

CERT-FI INFORMATIONSSÄKERHETSÖVERSIKT

9.7.2008

CERT-FI informationssäkerhetsöversikt 2/2008

WWW-tjänsternas informationssäkerhet och tillgänglighet har satts på prov på många sätt. Intrång har gjorts på sidorna och osakligt material har matats in. De angripna sidorna har använts för att sprida skadliga program och sidornas innehåll har ändrats. Genom att utnyttja cross site scripting sårbarheter är det möjligt att vilseleda användare av många www-sidor. Man har också försökt överbelasta servrar för att göra dem oanvändbara.

Spridningen av skadliga program eller försök att få uppgifter om lösenord riktas till allt mer specifika målgrupper. I stället för att allmänt sprida falsk information blir det vanligare att rikta bedrägeriet mot en viss organisation eller begränsad användargrupp. Fenomenet har också diskuterats offentligt livligare än tidigare.

Snabbkommunikationsprogram har använts för spridning av skadliga program. Intressant formulerade meddelanden, som ser ut att komma från andra användare, har lockat användarna att ladda ner skadliga program.

Sårbarheter av typen SQL-injektion möjliggör en olovlig omarbetning av sidorna

Webbsidorna har till sin struktur blivit komplicerade och svåra att administrera. Det innehåll som syns åt användaren upprätthålls och bearbetas ofta med hjälp av databaser och CMS-system (Content Management System).

Om de uppgifter som matas in på webbsidorna inte kontrolleras eller om databasen inte har skyddats omsorgsfullt kan det vara möjligt att omarbeta materialet på sidorna eller i databasen. Det oönskade materialet matas in via webbplatsen med hjälp av anpassade SQL-kommandon. SQL är ett frågespråk för databasförfrågningar och administrering av innehållet i databasen.

Omarbetade sidor kan användas t.ex. till att styra användaren in på sådana sidor från vilka

en attackkod, som utnyttjar någon känd sårbarhet, laddas ner i webbläsaren. Det här är möjligt t.ex. genom att tillägga en del av en JavaScript-kod, som laddar ner det skadliga programmet från en annan server. Avsikten kan vara att användarens dator smittas med ett spionerande skadligt program eller fogas till ett botnät som en slavdator. De angripna sidorna kan också användas för att distribuera skadliga program eller programmets konfigurationsfiler.

Ett enklare sätt att dra nytta av webbsidors sårbarhet är att t.ex. föra in politiskt material, som man försöker påverka den allmänna opinionen med. I Litauen genomfördes i slutet av juni en omfattande kampanj där en stor mängd webbsidor förvanskades.

Sårbarheter av typen SQL-injektion har hittats på ett otal webbsidor. Microsoft och OWASP har publicerat anvisningar och verktygsprogram, som gör det lättare att undvika SQL-injektion sårbarheterna i Windows-servermiljöer.

Cross site scripting sårbarheter finns fortfarande

I början av året började man söka sårbarheter av typen cross site scripting (XSS), och det har man fortsatt med. CERT-FI fick vetskap om flera finländska www-sidor som det med hjälp av användaren varit möjligt att mata in vilseledande innehåll på. XSS-sårbarheterna kan användas för att göra skämt eller förvanska sidorna med och också genom att vilseleda användaren för att samla lösenord som behövs i tjänsten. CERT-FI har förmedlat uppgifter om sårbarheterna till dem som upprätthåller tjänsterna, som i allmänhet har korrigerat sårbarheterna eller tillfälligt tagit den sårbara tjänsten ur bruk.

Effekten av blockeringsattackerna blev liten

I slutet av juni gjordes blockeringsattacker mot några populära finländska webbsidor, men effekten blev rätt liten. De attacker som gjordes mot medier väckte emellertid stort intresse och visade att de som upprätthåller tjänster också skall vara beredda på situationer med överbelastning, om man önskar undvika avbrott i tjänsterna.

Riktade attacker av skadliga program

CERT-FI har fått vetskap om fall där finländska organisationer har varit mål för attacker av skadliga program. Skadliga program har spritts som bilagor till e-postmeddelanden till en mycket begränsad och noggrant utvald mottagargrupp. En känd aktör har förfalskats till avsändare, och innehållet i meddelandena har varit trovärdiga och gällt organisationens normala verksamhet. En inbjudan till ett möte eller en konferens kan vara ett typiskt exempel på bilaga i ett skadligt program.

De skadliga program som utnyttjats vid riktade attacker är normalt en sådan version som antivirusprogrammen inte har känt igen då attacken har genomförts. Avsikten med programmen har varit att kunna administrera användarens dator på distans, och på det sättet skaffa information om organisationens verksamhet.

Man snokar reda på användarnamn och lösenord med e-postmeddelanden

Man har försökt samla in användarnamn och lösenord via e-postmeddelanden, där man bett mottagaren bekräfta sitt användarnamn respektive lösenord. Det speciella med meddelandena är att de inte har sänts till slumpmässigt valda adresser, utan koncentrerat till de utvalda organisationernas anställdas e-postadresser.

E-postserverna har tidvis blivit överbelastade på grund av skräppost

CERT-FI har fått vetskap om fall där e-postserverna tidvis har varit överbelastade på grund av felmeddelanden som servern returnerar. Överbelastning kan uppstå då förfalskade avsändaradresser, som hör till samma organisation eller e-posttjänsteleverantör, används vid omfattande skräppostkampanjer. Då en betydande del av de adresser som skräppost skickas till alltid är felaktiga, returneras en stor mängd meddelanden till den förfalskade avsändaradressen om att e-posten inte gått fram.

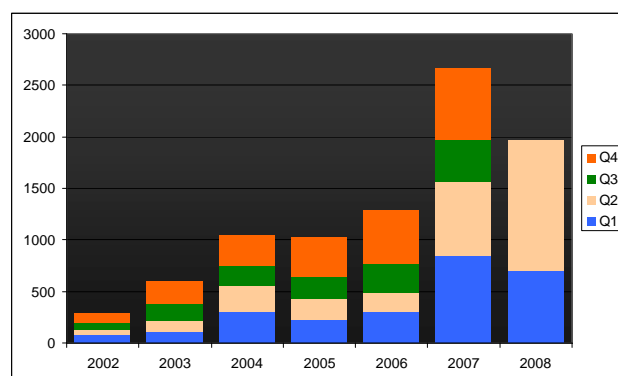
Det kan vara svårt att skilja detta från en blockeringsattack som riktas mot organisationen eller tjänsteleverantören, men å andra si-

dan kan en attack också genomföras indirekt. E-posttrafik som kommer till servern kan inte filtreras på basis av IP-adresser, ty förbindelserna kommer via e-postserverar, som också sänder sakliga meddelanden.

Också en enskild e-postadress kan utsättas för hård belastning, om adressen har förfalskats som avsändare vid en omfattande distribution av skräppost. I det fallet mottar användaren en stor mängd felmeddelanden. Emedan de felmeddelanden som sänds via serverna kanske lättare passerar skräppostfiltret kan man också försöka sända skräppost så att det verkliga målet för meddelandet de facto är den som får felmeddelandet.

Länkar till skadliga program spreds via messenger-snabbmeddelanden

Länkar till skadliga program har spritts via Windows Live Messenger-tjänsten. De spridda meddelandena har innehållit finskspråkig text som har lockat till att klicka på länkarna. Meddelandena ser ut att komma från användarna av tjänsten, men sänds i själva verket av ett skadligt program. Länkarna är formulerade så, att de ser ut att gälla en bildfil, men då man följer länken installeras ett skadligt program på datorn. Senare upptäcktes också i Norge skadliga program som sprids på motsvarande sätt.



I CERT-FI:s system för hantering av incidenter registrerades 1961 stycken ombesörjda kontakter under första halvåret.

Sårbarheter i programvaror publicerades på ett välavvägt sätt

Det är praxis att skapa nya program så att man sätter ihop dem bit för bit, och utnyttjar det man tidigare byggt upp. Programmen består ju av dels nya och dels av gamla delar, samt dels av gratisprogram som fritt får utnyttjas eller delar skaffade från andra tillverkare.

Omfattande program är väldigt invecklade, och det är utmanande att övervaka kvaliteten. I praktiken innehåller alla program fel. Sådana fel, som kan äventyra programmets informationssäkerhet, klassificeras som sårbarheter. Senaste år publicerades ca 8000 sårbarheter. Under första halvåret 2008 har CERT-FI publicerat 79 meddelanden om sådana sårbarheter som anses vara av betydelse.

CERT-FI meddelar om sårbarheter och deltar också i koordineringen av hur dessa skall kor-

rigeras. Man definierar programmen eller komponenterna och skapar kontakten mellan den som upptäckt sårbarheten och tillverkaren. Det är viktigt för CERT-FI att sårbarheten blir allmänt känd först då man har en lösning på problemet. Koordineringsprocesserna kan därför dra ut på tiden.

Codonomicon Oy upptäckte sårbarheter i de vanliga krypteringsprogrammen OpenSSL och GnuTLS, och uppgifterna publicerades i maj. De SSL- och TLS-protokoll som programmen erbjuder används för att kryptera de protokoll (t.ex. HTTP) som används på en högre nivå mellan kunden och servern.

Källkoden för sårbara program är avgiftsfri, och många produkter använder koden för att kryptera dataöverföring. I samband med koordineringen tog man också kontakt med andra programtillverkare, och flera Linux-distributörer publicerade korrigeringar till sårbarheterna.

CERT-FI kontakter	1-3/2008	4-6/2008	Totalt	1-6/2007
Intervju	17	29	46	44
Sårbarhet eller hot	39	232	271	24
Skadligt program	460	727	1187	1067
Rådgivning	64	87	151	177
Beredning av attack	32	27	59	3
Dataintrång	14	88	102	27
Blockeringsattack	15	26	41	41
Övrigt informationssäkerhetsproblem	10	11	21	21
Social ingenjörskonst	47	36	83	141
Totalt	698	1263	1961	1545

Antalet incidenter CERT-FI har behandlat har ökat med en fjärdedel jämfört med senaste år. Speciellt har meddelandena om sårbarheter i program och www-servrar, attackförberedelser samt genomförda attacker mot datasystem ökat i antal sedan senaste år.