Niina Autio

TUOTTEISTETTU TIETOTURVAKARTOITUS PIENILLE JA KESKISUURILLE YRITYKSILLE

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikka ja liikenne
Tietotekniikka
Kevät 2011

Kajaanin ammattikorkeakoulu

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikka ja liikenne	Koulutusohjelma Tietotekniikka
Tekijä(t) Niina Autio	
Työn nimi Tuotteistettu tietoturvakartoitus pienille ja keskisuurille yrityksille	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Ohjaaja(t) Jukka Heino
	Toimeksiantaja Janne Venäläinen / Tähtimediat Oy
Aika Kevät 2011	Sivumäärä ja liitteet 27 + 16

Insinöörityön tavoitteena oli suunnitella tuotteistettu tietoturvakartoitus pienille ja keskisuurille yrityksille. Työn taustalla on monien pk-yritysten puuttelliset tietoturvaratkaisut jo perustason tietoturvasta lähtien. Työn toimeksiantajana oli kajaanilainen IT-alan palveluja tarjoava Tähtimediat Oy. Tavoitteeseen kuului suunnitella, millä keinoin palvelua markkinoidaan ja mitä asiakastapaaminen sisältää. Näiden lisäksi tavoitteena oli suunnitella sovellustyökalu, johon syötetään haastattelun avulla kerätyt tiedot. Tämän jälkeen ohjelman tulisi analysoida haastattelusta saadut vastaukset sekä lähettää tulokset ja parannusehdotukset sekä Tähtimediat Oy:n edustajalle että asiakkaalle. Näiden lisäksi sovellukseen kuului suunnitella myös haastattelussa käytettävät kysymykset.

Alussa insinöörityössä esitellään työssä esiintyvät keskeisimmät käsitteet "Tietoturva" ja "Tietoturvakartoitus". Tietoturvalla tarkoitetaan tietojen, järjestelmien ja palvelujen suojaamista niin normaali- kuin poikkeusoloissakin erilaisten toimenpiteiden avulla. Tietoturvakartoituksen avulla taas saadaan kuva siitä, kuinka hyvin tietoturva on yrityksessä hoidettu ja onko siinä mahdollisesti jotain parantamisen varaa. Tämän jälkeen insinöörityössä kuvataan, kuinka palvelua on tarkoitus markkinoida puhelimitse ja sähköpostitse sekä kerrotaan lyhyesti asiakastapaamisen alkutoimet. Tämän jälkeen työssä suunnitellaan, kuinka sovellustyökalu toteutetaan HTML- ja PHP-kielten avulla.

Työn tuloksena saatiin suunnitelma siitä, kuinka ohjelman ensimmäinen versio eli prototyyppi toteutetaan. Työssä esitellään esimerkkejä koodeista, joita hyödyntämällä sovelluksen prorotyyppi tullaan ohjelmoimaan toimivaksi kokonaisuudeksi. Lisäksi työssä on esitetty yleisiä tekniikoita, joiden avulla on mahdollista liikennöidä turvallisesti Internetin yli. Näitä tekniikoita ovat muun muassa VPN(Virtual Private Netvork), OpenVPN, SSL (Secure Sockets Layer) sekä htaccess.

Lopuksi insinöörityössä pohditaan, kuinka palvelua voitaisiin jatkossa kehittää esimerkiksi hyödyntämällä tietokantoja kokoamalla kysymykset tietokantaan. Kehitysideoihin kuuluvat myös erilaiset dokumentit, kuten tietoturvapolitiikka sekä toipumissuunnitelma. Näiden lisäksi insinöörityön liitteenä on sovelluksessa käytettävät kysymykset.

Kieli	Suomi
Asiasanat	Tietoturva, Tietoturvakartoitus
Säilytyspaikka	☒ Verkkokirjasto Theseus ☒ Kajaanin ammattikorkeakoulun kirjasto

Kajaanin ammattikorkeakoulu
University of Applied Sciences

THESIS
ABSTRACT

School School of Engineering	Degree Programme Information Technology
Author(s) Niina Autio	
Title A Productized Data Security Survey for Small and Medium Sized Companies	
Optional Professional Studies Data Security	Instructor(s) Mr Jukka Heino, Senior Lecturer
	Commissioned by Mr Janne Venäläinen, Chief Executive Officer
Date Autumn 2011	Total Number of Pages and Appendices 27 + 16

This Bachelor's thesis was commissioned by a company called Tähtimediat Oy. The purpose of this thesis was to plan a service that provides a change to survey the level of data security in small and medium sized companies. The thesis should include a plan of how the service will be marketed, what kind of meeting with the client it will be, and an application program where all the information of the interview should enter. The application program should include questions of data security. It should also include two kinds of functions. The first function should enable entering data to the application program and the other function should compare the answers of the questions. After comparison, the application program should give a short summary of how data security has been taken care of in the company. The summary should be sent to the email addresses of Tähtimediat Oy and the client.

Firstly, it was explained what the terms data security and data security survey mean. Secondly, a few techniques that allow to operate securely over the Internet were introduced. These techniques were VPN (Virtual Private Network), OpenVPN, SSL (Secure Sockets Layer) and htaccess. How the service will be marketed and how the meeting with the client will proceed was planned next. Then it was planned how the application program will act and how it will be executed.

As a result, 77 multiple choice questions connected with data security, marketing, and the meeting with the client were thought of. Furthermore, the execution of the application program was planned. The application program was decided to execute with the help of the HTML and PHP languages.

In conclusion, the version of the application program which was planned will be the prototype. In the future the application program will be developed. This thesis also includes a few extension improvement ideas of how the service could be developed. For example, there are a few documents that could be included in the service.

Language of Thesis	Finnish
Keywords	Data Security, Data Security Survey
Deposited at	☒ Electronic library Theseus ☒ Library of Kajaani University of Applied Sciences

LYHENTEET JA TERMIT

IPsec	(Internet Protocol security) Liikenteen salaava protokollajoukko
L2TP	(Layer 2 Tunneling Protocol) VPN-tunnelointiprotkolla
PPTP	(Point-to-Point Tunneling Protocol) VPN-tunnelointiprotokolla
LAN	(Local Area Network) Lähiverkko
OSI	(Open Systems Interconnection) Seitsemänkerroksinen tiedonsiirtoprotokollien yhdistelmä
UDP	(User Datagram Protocol) Yhteydetön protokolla
TCP	(Transmission Control Protocol) Tietoliikenneprotokolla
IANA	Internet Assigned Numbers Authority
TLS	(Transport Layer Security) Salausprotokolla
ESP	(Encapsulating Security Payload Protocol) Pakettivirrat turvaava IPSec-standardin protokolla
NAT	(Network Address Translation) Tekniikka, joka muuntaa julkiset Internetin IP-osoitteet yksityisiksi IP-osoitteiksi
HMAC	(Hash-based Message Authentication Code) IPsec-protokolla
CRL	(Certificate Revocation List) Kumottujen varmenteiden lista
PEM	(Privacy Enhanced Mail) Tekstimuotoinen koodausmuoto
PAM	(Pluggable Authentication Modules) Käyttäjän tunnistusjärjestelmä
HTTP	(Hypertext Transfer Protocol) Tiedonsiirtoprotokolla
RSA	Salausalgoritmi

ALKUSANAT

Haluan kiittää työn tilaajana toiminutta Tähtimediat Oy:n toimitusjohtaja Janne Venäläistä sekä työn valvojana toiminutta Jukka Heinoa. Työn kielellisestä ohjauksesta haluan kiittää Eero Soinista suomen kielen osalta ja Kaisu Korhosta englannin kielen osalta.

SISÄLLYS

1 JOHDANTO

Tämän insinöörityön tavoitteena on suunnitella kokonaisuus tuotteistetusta tietoturvakartoituksesta pienille ja keskisuurille yrityksille. Työ tehdään Tähtimediat Oy:lle, ja työn taustalla on monien pk-yritysten puutteelliset tietoturvaratkaisut perustason tietoturvasta lähtien. Tuotteistetun tietoturvakartoitus -palvelun avulla voidaan kartoittaa yrityksen tietoturvan nykytilanne sekä ehdottaa toimenpiteitä, joilla yrityksen tietoturvaa saataisiin parannettua.

Tähtimediat Oy on kajaanilainen IT-alan palveluja tarjoava yritys. Yrityksen pääsääntöisenä tehtävänä on kehittää asiakasyritysten ja kumppaneiden toimintaa tietoteknisellä puolella sekä turvata niiden sähköisen liiketoiminnan jatkuvuutta. Tähän kuuluu muun muassa ohjelmistojen asennus, käyttöönotto sekä käytön opastaminen. Lisäksi yrityksen palveluihin kuuluvat muun muassa mikrotukipalvelut, tietoturvaratkaisut sekä varmuuskopiointipalvelu.

Tavoitteena on suunnitella kokonaisuus, johon kuuluu palvelun markkinointi, käynti asiakkaan luona, sovellustyökalu, johon syötetään asiakkaalta haastattelun avulla kerätyt tiedot sekä kysymykset, joita sovelluksessa ja haastattelussa käytetään. Sovelluksessa tulee olla syöttötoiminto, johon syötetään tietoturvakartoitushaastattelusta saadut tiedot sekä vertailutoiminto, joka osaa analysoida syötettyjen tietojen perusteella, missä tietoturvan osa-alueissa yrityksellä on puutteita ja mitkä osa-alueet ovat kunnossa. Vertailutoiminnon jälkeen sovelluksesta saadaan tietokoneen tai kommunikaattorin näytölle tietoturvakartoituksen tulokset sekä parannusehdotukset. Sovellus lähettää tulokset ja parannusehdotukset myös Tähtimediat Oy:n edustajan sekä asiakkaan sähköpostiin.

Näiden lisäksi työ sisältää kuvauksen siitä, mitä tietoturva- sekä tietoturvakartoitus-käsitteillä tarkoitetaan.

2 TIETOTURVA KÄSITTEENÄ

Tietoturva on tietojen, järjestelmien ja palvelujen suojaamista niin normaali- kuin poikkeusoloissakin. Tietojen, järjestelmien ja palvelujen suojaus tapahtuu erilaisten hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvan kolme perusperiaatetta ovat luottamuksellisuus, eheys ja käytettävyys. Näiden kolmen ominaisuuden turvaamisesta rakentuu tietoturva. [1.]

Käsite luottamuksellisuus tarkoittaa sitä, että tietoihin, järjestelmiin ja palveluihin pääsevät käsiksi vain ne, joilla niihin on oikeus päästä. Luottamuksellisuuteen kuuluu myös, ettei tietoa, järjestelmiä ja palveluja paljasteta luvatta tai muutoin saateta sivullisten tietoon. Eheydellä taas varmistetaan se, etteivät tiedot, järjestelmät tai palvelut ole päässeet muuttumaan tai tuhoutumaan laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena. Kolmannen ominaisuuden eli käytettävyyden avulla pyritään varmistamaan, että tiedot, järjestelmät ja palvelut ovat aina niihin oikeutettujen ja niitä tarvitsevien käytettävissä ilman esteitä. [1.]

Näiden kolmen ominaisuuden lisäksi tietoturvaan liittyy myös useita muita tärkeitä käsitteitä. Näitä ovat muun muassa todentaminen (autentikointi), kiistämättömyys sekä tunnistaminen. [1.]

Todentamisella tunnistetaan osapuolet luotettavasti eli varmistutaan siitä, että osapuolet ovat heitä, keneksi itseään väittävät. Yleensä tämä tapahtuu kohteen ominaisuuksien avulla eli sen avulla, mitä kohteella on hallussaan tai mitä kohde tietää. Vahvassa todennusmenetelmässä yhdistetään edellä mainitut menetelmät. Usein järjestelmä toteuttaa tunnistamisen ja todentamisen yhtäaikaisesti. Tästä on esimerkkinä henkilötietojen tarkistus, jolloin käyttäjän tiedot tarkastetaan esimerkiksi ajokortista ja samalla tunnistetaan käyttäjä. [1.]

Kiistämättömyydessä varmistetaan todisteet luomalla, etteivät tietojen käsittelyn tai siirron osapuolet voi jälkikäteen kiistää osuuttaan siihen. Tästä on esimerkkinä sähköisessä viestinnässä käytettävät toimenpiteet, joilla varmistutaan viestin lähettäjän ja viestin vastaanottajan tietojen oikeellisuudesta. [1.]

Tunnistaminen on menettelytapa, jolla kohde, kuten käyttäjä tai järjestelmä, yksilöidään. Tunnistaminen voi tapahtua esimerkiksi käyttäjätunnuksen tai sormenjäljen avulla. [1.]

Tämän lisäksi tietoturva voidaan jakaa kahdeksaan osa-alueeseen, joita ovat hallinnollinen tietoturva, henkilöstöturvallisuus, fyysinen tietoturva, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä käyttöturvallisuus. Näistä osa-alueista kerrotaan tarkemmin seuraavassa.

2.1 Hallinnollinen tietoturva ja henkilöstöturvallisuus

Hallinnollinen tietoturva käsittää organisaation toimintapolitiikat, toiminnan linjaukset, toiminnan johtamisen, toimintojen organisoinnin, toimintojen sijoituksen organisaation rakenteeseen, resurssit sekä tietoturvaan liittyvien vastuiden määrittelyt. Hallinnollinen tietoturva tarkoittaa tietoturvallisuuden osa-alueiden kokoamista yhtenäiseksi kokonaisuudeksi. Näitä kokonaisuuksia voidaan johtaa joko omana toimintonaan tai jonkin muun johtamisfunktion osana. [2.]

Henkilöstöturvallisuus tarkoittaa henkilöstöstä johtuvaa riskienhallintaa, ja sen perustan muodostaa osaava ja sitoutunut henkilöstö, joiden toimenkuvaan kuuluvat tietoturvavastuut sekä -tehtävät. Henkilöstöturvallisuuden keskeisiä asioita ovat prosessit, jotka liittyvät työhönottoon, muutoksiin toimenkuvissa sekä palvelusuhteen päättymiseen. Uuden työntekijän tausta, sopivuus ja osaaminen selvitetään ennen työhönottoa riippuen tehtävien vaativuudesta tai luottamuksellisuudesta. [3.] Henkilöstöturvallisuuteen kuuluvat myös henkilöstön koulutus, ohjeistus, työntekijöiden aiheuttamat tahattomat vahingot ja tahalliset sabotaasit sekä uuden työntekijän salassapito- ja kilpailukieltosopimukset työsopimusta allekirjoitettaessa[4, s. 112].

2.2 Fyysinen tietoturva ja käyttöturvallisuus

Fyysisen turvallisuuden tehtävänä on turvata organisaation toiminta ilman häiriötä kaikissa olosuhteissa ottaen huomioon niiden erityistarpeet sekä riskit. Fyysinen tietoturva kattaa muun muassa kulunvalvonnan, kameravalvonnan, murtosuojauksen, vartiointipalvelun sekä vesi-, sähkö- ja ilmastointivahinkojen torjunnan. [3.] Tämän osa-alueen tavoitteena on siis estää erilaiset laitevarkaudet, palo- ja vesivahingot sekä ulkopuolisten luvaton pääsy organisaation tiloihin.

Käyttöturvallisuudella tarkoitetaan sellaisten toimintaolosuhteiden luontia ja ylläpitoa, jotka takaavat tietotekniikan turvallisen käytön. Tällaiset toimintaolosuhteet saadaan toteutettua huolehtimalla muun muassa toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokitiedostojen valvonnasta, varmuuskopioinnista sekä häiriöraportoinnista. Lisäksi tulee huolehtia ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä. Käyttöturvallisuuteen kuuluu myös tietojärjestelmien suojaaminen erilaisten haittaohjelmien varalta. [3.]

2.3 Tietoliikenne- ja tietoaineistoturvallisuus

Tietoliikenneturvallisuudella pyritään turvaamaan tietoliikenteen jatkuvuus eli organisaation tietoliikennetoiminnot ja verkkojärjestelmät suunnitellaan ja rakennetaan siten, että valitun arkkitehtuurin avulla voidaan varautua erilaisia organisaatioon kohdistuvia uhkia vastaan. Tähän tietoturvan osa-alueeseen kuuluvat muun muassa tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja muutosten valvonta, kirjaus ongelmatilanteista, käytön valvonta, verkon hallinta sekä viestinnän salaus ja varmistaminen. Lisäksi osa-alue sisältää merkittävien tietoturvapoikkeamien tarkkailun, kirjauksen ja selvittämisen sekä tietoliikenneohjelmien testauksen ja hyväksymisen. [3.]

Tietoaineistoturvallisuudella tarkoitetaan eri tallennusmuodoissa olevien tietojen suojausta siten, etteivät luottamukselliset tiedot joudu ulkopuolisten käsiin. Tähän kuuluvat paperiasiakirjat, optiset ja magneettiset muistivälineet, mikrofilmit, äänitteet sekä muut vastaavat tekniset laitteet. Tietoaineistoturvallisuuteen kuuluu myös käsittelysäännöt tietoaineiston koko elinkaaren ajalle eli tiedon synnystä sen tuhoamiseen asti. Lisäksi tietoaineistoturvallisuus sisältää tietojen turvaluokitusjärjestelmän (julkinen, luottamuksellinen, salainen) sekä varmistuksen siitä, että tietoaineiston eheys ja käytettävyys säilyy. [3.]

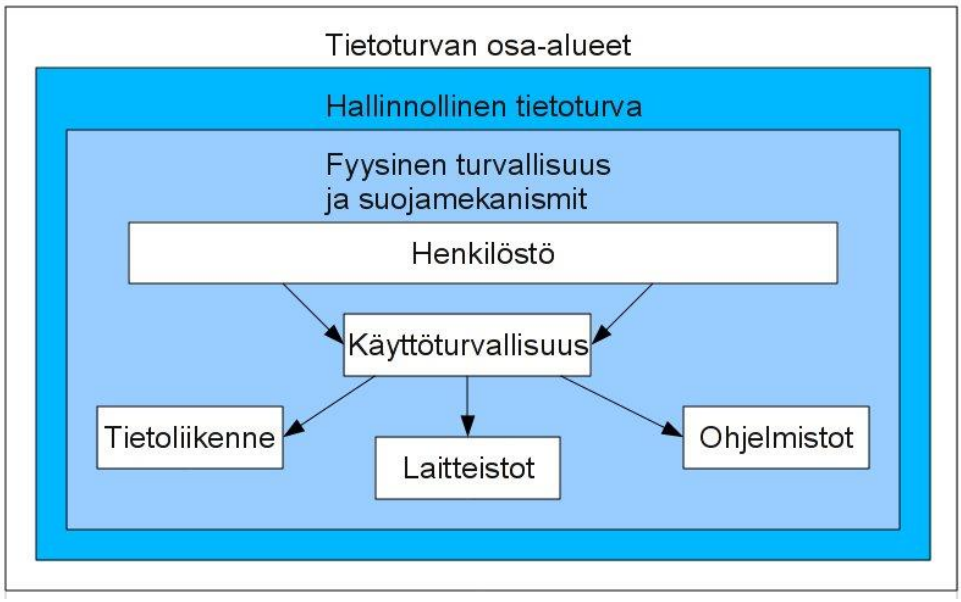
2.4 Laitteisto- ja ohjelmistoturvallisuus

Laitteistoturvallisuus on laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään, kuka laitteet omistaa ja laitteiden turvaluokka, sekä laitteiden valvontaa, niiden kapasiteettien suunnittelua ja varautumista sähkönsyötön katkok-

siin. Laitteistoturvallisuudella siis turvataan laitteiston elinkaarta. Laitteiston elinkaareen kuuluvat laitteiden asennus, takuu, ylläpito, erilaiset tukipalvelut ja -sopimukset sekä laitteiden turvallinen hävittäminen elinkaaren lopussa. Laitteiston ylläpidon avulla huolehditaan siitä, että poikkeamatilanteesta toivuttaessa voidaan laitteiden tiedot palauttaa milloin tahansa. Tämä onnistuu varmuuskopioiden avulla. [3.]

Ohjelmistoturvallisuus käsittää niin erilaiset turvallisuustoimenpiteet, jotka liittyvät ohjelmiston ylläpitoon ja päivitykseen, kuin myös käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistamis- ja suojausominaisuudet sekä valvonta- ja lokimenettelyt. Ohjelmistokehityksessä käytetyt prosessit, ohjelmiston käytönaikaiset asetukset ja ohjelmiston palvelualustan asetukset sekä käyttäjien saama koulutus ja ohjeistus ovat asioita, jotka vaikuttavat ohjelmistojen turvallisuuteen. Ohjelmistoturvallisuuteen on mahdollista vaikuttaa erilaisia teknisiä turvakeinoja käyttämällä. [3.] Tämän lisäksi ohjelmistoturvallisuus käsittää lisenssien hallinnan sekä ohjelmien rekisteröinnin. Ohjelmistoturvallisuuden tavoitteena on siis varmistaa ohjelmien luvallisuus ja estää laiton kopiointi ja käyttö. [4, s. 113.]

Nämä kahdeksan tietoturvan osa-aluetta on havainnollistettu kuvassa 1. Hallinnollinen tietoturva ja fyysinen tietoturva luovat perustan muille tietoturvan osa-alueille. Laitteistojen, ohjelmistojen ja tietoliikenneverkkojen turvallisesta käytöstä ovat vastuussa työntekijät, joten suuren kokonaisuuden oleellisia osia ovat henkilöstön osaaminen ja turvallisuus. [5.]



Kuva 1. Tietoturvan osa-alueet [5.]

3 TIETOTURVATEKNIIKOITA

Tietoturvasyistä suunnittelemani sovelluksen tietoturvaratkaisuja ei selosteta tässä dokumentissa. Seuraavassa on kuitenkin esitelty yleisesti muutamia tekniikoita, jotka mahdollistavat tietoturvallisen liikennöimisen Internetin yli.

VPN

VPN:llä eli Virtual Private Networkillä tarkoitetaan virtuaalista sisäverkkoa. Tällä tarkoitetaan joko laitteisto- tai ohjelmistototeutuksena tehtävää ratkaisua, jolla sisäverkko on mahdollista ulottaa turvattoman julkisen verkon yli turvallisesti. [6.]

VPN-tekniikan avulla yhdistetään joko kaksi tai useampia sisäverkkoja keskenään tai yksittäinen tietoliikennelaite organisaation verkkoon. Siirrettävä tieto suojataan salaamalla, jolla estetään julkisessa verkossa välitettävän liikenteen sisällön paljastuminen kolmansille osapuolille. Tämän lisäksi osapuolet, jotka liikennöivät VPN-ratkaisuissa, todennetaan vahvasti ennen kuin yhteys muodostetaan. [6.]

Käytännössä VPN-yhteyden muodostaminen tapahtuu tunneloimalla kaikki liikenne jonkin liikenteen salaavan protokollan sisään. Tällaisia protokollia ovat muun muassa IPsec (Internet Protocol security), L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point-to-Point Tunneling Protocol). VPN-tekniikan käyttö mahdollistaa kaiken turvattoman verkon yli VPN-tunnelissa lähetettävän liikenteen suojauksen ja tällöin suojaus ei ole riippuvainen sovellustason protokollista. [6.]

OpenVPN

OpenVPN on monipuolinen SSL (Secure Sockets Layer) VPN -ohjelmisto, joka on saatavilla monille eri käyttöjärjestelmille, esimerkiksi Windowsille ja Mac Os X:lle. OpenVPN toimii asiakaskoneeseen asennettavan OpenVPN-ohjelmiston avulla eikä toimi siis selaimen kautta. [7.]

Ohjelmistolla on mahdollista luoda sekä LAN-to-LAN- että etäkäyttöön sopivia yhteyksiä, jotka luodaan joko OSI-mallin (Open Systems Interconnection) toisella tai kolmannella ker-

roksella. Liikenne tunneloidaan käyttämällä joko UDP- (User Datagram Protocol) tai TCP-protokollaa (Transmission Control Protocol) IANA:n (Internet Assigned Numbers Authority) antaman oletusportin 1194 kautta. [7.]

OpenVPN toimii ytimen sijaan käyttäjäympäristössä, joka mahdollistaa sen, että järjestelmää voidaan suorittaa alennetuilla käyttöoikeuksilla ja hiekkalaatikossa. Yhteysosapuolten avaintenvaihtoon käytetään TLS-protokollaa (Transport Layer Security), jonka jälkeen hyödynnetään IPsec:n ESP-protokollaa (Encapsulating Security Payload Protocol) tiedon salaamiseen. Tällä mahdollistetaan NAT:n (Network Address Translation) ohittaminen asiakaspäässä. OpenVPN:n käytössä on kaikki OpenSSL-ohjelmiston salaus- ja tiivistysalgoritmit. TLS-kättelyssä on mahdollista ottaa käyttöön HMAC-allekirjoitus (Hash-based Message Authentication Code), jolloin avaintenvaihdon voivat aloittaa ainoastaan järjestelmät, joilla on oikeat staattiset avaimet. [7.]

Järjestelmään yhteyttä ottavien koneiden oikeellisuus tunnistetaan sertifikaateilla tai staattisilla salasanoilla. Sertifikaatteja käyttämällä mahdollistetaan sekä palvelimen että asiakaskoneen tunnistus. OpenVPN tukee myös CRL-listoja (Certificate Revocation List) PEM-muodossa (Privacy Enhanced Mail). Tämän lisäksi OpenVPN osaa hyödyntää PAM-moduuleita (Pluggable Authentication Modules). Näillä moduuleilla mahdollistetaan muun muassa käyttäjän tunnistus sekä kertakäyttöisten salasanojen käyttöönotto. [7.]

SSL

SSL eli Secure Sockets Layer (nykyisin TLS) on protokolla, jota käytetään varmistamaan turvallinen tiedonsiirto Internetissä. Protokolla toimii HTTP- (Hypertext Transfer Protocol) ja TCP-protokollien välisellä tasolla. SSL:n avulla varmistetaan turvallinen ja varmennettu yhteys kahden pisteen välillä verkossa, esimerkiksi asiakkaan ja palvelimen välillä. [8.]

SSL käyttää RSA:n julkisen ja yksityisen avaimen tekniikkaa, jossa julkinen avain on kaikkien saatavilla ja yksityisen avaimen tietää ainoastaan viestin vastaanottaja. Avaimia käytetään siten, että lähettäjä salaa lähetettävän tiedon julkisella avaimella ja vastaanottaja purkaa salauksen yksityisellä avaimella. [8.]

SSL:ää käytetään eniten HTTP-palvelimilla ja asiakassovelluksissa. Nykyisin melkein jokainen saatavilla oleva HTTP-palvelinsovellus tukee SSL-istuntoa, kunhan Internet-selain on varustettu SSL-tuella. [8.]

htaccess

htaccess on Apache-palvelinohjelmiston asetustiedosto, jonka avulla voidaan esimerkiksi salasana suojata kansioita ja tiedostoja, tehdä uudelleenohjauksia, piilottaa tiedostoja, estää tai sallia sivujen katseleminen tietystä IP-osoitteesta ja niin edelleen. [9.]

Yleensä tiedosto nimetään tiedostoksi .htaccess, mutta nimen voi muuttaa halutessaan määrittelemällä uuden nimen AccessFileName-ohjesääntöihin. htaccess-tiedostolla on vaikutus siihen kansioon, johon kyseinen tiedosto sijoitetaan. Tiedostolla on vaikutus myös kaikkiin kansiossa oleviin alikansioihin. htaccess-tiedostot noudattavat samaa syntaksia kuin tärkeimmät asetustiedostot. htaccess-tiedostoihin tehdyillä muutoksilla on välitön vaikutus, sillä htaccess-tiedostot luetaan jokaisen pyynnön yhteydessä.[9.]

4 TIETOTURVAKARTOITUS KÄSITTEENÄ

Tietoturvakartoituksen avulla taataan organisaation toiminnan luotettavuus ja tuottavuus sekä tuetaan tietoriskien hallintaa. Tietoturvakartoituksen avulla organisaation johto saa kuvan siitä, mikä on organisaation nykyinen tietoturvan taso sekä mitkä ovat vaatimukset. Kartoitus auttaa tekemään päätökset toteutettavista kehittämistoimenpiteistä tietoturvallisuuden saralla sekä laatimaan niille toteuttamissuunnitelmat. [10.]

Pohjatiedot kartoitusta varten kerätään esimerkiksi haastatteluin ja erilaisin kyselylomakkein. Pohjatietojen perusteella voidaan laatia kehittämissuunnitelma, riskianalyysi sekä tietoturvapolitiikka organisaatiolle. Näiden avulla organisaation tietoturvatoimintaa voidaan alkaa kehittää. [10.]

Kohteita, joita tietoturvakartoituksessa arvioidaan, ovat muun muassa organisaation tietoturvaohjeistus, tietoturvallisuuden johtaminen, työasemien, palvelimien ja tietoliikenneverkon tietoturvallisuus sekä sopimukset, jotka liittyvät palveluiden ulkoistamiseen. Näiden lisäksi arvioitavia kohteita ovat myös etäyhteydet ja niiden käyttö, mobiililaitteet, www-sovellukset, luokitellun aineiston käsittely, varautuminen poikkeusoloihin ja jatkuvuudesta huolehtiminen, tietoturvallisuuden tietämyksen taso ja henkilökunnan tietoturvakoulutus. [10.]

4.1 Tietoturvakartoituksen pohjalta laadittavissa olevia dokumentteja

Tietoturvapolitiikka on yrityksen johdon kannanotto tietoturvatoiminnan tavoitteista, vastuista ja toimintalinjoista. Erilaiset tietoturvasuunnitelmat ja -ohjeistukset rakentuvat juuri tietoturvapolitiikan perustan varaan. Organisaation toiminnan tarkoitus ja strategia, riskianalyysi, lait ja määräykset ohjaavat tietoturvapolitiikan luomisprosessia. [3.]

Tietoturvapolitiikka tulee olla organisaation ylimmän johdon hyväksymä. Lisäksi ylin johto vahvistaa noudatettavat turva- ja varautumisperiaatteet sekä määrittelee vastuut ja sisäisen toimintaorganisaation. Yleensä tietoturvallisuudesta vastaava henkilö on vastuussa tietoturvapolitiikan valmistelusta ja ylläpidosta. Johdon vastuulla on varmistaa asiakirjan tarkistus tai päivitys säännöllisesti. Tarkistus ja päivitys tulee tapahtua vähintään kolmen vuoden välein sekä silloin, kun toiminnassa tai organisaatiossa tapahtuu muutoksia. [3.]

Kehittämissuunnitelma on suunnitelma, jonka avulla ohjataan niitä toimenpiteitä, joilla korjataan puutteet, jotka on havaittu tietoturvakartoituksen yhteydessä. Näiden toimenpiteiden avulla pyritään myös hallitusti kehittämään tietoturvan nykytasoa vaaditulle tavoitetasolle. Tietoturvan kehittämissuunnitelma muodostaa loogisen kokonaisuuden tietoturvapolitiikan ja tietoturvakartoituksen kanssa. Tämä kokonaisuus kuvaa toiminnon suunnitelmallista kehittämistyötä. Kehityssuunnitelman raportointi on yksi osa organisaation raportointia. [3.]

Jotta johto saa oikean kuvan organisaation toimintaan ja palvelujen tietoturvallisuuteen kohdistuvista riskeistä, tarvitaan järjestelmällinen riskianalyysimenettely. Riskianalyysissä selvitetään toiminnan ja palvelujen tietoturvatarpeet ja vaatimukset, arvioidaan ulkoiset ja sisäiset riskit sekä selvitetään säädöksistä ja määräyksistä johtuvat vaatimukset. Näiden lisäksi analyysissa arvioidaan toiminnan ja tietotekniikan muutoksien vaikutukset tietoturvallisuuteen, selvitetään sidosryhmien odotukset sekä määritellään kaikkien edellä mainittujen perusteella tietoturvallisuuden tarpeet, periaatteet ja toteutustapa. [11.]

Riskianalyysi tulee tehdä säännöllisesti sekä silloin kun organisaatioon tai sen toimintaympäristöön kohdistuu suuria muutoksia. Riskinanalyysistä on tunnistettavissa suojattavat kohteet sekä siinä määritellään riskien hyväksyttävä taso ja sen pohjalta tarvittavat suojaustasot, luottamuksellisuus-, eheys- ja käytettävyysvaatimukset. [11.]

5 TUOTTEISTETTU TIETOTURVAKARTOITUS

Seuraavaksi insinöörityössä keskitytään selostamaan tietoturvakartoitus-palvelun suunnittelua. Tähtimediat Oy ei ole aiemmin tarjonnut tietoturvakartoitus-palvelua asiakkailleen, joten työhön kuului suunnitella myös se, millä tavalla palvelua tullaan markkinoimaan. Tämän lisäksi tuli miettiä, kuinka asiakastapaamisessa edetään. Seuraavassa on esitelty suunnitelma, kuinka valmista palvelua on tarkoitus markkinoida ja kuinka asiakastapaamisen on suunniteltu etenevän.

5.1 Markkinointi ja alkutoimet

Tietoa tietoturvakartoitus-palvelusta yritykset saavat muun muassa Tähtimediat Oy:n Internet-sivuilta. Tämän lisäksi palvelua markkinoidaan sähköpostitse, jossa yrityksille kerrotaan lyhyt kuvaus tietoturvan jatkuvasta kehittymisestä ja lisääntyvästä tarpeesta sekä tarjotaan mahdollisuutta kartoittaa oman yrityksen tietoturvan taso tietoturvakartoitus-palvelun avulla. Sähköpostiviestin lähettämisen jälkeen Tähtimediat Oy:n edustaja soittaa vielä puhelimitse sähköpostiviestin saaneille yrityksille ja tiedustelee, onko aiemmin markkinointi tarkoituksessa lähetetty viesti huomattu ja herättikö se mahdollisesti mielenkiinnon palvelua kohtaan. Palvelun markkinointi kohdistuu sekä jo Tähtimediat Oy:n asiakkaina oleville yrityksille että yrityksille, jotka eivät vielä ole Tähtimediat Oy:n asiakkaita ennestään. Palvelua voidaan kuitenkin myös markkinoida suoralla puhelinsoitolla ilman aiempaa sähköpostiviestiä.

Kun yritykset ovat saaneet tietoa palvelusta ja mielenkiinto palvelua kohtaan on herännyt, voi yritys tilata palvelun. Tämän jälkeen Tähtimediat Oy sopii tietoturvakartoituksen ajankohdan sekä keskustelee yrityksen edustajan kanssa siitä, kuka tai ketkä ovat parhaiten sopivat henkilöt vastaamaan kartoituksessa esitettäviin kysymyksiin.

Sovittuna ajankohtana Tähtimediat Oy:n edustaja menee käymään asiakkaan luona. Edustajalla tulee olla mukanaan joko kannettava tietokone tai kommunikaattori. Ensimmäiseksi Tähtimediat Oy ja asiakas allekirjoittavat salassapitosopimuksen esille tulevista luottamuksellisista ja salaisista tiedoista. Tämän jälkeen Tähtimediat Oy:n edustaja haastattelee asiakkaita palveluun sisältyvien kysymysten avulla ja kirjaa samalla ylös tarvittavat tiedot yrityksestä sekä syöttää kysymysten vastaukset sovellukseen.

5.2 Tietoturvakartoitussovellus

Tietoturvakartoitus-palvelun keskeisimpiä välineitä tulee olemaan sovellustyökalu, jonka avulla haastattelusta saatavat tiedot tullaan keräämään ylös. Tässä osiossa on kuvattu, mitä toimintoja sovellus tulee sisältämään ja kuinka niiden on suunniteltu toimivan.

Tietoturvakartoitussovellus sisältää kysymyksiä jokaisesta tietoturvan osa-alueesta sekä syöttö- ja vertailutoiminnon, joka vertailee ja analysoi vastaukset. Tämän perusteella saadaan arvio, missä osa-alueissa yrityksen tietoturva on kunnossa ja missä osa-alueissa olisi mahdollisesti kehitettävää.

Tietoturvan nykytaso kartoitetaan siis kysymysten avulla. Kysymyksiä on laadittu kaikista tietoturvan osa-alueista, ja ne on pyritty laatimaan siten, että haastattelun tuloksena saataisiin mahdollisimman oikea kuva yrityksen tietoturvan nykytasosta eri osa-alueittain. Kysymyksiä on yhteensä 77, ja ne ovat monivalintakysymyksiä. Kysymykset on esitetty liitteessä 1.

Kysymykset päätettiin toteuttaa monivalintakysymyksinä, sillä tulokset on helpompi käsitellä, mikäli kysymyksille on jo vastausvaihtoehdot olemassa. Lisäksi haastattelu ja vastausten kirjaaminen ei ole niin aikaavievää. Jokaiselle kysymykselle on rajattu määrä vastausvaihtoehtoja ja vastausvaihtoehdot ovat toisensa poissulkevia. Tämä mahdollisti sen, että kysymykset toteutettiin monivalintakysymyksillä. Mikäli haastatteluun olisi valittu avoimet kysymykset, olisi myös ohjelma, joka käsittelee kysymykset, työläämpi ja hankalampi ohjelmoida.

Syöttö- ja vertailutoiminto

Ensimmäisenä sovellukseen syötetään kartoituksen kohteena olevan yrityksen nimi, yhteyshenkilö (henkilö, joka edustaa yritystä kartoitusta tehdessä) sekä yhteyshenkilön puhelinnumero ja sähköpostiosoite. Tämän jälkeen Tähtimediat Oy:n edustaja haastattelee asiakasta kysyen jokaisen kysymyksen siinä järjestyksessä, kuin ne auki olevassa sovelluksessa ovat. Jokaiseen kysymykseen on vastausvaihtoehtoja kolme tai enemmän ja niistä voidaan valita vain yksi, joka parhaiten kuvaa yrityksen tilannetta. Tähtimediat Oy:n edustaja valitsee vaihtoehdoista sen vastausvaihtoehdon, jonka yrityksen edustaja valitsee. Kun jokaiseen kysymykseen on vastattu, painetaan Valmis-painiketta, jolloin vertailutoiminto vertailee vastaukset.

Jokaiselle kysymyksen vaihtoehdolle annetaan arvo. Jos vaihtoehtoja on esimerkiksi viisi, ovat vaihtoehtojen arvot yhdestä viiteen. Mitä suurempi arvo valitulla vaihtoehdolla on, sitä paremmin kyseinen asia on yrityksessä hoidettu. Kun kaikkien kysymysten vastaukset on käyty läpi, toiminto analysoi ne ja kertoo, missä osioissa oli mahdollisia puutteita ja mitkä osiot olivat kunnossa. Se, miten vertailutoiminto toteutetaan, on selitetty tarkemmin työn luvussa 6 ”Toteutuksen suunnittelu”.

Tulos, parannusehdotukset sekä palaute

Kun vastaukset on analysoitu, lähettää sovellus tulokset tietokoneen tai kommunikaattorin ruudulle sekä Tähtimediat Oy:n edustajan ja asiakkaan sähköpostiin. Tuloksissa näkyy alussa syötetyt yrityksen nimi ja yhteyshenkilön tiedot sekä kysymykset vastauksineen. Jokaisen kysymyksen kohdalla on pisteet, jonka yritys on vastauksellaan saanut ja jokaisen osa-alueen lopussa on yhteispisteet osiosta. Näin sovelluksen avulla näkee helposti, missä alueissa on mahdollisesti puutteita ja missä kohtaa sekä mitkä alueet ovat kunnossa.

Sovelluksen löytäessä mahdollisia puutteita yrityksen tietoturvassa pisteiden lisäksi tuloksissa näkyy sovelluksen ehdottama parannusehdotus asian korjaamiseksi. Parannusehdotus on suuntaa antava eikä sitä tule pitää ainoana oikeana vaihtoehtona. Tähtimediat Oy:n edustaja käy tulokset läpi ja katsoo, onko parannusehdotus sopiva vai puuttuuko vielä jotain tai onko parannusehdotuksessa jotain ”liikaa”. Tämän jälkeen tulokset käydään yhdessä läpi Tähtimediat Oy:n ja asiakkaan kanssa ja keskustellaan mahdollisista parannusehdotuksista ja mahdollisuuksista.

6 TOTEUTUKSEN SUUNNITTELU

Sovellus tullaan toteuttamaan siten, että sitä voidaan käyttää selaimen kautta. Sovellus olisi ollut mahdollista toteuttaa esimerkiksi Windows-sovelluksena, mutta tällöin sovellus jouduttaisiin asentamaan jokaiseen laitteeseen erikseen. Lisäksi sovellus ei välttämättä toimisi kuin tietyntyyppisissä laitteissa. Koska sovellus toteutetaan siten, että sitä käytetään selaimessa, pääsee sovellukseen käsiksi missä ja milloin vain.

6.1 Yleistä HTML-kielestä

Sovelluksen käyttöliittymä toteutetaan HTML-kielellä. Lyhenne HTML tulee sanoista HyperText Markup Language. HTML-kielellä tuotetaan siirtokelpoisia hypertekstiasiakirjoja eri ympäristöihin. Hypertekstiasiakirjalla tarkoitetaan asiakirjaa, joka sisältää tekstiä, jossa on linkkejä eli viittauksia muihin teksteihin tai dokumentteihin. HTML on siis dataformaatti eli toisin sanoen menetelmä, jonka avulla organisoidaan ja järjestetään dataan liittyvää informaatiota. [12.]

HTML-dokumentti aloitetaan dokumenttityypin kertovalla otsikolla `"!DOCTYPE"`. Tämän jälkeen varsinainen dokumentti aloitetaan aina `<html>`-tagilla. Tämän avulla selain tietää, mitä täytyy tulkata. Seuraavaksi tulee `<head>`-tagi, jonka avulla ilmoitetaan dokumentin otsikkotietojen alkaminen. `<head>`-tagi sijaitsee aina HTML-dokumentin alussa. `<title>`- ja `</title>`-tagien väliin tulee dokumentin otsikko. `</head>`-tagi ilmoittaa otsikkotietojen loppumisesta dokumentissa ja se sijoitetaan otsikkotietojen jälkeen. `<body>`-tagi aloittaa aina varsinaisen informaation sisältävän dokumentin osan. Varsinaisen informaation sisältävän dokumentin osan loppuessa, tulee toinen `</body>`-tagi, joka lopettaa varsinaisen dokumentin. Tämän jälkeen tulee `</html>`-tagi, joka lopettaa itse HTML-dokumentin. [13.] Kuvassa 2 on esitetty HTML-dokumentin perusrakenne.

```
<html><head><title>otsikko</title></head>
<body>
<h1>otsikko</h1>
<p>Tähän jotain tekstiä</p>
</body>
</html>
```

Kuva 2. HTML-dokumentin perusrakenne

6.2 Käyttöliittymä

Sovelluksen käyttöliittymänä toimii lomake. Tekstikenttien osalta lomakkeessa käytetään table-toimintoa eli taulukkoa. Taulukon avulla tekstikenttien tekstit saadaan vasempaan soluun ja oikeaan itse tekstikentät. Tämä mahdollistaa sen, että lomakkeen ulkoasu paranee. Kysymysten kohdalla table-toimintoa ei kuitenkaan käytetä, jotta itse kysymys saadaan ensin ja vastausvaihtoehdot sen alapuolelle.

Tekstikentät

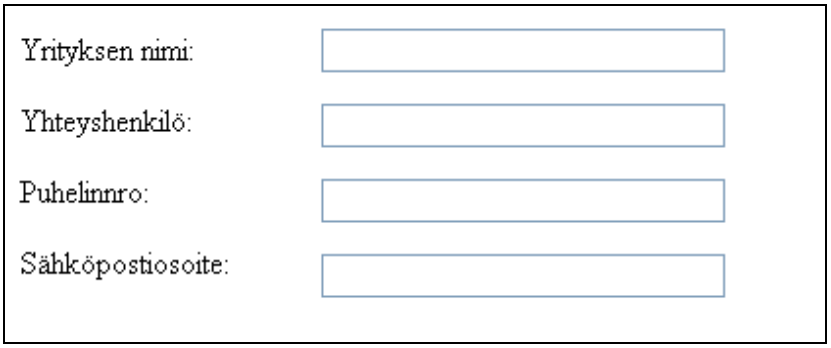
Tekstikenttiä lomakkeeseen tulee neljä kappaletta. Tekstikenttiin syötetään yrityksen nimi, yhteyshenkilö sekä yhteyshenkilön puhelinnumero ja sähköpostiosoite. Kuvassa 3 on esitetty esimerkki koodista, jonka avulla voidaan toteuttaa tekstikentät.

```
<html>
<body>

<table>

<tr>

<td valign="top" width="150">


        <p>Yrityksen nimi:</p>
        <p>Yhteyshenkilö:</p>
        <p>Puhelinnro:</p>
        <p>Sähköpostiosoite:</p>
        </td>

        <td valign="top" width="300">
        <p><INPUT NAME="Yrityksen nimi"
        TYPE="text" SIZE=30></p>
        <p><INPUT NAME="Yhteyshenkilö"
        TYPE="text" SIZE=30></p>
        <p><INPUT NAME="Puhelinnro"
        TYPE="text" SIZE=30></p>
        <p><INPUT NAME="Sähköpostiosoite"
        TYPE="text" SIZE=30></p>

<tr>

</body>
</html>
```

Kuva 3. Esimerkki koodista, joka toteuttaa tekstikentät

Taulukko luodaan `<table>`-tagilla. Taulukon rivi määritellään `<tr>`-tagilla. Rivi sisältää yhden tai useamman solun. Taulukon solu puolestaan määritellään `<td>`-tagin avulla. Attribuutti ”`valign`” määrittelee, kuinka kyseisellä rivillä olevat solujen sisällöt asetellaan pystysuunnittain. Samassa sarakkeessa olevien solujen leveys määritellään `width`-attribuutin avulla. Leveys voidaan määritellä joko täsmällisesti pikseleinä tai prosentteina taulukon leveydestä. `INPUT NAME` -attribuutti määrittelee kentän nimen, `TYPE`-attribuutti määrittelee, minkä tyyppisestä lomake-elementistä on kyse, ja `SIZE`-attribuutti kertoo, kuinka monen merkin levyinen tekstikentän tulee olla. [14.]

Kuvan 3 koodin avulla saadaan siis tekstikentät toteutettua siten, että pyydetty tieto sijoittuu lomakkeen vasempaan reunaan ja tekstikenttä, johon pyydetty tieto syötetään, sijoittuu lomakkeen oikeaan reunaan. Kuvassa 4 on esitetty näkymä, joka saadaan suorittamalla kuvan 3 koodi.



Kuva 4. Kuvan 3 koodin toteuttamat tekstikentät

Radiopainikkeet

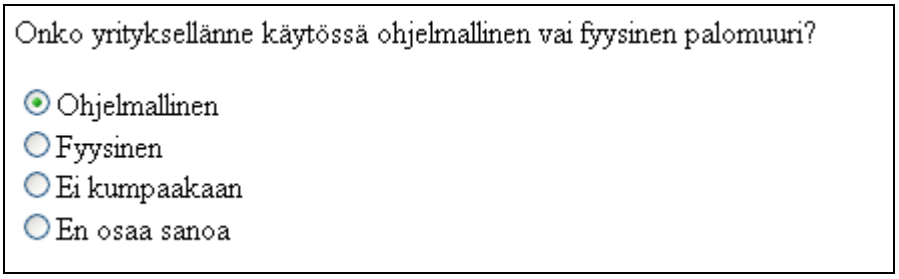
Kysymysten vastausvaihtoehdot toteutetaan radio-painikkeiden avulla. Tämä tarkoittaa, että ryhmään kuuluvista vastausvaihtoehdoista voi valita vain yhden vaihtoehdon. Kuvassa 5 on esitetty esimerkki koodista, jonka avulla voidaan toteuttaa radiopainike.

```
<html>
<body>

        <p>onko yrityksellänne käytössä ohjelmallinen vai fyysinen palomuuri?</p>

        <input type="radio" name="Kysymys1" value="V1" checked  >Ohjelmallinen<br>
        <input type="radio" name="Kysymys1" value="V2">Fyysinen<br>
        <input type="radio" name="Kysymys1" value="V3">Ei kumpaakaan<br>
        <input type="radio" name="Kysymys1" value="V4">En osaa sanoa</p>

</body>
</html>
```

Kuva 5. Esimerkki koodista, joka toteuttaa radiopainikkeen

Attribuutti ”`input type`” kertoo, mikä elementti on kyseessä eli tässä tapauksessa radiopainike. Nimi eli `name`-attribuutti tulee olla sama kaikissa samaan ryhmään kuuluvissa radiopainikkeissa. Attribuutti ”`value`” kertoo arvon, joka lähetetään lomakkeen mukana ja sen arvoksi voi valita minkä tahansa nimen tai koodin. Ensimmäisen vaihtoehdon lopussa olevan `checked`-attribuutin avulla ensimmäinen vaihtoehto on oletusarvoisesti valittuna. Vaihtoehdoista vain yksi voi olla valittuna oletusarvoisesti. [14.]

Kuvan 5 koodin suorittamisen jälkeen saadaan tulokseksi näkymä, jossa ensiksi on kysymys ja kysymyksen alapuolella on vastausvaihtoehdot. Ensimmäinen vastausvaihtoehto on oletuksena valittuna. Kuvassa 6 on esitetty näkymä, joka saadaan suorittamalla kuvan 5 koodi.



Kuva 6. Kysymys ja radiopainikkein toteutetut vaihtoehdot

Valmis- ja Tyhjennä-painikkeet

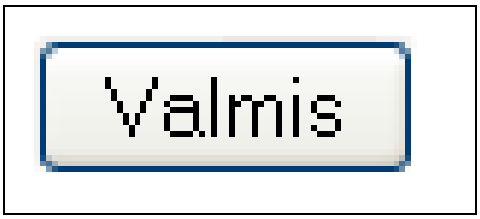
Valmis-painikkeen avulla lomakkeen tiedot lähetetään eteenpäin ohjelmalle, joka käsittelee ne. Kuvassa 7 on esitetty esimerkki koodista, jonka avulla voidaan toteuttaa Valmis-painike.

```
<html>
<body>
<form action="TTKSovellus.php" method="post">

<input type="submit" value="Valmis"></p>

</form>
</body>
</html>
```

Kuva 7. Esimerkki koodista, joka toteuttaa Valmis-painikkeen

Tagin `<form> action`-attribuutti määrittelee, minne lomakkeen tieto lähetetään. `input type` määrittelee syötekentän tyypin, joka tässä tapauksessa on `submit`. `Value`-attribuutti määrittelee sen, mikä teksti painikkeeseen halutaan. [14.]

Kuvasta 7 nähdään, että Valmis-painiketta painettaessa syötetyt tiedot lähtisivät `TTKSovellus.php`-skriptille. Tässä tapauksessa mitään tietoja ei kuitenkaan lähde skriptille, sillä kuvan tarkoituksena on havainnollistaa ainoastaan Valmis-painikkeen toteutus, eikä puuttua muuhun osaan koodista. Kuvassa 8 on esitetty näkymä, joka saadaan, kun suoritetaan edellä esitetty Valmis-painikkeen koodi.



Kuva 8. Valmis-painike

Tyhjennä-painikkeen avulla lomakkeen kaikki kentät saadaan tyhjennettyä yhdellä napin painalluksella, mikäli sellaiselle on tarvetta. Kuvassa 9 on esitetty koodi, jolla Tyhjennä-painike saadaan toteutettua.

```
<html>
<body>

        <input type="reset" value="Tyhjennä">

</body>
</html>
```

Kuva 9. Esimerkki koodista, joka toteuttaa Tyhjennä-painikkeen

Suoritettaessa kuvan 9 koodi on näkymä sama kuin edellä esitetyn Valmis-painikkeen kohdalla. Ainoastaan painikkeen teksti on eri eli ”Tyhjennä”.

6.3 Yleistä PHP:stä

Skripti, joka käsittelee HTML-lomakkeelle syötetyt tiedot, toteutetaan PHP-kielellä. Skriptin koodauskieleksi valittiin PHP-kieli, koska se on helppo kieli opetella ja sen saa toimimaan useilla eri alustoilla. Lisäksi PHP:n avulla sovellus saadaan toimimaan monilla eri laitteilla (esimerkiksi kannettavat tietokoneet, matkapuhelimet), sillä PHP-kieli tulostaa myös HTML-kieltä.

PHP, eli Hypertext Preprocessor, on tulkattava komentosarjakieli eli kieli, joka suoritetaan palvelinpuolella. Tällä tarkoitetaan sitä, että PHP-sivut niiden sisältämine koodeineen käsitellään www-palvelimella ennen sivun lataamista asiakkaan selaimelle. PHP-koodia käytetään usein yhdessä HTML- ja XHTML-kielten kanssa. [15.]

Uusin versio PHP:stä on PHP 5.0, joka julkaistiin heinäkuussa 2004. PHP:n aiemmilla versioilla on kuitenkin edelleen erittäin vankka asema tuotanto- ja kehityskäytössä. PHP muistuttaa syntaksiltaan C-, Java- ja Perl-kieliä. Ensisijaisena tavoitteena PHP:llä on tarjota nopea ja monipuolinen kehitysympäristö web-kehittäjille. [15.]

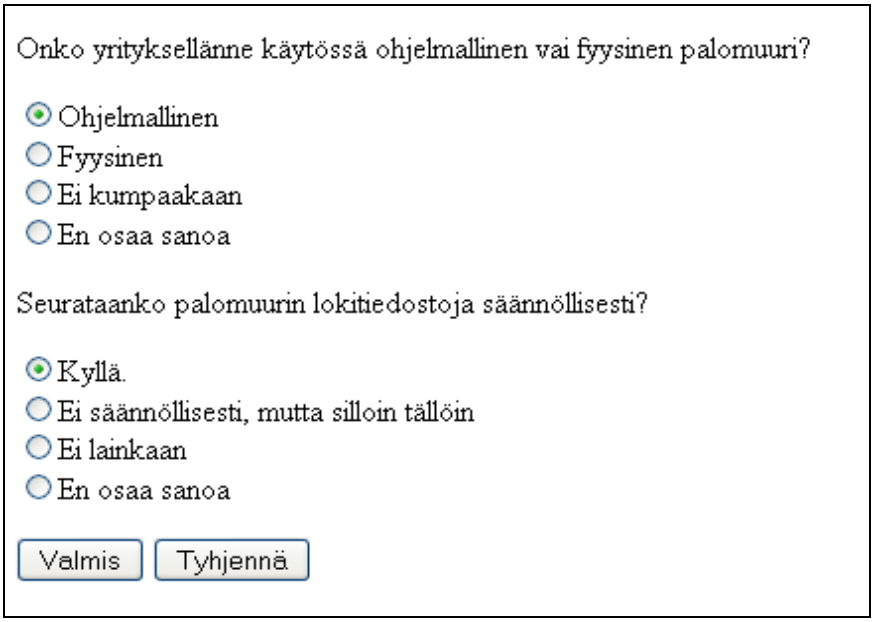
6.4 PHP-skripti

HTML-lomakkeelle syötetyt tiedot lähetetään palvelimella toimivalle PHP-skriptille. Osoite, johon tiedot lähetetään, kerrotaan lomakkeelle `action`-attribuutin avulla. Kuvassa 10 on esitetty esimerkki koodista, joka toteuttaa kaksi kysymystä ja vastausvaihtoehdot radiopainikkein. Kuvasta nähdään, että tiedot määritetään lähtevän skriptille nimeltä `switchcase.php` edellä mainitun `action`-attribuutin avulla.

```
<html>
<body>

        <form action="switchcase.php" method="post">

        <p>onko yrityksellänne käytössä ohjelmallinen vai fyysinen palomuuri?</p>


        <input type="radio" name="Kysymys1" value="V1" checked  >Ohjelmallinen<br>
        <input type="radio" name="Kysymys1" value="V2">Fyysinen<br>
        <input type="radio" name="Kysymys1" value="V3">Ei kumpaakaan<br>
        <input type="radio" name="Kysymys1" value="V4">En osaa sanoa</p>


        <p>Seurataanko palomuurin lokitiedostoja säännöllisesti?</p>


        <input type="radio" name="Kysymys2" value="V1" checked  >Kyllä.<br>
        <input type="radio" name="Kysymys2" value="V2">Ei säännöllisesti, mutta silloin
         tällöin<br>
        <input type="radio" name="Kysymys2" value="V3">Ei lainkaan<br>
        <input type="radio" name="Kysymys2" value="V4">En osaa sanoa</p>


        <input type="submit" value="Valmis">
        <input type="reset" value="Tyhjennä"></p>


</body>
</html>
```

Kuva 10. Koodi, joka toteuttaa kaksi kysymystä sekä lähettää vastaukset eteenpäin

Katsottaessa koodin tulostetta selaimella on näkymä kuvan 11 mukainen. Painettaessa kuvassa näkyvää Valmis-painiketta tiedot lähtevät edellä mainitulle `switchcase.php`-skriptille, joka käsittelee ne ja palauttaa kysymysten tulokset takaisin selaimelle sekä skriptin koodissa määritettyyn sähköpostiosoitteeseen.



Kuva 11. Kuvan 10 koodiesimerkin tuloste

Kuvassa 12 on esitetty osa `switchcase.php`-skriptin koodista. Tämä osa koodista määrittelee sen, mikä tulos on kunkin vastausvaihtoehdon kohdalla.

```
<?php
$maili = "YRITYKSENNE PALOMUURITILANNE ON SEURAAVANLAINEN:" . "<br/>" . "<br/>" . "\n\t" . "\n\t";

                        switch ($_POST["Kysymys1"]) {

                        case "V1" :
                        $ekapisteet = 3;
                        $maili .=  "Käytössänne on tällä hetkellä ohjelmallinen palomuuri, mutta
                        suosittelemme fyysistä. Edustajamme kertoo tästä vaihtoehdosta lisää." . "<br/>"
                        . "\n\t";
                        $maili .= "Pisteenne tästä kysymyksestä sijoittuvat alueelle 3-4." . "<br/>" .
                        "<br/>" . "\n\t" . "\n\t";
                        break;

                        case "V2" :
                        $ekapisteet = 4;
                        $maili .= "Käytössänne on tällä hetkellä fyysinen palomuuri ja tämä on paras
                        ratkaisu." . "<br/>" . "\n\t";
                        $maili .= "Pisteenne tästä kysymyksestä sijoittuvat alueelle 3-4." . "<br/>" .
                        "<br/>" . "\n\t" . "\n\t";
                        break;

                        case "V3" :
                        $ekapisteet = 1;
                        $maili .= "Tietoturvanne on todella uhattuna! Edustajamme kertoo heti lisää
                        palomuurin tarpeellisuudesta ja teidän tulee hankkia fyysinen palomuuri
                        välittömästi." . "<br/>" . "<br/>" . "\n\t";
                        $maili .= "Pisteenne tästä kysymyksestä sijoittuvat alueelle 1-2." . "<br/>" .
                        "<br/>" . "\n\t" . "\n\t";
                        break;

                        case "V4" :
                        $ekapisteet = 1;
                        $maili .= "Tilanteesta tulee ottaa heti selvää, tietoturvanne saattaa olla
                        uhattuna!" . "<br/>" . "\n\t";
                        $maili .= "Pisteenne tästä kysymysestä sijoittuvat alueelle 1-2." . "<br/>" .
                        "<br/>" . "\n\t" . "\n\t";
                        break;

                        default :
                        break;
```

Kuva 12. Osa switchcase.php-skriptin koodista

Kysymysten vastaukset käsitellään `switch case` -komentorakenteen avulla ja vastaukset poimitaan `$_POST`-funktion avulla. Kuvassa 12 on esitettynä koodin osa, joka käsittelee yrityksen palomuuritilannetta käsittelevän kysymyksen vastauksen. Mikäli kysymykseen on vastattu valitsemalla ensimmäinen vastausvaihtoehto, on tuloksena `case "V1":`n määrittelemä tulos. Mikäli kysymykseen on vastattu valitsemalla toinen vastausvaihtoehto, on tuloksena `case "V2":`n määrittelemä tulos ja niin edelleen.

Lisäksi jokaisessa `case`-kohdassa on määritelty vastauksesta saadut pisteet muuttujan avulla. Tässä kysymyksessä on kyseessä `$ekapisteet`-muuttuja, toisessa kysymyksessä muuttuja on `$tokapisteet` ja niin edelleen. Ensimmäisestä vastausvaihtoehdosta on saanut kolme pistettä, toisesta neljä ja niin edelleen. Pisteitä ei kuitenkaan ilmoiteta asiakkaalle tarkasti vaan asiakkaalle ilmoitetaan ainoastaan alue, mille pisteet sijoittuvat.

Jokaisessa `case`-kohdassa on myös kooste siitä, mitä kysymykseen on vastattu ja päätelmä siitä, onko kyseinen asia yrityksen sisällä kunnossa vai onko kenties jotain kehitettävää. Mikäli tuloksena on, että asia on epäkunnossa, lähettää skripti myös ehdotuksen, mitä asialle tulisi tehdä.

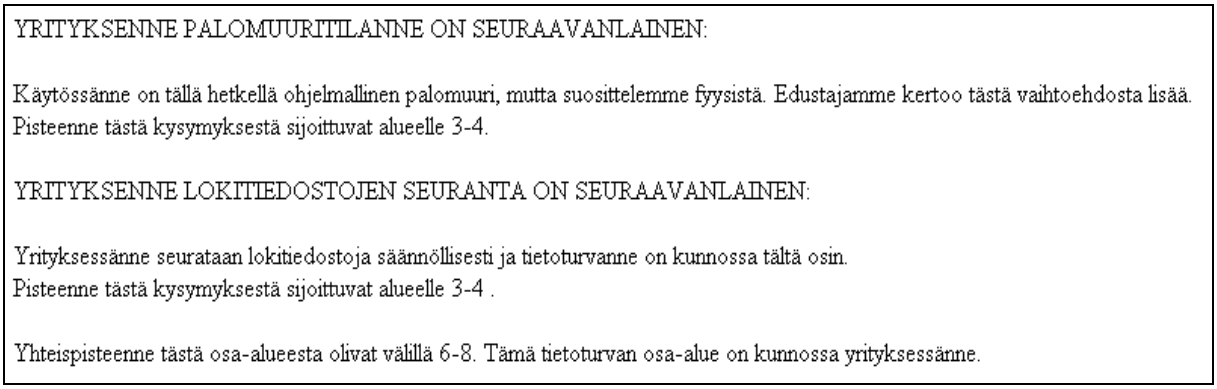
Kaikkien kysymysten vastaukset käydään tällä periaatteella läpi, ja aina yhden tietoturvan osa-alueen päättyessä ilmoittaa ohjelma yhteispisteet osa-alueesta. Tämä tapahtuu `$yhteis-pisteet`-muuttujan avulla. Kuvassa 13 on esitetty, kuinka kyseinen toiminto toteutetaan.

```
$yhteispisteet = $ekapisteet + $tokapisteet;
if($yhteispisteet >= 6)
{
        $maili .= "Yhteispisteenne tästä osa-alueesta olivat välillä  6-8. Tämä
        tietoturvan osa-alue on kunnossa yrityksessänne.";
}
elseif($yhteispisteet <=5)
{
        $maili .= " Yhteispisteenne tästä osa-alueesta olivat välillä 2-5. Tässä
        tietoturvan osa-alueessa teillä on parantamisen varaa ja edustajamme voi
                auttaa teitä siinä.";
}
```

Kuva 13. Koodi, joka toteuttaa pisteiden yhteenlaskun

Yhteispisteet on saatu laskemalla `$ekapisteet`-muuttujan ja `$tokapisteet`-muuttujan arvot yhteen. Pisteitä ei ilmoiteta tarkasti vaan alue, jolle pisteet sijoittuvat, esimerkiksi 2–5 tai 5–8 sen mukaan, kuinka paljon pisteitä on mahdollista saada. Tämä on to-

teutettu `if-else`-komentorakenteen avulla, joka vertailee saatua yhteispistemäärää, ja tulostaa tämän perusteella asiakkaalle yhteenvedon siitä, kuinka kyseinen osa-alue sujui sen mukaan, mille alueelle pistemäärä sijoittuu. Kuvassa 14 on esitetty näkymä siitä, millainen tuloste on, kun kuvan 11 kysymyksistä on valittu kumpaankin ensimmäiset vastausvaihtoehdot ja painettu Valmis-painiketta.


YRITYKSENNE PALOMUURITILANNE ON SEURAAVANLAINEN:

Käytössänne on tällä hetkellä ohjelmallinen palomuuri, mutta suosittelemme fyysistä. Edustajamme kertoo tästä vaihtoehdosta lisää.
Pisteenne tästä kysymyksestä sijoittuvat alueelle 3-4.

YRITYKSENNE LOKITIEDOSTOJEN SEURANTA ON SEURAAVANLAINEN:

Yrityksessänne seurataan lokitiedostoja säännöllisesti ja tietoturvanne on kunnossa tältä osin.
Pisteenne tästä kysymyksestä sijoittuvat alueelle 3-4 .

Yhteispisteenne tästä osa-alueesta olivat välillä 6-8. Tämä tietoturvan osa-alue on kunnossa yrityksessänne.

Kuva 14. Tulos vastausten käsittelyn jälkeen.

Tulosteena saadaan edellä mainittu kooste vastauksesta sekä päätelmä siitä, millä mallilla asia yrityksessä on. Tämän jälkeen nähdään, mille alueelle kysymyksestä saatu pistemäärä sijoittuu ja lopuksi, mille alueelle koko osa-alueen yhteispistemäärä sijoittuu. Kuvan 14 näkymä tulostuu selaimen näytölle sekä lähtee sähköpostiviestinä määritettyyn sähköpostiosoitteeseen. Kuvassa 15 on esitetty, kuinka lähetys tiettyyn sähköpostiosoitteeseen toteutetaan.

```
echo $maili;
mail("matti.meikalainen@testi.com", "Tietoturvakartoituksen tulokset",$maili);
```

Kuva 15. Sähköpostin lähetys

Ensimmäisenä sulkujen sisällä olevassa lauseessa on määritelty sähköpostiosoite, johon tulokset halutaan. Tämän jälkeen määritellään sähköpostiviestin otsikko ja lopuksi sähköpostiviestin sisältö. Tässä tapauksessa kaikki tieto on kerätty ”`$maili`”-nimiseen muuttujaan.

7 LOPPUTULOKSET

Työn tavoitteena oli suunnitella tuotteistettu tietoturvakartoitus pienille ja keskisuurille yrityksille. Tavoitteeseen päästiin ja lopputuloksena saatiin suunnitelma kokonaisuudesta, johon kuuluu tietoturvakartoituksen markkinointi, asiakaskäynti ja sovellustyökalu kartoituksen tekemiseen.

Palvelua markkinoidaan sähköposti- ja puhelinmarkkinoinnin kautta. Yksi tietoturvakartoitus-palvelun keskeisimpiä välineitä on edellä mainittu sovellustyökalu. Tässä työssä saatiin suunniteltua sovellustyökalun ensimmäinen versio eli prototyyppi. Sovellustyökalu sisältää 77 monivalintakysymystä, syöttötoiminnon sekä vertailutoiminnon, joka vertailee ja analysoi kaikki vastaukset. Vertailutoiminnon avulla saadaan kooste siitä, kuinka hyvin tietoturva on hoidettu yrityksessä ja onko siinä mahdollisesti kehittämisen varaa. Tulokset saadaan tietokoneen tai kommunikaattorin näytölle sekä valittuihin sähköpostiosoitteisiin. Käyttöliittymä toteutetaan HTML-kielen avulla, ja itse skripti, joka suorittaa vastausten vertailun ja analysoinnin, toteutetaan PHP-kielen avulla.

Työssä kuvattua sovellustyökalua tullaan toteutuksen jälkeen testaamaan ja kehittämään. Sovellus ohjelmoidaan kokonaisuudeksi työssä esitettyjen esimerkkikoodien avulla. Kaikki insinöörityössä esitetyt koodiesimerkit testattiin ja ne todettiin toimiviksi.

Sovellustyökalun jatkokehityksessä voitaisiin huomioida tietokantojen hyödyntäminen. Esimerkiksi kysymykset voisivat olla koottuna tietokantaan, josta tilanteen mukaan saataisiin poimittua sopivat ja tarvittavat kysymykset.

Kokonaisuuteen liittyviä jatkokehitysideoita olisi muun muassa se, että jokaisen kartoituksen jälkeen laadittaisiin dokumentti tietoturvan nykytasosta, jonka lopuksi tulisi kooste kehittämistoimenpiteistä sekä riskeistä, joita yrityksen toimintaa kohtaan mahdollisesti kohdistuu. Myös tietoturvapolitiikan ja toipumissuunnitelmien laatimista voitaisiin tarjota kartoituksen jälkeen, mikäli niille olisi tarvetta.

8 YHTEENVETO

Insinöörityössä suunniteltiin kokonaisuus tietoturvakartoituksesta, johon sisältyy tietoturvakartoituksen markkinointi, asiakaskäynti, haastattelukysymykset sekä sovellustyökalu, jonka avulla tietoturvakartoitus toteutetaan syöttämällä haastattelussa kerätyt tiedot ja kysymysten vastaukset sovellukseen.

Työssä suunniteltiin markkinointikeinot ja asiakastapaamisen eteneminen. Sovellustyökalun suunniteltiin sisältävän monivalintakysymykset jokaisesta tietoturvan osa-alueesta. Kysymysten lisäksi sovellustyökalun suunniteltiin sisältävän syöttö- ja vertailutoiminnot. Sovellukseen tullaan syöttämään haastattelussa saadut tiedot yrityksestä ja yrityksen tietoturva-asioista, jonka jälkeen vertailutoiminto vertailee ja analysoi tulokset. Tämän jälkeen tulokset lähetetään tietokoneen tai kommunikaattorin näytölle sekä sovittuihin sähköpostiosoitteisiin. Sovellus suunniteltiin toteutettavan HTML- ja PHP-kielten avulla.

Työssä tuli vastaan jo ennalta opittuja asioita sekä uusia asioita. Entuudestaan tuttua oli muun muassa tietoturvakartoitus vaihe vaiheelta, koska opiskeluni aikana pääsimme toteuttamaan tietoturvakartoituksen alusta loppuun olemassa olevalle organisaatiolle. Uutta työssä olivat HTML- ja PHP-kielet, joiden perusteita jouduin opiskelemaan, jotta sain toteutettua tarvittavat koodit ja esimerkit havainnollistamaan sovellustyökalun perusrakennetta ja -toimintaa. Näiden kielten opiskelu ei vienyt kuitenkaan kohtuuttomasti aikaa, sillä opetusmateriaaleja ja koodausympäristöt olivat helposti saatavilla. Lisäksi aiemmin opiskeltujen C- ja C++-kielten perusteista oli hyötyä.

Pääpiirteissään työ onnistui ja aiemmin asetettuihin tavoitteisiin päästiin. Aikataulussa oli helppo pysyä, sillä työ toteutettiin vasta sen jälkeen, kun opintojen lähiopetus oli kokonaan päättynyt. Suurimman osan ajasta vei sovellustyökalun suunnittelu. Ylitsepääsemättömiä ongelmia työn aikana ei tullut vastaan, ja ongelmat, joihin törmäsin, sain aina loppujen lopuksi ratkottua. Työtä oli kaikin puolin mielenkiintoista tehdä ja toivon, että työn jatkokehityksessä voisin myös itse olla mukana.

LÄHTEET

1. Viestintävirasto. Tietoturvalliseen yhteiskuntaan. Viimeksi muutettu 16.9.2009. [WWW-dokumentti]<http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html>

2. Miettinen, Juha E. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Kauppakaari. Helsinki 1999.

3. Valtiovarainministeriö. Tietoturvallisuudella tuloksia. 3/2007. [PDF-dokument-ti]<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf> . (Luettu 5.10.2010.)

4. Järvinen, Petteri. Tietoturva ja yksityisyys. WS Bookwell. 1. painos. Porvoo 2002. ISBN 951-846-152-X

5. Tietojesiturvaksi.fi. Tietoturvan osa-alueet. Viimeksi päivitetty 30.12.2010. [WWW-dokumentti]<http://www.tietojesiturvaksi.fi/content/tietoturvan-osa-alueet>

6. Viestintävirasto. VPN. Viimeksi päivitetty 27.9.2007. [WWW-dokumentti]<http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/vpn.html>

7. OpenVPN Technologies, Inc. [WWW-dokumentti]<http://openvpn.net/>.(Luettu 24.2.2011)

8. TechTarget. SSL. Viimeksi päivitetty 6.12.2010. [WWW-dokumentti]< http://searchsecurity.techtarget.com/sDefinition/0,„sid14_gci343029,00.html>

9.Apache. Apache Tutorial: .htaccess files.[WWW-dokumentti]< http://httpd.apache.org>. (Luettu 24.2.2011)

10. Loimaan seutukunta. Tietoturvakartoitus. [WWW-dokumentti]< http://www.loimaanseutu.fi/Default.aspx?id=576145>. (Luettu 14.10.2010)

11. Valtiovarainministeriö. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. 9/2006. [PDF-dokumentti]<https://www.vahtiohje.fi/c/document_library/get_file?uuid=d48cbc58-d7a4-4757-a0a1-78cd860a3912&groupId=10128>. (Luettu 10.4.2011)

12. Ek, Jesper; Norén, Karl-Johan. Dynaaminen HTML käytännössä. Tummavuoren kirjapaino Oy. Vantaa 1999.

13. Jaakkola, Tatu. Ohjeita web-sivuston tekijälle. [WWW-dokumentti]< http://www.sivut.org/html/oppaat/dokumentin_rakenne.php>. (Luettu 26.1.2011)

14. Oliver, Dick. HTML & XHTML – Trainer Kit. Edita Prima Oy. Helsinki 2002.

15. 2000-2010 Koulutus- ja konsultointipalvelu KK Mediat. PHP. [WWW-dokumentti]<http://www.2kmediat.com/php/johdanto.asp>. (Luettu 2.2.2011)

LIITELUETTELO

FYYSINEN TIETOTURVA

Onko yrityksen tiloissa käytössä kulunvalvontaa?

- Kyllä.
- Ei.
- En osaa sanoa.

Miten yrityksen ovien lukitus toimii?

- Ovet ovat lukittuina aina.
- Ovet ovat avoinna tiettynä kellonaikana, mutta muuten lukittuina.
- Ovia lukitaan ja avataan milloin mitenkin.
- En osaa sanoa.

Miten vierailijoiden kanssa toimitaan?

- Vierailijat voivat tulla ja mennä yrityksen tiloissa, miten itse haluavat.
- Joku on aina vastaanottamassa vierailijat heti aulassa.
- En osaa sanoa.

Onko vartija tarpeen tullen helposti tavoitettavissa?

- Kyllä on. Jokaisella on tiedossa vartiointiliikkeen puhelinnumero.
- Kaikilla ei ole tiedossa vartiointiliikkeen puhelinnumeroa.
- Yrityksellä ei ole käytössään vartiointipalvelua.
- En osaa sanoa.

Onko tiloissa käytössä kameravalvontaa?

- Kyllä.
- Ei.
- En osaa sanoa.

Kuinka työntekijän tulee toimia poistuessaan työhuoneestaan?

- Työntekijän tulee lukita joko työpisteensä tai työhuoneensa ovi.
- Työntekijän tulee lukita sekä työpisteensä että työhuoneensa ovi.
- Työntekijöille ei ole olemassa yhteistä käytäntöä tilanteeseen.
- En osaa sanoa.

Onko työntekijän helppo paeta työhuoneestaan vaaratilanteen sattuessa?

- Kyllä.
- Ei.
- En osaa sanoa.

Millainen hälytysjärjestelmä ja murtosuojaus tiloissa on käytössä?

- Hälytysjärjestelmä ja murtosuojaus ovat tarpeisiin nähden riittäviä.
- Tiloissa on hyvä hälytysjärjestelmä ja murtosuojaus.
- Tiloissa ei ole hälytysjärjestelmää eikä murtosuojausta.
- En osaa sanoa.

Onko laitteet turvamerkitty ja vakuutettu?

- Kyllä, sekä turvamerkitty että vakuutettu.
- Ainoastaan turvamerkitty.
- Ainoastaan vakuutettu.
- Ei kumpaakaan.
- En osaa sanoa

Onko tiloissa riittävästi alkusammutusvälineitä tulipalon sattuessa ja osaako henkilökunta käyttää niitä?

- Kyllä on riittävästi, mutta henkilökunta ei osaa käyttää niitä.
- Kyllä on riittävästi ja henkilökunta osaa käyttää niitä.
- Ei ole riittävästi vaikka henkilökunta osaisi käyttää niitä.
- Ei ole riittävästi eikä henkilökunta osaisi käyttää niitä.
- En osaa sanoa.

Onko poistumisteitä helppo käyttää ja ovatko ne hyvin merkittyjä?

- Kyllä on.
- Poistumisteitä olisi helppo käyttää, mutta merkit puuttuvat
- Erillisiä poistumisteitä ei ole olemassa.
- Poistumistiet ovat hyvin merkittyjä, mutta vaikeakäyttöisiä.
- En osaa sanoa.

Onko tiloissa järjestetty paloharjoitusta ja –tarkastusta?

- Ainoastaan paloharjoitus.
- Ainoastaan palotarkastus.
- Tiloissa on järjestetty sekä paloharjoitus että –tarkastus.
- Tiloissa ei ole järjestetty kumpaakaan.
- En osaa sanoa.

Onko yrityksellä olemassa pelastussuunnitelmaa?

- Ei.
- Kyllä.
- En tiedä, mikä pelastussuunnitelma on.
- En osaa sanoa.

Onko tilojen turvallisuudesta vastaavaa henkilöä nimetty?

- Kyllä.
- Ei.
- En osaa sanoa.

Onko työntekijöillä mahdollisuus ensiapukoulutukseen?

- Kyllä.
- Ei.
- Kyllä on ja osa työntekijöistä on ensiaputaitoisia.
- En osaa sanoa.

Miten sähkökatkoksiin on varauduttu?

- Sähkö riittää hallittuun alasajoon.
- Sähkökatkoksiin ei ole varauduttu.
- En osaa sanoa.

HENKILÖSTÖ- JA KÄYTTÖTURVALLISUUS

Onko työntekijöiden käyttöoikeuksia rajoitettu?

- Ei, työntekijöillä on rajattomat oikeudet.
- Kyllä, työntekijöiden käyttöoikeuksia on rajoitettu jossain määrin.
- Kyllä, työntekijöiden käyttöoikeudet on rajoitettu työssä tarvittaviin oikeuksiin.
- En osaa sanoa.

Pääsevätkö mahdolliset vierailijat yrityksen verkkoon?

- Kyllä.
- Ei.
- Kyllä, mutta ainoastaan vierailijoille varatuilla tunnuksilla.
- En osaa sanoa.

Onko työntekijöillä etäkäyttömahdollisuus?

- Kyllä.
- Kyllä, suojatun yhteyden avulla.
- Ei ole.
- En osaa sanoa.

Järjestääkö yritys säännöllisesti tietoturvakoulutusta henkilöstölle?

- Kyllä, koulutusta järjestetään säännöllisesti.
- Koulutusta järjestetään silloin tällöin, muttei säännöllisesti.
- Koulutusta ei järjestetä.
- En osaa sanoa.

Onko yrityksellä olemassa selkeät ohjeet tietojärjestelmien tietoturvallisesta käytöstä?

- Kyllä on, ja ne on saatettu jokaisen tietoon.
- Kyllä on, mutta jokainen ei välttämättä niistä tiedä.
- Kyseisiä ohjeita ei ole olemassa.
- En osaa sanoa.

Kuinka usein salasana tulee vaihtaa ja onko salasanalle erityisvaatimuksia?

- Salasana tulee vaihtaa tietyin väliajoin ja sen vahvuudelle on asetettu tietyt vaatimukset.
- Salasanaa ei tarvitse vaihtaa muuten kuin käyttäjän halutessa tai poikkeustilanteissa, mutta salasanan vahvuudelle on asetettu tietyt vaatimukset.
- Salasanaa ei tarvitse vaihtaa muuten kuin käyttäjän halutessa tai poikkeustilanteissa, eikä salasanan vahvuudelle ole asetettu vaatimuksia.
- Salasana tulee vaihtaa tietyin väliajoin, mutta sen vahvuudelle ei ole asetettu vaatimuksia.
- En osaa sanoa.

Onko käytössä tunnistuskeinoa, jolla esimerkiksi salasanan resetointia pyytävä henkilö tunnistetaan?

- Kyllä on. Jokaisen henkilöllisyys varmistetaan tietyin keinoin.
- Ei ole.
- En osaa sanoa.

Onko tietoturvarikkomuksista aiheutuvat seuraukset määritelty ja saatettu työntekijöiden tietoon?

- On määritelty, muttei saatettu työntekijöiden tietoon.
- On määritelty ja saatettu työntekijöiden tietoon.
- Ei ole määritelty ollenkaan
- En osaa sanoa.

Onko avainhenkilöille olemassa varahenkilöt?

- Kyllä, varahenkilöt on nimetty avainhenkilöille.
- Avainhenkilöille ei ole olemassa varahenkilöitä.
- En osaa sanoa.

Mitä työntekijän käyttöoikeuksille tapahtuu työsuhteen päättyessä?

- Käyttöoikeudet poistetaan tietyn ajan kuluessa.
- Käyttöoikeudet poistetaan sitten kun muistetaan.
- Käyttöoikeuksia ei poisteta lainkaan.
- En osaa sanoa.

Onko yrityksessä nimetty väärinkäyttötapauksia valvova henkilö?

- Kyllä.
- Ei.
- En osaa sanoa.

Onko seuraukset väärinkäyttötapauksista määritelty ja saatettu työntekijöiden tietoon?

- On määritelty, muttei saatettu työntekijöiden tietoon.
- On määritelty ja saatettu työntekijöiden tietoon.
- Ei ole määritelty ollenkaan
- En osaa sanoa.

Onko jokaisella työntekijällä tiedossa omat vastuunsa ja velvoitteensa tietoturvaan liittyvissä asioissa?

- Kyllä.
- Kyllä, jossain määrin.
- Ei.
- En osaa sanoa.

Huomioidaanko tietoturva yhteistyökumppaneiden kanssa?

- Kyllä.
- Ei.
- En osaa sanoa

Allekirjoittaako työntekijä salassapitosopimuksen työsuhteen alkaessa?

- Kyllä, jokainen työntekijä allekirjoittaa salassapitosopimuksen.
- Riippuu työtehtävästä allekirjoittaako työntekijä salassapitosopimuksen.
- Ei allekirjoita.
- En osaa sanoa.

Tarkistetaanko uutta työntekijää palkatessa hänen taustansa ja muiden tietojen oikeellisuus (henkilötiedot, aikaisemmat työpaikat, koulutus jne.)?

- Uuden työntekijän taustat tarkistetaan, muttei puututa muihin tietoihin.
- Uuden työntekijän taustat ja muut tiedot tarkistetaan perusteellisesti.
- Riippuu työtehtävästä.
- Taustoihin ja muiden tietojen oikeellisuuteen ei puututa.
- En osaa sanoa.

Miten ulkopuolisten työntekijöiden (siivoojat, vartijat, huoltohenkilöstö) kanssa menetellään?

- Ulkopuoliset työntekijät ovat kirjoittaneet salassapitosopimuksen yrityksen kanssa.
- Ulkopuolisten työntekijöiden salassapitosopimuksista huolehtii heidän oma työnantajansa.
- Ulkopuolisten työntekijöiden salassapitosopimuksista ei ole tietoa.
- En osaa sanoa.

Mikäli työssä käsitellään henkilötietoja, onko niiden suojaamisesta huolehdittu kaikissa niiden käsittelyvaiheissa?

- Kyllä on.
- Ei ollenkaan.
- Suojaamisessa esiintyy puutteita.
- En osaa sanoa.

HALLINNOLLINEN TIETOTURVA

Onko yrityksellä johdon hyväksymä tietoturvapolitiikka?

- Tietoturvapolitiikka on laadittu, mutta sillä ei ole johdon tukea.
- Tietoturvapolitiikka on laadittu ja sillä on johdon tuki.
- Tietoturvapolitiikkaa ei ole laadittu.
- En osaa sanoa

Onko tietoturvasta vastaava henkilö nimetty?

- Kyllä.
- Ei.
- En osaa sanoa.

Onko organisaation tietoturvaa kohtaan kohdistuvat mahdolliset uhkat tiedostettu ja otettu huomioon?

- Kyllä on tiedostettu ja otettu huomioon.
- Kyllä on tiedostettu, muttei otettu huomioon.
- Ei ole tiedostettu.
- En osaa sanoa.

Mitataanko tietoturvan toteutumista säännöllisesti?

- Kyllä.
- Kyllä mitataan, muttei säännöllisesti.
- Ei mitata ollenkaan.
- En osaa sanoa.

Onko yritykselle laadittu riskianalyysi ja riskienhallintadokumentti?

- Kyllä, molemmat.
- Ainoastaan riskianalyysi.
- Ei kumpaakaan.
- En osaa sanoa.

Onko yritykselle laadittu jatkuvuus- ja toipumissuunnitelmat?

- Kyllä, molemmat.
- Ainoastaan jatkuvuussuunnitelma.
- Ainoastaan toipumissuunnitelma.
- Ei kumpaakaan.
- En osaa sanoa.

Onko tietoturvan toteutumisesta vastaava henkilö nimetty?

- Kyllä.
- Ei.
- En osaa sanoa.

Onko tietoturvallisuudesta tarvittava ohjeistus helposti saatavilla?

- Kyllä.
- Ei.
- En osaa sanoa.

OHJELMISTOTURVALLISUUS

Voivatko työntekijät asentaa ohjelmia koneisiinsa?

- Kyllä, rajoittamattomasti.
- Kyllä, oikeuksia ohjelmien asentamiseen on kuitenkin rajoitettu.
- Ei lainkaan.
- En osaa sanoa.

Miten ohjelmistojen levyjä ja lisenssejä säilytetään?

- Milloin missäkin.
- Aina lukitussa tilassa.
- En osaa sanoa.

Miten käyttöjärjestelmien ja ohjelmistojen päivitykset hoidetaan?

- Kaikki päivittyvät automaattisesti.
- Päivityksistä vastaa ATK-henkilöstö.
- Osa päivittyy automaattisesti ja osasta vastaa ATK-henkilöstö.
- En osaa sanoa.

Voivatko työntekijät asentaa ohjelmia kotikoneisiinsa työpaikan lisensseillä?

- Kyllä voivat.
- Kyllä, mutta vain joitain ohjelmia.
- Eivät lainkaan.
- En osaa sanoa.

Onko Internetin käyttöä rajoitettu?

- Kyllä, työntekijät saavat vierailla vain sivustoilla, joita tarvitsevat työtehtäviensä hoitamiseen.
- Ei, työntekijät voivat surfata netissä missä vain.
- Kyllä osittain, esimerkiksi Facebook on kielletty työaikana.
- En osaa sanoa.

Seurataanko www-sivustoja, joilla työntekijät vierailevat?

- Kyllä.
- Ei.
- En osaa sanoa.

Onko sähköpostissa käytössä roskapostisuodatin?

- Kyllä on.
- Ei, mutta roskapostin käsittely on huomioitu muuten.
- En osaa sanoa.

Salataanko sähköpostiliikenne?

- Ei, mutta se on mahdollista.
- Kyllä, aina.
- Kyllä, joissain tapauksissa.
- En osaa sanoa.

TIETOVERKOT

Onko käyttörajatun tiedon tallennuksessa käytössä salakirjoitusta ja/tai sähköistä allekirjoitusta?

- Kyllä, molemmat.
- Ainoastaan salakirjoitus.
- Ainoastaan sähköinen allekirjoitus.
- Ei kumpaakaan.
- En osaa sanoa.

Onko omien muistitikkujen liittäminen työpisteen koneisiin sallittua?

- Kyllä.
- Ei.
- En osaa sanoa.

Tiedetäänkö tietoverkkoyhteyden palveluntarjoajan turvallisuusmenetelmistä?

- Kyllä, tarpeeksi.
- Kyllä, muttei tarpeeksi.
- Ei tiedetä juuri mitään.
- En osaa sanoa.

Onko yrityksellä käytössä fyysinen palomuuri?

- Kyllä.
- Ei, mutta ohjelmallinen on.
- Yrityksellä ei ole käytössään palomuuria.
- En osaa sanoa.

Seurataanko palomuurin lokitiedostoja säännöllisesti?

- Kyllä.
- Ei säännöllisesti, mutta silloin tällöin.
- Ei lainkaan.
- En osaa sanoa.

Onko yrityksessä käytössä WLAN ja onko yhteys salattu?

- Kyllä on ja yhteys on salattu.
- Kyllä on, mutta yhteyttä ei ole salattu.
- Kyllä on, muttei tietoa onko se salattu
- Yrityksellä ei ole käytössä WLANia.
- En osaa sanoa.

Näkyvätkö yrityksen palvelimet ulkoverkkoon?

- Kyllä.
- Ei.
- Osa näkyy.
- En osaa sanoa.

Kuinka tietoja varmuuskopioidaan?

- Varmuuskopiointi hoituu automaattisesti ja säännöllisesti.
- Varmuuskopioita otetaan silloin kun on tarvetta.
- Varmuuskopioita otetaan harvoin tai ei laisinkaan.
- Jokainen huolehtii omista varmuuskopioistaan.
- En osaa sanoa.

Miten varmuuskopioita säilytetään?

- Erillisessä paloturvallisessa tilassa.
- Siellä täällä.
- Kirjahyllyssä.
- En osaa sanoa.

Testataanko palautuksen onnistumista säännöllisesti?

- Kyllä.
- Palautuksen onnistumista tulee testattua silloin, kun täytyy palauttaa jotain.
- Palautuksen onnistumista testataan, muttei säännöllisesti.
- Palautuksen onnistumista ei testata lainkaan.
- En osaa sanoa.

Testataanko tietoverkkoa hyökkäysten varalta säännöllisesti?

- Kyllä.
- Kyllä, muttei säännöllisesti.
- Ei lainkaan.
- En osaa sanoa.

Voiko verkkoon liittää ulkopuolisia koneita tai laitteita?

- Kyllä, mutta se on kiellettyä.
- Ei, koska se on estetty.
- En osaa sanoa.

LAITTEISTOTURVALLISUUS

Ovatko laitteistot katkottoman sähkönsyötön piirissä?

- Ainoastaan palvelimet, mutta muut kriittiset laitteistot on tunnistettu ja dokumentoitu.
- Ainoastaan palvelimet.
- Kyllä, kaikki laitteistot.
- Eivät ole.
- En osaa sanoa.

Riittääkö varasähkö kaikkien järjestelmien hallittuun alasajoon?

- Kyllä, kapasiteetti on riittävä.
- Ei, kapasiteetti ei riitä.
- En osaa sanoa.

Onko varasähkön kapasiteetin riittävyys varmistettu onnistuneesti, esimerkiksi simuloimalla sähkökatkoa?

- Kyllä.
- Ei.
- En osaa sanoa

Ovatko laitteistot huoltosopimusten tai takuun piirissä?

- Kyllä, kaikki laitteet ovat sekä huoltosopimusten että takuun piirissä.
- Osa laitteista on sekä huoltosopimusten että takuun piirissä.
- Ainoastaan huoltosopimusten piirissä.
- Ainoastaan takuun piirissä.
- Eivät kummankaan.
- En osaa sanoa.

Onko toipumissuunnitelma laadittu ja testattu käytännössä?

- Toipumissuunnitelma on laadittu, mutta sitä ei ole testattu.
- Toipumissuunnitelma on laadittu ja testattu.
- Toipumissuunnitelmaa ei ole laadittu.
- En osaa sanoa.

Onko työasemista olemassa laiterekisteriä?

- Kyllä on.
- Ei ole.
- En osaa sanoa.

Kirjataanko hävitetty tai käytöstä poistettu laite rekisteriin?

- Kyllä.
- Ei.
- En osaa sanoa.

Onko laitteiden varkaudenestosta huolehdittu?

- Kyllä.
- Ei.
- En osaa sanoa.

Miten toimitaan käytöstä poistettavien tallennusvälineiden kanssa?

- Kiintolevyt tuhotaan fyysisesti ja CD-levyt ja disketit tuhotaan silppurissa.
- Tallennusvälineet nakataan roskiin.
- Riippuu tilanteesta.
- Ne toimitetaan hävitettäväksi yritykselle, joka tarjoaa kyseistä palvelua.
- Jokainen tuhoaa kuten haluaa.
- En osaa sanoa.

TIETOAINEISTOTURVALLISUUS

Onko yrityksellä käytössä tietoaineiston luokittelu?

- Kyllä, kaikki tieto luokitellaan.
- Osa tiedoista luokitellaan.
- Ei lainkaan.
- En osaa sanoa.

Salataanko tietoaineisto?

- Kyllä, kaikki.
- Kyllä, tarpeen vaatiessa.
- Ei.
- En osaa sanoa.

Pääseekö jokainen työntekijä käsiksi eri tietoaineistoihin?

- Kyllä.
- Ei, koska työntekijöiden käyttöoikeuksia on rajoitettu.
- Ei lainkaan.

Onko yrityksellä ohjeistusta asiakirjojen säilyttämisestä?

- Kyllä, asiakirjat tulee säilyttää aina ohjeistuksen mukaan.
- Kyllä, mutta sitä ei juuri noudateta.
- Ei ole.
- En osaa sanoa.

Kuinka luottamuksellista tietoa sisältävä paperiaineisto hävitetään?

- Silppurissa.
- Revitään ja laitetaan roskiin.
- Laitetaan roskiin.
- Ne toimitetaan hävitettäväksi yritykselle, joka tarjoaa kyseistä palvelua.
- Jokainen hävittää, miten haluaa.
- En osaa sanoa.

Onko käytössä erillinen arkistointitila säilytettäville asiakirjoille.

- Kyllä on, lukollinen arkistointitila.
- Kyllä on, lukollinen ja paloturvallinen arkistointitila.
- Kyllä on.
- Ei ole erillistä arkistointitilaa vaan asiakirjat säilytetään työhuoneissa mapitettuina.
- En osaa sanoa.

Tämä on liite 2, joka on 5-sivuinen, ja tämä on liitteen 3. sivu.