

27.12.2007

CERT-FI

CERT-FI ÅRSRAPPORT 2007

Identitetjuvar är intresserade av en om användare av elektroniska tjänster. I undersökningar av skadliga program och missbruk har man hittat stora mängder lagrade användaruppgifter. CERT-FI har dock inte hört att de finländska användarnas uppgifter skulle ha lagrats i en alarmerande grad.

Elektroniska tjänster som tillhandahålls på nätet kan vara utsatta för missbruk på många olika sätt. Själva tjänsten kan lamslås lätt genom att styra tillräckligt mycket nättrafik till servern. En sårbar server kan utnyttjas för att sprida skadliga program, upprätthålla bluffsidor eller ta över användaruppgifter som sparats på servern.

Skadliga program har upptäckts i finländska nät i något mindre grad trots att bredbandsanslutningarnas antal fortsätter att öka. Samarbete med de inhemska tjänsteleverantörerna har medfört att man snabbt har kunnat reagera på de upptäckta problemen.

Blockeringsattacker väckte stort intresse

I februari gjordes en blockeringsattack mot internets rotnamnserverar. Attacken, som varade ungefär ett dygn, utfördes med hjälp av ett botnät, dvs. nätverk av angripna datorer. Belastningen var stor men inverkningarna blev små därför att största delen av de logiska rotnamnserverarna behöll sin funktion. De finländska användarna såg enbart att deras internetanvändning blev något långsammare. En del av serverarna som blev attackerade svarar också för vissa nationella domännamns namnservice där det också fanns svårigheter i funktionen. Attackerna påverkade inte fi-domännamn och deras funktion.

Samtidigt blev CERT-FI informerad om två omfattande blockeringsattacker som till att förstärka attacken utnyttjade namnservrar som hade alltför öppna inställningar. Attackerna utnyttjade även finländska namnservrar. Kommunikationsverket tog kontakt med aktörer som upprätthåller dessa servrar och uppmanade dem att ändra servrarnas inställningar så att något utnyttjande inte längre var möjligt.

Efter det att ett bråk kring en bronsstaty bröt ut i Estland i slutet av april försökte attackerarna lamslå estländska myndigheters webbtjänster med allt starkare blockeringsattacker. Dessutom utsattes åtminstone betalningsförmedlingssystemen och nyhetstjänsterna för attacker som pågick i flera veckor.

Efter avmattning i attackerna i Estland rapporterades det om attacker mot finländska tjänster. Under en attack mot Rundradions www-server fungerade webbsidorna långsamt och tidvis inte alls. I attacken styrdes P2P-fildelningsprogramms kontakter för att belasta servern. Enligt CERT-FI:s uppgifter hade attacken inte samband med händelserna i Estland. Också andra www-serverar och e-postserverar blev utsatta för attacker som dock var mindre kraftiga. I september blev Kommunikationsverkets och CERT-FI:s www-sidor föremål för attacker. Också en stor mängd skräppost har ibland orsakat att meddelandeförmedling blivit något långsammare.

27.12.2007

CERT-FI

Attackerna fick mycket publicitet och därför drogs fel slutsatser även när det gällde vanliga driftavbrott, eftersom tjänsterna och deras funktion var under exceptionellt noggrann tillsyn. Majoriteten av de fall som rapporterades till CERT-FI visade sig dock inte vara blockeringsattacker. Attackerna ledde till livlig diskussion om de elektroniska tjänsternas funktionssäkerhet i fall det förekommer attacker.

Många sätt att samla in användaruppgifter

De som gör skadliga program och bluffsidor är mycket intresserade av användaruppgifter som behövs för elektroniska tjänster. Skadliga program avlyssnar webbläsarförbindelser och samlar in uppgifter med hjälp av bluffsidor. Dessutom kan de sända uppgifter som matats in på webblanketter till insamlingsservrar från vilka de senare hämtas för eventuellt utnyttjande. CERT-FI har under året fått anmälningar också om finländska användarnas uppgifter som på så sätt har hamnat i obehöriga händer. Finländarnas andel av alla hittade uppgifter har än så länge varit liten, några tiotals fall.

Skadliga program kan samla in koder, lösenord och andra identifieringsuppgifter och dessutom kan de under en förbindelse ändra uppgifter som användaren matat in och sett med hjälp av webbläsaren. Programmet kan exempelvis under nätbanksförbindelsen girera pengar till ett på förhand definierat konto utan att användaren märker detta. Än så länge har CERT-FI inte fått höra om sådana skadliga program som kapar sessioner i finländska tjänster. Ett av fallen som CERT-FI har analyserat innehöll dock uppgifter som hänvisar till Finland. Ett skadligt program som kapar en nätbankssession överför pengar från den angripna datoranvändarens konto utan att någon märker det. Efter det försöker man störa spåren med hjälp av mulor, dvs. bulvaner, som är kända i ekonomisk brottslighet.

I oktober spreds på www-sidorna och peer-to-peer-tjänsterna en fil som innehöll cirka 80 000 finländares användarnamn och lösenord eller hash för internets webbtjänster. Lösenorden hade skaffats genom att utnyttja sårbarheter i programvarukomponenter som de som upprätthåller www-tjänster själv hade utvecklat eller som tredje parter hade producerat.

Fallet framförde brister i många webbtjänsters informationssäkerhet. I en del av tjänsterna hade lösenorden sparats på servern i form av vanliga ord eller med svagt skydd. Webbtjänster erbjuds inte bara av företag utan också av andra intresserade som inte alltid har tillräcklig kännedom om hur systemen och programvaran underhålls på ett informationssäkert sätt. Det upptäcks hela tiden sårbarheter i programvaran som används i tjänsterna. Användarnas handlingsätt var också bristfälligt. Om man till exempel använder ett och samma lösenord för olika tjänster, betyder det att när lösenordet för en av tjänsterna avslöjas kan användarens uppgifter samlas in från andra tjänster med samma lösenord. Genom att kombinera uppgifter från olika tjänster kan användarens integritetsskydd äventyras. Det är också möjligt att någon uppträder i en annan persons namn i olika tjänster.

27.12.2007

CERT-FI

Botnät är fortfarande grundverktyget för skadliga åtgärder

Nätverk av angripna datorer, botnät, används fortfarande för skadlig verksamhet av olika slag. Det är till exempel möjligt att sända skräppost eller utföra blockeringsattacker med dem.

Det skadliga programmet Storm Worm upptäcktes första gången i januari 2007 och det sprids via bilagor till e-post och via www-sidor. Under sommaren och hösten spreds många skräppostmeddelanden som innehöll en länk till en webbplats som sprider Storm Worm. När Storm Worm smittar en dator installerar det samtidigt en rootkit-funktion som gör att användarna och antivirusprogrammen inte lätt upptäcker det. Därför är det också svårt att rensa datorn. Storm Worm är för tillfället ett av de mest spridda skadliga programmen.

Infekterade datorer blir en del av ett väldigt omfattande nätverk av Storm Worm-botnät. Nätverket, som de angripna datorerna bildar, får sina kommandon genom en effektivt decentraliserad mekanism som liknar peer-to-peer-nät, utan någon enskild och centraliserad kommandoserver. Då blir det svårare att undersöka nätets funktion och uppbyggnad. Som en motåtgärd kan ett botnät också starta en blockeringsattack för att skydda sig från undersökningen. Hur avgörande Storm Worm var för de finländska användarna kunde ännu inte ses i början av året men CERT-FI har inte hört att det skulle finnas något större antal smittade datorer i finländska nät. Det är dock möjligt att botnätet senare har utnyttjats vid attacker mot finländska föremål.

Sårbarheter i programvaran medför missbruk

Kampanjer för publicering av sårbarheter som pågick i slutet av förra året och i början av detta år började falna av. Fortfarande hittades dock många sårbarheter i mjukvara som hänför sig till operativsystemets komponenter, kontorsprogram och läsarprogram och gäller en stor mängd användare av arbetsstationer. De utnyttjas oftast även för spridning av skadliga program och för kapning av datorer i syfte att få dem fungera som slavdatorer för botnät.

För servrar är det värt att i synnerhet notera sårbarheterna i programmeringsspråket PHP och publikationssystem som genomförts med PHP, för de kan möjliggöra olovlig bearbetning av www-sidorna. Angripna www-servrar används generellt för spridning av skadliga program och bluffsidor utan att den som upprätthåller servern själv märker det. Sårbarheter hittades också i programvaran för routrar som internetoperatörerna använder. Med dessa sårbarheter kunde det ha varit möjligt att störa nätets funktion. Enligt CERT-FI:s uppgifter har sårbarheterna dock inte utnyttjats. Tillverkaren har levererat uppdatering av programvaran till sina registrerade kunder.

Ofta strävar man efter att få ekonomisk nytta av sårbarheterna i mjukvaran. Uppgifter om sårbarheter har sålts offentligt åtminstone från år 2002, men under det gångna året har marknaden blivit livligare genom den schweiziska WabiSabiLabi-auktionsplatsen. Uppgifter om sårbarheter köps bl.a. av tillverkare av informationssäkerhetsprodukter som använder dem i sina egna produkter, vilket sedan utnyttjas i marknadsföringen. Generellt publiceras sårbarheterna inom en tid i samarbete med tillverkarna av den sårbara programvaran.

Saluförandet av sårbarheterna medför också problem. Tillverkarna av skadliga program kan få uppgifter om sårbarheter genom att analysera informationssäkerhetsprodukter i vilka de köpta uppgifterna används. Det finns ingen garanti för att personer som saluför sårbarheterna är tillförlitliga. Sårbarhetsuppgifterna är önskat och värdefullt material bland knäckare. Sårbarheter som ännu inte har publicerats kan utnyttjas särskilt i riktade attacker.

27.12.2007

CERT-FI

Webbsidor som sprider skadliga program oftast i vissa utländska nät

Serverar som sprider skadligt innehåll tycks vara kunder för samma nätoperatörer eller serverhotell. En del av internetoperatörerna har spärrat trafiken till några av de mest illa beryktade webbadresserna. Man har i synnerhet protesterat offentligt mot gruppen Russian Business Network. Det ser ut att gruppen i slutet av året har försökt ändra de IP-adressrymder den använder.

Framtidsutsikter

CERT-FI publicerade så gott som 200 anmälningar om sårbarheter i mjukvara och sju varningar. Anmälningarna och varningarna har sedan början av året publicerats skilt för sig, och grunderna för publicering har förnyats. Dessutom publicerade CERT-FI över ett hundra artiklar om aktuella ärenden under Tietoturva Nyt!

Sårbarheterna i programvara har fortfarande en stor betydelse. Sårbarheter hittas även i mera stängda omgivningar, så som i tillämpningar inom industrin. System, som planerats utan att beakta möjligheten till spridning av skadliga program, kan vara mycket sårbara.

Under året har CERT-FI sysslat med många mindre sårbarhetsfall och dessutom med ett stort koordineringsprojekt som påverkar flera tillverkares produkter. Resultaten förväntas vara färdiga för publicering i början av 2008.

Sårbarheter som inte rättats till eller publicerats kan utnyttjas i riktade attacker där ett skräddarsytt skadligt program enbart sprids till ett utvalt föremål. Syftet kan till exempel vara att skaffa information om målorganisationen.

E-post används fortfarande för att sprida skadliga program. Det kan ske med bilagor till e-postmeddelanden eller med länkar som lockar oförsiktiga användare att klicka sig till www-sidor som utnyttjar kända sårbarheter.

Skadliga program utvecklas tekniskt hela tiden och de medför nya utmaningar. Det blir allt svårare att undersöka hur nya typer av botnät fungerar på grund av deras decentraliserade styrsystem. Elektroniska tjänster är fortfarande relativt utsatta för blockeringsattacker som görs antingen med botnät eller med peer-to-peer-nät. Det är inte alls omöjligt att skadliga program som avlyssnar eller kapar webbläsarförbindelser utvidgar sitt urval av tjänster för att även omfatta finländska webbplatser. Informationssäkerhetsaspekter som redan är kända hos datorer måste även beaktas vid användning av mobiltelefoner.

Samtidigt som bredbandsanslutningarnas antal fortsätter att öka, ser det ut som om skadliga program i finländska nät hittas i något mindre grad. Den gynnsamma utvecklingen har påverkats av smidigt samarbete bland teleföretagen, informationssäkerhetsbolagen och informationssäkerhetsmyndigheterna samt av nationell lagstiftning och föreskrifter om informationssäkerheten. Den finländska modellen är en förebild i internationella sammanhang, t.ex. inom EU.