# E-Business Systems 1

# Portfolio

# Kevät 2005

## *01) Planning the DotCom Business (1) ja (2)*

1.1 i **Tehtävänanto:**

Vertaa online-kirjakauppoja www.amazon.com and www.bn.com (Barnes & Noble)

**Vastaus:**

Nämä sivut näyttävät ulkoasuiltaan melko samannäköisiltä, varsinkin navigaatiopalkki on molemmilla melko samannäköinen. Molemmilla sivuilla on onnistuttu linkkien asettelussa hyvin; Vaikka linkkejä alasivuille on todella paljon, on oikean alasivun löytäminen silti (ainakin useimmiten) helppoa. Barnes & Noblen sivustoa en ole aiemmin käyttänyt joten sen varsinaisesta käytettävyydestä en osaa sanoa oikein mitään, mutta Amazonista olen monta kertaa katsellut / etsinyt kirjoja. Näin olenkin huomannut, että vaikka Amazonin linkit ovatkin selkeästi järjestettyjä ja johdonmukaisia, niin silti sivuille on helppo ”eksyä”, eli kaikkien linkkien painaminen ei viekään sinne minne niiden kuvittelisi vievän. Tämä tosin on ehkä täysin ymmärrettävääkin, koska Amazonin sivu on yksi suurimmista sivuista netissä. Amazonilla on yksi ominaisuus, mitä B & N:llä ei ole (ainakaan en sitä löytänyt), ja se on tuo ”recent searches” tuolla sivun alareunassa. Se on mielestäni hyödyllinen, ei tarvitse mennä selaimen back-nappulalla kokoajan taaksepäin vaan pääsee sieltä suoraan haluamaansa hakuun. Molemmilla näistä sivuista on varmasti omat hyvät ja huonot puolensa, mutta niiden arviointi keskenään on kohtuullisen vaikeaa koska molemmat sivut ovat todella laajoja. Itse en oikein osaa valita edes omaa suosikkiani, molemmat sivut näyttävät ja tuntuvat yhtä hyviltä.

1.1 ii **Tehtävänanto:**

www.chevroncars.com – äänestettiin innovatiivisimmaksi sivustoksi jo vuonna 1998. Mikä mielestäsi tekee sivustosta innovatiivisen tänä päivänä?

**Vastaus:**

Sivustolla ei mielestäni ole mitään mikä tekisi siitä erityisen innovatiivisen. Onhan sivuilla toki flashia, pelejä ja yleisesti ottaen paljon kaikkea pientä sälää lapsille, mutta ne eivät vielä tee sivusta innovatiivista. Jos sivu on näyttänyt tuollaiselta vuonna –98 niin se onkin varmasti ollut todella edistyksellinen, mutta nykyään kaikkea tuota tulee kohtuullisen usein vastaan netissä surffatessa. Mielestäni oikeasti innovatiiviset sivut sisältävät nykyään esim. 3D-mallinnusta, kuten esim. Cult3D (http://www.cult3d.com/gallery/default.asp ).

1.1 iii **Tehtävänanto:**

Vertaa seuraavia kuluttajakauppaa harjoittavia palveluita:

www.sf-mall.com
www.gigagolf.com
www.choicemall.com

**Vastaus:**

Ensimmäisenä pisti silmään se, että kun avasin kaikki kolme sivua suurin piirtein samaan aikaan niin SF-Mall ja Choicemall olivat latautuneet jo aikoja sitten kun Gigagolf oli ladannut vasta 40 prosenttia etusivustaan. Mutta latauksen tullessa valmiiksi syykin tähän selvisi; Gigagolfin sivut olivat täysin flashilla toteutetut. Gigagolfin sivut olivat myös tästä porukasta ehdottomasti tyylikkäimmät, kuten flash-sivut yleensä ovat. Tuota SF-Mallin sivua ei ilmeisesti ole enää olemassa, tai ainakin tuo linkki meni johonkin Web Searchiin, jossa kyllä oli lista kaikenlaisista tuotekategorioista, mutta silti näytti vähän siltä että SF-Mall on lopettanut toimintansa; Tuo osoite on nimittäin myynnissä. Mutta jos noita kahta muuta nyt lähtee arvioimaan niin Gigagolf vie kyllä ehdottomasti voiton. En löytänyt sivuilta mitään mikä toimisi huonosti, kaikki toimii hyvin ja vielä kohtuullisessa ajassakin. Erityiskiitoksen saa tuo ”Build and Buy” - osio joka on toteutettu mielestäni todella siististi ja toimivasti. Mutta ettei koko tämä vastaus nyt menisi Gigagolfin kehumiseksi niin pari sanaa

Choicemallistakin. Sivuston ulkonäkö nyt on aivan eri luokkaa kuin Gigagolfin, paljon konservatiivisempi. Sivun ehdottomasti huonoin asia on tuo vasemman reunan violetti väri-feidaus, se ei sovi sivuille yhtään. Muutenkin sivu on hyvin pelkistetty, mutta se tuo mukanaan sen edun, että sivu latautuu paljon nopeammin kuin esim. nuo flashilla toteutetut sivut. Ideana Choicemall on mielestäni hyvä; Online-ostoskeskus josta saa kaikki palvelut mitä tavallisestakin isosta ostoskeskuksesta. Ja vähän enemmänkin.

1.1 iv **Tehtävänanto:**

Vertaa kahden maailmanlaajuisen kuljetusyhtiöt sivustoja
www.dhl.com (DHL) and
www.fedex.com (Federal Express)

**Vastaus:**

Voisin melkein uskoa että nämä ovat yksi ja sama yritys, ainakin tuon indexin perusteella. Molemmilta sivuilta aukeaa nimittäin suurin piirtein samankokoinen ja suurin piirtein samassa paikassa oleva laatikko, jossa pyydetään valitsemaan oma sijainti. DHL:n sivu tosin voittaa sillä että se asettaa asiakkaan niin halutessa keksin joka muistaa sijainnin myöhemminkin kun asiakas tulee takaisin sivulle. Kun maa on valittu niin molemmat sivut aukeavat kohtuullisen nopeasti, mutta sivuilla on yksi suuri ero. DHL:n sivu on oikeasti suomenkielinen, mutta FedExin sivuilla sijainnin ainut merkitys on noissa verojen ja muiden kuljetukseen liittyvien asioiden (hinta, kesto, jne.) laskemisessa eli sivu määrittää lähtöpaikaksi automaattisesti Suomen. Ulkonäöllisesti sivut ovat mielestäni suurin piirtein yhtä hyviä; Toinen on hieman värikkäämpi ja ehkä hieman sekavampi mutta hienommin toteutettu (DHL), toinen taas on selkeämpi ja pelkistetympi, mutta loppujen lopuksi melko tylsä (FedEx). Yksi suuri miinus FedExin sivuissa ovat myös latausajat. Sivuilla ei ole mitään suurta mitä pitäisi ladata, joten todennäköisesti syy on vain hitaassa palvelimessa.

1.1 v **Tehtävänanto:**

Miten kaikkia yllä olevia erilaisia sivustoja voisi vertailla keskenään? Mitä kriteereitä voitaisiin käyttää yleisesti arvioitaessa sivustoa / palvelua?

**Vastaus:**

Erilaisia sivustoja pitäisi pystyä vertaamaan siten, että varsinaiseen sisältöön ei kiinnitetä huomiota vaan huomio kiinnittyy sivun rakenteeseen ja toimivuuteen. Yksi tärkeimmistä kriteereistä on latausaika eli kuinka ”raskasrakenteinen” sivu on. Tosin, jos sivuja rupeaa arvostelemaan ihan kotikoneelta niin tulokseen vaikuttaa myös palvelimen teho, jolloin tulos ei anna hyvää kokonaiskuvaa sivun nopeudesta ja toimivuudesta. Vertailtavat sivut pitäisi saada kaikki samalle koneelle, jolloin niiden latausaikoja pystyisi vertaamaan oikein. Toinen vertailukriteeri voisi olla käytetyt tekniikat, eli flash-sivuja vertailtaisiin omana ryhmänään, jsp-sivuja omana ryhmänään, php-sivuja omana ryhmänään etc. Mielestäni ei ole mitään järkeä sanoa että ”tämä html-sivu on parempi kuin tämä flash-sivu koska html-sivu latautuu neljä kertaa nopeammin”. Flash-sivut ovat kuitenkin useimmiten tyylikkäitä ja ammattimaisemman näköisiä ja niihin saa sisällytettyä paljon sellaista mitä perus-html-sivuihin ei saa. Sivuilla käytetyt tiedostomuodot eivät tietenkään ole ainoa vertailukohde kun vertaillaan sivustolla käytettyjä teknologioita, vaan pitäisi kiinnittää huomiota myös käytettyjen kuvien kokoon ja tiedostomuotoon ja siihen onko sivut tehty frameseteillä, tauluilla vai kenties div-tageilla. Yleisesti ottaen sivujen vertaileminen keskenään on kohtuullisen vaikeaa, joidenkin asioiden esittämiseen sopivat esim. flash-sivut paremmin ja toisinaan on parempi jos sivu on pelkistetty ja tehty ihan frameseteillä ja html-tiedostoilla. Esim. jos www-suunnittelija tekee itselleen oman esittelysivun niin hän todennäköisesti haluaa sisällyttää sivuille kaiken osaamisensa jolloin sivu on markkinoiva ja näin ollen sivulle tulee flashia (jos ohjelmoija sitä osaa) ja sivut ovat myös todennäköisesti dynaamiset (eli sivuilla on tietokantayhteys jne.). Kun taas jos sivujen käyttötarkoitus on vaikka toimia vain tiedotuskanavana jollekin ihmis-

ryhmälle (esim. Ixoksen sivut) niin siihen riittävät yksinkertaiset sivut, joilla ei tarvitse olla mitään erikoista, kunhan tarpeellinen tieto saadaan välitettyä.

1.2 i **Tehtävänanto:**

Millaisia palveluita seuraavat yritykset tarjoavat asiakkailleen sivuillaan ja mitä hyötyä niistä on asiakkaalle ja yritykselle?

www.iprint.com

**Vastaus:**

I-Print tarjoaa asiakkailleen hyvin monenlaisia painatuksia. Esimerkkeinä voisin mainita vaikka kirjekuoret, tarrat, muistilaput, banderollit, mukit, t-paidat, hiirimatot ja kalenterit. Näihin saa siis kaikkiin haluamansa painatuksen. Tosin aivan mitä tahansa tuotteisiin ei saa, esim. käyntikorteissa on 24 eri taustaa (saman kuvion saa sekä vaaka- että pystysuuntaisiin käyntikortteihin) joista saa valita sen mikä miellyttää eniten omaa silmää. Kahvikuppeja joihin saa haluamansa valokuvan on saatavana vain kahta eri kokoa, 3,1:n desin ja 4,3 desin kuppeja. Eli valikoima ei ole mikään erityisen laaja, mutta uskoisin kuitenkin tämänkaltaisen yrityksen kannattavan koska yritykset kuitenkin tilaavat itselleen mainostuotteita kokoajan, kyseisessä bisneksessä liikkuvat varmasti suuret rahat. Asiakkaalle tällaisen internet-sivun hyöty verrattuna tavallisiin mainostoimistoihin on se, että tilauksen voi tehdä kotoa. Erilaisia tausta- ja kuviovaihtoehtoja saa myös vertailla rauhassa eikä tarvitse mennä minnekään mainostoimiston toimistolle.

1.2 ii **Tehtävänanto:**

Millaisia palveluita seuraavat yritykset tarjoavat asiakkailleen sivuillaan ja mitä hyötyä niistä on asiakkaalle ja yritykselle?

www.ford.com

**Vastaus:**

Tässä kysymyksessä oli hieman eri kysymys noissa englanninkielisissä, eli siellä puhuttiin tuosta Fordin ”suunnittele tulevaisuuden autosi” - palvelusta. Ensin minulla kesti n. 5 minuuttia löytää kyseiseen paikkaan mutta löydettyäni perille ymmärsin kyllä heti kyseisen sivun hyödyn. Tuolla on hauska kokeilla millaisia autoja Fordilla / sen tytärmerkeillä olisi juuri minun tarpeisiini ja paljonko mikäkin auto maksaisi. Tuon sivun hyöty asiakkaalle on mielestäni lähinnä hupi; En usko että kukaan päättää uuden autonsa merkkiä vain yhdellä netissä tehdyllä testillä, useimmat ihmiset haluavat todennäköisesti myös koeajaa autoa ja nähdä sen luonnossa. Fordille tuon sivun hyöty on se, että jos ihminen näkee tuolta jo valmiiksi auton joka sopii omaan perhe- ja rahatilanteeseen niin ostopäätöksessä saatetaan kallistua helpommin Fordin puolelle.

1.3 **Tehtävänanto:**

Millaisia palveluita asiakkaille tarjotaan sivulla www.nasdaq.com?

**Vastaus:**

Nasdaqin tärkein tehtävä on tietenkin välittää osakkeita internetissä. Tämän lisäksi sivuilta löytyy toki paljon muutakin, mm. tuoreimmat pörssikurssit, uutisia bisnesmaailmasta, osake-alan asiantuntijoiden arvioita yrityksistä ja yritysten vuosiraportteja. Sivujen sisältö kattaa oikeastaan kaiken mitä pörssialalla työskentelevä (tai muuten vain alasta kiinnostunut) henkilö tarvitsee. Osa sivun sisällöstä on ikävä kyllä .NET Passport – suojauksen takana, joten sinne en päässyt koska en kyseistä tunnusta omista.

1.4 **Tehtävänanto:**

www.opensource.org – tarjoaa informaation avoimen lähdekoodin ohjelmistoista. Miksi esim. aloittavan yrityksen kannattaa harkita avoimeen lähdekoodiin perustuvien ohjelmistojen käyttämistä?

**Vastaus:**

Aloittelevat yritykset ovatkin juuri niitä joiden kannattaa harkita avoimien lähdekoodien ohjelmistoja. Ehdottomasti tärkeimpänä syynä on tietenkin, jälleen kerran, raha. Open source – ohjelmistot ovat joko ilmaisia tai sitten niistä perittävä maksu on vain murto-osa ”tavallisen” ohjelmiston hinnasta. Usein tämäkin maksu on vapaaehtoinen. Jos yritys esim. harkitsee palvelimen pystyttämistä niin valitsemalla avoimen lähdekoodin ohjelmiston se säästää suuria summia. Esim. Windows 2003 Server Enterprise Edition maksaa muistaakseni noin 7000 dollaria, kun taas Fedora Core 3:sen voi joko hakea suoraan suomalaiselta FTP-palvelimelta tai sitten ostaa. Ostettaessa FC3:sen hinta riippuu myyjästä (lista myyjistä löytyy Fedoran kotisivuilta), mutta hinta on kuitenkin n. 3 – 25 euroa, joka on vain murto-osa tuosta Win2k3Srv:n hinnasta. Tosin, olen itse huomannut että tuon Windowsin asentaminen on todella paljon helpompaa kuin Fedoran, ja jos yritys on uusi niin sillä ei välttämättä ole vielä käytössään osaavaa ATK-tukihenkilöstöä joka pystyisi pyörittämään Fedoraa sujuvasti, joten kyllä open source – ohjelmistoilla on huonotkin puolensa. Toinen hyvä puoli on sitten ohjelmiston kehittäjien määrä, ja tarkoitan tällä nyt sitä että kuka vain voi hakea netistä itselleen open source – ohjelmiston lähdekoodit ja muokata sitä haluamakseen, eli open source – ohjelmistoja voi kuka tahansa parantaa ja kehittää vaikka kotikoneellaan. Tämä tuo mukanaan myös toisen hyvän asian; Nimittäin sen, että kun avoimen lähdekoodin ohjelmistosta löydetään bugi, tietoturva-aukko tai muu vastaava minkä olemassaolo huonontaa ohjelman toimivuutta niin sitä ryhtyvät saman tien parantamaan kymmenet / sadat / tuhannet henkilöt ympäri maailmaa, ja esim. uuden viruksen ilmestyessä se eliminoidaan jo ennen kuin se ehtii saamaan mitään todellista vahinkoa aikaiseksi. Juuri tästä syystä hyvin suuri osa viruksista onkin suunnattu Windowsiin, Internet Exploreriin, Wordiin ja muihin Microsoftin valmistamiin ohjelmistoihin.

1.5 i **Tehtävänanto:**

Mikä on seuraavien yritysten liiketoimintamalli: www.ebay.com

**Vastaus:**

eBay:n tarkoituksena on tarjota internetin käyttäjille kauppapaikka, joka on auki 24 tuntia vuorokaudessa ja 7 päivää viikossa. eBay:hän on käsittääkseni kasvanut maailman johtavaksi ”online-kauppapaikaksi”, joten tämän yrityksen suunnittelu on aikanaan mennyt todella nappiin. eBay rahoittaa toimintansa perimällä pientä maksua jokaisesta tuotteesta joka eBay:hin asetetaan myyntiin (insertion fee) ja myös pientä maksua jokaisesta myydystä tuotteesta (final value fee). Kaikki maksut mitä eBay perii löytyvät täältä: http://pages.ebay.com/help/sell/fees.html . Yritin kovin pohtia että mikä tekee eBay:sta niin hyvän että se on kirkkaasti muita vastaavia online-kauppapaikkoja tunnetumpi, mutta päädyin siihen tulokseen että ehkä se on vain ollut ensimmäisten joukossa perustamassa kauppapaikkaa internetiin ja siitä on vain tullut koko ajan tunnetumpi ja tunnetumpi. Kunnes se on saavuttanut sen tilan missä se tänä päivänä on.

1.5 ii **Tehtävänanto:**

Mikä on seuraavien yritysten liiketoimintamalli: www.christies.com

**Vastaus:**

Tämä yritys olikin minulle uusi tuttavuus. Christie’sin toiminta vaikuttaisi perustuvan hieman samaan kuin eBaynkin, eli se myy tavaraa verkossa ja ottaa myydyistä tuotteista pienen osingon itselleen. Tosin Christie’sissä myytävät tavarat eroavat eBay:sta siinä että Christie’s myy suurempaa ja hienostuneempaa tavaraa kuin eBay. Suurin osa yrityksen myyntiartikkeleista näyttäisi olevan enemmän tai vähemmän keräilytavaraa, esim. tauluja, aseita, viinejä, kirjoja jne. Tämän lisäksi yritys myy myös koruja ja moottoripyöriä joita nyt ei voi mielestäni keräilytavaroiksi laskea. Christie’sin ja eBay:n toiminta eroaa suuresti tavassa miten uusia myyntiartikkeleita voi lisätä sivuille. eBay:hin kuka tahansa Matti Meikäläinen voi tehdä tilin ja asettaa omaisuuttaan myyntiin, mutta Christie’siin tuotteet pitää ilmoittaa sähköpostin tai tavallisen postin

välityksellä tai sitten voi kävellä suoraan Christie’sin lähimpään toimistoon tai edustajan luo, joita löytyy Euroopasta vähän yli 10 kappaletta. Christie’sin pärjäämiseen alalla vaikuttaa todennäköisesti suuresti se, että tämänkaltaisia yrityksiä ei mahdu paljoa yhteen maanosaan (ainakaan kannattavasti) ja Christie’s on jo onnistunut levittäytymään joka puolelle maailmaa. Christie’sin yksi vahva puoli ovat varmasti myös firmassa työskentelevät ammattilaiset; Yrityksen työntekijät osaavat arvioida hyvin taulujen ja muiden sellaisten hintoja ja heidän hinta-arvioihinsa luotetaan.

## *02) Yleinen tietoturva*

Tietoturva on tiedon luotettavuudelle asetettuja kriteereitä. Tietoturvan yleiset tavoitteet ovat

- Saatavuus
- Luottamuksellisuus
- Eheys
- Kiistämättömyys
- Tunnistus
- Todennus

2.1 a) **Tehtävänanto:**

Mitä näillä tietoturvan yleisillä tavoitteilla käytännössä tarkoitetaan (määrittele)?

**Vastaukset: (osittainen lähde: www.tietoturvapalvelu.com )**

- Saatavuus (availability)

  Tiedon saatavuus on sitä että tiedot ovat saatavilla aina kun niihin oikeutettu ihminen pyrkii lukemaan tai muokkaamaan niitä ja tiedot ovat myös saatavilla ilman kohtuutonta viivettä ja estettä. Saatavuus liittyy tietojärjestelmien toiminnan turvaamiseen eli laitteistojen pitää toimia silloin kun tietoa halutaan käyttää. Saatavuus on riippuvainen hyvin monesta tekijästä, näitä tekijöitä ovat: Tiedon luottamuksellisuus, laitteiston määrä, ohjelmistolisenssit, tietoliikennekapasiteetti, laitteisto-, ohjelmisto- ja tietoliikennehäiriöt, käyttäjien toiminta ja oheismateriaalin saatavuus (lomakkeet, nauhat, levykkeet).
- Luottamuksellisuus (confidentiality)

  Luottamuksellisuus on sitä, että ihminen jolla ei ole oikeutta tietoon ei myöskään pääse lukemaan / muokkaamaan sitä. Eli

luottamuksellisuus on tietojen suojaamista luvatonta käyttöä vastaan.

- Eheys (integrity)

  Tiedon eheys on sitä, että mikään / kukaan ulkopuolinen ei pääse muuttamaan tiedon sisältöä. Tiedon muuttamisella tarkoitetaan tässä joko tiedon tuhoamista tai sitä, että lisätään tietoon asioita jotka eivät sinne kuulu. Tiedon eheys ei aina ole uhattuna vain ulkopuolisten tekijöiden toimesta; Tiedon eheys voi särkyä myös tahattomasti, esim. jos tiedonsiirrossa tulee virhe.

- Kiistämättömyys (non-repudiation)

  Kiistämättömyys on erityisen tärkeää sähköisessä kaupankäynnissä, jossa tyypilliset ostotapahtumaan liittyvät vaiheet pitää pystyä sitovasti todistamaan. Kiistämättömyys voidaan saavuttaa soveltamalla eheyden ja todentamisen periaatteita. Kiistämättömyys edellyttää myös tapahtumien varustamista aikaleimoilla, ja myös aikaleimojen lähde pitää pystyä todistamaan luotettavasti jotta ne olisivat luotettavia. Eli kiistämättömyys on sitä että kumpikaan kaupan osapuolista ei pysty kiistämään mitään, esim. sähköisessä kaupankäynnissä ostaja ei pysty kiistämään tilauksen tekemistä eikä myyjä pysty kiistämään sen vastaanottamista.

- Tunnistus (identification)

  Tunnistaminen on sitä että käyttäjä kirjautuu sisään järjestelmään ja tietojärjestelmä vastaanottaa käyttäjän lähettämän tunnistetiedon, jonka perusteella tietojärjestelmä joko sallii tai hylkää yhteyden muodostamisen kyseiseen kohteeseen.

- Todennus (authentication)

  Edellä mainittu luottamuksellisuus edellyttää todentamista, jolla varmistutaan että henkilö / ohjelma tms. on juuri se mikä pitääkin. Todentamista käytetään hyvin paljon esim. pankkien internetsivustoilla. Eli todennuksella ihminen todistaa olevansa juuri se minkä tunnistuksessa mainitsi. Todentamiseen täytyy myös

sisältyä mahdollisuus toimia anonyymisti, koska monissa palveluissa käyttäjän henkilöllisyydellä ei ole niin paljoa väliä, vaan ainoastaan tiettyjen kriteerien täyttymisellä, esim. maksukyvyn. Esimerkiksi kun bussissa käyttää matkakorttia niin kortinlukijan ei tarvitse tietää kuka olet, riittää että matka on maksettu.

2.1 b) **Tehtävänanto:**

Millä keinoilla nämä tietoturvaan liittyvät yleiset tavoitteet pyritään saavuttamaan?

**Vastaus:**

Tähän en onnistunut löytämään mitään hyvää vastausta mutta todennäköisesti sillä että luodaan turvallisempia tietojärjestelmiä, jolloin mitään riskitekijöitä ei pääse syntymään. Mielestäni yrityksellä pitäisi olla erilliset tietoturvastandardit, joita noudatettaisiin kaikissa yksiköissä kaikkien työntekijöiden toimesta. Kun yrityksellä on selkeät pelisäännöt tietoturva-asioihin niin työntekijöiden on helpompi noudattaa niitä.

## *03) Tietoturvariskit ja suojausmekanismit*

3.1 **Tehtävänanto:**

Tietoturva ei ole ainoastaan suojautumista ja vastaamista verkosta tuleviin hyökkäyksiin ja tunkeutumisyrityksiin.

Kun esimerkiksi sinä käyttäjänä haet Internetistä tietoa jostain tuotteesta ja otat selaimellasi yhteyttä palvelimeen saadaksesi haluamaasi tuoteinformaatiota, hyvin usein sinua pyydetään rekisteröitymään ja antamaan tietoja itsestäsi.

Pohdi millaisia tietoturvaan liittyviä kysymyksiä tällaisessa tilanteessa nousee esiin riippuen siitä, oletko käyttäjä tai palvelua tarjoava yritys verkossa? Millaisia yhteisiä tietoturvaan kohdistuvia uhkia osapuolilla on?

**Vastaus:**

Jos olen palvelun käyttäjä niin oikeastaan ainoa asia joka merkitsee tietoja annettaessa on terve järki. Jos sivusto on esim. jollakin tavalla ”hämärän” oloinen, esim. sivun osoite on sellainen johon en normaalisti luota tai sivun sisältö on jollakin tavalla arveluttavaa niin en yleensä anna sivulle edes sähköposti-osoitettani, saati sitten oikeita osoite-, puhelin- tai nimitietojani. Pankkitilini numeroa en myöskään anna missään tilanteessa, vaikka sitä kysyttäisiin esim. Nordean sivuilla (Nordeahan ei koskaan kysy sitä, se kuuluu heidän omaan tietoturvaansa).

Jos taas olen palvelun tarjoaja niin minun pitää miettiä useampia asioita ennen kuin pistän palveluni verkkoon. Ensimmäinen asia tässä lienee Suomen laki. On tiettyjä asioita joita saa kysyä käyttäjältä ja tiettyjä joita ei saa. Kun olen huolellisesti miettinyt ne kohdat joita lain mukaan saan kysyä ja joita uskoisin tarvitsevani niin seuraava vaihe on sitten suojaus. Jos palveluni käsittelee erityisen salassa pidettävää tai muuten arkaluontoista tietoa (esim.

jonkin pankin verkkopalvelu) niin järjestelmän suojaus pitää varmistaa viimeisen päälle, ettei siitä löydy ainuttakaan tietoturva-aukkoa. Järjestelmä pitää myös todella huolellisesti testauttaa ennen varsinaista julkistamista, koska rahavirtoja käsittelevissä järjestelmissä pienikin bugi saattaa olla todella kohtalokas.

Molempia osapuolia koskevia riskitekijöitä on mielestäni vain yksi, ja se on ulkopuoliset jotka yrittävät saada tietoa käsiinsä mutta joiden ei sitä kuuluisi saada. Eli jos ulkopuolinen hakkeri murtautuu järjestelmään ja ”varastaa” pankkikorttini numeron tai muuta vastaavaa arkaluontoista materiaalia niin se on hieman molempien ongelma. Hakkerien ehkäisemiseksi palvelun pitäisi olla niin turvallinen ettei siitä löydy tietoturva-aukkoja ja käyttäjän pitäisi pitää huoli oman koneensa tietoturvasta. Mielestäni muita molempia koskevia riskitekijöitä ei ole.

3.2 a) **Tehtävänanto:**

Tietoturvan uhat voidaan jakaa teknisiin ja ei-teknisiin hyökkäyksiin.

a) Yksi ei-teknisen hyökkäyksen muoto on ns. 'social engineering'. Mitä sillä tarkoitetaan, ja miten siltä voi suojautua?

**Vastaus:**

Social engineering tarkoittaa sitä, että ulkopuolinen henkilö esim. pikkuhiljaa tutustuu yrityksen työntekijään ja vähitellen saa hänet paljastamaan luottamuksellisia tietoja yrityksestä. Olen ollut aikoinani 9 kuukautta Nokialla töissä ja siellä tästä aiheesta pidettiin esityksiä ja palavereja, mutta en nyt viitsi niitä siellä kerrottuja esimerkkejä tähän lähteä kirjoittamaan koska se ei ehkä ole tämän portfolion tarkoitus. Toinen tapa miten social engineeringiä voidaan käyttää on puhdas huijaus. Esim. soitetaan yritykseen ja esittäydytään tärkeänä henkilönä joka on unohtanut salasanansa ja joka tarvitsee suojauksen takana olevia tietoja välittömästi. Useimmiten tätä kuulemma tapahtuu

kesälomien alussa, jolloin yritysten puhelinvaihteissa työskentelee kesätyöntekijöitä, jotka eivät ensinnäkään tunne yrityksen korkeampaa johtoa eivätkä näin ollen myöskään tunnista johtajia äänestä. Toinen syy miksi kesätyöntekijöiltä saa tietoja helpommin on se, että he eivät useimmiten yksinkertaisesti uskalla olla antamatta pyydettyä informaatiota. Sillä jos soittaja oikeasti onkin korkea johtaja, jolla menee tiedon panttaamisen tähden tärkeä kokous tai sopimus sivu suun niin siitä saa kesätyöntekijä todennäköisesti ainakin haukut, pahimmassa tapauksessa jopa potkut. Sitten social engineeringistä on myös kolmas tapa, eli se että kylmän rauhallisesti kävellään yritykseen sisään ja yritetään sieltä varastaa kovalevyjä, salasanoja ja muuta vastaavaa jolla on merkitystä yritykselle.

3.2 b) **Tehtävänanto:**

Tietoturvan uhat voidaan jakaa teknisiin ja ei-teknisiin hyökkäyksiin.

b) Mitä eri teknisen hyökkäyksen tapoja on olemassa, joilta organisaation täytyy suojautua?

**Vastaus:**

Näitä tapoja en keksi kuin kaksi, eli ensinnäkin varsinaiset tunkeutumiset, eli ulkopuolinen henkilö yrittää tunkeutua yrityksen tietokoneisiin etsimällä niistä tietoturva-aukkoja. Tämä on varmastikin teknisistä hyökkäyksistä se yleisempi. Toinen tapa on sitten eräs muunnelma tästä; eli se, että aiheutetaan niin paljon liikennettä yrityksen palvelimelle että sen tietoturva kaatuu jolloin palvelin on oikeastaan alasti ja kaikki pääsevät sinne sisään. Tätä ei käsittääkseni tapahdu enää paljoa nykyään, tämä oli suurempi ongelma 90-luvun loppupuolella.

3.3 **Tehtävänanto:**

Mitä tarkoitetaan salauksella (encryption) tietoturvassa? Mitä eri salaustekniikoita on olemassa ja miten ne eroavat?

**Vastaus:**

Salauksella tarkoitetaan sitä, että yritys muuttaa jonkin tiedon systemaattisesti toiseksi tiedoksi. Salatun tekstin pystyy purkamaan vain siihen tarkoitetut henkilöt, joilla on purkuavaimet hallussaan. Salauksen käyttötarkoitus on se, että jos joku saa salatun tiedon luvattomasti haltuunsa niin hän ei voi purkaa sitä koska ei omista purkamiseen tarvittavaa avainta. Tiedon salaaminen ei varsinaisesti vaikeuta tiedon saatavuutta, mutta vaikeuttaa kyllä suuresti tiedon muuttamista luettavaan muotoon (tai tekee siitä jopa mahdotonta).

Noista ”symmetric encryption”- ja ”asymmetric encryption” - luennoista löytyikin vastaus tähän osaan joka käsitteli eri salaustekniikoita, eli salausmenetelmät voidaan jakaa kahteen pääkategoriaan jotka ovat symmetrinen ja epäsymmetrinen salaus.
Näistä ensimmäinen eli symmetrinen salaaminen voidaan jakaa kahteen alaosioon, jotka ovat transponointi ja substituutio. Näihin molempiin löytyy esimerkki tehtävästä numero 4.5, mutta selitän nyt molempien toimivuuden tässäkin. Transponointi on sitä, että muutetaan teksti järjestelmällisesti viiden kirjaimen kokoisiksi laatikoiksi, esim. kuten tehtävässä 4.5 on tehty:

TSHJN
TSHJNSFGQZJRTTS → SFGQZ → TSJSFRHGTJQTNZS
JRTTS

Substituutio on sitten sitä, että siirretään kirjaimia ennalta määrätyn luvun verran eteenpäin, esim. G = J, S = V, R = U, L = O jne. Esim. Toni substituoituna kahdella olisi sitten T = V, O = Q, N = P ja I = K. Eli Toni-sanasta tulisi sitten VQPK.
Asymmetrinen salaus on sitten sitä, että avaimet ovat aina pareittain, eli julkinen avain (public key) ja yksityinen avain (private key). Toinen avaimista (public) on julkisesta hakemistosta ja private on vain avaimia käyttävän parin hallussa. Eli yksityisellä avaimella salattu tieto voidaan purkaa vain vastaavalla julkisella avaimella ja toisin päin.

3.4 **Tehtävänanto:**

Mikä on VPN (Virtual Private Network)? Mitkä ovat VPN:n toimintaperiaatteet ja mitä se mahdollistaa yrityksille/organisaatioille?

**Vastaus:**

VPN:n avulla yrityksen intranet voidaan ulottaa turvallisesti ”turvattoman” julkisen verkon, esim. internetin yli. VPN:n toimintaperiaate on seuraavanlainen: Kaksi tai useampi sisäverkkoa yhdistetään keskenään tai yksi tietokone yhdistetään organisaation verkkoon, jonka jälkeen päätteiden välillä käytävään tiedonsiirtoon käytetään salausta. Tällöin yhteys on turvallinen eikä julkisessa verkossa käytävän tiedonsiirron sisältö paljastu ulkopuolisille. Tämän lisäksi ennen VPN-yhteyden muodostamista molemmat osapuolet todennetaan vahvasti ennen kuin varsinainen yhteys luodaan, jolloin yhteyden turvallisuus kasvaa entisestään. VPN-yhteys tapahtuu käytännössä tunneloimalla kaikki tiedonsiirto yhden salausmenetelmän sisään. Yleisesti käytössä olevia VPN-protokollia on kolme ja ne ovat IPSec, L2TP ja PPTP. Yrityksille / organisaatioille VPN mahdollistaa siis sen, että esim. etätyöntekijät voivat työskennellä turvallisesti yrityksen fyysisten tilojen ulkopuolellakin ja siirtää koneidensa ja organisaation palvelinten välillä salaista materiaalia.

3.5 **Tehtävänanto:**

Mikä on palomuuri (firewall), miten se toimii ja suojaa organisaation tietoliikennettä ja tietoturvaa?

**Vastaus:**

Palomuuri on joko ohjelmisto tai hardware joka suojaa organisaation verkkoa ulkoapäin tulevilta hyökkäyksiltä. Useimmiten yritysten palomuurijärjestelyt on toteutettu siten, että organisaation ulospäin suuntautuvaa liikennettä ohjaava palvelin on palomuurin takana, ja kaikki yhteydet ulkomaailmaan ovat tämän palvelimen kautta, jolloin kaikki organisaation koneet ovat suojassa ulkoisilta

hyökkäyksiltä. Palomuuri tukkii oletusarvoisesti kaiken liikenteen, mutta siihen voi / pitää määrittää esim. ohjelmat joilla on lupa ottaa yhteys verkkoon (tulostinohjelmat, selaimet, Adobe Acrobat jne.) sekä koneet joilla on oikeus tulla sisälle. Palomuurilla voi myös tukkia vaikka vain yksittäisen portin liikenteen ja tämän hyöty on siinä että esim. uuden viruksen ilmestyessä se saattaa käyttää yhtä tiettyä porttia ja jos tämä ko. portti on tyhjä, eli kyseisen portin kautta ei ole mitään vakioliikennettä niin tämä portti voidaan tukkia palomuurilla jolloin yritys ehkäisee kyseisen viruksen uhan yrityksen sisällä. Palomuuri siis estää ulkopuolelta tulevan haittaliikenteen ja näin suojaa yrityksen tietoliikennettä ja tietoturvaa. Pidin itse n. vuosi sitten omaa konettani puoli tuntia ilman palomuurin suojaa kun asensin siihen uuden kiintolevyn (ja näin ollen myös kaikki ohjelmat uudestaan) ja sain tämän puolen tunnin aikana koneelleni 7 tai 8 virusta. Eli itseni mielestä ainakin palomuuri on pakollinen väline / softa missä tahansa julkiseen verkkoon liitetyssä tietokoneessa.

3.6 **Tehtävänanto:**

Mitä ovat Tunkeutumisen havaitsemis- ja estojärjestelmät (Intrusion Detection System, Intrusion Prevention System), ja miten ne toimivat?

**Vastaus:**

Tunkeutumisen havaitsemisjärjestelmiä on kahdenlaisia: Konekohtaiset (Host IDS) ja verkkopohjaiset (Network IDS). Konekohtaiset tunkeutumisen havaitsemisjärjestelmät toimivat siten, että ne tarkkailevat koneen lokeja ja koneen tiedostojärjestelmään tehtyjä muutoksia ja koittavat etsiä niistä merkkejä mahdollisista tunkeutumisista. Verkkopohjaiset tunkeutumisen havaitsemisjärjestelmät taas toimivat siten että ne sijoittavat verkkoon sensoreita jotka keräävät liikennettä. Tällä järjestelmällä on sitten oma ylläpitäjänsä joka käyttää hallintaliittymää murtojen havaitsemiseen ja tutkimiseen. Molemmat, sekä kone- että verkkopohjaiset tunkeutumisen havaitsemisjärjestelmät siis toimivat samaa periaatetta käyttäen eli ne yrittävät etsiä niiden läpi menevästä tietovirrasta tunkeutumiseen viittaavia merkkejä. Jotkin tunkeutumisen havaitsemis-

järjestelmät osaavat myös reagoida havaittuun tunkeutumiseen katkaisemalla tunkeutujan yhteyden. Tällaisista aktiivisista tunkeutumisen havaitsemisjärjestelmistä käytetään myös nimeä tunkeutumisen estojärjestelmä (IPS).

3.7 **Tehtävänanto:**

Mitä tarkoitetaan salausmenetelmillä, ja miten salaus (encryption) toimii? Missä eri tilanteissa salausta tarvitaan ja käytetään toimittaessa verkossa?

**Vastaus:**

Tuohon salausmenetelmien määrittelyyn ja salauksen toimimiseen löytyy vastaus kysymyksestä numero 3.3. Erilaisia tilanteita joissa salausta käytetään verkossa on monia, mutta kaikkein tärkeimpänä ehkä erilaiset kirjautumissysteemit. Tämän lisäksi myös esim. kun ihminen rekisteröityy jollekin foorumille niin hänen tietonsa lähetetään kantaan salatussa muodossa, useimmiten salausmuotona on aivan perinteinen 256-bittinen md5-hashaus. Ilman tätä salausta kuka vain asiansa osaava voisi tulla yhteyteen väliin ja kaapata suoraan ko. henkilön salasanan ja käyttäjätunnuksen foorumille. Salasanojen hashaamattomuudesta (jos tällaista termiä nyt voi käyttää) muodostuu myös toinen tietoturvariski. Itse käytin ennen kotisivuillani ilmaista kävijälaskuria (palveluntarjoajan osoite: http://www.viihdekeskus.net/) johon sisäänkirjautuessa käyttäjätunnus ja salasana näkyivät suoraan osoiterivillä. Esim. jos tunnukseni olisi eemeli ja salasanani eemeli niin avatessani omalle tunnukselleni määritetyn kotisivun logi-tiedot avautuvan sivun osoite oli tällainen: http://www.viihdekeskus.net/laskuri/counter.cgi?command=viewlogs&username=eemeli&password=eemeli ja jos käytän laskuripalvelua julkisella tietokoneella (esim. kirjasto) niin tuo osoitehan jää selaimen historia-muistiin. Jolloin kaikilla koneen käyttäjillä olisi mahdollisuus muuttaa laskurini asetuksia ja katsella sen logeja siihen asti kunnes selaimen historia-muisti tyhjentyy. Tätä tehtävää kirjoittaessani (7.2.2005) sivu ainakin käyttäytyy vielä tuolla tavalla, en sitten tiedä onko siihen tulossa muutosta.

3.8 **Tehtävänanto:**

Mitä tarkoitetaan digitaalisella allekirjoituksella, ja miten se toimii? Mitä ohjelmistoja on tarjolla sähköisen allekirjoituksen käyttämiseen?

**Vastaus:**

Kun ihminen haluaa tehdä kirjoittamastaan viestistä digitaalisesti allekirjoitetun niin hän käyttää tiettyä funktiota ja laskee viestistä tiivisteen, jonka hän salaa yksityisellä avaimellaan (private key). Tiivisteitä ovat esim. MD5:n (message digest 5) ja SHA1:n (secure hashing algorithm 1 tuottamat sekavat mutta lyhyet merkkijonot, jotka sisältävät viestin kokonaisuuden hashattuina. Kun viestin vastaanottaja vastaanottaa viestin niin hän laskee ensin viestistä samalla tavalla tiivisteen ja tämän jälkeen vertaa laskemaansa tiivistettä lähettäjän lähettämään tiivisteeseen. Hänen pitää toki ensin avata vastaanottamansa tiiviste, ja tämän hän voi tehdä julkisella avaimella (public key), jonka hän saa lähettäjän varmenteesta. Jos viestin vastaanottajan tulokseksi saama tiiviste on sama kuin viestin lähettäjän lähettämä tiiviste niin viesti on ”aito” eikä sitä ole muutettu mitenkään matkan varrella. Eli vastaanottaja voi olla varma että viestin on lähettänyt juuri se henkilö joka viestin on allekirjoittanut. Digitaalinen allekirjoitus on vuodesta -99 lähtien ollut Suomessa oikeudessa vähintään yhtä luotettava kuin tavallinen ”fyysinen” allekirjoituskin. Tämä ”vähintään yhtä luotettava” perustuu siihen että joissain tilanteissa tavallinen allekirjoitus on jopa helpompi väärentää kuin digitaalinen. Noista sähköisen allekirjoituksen käyttöön tarjolla olevista ohjelmistoista sen verran että ohjelman joka muuttaa tekstin md5- tai sha1 – hashiksi voi koodata vaikka itse (jopa minulla on sellainen kotisivuillani), ja myös toiseen suuntaan kääntäviä freeware-ohjelmia on internet täynnä. Tosin kyseiset ohjelmathan eivät varsinaisesti murra tiivistettä (md5 ja sha1 ovat vielä toistaiseksi pysyneet murtamattomina, mutta tuskin pysyvät hirveän kauaa), vaan vertaavat tiivistettä olemassa olevaan tiedostoon joka sisältää käsittääkseni listan hasheja ja niiden selkeäkieliset vastineet ja ilmoittavat jos löytävät sieltä

vastaavan. Tähän voisin kopioida pätkän keskustelusta osoitteesta http://mureakuha.com/keskustelut/2?8050 :

```
$ crunt 1ad99cbe9e425d4f19c53a29d4f12597
<finnish.txt

CRUNT - Small Dictionary Hacker
Version 1.0 - (C) AKX 2004

The hash resolves to 'kissa'.
CPU time used: 0.265 seconds, tries: 91618
```

Tuosta siis näkyy hyvin tuo kuinka nopeaa salasanojen ”murtaminen” on tietokoneella. Mutta takaisin ohjelmistoihin, ehkä yleisimmin käytetty ja hyväksytty digitaalinen allekirjoitus on Microsoftin .NET (dotNET), jota tukevat monet suomalaisetkin organisaatiot, mutta tätä kirjoittaessani en onnistunut löytämään yhtään esimerkkiä, vaikka muutamiin olen itsekin törmännyt. Muihin sähköisen allekirjoituksen käyttämiseen tarkoitettuihin ohjelmistoihin en ole itse vielä törmännyt.

## *04) Symmetric Encryption*

4.1 **Tehtävänanto:**

Encrypt the ASCII bit-stream for the name DAVID using the repeated 8-bit key 01110101.

| | D | A | V | I | D |
|---|---|---|---|---|---|
| Plaintext ASCII | 01000100 | 01000001 | 01010110 | 01001001 | 01000100 |
| Repeated Key: | 01110101 | 01110101 | 01110101 | 01110101 | 01110101 |

**Vastaus:**

| | | | | | |
|---|---|---|---|---|---|
| Ciphertext bitstream: | 00110001 | 00110100 | 00100011 | 00111100 | 00110001 |
| | 49 | 52 | 35 | 60 | 49 |
| | 1 | 4 | # | < | 1 |

4.2 **Tehtävänanto:**

Hakkeri haluaa murtaa salatun viestisi 'DAVID' ja hän tietää että olet käyttänyt 8-bittistä avainta. Hän päättää yrittää ns. 'brute-force' hyökkäystä koodisi murtamiseksi ja yksinkertaisesti kokeilla eri mahdollisuuksia niin kauan kuin oikea avain löytyy.

- Montako eri mahdollisuutta hänen täytyy kokeilla löytääkseen oikean avaimen?
- Jos olisit käyttänyt 10-bittistä avainta, kuinka monta mahdollisuutta enemmän olisi pitänyt kokeilla?

**Vastaukset:**

2^8 = 256 eri avainta.

2^10 = 1024

1024 – 256 = 768 enemmän.

4.3 **Tehtävänanto:**

A newly invented commercial cryptography product uses bit-streams that are blocked and a different key used for each block. Block the ASCII bit-stream for DAVID into blocks of 10 bits as shown below.

Encrypt block 1 using the 10-bit key shown and then encrypt succeeding blocks with the cipher-text from the preceding block (i.e the key for the block 2 is the cipher-text from the preceding block 1 and so forth).

**Vastaus:**

| | Block 1 | Block 2 | Block 3 | Block 4 |
|---|---|---|---|---|
| In 10bit blocks: | 0100010001 | 0000010101 | 0110010010 | 0101000100 |
| Key: | 0101011111 | 0001001110 | 0001011011 | 0111001001 |
| Ciphertext: | 0001001110 | 0001011011 | 0111001001 | 0010001101 |

4.4 **Tehtävänanto:**

Hakkeri haluaa murtaa salatun viestisi 'DAVID' aiemmassa kysymyksessä. Hän ei tiedä että olet käyttänyt 10-bittistä avainta ja 'blocking' tekniikkaa. Monta eri yhdistelmää maksimissaan hänen täytyy enimmillään kokeilla löytääkseen oikean yhdistelmän tämän lyhyen viestin purkamiseksi?

**Vastaus:**

Tästä en ole aivan varma mutta käsittääkseni tämä lasketaan näin:
2^(4x10) = 1 099 511 627 776
Eli **1 099 511 627 776 eri vaihtoehtoa**.

4.5 **Tehtävänanto:**

Find out what the plain-text was if you knew that this 15 character encrypted message TSJSFRHGTJQTNZS was produced using a caesar substitution cipher key 5 and a columnar transposition cipher key 5.

**Vastaus:**

Alkuperäinen: TSJSFRHGTJQTNZS

Ensin transposition pois, jää:

TSHJN

SFGQZ

JRTTS

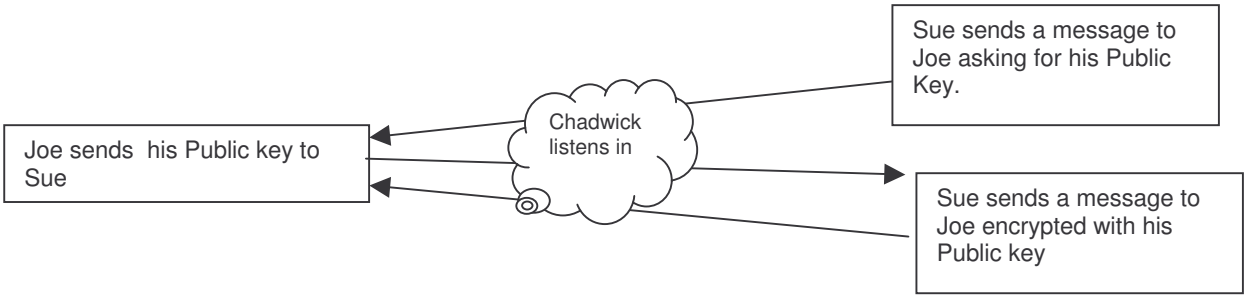
eli: TSHJNSFGQZJRTTS

Sitten substitution pois ja vastaus on: **ONCEINABLUEMOON**

## *05) Asymmetric encryption*

5.1 **Tehtävänanto:**

Chadwick, kansainvälinen hakkeri, 'haistelee' tietoliikennettä verkossa Matin ja Liisan välillä. Mitä vahinkoa / kiusaa Chadwick voi saada aikaan?




**Vastaus:**

Chadwick voi saada avaimia haltuunsa ja muuttaa viestejä joita Matti ja Liisa lähettelevät toisilleen. Jos ajatellaan vaikka että Matti ja Liisa ovat jonkin yrityksen edustajia ja Chadwick haistelee heidän välistä tietoliikennettä niin hän saattaisi saada haltuunsa luottokorttinumeroita, salasanoja, käyttäjätunnuksia ja muita tuollaisia joita ei ole tarkoitettu kaikkien nähtäväksi. Chadwick pystyy myös muuttamaan tietoja, joka saattaa johtaa esim. siihen että Matti siirtääkin Liisalle tarkoitetut rahat Chadwickin tilille.

5.2 **Tehtävänanto:**

Fred on tilaamassa CD -levyä verkosta yritykseltä nimeltään YourPriceRecords.com. YourPriceRecords.com sanoo hyväksyvänsä tilaukset sähköpostitse jos luottokortin numero on ilmoitettu, ja lähettää 'digitaalisen sertifikaatin' Fredin selaimeen.

***DIGITAL CERTIFICATE***

Details: YourPrice Records
Email: YourPrice@demon.net
Public Key: DD:64:A5:7D:23:B7:E1:C2
Validity: 25/1/03 – 24/1/04

10, Smith Gardens London SE10
URL http://www.yourprice.com/

Details verified: 31/12/02 Class: 1

CA: BT Trustwise, 29 Back Alley, Hackney London Digital Signature Type: MD5
Digital Signature: BD:44:15:3D:2A:57:F1:72:EO:5D:89:B1:E5:8D:B3:ED

5.2 a) **Tehtävänanto:**

Fredin selaimen tietoturvasääntö (security policy) on pyytää digitaalista sertifikaattia kaikilta joilta hän ostaa tuotteita. Miksi Fred on päättänyt toimia kyseisellä tavalla?

**Vastaus:**

Tässä on varmaankin virhe, nimittäin tuolla englanninkielisissä tehtävissä ei puhuta mitään Fredin selaimen tietoturvasäännöstä, vaan ainoastaan Fredin tietoturvapolitiikasta. Vastaan siis jälkimmäiseen. Tällainen ajattelutapa perustuu siihen että vain luotettavilla yrityksillä on digitaaliset sertifikaatit, itse ainakin luottaisin enemmän yritykseen jolla tällainen on. Digitaalisen sertifikaatin omaaminenhan on merkki siitä et CA (Certificate Authority) on identifioinut sertifikaatin hallussapitäjän, ja tällöin ostaja voi olla varma että internetissä toimivalla kaupalla on myös oikea fyysinen osoite ja puhelinnumero. Tällainen varmuus tietenkin parantaa ostajan luottamusta myyjään.

5.2 b) **Tehtävänanto:**

Mitä Fred voi tehdä sertifikaatissa olevalla informaatiolla salatakseen luottokorttitietonsa?

**Vastaus:**

Ensin laskea luottokorttitiedoista tiiviste ja sitten salata tiiviste private keyllä, jolloin vain YourPrice Records ja Fred ovat kykeneviä avaamaan viestin.

5.2 c) **Tehtävänanto:**

Fred on vastaanottanut sertifikaatin mutta hänen selaimensa ei hyväksy sitä. Mistä tämä voi johtua?

**Vastaus:**

Koska sertifikaatin viimeinen voimassaolopäivä on 24.1.2004.

5.2 d) **Tehtävänanto:**

Kuka on (digitaalisesti) allekirjoittanut yllä olevan sertifikaatin?

**Vastaus:**

Tuo CA joka tuossa on mainittu, eli BT Trustwise jonka osoite on 29 Back Alley, Hackney London.

5.2 e) **Tehtävänanto:**

Jos Hakkeri-Chadwick muuttaisi yllä olevaa sertifikaattia niin että YourPrice Recordsin julkinen avain olisi DD:64:A5:7B:23:B7:E9:C2 ja sähköpostiosoitteena lukisi Yorprice@demon.net, mitä voisi tapahtua jos Fred hyväksyisi sertifikaatin tarkistamatta sitä ensin?

**Vastaus:**

Jos tuo Yorprice@demon.net on Chadwickin oma mailiosoite niin Fredin luottokorttitiedot menisivät Chadwickille eivätkä yritykselle jolta Fred yrittää levyjä tilata.

5.2 f) **Tehtävänanto:**

Miten Fred voi tarkistaa että yllä olevaa sertifikaattia ei ole muutettu?

**Vastaus:**

Fredin pitää ajaa dokumentti läpi ja verrata tulosta tuohon digitaaliseen allekirjoitukseen. Jos Fred saa tulokseksi saman tiivisteen niin sitten dokumenttia ei ole muutettu matkan varrella, mutta jos Fred saa eri tiivisteen niin joku on muuttanut dokumenttia.

5.2 g) **Tehtävänanto:**

Jos Fred ei yleensä hyväksy sertifikaatteja kyseisen sertifikaatin allekirjoittajalta, miten hän voi varmistaa että kyseinen sertifikaatti on aito?

**Vastaus:**

Itse asiassa ei varmaan mitenkään, ellei sertifikaatin hallussapitäjällä (eli YourPrice Recordsilla) sitten ole sertifikaattia joltain toiseltakin taholta. Tämän toisen tahon pitäisi sitten olla sellainen johon Fred luottaa.

5.3 **Tehtävänanto:**

Missä tapauksissa CA voi peruuttaa annetun sertifikaatin?

**Vastaus:**

Jos sitä hallussaan pitävä taho väärinkäyttää sertifikaattia jollain tavalla tai ei ole CA:n mielestä enää luotettava taho. Tietenkin myös jos yritys lopettaa toimintansa niin CA peruuttaa sertifikaatin.

5.4 **Tehtävänanto:**

Mitkä ovat asymmetrisen salauksen (asymmetric encryption) edut ja haitat?

**Vastaus:**

Edut:

- Avainten välittäminen helpompaa kuin symmetrisessä salauksessa.
- Ainoastaan yksi avain (private key) täytyy pitää salassa.
- Avainten elinikä paljon pidempi kuin symmetrisessä salauksessa, jopa vuosia. Käyttöikä tosin riippuu avaimen pituudesta.
- Avaimia voidaan jakaa ilman että tarvitsee paljastaa salaisuuksia.

Haitat:

- Pitkät avaimet, paljon pitemmät kuin symmetrisessä salauksessa.
- Hitaus. Tämä on seurausta pitemmistä avaimista.
- Salaista avainta ei voi muistaa ulkoa, josta muodostuu säilytysongelma.
- Tällä hetkellä ainakin myös salauksen ikä on haitta; Salaus on niin uusi että voi löytyä uusia tapoja ratkaista salaus.

## *06) Computer Misuse and Foresics*

Allaolevat tapaukset ovat esimerkkejä tietosuojaan ja tietoturvan liittyvistä rikkeistä. Määrittele jokaisessa tapauksessa:

a) kuka on syyllistynyt rikkeeseen ja miten

b) mitä tapauksen 'uhrin' tulisi tehdä tulevaisuudessa estääkseen vastaavan tapauksen uusiutuminen?

6.1 **Tehtävänanto:**

An industrial placement student at ICL, Bracknell, had such poor work performance that he was dismissed and escorted from the premises. However, he had been busy learning UNIX and created a 'supervisor' account for himself on the ICL system. The next day he dialled in, destroyed a few files and sent obscene email messages to ICL staff. The cost to ICL was £33,000. [IEE Seminar 'Computer Crime']

**Vastaukset:**

a)

Rikkeeseen on syyllistynyt ehdottomasti työharjoittelija. Kysymykseen ”miten” vastaus löytyykin tuosta ylhäältä; Oikeastaan kaikki mitä hän teki oli rikollista. Ensinnäkin, hän ei saisi tehdä järjestelmänvalvoja-tunnuksia ilman työharjoittelua ohjaavan henkilön lupaa. Hän ei myöskään saisi ottaa luvattomasti yhteyttä ICL:n palvelimeen. Eikä hän luonnollisesti saisi myöskään poistaa tiedostoja tai lähettää rivoja sähköpostiviestejä ICL:n työntekijöille.

b)

Yrityksen pitäisi pitää huoli siitä että työharjoittelijoilla ei ole oikeuksia / mahdollisuuksia luoda järjestelmänvalvoja-tunnuksia mihinkään. Sillä kaikki rikok-

set mitä työharjoittelija tuossa teki olisivat jääneet tapahtumatta jos harjoittelijalla ei olisi ollut järjestelmänvalvoja-tunnuksia.

6.2 **Tehtävänanto:**

A Bank employed a contract programmer and sat him next to one of their account managers working on the web-banking side of the business. The account manager had two password levels to gain access to the online customer accounts - the programmer oversaw the managers keystrokes and deduced one of the passwords - the other password was written on a piece of paper stuck to the side of the managers terminal. At the end of his contract the programmer left. The next day £1.2 million went missing. [IEE Seminar ]

**Vastaukset:**

a)

Varsinaiseen rikkeeseen syyllistyi tilattu ohjelmoija, sehän nyt on päivänselvää että rahan varastaminen on rikos. Toisaalta, myös pankki teki tässä väärin koska jos salasanojen takana on hyvinkin suuria rahasummia niin niitä salasanoja ei pitäisi koskaan kirjoittaa millekään paperilapuille. Tai jos ne on aivan pakko pistää muistiin jonnekin niin paperilappua voisi säilyttää esim. kukkarossaan tai muussa vastaavassa ”henkilökohtaisessa” paikassa. Mutta lähtökohtaisesti noin tärkeät salasanat pitää aina muistaa.

b)

Ensimmäinen asia jossa toimintaa voidaan parantaa on tietenkin tuo edellä mainittu salasanojen tallentaminen. Eli ne pitää painaa mieleen. Toinen asia jonka voisi sitten tehdä paremmin on uusien tulokkaiden sijoittaminen. Ei ehkä ole hyvä että he istuvat juuri sen henkilön vieressä joka tekee organisaation tärkeintä projektia, koska yrityksellä ei ole mitään varmuutta työntekijän rehellisyydestä. Ei heitä kyllä voi omaan huoneeseenkaan pistää, koska pitäähän aloittelijoilla olla lähellä joku jolta kysyä neuvoa ongelmatilanteissa. Mutta kuitenkin, heidän sijoittamistaan työpaikalle pitäisi harkita tarkemmin.

6.3 **Tehtävänanto:**

A University lecturer did some consultancy work building an ecommerce website for a client. However, the client deducted part of the fee to pay for the personal telephone bill incurred by the lecturer. The lecturer retaliated by placing a logic bomb in the clients computer with a message that he was owed money, customer transactions were being modified and the sooner the matter was settled, the less damage would occur. [Computing magazine]

**Vastaukset:**

a)

Rikkeen teki opiskelija joka asetti loogisen pommin asiakkaan koneeseen. Tällaiset asiat pitäisi pyrkiä ratkaisemaan ensin puhumalla ja sopimalla ja sitten jos se ei tuota tulosta niin sitten vaikka käräjäoikeuden kautta. Mutta tuollaista ”ratkaisutapaa” ei saisi koskaan käyttää.

b)

Uhri olisi voinut välttää tämän tekemällä tehdystä työstä tarkan sopimuksen etukäteen. Jos sopimuksessa olisi ollut kohta että työn tekijä korvaa tuon tyyliset menot itse niin siinä tapauksessa opiskelijalla ei olisi ollut mitään oikeutta vaatia asian korjaamista. Ja jos opiskelija olisi silti asettanut pommin asiakkaan koneeseen niin asiakas olisi voinut vaatia opiskelijalta korvauksia oikeusteitse. Jos sopimuksessa taas ei ollut tuollaista kohtaa niin silloin asiakas ei mielestäni olisi oikeutettu pidättämään puheluista tulleita kustannuksia opiskelijan palkasta. Jos sopimusta ei tehty ollenkaan (uskoakseni se todennäköisin tilanne) niin silloinkaan asiakkaalla ei ole mielestäni oikeuksia pidättää puhelukustannuksia palkasta.

6.4 **Tehtävänanto:**

A 1990 audit of a company's access log showed accesses to the network during the night when the company was closed. A check revealed no obvious

misdemeanour but an all-night vigil was kept for several days. One night a logon was made from a telephone number eventually traced to a business student in Norway. Apparently, he regularly logged on to eight UK companies 'to get inside knowledge for a college project'. The other 7 companies were unaware. [NCC]

**Vastaukset:**

a)

Rikkeeseen syyllistyi tässä tuo norjalainen college-opiskelija, kirjautuminen organisaatioiden koneisiin on laitonta, vaikka siellä ei tekisikään mitään harmia.

b)

No eivät uhriksi joutuneet yritykset oikeastaan muuta voi tehdä kuin koittaa parantaa järjestelmiensä tietoturvaa niin hyväksi että tällainen laiton sisäänkirjautuminen on mahdotonta. Itse en ainakaan keksi parempia tapoja.

6.5 **Tehtävänanto:**

An newly-redundant employee of a Midlands company returned to his workplace and hid in a utility room. During the night, after blocking overflow pipes, he turned on all taps in washrooms above the computer suite where the webserver was located. Next morning, staff found water running down the stairs. It took 24 hours to dry out computers, 36 hours to rebuild corrupted data. The company did most of its business via it’s website - one weeks disruption cost £150,000 in lost business. [NCC]

**Vastaukset:**

a)

Tässä kysymyksessä rikkeeseen syyllistyi työntekijä, joka vesivahingon aiheutti koska tuollaisen tason sabotaasi on aina rikos.

b)

Yritys voisi pistää oviin sellaiset kulkutunnistimet joista ei pääse sisälle kuin avaimella. Ja erotetuilta työntekijöiltä pitäisi ottaa avaimet pois samana päivänä kuin heidän työsopimuksensa loppuu, ei mitään ”tuo sitten kun jaksat” -mentaliteettia. Muille työntekijöille pitäisi myös tehdä selväksi että ihmisiä ei saa päästää sisään samalla ovenavauksella ellei ole ehdottoman varma että kyseinen henkilö työskentelee yrityksessä. Toinen vaihtoehto saattaisi olla liiketunnistimet yrityksen käytäviin ja tärkeimpiin tiloihin, jotka aktivoituisivat työpäivän päättyessä. Jos sabotaasia tehnyt entinen työntekijä olisi tässä tapauksessa laukaissut sellaisen niin vartioliikkeen edustaja olisi ehtinyt paikalle todennäköisesti viimeistään puolessa tunnissa ja vesivahinko olisi voitu estää.

6.6 **Tehtävänanto:**

A company's travelling salesmen uploaded orders from laptops to the company mainframe by telephone. To improve speed and reduce phone bills, management disabled the system that logged incoming calls to the computer. Also, one of the salesmen had created an account called DEMO with a password DEMO. A hacker found the DEMO account, placed a program in it and used this to randomly generate passwords to break into other computers in Europe and the USA. In one week the hacker ran up a £15000 phone bill. [NCC]

**Vastaukset:**

a)

Rikkeeseen syyllistyivät mielestäni kaksi tahoa; Yrityksen johto joka lopetti puheluiden sisäänkirjautumis-järjestelmän sekä myyntimies joka loi DEMO-tunnuksen. Ensinnäkin, jokin sisäänkirjautumis-järjestelmä olisi hyvä olla järjestelmissä joiden kautta voi tehdä noinkin suuria rahallisia vahinkoja. Mielestäni tämän pitäisi olla itsestäänselvyys. Toinen rike oli siis tuon DEMO-tun-

nuksen luominen, tuon kaltaisia tunnuksia ei saisi koskaan tehdä minnekään, ei ainakaan jos tunnuksella on kaikki samat oikeudet kuin muillakin tunnuksilla.

b)

Yrityksen pitäisi ottaa myyntimiehiltään pois tunnustenluontioikeudet. Eli firmalla pitäisi olla yksi ATK-tukihenkilö (tai ATK-tukiosasto) joka luo uusia tunnuksia ja kellään muulla ei ole oikeuksia tehdä uusia tunnuksia. Tunnusten pitäisi olla myös sellaisia että ne esim. sisältävät vähintään 8 merkkiä, joista ainakin yhden pitää olla numero ja ainakin yhden iso kirjain. Eli suurin piirtein samankaltainen salasana-järjestelmä kuin meillä koulussakin. Sitten toinen parannus mikä pitäisi tehdä on tuon kirjautumisjärjestelmän uudelleenpystyttäminen. Ja sen pitäisi olla myös turvallinen, eihän noilla salasanoilla tee yhtään mitään jos järjestelmä muuten vuotaa kuin siivilä.

6.7 **Tehtävänanto:**

A company manager was surprised to receive a parcel containing a copy of confidential customer files with credit card details held on the company’s web-server. A letter of explanation was enclosed stating that the company's network had been hacked and that copies of the customer files would be sent to the customers with a letter pointing out that computer security was so lax that confidentiality could not be guaranteed. The letter also pointed out that to save further embarrassment the company could pay £500,000 and then the entire matter would be forgotten. [IIA seminar]

**Vastaukset:**

a)

Tässä kysymyksessä ei ole muita vaihtoehtoja rikkeen / rikoksen tekijälle kuin henkilö / henkilöt jotka sivuille murtautuivat. Tosin tässä ei puhuta mitään yrityksen palvelimen turvallisuustasosta, mutta jos palvelimen tietoturvataso on ollut jotakuinkin ”toivotaan et ketään ei tuu sisään meiän serveriin”-tasoa niin sitten

rikkeeseen syyllistyi henkilö joka vastaa palvelimen tietoturvasta. Koska luottokorttinumeroita sisältävän palvelimen pitäisi aina olla hyvin turvattu.

b)
Tähän tuskin on muuta lääkettä kuin parantaa palvelimen tietoturvaa niin hyväksi ettei sinne yksinkertaisesti pysty murtautumaan. Eli yrityksen pitäisi esim. palkata asiansaosaava tietoturvakonsultti joka osaisi tehdä palvelimesta turvallisen ja sitten vielä varmistaa turvallisuus monilla eri testauksilla.

6.8 **Tehtävänanto:**

A NatWest Bank employee was caught after he successfully transferred $32.5 million to a private account in Switzerland. He was about to board an aeroplane when he was arrested. NatWest security explained that he had been caught because the limit on any one transfer was $30 million.[IEE Seminar]

**Vastaukset:**

a)
No tässä kyllä rikkeeseen syyllistyi NatWestin turvallisuusosasto. Jos maksimisiirto on 30 miljoonaa dollaria mutta tämä työntekijä kuitenkin siirsi onnistuneesti 32.5 miljoonaa niin silloin vika on pankin järjestelmissä, ja varsinkin niiden turvallisuudessa.

b)
Luulisi että suuria rahasummia käsittelevillä pankeilla on tehokkaat varmistukset noin suurille rahasummille, ettei niitä pääse noin vain häviämään. Oikeastaan ainut keino tällaisten ikävien tapahtumien estämiseen tulevaisuudessa on pankin tietojärjestelmien turvallisuuden ja pankin omien käytäntöjen muuttaminen siten että esim. yli miljoonan dollarin nostot vaativat pankinjohtajan tai hänen edustajansa läsnäolon ja hyväksynnän. Jos pankki toimisi näin niin työntekijä joutuisi siirtämään 30 kertaa 999000 euroa joka olisi paljon riskialttiimpaa kuin siirtää kerran 29.5 miljoonaa euroa.

## *07) Forming Contracts*

(teimme tämän osuuden parityönä, minä ja Kalle Palokankare)

7.1 **Tehtävänanto:**

Yritys tarjoaa mahdollisuuden ladata verkkopalvelustaan tietyn laatuisia kuvia 10 euron hintaan. Jos maksaa 2 euroa lisää, kuvan laatu on parempi ja sopivampia ammattimaiseen käyttöön esim. esitteissä ja lehdissä. Palvelun teknisessä toteutuksessa on kuitenkin tapahtunut virhe, ja asiakas pystyy lataamaan myös laadukkaampia kuvia 10 euron hintaan ilman lisämaksua. Onko palvelua tarjoavalla yrityksellä laillisia perusteita vaatia jo kuvia ladanneilta kahden euron maksua jälkikäteen?

**Vastaus:**

Yrityksellä ei ole laillisia perusteita vaatia 2€ korvausta jälkikäteen. Yritys on itse vastuussa virheestään. On otettava huomioon, että asiakas on saattanut huomaamattaan tilata arvokkaampia kuvia.

7.2 **Tehtävänanto:**

Doylesbooks.co.uk myy kirjoja verkossa Hollannissa sijaitsevan palvelimen kautta. Doylesbooks.co.uk tekee sopimuksen toisen kirjoja tarjoavan palvelun, Yhdysvaltalaisen AngelBooks.com:n kanssa. Sopimuksen mukaan Doylesbooks.co.uk sijoittaa linkin palveluunsa jonka kautta asiakas ohjautuu AngelBooks.com:n sivuille, ja Doylesbooks.co.uk saa provision jokaisesta asiakkaasta joka tätä kautta ostaa sopimuksen toiselta osapuolelta. Sopimuksessa sanotaan, että kiistatapauksissa sovelletaan 'New Yorkin lakeja (laws of New York)'. Muutaman kuukauden kuluttua Doylesbooks.co.uk huomaa ettei ole saanut yhtään sopimuksen mukaista provisiota ja haluaa nostaa kanteen. Missä maassa kanne tulisi nostaa?

**Vastaus:**

Kanne tulisi nostaa Amerikassa, jossa vastaaja harjoittaa liiketoimintaa. Lakina tulisi alustavasti soveltaa ”New Yorkin lakeja” kuten sopimuksessa sovittiin. Muussa tapauksessa Amerikan valtion yhteistä lakia.

7.3 **Tehtävänanto:**

Yritys X myy ohjelmistoja verkkopalvelussaan. Palvelun pääsivulla on kaksi linkkiä: lisenssiehdot ja lataa ohjelma. Asiakas kuitenkin lataa ohjelman suoraan valitsematta ensin linkkiä 'lisenssiehdot'. Muutamia viikkoja myöhemmin yritys saa tietää että asiakas on rikkonut lisenssiehtoja ja haluaa haastaa tämän oikeuteen. Miten juttu mielestäsi ratkeaa?

**Vastaus:**

Tämä juttu tulisi todennäköisesti ratkeamaan siihen että asiakas ei ole syyllistynyt mihinkään varsinaiseen rikokseen. Yrityksen olisi pitänyt sijoittaa lisenssiehdot niin että niitä ei voi sivuttaa ohjelmaa asennettaessa, ne voisi laittaa vaikka samalla tavalla kuin Microsoftin ohjelmistoissa eli ne on pakko selata läpi ennen kuin pääsee eteenpäin asennuksessa.

7.4 **Tehtävänanto:**

Sähköinen allekirjoitus on myös oikeudessa kelpaava todiste, mutta mitkä tekijät heikentävät sellaisen 'sähköisen allekirjoituksen' luotettavuutta joka on ainoastaan kuva joka esittää käsin kirjoitettua allekirjoitusta ja joka on liitetty sähköpostiin?

**Vastaus:**

Digitaalinen kuva jossa on ihmisen käsin kirjoittama nimikirjoitus ei ole digitaalinen nimikirjoitus, eikä se kelpaa todistusaineistona oikeudessa. Käsinkirjoitetun nimikirjoituksen saaminen on äärimmäisen helppoa (esim. luottokorttioston yhteydessä) ja sen skannaaminen digitaaliseksi on vähintään yhtä helppoa.

7.5 **Tehtävänanto:**

Verkkopalvelu mainostaa kilpailua jossa annetaan palkinto kaikille jotka ratkaisevat esitetyn ongelman. Kilpailusäännöt sanovat että ratkaisu on vastaanotettava 24. marraskuuta 2005 kello 16:00 mennessä. Lähetät oman vastauksesi ja saat myöhemmin tietää että se on ollut oikea. Yritys kuitenkin kieltäytyy maksamasta luvattua palkintoa koska he ovat vastaanottaneet lähettämäsi sähköpostin aikarajan jälkeen. Miten kyseiseen tilanteeseen tulisi suhtautua lain valossa?

**Vastaus:**

Kilpailusäännöistä ilmenee selvästi että ratkaisu on oltava vastaanottajalla tiettyyn aikarajaan mennessä. Yritys ei ole velvollinen maksamaan luvattua palkintoa osallistujalle jos vastaus ei saapunut ajoissa. Vaikka kilpailija olisikin lähettänyt ratkaisunsa ajoissa, mutta kilpailun järjestäjä vastaanottanut sen myöhässä, ei kilpailija ole oikeutettu palkintoon, koska järjestäjä ei ole vastuussa tiedon kulusta ajoissa.

7.6 **Tehtävänanto:**

Vakuutusyhtiö rakentaa verkkopalvelun jossa mahdolliset asiakkaat voivat lähettää taideteoksensa tiedot vakuutusta varten. Vakuutettavan kohteen arviointi ja vakuutussopimuksen laatiminen tapahtuu verkon välityksellä. Yritys lähettää asiakkaalle vakuutustarjouksen ja asiakas vastaa sähköpostitse hyväksyvänsä tarjouksen ja ottavansa vakuutuksen, mutta vastaus ei koskaan saavu perille koska asiakas ei ole suorittanut kuukausimaksuaan omalle internet -palvelun tarjoajalleen. Sillä välin kun vastaus on 'matkalla' vakuutettava kohde varastetaan. Joutuuko vakuutusyhtiö korvaamaan teoksen ja miksi?

**Vastaus:**

Ei tietenkään joudu. Vakuutusyhtiön ja asiakkaan välinen suhde on vasta tarjous-vaiheessa joten mitään varsinaista sopimusta ei ole vielä tehty. Vakuutusyhtiö ei myöskään voi olla vastuussa siitä että maksavatko heidän tarjoustensa vastaanottajat internet-liittymiensä kuukausimaksuja.

7.7 **Tehtävänanto:**

Goodfood Inc. on maailmanlaajuinen terveys-tuotteita valmistava yritys joka on rekisteröity Englantiin ja myös operoi sieltä käsin. Yrityksen Internet -palvelin on kuitenkin Uudessa-Seelannissa ja verkkopalvelussa käytetään .com -päätettä. Ranskalainen yritys Sante Marge, joka on samalla alalla, solmii yhteistyö -sopimuksen Goodfood Inc. kanssa. Sante Marge vastaanottaa sopimuksen mukaisesti suuren määrän tuotetta X joka saapuu ja laskutetaan frangeina. Yritys kuitenkin huomaa, että kun laskun summa on muutettu punnista frangeiksi, on valuuttakurssi ollut virheellinen. Saman virheen huomataan tapahtuneen useissa aikaisemmissakin laskuissa. Goodfood kiistää virheen. Missä maassa ranskalaisen yritysen tulisi haastaa Goodfood Inc. oikeuteen ratkaistakseen riidan?

**Vastaus:**

Mielestämme Englannissa. Koska jos esim. minä myyn Ruotsissa asuvalle henkilölle jotakin vaikka sadalla eurolla ja hän ei maksa niin oikeusjuttu käydään Ruotsissa koska eihän Suomen laki voi tuomita Ruotsin kansalaista Suomessa. Tässä tehtävässä kyseessä olleessa kiistatilanteessa saattaa tosin vaikuttaa myös EU:n oma monikansallinen tuomioistuin.

## *08) Risks and Business Continuity*

8.1 **Tehtävänanto:**

Tietoturvan uhat voidaan jakaa tahalliseen vahingon tuottamiseen (malicious damage), laiminlyönteihin/huolimattomuuteen (negligence), onnettomuuksiin (accident), varkauksiin (theft) ja katastrofeihin (disaster). Mihin kategoriaan alla olevat tapaukset kuuluvat? Olisiko tapahtunut voitu estää ja miten?

a) Sihteeri formatoi levyn luullen että se ei sisällä mitään tärkeää, mutta kuulee myöhemmin että se sisälsi tärkeän raportin toimitusjohtajalle.

b) Juuri irtisanotulle työntekijälle annetaan mahdollisuus hakea työpöydältään henkilökohtaiset tavarat. Samalla hän kuitenkin poistaa tärkeitä liiketoimintaan liittyviä tietoja järjestelmästä ja lähettää asiakkaille yrityksen kannalta haitallista sähköpostia

c) Kassa ottaa vastaan käteistä asiakkailta normaalin aukioloajan ulkopuolella ja antaa heille käsin kirjoitetun kuitin ilman että ostosta kirjataan viralliseen tietokonepohjaiseen kassajärjestelmään. Rahat päätyvät kassan omaan taskuun.

d) Sihteeri päättää kopioida toimistossa käytetyn grafiikkaohjelman pojalleen, joka tarvitsee sitä opiskeluissaan.

**Vastaukset:**

8.1 a) Negligence (laiminlyönti)
8.1 b) Malicious damage (tahallinen vahingon tuottaminen)
8.1 c) Theft (varkaus)
8.1 d) Theft (varkaus)

8.2 **Tehtävänanto:**

Luokittele olla olevat uhat sen mukaan, ovatko ne organisaation sisäisiä vai ulkoisia uhkia.

a) Sihteeri kirjoittaa salasanasi tarralapulle ja kiinnittää sen tietokoneeseen ettei pomo unohtaisi sitä.
b) Yrityksen tarkastaja on huomannut että kolmella alihankkijallasi on sama osoite kuin yhdellä tavaranostajallasi. Kukaan ei ole huomannut tätä aikaisemmin
c) Tuntematon soittaja soittaa työntekijälle joka on vastuussa yrityksen lähiverkosta. Soittaja huijaa tämän paljastamaan salasanasi.

**Vastaukset:**

8.2 a) Sisäinen.
8.2 b) Sisäinen.
8.2 c) Ulkoinen.

8.3 **Tehtävänanto:**

In 1985, the Atomic Energy of Canada Limited (AECL) introduced a new radiation therapy machine THERAC-25 for treatment of cancer. AECL had a decade of experience in building such machines, and incorporated many of the old tried and tested safety features into the new THERAC-25. However this was the first time they had designed a machine controlled entirely by computer. An error in the program logic had the result that the operator could unknowingly deliver over 100 times the correct dosage. As this happened only occasionally it was sometime before the error was discovered by which time at least six patients had received potentially lethal doses of radiation.

Olisiko AECL:n pitänyt huomioida tämä riski? Jos olisi, niin millainen riskitekijä kyseinen tilanne on?

**Vastaus:**

Tietenkin se on riski. Jos kuusi potilasta joutui kuolemanvaaraan, on mielestäni päivänselvää että se on riski ja vakava riski onkin. Tällaiset ”uraauurtavat” sairaanhoidon ohjelmat pitäisi aina testata todella tarkasti ennen niiden hyödyntämistä varsinaisessa hoidossa, koska jos ohjelma pystyy tappamaan ihmisiä tai saattamaan ihmisiä hengenvaaraan virheen sattuessa on niiden käyttö ilman testaamista todella riskialtista. Itse en ainakaan haluaisi mennä röntgen-kuvauksiin ja kuulla sairaanhoitajan suusta lausetta: ”Me tässä testaammekin sinulla tällaista uutta järjestelmää jonka saimme käyttöömme viime viikolla, ohjelmassa ei ole ainakaan vielä ilmennyt mitään puutteita tai parannettavaa, toivottavasti ei ilmene nytkään…” Tämän järjestelmän riski kuuluu kategoriaan ”integrity” eli ehjyys, koska jos ohjelma pystyy virheen sattuessa antamaan edellä mainitun kaltaisia hengenvaarallisia yliannostuksia, vika on ennen kaikkea ohjelman toimivuudessa.

8.4 **Tehtävänanto:**

What might be the benefits and disadvantages to an organisation in obtaining accreditation with a recognised information system security standard such as BS7799 ?

**Vastaus:**

Tärkein hyöty tällaisesta on tietenkin yrityksen tietoturvan parantuminen. Tämän lisäksi vastuunjako yrityksen tietoturvasta selkiytyy ja paranee, tietoturva-ohjeistuksen laatu paranee (jos sitä edes on ollut olemassa aikaisemmin), tietoturva-asioiden hallinnointi yhtenäistyy ja yrityksen tietoturva-käytännöt standardisoituvat, eli tietoturvaan liittyviin asioihin tulee yksi oikea menettelytapa, eikä asioita hoideta enää miten sattuu. Ja tietenkin jos yrityksen toimialaan liittyy salaisten / arkaluontoisten dokumenttien käsittely niin yritys voi tällaisen omatessaan tällä osoittaa että sen tietoturva on kunnossa, jolloin asiakkaat luottavat yritykseen paremmin.

On tällaisesta sertifioinnista sitten haittojakin yritykselle, ja yksi suurimmista on varmastikin hinta, joka on melko korkea. Sertifikaatin saamiseen menee n. vuosi, joten tällaista ei myöskään hankita aivan hetkessä. Tällaisen hankkiminen syö myös yrityksen resursseja, koska henkilökuntaa pitää kouluttaa uuden standardin käyttöön ja laitteistoa pitää hyvin todennäköisesti päivittää.

8.5 **Tehtävänanto:**

Lue alla oleva muistio. Mitä epäloogisuuksia/virheitä se sisältää?

To All Staff From The Chief Executive Officer

**Ashley Online Banking plc: Disaster Recovery Plan**

I am pleased to announce that the bank has reviewed its procedures in the event of a disaster affecting its IT systems, and these have been documented in the Disaster Recovery Plan.

The documentation will be kept in my office (on the fourth floor of the Ashley Building, above the main computer server room). The plan will also be available on-line on the employee's electronic notice-board.

In the event of a disaster, back-up facilities will be provided by arrangement with Cadle & Co,. on the seventh floor of the Ashley Building, who use equipment we believe to be similar to our own. We shall be asking for volunteers to assist in testing these arrangements, by simulating the conditions of a disaster at 10.00am next Saturday morning. All our main business partners have been contacted and have agreed to help with this exercise.

You are reminded that if you hold crucial data on your desk computer, you should make regular copies onto floppy discs and keep these where they can easily be found.

Should a disaster affect the Ashley Building out of working hours, may I remind staff that they should ring the number of the IT server room help desk right away.

**Vastaus:**

1. Lauseessa "on the fourth floor of the Ashley Building, above the main computer server room" on mielestäni epäloogisuus, harvemmin sanotaan että tilaisuus pidetään jonkin huoneen yläpuolella.
2. Lauseessa " who use equipment we believe to be similar to our own" on myös epäloogisuus, jos yritys tekee jonkin suunnitelman se tuskin antaa projektiin osallistuvan yrityksen käyttää laitteita joiden yhteensopivuudesta omiensa kanssa ei ole 100-prosenttista varmuutta.

3. Kyseistä dokumenttia ei ole allekirjoitettu, ainut tieto lähettäjästä on tuo ”From The Chief Executive Officer” ilmoituksen otsikossa.