Luku IV: Haittaohjelmat

Tässä luvussa käsitellään

- viruksia,
- sisäisiä hyökkäyksiä,
- Troijan hevosia, matoja, murtopakkeja, botnetteja,
- yksityisyyden suojaa murtavia ohjelmia ja
- vastatoimenpiteitä.

Virukset I

Tietokonevirus on ohjelmakoodia, joka pystyy kopioimaan ja levittämään itseään uusiin kohteisiin. Tietokonevirus tarvitsee leviäkseen ja aktivoituakseen aputiedoston samalla tavoin kuin biologinen virus tarvitsee avukseen isäntäsolun.
Virukset voidaan jakaa niiden tartuttamien kohteiden perusteella neljään päätyyppiin:

- tiedostovirukset,
- makrovirukset,
- komentojonovirukset ja
- käynnistyslohkovirukset.

- Virus voi kuulua samalla useampaan kuin yhteen edellä mainituista tyypeistä. Tiedostovirukset tarttuvat suorituskelpoisiin ohjelmatiedostoihin, joista tyypillisimpiä ovat Windows-käyttöjärjestelmässä .com, .pdf ja .scr-päätteiset tiedostot.
- Leviäminen tapahtuu aina kun saastunut ohjelma suoritetaan koneen muistissa. Tiedostovirukset voivat levitä kaikilla tiedonsiirtotavoilla, joilla siirretään ohjelmatiedostoja.
- Makrovirukset on ohjelmoitu toimisto-ohjelmissa käytettävien makrokielten avulla. Makrovirusten leviäminen tapahtuu dokumenttien mukana ja ne saatetaan suorittaa automaattisesti kun dokumentti avataan toimisto-ohjelmassa.
- Makrovirukset voivat levitä käyttöjärjestelmästä riippumatta, mikäli käytössä on sama toimisto-ohjelma. Toimisto-ohjelmiin on lisätty sisäänrakennettuja ominaisuuksia, joilla makrojen tahatonta suorittamista pyritään estämään.

- Komentojonovirukset on tehty käyttäen hyväksi kohdejärjestelmän tarjoamia komentikieliä. Esimerkiksi Windowsin Visual Basic Scripting on ollut suosittu tähän tarkoitukseen. Komentojonoja pystytään luomaan tavallisella tekstieditorilla.
- Käynnistyslohkovirukset tarttuvat tietovälineen, kuten kiintolevyn tai USB-muistin käynnistyslohkoon, josta tietokone etsii käynnistykseen tarvittavia tietoja. Virus voi tarttua ulkoiselta laitteelta kiintolevyn käynnistyslohkolle ja tämän jälkeen saastuttaa tietokoneessa käytettvät muut suojaamattomat muistilaitteet. Käynnistyslohkovirukset leviävät hitaasti, koska ne siirtyvät käytännössä vain muistilaitteelta toiselle. Ne ovatkin nykyään harvinaisia.

Virusten muita luokitteluja I

Viruksia voidaan luokitella myös muiden kriteerioiden mukaan:

- TSR-virus (terminate and stay resident) on sellainen, joka pysyy aktiivisena muistissa sovelluksen päättymisen jälkeen.
- Häivevirus (stealth virus) on virus, joka kätkee saastuneen tiedoston. Nämä virukset sieppaavat tiedostoon liittyvät käyttöjärjestelmäkutsut. Jos kutsun tavoitteena on saada tiedostoattribuutit, tiedoston alkuperäiset attribuutit annetaan. Jos kutsu on tiedoston lukuoperaatio, tiedosto puhdistetaan ensin ja vasta sitten luovutetaan luettavaksi. Mutta jos kutsu on tiedoston suoritus, tiedosto annetaan sellaisenaan.

Virusten muita luokitteluja II

- Salattu virus on sellainen, jonka koodista suurin osa on salakirjoitettu. Vain purkamiseen tarkoitettu koodi on selväkielisenä. Varhaiset virustentorjuntaohjelmistot olivat vaikeuksissa tällaisten virusten kanssa. Ne voidaan paljastaa rakentamalla virtuaalikone, joka suorittaa koodin. Koodi purkaa salauksen ja sen jälkeen virus voidaan tunnistaa.
- Polymorfinen virus muuttaa muotoaan joka kerta, kun se tunkeutuu toiseen ohjelmaan. Tällaisten virusten tuottamista on automatisoitu. Esimerkiksi jo 1992 oli saatavilla Mutation Engine (MtE) ja Trident Polymorphic Engine (TPE).

Täydellisen virustorjunnan mahdottomuus I

- On todistettu, että täydellinen virustorjunta on mahdotonta. Toisin sanoen ei ole olemassa algoritmia, joka löytäisi tai paljastaisi kaikki virukset.
- Sen tähden virustentorjunta perustuu tunnettujen virusten etsimiseen. Tämäkin näyttää toimivan käytännössä hyvin. Lisäksi järjestelmien omat tietoturvaominaisuudet ovat parantuneet.
- Tietokone-lehden numerossa 1-2010 yritettiin tartuttaa tahallaan syksyllä 2009 liikkuneita viruksia Windows Vista -koneeseen. Käyttäjällä eli tässä tapauksessa tartuttajalla oli vain perusoikeudet.
- Tartuttaminen osoittautui yllättävän vaikeaksi, sillä Vistan oma Defender huomasi ja esti virusten toimintaa.

Täydellisen virustorjunnan mahdottomuus II

- Ja vaikka tartunta olisikin tapahtunut, Windows olisi helppo puhdistaa: kone käynnistetään admin-tunnuksella ja käyttäjähakemiston työtiedostot kopioidaan turvaan. Sen jälkeen käyttäjätili poistetaan ja tarvittaessa perustetaan uudelleen. Kone on jälleen puhdas. Ongelmia syntyy vasta, jos virus on päässyt koneeseen admin-oikeuksilla.

Sisäiset hyökkäykset I

Takaportit ovat salaisia piirteitä ohjelmassa, jotka sallivat käyttäjän tehdä toimenpiteitä, jotka eivät ole normaalisti mahdollisia. Kun ohjelmaa käytetään normaalilla tavalla, se käyttäytyy odotetusti. Mutta takaportin avaamisen jälkeen ohjelma tekee jotain odottamatonta, usein rikkoen samalla turvallisuusmäärittelyjä.

Takaportteja voidaan käyttää testaustarkoituksiin.Esimerkiksi jos ohjelmoija on tekemässä monimutkaista biometristä todennussysteemiä, voi olla järkevää, että hän voi myös ohittaa biometrisen tunnistuksen siltä varalta, ettei systeemi toimikaan vielä oikealla tavalla. Tällainen takaportti tulee kuitenkin poistaa, kun ohjelma on valmis.

Joskus saattaa tosin olla tarpeellista jättää takaportti valmiiseen ohjelmaan. Esimerkiksi biometriseen tunnistukseen perustuvaan kulunvalvontaan voidaan jättää takaportti hätätilanteita varten. Jos vaikka työntekijä on loukannut itsensä niin, ettei hän voi käyttää biometristä dataansa, esimerkiksi sormenjälkeänsä, ja hänen olisi päästävä ensiapuun

Sisäiset hyökkäykset II

pian, niin takaporttina voisi olla kertakäyttöinen salasana, jonka saisi puhelimitse valmistajalta.

Todelliset pahoihin tarkoituksiin suunnitellut takaportit voivat olla vaikeita löytää. Ohjelmoija voi esimerkiksi tehdä tahallaan ohjelmasta sellaisen, että puskurin ylivuoto on mahdollinen. Mikäli takapportti paljastuu, hän voi väittää, että virhe on tehty vahingossa.

Pääsiäismunat ovat harmittomia piirteitä, jotka aktivoituvat, kun salasana tai erikoinen syöte annetaan. Esimerkkejä ovat vanhoissa Unix-järjestelmissä oleva piirre, joka antoi hauskoja vastauksia komentoon "make love"ja Solitaire-peli Windows XP:ssä, joka antoi käyttäjän voittaa, jos painoi yhtäaikaa näppäimiä Shift, Alt ja 2. Myös joissakin dvd-elokuvissa on ollut pääsiäismunia, jotka aktivoituvat, kun kaukosäädintä painetaan erikoisilla tavoilla. Tällöin näytetään poistettuja kohtauksia yms.

Sisäiset hyökkäykset III

Looginen pommi on haittaohjelma, joka tekee haitallisia toimenpiteitä jonkin loogisen ehdon lauettua. Esimerkiksi ohjelmoija voi koodata palkkaohjelmaan piirteen, että ohjelma kaatuu, jos ohjelmoija ei ole saanut palkkaa kahteen kuukauteen. Toinen esimerkki on loogisen pommin ja takaportin yhdistelmä, jossa ohjelma romahtaa tiettynä päivänä, ellei ohjelmoijalle makseta ennen sitä jotain summaa. Mikäli maksu tulee, ohjelmoija estää romahduksen takaportin avulla. Kysymyksessä on siis kiristys.

Puolustautuminen sisäisiä hyökkäyksiä vastaan I

- Vältä tilanteita, että järjestelmässä on yksi haavoittuva kohta. Useamman kuin yhden ihmisen tulisi olla vastuussa varmistuskopioista tai valvoa kriittisia systeemeitä.
- Käytä koodinlukua. Eli ohjelmoijien tulisi lukea toistensa koodia rivi riviltä virheiden ja takaporttien löytämiseksi.
- Käytä arkistointi- ja raportointimenetelmiä. Ohjelmistotuotantoympäristöön kuuluvat tuotteet kuten automaattinen dokumentointi ja ohjelmistojen arkistointi paljastavat myös sisäisiä hyökkäyksiä.
- Rajoita valtuuksia. Käytä pienimmän oikeuden -periaatetta.
- Suojaa järjestelmät myös fyysisesti. Tärkeiden järjestelmien yhteydessä lukitse ovet, huolehdi varasähköstä ja suojaudu tulta ja vesivahinkoja vastaan.
- Seuraa työntekijöitä. Erityisesti seuraa tyytymättömiä ohjelmoijia.

Puolustautuminen sisäisiä hyökkäyksiä vastaan II

- Valvo ohjelmistojen asennusta. Asenna vain ohjelmia, jotka tulevat luotettavilta toimittajilta ja jotka on verifioitu.

Madot I

- Madot ovat haittaohjelmia, jotka kykenevät leviämään itsenäisesti ilman aputiedostoa. Madot voivat levitä nopeasti esimerkiksi sähköpostin avulla.
- Sähköpostimadot voivat olla liitetiedostoina tai osana itse viestiä. Liitetiedostoina leviävät madot vaativat yleensä aktivoituakseen, että käyttäjä avaa tiedoston. Eräät madot aktivoituvat tietyillä sähköpostiohjelmilla jo viestin esikatselutilassa. Aktivoiduttuaan sähköpostimato etsii kohdekoneesta sähköpostiosoitteita, joihin se voi lähettää itsensä edelleen.
- Verkkomadot leviävät tietokoneverkossa tarvitsematta sähköpostin tai tietokoneen käyttäjän apua. Ne käyttävät hyväkseen reaaliaikaista verkkoyhteyttä koneiden välillä. Verkkomatojen leviämiselle otollisia ovat jatkuvasti verkossa kiinni olevat, puutteellisesti ylläpidetyt palvelimet tai kotitietokoneet, joissa on madon leviämisen mahdollistavia paikaamattomia tietoturvahaavoittuvuuksia.

Madot II

- Eräs laji matoja ovat botnet-verkkoja rakentavat madot. Botnet-verkot ovat valloitetuista koneista koostuvia kokonaisuuksia, joita käytetään hajautettuihin palvelunestohyökkäyksiin, roskapostitukseen, verkkourkintaan, identitettivarkauksiin sekä lukuisiin muihin rikollisiin tarkoituksiin.
- Botnet-verkkojen rakenne on melko samanlaista kuin vertaisverkkojen. Storm-verkko on tunnetuin botnet-verkko.
- Erään tutkimuksen mukaan Storm oli vastuussa jopa yli viidenneksestä kaikesta roskapostista vuoden 2008 ensimmäisellä neljänneksellä. On myös arvoitu, että Storm koostui noin kahdesta miljoonasta koneesta vuonna 2008. Verkko katosi kokonaan syyskuussa 2008, mutta heräsi eloon uudistuneena Waledac-verkkona vuoden 2008 lopussa.
- Conficker (myös Downup, Downaup, Kido) on yksi suurimmista botnet-verkoista, joita on löydetty. Tartunnan saaneita koneita arvioitiin olevan 9-15 miljoonaa tammikuussa 2009.

Madot III

- Conficker kulkee dynaamisen linkkikirjaston (DLL) mukana, joten se ei voi asentua koneeseen ilman apua. Alun perin Conficker rupesi leviämään Windowsin eri versioissa olevan MS08-067 tietoturva-aukon kautta.
- On myös kaksi muuta tapaa, joilla se pyrkii leviämään. Ensimmäinen tapa on hyödyntää verkkoon kytkettyjen Windows-käyttöjärjestelmien avoimia levyjakoja. Toinen tapa levitä tapahtuu USB-muistitikkujen avulla. Kun muistitikku työnnetään koneen USB-porttiin, käynnistyy automaattisesti autorun-prosessi, joka lataa ja suorittaa haittakoodin.
- Confickerin käyttämä vertaisverkkoteknologia on osittain tuntematonta. Tämä johtuu siitä, että Confickerin ohjelmoijat ovat tarkoituksellisesti kirjoittaneet haittakoodista vaikeaselkoista.

Madot IV

- Conficker pyrkii myös sammuttamaan kaikki Windowsin tietoturvaominaisuudet. Esimerkiksi palautuspisteet (Windows Restore Points), Windows Update sekä sen yhteydessä hyödynnettävä tietoturvapäivitysten latausohjelma BITS (Background Intelligent Transfer Service) poistetaan käytöstä.
- Samalla Conficker lisää Windowsin rekisteriin rekisteriavaimet, jotka sallivat Confickerille tarpeellisen liikenteen palomuurin läpi. Confickerissä on myös sisäänrakennettu lista eri virustorjuntaohjelmistojen käynnistystiedostoista. Mikäli tartunnan saaneesta koneesta löytyy jokin listan ohjelmista, Conficker sammuttaa ja poistaa kyseisen ohjelman käytöstä.

Madot V

- Huolimatta siitä, että Conficker on ollut olemassa jo pitkään, ei ole keksitty tehokasta tapaa tuhota sitä keskitetysti. Myöskään viitteitä siitä, kuka Confickerin on alun perin luonut, ei ole saatu. Helmikuussa 2009 Microsoft yhteistyössä muutamien muiden teollisuuden alan yritysten kanssa ilmoitti antavansa $250 000 palkkion syyllisen jäljille johtavasta vihjeestä. Black Hat -hakkeriryhmä on vihjannut, että Confickerin rakentajat olisivat ukrainalaisia.

Troijalaiset I

- Troijalaiset ovat ohjelmia, jotka tekevät ohjelman käyttäjältä salassa jotain arvaamatonta. Troijalaiset leviävät jollain tapaa houkuttelevan tai hyödyllisen ohjelman mukana tai ovat osa itse ohjelmaa sisältäen dokumentoimattomia toimintoja. Troijalaisissa itsessään ei ole leviämismekanismia, vaan niitä käytetään tyypillisesti muun haittaohjelman haittakuormana.
- Troijalaiset voivat avata kohdekoneelle takaportin, jonka kautta luvaton tunkeutuja voi päästä murtautumaan tietokoneelle ja etähallitsemaan sitä jopa organisaation palomuurin läpi.
- Murrettua konetta voidaan käyttää roskapostitukseen, palvelunestohyökkäyksiin tai tietomurtoihin. Troijalaiset voivat myös kerätä ja lähettää verkossa eteenpäin salasanoja, sähköpostiosoitteita, näppäinpainalluksia tai tietoa kyseisestä tietokoneesta tai käyttäjän toimista, kuten vierailuista verkkosivuilla.

Murtopakit I

- Murtopakki (rootkit) on erityisen etevä salaamaan itsensä. Se muuttaa tavallisesti systeemifunktioita tai KJ:tä itseään estääkseen paljastumisen.
- Murtopakit käyttävät useita tekniikoita kätkekseen itsensä. Ne voivat toimia sekä normaalissa että etuoikeutetussa tilassa.
- Jotkut tavallisin oikeuksin toimivat murtopakit muuttavat systeemikirjastoja levyllä. Tämä on kylläkin helppo havaita ulkoisten eheystarkistusten avulla. Toiset murtopakit soluttavat haittakoodia normaalioikeuksin toimivan prosessin muistivaruuteen. Tämäkin voidaan havaita sellaisten torjuntaohjelmistojen avulla, jotka toimivat ytimessä.

Murtopakit II

- KJ:n ytimessä etuoikeutettuina toimivia murtopakkeja on vaikeampi havaita. Tällaiset pakit Windowsissa ladataan yleensä laiteajureina, koska laiteajurijärjestelmä sallii käyttäjien ladata mielivaltaista koodia ytimeen. Tämä piirre on hyödyllinen ylläpitäjille, mutta se on myös turvallisuusaukko.
- Linuxiin on suunniteltu myös murtopakkeja, tosin vähemmän kuin Windowsiin. Nämä ladataan ytimeen käyttäen Linuxin LKM:ää (Loadable Kernel Module), joka toimii samoin kuin Windowsin laiteajurijärjestelmä.
- Kun murtopakki on ytimessä, se voi käyttää useita tekniikoita salatakseen itsensä. Eräs menetelmä tunnetaan nimellä "function hooking". Tämä tarkoittaa menetelmää, jossa systeemifunktioita muutetaan niin, etteivät ne paljasta haittaohjelmaa. Esim. funktio, joka luetelee tiedostot, voidaan muuttaa sellaiseksi, ettei se näytä murtopakkitiedostoja.

Murtopakit III

- Toinen tekniikka on muuttaa KJ:n sisäisiä tietorakenteita. Esim. Windows pitää kirjaa ladatuista laiteajureista. Murtopakki voi muuttaa tätä kirjanpitoa siten, etti se näy listalla.
- Kun murtopakki on päässyt koneeseen, sen täytyy huolehtia, että se säilyy yli uudelleenkäynnistysten. Koska torjuntaohjelmat käyttävät Windowsin tietokantaa nimeltä Windows Registry etsiessään epäilyttäviä prosesseja, jotkut murtopakit muuttavat funktioita, jotkam listaavat rekisterin sisällön.

Murtopakkien havaitseminen I

- Tavallisessa moodissa toimivat murtopakit voidaan havaita tarkkailemalla tiedostojen muutoksia levyllä.
- Windowsissa tärkeät koodikirjastot on allekirjoitettu digitaalisesti, joten kaikki muutokset aiheuttavat sen, ettei allekirjoitusta voi verifioida.
- Eräs mahdollisuus on vielä laskea tiiviste tärkeimmistä komponenteista, kun systeemiä ei ole kytketty verkkoon ja kun systeemi on verkossa. Jos tiivisteet eroavat, murtopakki saattaa olla syyllinen.
- Ytimessä oleva murtopakkien torjuntaohjelmisto voi lisäksi havaita, jos koodia solutetaan systeemifunktioihin.
- Ytimessä olevia murtopakkeja on vaikeampi havaita. Useimmat torjuntaohjelmistot etsivät merkkejä function hooking -tekniikasta ym vastaaviasta tekniikoista. Torjuntaohjelmistot pitävät kirjaa ytimen osien allekirjoituksista havaitakseen, onko näihin tehty muutoksia.

Murtopakkien havaitseminen II

- Koska murtopakit toimivat etuoikeutettuina, ne voivat havaita torjuntaohjelmistot ja estää niiden toimintaa. Siten toisinaan tarvitaan varsin syvällistä offline-analyysiä, jolloin tutkitaan myös Windows registry ja käynnistystiedot.
- Yksinkertainen mutta voimakas menetelmä havaita murtopakkeja on tiedostojärjestelmän kaksinkertainen läpikäynti. Ensimmäinen suoritetaan korkean tason systeemifunktioilla, joita murtopakki on luultavasti muuttanut. Toinen läpikäynti tehdään matalan tason systeemiohjelmilla, jotka lukevat levyltä lohkoittain. Jos tulokset eroavat, murtopakki voi olla syyllinen. Toisaalta kehittynyt murtopakki voi saastuttaa molemmat systeemifunktiot.
- Koska havaitseminen ja poistaminen on niin vaikeaa, käyttäjiä neuvotaan usein formatoimaan levy ja sentamaan KJ ja ohjelmistot uudestaan.

Vakoilu- ja mainosohjelmat I

- Jotkut ilmaiset ja jopa maksullisetkin hyöty- tai apuohjelmat sisältävät vakoilukomponentteja, jotka keräävät ja lähettävät tietoa koneen käytöstä eteenpäin.
- Kerättävät tiedot voivat olla tietoja käyttäjän vierailemista www-sivuista tai jopa verkkopalvelujen salasanoja. Ohjelmat voivat pakottaa selaimen aloitussivun omalle sivulleen siten, että aloitussivua on vaikea muuttaa takaisin halautuksi sivuksi tai ne saattavat avata lukuisia mainosikkunoita selainta käytettäessä.
- Näistä vakoiluohjelmista saatetaan kertoa ohjelmaa ladattaessa tai ohjelman lisenssisopimuksessa. Koska joillekin vakoiluohjelmille saadaan asennettaessa käyttäjän suostumus, näitä ohjelmia ei välttämättä tunnisteta virustorjunta-ohjelmalla, vaan ne vaativat tähän tarkoitukseen kehitetyn oman torjuntaohjelmansa. Osa vakoiluohjelmista asentuu työasemalle salaa käyttäjän tietämättä ja lupia kysymättä.

Vakoilu- ja mainosohjelmat II

- Nykyään yleisiä ovat myös tietoturvaohjelmat, jotka ovat joko tehottomia tai suorastaan haitallisia. Osa ohjelmista on jopa suomenkielisiä ja niitä mainostetaan hyvämaineisilla www-sivuilla. Ne väittävät löytäneensä ongelmia, joiden korjaaminen vaatii maksullisen version asentamista. Muutama "turvaohjelma jopa lataa koneelle haittaohjelmia, jotka se sitten lupaa poistaa. Älä käytä koneen siivoamiseen muita kuin turvalliseksi todettuja apuohjelmia.
- Evästeet voivat olla hyödyllisiä, mutta niitä voidaan käyttää myös jäljittämiseen. Esimerkiksi ryhmä web-palvelimia voi sopia yhteisestä evästeestä, jolloin ne voivat seurata käyttäjän toimia. Samoin mainostoimisto voi kerätä evästeiden avulla tietoa kuluttajien käyttäytymisestä. Siten eväste voi toimia myös vakoiluohjelmana.

Huijausviestit, ketjukirjeet, pilailuohjelmat ja sosiaalinen hyväksikäyttö I

- Huijausviestit eivät ole ohjelmia, vaan sähköpostiviestejä, jotka leviävät hyväuskoisten käyttäjien lähettäminä. Näissä viesteissä saatetaan varoittaa vaarallisesta viruksesta ja kehottaa käyttäjää lähettämään viesti eteenpäin mahdollisimman monelle.
- Huijausviestien, samoin kuin ketjukirjeiden, välittämiseen kuluu sekä lähettäjän että vastaanottajan työaikaa. Pahimmillaan huijausviestit erehdyttävät käyttäjän toimimaan virheellisesti, kuten poistamaan käyttöjärjestelmälle tärkeitä tiedostoja viruksina. Huijausviesteihin kuuluvat myös viestit, joissa pyydetään lähettään esimerkiksi pankkitunnuksia.
- Internetistä on saatavana paljon erilaisia vitsi- ja pilailuohjelmia, joilla säikytellään tavallisia käyttäjiä. Ohjelmat voivat antaa kummallisia virheilmoituksia, olla alustavinaan käyttäjän kiintolevyä tai tuhoavinaan tiedostoja.

Huijausviestit, ketjukirjeet, pilailuohjelmat ja sosiaalinen hyväksikäyttö II

- Tietokoneen hiiren tai näytön toimintaa voidaan manipuloida siten, että ne vaikuttavat olevan rikki. Nämä ohjelmat eivät yleensä ole vihamielisiä, mutta niiden mukana voi levitä vaarallisia haittaohjelmia ja ne voivat kuluttaa henkilöresursseja laitteiden tarkastukseen.
- Monet menestykselliset hyökkäykset ovat perustuneet ihmisten harhauttamiseen muutenkin kuin tietokoneen käytössä. Esimerkiksi luottamuksellisia tietoja, vaikkapa salasanoja, voi kysellä johtotason henkilöksi tekeytyvä hyökkääjä.
- Salasanoja voi urkkia hiiviskelemällä toimistoissa ja tutkimalla muistilappuja. Myös kiikarointi vastapäisestä rakennuksesta voi paljastaa salasanoja ja käyttäjätunnuksia.
- Troijalaisia voidaan myös levittää kylvämällä saastutettuja muistitikkuja organisaation parkkipaikalle ja toivomalla, että joku henkilökunnasta olisi utelias ja tutkisi tikun sisältöä.

Haittaohjelmien torjunta I

VAHTI-sarjan julkaisussa 3/2004 on laajasti tarkasteltu haittaohjelmilta suojautumista. Seuraavassa muutamia tärkeimpiä kohtia:

- Virusten torjunta vaatii käytäntöjä monella eri tapaa:
  - Käytä organisaatiossa erilaisia järjestelmiä. Näin haittaohjelma ei saastuta kaikkia yhtäaikaa. Tästä aiheutuu kuitenkin lisätyötä ylläpitäjille.
  - Organisaatiolla tulisi olla koulutusohjelma, jossa valistetaan viruksista ja muista haittaohjelmista.
  - Säännölliset tiedotteet virusongelmista ovat tarpeellisia.
  - Älä koskaan siirrä koneeseesi tiedostoja epävarmoista lähteistä, ellei virustorjunta ole ajan tasalla.
  - Testaa uudet ohjelmat tai avoimet dokumentit erillisessä koneessa ja siirrä vasta sitten tuotantokäyttöön.
  - Huolehdi, etteivät asiaankuulumattomat pääse asentamaan koneille haittaohjelmia, erityisesti Troijan hevosia.

Haittaohjelmien torjunta II

- Käytä käyttöjärjestelmiä, joiden sisäänkirjautumiskäytännöt ja todentamiset ovat turvallisia.

- Haittaohjelmilta suojautuminen:
  - Virustentorjunta on tehokkainta, kun se tapahtuu automaattisesti. Toisaalta automaattiset menetelmät eivät huomaa uusia haittaohjelmia, joten torjuntaohjelmistojen päivitysten on oltava tiheää.
  - Työasemia voidaan monitoroida haittaohjelmien aiheuttamien systeemifunktioiden aktiviteetin havaitsemiseksi.
  - Jos käytetään vain kaupallisia ohjelmistoja, jotka asennetaan esim. CD:ltä, vältytään perinteisiltä viruksilta.
  - Vältä P2P-musiikki- ja videojakelusysteemeitä.
  - Kannettavan työaseman käynnistys on aina suojattava salasanalla. Se voidaan toteuttaa työasemassa olevalla nk. turvapaneelilla, kiintolevyn salakirjoitusohjelmaan kuuluvalla käynnistyssalasanalla tai BIOS-asetuksista löytyvällä koneen käynnistyssalasanalla. Vasta salasanan syöttäminen käynnistää tietokoneen käyttöjärjestelmän ja antaa käyttäjälle kirjautumisikkunan.

Haittaohjelmien torjunta III

- Jos kannettavan kiintolevyä ei ole salakirjoitettu, on se suojattava BIO-asetuksista löytyvällä kiintolevyn suojaussalasanalla. Menettely estää levyn käytön toisessa samanlaisessa koneessa.
- Työaseman käynnistys on sallittava vain kiintolevyltä. Jos tähän turva-asetukseen on jostain syystä tehtävä kevennyksiä, suositellaan käynnistysjärjestykseksi: kiintolevy, cd-rom, muut siirrettävät mediat (esim. USB).
- Kaikki BIOS-tason muutokset on suojattava muutoksilta salasanalla, jota ei saa antaa loppukäyttäjälle,
- Käytä Microsoftin Macro Virus Protection -ohjelmaa kaikissa Microsoftin sovelluksissa äläkä koskaan aja dokumentin makroja, jos niiden toiminta ei ole tiedossa.
- Päivitä käyttöjärjestelmät säännöllisesti.
- Käytä palomuureja.