Tietoturva

Sisällysluettelo

1. Palomuurit

1.1. Palomuurityypit

Palomuurityyppejä on kolme erilaista: pakettisuodattimet, yhteyssuodattimet ja sovellusyhdyskäytävät. [1] Pakettisuodattimet ovat kaikista yksinkertaisimpia ja nopeita, mutta niitä ei yleensä pidetä riittävän turvallisina. Pakettisuodattimet suodattavat IP-paketit pääsylistan (ACL) perusteella. Jos paketti ei ole erikseen sallittu, se ei pääse läpi. Yhteyssuodattimet toimivat muuten samalla tavalla, mutta ne myös seuraavat yhteyden tilaa ja pitävät kirjaa istunnosta. Suodatuspäätöksissä käytetään näitä tietoja ja läpi päästetään ainoastaan hyväksyttyyn istuntoon kuuluvat paketit. [2]

Sovellusyhdyskäytävätason palomuurit tarkistavat, onko liikenne protokollan mukaista ja vasta sen jälkeen lähettävät paketit eteenpäin. Sekä sisään että ulos lähtevät paketit tutkitaan ja tiedot liikenteestä tallennetaan lokeihin. Näitä pidetään yleensä turvallisina. [3]

1.2. Mitä vastaan palomuuri suojaa

Palomuuri estää ulkopuolisten pääsyn tietokoneelle verkkoyhteyksien kautta. Palomuuri suodattaa pois kaikki muut paitsi välttämättömät yhteydet, jotka käyttäjä sallii. Palomuuri siis valvoo sisäisen ja ulkoisen tietoverkon välistä liikennettä. Hyvässä palomuurissa kaikki tietoliikenne kulkee sen kautta.

1.3. Mitä vastaan palomuuri ei suojaa

Koska palomuuri valvoo ainoastaan verkkoyhteyksiä, siitä ei ole apua, jos tunkeutuja pääsee fyysisesti käyttämään suojattua tietokonetta tai sen lähiverkossa olevia tietokoneita. Myöskään sellaisille yhteyksille, jotka eivät kulje palomuurin kautta, palomuuri ei voi mitään. Salattuja yhteyksiä palomuuri ei kykene suodattamaan, koska se ei pysty lukemaan niistä suodattamiseen tarvittavia tietoja. Palomuuri on myös hyödytön, jos käyttäjä sallii kaiken liikenteen sen läpi.

2. Virusturvasta huolehtiminen

2.1. Virus- ja haittaohjelmien leviämismekanismeja

Tietokonevirus on haitallinen ohjelma, joka pystyy monistamaan itseään ja leviämään verkon kautta tietokoneesta toiseen. Virukset tarvitsevat isäntäohjelmiston, jonka mukana ne leviävät. [4] Tällainen isäntäohjelma on yleensä suoritettava .exe-tiedosto, joka kannattaa aina skannata ennen suorittamista virusten varalta.

Muita haittaohjelmia ovat troijalaiset ja madot. Troijalaiset naamioituvat hyödyllisiksi ohjelmiksi, joten käyttäjä asentaa ne tietoisesti tietokoneelleen. Nämä ohjelmat myös tekevät sitä, mitä niiltä odotetaan, mutta lisäksi ne tekevät muutakin käyttäjän tietämättä. Troijalanen voi esimerkiksi avata takaportin, jonka kautta tietokoneeseen voi tunkeutua ulkopuolinen.

Madot eivät tarvitse varsinaisia isäntäohjelmia levitäkseen. Madot hyödyntävät tietoturvareikiä, siksi on tärkeää päivittää käyttöjärjestelmää ja ohjelmia riittävän usein. Madot myös leviävät sähköpostin liitetiedostoina. Aktivoiduttuaan mato levittää itsensä eteenpäin hyödyntäen tietokoneelta löytyneitä uusia sähköpostiosoitteita. [5] Tältä voi suojautua poistamalla epäilyttävät sähköpostit avaamatta niitä.

2.2. Virusturvaohjelmiston asennus ja päivitys

Internetiin kytketystä tietokoneesta on löydyttävä vähintään palomuuri ja virustorjuntaohjelma. Näitä saa ilmaiseksikin verkosta yksityiskäyttöön. Oikeaa virustorjuntaohjelmaa valittaessa on tärkeää varmistua siitä, että ohjelmaa päivitetään yhä. Päivitys on tärkeää, sillä uusia viruksia leviää verkossa koko ajan, eikä virustorjuntaohjelma välttämättä pysty tunnistamaan viruksia, jotka on kirjoitettu edellisen päivityksen jälkeen. [6] Monet virusten tekijät testaavat viruksiaan yleisimmillä käytössä olevilla virustorjuntaohjelmilla ja suunnittelevat virukset niin, ettei niitä pysty löytämään. Palomuuria ei tarvitse päivittää yhtä usein, sillä palomuuri päästää läpi ainoastaan erikseen sallitut ohjelmat. Päivittäminen on käyttäjän kannalta yleensä helppoa: virustorjuntaohjelmat ilmoittavat, kun uusi versio on saatavilla ja sen asentaminen vaatii yleensä vain pari klikkausta.

3. Käyttöjärjestelmän asennus ja ylläpito

Käyttöjärjestelmän asennuksessa ensimmäinen vaihe on luonnollisesti asennettavan järjestelmän ja version valinta. Suosituimmat käyttöjärjestelmät ovat otollisimpia alustoja virusten ja muiden haittaohjelmien leviämisen kannalta.

Edes vanhaan tietokoneeseen ei tulisi asentaa käyttöjärjestelmäversiota, jonka tuen valmistaja on lopettanut, mikäli se aiotaan liittää tietoverkkoon. Vanhoissa versioissa on runsaasti tunnettuja tietoturva-aukkoja, joiden kautta haittaohjelmat pääsevät leviämään.

3.1. Tarpeettomat ohjelmat

Tietokoneen mukana tulevaan käyttöjärjestelmään on usein liitetty tietokoneen valmistajan omia ohjelmistoja, joista kaikkia käyttäjä ei välttämättä tarvitse. Kuten muidenkin ohjelmien kanssa, ylimääräisistä ohjelmista ei ole hyötyä, ne vievät levytilaa, ja voivat sisältää turvallisuusongelmia.

Järjestelmään voi myös asentua käyttäjän huolimattomuuden seurauksena automaattisesti ohjelmia Internetistä. Koska näiden ohjelmien asentumistapa on varsin epäilyttävä, kannattaa niihin suhtautua epäluuloisesti ja mieluiten poistaa ne.

3.2. Päivityksistä huolehtiminen

Käyttöjärjestelmän automaattiset päivitykset kannattaa kytkeä päälle asennuksen jälkeen. Useimmissa järjestelmissä tämä asetus onkin oletuksena päällä. Automaattistenkin päivitysten julkaisussa kestää usein varsin kauan turvalisuusaukon ilmenemisen jälkeen, joten täydellistä suojaa ne eivät tarjoa.

Käyttöjärjestelmän lisäksi myös joissakin sovellusohjelmissa on omia päivitystyökaluja. Näiden tarpeellisuuden voi harkita itse, lähinnä sen mukaan, onko ohjelma alttiina esimerkiksi Internetistä tulevien tiedostojen sisältämille viruksille.

Automaattisista päivityksistä voi olla myös haittaa esimerkiksi hitaita kännykkäyhteyksiä käytettäessä. Päivitysten lataus hidastaa muuta verkon käyttöä ja kasvattaa siirtomäärään perustuvaa laskua.

3.3. Milloin koneen uskaltaa liittää verkkoon

Ennen tietokoneen liittämistä vieraaseen verkkoon kannattaa varmistua palomuurin toiminnasta, ja siitä, että tarpeettomat palvelut kuten tiedostojen verkkojaot on suljettu. Kotiverkossa verkkojaot on saatettu avata palomuurista, ja toisaalta oma ADSL-laite saattaa sisältää palomuurin. Aiemmin harmittomat tietoturva-aukot saattavat siten olla alttiina hyökkäyksille toisessa verkossa.

Tuntemattomassa verkossa saattaa myös olla käyttäjiä tai haittaohjelmia, jotka tarkkailevat verkkoliikennettä. Verkkosivujen siirtoon tarkoitettu salattu https-protokolla on melko turvallinen, mutta myös sitä käytettäessä kannattaa olla varovainen.

Käyttöjärjestelmän asennuksen aikana tietokoneen ei kannata olla kytkettynä edes kotiverkkoon. Asennettaessa palomuuri ei ole välttämättä käytössä, eikä uusimpia turvapäivityksiä ole vielä ladattu. Palomuuri täytyy kytkeä käyttöön ennen koneen liittämistä verkkoon turvapäivitysten latausta varten.

4. Oikeudet Unixissa

Unixissa jokaisella tiedostolla ja hakemistolla on omistaja ja ryhmä, sekä käyttöoikeudet omistajalle, ryhmälle ja muille käyttäjille. Ainoastaan root-pääkäyttäjä pystyy käsittelemään tiedostoja käyttöoikeuksista riippumatta.

4.1. Käyttäjien rajoittaminen

Normaalisti pyritään rajoittamaan käyttäjien pääsyä laitteistoon, järjestelmätiedostoihin ja muiden käyttäjien tiedostoihin. Järjestelmätiedostojen ja laitteiden käyttöoikeuksia hallitaan ryhmien kautta, käyttäjien tiedostojen oikeudet asettaa käyttäjä itse.

4.2. Käyttötavan rajoittaminen

Tiedostoilla on kolmenlaisia käyttöoikeuksia: luku-, kirjoitus- ja suoritusoikeudet. Näistä kaksi ensimmäistä ovat selkeitä. Suoritusoikeudella merkitään suoritettavat tiedostot, eli ohjelmat ja skriptit. Hakemistoilla suoritusoikeus tarvitaan hakemistoon siirtymiseen, lukuoikeus hakemiston sisällön listaukseen.

4.3. Oikeuksien hallinnan tarve ja tyypillinen käyttö

Oikeuksien hallinnan tarve on selkeintä monen käyttäjän järjestelmissä, mutta siitä on hyötyä myös työasemissa.

Työasemissa käyttöoikeuksien ja erillisten käyttäjien avulla voidaan rajoittaa ohjelmien toimintaa ja vähentää siten esimerkiksi turvallisuusaukkojen vaikutusta. Työaseman käyttäjälle annetaan tavallisesti oikeus mm. cd-aseman ja äänikortin käyttöön. Monen käyttäjän järjestelmissä estetään yleensä järjestelmätiedostojen muokkaus ja laitteiden käyttö kokonaan.

5. Salasana

5.1. Mihin salasanaa tarvitaan

Salasanaa tarvitaan tiedon salaamiseen. Vain salasanan tietävät pääsevät käsiksi salasanan takana olevaan informaatioon. Salasanaa myös tarvitaan käyttäjätunnuksen lisäksi henkilön tunnistamiseen. Henkilökohtaisella salasanalla todistetaan henkilöllisyys ennen palveluun sisäänkirjautumista.

5.2. Millainen on hyvä salasana

Hyvä salasana on satunnainen merkkijono, jossa on isoja ja pieniä kirjaimia ja numeroita sekaisin. Hyvässä salasanassa pitää olla mahdollisimman monta merkkiä, eikä se saa tarkoittaa mitään. Tämä on perusteltua, koska eri sanojen kokeileminen on murtautujalle helppoa ja nopeaa. Tietotekniikan avulla voi käydä melkein kaikki maailman olemassa olevat sanat läpi sanakirjoja apuna käyttäen, mutta satunnaisten merkkijonojen arvaamisessa menisi niin pitkään, että yrittämisessä ei ole mitään mieltä. Myös mitä pidempi salasana on, sitä kauemmin sen arvaamiseen menee. Hyväkin salasana kannattaa vaihtaa tietyin väliajoin turvallisuuden lisäämiseksi.

5.3. Miksi oma salasana eri järjestelmissä

Koskaan ei voi tietää, voiko palveluntarjoajaan luottaa. Jos käytät samaa käyttäjätunnusta ja salasanaa eri järjestelmissä, jonkun järjestelmän ylläpitäjä voi saada selville salasanasi ja käyttää sitä muissa käyttämissäsi palveluissa esimerkiksi tiedon urkkimiseen tai haittaohjelmien levittämiseen. Joissakin järjestelmissä salasanan suojaus on heikolla tasolla, joten myös ulkopuoliset voivat halutessaan päästä käsiksi salasanaasi.

6. Käytännön tietoturva TTY:lla

> *"Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä . Yliopiston tavoitteena on turvata riittävällä ja tarkoituksenmukaisella tasolla toiminnalleen tärkeiden tietojen, tietojärjestelmien, palveluiden ja tietoverkkojen toiminta, estää niiden valtuudeton käyttö sekä tahaton tai tahallinen tiedon tuhoutuminen ja vääristyminen."* [7]

6.1. Miksi TTY:lla tietoturva on erityisen tärkeää

Mahdolliset haittaohjelmat leviävät yliopiston laajassa verkossa nopeasti useille koneille, ellei tietoturvasta pidetä huolta. Verkossa käsitellään lisäksi työntekijöiden ja opiskelijoiden henkilökohtaisia tietoja.

Verkon käyttäjäkunta on laaja ja sekalainen, joten hyökkäyksiä tulee tahallisesti ja tahattomasti myös verkon sisäpuolelta. Riskitekijöitä ovat mm. kannettavat tietokoneet, joille saattaa olla asentunut muualta haittaohjelmia.

6.2. Miten TTY huolehtii tietoturvasta

TTY:n tietoverkon käyttäjillä on henkilökohtaiset tunnukset, joilla kirjaudutaan tietoverkkoon. Tällä tavoin estetään käyttäjiä häiritsemästä toistensa toimintaa, ja toisaalta voidaan jäljittää mahdolliset rikkeet.

Käyttäjien toiminnasta on käyttösäännöt, joilla pyritään muiden asioiden lisäksi myös tietoturvan parantamiseen. Lisäksi käyttösäännöissä on määrätty tietohallinnon reaktioista väärinkäytöksiin, kuten tunnuksen lukitsemisesta.

Ongelmien ennaltaehkäisemiseksi jokaisella palvelulla on nimetty ylläpitäjänsä, joka huolehtii järjestelmän päivityksistä. Palveluille suoritetaan myös riskikartoituksia, jotta tarvittaessa voidaan parantaa valvontaa tai lisätä rajoituksia.

6.3. Miten TTY:n opiskelijat kantavat vastuuta tietoturvasta

Opiskelijoiden velvollisuutena on noudattaa tietojärjestelmien käyttösääntöjä. Tärkeää on pitää käyttäjätunnuksensa salaisena ja käyttää hyvää salasanaa. Käytettäessä omaa kannettavaa tietokonetta yliopiston verkossa täytyy huolehtia myös sen tietoturvasta.

Lähdeluettelo

1. Qvick J.-C. Palomuurit (viitattu 22.09.2007)
http://it.lut.fi/kurssit/02-03/010626000/palautukset/seminaarit/Palomuurit_Jan_Qvick.pdf

2. Palomuurityypit (viitattu 22.09.2007)
http://www.tct.hut.fi/opetus/s38118/s00/tyot/30/ptyypit.shtml

3. Lapinlampi, T., Asikainen, A., Oinas, J., Tietoturva lähiverkossa (viitattu 22.09.2007).
http://vega.lnet.lut.fi/lahiverkot/tietoturva.html

4. Viestintävirasto: Virukset (viitattu 22.09.2007)
http://www.ficora.fi/index/palvelut/tietoturva/haittaohjelmat/virukset.html

5. Viestintävirasto: Madot (viitattu 22.09.2007)
http://www.ficora.fi/index/palvelut/tietoturva/haittaohjelmat/madot.html

6. Viestintävirasto: Virustorjunta (viitattu 22.09.2007)
http://www.ficora.fi/index/palvelut/tietoturva/virustorjunta.html

7. TTY:n tietoturvapolitiikka (viitattu 24.09.2007)
https://www.tut.fi/haavi/index.cfm?MainSel=13173&Sel=13333&Show=18035