Jari Karjalainen

Tietoturva Internetissä

Opinnäytetyö
Kajaanin ammattikorkeakoulu
Hallinnon ja kaupan ala
Tietojenkäsittelyn koulutusohjelma
Kevät 2002

SISÄLLYS

1 JOHDANTO

Internet on avoin globaali tietoverkko, jossa on miljoonia käyttäjiä ympäri maailmaa. Hyötykäyttäjien lisäksi Internetissä on valitettavasti mukana tahoja, jotka pyrkivät tietoisesti vahingoittamaan tai häiritsemään joko muiden verkkopalvelujen käyttöä tai tietojärjestelmiä.

Tietojärjestelmien ja niiden käytön häirinnän lisäksi Internetistä löytyvän tiedon oikeellisuudesta ei ole takeita. Avoimen luonteensa takia Internetissä on mahdollista levittää virheellistä informaatiota.

Lopputyöni tarkoituksena on selvittää mitä uhkia Internetissä on ja miten niiltä voi suojautua. Lisäksi pyrin kuvaamaan tietoturvallisuuden peruskäsitteitä sekä Internet – yhteyksien rakennetta ja niihin liittyviä turvaongelmia.

2 TIETOTURVALLISUUDEN PERUSKÄSITTEITÄ

Internetin tietoturvaa käsiteltäessä on hyvä selventää mitä tietoturva tarkoittaa, sekä käsitellä tietoturvan peruskäsitteistöä.

2.1 Tietoturvan osa-alueet

Tietoturvallisuus voidaan jaotella usein eri tavoin. Jyrki Kivimäen kirjassa [1,s.936-937] käytetään seuraavanlaista jakoa:

- Hallinto
- Henkilöstö
- Rakenteellinen ja tekninen turvaaminen
- Käyttötoiminta
- Tietojenkäsittelytoiminnan varmistaminen
- Jatkuvuussuunnittelu
- Käyttövaltuuksien hallinta ja asiakirjaturvallisuus
- Tietoliikenteen turvaaminen ja oheispalvelut
- Laadunvarmistaminen, dokumentointi ja järjestelmämuutokset
- Vakuutukset, sopimukset ja vastuu

Hallinto huolehtii turvastrategian luomisesta ja sen organisoinnista sekä valvonnasta.

Henkilöstön asema on luonnollisesti ensiarvoisen tärkeä. Useimmiten yrityksen oma henkilöstö aiheuttaa suuremman turvallisuusriskin kuin Internet -yhteydenottajat.

Henkilöstön tulee tuntea tietoturvallisuustoiminnot sekä olla motivoitunut käyttämään niitä jotta turvastrategiasta olisi käytännön hyötyä.

Rakenteellinen ja tekninen turvaaminen on suojautumista varkauksilta , sähkökatkoksilta, tulipaloilta ja muilta fyysisiltä uhilta. Keinoja tähän ovat mm. paloturvalliset ja lukitut tilat, vartiointi sekä valvonta.

Käyttötoiminta on tietojen ja järjestelmien, yleisimmin tietokonejärjestelmien ammattimaista käyttöä. Turvallisuuden kannalta on tärkeää noudattaa käytössä sovittua tietoturvapolitiikkaa, varautua vikatilanteisiin ja seurata järjestelmän käytettävyyttä ja häiriöitä.

Tietojenkäsittelytoiminnan varmistaminen on tietokoneiden ja oheislaitteiden sekä tietojen ja ohjelmistojen varmistamista. Tätä voidaan tehdä sähkönsaannin varmistuksella ja koneiden varmennuksella sekä varmuuskopioinnilla.

Jatkuvuussuunnittelu on varautumista pitkäaikaisiin keskeytymisiin tietoliikenteessä ja niistä toipumiseen. Tilanteiden varalta on oltava valmis toimintasuunnitelma jonka kohteena ovat erityisesti yritykselle kriittisimmät resurssit.

Käyttövaltuuksien hallinta ja asiakasturvallisuus sisältää lain määräämät salausvelvollisuudet , liike- ja asiakastietojen salauksen sekä luottamuksellisten tietojen salauksen. Tämä voidaan toteuttaa mm. rajoitettujen oikeuksien , salauksen , kulunvalvonnan sekä vaitiolovelvollisuuksien avulla.

Tietoliikenteen turvaaminen ja oheispalvelut liittyvät erilaisiin tietoliikenneyhteyksiin, puhelin- ja radioyhteyksiin sekä fyysisten tietolaitteiden kuljetukseen. Turvaamisessa vallitsevat menetelmät ovat teknisiä, mutta inhimillinen tekijä on huomioitava, ettei turvallisuusjärjestelmä hidasta tai vaikeuta liikaa tavallista työntekoa.

Laadunvarmistaminen, dokumentointi ja järjestelmämuutokset ovat olennaisia tekijöitä toimivan ja dynaamisen turvallisuus-järjestelmän luonnissa.

Vakuutukset, sopimukset ja vastuu ovat osa käytännön tietoturvallisuutta. Näiden avulla voidaan taata tietty turvallisuustaso, sopia käytettävistä suojauksista ja etukäteen määrittää kenelle tulee vastattavaksi tietoturvallisuus vahingon aiheuttama haitta.

2.2 Tietoturvallisuuden uhat ja vahingot

Tietoturvallisuusuhkia kohdistuu monelta taholta. Analysoitaessa uhkatekijöitä tulee huomioida seuraavat tekijät: mistä uhka tulee, millaisia seurauksia se voi aiheuttaa, kuinka vakava on aiheutettu vahinko ja kuinka se korjataan sekä miten uhka aiheuttaa vahingon.

Turvallisuusuhkien aiheuttajia voivat olla oma henkilökunta, teollisuusvakoilu, tulipalot, vesivahingot, tekniset viat, ulkopuoliset tunkeutujat ja tietokonevirukset.

Oman henkilökunnan tietotekniset valmiudet eivät ole riittävät. Yleensä ei ymmärretä tietoturva ohjeiden tärkeyttä. Teollisuusvakoilu on varsinkin nykyään laajentunut uhka. Kilpailu on kovaa ja halutaan pysyä kilpailijoiden tasolla markkinoilla ja jopa edellä. Ehkä suurin uhka 2000-luvulla tiedotusvälineiden mukaan ovat virukset, joiden lukumäärä on kasvanut räjähdysmäisesti. Virus voi mm. tuhota, varastaa tai muuttaa tietoa.

Turvallisuutta heikentävät vahingot eivät välttämättä itsessään ole haitallisia, vaan ne altistavat systeemin muille uhille. Tällaisia ovat mm. varmuuskopiointivirheet, virheelliset ohjelmat, ulkopuolisten tunkeutuminen järjestelmään ja järjestelmän turvatasojen murtaminen. Virheellisten ohjelmien aiheuttamat tietoturvavahingot ovat lisääntyneet ohjelmien tuotantonopeuden ja kilpailun lisääntyessä, jolloin uusia ohjelmia ei ole kunnolla testattu.

Tietoihin kohdistuvia vahinkoja ovat tietojen vuoto ja varastaminen, tietojen tuhoutuminen tai korruptoituminen sekä väärän tiedon luonti ja levitys.

Laitteistoihin kohdistuvia tietoturvavahinkoja ovat laitteiston turmeleminen tai varastaminen. Laitteistojen varastaminen on viime aikoina lisääntynyt yhä enemmän.

Varkaustapauksissa on kiusallista arvokkaan datan katoaminen varkaalle, joka on kiinnostunut vain laitteistosta. Tulipalo tai vesivahinko voi aiheuttaa vahinkoa. Tieto tuhoutuu tai vahingoittuu käyttökelvottomaksi.[1,s.938-1015]

2.3 Murtautumismenetelmiä

Tunkeutujan käyttämät murtautumismenetelmät voidaan jakaa sosiaalisiin ja teknisiin menetelmiin. Sosiaalisissa menetelmissä tunkeutuja käyttää väärin omia oikeuksiaan tai huijaa toisia käyttäjiä. Tämä on hyvin usein helpompaa kuin teknisten ratkaisujen käyttö. Myös laitteistojen heikkouksia voi käyttää hyväksi, esimerkiksi suojaamaton muistijärjestelmä on tehokas keino salasanojen selvitykseen.[1,s.921-929]

Salakuuntelu on tehokas murtautumistapa ja se on päätteiden ja lähiverkkojen tapauksessa melko helppoa. Helppoutta lisää nykyään varsinkin johtajilla yleistyneet kannettavat tietokoneet, joissa on langaton verkkoyhteys. (Langattomasta yhteydestä lisää luvussa 9).

Troijanhevoset ovat ohjelmanpätkiä, joita pyritään huomaamattomasti ujuttamaan suojattuun järjestelmään. Päästyään järjestelmään ohjelman tekee suojamuuriin aukon, josta murtautuja pääsee halutessaan sisään järjestelmään ja saa näin melko vapaat kädet tehdä järjestelmässä mitä haluaa.

Suojausaukot ovat virheellisiä suojausmäärittelyjä, jotka altistavat järjestelmän turvallisuusuhalle. Tyypillinen tapaus on Unix –tiedosto, jonka käyttöoikeudet on väärin määritelty.

Salasanojen arvailu on yleinen tapa päästä järjestelmään. Esimerkki milloin salasanan arvailulla voi päästä järjestelmään on aloitteleva käyttäjä, joka käyttää salasanana jotain selväkielistä sanakirjasanaa tai liian lyhyttä salasanaa.

Salasanojen purkamiseen käytettäviä purkutekniikoita on olemassa monenlaisia. Yksinkertaisin ns. brute-force eli raaka voima –tekniikka perustuu kaikkien mahdollisten salausalgoritmien avainvaihtoehtojen läpikäymiseen. Tämä tapa vaatii luonnollisestikin

paljon laskentakapasiteettia, eikä sovellu tapauksiin joissa avainvaihtoehtoja on liian paljon. Nykyisin 128 bittiä pitkät avaimet eivät ole murrettavissa raa'alla voimalla.

Ohjelmistovirheet ovat myös tapa päästä järjestelmään. Jokainen ohjelma sisältää virheitä, joista monia ei edes koskaan havaita (esim. Microsoft Explorer selainohjelmasta löytyy paljon virheitä, jotka mahdollistavat pääsyn järjestelmään). Käytännössä ohjelmisto-virheiden täydellinen poistaminen on mahdotonta. Tämä johtuu yleisestä kiireestä saada ohjelma markkinoille ja siitä, että ihmisellä on taipumus tehdä virheitä.

2.4 Suojautumismenetelmiä

Suojautumisessa on olennaisen tärkeää ennakkosuunnittelu. Riskit on analysoitava ennakolta, todennäköiset uhat sekä turvallisuusjärjestelmän kyvyt on tiedostettava. Lisäksi on suunniteltava ja luotava oikeantasoiset suojatoimenpiteet.

Suojajärjestelmä ei ole koskaan valmis toimimaan omillaan. Toimiva suojaus edellyttää systeemin päivitystä tasaisesti sekä jatkuvaa käytön seurantaa. Käytön seurannalla voi havaita joko murtautujan paikan päältä tai löytää tämän jälkeensä jättämiä jälkiä tai turvallisuusaukkoja. Seuranta toteutetaan useimmiten turvalokin avulla, jotka tallennetaan käyttäen esim. kerrankirjoittavaa mediaa tai erillistä lokikonetta. Seurantaa voi tehostaa liittämällä lokiin ohjelman, joka analysoi poikkeukselliset tilanteet ja raportoi niistä.[1,s921-928]

2.5 Internetin erikoispiirteitä

Internetin saadessa alkunsa 1960- ja 70-lukujen vaihteessa se oli vain muutaman tutkijan käyttämä tietoverkko, johon kuului vain muutama supertietokone Yhdysvalloissa. Verkko alkoi hitaasti laajentua ja myös tarve yhteiselle protokollalle ("kielelle jolla koneet keskustelevat verkossa") kasvoi. Näistä TCP/IP (Transmission Control Protocol/Internet Protocol) yleistyi, ja 80-luvun alkupuolella verkossa liikennöitiin melkein pelkästään sitä käyttäen.

Parikymmentä vuotta sitten kukaan ei olisi osannut aavistaakaan, että Internet kasvaisi näinkin suureksi; tällöin verkossa koneita oli vain satakunta, kun nyt niitä on yli 50 miljoonaa ja käyttäjiä vielä paljon, paljon enemmän. Verkon ollessa noinkin pieni, sen käyttäjät tunnettiin ja heihin voitiin jossain määrin luottaa eikä TCP/IP:tä ollut tarvetta suunnitella erityisen tietoturvalliseksi. Kaikesta huolimatta nykyään käytetään vielä perusrakenteeltaan samaa TCP/IP -protokollaa kuin 80-luvulla.

Tämä on syynä siihen, miksi TCP/IP:tä on mahdollista käyttää hyväksi. Jos TCP/IP:n korvaava protokolla suunniteltaisiin nyt uudelleen, ei käyttäjien tarvitsisi luultavimmin huolehtia tietoturvasta. Periaatteessa kuka tahansa voi väärentää verkkoliikennettään siten, että vastaanottaja luulee yhteyden tulleen jostain toisesta koneesta kuin todellisuudessa. Verkkoliikenne ei ole myöskään millään lailla salakirjoitettua. Jos liikenne halutaan salata, on käytettävä erillisiä erikoisohjelmistoja. Tietoliikenteen avoimuus mahdollistaa sen, että periaatteessa kuka tahansa voi salakuunnella verkossa liikkuvaa tietoliikennettä. [2][3,s.561-575]

3 MIKÄ ON TCP/IP -PROTOKOLLA?

TCP/IP huolehtii tietopakettien kuljettamisesta ja se tekee mahdolliseksi yhteydenpidon kaiken tyyppisten laitealustoiden ja käyttöjärjestelmien välillä. TCP/IP –protokolla on kehitelty Yhdysvalloissa 1970-luvulla Yhdysvaltain puolustusministeriön toimesta. TCP/IP –tietoliikenne on perusta Internetille. Perusprotokollan päälle kehitetään jatkuvasti uusia sovelluksia, joista tunnetuimpia on WWW.

TCP, Transmission Control Protocol, muodostaa kaksisuuntaisia yhteydellisiä tietoliikenneyhteyksiä. IP:n huolehtiessa vain yhdestä paketista kerrallaan TCP huolehtii peräkkäisten pakettien perillepääsystä ja lähettää uudelleen kadonneet tai vaurioituneet paketit. TCP paketti sisältää lähettäjän ja vastaanottajan IP -osoitteiden lisäksi myös TCP -porttien numerot, sekä tarkistussumman joka on pakollinen , toisin kuin UDP:ssä, jossa sitä ei kaikissa järjestelmissä käytetä. Tietoturvan kannalta merkittävä on yhteyden sekvenssinumero. Avattaessa TCP yhteyttä saavat molemmat osapuolet koneiden ISN -laskurien mukaiset sekvenssinumerot, joita kasvatetaan 4ms välein. Näitä numeroita käytetään vuonohjauksessa vanhentuneiden pakettien havaitsemiseksi.

IP eli Internet Protocol on yhteydetön tietosähkeprotokolla. Se käsittelee kaikki IP-paketit erillisinä. IP -pakettien lähettäjä ja vastaanottaja ilmaistaan IP -osoitteella joka on 32 –bittinen kokonaisluku, joka esitetään yleisesti pisteillä erotettuna desimaalilukuna, esim.

alfa.hut.fi:130.233.224.50. IP -protokolla reitittää paketin lähettäjältä vastaanottajalle automaattisesti, ilman että lähettäjän tarvitsee tietää siirrosta muuta kuin saajan IP –osoite.

Nykyisissä TCP/IP systeemeissä on huomattavan paljon turvallisuusongelmia, mikä johtuu siitä, että protokollaperhe suunniteltiin ajatellen käyttöympäristön olevan riittävän turvallinen eli että esim. käytetty verkko turvaa IP-pakettien eheyden. Yleisimmät turvallisuusheikkoudet ovat: [2]

- Verkon salakuuntelu, kun tiedetään kuunneltavan IP –osoite niin voidaan mm. poimia liikenteestä käyttäjien salasanoja.

- IP –osoitteiden väärennys eli vastaanottaja luulee yhteyden tulleen jostain toisesta koneesta kuin todellisuudessa.

4 TIETOTURVARATKAISUT INTERNETISSÄ

Internetin tietoturvaratkaisut voidaan jakaa tietoliikenteen suojaamiseen sekä palvelinkoneen suojaamiseen. Tietoliikenteen suojaamisella tarkoitetaan kahden tietokoneen välisen liikenteen kuuntelemisen estämistä. Tietoliikenteen suojaus tapahtuu käytännössä salaamisella ja käyttämällä viruksentorjunta ohjelmia. Palvelinkoneen suojaus tapahtuu käyttämällä käyttäjätunnuksia ja salasanoja sekä eristämällä palvelin Internetistä palomuurin avulla, käyttämällä reitittimiä ja yhdyskäytäviä sekä näiden yhdistelmiä.

4.1 Salakirjoitusmenetelmät

Salausmenetelmät pyrkivät paikkaamaan TCP/IP –protokollan yleiset turvallisuuspuutteet. Salakirjoitukseen voidaan käyttää useita menetelmiä. Perussalausmenetelmiä on kaksi: symmetrinen ja asymmetrinen.

Yleisimpiä tällä hetkellä käytettyjä symmetrisiä algoritmeja ovat DES ja IDEA. Eniten käytetty asymmetrinen algoritmi on RSA. Muita ovat mm. Diffie-Hellman. Näiden lisäksi on symmetrisen ja asymmetrisen kryptografian yhdistelmiä kuten PGP ja SSL.

Salausalgoritmi on sitä luotettavampi mitä pidempi salausavain on. Luotettavana voidaan pitää 128 bitin avainta käyttäviä salausalgoritmeja.[1,s.1007-1015]

4.2 Virustorjuntaohjelmat

Vakoilija virukset voi torjua ainoastaan käyttämällä ajantasalla olevaa viruksentorjunta ohjelmaa, kuten F-Securen antivirus ohjelmaa.

Virustorjunta ohjelmat käyttävät periaatteessa neljää erilaista menetelmää viruksen havaitsemiseen [1,s.1002-1003]

- Merkkijonoon pohjautuvassa etsintäohjelmassa etsitään kaikista läpikäytävistä viruksista siitä eristettyä esimerkiksi 40 merkin mittaista merkkijonoa. Mikäli kyseinen merkkijono löytyy tehdään lisätarkistus, ja mikäli sekin pitää paikkansa, annetaan virusilmoitus.

- Tarkistussummamenetelmässä lasketaan jokaiselle ohjelmatiedostolle tiedoston pituuteen liittyvä matemaattisten algoritmien mukainen tarkistussumma ja salakirjoitetaan se. Kun etsintäohjelmaa käytetään, se laskee tiedot uudelleen ja jos tiedoston pituus on muuttunut, annetaan virusilmoitus.

- Taustalla toimiva merkkijonon etsintäohjelma lukee käynnistettävän tai kopioitavan tiedoston ennen sen käyttöä ja havaittuaan viruksen estää virustartunnan antamalla hälytyksen. Tällainen taustaohjelma vie jonkin verran muistia ja periaatteessa hidastaa jonkin verran ohjelmien käynnistystä ja tiedostojen kopiointia.

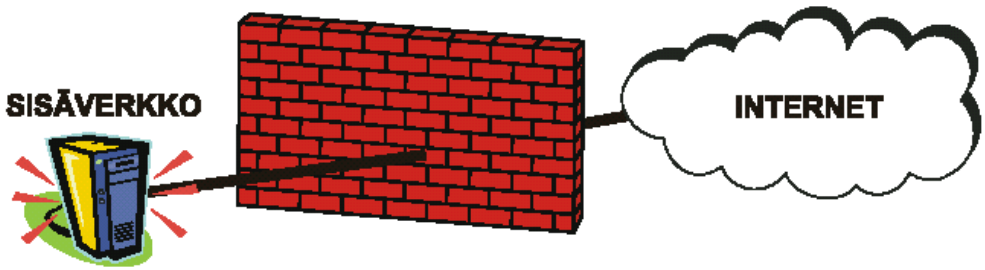
- Heuristinen menetelmä ei yritä etsiä viruksia merkkijonojen pohjalta vaan päättelemällä tiedoston sisällöstä, voisiko se olla virus. Tällä menetelmällä ei voida saavuttaa läheskään 100% varmuutta.

4.3 Palomuuri

Palomuurit eli firewall-ratkaisut ovat tietojärjestelmien linnakkeita. Palomuuri estää luvattoman ja sallii luvallisen liikenteen lähiverkon ja Internetin välillä. Palomuurin avulla luodaan valvottu yhdyskäytävä, jonka kautta kaikki liikenne verkkojen välillä tapahtuu.

Palomuurit myös keräävät tietoa muurin läpiotetuista yhteyksistä ja tarvittaessa hälyttävät apuvoimat paikalle. Palomuurin avulla pystytään korvaamaan verkossa olevien ohjelmien ja protokollien puutteellisia suojauksia.

Palomuuri on siis tietokonejärjestelmä, joka eristää yrityksen sisäisen verkon ja avoimen Internet-verkon toisistaan niin, että läpikulkevaa liikennettä voidaan hallita molempiin suuntiin ja että vain sallittu liikenne päästetään läpi. Se voidaan sijoittaa suojelemaan myös jotain pienempää osaverkkoa tai -kokonaisuutta. Palomuuri estää ei-toivotut (hakkerit) ja mahdollisesti vahingolliset tunkeutumiset verkkoon sekä takaa suojatun verkon käyttäjille turvalliset ulkoiset yhteydet.



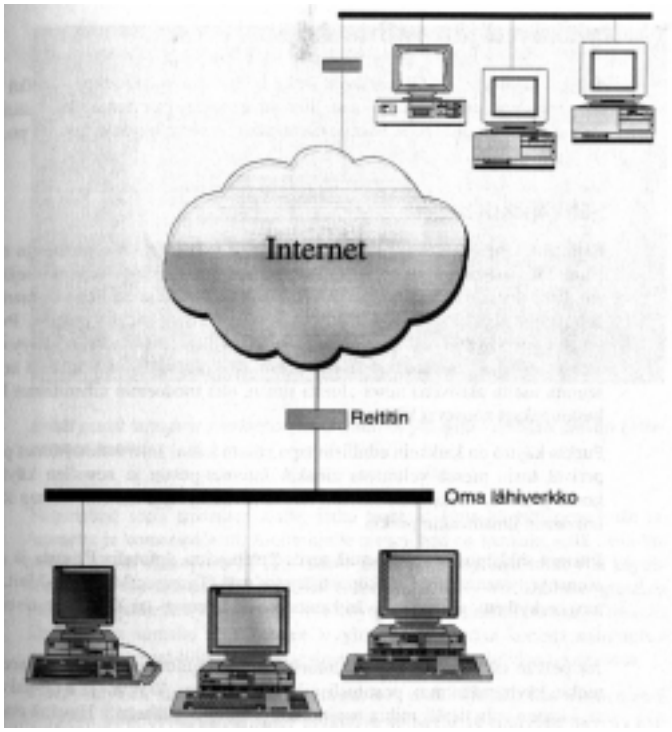
Kuva 1. Kuvaus palomuurista

Palomuurin vahvuutena voidaan pitää mm. liikenteen ja tietoturvan keskitettyä hallintaa. Palomuuri antaa suojaa lähiverkon ulkoisilta hyökkäyksiltä ja sen avulla voidaan kerätä seurantatietoja verkon- ja liikenteen käytöstä.

Palomuurin heikkoutena voidaan pitää mm. sitä, että se ei suojaa verkon sisältä tulevilta hyökkäyksiltä, se vaatii toimiakseen hallintaa ja seurantaa, ja se voi estää käyttäjien tarvitsemia palveluja.[4]

4.4 Reititin

Reititin (Router) ohjaa Internetiin menevän liikenteen ulos omasta lähiverkosta ja edelleen palveluntarjoajan reitittimeen. Reititin pystyy tarvittaessa käyttämään rinnakkaisia reittejä tai ohjaamaan paketit varatietä pitkin ruuhkan tai katkenneen reitin takia.



Kuva 2. Kun lähiverkko kytketään Internetiin, väliin tarvitaan liikennettä ohjaava reititin.

Reitittimillä voidaan rajoittaa verkon liikennettä siten, että vain erikseen määriteltyjen aliverkkojen tai verkko-osoitteiden (IP-osoite) sallitaan liikennöivän keskenään. Määrittely tehdään reitittimien pääsylistoihin (Access list).[5,s.55]

4.5 Yhdyskäytävä

Yhdyskäytävä on tavallisimmin jokin työasema ja ohjelmisto, jolla erityyppisiä verkkoja liitetään toisiinsa.

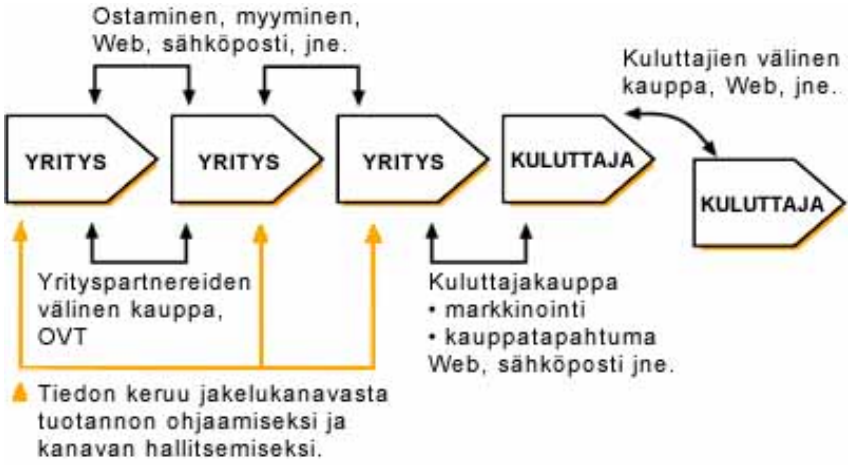
Yhdyskäytäviä (Gateways) käytetään yleisesti palomuurien yhteydessä. Yhdyskäytävissä määritellään mitkä verkot ja sovellukset ovat käytettävissä yhdyskäytävän kautta.[5,s.43]

5 OSTAMINEN INTERNETISTÄ (VERKKOKAUPPA)

Sähköinen kaupankäynti Internetissä yleistyy koko ajan. On nähtävissä, että Internetistä on tulossa yleinen kaupankäyntikanava, jota suuri joukko ihmisiä käyttää erilaisiin ostoksiinsa. Tutkimuksista voi todeta, että kaupankäynti Internetissä kasvaa tasaisesti koko ajan; Internetiä käyttävien ihmisten osuus koko väestöstä kasvaa, samoin verkkokaupassa vierailevien kuluttajien osuus.

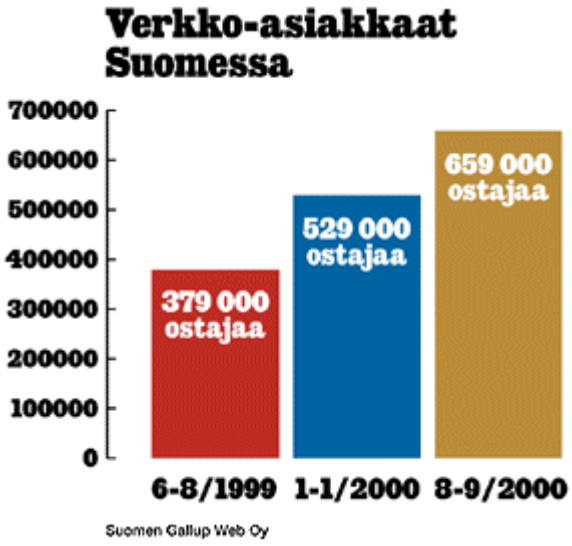
5.1 Mitä verkkokauppa on?

Verkkokauppa on osa sähköistä kaupankäyntiä, joka voi tapahtua tietoverkkojen, puhelimen, television tai faksin välityksellä. Verkkokaupan synonyymisanoja ovat www-kauppa, nettikauppa ja e-kauppa, englanniksi e-commerce. Siihen sisältyy palvelujen, tuotteiden ja informaation myyminen, maksaminen, esittely, markkinointi ja jakelu monissa eri muodoissaan sekä teknologiat, jotka mahdollistavat nämä toiminnot. OECD määrittelee verkkokaupan joko yritysten tai yritysten ja kuluttajien väliseksi Internetin kaltaisissa avoimissa verkoissa tapahtuvaksi liiketoiminnaksi. Tämän määritelmän mukaan suljetuissa verkoissa tapahtuva sähköinen kauppa (EDI=Electronic Data Interchange/OVT=organisaatioiden välinen tiedonsiirto) ei ole verkkokauppaa.



Kuva 3. Sähköisen kaupankäynnin määritelmä[11].

Verkkokaupasta on tullut vuosi vuodelta suositumpi tapa tehdä ostoksia. Etuna normaaliin kauppaan verrattuna on ostamisen helppous ja se, että kauppa on auki ympäri vuorokauden.



Kuva 4. Verkko-asiakkaiden määrän kehitys[6].

5.2 Tietoturva

Verkko-ostoksia tehdessä voidaan yleisenä ohjeena sanoa ettei ostoksia kannata tehdä yhteiskäytössä olevalla tietokoneella, jos se ei ole luotettavassa ja valvotussa julkisessa tilassa. Näin varmistetaan, että tietokoneen tietoturvajärjestelyt ovat asianmukaiset ja että konetta käsittelevä henkilökunta toimii vastuullisesti ja koneen käyttäjiä valvotaan.[8,s.103-137][9,s.128-158][10,s.113-124]

5.3 Asiakastietojen salaaminen ja turvallisuus

Pääsääntö tietosuojan osalta on, että verkkokaupan sivuilta pitäisi löytyä tiedot siitä, kuka käsittelee henkilötiedot, missä tarkoituksessa se tapahtuu, luovutetaanko tietoja edelleen ja miten omat tiedot voidaan tarkastaa ja korjata tai voiko niiden luovuttamista markkinointi tarkoituksiin kieltää. On myös tarkastettava voidaanko tiedot antaa salattuina. Jos kauppa vaikuttaa luotettavalta näiden tarkastusten jälkeen, on myös rekisteröityminen kaupan asiakkaaksi todennäköisesti turvallista.

Rekisteröidyttäessä jonkin verkkokaupan asiakkaaksi yleensä kysytään yhteys- ja henkilötietoja. Lisäksi voidaan myös kysyä tietoja elämän tilanteesta, esim. asumismuodosta sekä asiakkaan kiinnostuksen kohteista. Näin palvelun tarjoaja voi kertoa uutuuksista asiakkaalle. Toisin sanoen näitä tietoja tullaan todennäköisesti käyttämään verkkokaupan suoramarkkinoinnissa, joten kannattaa harkita haluaako antaa itsestään näitä tietoja, sillä pakkoa tietojen antamiseen ei ole. Kaupassa liikkumisesta kertovia tietoja tallentuu kauppojen tietojärjestelmiin myös automaattisesti. Tiedot tallentuvat evästeeseen eli cookieen, joka on pieni tiedosto, jonka verkkokauppa lähettää käytettävälle www-selaimelle. Evästeiden avulla verkkokauppa esimerkiksi pitää muistissa asiakkaan ostoskoriin poimimat tuotteet, saa selville www-sivuilla kävijöiden määrän sekä selatut sivut, mutta ei tietokoneen ja selaimen käyttäjää. Jos rekisteröidytään kaupan asiakkaaksi eli annetaan nimi ja yhteystiedot, kauppa voi yhdistää annetut tiedot evästeen avulla saatuihin tietoihin. Vastuullinen kauppias kertoo asiakkaalleen mahdollisesta tulevasta suoramarkkinoinnista.

Selainohjelmat tallentavat osoitteet niistä web-sivuista, joissa käyttäjä on vieraillut. Osoitteet tallentuvat selaimen välimuistiin ja niin sanottuun sivuhistoriaan. Nämä muistijäljet helpottavat www:ssä liikkumista, esimerkiksi selaimen Takaisin-painike (Back) toimii muistijälkien avulla. Joihinkin kauppoihin muistijälkien tyhjentäminen on rakennettu automaattisesti ulos kirjautumisen yhteyteen. Tästä syystä verkkokaupoista on hyvä poistua "Kirjaudu ulos" -painiketta tai ”Exit” -painiketta käyttäen, jos sellainen on. Edellä mainittuja painikkeita on erityisen suositeltavaa painaa yleisessä käytössä olevissa koneissa, ettei seuraava tietokoneen käyttäjä pääse näille sivuille tekemään mm. lisätilauksia.

Kauppias hoitaa salauksen tietokoneohjelmien avulla. Salauksen tunnistaa selaimen alareunassa olevasta lukkosymbolista. Kannattaa tarkista, että niillä www-sivuilla, joille luottamuksellisia tietoja kirjoitetaan, on kiinni olevan riippulukon kuva selaimen alareunassa. Kun annetaan luottamuksellisia tietoja vain silloin, kun salaus on käytössä, tietoja ei pääse katsomaan selaimellakaan sen jälkeen, kun kyseiseltä sivulta on poistunut.

Kauppa tallentaa annetut tiedot asiakasrekisteriinsä. Tietojen tallentaminen kaupan rekisteriin nopeuttaa ostamista seuraavalla kerralla, sillä samoja tietoja ei tarvitse antaa enää uudelleen. Annetut tiedot suojataan käyttäjätunnuksella ja salasanalla. Verkkokaupoissa kannattaa käyttää eri salasanaa kuin muissa yhteyksissä. Erityisen huolellisella asiakkaalla on eri salasana eri kaupoissa.

Salasanoja käytetään, jotta kukaan ei voisi esiintyä toisena henkilönä tai saada muita henkilöitä koskevia tietoja käsiinsä. Salasana toimii, kun se pysyy salaisena eikä ole arvattavissa. Salasanan tulee olla tarpeeksi pitkä. Kolmetoista merkkiä on salasanan murtajalle kova tehtävä. Hyvä salasana muodostetaan esimerkiksi ottamalla jostakin lauseesta kaikkien sanojen ensimmäiset kirjaimet. Tällainen salasana on helppo muistaa, mutta vaikea arvata. Salasana, joka sisältää kirjaimia, numeroita ja muita merkkejä, on erityisen hyvä. Salasanana ei tulisi käyttää perheenjäsenten nimiä, syntymäpäiviä tai puhelinnumeroita. Salasanoja ei saa kirjoittaa muistiin eikä niitä saa antaa muille.[7,s.161-178][8,s.103-137][9,s.128-158][10,s.113-124]

Viestin lähettäjä sekä tiedonsiirron eheys voidaan vielä varmistaa digitaalisella allekirjoituksella. Digitaalinen allekirjoitus tehdään muodostamalla viestistä hajoitealgoritmilla hajoite (hash), joka salataan lähettäjän henkilökohtaisella avaimella. Vastaanottaja purkaa salauksen lähettäjän julkisella avaimella. Viestin muuttumattomuuden voi tarkistaa laskemalla viestistä uudestaan hajoite ja vertaamalla sitä lähetettyyn hajoitteeseen.[12,s.65]

Suomessa on käytössä myös sähköinen henkilökortti. Sähköisen henkilökortin avulla voidaan tunnistaa tiedon lähettäjä ja varmistua siitä, että tieto ei muutu siirrettäessä. Sähköisen henkilökortti ei ole vielä Suomessa yleistynyt, mutta sen toivotaan yleistyvän, koska se tehostaa henkilön tunnistamista ja tiedon muuttumattomuuden varmistamista. Erityisesti sähköistä henkilökorttia suositellaan viranomaisten kanssa tapahtuvaan asiointiin. Sähköisen henkilökortin voi hankkia poliisilaitokselta.

6 MAKSAMINEN VERKKOKAUPASSA

Internet-ostosten maksaminen ei ole enää ongelmallista. Yleisimpiä maksutapoja Suomessa ovat postiennakko, laskutus ja verkkopankkisiirto. Verkkopankkisiirtotapoja ovat Leonia Pankin verkkomaksu, Merita Pankin Solomaksu ja Osuuspankkien Kultaraha. Monet kauppiaat tarjoavat useita turvallisia maksuvaihtoehtoja, joista asiakas voi valita hänelle sopivimman.

Tavallista on, että ostokset maksetaan postiennakolla. Monet kaupat käyttävät myös verkkomaksupalveluja eli Meritan Solo-maksua, Osuuspankkien Kultarahaa tai Leonian verkkomaksupalvelua. Verkkomaksu tehdään helposti WWW-selaimen avulla. Maksu lähtee välittömästi asiakkaan tililtä kauppiaan tilille, jolloin tuote voidaan toimittaa nopeasti. Tarvittavat tunnukset ja salasanalistat asiakas saa omasta pankista.

Luottokorttimaksaminen on yleistymässä SET-turvallisuusjärjestelmän myötä. Sähköiseen liiketoimintaan soveltuvia maksutapoja on muitakin, ja niitä kehitellään jatkuvasti. Aivan kuten "vanhassa maailmassa" on kolikoita, seteleitä sekä pankki- ja luottokortteja, Internetissäkin on erilaisia maksutapoja eri tarkoituksiin. Maksutavan sopivuus riippuu mm. maksun suuruudesta.

6.1 Rahakortit

Rahakortit ovat kaikille tuttujen puhelinkorttien kaltaisia kortteja, joihin voi ladata katetta pankkiautomaatista. Voidakseen maksaa verkko-ostoksensa Rahakortilla asiakas tarvitsee

tietokoneeseen liitettävän erillisen kortinlukulaitteen. Nykyisellään Rahakorteilla ei ole oikeastaan minkäänlaista asemaa verkkokaupan maksuvälineenä.

6.2 Verkkopankkisiirto

Verkkopankkisiirtoa voidaan pitää erittäin luotettavana tapana maksaa ostokset Internetissä, koska maksutapahtuman aikana olet sen pankin salatulla maksusivulla, jolta maksat ostoksen . Verkkopankkisiirto siis tarkoittaa Internetissä WWW-selaimen avulla tilaushetkellä tehtävää pankkisiirtoa. Verkkopankkisiirtotapoja ovat Merita Pankin Solo-maksu, Osuuspankkien Kultaraha ja Leonia Pankin verkkomaksu. Verkkopankkisiirtoa voidaan maksutapana tarjota suomalaisille asiakkaille. Verkkopankkisiirron osalta on muistettava, että sekä asiakkaalla että kaupalla täytyy olla tili ja verkkomaksusopimus samassa pankkiryhmässä, jotta maksaminen onnistuisi. Jotta kauppa voisi palvella mahdollisimman monia asiakkaita, kannattaa sen tarjota mahdollisimman monen pankin maksumenetelmä. Kauppiaan kannalta verkkopankkisiirto on helppo maksumenetelmä. Kauppajärjestelmä saa tiedon tapahtuneesta maksusta automaattisesti.[9,s.131-132]

6.3 Luottokortti

Viime aikoina on uutisoitu nuorista hakkereista, jotka ovat hakkeroineet luottokortti numeroita verkkokauppiaiden palvelimilta ja julkaisseet niitä. Mikä sitten on todellisuudessa luottokorttimaksamisen turvallisuus? Käyttäjiä on varoitettu kirjoittamasta luottokorttinsa numeroa mihinkään verkon palvelimeen, koska hakkerit saattavat väijyä verkon liikennettä ja napata ohikiitävien luottokorttien numeroita.

Käytännössä luottokorttinumeroiden poimiminen miljardien bittien tietovirrasta on likipitäen mahdotonta. Paljain silmin numeroita ei voi kalastaa, mutta joku voi tehdä verkon liikennettä seuraavan ohjelman, joka seuraa ja poimii virrasta luottokortilta näyttäviä numerosarjoja. Tällaisen ohjelman tekeminen on kuitenkin hankalaa ja sen toimivuus kyseenalaista, koska nimi- ja numerotiedot eivät välttämättä kulje peräkkäin.

Luottokortilla maksaminen on Internetissä mahdollista SET-nimisen turvallisuusjärjestelmän avulla. Vaihtoehtoisia tapoja maksamiseen on kaksi: asiakas voi käyttää maksamiseen luottokorttinumeroaan, jolloin SSL-suojaus huolehtii tietoturvasta. Toisena vaihtoehtona on maksaa SET-lompakko-ohjelman avulla, jonka asiakas saa ilmaiseksi Internetistä. Ohjelma välittää luottokorttitiedot turvallisesti Internet-kaupan tietokoneelle. Luottokorttimaksamisessa ei maksettavalla summalla ole alarajaa.

Pohjoismaat ovat SET:in kehityksen kärjessä. Suomi olikin ensimmäinen maa, jossa SET otettiin käyttöön.

Luottokortti on kansainvälisesti merkittävin maksutapa kuluttajakaupassa. SET on perustaltaan kansainvälinen järjestelmä, jota kaikki merkittävimmät luottokorttiyhtiöt tukevat.

Luottokortilla ostettaessa on hyvä tarkistaa aina maksuerittely ja säilyttää ostosten tilausvahvistukset. Ainahan on mahdollista, että myyjä veloittaa summan vahingossa useampaan kertaan tai kirjoittaa laskun liian suureksi. Käytä luottokorttia maksuvälineenä ainoastaan luotettavissa ja tunnetuissa verkkokaupoissa. [9,s.132-133]

6.4 Asiakastili

Asiakastilillä tarkoitetaan järjestelyä, jossa asiakas maksaa etukäteen myyjän tilille tietyn summan. Tämän jälkeen hän voi ostaa myyjän verkkokaupasta tuotteita tallettamaansa summaa vastaavalla määrällä. Vakiintuneissa asiakassuhteissa tili voidaan luonnollisesti muuttaa luotolliseksi mikäli näin halutaan. Asiakastili voi toimia myös toisinpäin, eli asiakkaan ostojen tiedot kerätään asiakastilille, jonka saldon asiakas maksaa jälkikäteen laskulla. Molemmissa tapauksissa kaupan osapuolilta edellytetään luottamusta toisiinsa.

Asiakastilit ovat käteviä varsinkin todella pienten maksujen maksamiseen. Näitä pieniä maksuja tarvitaan varsinkin uusien digitaalisten tietotuotteiden kaupan yhteydessä.

6.5 Muut maksutavat

Muita maksutapoja on mm. postiennakko, etukäteen normaalilla tilisiirrolla maksaminen ja lasku.

Postiennakko on varsin kätevä ja luotettava tapa laskuttaa, jos tuote toimitetaan postitse. Postiennakko sopii yli 50 mk:n laskuihin. Postiennakolla voidaan myydä sekä Suomeen, että myös muihin Länsi-Euroopan maihin. Postiennakko on tutkimusten mukaan edelleen suosituin maksutapa. Riskit ostajalle ovat, ettei tuote ole se mikä sen piti olla tai tuote on viallinen, ja kauppiaalle ettei ostaja käy lunastamassa ostoksiaan, jolloin kauppiaalle tulee menetyksiä postituskuluista.

Etukäteen maksu tarkoittaa sitä, että asiakas maksaa ostoksensa etukäteen kaupan tilille käyttäen viitenumeroa. Saapuneiden maksujen viitenumeron perusteella kauppias tietää, mikä tilaus vastaa mitäkin maksua, ja voi toimittaa tilaukset perille.

Viitepankkisiirtoa voidaan maksutapana tarjota suomalaisille asiakkaille. Tässä maksutavassa ainut riski on ostajalla. Tuote ei ole se mikä sen piti olla tai se on viallinen tai kauppias ei lähetä sitä ollenkaan.

7 VERKKOPANKIT

Suomalaiset verkkopankkien palvelut ovat maailman huippuluokkaa. Amerikkalainen käyttäjä voi vain unelmoida siitä mukavuudesta, joka suomalaiselle on itsestään selvää. Laskut voi maksaa ja saldon nähdä reaaliajassa suoraan omalta tietokoneelta. Rahan siirto tililtä toiselle käy yhdessä päivässä, vaikka pankit olisivat toistensa kilpailijoita.

7.1 Tietoturva

Pankkipalveluissa käytettävä salaus noudattaa normaalia SSL-tekniikkaa. Eurooppaan toimitettavissa selaimissa salauksen pituus on yhä rajattu 40 bittiin ja huomattavasti turvallisempaa 128-bittistä salausta jaetaan vain amerikkalaisille käyttäjille.

Käytännössä 40-bitin salaus on aika turvallinen. Se on murrettavissa, mutta murron tuloksena saatavasta avaimesta ei ole hakkerille mitään iloa. sillä avain on istuntokohtainen ja voimassa vain niin kauan kuin pankkiyhteys on käytössä. Seuraavalla käyntikerralla avain on jo toinen.

Istuntokohtaisen avaimen käyttö on SSL:n perustekniikkaa ja käytössä kaikissa suojatuissa WWW-yhteyksissä. Ne tunnistaa selaimen alapalkissa näkyvästä lukon kuvasta ja URL-osoitteessa näkyvästä HTTPS-protokollasta. Käyttäjä ei koskaan edes näe omaa istuntokohtaista avaintaan.

Lisäksi pankkipalveluissa käytetään kertakäyttöisiä tunnuslukuja, mikä entisestään vaikeuttaa murtajan työtä. Suurimpana riskitekijänä voidaan pitää huolimatonta käyttäjää,

joka ei säilytä henkilökohtaisia käyttäjätunnuksia ja salasanojaan riittävän huolellisesti muilta piilossa. Eli jos säilyttää tunnuslukuja huolellisesti, eikä kirjoita asiakastunnusta arkin yläreunaan, voi verkkopankkia käyttää turvallisin mielin.[13,s.33][15]

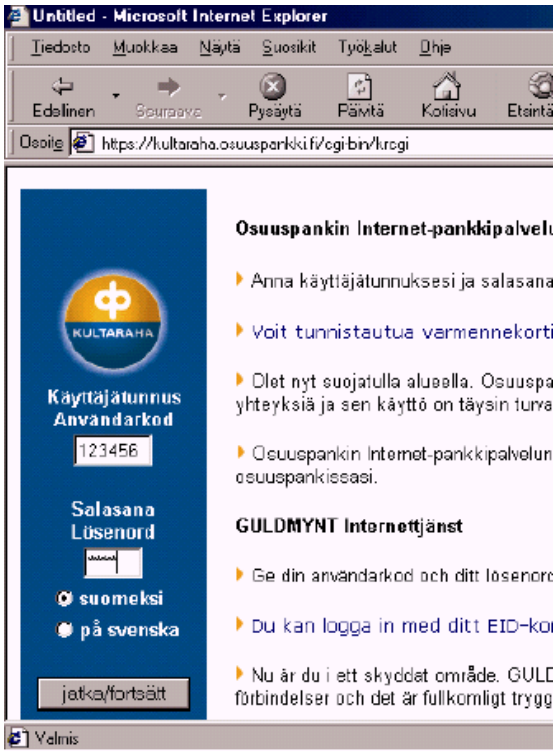
Seuraavassa Suomalaisen Osuuspankin turvallisuus esiteltynä.

7.2 Osuuspankki

Osuuspankki on tarjonnut jo usean vuoden ajan asiakkailleen mahdollisuutta hoitaa pankkiasioita Internetin kautta.

7.2.1 Käytön kuvaus

Verkkopankin käyttöä varten tarvitaan henkilökohtainen kuusinumeroinen käyttäjätunnus ja nelinumeroinen salasana. Näiden avulla verkkopankki tunnistaa käyttäjän. Lisäksi tilitietoihin ja laskunmaksuun pääseminen edellyttää yhteyskohtaista avainlukua.



Kuva 5. Ote Osuuspankin verkkopankkipalvelusta

Kun asiakas tekee verkkopankin käyttösopimuksen, hän saa pankistaan käyttäjätunnuksen, salasanan sekä 100 avainlukuparia sisältävän listan. Lukupareista toinen on pankin luku ja toinen sitä vastaava asiakkaan luku. Pyrkiessään käyttämään tiliään esimerkiksi maksaakseen laskuja asiakkaalta kysytään tiettyä pankin avainlukua vastaavaa lukua, jonka tietäminen vasta mahdollistaa tilille pääsyn. Avainluvut ovat nelinumeroisia ja parit ovat istuntokohtaisia. Uuden avainlukulistan voi tilata verkkopankista, mutta se on haettava omasta pankista perinteiseen tapaan käymällä henkilökohtaisesti virkailijan puheilla.

Myös verkkokaupassa käytettävä suoramaksupalvelu on Osuuspankin järjestelmässä mahdollista. Verkkokauppiaat voivat tehdä Osuuspankin kanssa sopimuksen laskujen maksamisesta verkkopankin kautta. Kaikki sopimuksen tehneet yritykset löytyvät Optorilta, jonne pääsee Osuuspankin kotisivulta (www.osuuspankki.fi). Kun asiakas tekee verkkokaupasta ostoksia, hän voi maksaa ne suoramaksupalvelun avulla. Tällöin siirrytään verkkopankin palvelimelle ja maksaminen tapahtuu samojen periaatteiden mukaisesti kuin normaali laskujenmaksu, jolloin tietoturva on ihan vastaava kuin muussakin verkkopankin käytössä. [14][15]

7.2.2 Tietoturva

Tietoturvan kannalta keskeistä on käyttäjätunnuksen ja salasanan pysyminen salaisina. Siksi niitä olisi säilytettävä turvallisessa paikassa, ei aivan tietokoneen läheisyydessä. Jos epäilee käyttäjätunnuksen ja salasanan joutuneen jollekin ulkopuoliselle, on verkkopankin palveluvalikosta mahdollista lukita palvelujen käyttö. Lukituksen voi ainoastaan pankki purkaa.

Yhteyden alussa kirjoitettava käyttäjätunnus näkyy ruudulla, jolloin joku voi sen selän takaa nähdä. Käyttäjätunnus voi näin paljastua. Tämä on pieni tietoturvan heikennys, joskin tilille pääsy edellyttää vielä salasanan, joka syötettäessä ei näy ruudulla, ja avainlukujen tuntemista.

Salasana on heikko: se on neljä merkkiä pitkä ja siinä saa esiintyä vain numeroita. Näin erilaisia salasanoja on vain 10 000 kappaletta. Näistä liian säännölliset salasanat eivät

kelpaa (kaikki numerot samoja, nouseva tai laskeva numerosarja). Kuitenkin esimerkiksi kolme samaa numeroa sisältävä salasana kelpaa. Esimerkiksi salasanan 8889 antama turva on vähäinen. Tietysti lyhyt salasana on helppo muistaa, joten sitä ei välttämättä tarvitse kirjoittaa muistiin, mutta se on myös helppo murtaa. Niinpä tietoturvan parantamiseksi salasanojen tulisi olla monipuolisempia: kirjaimet ja erikoismerkit tulisi sallia, ei hyväksyä salasanoja, jotka ovat jonkun kielen sanoja ja ehkä myös kasvattaa salasanan pituutta.
Tietoturvallisuuden parantamiseksi salasanaa tulisi aika ajoin vaihtaa. Tämä on mahdollista tehdä näppärästi verkkopankin palveluvalikosta. Pankkipalvelu ei kuitenkaan pakota vaihtamaan salasanaa. Tietoturvallisuus olisi kyllä parempi, jos pankki vaatisi salasanan vaihtamista ainakin pari kertaa vuodessa. Ainakin järjestelmän tulisi vaatia, että salasana vaihdetaan ensimmäisellä kirjautumiskerralla, kun verkkopankki otetaan käyttöön, koska on mahdollista, että pankilta saatu salasana on joutunut vieraisiin käsiin siinä vaiheessa, kun se toimitetaan pankin konttorin välityksellä asiakkaalle.

Järjestelmä antaa käyttäjälle mahdollisuuden yrittää sisäänpääsyä verkkopankkiin viisi kertaa. Tämän jälkeen yhteys automaattisesti katkeaa.

Avainlukulistaa tulisi säilyttää erillään käyttäjätunnuksesta ja salasanasta, koska nämä kolme tunnistetietoa mahdollistavat tilin käytön. Jos epäilee tietoturvarikkomusta, voi avainlukulistan lukita, jolloin verkkopankin käyttö estyy. Avainlukulistan voi avata ainoastaan pankki ja vain käymällä henkilökohtaisesti pankissa pyytämässä avaamista.

Tilin käytön jälkeen yhteys verkkopankin palvelimeen on suljettava. On mahdollista, että käyttäjä epähuomiossa tai tietämättömyyttään jättää yhteyden auki esimerkiksi pudottamalla selaimen kuvakkeeksi ja poistuu koneelta. Tällöin yhteys on siltä koneelta kenen tahansa käytettävissä. Joskin käyttämätön yhteys katkeaa tietyn ajan kuluttua.

Verkkopankin käyttö edellyttää, että selain sallii evästeiden (cookies) tallentamisen. Palvelin lähettää asiakkaan koneelle tunnistetiedoston, jonka avulla hallitaan laskunmaksutapahtumaa. Tämä tiedosto ei kuitenkaan tallennu kiintolevylle, vaan se talletetaan käyttömuistiin (RAM). Cookie häviää käyttömuistista kun selain sammutetaan. Näin olen pankkiyhteyden jälkeen selain olisi suljettava varsinkin, jos tietokone on

yhteiskäytössä. Cookien selvittäminen ei kuitenkaan mahdollista tilille pääsyä, koska jokaisella yhteyskerralla on oma avainluku.

Selaimet käyttävät välimuistia eli cachea, jonne ne tallettavat www-sivuja nopeuttaakseen niiden uudelleenlatausta. Tiedot, jotka on suojattu SSL-salauksella eivät tallennu välimuistiin. On kuitenkin aina käytön loputtua syytä tyhjentää välimuisti, jolloin kukaan ei saa tietää, millä sivuilla on käyty. Tämä on varsinkin silloin tärkeää, kun käytetään konetta, joka on muidenkin käytössä esimerkiksi kirjastossa tai työpaikalla.

Verkkopankki käyttää myös Javascriptiä lähinnä syöttötietojen oikeellisuuden tarkistamiseen (viitenumero, tilinumero). Näin ollen selaimessa on sallittava Javascriptien käyttö. SSL suojaa kuitenkin käyttäjän ja palvelimen väliset Javascript-ohjauskomennot, joten tästä ei aiheudu ylimääräistä tietoturvariskiä.

Verkkopankki ei käytä java-appletteja eikä myöskään Microsoftin Active-X komponentteja. [14][15]

7.2.3 Salaustekniikka

Verkkopankki käyttää SSL-salaustekniikkaa (SSL eli Secure Sockets Layer), jota tukevat Microsoftin ja Netscapen selaimet, joiden versionumero on kolme tai sitä suurempi. Näin kaikki asiakkaan ja pankin välinen tiedonsiirto yhteyden luomisesta lähtien toimii suojattuna.

SSL-salaustekniikkaa takaa tietoturvallisuuden kolmella eri tasolla: kiistämättömyyden, luottamuksellisuuden ja eheyden.

Kiistämättömyys merkitsee, että asiakas varmistuu siitä , että yhteys on otettu todella haluttuun paikkaan, siis verkkopankkiin, eikä kolmannen tahon luomaan väärään paikkaan.

Luottamuksellisuus taataan salakirjoittamalla asiakkaan ja pankin palvelimen väliset viestit. Turvallisuuden lisäämiseksi otetaan asymmetrisen salauksen avulla käyttöön vielä symmetrinen salausalgoritmi (RC4), jonka salakirjoitusavaimen pituus on 40 bittiä.. Kun

yhteys on edellä kuvatulla tavalla varmennettu, asiakas lähettää pankin julkisella avaimella kryptatun istuntokohtaisen symmetrisen salakirjoitusavaimen pankille. Tämä avaimen voi ainoastaan pankki selvittää omalla yksityisellä salakirjoitusavaimella. Vaihdettavat viestit kryptataan tällä symmetrisellä salasanalla. Salasanan selvittäminen on nyt erittäin vaikeaa, mutta se saattaa olla murrettavissa. Koska kuitenkin salakirjoitusavain on yhteyskohtainen, riski ei ole suuri: avain tulisi murtaa yhteyden aikana, mutta yhteyden kesto on suurella todennäköisyydellä lyhyempi kuin avaimen purkamiseen käytetty aika.

Eheys taataan laskemalla salakirjoitusavaimen avulla jokaiseen sanomaan MAC-tarkistusluku (MAC=message authentication code). Jos ulkopuolinen muuttaa sanomaa, niin sanoman sisältö ei enää vastaa tarkistuslukua. Näin pankin palvelin huomaa väärennöksen ja hylkää sanoman. Ulkopuolisen tunkeutujan pitäisi näin ollen myös pystyä laskemaan muutettua sisältöä vastaava tarkistusluku, jolla korvattaisiin alkuperäinen tarkistusluku. Tämä on kuitenkin mahdotonta ilman salakirjoitusavainta, jota väärentäjällä ei ole. [14][15]

8 SÄHKÖPOSTI

Sähköpostista on muodostunut yksi eniten käytetyimmistä tavoista ihmisten välisessä kommunikoinnissa. Näin ollen sähköpostin tietoturvariskit ovat tai ainakin tulisi olla tiedossa kaikille sähköpostin käyttäjille.

8.1 Yleistä sähköpostin tietoturvasta

Sähköpostin turvallisuus ja turvattomuus ovat pitkälti kiinni myös Internet-verkon turvallisuudesta. Sähköpostiin liittyvät tietoriskit ja uhkat sähköpostin kautta leviävien virusten lisäksi ovat:

- Sähköpostin lähettäjän luotettava tunnistaminen
- Sähköpostien sieppaaminen verkosta
- Väärään osoitteeseen tai liian laajalle ryhmälle menevät sähköpostit
- Sähköpostien väärentäminen
- Sähköpostihyökkäys
- Mainospostit (SPAM)
- Sähköpostien kierrättäminen läpi vieraiden organisaatioiden
- Sähköpostin häviäminen tai perille menon estyminen

Sähköpostin osoite- ja lähettäjätiedot voidaan väärentää, jolloin kuka tahansa voi lähettää sähköpostin kenen tahansa nimissä siinä missä tavallisen kirjeenkin. Nykyisin käytetyllä tekniikalla ei voi olla varma viestin lähettäjästä.

Internet-verkon luonteesta johtuen lähetetyn viestin reittiä vastaanottajalle on vaikeaa määrätä ennakolta. Koska viesti liikkuu pääsääntöisesti selväkielisenä voidaan se siepata, lukea, muuttaa ja lähettää edelleen vastaanottajalle. Sähköpostin saavuttua perille ei se ole vieläkään turvassa. Käyttäjän omassa postilaatikossa olevat viestit ovat yleensä tekstitiedostossa, joka on luettavissa tavallisella tekstieditorilla. Postipalvelimella tarvitaan käyttäjätunnus ja salasana niiden lukemiseen, mutta jos postit siirretään omalle mikrolle, ovat ne yleensä luettavissa ilman salasanoja.

Tietoturvaongelmia voi syntyä väärään osoitteeseen menevistä viesteistä. Se voi johtua käyttäjän huolimattomuudesta, kirjoitusvirheestä tai väärennetystä viestistä, jolloin lähettäjä uskoo viestin menevän toiselle henkilölle. Toinen vieläkin ongelmallisempi tilanne tapahtuu, jos vastaanottajaksi valitaan yhden vastaanottajan sijasta suurempi joukko. Tämä voi tapahtua käytettäessä alias-nimiä tai postituslistoja, joiden taakse kätkeytyy suuri joukko vastaanottajia. Yleensä tilanne on lähinnä kiusallinen, mutta viestin luonteesta riippuen se voi olla myös vakavampaa.

Yhden huomionarvoisen uhkatekijän muodostavat myös sähköpostihyökkäykset. Siinä sähköpostijärjestelmä tukitaan lähettämällä palvelimelle suuri määrä sähköposteja.

Viimeisen parin vuoden aikana on yleistynyt massapostien eli spammien lähettäminen. Massapostit ovat enemmän tai vähemmän huuhaata sisältävää mainospostia tarjoten mitä erilaisimpia ilmaispalveluita tai maksullisia neuvoja. Oleellisia piirteitä spammeille ovat väärennettyjen lähettäjätietojen koodaaminen viestien otsikoihin sekä sähköpostien kierrättäminen vieraiden organisaatioiden läpi lähetysosoitteiden hämäämiseksi. Muutamat yliopiston sähköpostipalvelimet ovat joutuneet tällaisen kierrättämisen välikappaleiksi.

Sähköpostien häviäminen ei enää ole kovin todennäköistä, mutta sitäkin voi tapahtua. Sähköposteja voi kadota esimerkiksi kiintolevyjen rikkoontumisten yhteydessä tai ohjelmistojen asennus- ja muutostöiden yhteydessä. Sähköpostien perille meno voi myös viivästyä verkossa olevien katkosten seurauksena joskus jopa useita päiviä.

8.2 Sähköpostin suojaus

Sähköpostiviestejä voidaan suojata salaamalla viestit ennen niiden lähettämistä. Sähköpostiviestit voidaan myös allekirjoittaa digitaalisesti, jolloin voidaan varmistua viestin lähettäjän henkilöllisyydestä sekä viestin eheydestä. Jotta henkilöllisyys voidaan varmistaa luotettavasti, tulee käyttää varmenteisiin perustuvia allekirjoitusmenetelmiä.

Sähköpostiviestien salaus on äärimmäisen harvinaista. Amerikkalaisen Phil Zimmermannin kehittämä Pretty Good Privacy eli PGP on saavuttanut lähes standardin aseman sähköpostin salauksessa. PGP:n antama suoja on kohtuullisen hyvä ja yleensä myös riittävä. PGP ei kuitenkaan takaa viestin lähettäjän ja hänen julkisen avaimensa yhteyttä. Voi siis olla mahdollista, että viestin vastaanottajan tiedossa oleva lähettäjän julkinen avain ei kuulukaan lähettäjälle, vaan jollekin kolmannelle osapuolelle.[16]

Toinen yleisesti käytetty viestien salausmenetelmä on S/MIME, joka kuuluu monien sähköpostiohjelmien perusominaisuuksiin. S/MIMEn käyttäjä joutuu hakemaan salausavaimensa joltakin sertifikaatteja myöntävältä yritykseltä kuten VeriSigneltä tai TraWavelta.[12]

Pelkän salauksen lisäksi viestiin voi liittää digitaalisen allekirjoituksen. Tämä tarkoittaa sitä, että viestin sisällöstä lasketaan tarkistussumma ja se salataan lähettäjän salaisella avaimella. Viestin vastaanottaja laskee viestistä vastaavan tarkistussumman. Jos ne täsmäävät, voi vastaanottaja olla varma, ettei viestin tekstiä ole muutettu matkan varrella.[12][16]

9 WLAN

Wlan on pääasiassa tietokoneiden yhdistämiseen käytetty langaton lähiverkkostandardi. Langaton lähiverkko koostuu tukiasemista ja liikkuvista "mobiili"-asemista, jotka on varustettu standardin IEEE 802.11 mukaisella verkkokortilla. Verkkokortti sallii 11Mbit/s siirtonopeuden. Liikkuva asema on tyypillisesti kannettava tietokone. Liikkuva asema voi liikkua langattoman lähiverkon kuuluvuusalueella siirtyen automaattisesti tukiasemasta toiseen, yhteyden lähiverkkoon siitä häiriintymättä. Tukiasemat liittyvät verkkoon normaalin lähiverkkoliitynnän kautta.

Kuva 6. Wlan verkkokortilla varustettu kannettava tietokone.

Wlan-verkkoissa on useita tietoturvaa parantavia suojausmenetelmiä, kuten käyttäjien tunnistus ja liikenteen salaus.

Wlan-verkossa jokaisella laitteelle voidaan määritellä oma yksilöllinen MAC-osoite, joka kirjataan tukiasemalle. Näin tietokone, jonka MAC-osoite ei ole määritelty tukiasemalle ei pääse verkkoon.

Jos kaikille sallitaan pääsy verkkoon, eli ei määritellä MAC-osoitteita, Wlan aiheuttaa turvallisuusriskin. Käytännössä silloin kuka tahansa, jolla on Wlan kortti voi kytkeytyä tukiasemaan ilman käyttäjätunnuksia. On myös mahdollista väärentää langattoman laitteen MAC-osoite, esimerkiksi "opettelemalla" hyväksytyt osoitteet tunkeilija voi muuttaa oman laitteensa MAC-osoitteen vastaamaan verkossa olevaa laitetta ja siten aiheuttaa ongelmia Wlan-verkossa.

Liikenteen salaus Wlan-verkossa salataan WEP-salaus- ja tunnistusmenetelmällä (Wired Equivalent Privacy). WEP käyttää 40-, 56- tai 128-bittistä RC4-jonosalaajaa.

RC4-salaus Wlan-verkossa on helposti haavoittuva tunnetulle ja nopealle hyökkäykselle. Salaus murtuu helposti tietokoneella, jossa on sopiva murto-ohjelma ja Wlan-verkkokortti. 40-bittisen salauksen selvittäminen onnistuu parissa tunnissa. Tämän jälkeen tukiasemaan voi liittyä, vaikka WEP olisikin kytkettynä päälle. Suositeltavaa olisi suojata tukiasemat samalla tavalla kuin Internet-yhteydet, kuten esimerkiksi palomuurilla.[18]

10 TULEVAISUUDEN NÄKYMÄT

Tulevaisuuden ennustaminen on tunnetusti ollut vaikeaa tietotekniikassa. Monet varmaan muistavat Bill Gatesin kuuluisan kommentin 640 kilotavun riittävyydestä ("640k should be enough for anybody" -Bill Gates). Tietoturvallisuuden kehittymisestä ei paljoakaan ole arveltu, mutta uhkakuvia on luotu riittävästi. Monet elokuvat mässäilevät aiheilla, joissa tietotekniikka on pitkällä ja jokin on mennyt pieleen. Ikävä tosiasiahan on nytkin se, että tietoturvallisuus on kilpajuoksua, jossa ikävä kyllä "pahat" ovat voitolla. Tulevaisuudessa toivottavasti päästään eroon monista virheistä, joita vielä kylvetään.

Verkkokaupan kehittyminen on ollut suoraan verrattavissa tietokoneiden, tietokone-ohjelmien ja tiedonsiirron kehittymiseen. Aikaa on kulunut kymmenisen vuotta verkkokaupan alkamisesta ja kasvun odotetaan ennusteiden mukaan olevan voimakasta lähivuosina. Vuonna 1999 Ulkoministeriön kauppapoliittinen osasto arvioi kaupan kasvavan kymmenkertaiseksi vuoteen 2002 mennessä. Suurimmat volyymit sijaitsevat yritysten välisessä kaupassa, jossa katsotaan olevan myös suurimmat kasvuodotukset. Kauppalehti Option [17] mukaan yritysten välinen verkkokauppa esim. USA:ssa kasvaa vuoden 1998 USD 43 miljardista USD 1 000 miljardiin vuoteen 2003 mennessä.

Yritysten ja kuluttajien välisen verkkokaupan volyymien arvellaan kasvavan Suomessa ja Euroopassa huomattavasti hitaammin kuin USA:ssa muun muassa siitä syystä, että USA:ssa postimyynti on perinteisesti kattanut huomattavasti suuremman osan vähittäismyynnistä kuin Euroopassa. Toisin sanoen, amerikkalaisten kuluttajien ostotottumukset suosivat verkkokauppaa. Lisäksi USA:ssa sähköiseen kaupankäyntiin tarvittava infrastruktuuri (esim. logistiikka ja muut etäostosten tekoon liittyvät palvelut) on paremmin kehittynyt kuin Euroopassa. Verkkokaupan kasvua Euroopassa voi hidastaa

myös se, että puhelinverkon kautta Internetiä käyttäviä kotitalouksia laskutetaan käyttöajan mukaan toisin kuin USA:ssa, jossa paikallispuhelut kuuluvat kiinteään kuukausimaksuun. Myös palvelutarjoajien tarvitsemien vuokrajohtojen hinnat ovat Euroopassa Yhdysvaltoja korkeammat. Suurimpana Internetin hyödyntämisen esteenä yrityksissä ovat tietoturvaongelmat.

Eräitä tärkeimpiä sähköisen kaupankäynnin kasvuun vaikuttavia tekijöitä ovat tietosuoja ja –turvallisuus sekä verkkoliiketoimintaan liittyvä kuluttaja- ja yksityisyydensuoja. Euroopan Unioni pyrkii poistamaan sähköisen kaupan lainsäädännöllisiä esteitä, parantamaan turvallisuutta sekä suojaamaan henkilötietoja.

Sähköpostista tulee mitä luultavimmin tulevaisuudessa yhä merkittävämpi kommunikaation väline mm. sen nopeuden ja monipuolisten käyttömahdollisuuksien takia. Esimerkiksi jo nyt voi osan yritysten laskuista tilata tulemaan suoraan omaan henkilökohtaiseen sähköpostiosoitteeseen.

11 TIETOTURVAN MUISTILISTA INTERNETISSÄ

Internetissä liikuttaessa seuraavat asiat kannattaa ottaa huomioon:

- Säilytä salasanasi ja käyttäjätunnuksesi huolella.
- Käytä ajantasalla olevaa virustentorjuntaohjelmistoa.
- Älä avaa sähköpostin liitetiedostoja, jos et tunne lähettäjää.
- Tarkista liitetiedostot ennen avaamista virustentorjuntaohjelmalla.
- Käytä laillisia ohjelmia.
- Käytä tunnettujen palveluntarjoajien sivustoja ladatessasi ohjelmia Internetistä.
- Älä anna henkilötietojasi ja sähköpostiosoitettasi, jos epäilet palveluntarjoajaa.
- Suhtaudu kriittisesti Internetistä löytyviin tietoihin.
- Opasta lasta Internetin käytössä.
- Käytä palomuuria.

KÄSITELUETTELO

Algoritmi	Prosessointiaskelien jono. Suorittaa määrättyä toimintaa, kuten sanoman salaamista tai salauksen purkamista.
Asymmetrinen salausmenetelmä	Kahden avaimen periaatteeseen perustuva salausmenetelmä. Toinen avain on salainen ja toinen avain on julkinen. Viesti salataan vastaanottajan julkisella avaimella ja avataan vastaanottajan salaisella avaimella.
Bitti	Tietokoneen pienin tietoyksikkö, joka on binaariluku 0 tai 1.
DES	(Data Encryption Algorithm) Symmetrinen lohkosalain.
Diffie-Hellman	Diffie-Hellman algoritmi on yleisesti käytössä oleva asymmetrinen algoritmi symmetristen salausalgoritmien avainten vaihtoon.
IDEA	(International Data Encryption Standard) Euroopassa kehitetty 128 bitin avaimeen perustuva symmetrinen lohkosalaaja.
IEEE 802.11	Vuonna 1997 valmistunut määrittely langattomista lähiverkoista radiotaajuuksilla.

Jonosalaus (stream cipher)

Vanha menetelmä jossa peräkkäiset selväkielitekstin “lohkot” syötetään eri salausfunktioiden läpi yleensä merkki kerrallaan. Jonosalaajat ovat tärkeitä suurta nopeutta edellyttävissä reaaliaikaisissa multimediasovelluksissa.

OECD (Organization for Economic Cooperation and Development) Taloudellisen yhteistyön ja kehityksen järjestö, Pariisi, perustettu 1961.

Palomuuri (firewall) Tietokone, joka yhdistää paikallisverkon Internetiin ja päästää turvallisuussyistä vain tietyn tyyppisiä viestejä sisään ja ulos.

PGP (Pretty Good Privacy) Symmetrisen ja Asymmetrisen kryptografian yhdistelmä.

RSA Ensimmäinen asymmetrinen salausjärjestelmä.

SSL (Secure Sockets Layer) WWW-tekniikka, jolla tietokone tunnistaa toisen tietokoneen ja mahdollistaa turvatun yhteyden.

Symmetrinen salausmenetelmä

Salausmenetelmä perustuu sekä lähettäjällä että vastaanottajalla olevaan yhteiseen ja samaan salaiseen avaimeen.

TCP/IP Tapa, jolla tietoverkot viestivät keskenään Internetissä. Lyhenne tulee sanoista Tranmission Control Protocol/Internet Protocol.

UDP (User Datagram Protocol) TCP:tä kevyempi protokolla. Ei vastaa pakettien perille pääsystä ja oikeellisuudesta.

Unix	Alun perin Bell Labsin kehittämä kinkkinen käyttöjärjestelmä. Sitä käytetään monissa Internetin palvelimissa. Tämän hetken suosituin versio on Linux.
URL	(Uniform Recource Locator) Standardoitu verkkoresurssien nimeämistapa, käytetään linkittämään sivuja WWW:ssä.
WEP	(Wired Equivalent Privacy) Wlan –verkon salaus- ja tunnistusmenetelmä.
WWW	(World Wide Web) Hypermediaa käyttävä järjestelmä, jonka avulla voi selata valtavaa määrää kiinnostavaa tietoa. WWW tulee olemaan ihmiskunnan keskeisin tietovarasto 2000-luvulla.

12 YHTEENVETO

Tietoturva Internetissä on kehittynyt paljon vuosien saatossa ja sitä voidaan pitää melko luotettavana järjestelmänä.

Parannettavaakin turvallisuudessa on, kuten erilaisissa ohjelmistoissa. Nettiselaimissa ilmenee uusia tietoturvallisuutta heikentäviä aukkoja jatkuvasti, joihin kyllä tulee aika pian päivityksiä.

Tavalliselle käyttäjälle näiden turvallisuus aukkojen korjauspäivitysten pitäminen ajan tasalla on kuitenkin lähes mahdotonta, johtuen taitojen puutteesta ja toisaalta ajan tasalla pysyminen vaatisi jatkuvaa atk-alan seurantaa.

Suomalaisia verkkopankkeja voidaan pitää hyvin luotettavina, kunhan muistaa pitää tunnukset ja salasanat erillään toisistaan ja niin ettei kukaan ulkopuolinen voi niitä saada haltuunsa.

Lopuksi voidaan sanoa, että vaaditaan melkoista asiantuntemusta saada Internetiä käyttävän tietokone tietoturvan osalta täysin turvalliseksi.

LÄHTEET:

[1] Kivimäki, Jyrki, P.1999. Windows tietoturva. Helsinki: IT Press

[2] Hunt, Graig, P.1998. TCP/IP Verkonhallinta. Jyväskylä: Gummerus kirjapaino Oy

[3] Jaakohuhta, Hannu, Lahtinen Tapani, P.1997. Tietoliikenneverkot. Jyväskylä: Gummerus kirjapaino Oy

[4] ES artikkelit. http://www.geocities.com/viileewebbi/articles/palomuuri.html>18.2.2002

[5] Järvinen, Petteri, P.1995. Internet verkkojen verkko. Juva: WSOY

[6] Valitutpalat. http://www.valitutpalat.fi/lehti/lehti0012/artikkeli01.html>8.1.2002

[7] Levine, John, P.2000. Internet keltanokille. Jyväskylä: Gummerus kirjapaino Oy

[8] Järvinen, Petteri, P.1996. Internet muutostentekijä. Juva: WSOY

[9] Hintikka, Kari, P.2000. Internetin käyttäjän opas 2000. Helsinki: Edita

[10] Nikkilä, Timo, P.2001. Internet 2001. Jyväskylä: Docendo Finland Oy

[11] Tieke. http://www.tieke.fi/kauppa/aapinen/aapinen/johdanto/maaritelma.htm>18.2.2002

[12] Majander, Olli, Tietokone 3/2001

[13] Järvinen, Petteri, Tietokone 5/2000

[14] Osuuspankki. http://www.osuuspankki.fi>18.2.2002

[15] Puusola, Tom, J.1998. http://www.tct.hut.fi/opetus/s38118/s98/htyo/49/pankit.shtml>12.1.2002

[16] Viestintävirasto. http://www.ficora.fi/suomi/tietoturva/sahkoposti.htm>12.1.2002

[17] Kauppalehti Optio 6.4.2000

[18] Elo, Tommi, Tietokone 1/2002

Kajaanin ammattikorkeakoulu

ABSTRACT OF THE FINAL YEAR PAPER

Faculty	Degree programme
Administration and Business	Data Processing
Author(s) Jari Karjalainen	
Title Data Security in Internet	
Alternative professional studies	Instructor(s) Sirpa Haataja
Date 12.2.2002	Total number of pages 38+9

Abstract

The purpose of my final year project was to determine the threats of Internet and how to protect oneself from them. Data security was processed through different topics dealing with e-commerce and e-banking, e-mail and the wireless nets which have generalized over the past few years.

The final year project began with the basics of data security by getting to know the fields of data security, the general break-in methods, protective methods and the special features of the Internet (TCP/IP). After getting deeper into the data security solutions in the Internet, e-commerce, bill payment in netbank, e-mail usage and wireless nets were dealt with. And finally, of course, a short insight into the future was included.

The result was that nowadays the Internet is quite a reliable system, but there are some things to improve, such as the TCP/IP -protocol and the security gaps in Internet browsers. Maybe instead of getting the best selling software the companies should test their products thoroughly. The basic users of the Internet are now mostly in charge of data security of the Internet, which is too much for them. Because if this is supposed to work properly, it would require such a wide knowledge of data security from all the users, that it is not possible. If the providers of Internet services, software and pages took more responsibility of data security, the Internet could be a much safer place.

Confidentiality status	public
Keywords	Data security, netcommerce, netbank, firewall, router, gateway, WLAN
Deposited at	The library of Kajaani Polytechnic

Osasto	Koulutusohjelma
Hallinto ja kauppa	Tietojenkäsittelyn koulutusohjelma

Tekijä(t)

Jari Karjalainen

Työn nimi

Tietoturva internetissä

Vaihtoehtoiset ammattiopinnot	Ohjaaja(t)
	Sirpa Haataja

Aika	Sivumäärä
12.2.2002	38+9

Tiivistelmä

Lopputyön tavoitteena on selvittää, mitä uhkia internet pitää sisällään ja miten uhkilta voi suojautua. Lopputyössä käsitellään tietoturvaa eri alueiden kautta. Alueina ovat verkkokaupassa ja -pankissa asiointi, sähköposti ja viime vuosina yleistyneet langattomat verkot.

Lopputyönkäsittely aloitetaan tietoturvan perusteista, selvittämällä tietoturvan osa-alueet, yleisimmät murtautumismenetelmät, suojautumismenetelmät ja mitä erikoispiirteitä internet sisältää (TCP/IP). Seuraavana lopputyön käsittelyssä syvennytään tietoturvaratkaisuihin internetissä. Lopuksi käsitellään verkkokauppaa, laskujen maksamista verkkopankissa, sähköpostin käyttöä ja langattomia verkkoja unohtamatta tulevaisuudennäkymiä.

Nykyään internetiä voidaan pitää melko luotettavana järjestelmänä, mutta parannettaviakin kohtia on. TCP/IP –protokollaa olisi syytä kehittää, internet selaimista olisi saatava tietoturva aukot korjatuksi. Ehkä ohjelmien perusteellisempi testaus olisi syytä nostaa kunniaan kaupallisuuden tieltä. Internetin tietoturva on annettu liiaksi normaalien käyttäjien huolehdittavaksi, mikä taas toimiakseen vaatisi kaikilta internetin käyttäjiltä niin laajaa asiantuntemusta tietoturva-alalta, ettei se voi onnistua. Jos palvelujen-, ohjelmien- ja sivustojen tekijät ottaisivat enemmän vastuuta tietoturvasta, voisi internet olla turvallisempi paikka kaikille.

Luottamuksellisuus

Julkinen

Hakusanat

tietoturva, verkkokauppa, verkkopankit, palomuuri, reititin, yhdyskäytävä, WLAN

Säilytyspaikka

Kajaanin Ammattikorkeakoulun kirjasto