mitten av april. Sårbarheterna i webbläsarprogram var fortfarande ett allmänt använt sätt att angripa datasystem.

CERT-FI fick många rapporter om servrar som hade blivit angripna i finländska nät och användes för bedrägeriförsök (phishing). Antalet bedrägerier har nödvändigtvis inte ökat men företag som blivit utsatta för phishing har börjat rapportera fallen mera aktivt än tidigare.

Serien av phishing-bedrägerier som riktade sig mot Nordeas finländska nätbankskunder fortsatte i början av april. Andra bedrägeriförsök som skulle ha riktat sig mot finländska nätbankskunder rapporterades inte under andra kvartalet.

Sårbarheter i programvaror

I slutet av förra granskningsperioden upptäcktes fyra sårbarheter i Internet Explorer-webbläsaren. En av dessa utnyttjades omedelbart genom att placera skadlig programkod på hundratals webbplatser. Microsoft publicerade en korrigeringsuppdatering för sårbarheterna den 11 april 2006. Under andra kvartalet korrigerade Microsoft även flera andra sårbarheter i Internet Explorer-webbläsaren och sårbarheter i Windows-operativsystemet och Office-programvaror. Vid publiceringen av denna lägesrapport hade alla upptäckta Office-sårbarheter ännu inte korrigerats och de utnyttjades fortfarande.

Under granskningsperioden upptäcktes flera sårbarheter som kan klassificeras som kritiska i många databasprogramvaror. Korrigeringsuppdateringar publicerades för flera programvaror som allmänt används. Sårbarheterna i databasprogramvaror kan möjliggöra tillgången till system som innehåller känslig information.

Apple publicerade flera viktiga uppdateringar för Mac OS X-operativsystemet för att förbättra dess informationssäkerhet. De mest betydande sårbarheterna som korrigerades gör det möjligt för attackeraren att köra sin egen programkod på det sårbara datasystemet. Sårbarheter letas aktivt efter också i andra operativsystem än bara Windows, och det är sannolikt att de också kommer att utnyttjas alltmer.

I Mozilla-programvaror, som t.ex. webbläsaren Firefox och e-postprogrammet Thunderbird, upptäcktes flera sårbarheter, många av vilka var allvarliga. För programvarorna publicerades också korrigeringar.

I e-postprogrammet Sendmail upptäcktes en sårbarhet som berör behandlingen av signalering, och den utgjorde ett allvarligt hot mot informationssäkerheten i e-postprogram. Det är dock tekniskt så svårt att utnyttja sårbarheten att något attacksverktyg inte har kommit ut. Även de komponenter i e-postserverprogrammet Microsoft Exchange som behandlar iCal och vCal-kalenderuppgifter visade sig vara sårbara.



4.7.2006

CERT-FI

Det upptäcktes ett avsevärt antal sårbarheter som berör behandlingen av olika bildformat. Korrigeringar publicerades för de WMF-sårbarheter i äldre Windows-versioner som upptäcktes i början av året.

Phishing-bedrägerier

CERT-FI fick flera rapporter om angripna servrar i finländska nät som användes för bedrägeriförsök (phishing). Bedrägerierna som använde finländska servrar har riktat sig mot användare av utländska nättjänster.

Gemensamt för de undersökta bedrägerifallen har varit att webbplatserna som har använts för bedrägerierna har grundats genom att angripa servrar med installerad Horde-service. Horde är en serverprogramvara med vilken det är möjligt att bygga en e-posttjänst som används med en webbläsare. Även nättjänster som har förverkligats med PHP-skriptspråket har fortfarande varit populära föremål för attacker mot informationssäkerhet. Enligt CERT-FI:s iakttagelser är brist på regelbundet upprätthållande och uppdateringsrutiner det största problemet för många tillämpningar som används med webbservrar, för då blir de lätta mål för attackerare.

I början av granskningsperioden utsattes Nordeas finländska nätbankskunder för en ny phishing-bedrägerikampanj. I bedrägeriförsöket användes igen engelskspråkiga skräppostmeddelanden. Även Nordeas kunder i Sverige utsattes för en phishing-bedrägerikampanj i början av maj. I den här attacken var skräppostmeddelanden skrivna på dålig svenska. På basis av olikheter i handlingssätten är bedragarna nödvändigtvis inte samma.

Skadliga botnet-program

Under granskningsperioden upptäcktes allt oftare skadliga program som använde något annat än IRC-protokollet, t.ex. P2P-baserad kommunikation. Med hjälp av Peer-to-Peer-protokollet är det möjligt att förebygga att nätverket går sönder vid avstängning av kommandoservrar. Allt oftare upptäcktes även skadliga program som använde ett modifierat IRC-protokoll.

Skadliga program används fortfarande för att få ekonomisk nytta. Information samlas in på ett professionellare sätt än tidigare och antalet insamlad information har ökat. För att inte bli upptäckta är skadliga program nödvändigtvis inte i beständig kontakt med sin server utan överför information dit som impulser, och då är det möjligt att användaren inte upptäcker överföringen.

Riktade attacker

I slutet av maj blev sårbarheten i Microsoft Word-programvaran stor nyhet, och korrigeringsuppdateringen för den kom ut först den 13 juni 2006. Sårbarheten utnyttjades i attacker mot enskilda företag och organisationer. CERT-FI känner emellertid inte till några attacker mot finländska organisationer där den här sårbarheten skulle ha utnyttjats.

Framtidsutsikter

Flera CERT-aktörer har rapporterat att antalet anmälda fall har minskat, vilket kan betyda att andelen riktade attacker har ökat. Det är allt svårare att försvara sig mot attacker och upptäcka dem. Attackerna är planerade att kringgå organisationers vanligaste försvarsmekanismer, som t.ex. antivirusprogram och brandväggar. Med hjälp av uppgifter som på förhand samlats in om föremålet är det möjligt att skapa trovärdigare e-postmeddelanden för att förverkliga de riktade attackerna.



4.7.2006

CERT-FI

Samtidigt som identifieringsmetoder utvecklas försöker attackerare kapa innehållet i användarens förbindelse istället för användaridentifikationen. Ett exempel på detta är skadliga program som installerar sig som proxy-servrar och försöker kapa webbankskoder och annan känslig information som överförs under förbindelsen.