



PIENYRITYKSEN TIETOTURVASUUNNITELMA

Opinnäytetyö

Lasse Litmanen

Tietotekniikan koulutusohjelma
Tietoverkkotekniikka

Hyväksytty _____.____.____

SAVONIA UNIVERSITY OF APPLIED SCIENCES Degree Programme Information Technology		
Author Lasse Litmanen		
Title of Project Information security plan for a small company		
Type of Project Final Project	Date 22 June 2010	Pages 43
Academic Supervisor Mr Matti Kuosmanen, Information Systems Manager	Company Supervisor Mr Samppa Sihvonen, IT Expert	
Company Wellness technology specialized company		
Abstract <p>The aim of this thesis was to study how to create a functional information security plan, and use this information security plan for future purposes. It was also important to discover any major information security gaps to ensure best possible safety to valuable data.</p> <p>At the starting point of this thesis there were held couple of meetings about the aspects of the information security plan. The biggest issue was concerning how the information security plan would adapt to possible organizational changes in the future.</p> <p>After the discussion, the actual process of writing quite straightforward. The guidelines given by the CEO cleared any possible confusion concerning the information security plan. The expansion of the company that will be dated in near future is also being considered in the information security plan.</p> <p>The thesis was successful but the real test comes in 2011 when the retail business starts.</p>		
Keywords Information security, VPN, firewalls		
Confidentiality public		

SAVONIA-AMMATTIKORKEAKOULU TEKNIikka KUOPIO

Koulutusohjelma

Tietotekniikan koulutusohjelma

Tekijä

Lasse Litmanen

Työn nimi

Pienyrityksen tietoturvasuunnitelma

Työn laji

Insinööritö

Päiväys

22.06.2010

Sivumäärä

43

Työn valvoja

tietohallintopäällikkö Matti Kuosmanen

Yrityksen yhdyshenkilö

IT-asiantuntija Samppa Sihvonen

Yritys

Hyvinvointiteknologia-alan yritys

Tiivistelmä

Tämän insinööritöön aiheena oli tutkia kuopiolaisen hyvinvointiteknologiaan erikoistuneen yrityksen tietoturvaa ja laatia havaittujen puutteiden pohjalta riittävän kattava tietoturvasuunnitelma. Tietoturvasuunnitelman laatiminen on tärkeää, jotta pystyttäisiin tunnistamaan tiedot, joita suojata.

Työn aloitusvaiheessa oli tutkittava yrityksen kannalta suurimmat tietoturvauhat ja löytää niihin toimivat ratkaisut. Tämä toteutettiin keskustelemalla henkilökunnan kanssa ja etsimällä puutteita tietoturvasta sekä fyysisesti että teknisesti.

Tietoturva-aukkojen löytymisen jälkeen tarkoituksena oli laatia sellainen tietoturvasuunnitelma, jossa on otettu huomioon myös yrityksen lähitulevaisuudessa todennäköisesti kokemat organisaatiomuutokset ja liiketoiminnan laajentuminen.

Työ onnistui siinä määrin, että ne asiat, joita kyseessä oleva yritys halusi painottaa tietoturvasuunnitelmaa laadittaessa, on otettu huomioon.

Avainsanat

tietoturva, VPN, palomuurit

Luottamuksellisuus

julkinen

Sisällysluettelo

Sisällysluettelo	4
1. Johdanto	7
2. Tietoturvariskit	8
2.1. Järjestelmien toimivuus.....	8
2.2. Internetin uhkakuvat	9
2.3. Työyhteisö ja tiedonkulku	9
2.4. Sosiaalisen median tietoturva	10
3. Tietoliikenteen tietoturvasuus	11
3.1. Vikasietoisuus.....	12
3.2. Virukset, madot, troijalaiset.....	12
4. Sosiaalinen tietoturva.....	13
4.1. Salasanapolitiikka	13
4.1.1. Vaatimukset	13
4.1.2. Hallinta	13
4.2. Henkilöstön riskienhallinta.....	14
4.2.1. Sosiaalinen manipulointi	14
4.2.2. Kulunvalvonta.....	15
5. Etätyöskentely	16
5.1. VPN.....	16
5.1.1. Todentaminen	16
5.1.2. VPN yrityskäytössä.....	17
5.2. Kannettavat tietokoneet.....	17
5.2.1. Kovalevyn suojaus	17
5.2.2. WLAN	18
6. Varmuuskopiointi.....	19
6.1. Online-varmuuskopiointi	19
6.2. Nauhavarmistusasema.....	19
6.3. Kannettavat tallennusvälineet.....	19
6.4. Verkkotallennus	19
7. Palomuri.....	20
7.1. Palomuurin toimintaperiaate	20
7.1.1. Palomuurisäännöt.....	22
7.1.2. Fyysinen rakenne	22
7.2. Palomuurin heikkoudet	22
7.2.1. Konfiguroinnin vaikeus	22
7.2.2. Hyökkäykset, joita palomuri ei pysty torjumaan	22
7.3. Ylläpito, testaus ja päivittäminen	23
8. Toiminnan keskeytyminen.....	24
8.1. Palvelimen käyttökatkos	24
8.1.1. UPS.....	24
8.1.2. Vahinkojen välttäminen.....	25
8.2. Ulkopuolisten vahingonteko.....	25
9. Tietoturvasuunnitelma pienyritykselle	26
9.1. Fyysinen tietoturva.....	27
9.1.1. Kulunvalvonta.....	27
9.1.2. Laitteiden suojaus.....	28
9.1.3. Vastuuhenkilöt	29
9.2. Tietoliikenneyhteydet.....	30
9.2.1. Palvelin	32

9.2.2.	Palomuri.....	32
9.2.3.	Extranet.....	33
9.2.4.	Työasemat.....	34
9.3.	Kriittisen tiedon käsittely	36
9.3.1.	Tiedon säilytys	37
9.3.2.	Tiedon tuhoaminen.....	37
9.4.	Suunnitelman käyttöönotto.....	38
9.4.1.	Ohjeistus v. 2011 ja sen jälkeen.....	39
9.4.2.	Hyötynäkökulma sujuvasta ohjeistuksesta	40
10.	Yhteenveto	41
	Lähdeluettelo.....	42

Lyhenteet

ASIC	Application-Specific Integrated Circuit
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
SAN	Storage Area Network
SLA	Service level Agreement
UPS	Uninterruptible power supply
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1. Johdanto

Turvallisuudella tarkoitetaan yleisesti vaaran minimoimista. Sähköisen tiedon turvaamisella tarkoitetaan tietojärjestelmässä olevan tiedon suojelemista luvattomalta käytöltä, tuhoamiselta ja tietokoneen itsensä turvaamista väärinkäytöksiltä. Tietoturva voi olla fyysistä, teknistä tai hallinnollista. Nämä kolme kategoriata voidaan jaotella ennaltaehkäiseviin ja tutkiviin menetelmiin. Ennaltaehkäisevät pyrkivät estämään vahinkoja tapahtumasta ja tutkivat etsivät mahdollisia ei-haluttuja tapahtumia ennen kuin ne tapahtuvat. [1].

Pk-yritysten tietoturva

Jostain syystä suuret kansainväliset yritykset ovat panostaneet tietoturvaan huomattavasti enemmän kuin pienet ja keskisuuret yritykset. Tämä voidaan selittää suuremmalla markkinaosuudella: mitä enemmän suojeltavaa, sitä enemmän sen turvaamiseen kiinnitettävä huomiota.

Kun puhutaan kansainvälisistä markkinoista, voitaneen olettaa huolellisesta perehtymisestä eri maiden käytäntöihin olevan hyvinkin paljon hyötyä pitkällä aikavälillä. Ensikosketus vieraaseen kulttuuriin voi olla järkyttävä, kun ei muistettukaan olla hiljaa niistä yrityksen sisäisistä asioista.

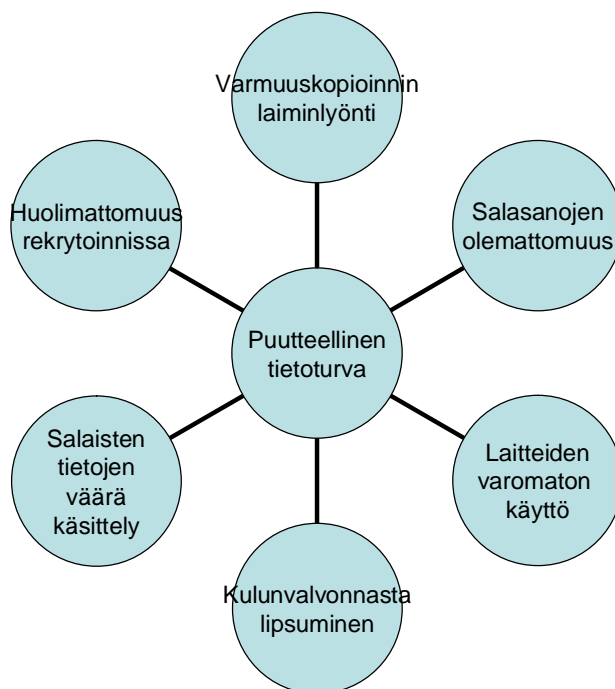
Insinööriyön keskeinen sisältö

Tämän insinööriyön tarkoituksena oli laatia hyvinvointiteknologiaan erikoistuneelle Pk-yritykselle tietoturvasuunnitelma. Kyseisen suunnitelman tärkeimpiä yksityiskohtia ovat tulevaisuuden tietoturvatarpeiden huomioon ottaminen ja uusien työntekijöiden perehdyttäminen noudattamaan suunnitelmassa annettuja ohjeita.

2. Tietoturvariskit

Jotkut tietoturvariskit ilmenevät mahdollisuudesta tahalliseen tietokoneen väärinkäyttöön internetin välityksellä. Toiset ovat niitä, jotka eivät liity millään lailla internetiin: kovalevyn hajoaminen, varkaus tai sähkökatkos. Vaikka kaikkiin mahdollisiin uhkiin on vaikeaa varautua, muutamilla yksinkertaisilla konsteilla voidaan vähentää riskiä kaikkein yleisimpien riskien osalta, olivat ne tahallisia tai tahattomia. [2].

Tietoturvaaukia voi ja pitääkin ennaltaehkäistä. Tämä ei valitettavasti ole tullut kaikille selväksi. Omalla panostuksella on mahdollista saada turvallinen olotila vaikka useat eri tahot olisivatkin valmiita käyttämään häikäilemättömiä keinoja hyväkseen, jotta arvokkaiisiin tietoihin päästäisiin käsiksi. Kuvan 1 avulla on helppo huomata kuinka pienistä asioista tietoturva on loppujen lopuksi kiinni. Esimerkkinä otettakoon varmuuskopiointi, joka ei ole vielä tänäkään päivänä yksityishenkilöillä, yrityksillä tai yhteisöillä hallussa. Vaikka varmuuskopioita tunnollisesti otettaisiinkin, niin yleensä ne jätetään työaseman viereen, jolloin tulipalon sattuessa niistä ei hyötyä ole. Samanlaista huolettomuutta esiintyy salasanojen kanssa. Niitä ei joko ole, tai sitten ne ovat käsittämän helposti arvattavissa. Onhan se jo huvittavaa, että maailman yleisin salasana on edelleen ”password”, Suomessa se lienee ”salasana”. Toisessa ääripäässä onkin sitten liian vaikeasti muistettavat salasanat. Helppohan se on arvata, että erilliselle muistilapulle kirjoitetut salasanat ovat nopeammin selvitettävissä kuin ne, jotka sijaitsevat vain ja ainoastaan käyttäjän päässä. Tässä asiassa onkin hyvin tärkeää löytää kompromissi liian vaikean ja liian helpon salasanan välillä.



Kuva 1 Yleisimmät syyt parantaa tietoturvaa [1].

2.1. Järjestelmien toimivuus

Vaikka tietoturvasta huolehtiminen on hyvä asia, ei siinä kannata mennä liian pitkälle. Yrityksen järjestelmä vastaava on saattanut kehittää niin monimutkaiset kirjautumismenetelmät, että työntekijöiden pääsy omiin tietoihin on lähestulkoon mahdotonta.

2.2. Internetin uhkakuvat

Kun internet noin 30 vuotta sitten sai alkunsa, se oli vain media jota käytti vain yhdysvaltain hallitus ja muutama akateemikko tiedon jakamiseen. Tuohon aikaan vaatimuksia internetin saatavuudelle ja luotettavuudelle ei ollut toisin kuin nykyään, koska internetin käyttö on kasvanut 80-luvulta lähtien eksponentiaalisesti. Suuren suosion ansiosta internetin turvallisuus on uhattuna roskapostituksen, huijausyritysten ja hakkerionnin kaltaisten kyseenalaisten toimien takia. [1].

Turvallinen verkossa liikkuminen

Yleisen tietokoneen käyttäminen esimerkiksi kirjastossa voi olla riskialtista, mikäli ei ole muistanut tyhjentää selaimen välimuistia käytön jälkeen. Sähköpostin käyttäminen on turvallista siihen pisteeseen saakka, kunnes käyttäjä avaa epäilyttävän liitetiedoston. Roskapostituksen välttämiseksi on syytä avata toinen sähköpostilaatikko erilaisiin verkkopalveluihin rekisteröitymistä varten.

Sosiaalisen median tietoturvasta on mainittava ensimmäisenä hyvä ohje, että mitä suositumpi sitä turvallisempi. Sekä tässä, että muissakin luottamuksellista tietoa käsittelevissä verkkopalveluissa on hyvä muistaa, että jos osoitteen alussa lukee ”https”, on yhteys SSL-suojattu. Käyttäjän on hyvä pitää mielessä verkkoidentiteettiä luodessaan, että se voidaan varastaa aivan kuten oikea identiteettikin, joten varovaisuus valttia.

Esimerkkinä sosiaalisen median tietoturvan heikentymisestä mainittakoon sisällöntuottajien suuri tarve tallentaa kaikki käyttäjien tiedot, viestit ja kuvat omille palvelimilleen. Tällainen yksityisyyden loukkaus on arkipäivää ainakin Facebookissa, jonka toimitusjohtajan epäeettinen toiminta on synnyttänyt laajaa keskustelua.

2.3. Työyhteisö ja tiedonkulku

Yhteisöllisyys ei ole uusi keksintö, mutta se on käytössä edelleen. Nykyisin se on yksi tärkeimmistä epävirallisen tiedon jakelukanavista, eikä mikään estä sitä kehittymästä myös virallisen tiedon välittäjäksi. Yhteisöllisyyden peruspiirteinä voidaan pitää tilannetta, jossa useat ihmiset tekevät samaa asiaa samanaikaisesti ja käsittelevät uudelleen toistensa tuotteita tai informaatiota.

Työyhteisö voi tuoda liiketoimintaan lisää turvallisuutta tai turvattomuutta. Pätevä tietoturvavastaava voi parantaa turvallisuutta kouluttamalla henkilökuntaa enemmän tietoisiksi riskeistä.

Jos yrityksessä eri henkilöt tekevät erilaisilla ohjelmilla eri asioita on sanomattakin selvää, että tieto joka tässä tapauksessa syntyy, on kovin heterogeenista. Tämä hankaloittaa selvästi esimerkiksi tuotekehitystyötä. [3].

Web 2.0 on tekniikka, jota sanotaan osallistuvaksi Webbiksi. Tämä tarkoittaa sitä, että käyttäjät voivat itse osallistua sisällön tuottamiseen. Vaikka blogit, Wikit ja valokuvien jakopalvelut ovatkin hyvin käteviä tiedon välittäjiä, ne eivät kuitenkaan ole turvassa määrätietoisilta hyökkääjiltä.

Edellä kuvatulla tekniikalla luotuja palveluja kutsutaan myös sosiaalisen median nimellä. Nimitys on lähtenyt todennäköisesti ajatuksesta, että ihmisten sosiaalinen kanssakäyminen

on siirtynyt verkkoon ja Internet on noussut haastamaan perinteisiä medioita ihmisten ajankäytöstä.

Wikit työvälineenä

Kun työelämä kehittyy yhä enemmän intensiivisemmäksi ja tieto-riippuvaisemmaksi, on taattua tarvetta saada työntekijät paikallistamaan ja uudelleen käyttämään jo olemassa oleva tieto yrityksen sisällä. Paljon hyödyllistä tietoa sekä tieto-taitoa löytyy yhä useammin ihmisten päästä. Mikäli tietoa ei ole dokumentoitu, sen löytäminen saattaa tarkoittaa kollegan ajatusten lukemista. Pienemmissä yrityksissä työkavereiden tunteminen on helpompaa, mutta henkilöstön kasvaessa tiedon välitys ihmisten kesken vaikeutuu huomattavasti.

Idea järjestää alue, jonne voidaan säilöä kaikki yrityksen sisällä liikkuva tieto, on järkeenkäypä. Toteutus onkin sitten toinen asia, sillä työntekijöillä ei aina ole motivaatiota lähettää webmasterille viimeisimpiä tietoja edistymisestään. Tässä vaiheessa ajatus Wikin käyttämisestä tulee houkuttelevammaksi, sillä yrityksen sisäinen wiki-sivusto alentaa huomattavasti kynnystä osallistua tiedon jakoon. [4].

2.4. Sosiaalisen median tietoturva

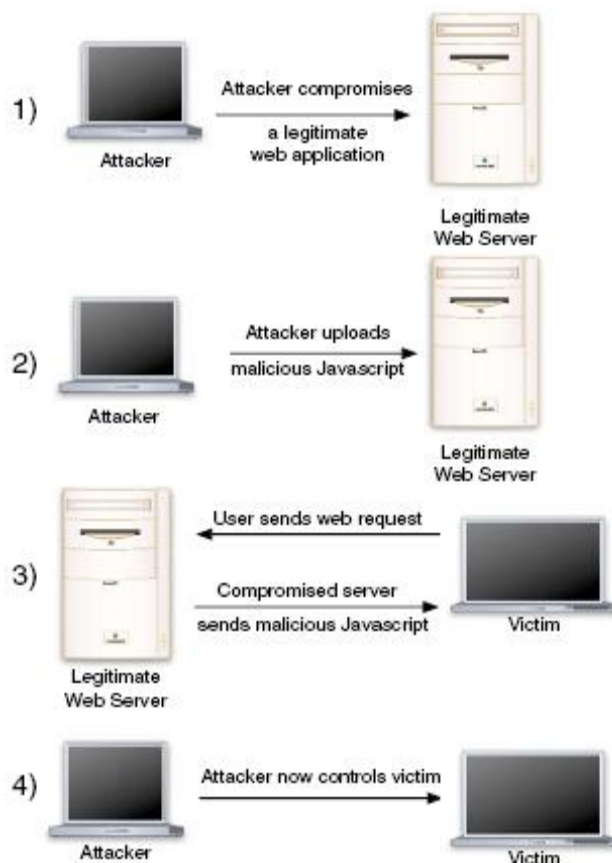
Jokaisella työpaikalla on sovittava yhteiset pelisäännöt sosiaalisen median käytöstä työntekijöiden ja johtoportaalle välillä. Oli sitten kyse Twitteristä, Facebookista tai Youtubesta, jatkuva tiedonjako molempiin suuntiin aiheuttaa varmasti riskejä, mikäli ohjeistusta ei ole olemassa. Ylivoiimaisesti suurin riski on kuitenkin riskin tiedostamattomuus. Verkossa kyllä selviää ilman suurempia tietoturvaohjeita käyttämällä tervettä järkeä. Toinen suuri riski piilee tiedostojen jakamisessa toisten käyttäjien kesken. Tästä syystä kuka tahansa voi halutessaan lähettää haittaohjelman varsin vaivattomasti.

3. Tietoliikenteen tietoturvallisuus

Tietoliikennelaitteisiin kuuluvat tyypillisesti reitittimet, kytkimet, palomuurit ja muut telekommunikaatiolaitteet. Tällaiset laitteet tulisi olla:

- Fyysisesti suojattu
- Ennalta tarkastettu
- Huolellisesti konfiguroitu
- Tarkasti monitoroitu
- Kriittisiltä osin kryptattu [5].

Suojauksella tarkoitetaan laitteiden fyysistä turvaamista, jolla pyritään ehkäisemään rikoutumisia. Tähän tarkoitukseen on myös olemassa erikseen ostettavia laitteita, joista hyvinä esimerkkeinä mainittakoon ylijännitesuoja sekä UPS. Tarkastamisen voi käsittää niin, että yrityksen tietoturvavastaava käy ennen laitteen käyttöönottoa toteamassa, että laite on valmis käytettäväksi. Konfigurointia tapahtuu varsinkin palomuurin ja palvelimen asennuksen yhteydessä. Tällä pyritään välttämään tehdasasetusten jättämistä laitteisiin, mikä on yleensä varsin huono vaihtoehto. Monitorointi tulee silloin kysymykseen, kun tietoliikenteessä havaitaan katkos tai muu vastaava häiriö. Tällöin tarkastetaan laitteiden lokitiedot, joista käy ilmi mikä oli vialla. Kryptauksella viitataan lähinnä palvelimen kiintolevyjen salaamiseen. Toinen hyvä käyttökohde voisi olla kannettavat tietokoneet, koska näissä kuljetettavat tiedot ovat helposti varastettavissa. Käytännössä kyseinen toimenpide edellyttää käyttäjältä salasanan muistamista, jolla tietokoneen tietoihin voi ylipäätensä olla mahdollista päästä käsiksi.



Kuva 2 Hyökkääjä ottaa haltuunsa Web-palvelimen [6].

Oma lukunsa tietoliikennelaitteissa ja niiden suojauksessa on Web-palvelin. Jos virustorjunta ei ole ajan tasalla, ensimmäistä hyökkäystä ei tarvitse pahimmassa tapauksessa odottaa montaakaan sekuntia. Tällöin Kuvan 2 mukaisesti hyökkääjä ottaa haltuunsa haavoittuvan Web-palvelimen, syöttää sinne haluamansa koodin, käyttäjä ottaa yhteyden palvelimeen ja käyttäjän kone on hyökkääjän hallussa.

3.1. Vikasietoisuus

Vikasietoisuus tarkoittaa kykyä jatkaa annettua tehtävää huolimatta ilmenneistä virheistä. RAID-tekniikka on hyvä esimerkki vikasietoisuudesta: levyn kirjoitusnopeus laskee, mutta systeemi kykenee silti jatkamaan tehtäväänsä ilman, että virhettä on edes ehditty korjata.

Redundanttisuus tietoliikenteessä

Kun tietoverkkojen käytön edellytyksenä on niiden katkeamaton ja häiriötön tiedonkulku, täytyy vikasietoisuuden olla kunnossa. Jotta odottamattomilta katkoksilta vältyttäisiin, ratkaisuna tähän löytyy redundanttisuudesta. Tietoliikenteen kohdalla tämä voi tarkoittaa esimerkiksi kahden tai useamman verkon rakentamista, jolloin yhden viallisen verkkokortin mukana ei kaadu koko tiedonkulku, vaan tieto kulkee sen jälkeen jotain vaihtoehtoista reittiä.

Jos yrityksellä on ainoastaan yksi palvelin, jota käytetään moneen eri tarkoitukseen, tietojen häviämisen riski voi olla suuri. Suosittu ratkaisu tähän tilanteeseen on yleensä niin sanottu klusteritekniikka, jossa tarkoituksena on liittää yhteen kaksi tai useampia tietokoneita tai palvelimia. Hyvänä esimerkkinä tällaisesta ratkaisusta on Blade Server-tekniikka, jossa pienikokoisia palvelimia on sijoitettuna niin sanottuun palvelinräkkiin säästäten näin tilaa ja sähköä.

3.2. Virukset, madot, troijalaiset...

Kolme edellä mainittua ovat mahdollisesti kaikkien häiritsevimpiä tietoturvauhkia mitä yksittäinen käyttäjä voi kohdata. Nämä voivat yhdessä tai erikseen muuttaa tai poistaa verkossa jaettavia tiedostoja, tukkia sähköpostipalvelimen häijyllä verkkoliikenteellä ja luoda ”takaoven” järjestelmääsi, jonka avulla hyökkääjä voi ottaa tietokoneesi kokonaan haltuunsa. [5].

4. Sosiaalinen tietoturva

Monissa yrityksissä tekninen tietoturva on kunnossa. Tärkeimmät tiedot on suojattu palomuurilla ja virustorjuntaohjelmistolla, mutta suurin tietoturvariski löytyy edelleen näppäimistön ja tuolin välistä. Esimerkkinä otettakoon ulkoistettu tietoturvan hoitaminen, jolloin yrityksen ulkopuolinen henkilö pääsee käsiksi kriittisiin tietoihin, jotka voivat olla tuotekehitys- tai asiakastietoja.

Tyypillisimpiä keinoja tällaisten tapausten ehkäisyyn ovat tiedon saamisen kontrollointi, juridinen vastuu ja henkilökunnan koulutus. Liian suuri luottamus henkilöstön etiikkaan laskee tietoturvan tasoa merkittävästi. Kun organisaation sisällä säilytetään luottamuksellista tietoa sähköpostissa tai henkilön päässä, sitä hankala pitää turvassa ja hallinnassa.

4.1. Salasanapolitiikka

Salasanat ovat nykyisin kaikkialla. Todentaminen toteutetaan yleensä käyttämällä yhdistelmää: käyttäjätunnus ja salasana. Tästä syystä, uhrin henkilökohtaisten tietojen ja hyökkääjän välillä ei ole mitään muuta kuin salasana. Tietämällä kyseessä olevan henkilön salasan, kuka tahansa voi esiintyä verkossa jonain toisena henkilönä. Yhteiskunnan ollessa yhä enemmän riippuvaisempi salasanoista, se on myös yhä enemmän haavoittuvaisempi, mikäli näitä salasanoja onnistutaan murtamaan.

4.1.1. Vaatimukset

Salasanapolitiikan ei ole tarkoitus hankaloittaa työntekijöiden elämää, vaan antaa mahdollisuus turvalliseen työskentelyyn. Tiettyjä erikoismerkkejä ei ole tarkoitus vaatia salasanoihin, vaan enemmänkin isojen ja pienten kirjainten monipuolista käyttöä. Ehkä tärkein vaatimus on kuitenkin salasanan riittävä pituus: lyhyt salasana on helpompi murtaa kuin pitkä. [7].

Hyvän salasanan ominaisuudet:

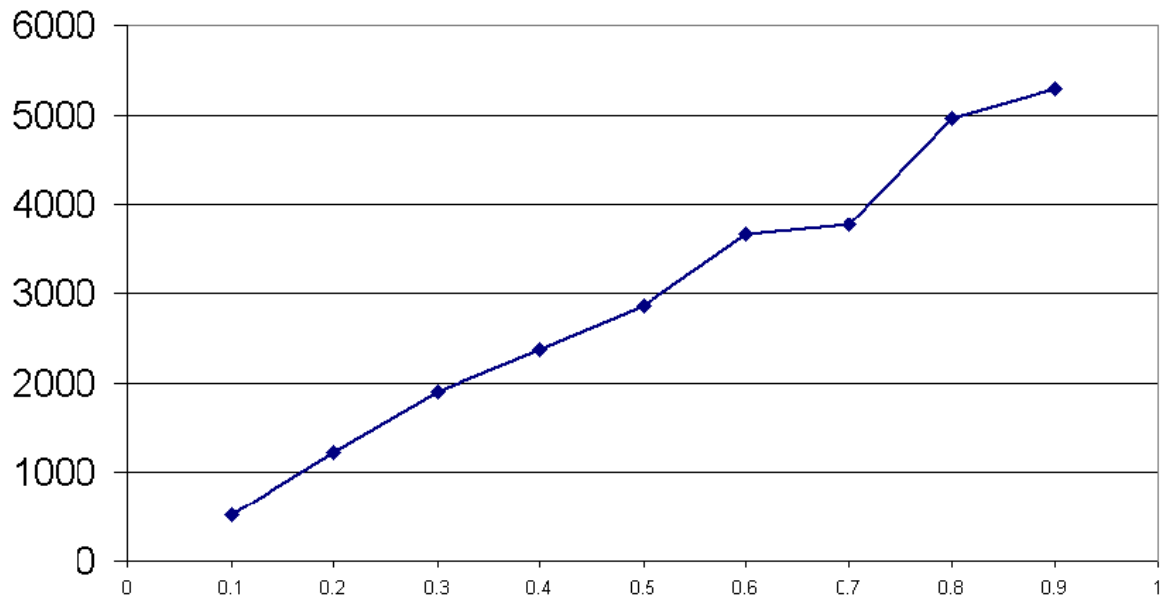
- vähintään 8 merkkiä pitkä
- sisältää isoja sekä pieniä kirjaimia, numeroita ja erikoismerkkejä
- ei ole arvattavissa
- ei ole sana
- ei ole käytössä muualla
- vaihtuu aina välillä

4.1.2. Hallinta

Otettaessa huomioon ihmisten rajoittuneen muistikapasiteetin, on mietittävä tarkkaan, kuinka hankalan salasanan voi vaatia muistamaan? Helppo salasana ei vaadi ihmeitä muistamisen kannalta, mutta tämä tarkoittaa myös sitä, että se on myös helpompi murtaa. Tämän voi ratkaista siten, että käyttäjiä huomautetaan ohjelmallisesti vaihtamaan salasana esimerkiksi 60 päivän välein. [7].

Kuvan 3 kuvaajasta voimme huomata kuinka paljon vahinkoa huonomuistiset käyttäjät voivat aiheuttaa. X-akselilla on kuvattuna käyttäjän todennäköisyys unohtaa seitsemän numeroa sisältävä luku ja y-akselilla kuinka paljon haittaa siitä aiheutuu. Ihmiset, jotka eivät muista salasanoja, kirjoittavat niitä paperille, joten ne ovat helpommin murrettavissa.

Kultaisen keskitien löytäminen tässä asiassa on hankalaa, mutta ei mahdotonta. Salasana, joka on helppo muistaa, mutta vaikea murtaa, saadaan yhdistämällä numeroita, kirjaimia (isoja sekä pieniä) ja erikoismerkkejä. Näitä ei kannata yhdistellä täysin sattumanvaraisesti, koska kätevän muistisäännön kehittäminen tässä tapauksessa ei välttämättä nopeasti löydy. Järkevintä olisi keksiä ensin sana, joka alkaa isolla alkukirjaimella. Tämän jälkeen sanan molemmille puolille sijoitetaan muutama numero ja erikoismerkki.



Kuva 3 Käyttäjän vähäisestä muistista aiheutuva haitta [7].

4.2. Henkilöstön riskienhallinta

Erehtyminen on inhimillistä, kuullaan sanottavan. Tämä pätee myös yritysmaailmaan. Kaikki uhkakuvat mitkä voivat käydä toteen, eivät välttämättä koske yrityksen ulkopuolelta tulevia riskejä. Henkilökuntaan kuuluvat ihmiset voivat huolimattomalla käytöksellään olla suurikin riski tietoturvallisuuden kannalta. Esimerkkinä mainittakoon kahvikupin kaatuminen kannettavan tietokoneen päälle, jolloin kaikki tallentumattomat tiedot menetetään. [8].

4.2.1. Sosiaalinen manipulointi

Meillä ei ole suurta tarvetta epäillä auktoriteettiasemassa olevia henkilöitä mistään vilpillisestä. Juuri tähän ”Social Engineering”, suomeksi sosiaalinen manipulointi luottaakin. Kyseessä on yksinkertaista psykologiaa käyttävä menetelmä, jonka avulla on mahdollista saada haltuunsa yrityksen salasanoja sekä avaimia. Eräs yleisimmistä keinoista on esittäytyä mikrotukihenkilöksi tai Internet-operaattorin vastuuhenkilöksi ja pyytää verkkotunnuksia puhelimen välityksellä. [9].

4.2.2. Kulunvalvonta

Kulunvalvonta ei välttämättä tarkoita pääsyn estämistä vaan enemmänkin sen kontrolloimista. Tietoturvapäällikön on oltava tietoinen siitä, kuka on oikeutettu pääsemään esimerkiksi palvelinhuoneisiin ja kuka ei. Onnistuneen kulunvalvonnan edellytyksenä on kolme seikkaa:

- Pääsyn rajoittaminen vain ja ainoastaan oikeille henkilöille
- Luvattoman tunkeutumisen ilmaiseminen hälytyksenä
- Kattava tallennus kaikista liikkeistä mitä valvotuissa tiloissa ilmenee. [1].

5. Etätyöskentely

Kun etätyöskentely tulee yritykselle välttämättömäksi, on otettava myös huomioon etätyöskentelyn tietoturva. Tiedot, joihin otetaan yhteys etänä, tulisi pitää vahvan todennuksen takana. [1].

Internetin ansiosta nopea tiedonvälitys on mahdollista yhteistyökumppaneiden, etätyöntekijöiden ja asiakkaiden kanssa. Maantieteellinen kaukaisuus ei ole enää läheskään niin suuri ongelma kuin ennen. Lyhyesti sanottuna, kansainvälinen markkinapotentiaali on Internetin ansiosta lähes rajaton. [11].

5.1. VPN

Tietoverkko koostuu muutamasta tai useammasta laitteesta, jotka kykenevät kommunikimaan keskenään siihen tarkoitettulla menetelmällä. Tällaiset laitteet ovat esimerkiksi tietokoneet, tulostimet ja reitittimet, jotka voivat sijaita maantieteellisesti hyvinkin erilaisissa paikoissa.

VPN on kommunikaatioympäristö, jonne pääsy on sallittu ainoastaan ennalta määrätyn yhteisön jäsenillä. Se on rakennettu tiedonkulkuun osallistumista varten ja tätä tietoa jaetaan ei-julkisesti. [10].

VPN:n kriittisin elementti on turvallisuus. Tieto täytyy saada siirrettyä turvallisesti paikasta toiseen. Toinen tärkeä elementti on luotettavuus. Tätä tosin voidaan parantaa käyttämällä QOS:ia ja SLA:ta. [11].

5.1.1. Todentaminen

Tunnettu ja luotettu käyttäjä (joskus ainoastaan käyttäessään luotettuja laitteita) voi saada haltuunsa oikeudet käyttää resursseja, joita ei ole tarkoitettu tavallisille käyttäjille. Palvelimetkin voivat joutua todentamaan itsensä liittyäkseen VPN-verkkoon.

Todentaminen voidaan hoitaa monella eri tavalla. Se voidaan tehdä käyttämällä apuna fyysisiä laitteita kuten palomureja. Muita menetelmiä ovat salasanat, biometrinen tunnistaminen ja salaus. Vahvassa todentamisessa käytössä on salauksen lisäksi jokin muu todentamismenetelmä.

Salaus

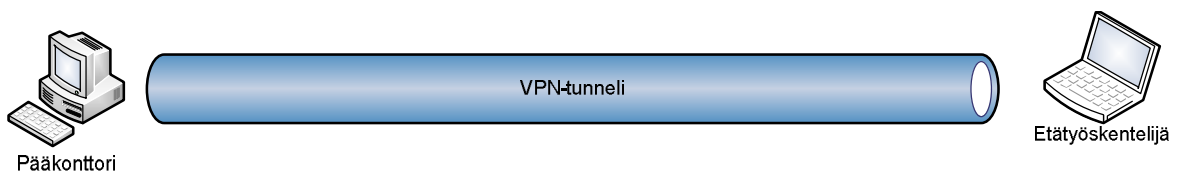
Eräs VPN:n salausmenetelmistä on PKI. PKI käyttää hyödykseen logaritmeja, tekijöihin jakoa sekä suuria alkulukuja (512-, 768- ja 1024-bittisiä). PKI-tekniikkaan kuuluu kahden asymmetrisen avaimen muodostama pari: julkinen avain ja yksityinen avain, joita on melkein mahdotonta johtaa laskennallisesti toisistaan. Kaksi osapuolta voi käyttää toistensa julkista avainta tiedon salaamiseen ja käyttää omaa yksityistä avainta purkamaan saatu tieto. [11].

Tunnelointi

Useat VPN-tekniikat käyttävät jotakin tunnelointiprotokollaa luodakseen yksityisen tietoverkon. Näitä ovat esimerkiksi PPTP, layer 2 forwarding protocol ja IPSec Tunnel mode. Tunnelointia käyttämällä verkossa liikkuva tietopaketti voidaan koteloida toisen paketin sisälle liikuttaessa protokollasta toiseen. Tämä tarkoittaa sitä, että käyttäjä voi lähettää paketin satunnaisella osoitteella, jos se sisältää paketin, jossa on hyväksyttävä osoite. [12].

5.1.2. VPN yrityskäytössä

Tietoturvallisuuden mittava kasvu on mitä suurimmissa määrin tarpeellisin yksittäinen asia minkä yritys huomaa käyttöönoton jälkeen. Asiakkaat, jotka haluavat kirjautua omilta koneiltaan niin sanottuun extranet-palveluun (jollaiseksi myös verkkokauppa lasketaan), eivät voi saastuttaa yrityksen koneita edes niin halutessaan. [5].



Kuva 4 VPN yksinkertaistetussa muodossa

Kuten kuva 4 selkeästi osoittaa, VPN on pohjimmiltaan tunneli, jonka avulla pystytään kommunikoimaan turvallisesti ilman, että tarvitsisi pelätä tiedon vuotamista tietoverkon ulkopuolelle. Tieto, joka kulkee VPN-tunnelissa, on kryptattu, joten tunkeutujan täytyy nähdä erikoisen paljon vaivaa saadakseen haluamansa. Helpoiten tämä onnistuisi tekeytymällä IT-tukeen kuuluvaksi henkilöksi ja kysymällä tunnuksia.

5.2. Kannettavat tietokoneet

Tietotekniikka on kehittynyt hyvin pitkälle niistä ajoista, kun PC oli liian raskas nostettavaksi työpöydälle. Kannettavat tietokoneet ovat nykyisin yhtä tehokkaita kuin työpöytämallit, mutta tuovat mukanaan uusia ongelmia, koska helppo liikuteltavuus tarkoittaa myös helppoa varastamista.

5.2.1. Kovalevyn suojaus

Kaikkein ilmeisimmät kustannukset kannettavan varastamisesta tulevat tietenkin laitteiston uusimisesta ja tiedon pelastamisesta. Kustannukset, jotka käytetään liikuteltavien laitteiden tietoturvaan, ovat murto-osan siitä, mitä ne ovat varkauden sattuessa. Tällaisia tapauksia varten on kehitetty kokonaisen kovalevyn salaavia ohjelmia, joiden ansiosta varas ei kykene saamaan tietokonetta käyntiin ilman toimivaa salasanaa.

5.2.2. WLAN

Ilman kaapeleita toimiva verkko ylläpitää suosiotaan helppoudellaan ja joustavuudellaan. Epäilemättä, langaton yhteys tarjoaa enemmän joustavuutta kuin langallinen. Ihmisten ei tarvitse etsiä enää verkkopistoketta seinästä eikä myöskään kompastella verkkokaapeleihin. Suosion innoittamana kahvilat, lentokentät ja muut julkiset tilat ovat alkaneet tarjota mahdollisuutta käyttää langatonta internet-yhteyttä.

Kuitenkin, laajalle levinneen teknologian haittapuoliin kuuluvat tietoturva-aukot ovat hädastaneet kehitystä yritysmaailmassa. WLAN liikkuu ilmateitse, mikä tarkoittaa sitä, että siinä ei ole samanlaisia rajoitteita kuin langallisessa verkossa. Negatiivisen asian tästä tekee se, että signaalin lähetysalueella kukaan ei voi fyysisesti suojella verkossa tapahtuvaa liikennettä. [1].

6. Varmuuskopiointi

Kymmenen vuotta sitten varmuuskopiointistrategian suunnittelu oli varsin suoraviivainen prosessi: pienillä ja keskisuurilla yrityksillä oli tapana ylläpitää useita palvelimia, jokaisella oma nauhavarmistussysteemi, josta vastuuhenkilöt kävivät säännöllisin väliajoin vaihtamassa nauhat. Viime vuosina, vaihtoehdot joilla varmuuskopiointi voidaan hoitaa, ovat kasvaneet. Tämän lisäksi, laitteiden monipuolistuminen ja suojeltavan tiedon nopea kasvu ovat monimutkaistaneet tiedon turvaamista. [13].

6.1. *Online-varmuuskopiointi*

Online-varmuuskopiointi on palvelu, joka tarjoaa käyttäjille verkossa olevan systeemin varmuuskopiointiin ja tietokoneella luotujen tiedostojen säilömiseen. Tyypillisesti tällaiset systeemit on rakennettu käyttäjän koneelle asentaman ohjelman ympärille, joka toimii yleensä ajastetusti kerran päivässä. Kyseinen ohjelma kerää, pakkaa, kryptaa ja lähettää tiedot ulkoisen palveluntarjoajan palvelimille.

6.2. *Nauhavarmistusasema*

Kuten tavallinen nauhuri, nauha-asemat nauhoittavat tietoa joustavalle, selluloidin kaltaiselle materiaalille, jota voidaan lukea tai poistaa. Nauha-asemien yksi hyöty on suuri kapasiteetti ja erinomainen hinta-laatusuhde verrattuna varmuuskopiointiin kiintolevyille. Haittapuolena mainittakoon se, että tieto tallennetaan nauhoille peräkkäin, joten käyttäjän täytyy kelata nauha saadakseen haluamansa tiedon esiin.

6.3. *Kannettavat tallennusvälineet*

Levykkeet eivät ole enää standardin asemassa tietokoneissa. Useimmat käyttäjät ovat siirtyneet käyttämään helpommin liikuteltavia, nopeammin tallentavia ja suuremman tallennuskapasiteetin omaavia niin sanottuja usb-”muistitikkuja”, jotka erinomaisen hinta-laatusuhteensa ansiosta tulevat varmasti olemaan kotikäyttäjien suosiossa vielä pitkään. [13].

6.4. *Verkkotallennus*

Siitä ei ole kovinkaan kauaa, kun tallennuslaitteiden säilytyspolitiikka tarkoitti varmuuskopioitujen tietojen säilytystä täsmälleen samassa tilassa muiden yrityksen tietokoneiden kanssa. SAN-teknologian kehityksen myötä, kiintolevyt ja nauha-asemat eivät välttämättä olekaan pääkonttorin tiloissa vaan jopa useiden satojen kilometrien päässä missä päin tahansa maapalloa. [1].

7. Palomuuuri

Internet tarjoaa pääsyn tiedon lähteille ja kyvyn julkaista tietoa vallankumouksellisella tavalla. Tässä on mitä suurimmassa määrin myös vaarana vääristää ja tuhota tietoa. Palomuuuri on suojausmekanismi, joka sallii tietoverkon pääsyn Internetiin pitämällä samalla yllä tietyn tasoista turvaa. [14].

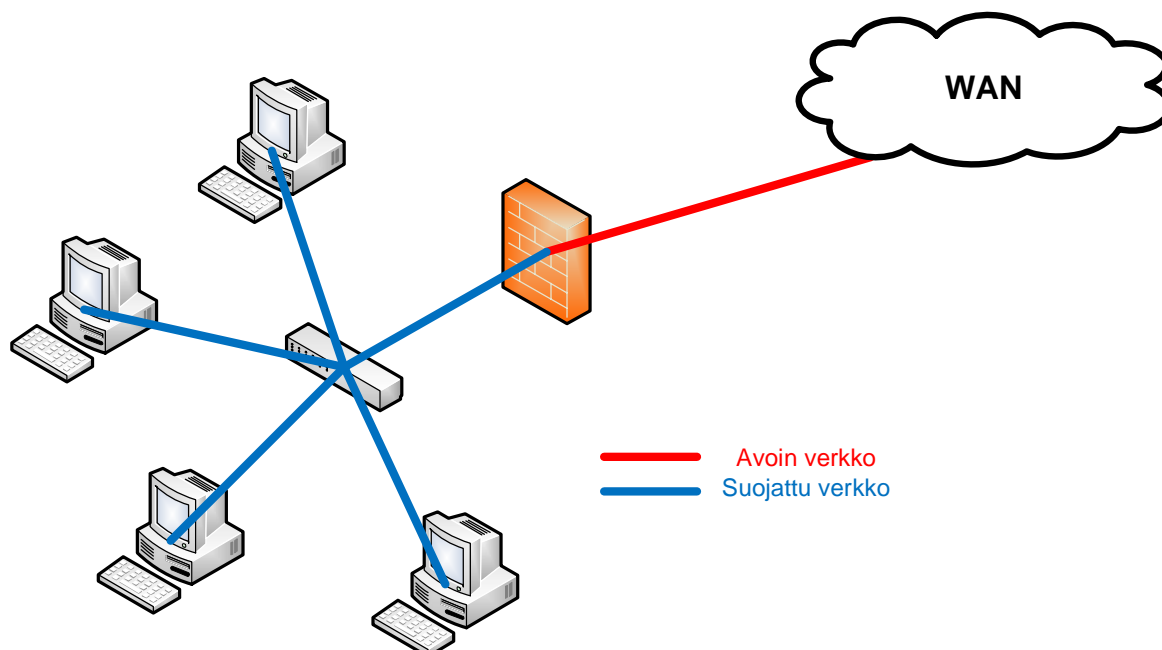
On järkevää pitää mielessä, että palomuuuri voi ainoastaan vähentää tietoturvamurron mahdollisuutta. Ainoa täysin varma tapa estää vahingon syntyminen on yksinkertaisesti katkaista yhteys Internetiin ja sulkea kaikki verkossa sijaitsevat laitteet. Tämän lisäksi, palomuuuri tulisi aina olla ainoastaan lisänä isäntä-koneen turvallisuudelle, ensisijaisesta turvallisuuspolitiikasta päättää käyttäjä itse. Tästäkin huolimatta, palomuuuri on tärkeä turvallisuuslaite, jota tulisi käyttää aina kun organisaation täytyy suojella tietoverkkoa. [14].

Ominaisuudet, jotka nykyaikaisissa palomuuureissa ovat standardien mukaan käytössä:

- VPN
- NAT
- lokitietojen tarkastelu
- virustorjunta
- hälytysominaisuus
- kryptaus

7.1. *Palomuurin toimintaperiaate*

Palomuurit ovat olleet olemassa jo useiden vuosien ajan ja ne ovat vakiinnuttaneet paikansa luonnollisina Internetiin kytkettyjen tietoverkkojen komponentteina. Normaalisti palomuuuri suojelee tietoverkkoa Internetistä päin tulevilta pääsy-yrityksiltä. Samanaikaisesti palomuuuri antaa turvatun verkon kommunikoida ulkoisen verkon kanssa. Tämän mahdollistaa palomuurin kyky erottaa yhteydet ulkoapäin tulevien ja sisältäpäin tulevien välillä. Näin ollen sen on mahdollista rajoittaa ulkoapäin tulevia yhteyksiä ja samalla pitää sisältäpäin tulevien määrän suurena. [15].



Kuva 5 Palomuurin toimintaperiaate

Kuvassa 5 on yksi yleisimmistä palomuuriratkaisuista. Tarkoituksena on siis suojata lähiverkko ulkoapäin tulevilta hyökkäyksiltä. Tähän skenaarioon tarvitaan palomuurin lisäksi kytkin, joka jakaa suojatun verkon kaikille lähiverkon työasemille. Tämän jälkeen kytkin ja palomuri yhdistetään, jolloin kaikki ulkoapäin tuleva tietoliikenne suodattuu palomuurin läpi, joten lähiverkko on siis siltä osin suojattu.

Yllä on kuvattu lähinnä fyysisiä palomureja, jotka voidaan kytkeä päälle ja pois virtakytimestä. Näiden lisäksi on olemassa myös niin sanottuja ohjelmallisia palomureja, jotka yksinkertaisesti vain asennetaan tavallisten tietokoneohjelmien tapaan käyttöjärjestelmään. Yksi esimerkki tällaisesta on Windowsin oma palomuri, joka XP:ssä estää ainoastaan ulkoa tulevan liikenteen, mutta Vista:ssa se pystyy jo estämään ulospäin menevän liikenteen.

Palomuurin voi myös rakentaa itse. Tämä onnistuu, kun hankkii itselleen juuri tähän tarkoitukseen tarkoitetun Linuxin palomuri-jakelun. Tällaiset jakelut eroavat muista Linux-jakeluista siinä, että niiden tarkoitus on toimia palomuri-ohjelmistona sulautetuissa järjestelmissä, yleensä PC:ssä. Suosituimpia versioita näistä ovat IPCop ja m0n0wall.

Palomuurien erot tiedon turvaamisessa

Ensimmäisen sukupolven palomuurien käytäntö suojata tietoa oli pakettisuodatus. Tällä tarkoitetaan TCP/IP-pakettien tarkkaa seulomista siten, että ainoastaan hyväksytyistä osoitteista tulleet paketit pääsevät läpi. Luonnollisestikin tämä ei ole riittävä tapa suojautua verkon vaaroilta, mutta onneksi pakettisuodatuksen kehittyneempi menetelmä pystyy suodattamaan myös ei-toivotut Internet-protokollat, jolloin tietoturva kasvaa merkittävästi.

Palomuuria voi myös käyttää yhdessä välityspalvelimen kanssa Intranet-tyyppisissä ratkaisuissa. Tällöin esimerkiksi yritys haluaa rajoittaa työntekijöidensä verkkoliikennettä pois sivustoilta, jotka eivät liity heidän toimenkuvaansa. Samanlaista sisältösuodatusta käytetään myös lukuisissa kouluissa ja kirjastoissa, joissa halutaan välttää alaikäisten pääsevän käsiksi kiellettyyn materiaaliin.

7.1.1. Palomuurisäännöt

Palomuurisäännöillä voidaan määritellä mitä palveluita halutaan päästää läpi ja mitä ei. Sääntö määrittelee muuttujat, jotka valitsevat oikean toimintatavan kulloisellekin yhteydelle. Riippumatta palomuurin mallista, minimissään sääntö koostuu kahdesta ip-osoitteesta, palvelusta ja toimintatavasta.

Yleensä uutena ostetuissa palomuuureissa on oletuksena palomuurisääntö, joka sallii ulospäin menevän liikenteen ja estää ulkoapäin tulevan liikenteen. Lähtökohtaisesti tämä on hyvä asia, mutta riittävän turvallisen systeemin rakentamiseksi tarvitaan myös sääntöjä, jotka suodattavat ulospäin menevää liikennettä

7.1.2. Fyysinen rakenne

Markkinoijien keksimä termi rautapohjainen palomuri sisältää ainakin mikroprosessorin, firmwaren ja oman käyttöjärjestelmän. Jotkut valmistajat menevät niinkin pitkälle, että korvaavat kovalevyn flash-muistilla ja asentavat mikroprosessorin rinnalle asic-mikrosirun. Näitä innovaatioita on perusteltu muun muassa alhaisemmalla toimintalämpötilalla ja ympäristöystävällisyydellä. [1].

7.2. *Palomuurin heikkoudet*

Monet yritykset painottavat oman tietoliikenteensä turvaamisessa ulkoapäin tulevien hyökkäysten ennaltaehkäisyyn. Tällä menetelmällä pyritään estämään tietoverkon käyttö niiltä, joilla ei ole sinne pääsyoikeutta. Palomuurit ovat suuressa roolissa näin toteutetussa hyökkäysten torjunnassa. Huolimatta suurista rahamääristä joita käytetään tietoturvaan, hyökkääjille on kuitenkin vaivatonta päästä käsiksi kriittisiin tietoihin, ohitettuaan ensin palomuri. [5].

Tällaisen skenaarion pystyy kiertämään käyttämällä niin sanottua demilitarisoitua aluetta. Kyseessä on aliverkko, joka on sijoitettuna Internetin ja yrityksen oman sisäverkon väliin. Ideana tässä systeemissä on se, että hyökkääjä ei pääsekään sisäverkossa sijaitseviin resursseihin murettuaan Internetin ja aliverkon yhdistävän palomuurin, vaan tämän jälkeen edessä olisi vielä toinen palomuri sisäverkon esteenä.

7.2.1. Konfiguroinnin vaikeus

Palomuri tulisi konfiguroida suojelemaan itseään, tietoverkkoja joihin se on kytkettynä ja kaikkia systeemejä joiden välillä se liikuttelee dataa. Itse asiassa, palomuurin tulisi suojella myös Internetiä, tarkoittaen sisältäpäin tulevien hyökkääjien torjumista saastuttamasta muita Internetiin kytkettyjä systeemejä. Tämän lisäksi muut laitteet palomuurin ympäristössä tulisi myös konfiguroida turvallisuuden takaamiseksi. [1].

7.2.2. Hyökkäykset, joita palomuri ei pysty torjumaan

Palomuri voi rajoittaa ainoastaan yhteyksiä, jotka menevät sen läpi. Se ei pysty suojelemaan henkilöiltä, jotka osaavat kiertää sen esimerkiksi yrityksen lähiverkossa olevien jaet-

tujen kansiodien kautta. Jos hyökkääjät pystyvät jotenkin saamaan haltuunsa salasanat joihin heillä ei ole oikeutta, palomuri ei hyödytä siinä vaiheessa mitään. Esimerkiksi järjestelmän valvojana esittäytyvä henkilö voi kysellä henkilöstön tunnuksia, jotta voisi ”korjata ongelman”. [16].

Tavallinen palomuri pystyy torjumaan tietoverkon ulkopuolelta tulevat hyökkäykset paremmin kuin hyvin. Nykyiset liike-elämän vaatimukset asettavat kuitenkin paineita laajentaa organisaatiota etäkonttoreihin. Näihin luodaan yhteys pääkonttorista, joten periaatteessa saman yrityksen tietoverkko on laajennettu kattamaan kaukaisetkin työntekijät. Tämän tavallista laajemman tietoverkon suojeleminen on tyypillisillä menetelmillä hankalaa. Jotta organisaation sisältäpäin tulevat hyökkäykset olisi mahdollista torjua, täytyy palomuurille antaa tarvittavat tiedot kyseisen tehtävän suorittamiseen. [15].

7.3. Ylläpito, testaus ja päivittäminen

Järjestelmän valvojan tehtäviin kuuluu verkon suorituskyvyn seuraaminen silloin kun siinä ilmenee jotain epäsäännöllisyyksiä. Paras tapa seurata mitä kaikkea erikoista sisäverkossa tapahtuu on järjestää viikoittaiset tarkistukset koko systeemille. Tämä onnistuu joko palomuurin omalla ohjelmistolla tai sitten voi käyttää jotain ilmaiseksi ladattavaa ohjelmaa. [17].

8. Toiminnan keskeytyminen

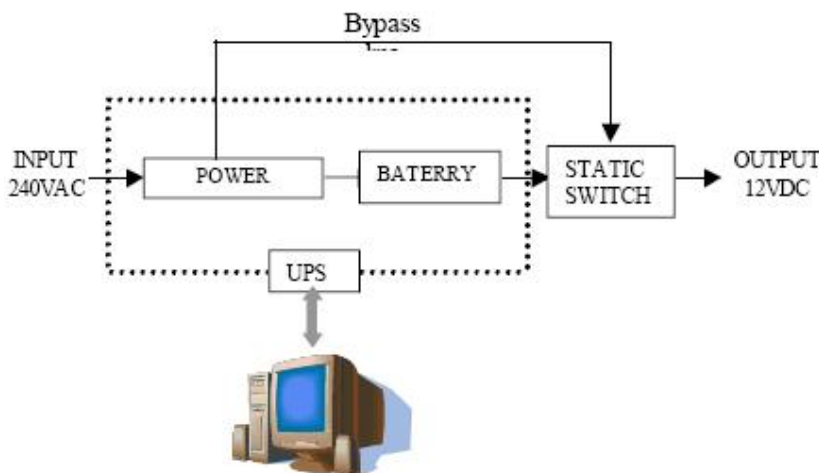
Ilman elektronisen tiedon kulkua, yritys voi lamaan täysin. Kun yrityksen tietojärjestelmät ja – verkot ovat vaurioituneet ja prosessit keskeytyneet, ongelma voi olla vakava ja seuraukset pitkään vaikuttavia. Tällaiset seuraukset voivat tuottaa jotain muutakin kuin vain minimaalisen epämukavuuden tunteen jos töitä ei ehditty tallentaa ennen katkosta.

8.1. Palvelimen käyttökatkos

Tietoturavastaavan tehtäviin kuuluu ehdottomasti muiden teknisten ratkaisujen lisäksi myös palvelimen virran katkeamattomuuden valvonta. Kaikki virta mitä palvelimelle syötetään, tulee tarkistaa siltä varalta, että sitä on tarjolla riittävä määrä, jottei ylikuormituksille altistuttaisi. Sähköjohtojen sijoitteluun kannattaa kiinnittää sen verran huomiota, että siivoojat tai muu henkilöstö ei kompastu niihin ja aiheuta vahingossa satojen tuhansien eurojen vahinkoa. [1].

8.1.1. UPS

UPS-järjestelmät tarjoavat suoraviivaista ja keskeytymätöntä virtaa sitä suuria määriä tarvitseville laitteille kuten teollisuuskoneille, tietokoneille ja lääkintälaitteistoille sekä antavat suojaa virtalähteen häiriöille ja katkoksille. UPS takaa vakaan virransyötön silloinkin kun verkkovirta on väliaikaisesti poissa käytöstä. Tällaisissa tilanteissa on äärimmäisen tärkeää varavirtalaitteen välitön toimiminen tietojen katoamisen välttämiseksi. [18].



Kuva 6 Online UPS-systeemi. [17].

Tavallisen UPS-systeemin komponentteihin kuuluu akkulaturi, akkuja sekä muuntaja. Akkulaturi toimii tasasuuntaajana joka muuttaa vaihtovirran tasavirraksi, jotta akut saadaan ladattua. Akut keräävät virran talteen, jota käytetään äkillisen varavirran tarpeen yllättäessä. Tämän jälkeen muuntaja muuntaa akkujen tasavirran takaisin vaihtovirraksi. [19].

Kuluttajan päänaivaksi UPS ei olekaan niin yksinkertainen laite kuin voisi olettaa. Moniin eri tarpeisiin tehdään erilailla valmistettuja UPS-laitteita. Yksi tällainen on Online UPS, jonka toimintaperiaatteen voi nähdä kuvasta 6. Toisin kuin Offline UPS, tässä mallissa virtaa syötetään laitteille jatkuvasti, eikä ainoastaan silloin kun sähkökatkos ilmenee.

8.1.2. Vahinkojen välttäminen

Jos kuitenkin tapahtuu pahin mahdollinen ja palvelin kaatuu ja arvokkaita tietoja menetetään, ennen epäsuotavia tapahtumia on suotavaa analysoida mitä kaikkea tietoa ollaan palvelimelle säilömässä. Ensi alkuun voisi olla järkevää varmistaa, että palvelimen tiedostoista löytyy vähintään yhdet kopiot jossakin muodossa, jotta yrityksen ei tarvitse maksaa kallista hintaa liian heppoisesta varmuuskopointipolitiikasta.

8.2. *Ulkopuolisten vahingonteko*

Yrityksen toiminta voidaan myös pakottaa keskeytymään. Tällöin puhutaan määrätietoises- ta verkkorikollisuudesta. Kräkkeriryhmät voivat tehtailla ajankulukseen palvelunestohyök- käyksiä, joilla nimensä mukaisesti estetään palvelua toimimasta normaalisti. Riittävän monta yhtäaikaista sähköpostiviestiä voi pahimmassa tapauksessa kaataa koko sähköposti- palvelimen, kun kovalevyt joutuvat liian suurelle rasitukselle. [20].

9. Tietoturvasuunnitelma pienyritykselle

Suunnitelman laatimisen ohella tehtäviini kuului muun muassa selvittää kaikkein järkevin ratkaisu hoitaa yrityksen varmuuskopiointi. Vaihtoehtoja ei oikeastaan ollut kuin kaksi: online-varmuuskopiointi tai nauhavarmistusasema. Molemmissa on sekä hyvät että huonot puolensa. Online-systeemin puolesta puhuu aloituskustannusten olemattomuus, mutta palveluntarjoajan mahdollinen konkurssi veisi kaikki tiedostot mukanaan. Nauhavarmistusaseman käyttö olisi täysin itse kontrolloitavissa, mutta sekä nauhat, että asemat ovat varsin kalliita.

Mahdollisia lisäkustannuksia on vaikea välttää, oli sitten kyseessä vaihtoehtoista kumpi tahansa. Online-vaihtoehto voi pakottaa hankkimaan nopeamman nettiyhteyden, koska suuria määriä tietoa ei siirretä verkon yli hetkessä. Jos nauhoja ruvetaan käyttämään, ja niitä säilytetään yrityksen omissa toimitiloissa, se edellyttää paloturvakaapin hankkimista.

Taulukko 1 Online-varmuuskopiointiin erikoistuneiden palveluntarjoajien hintavertailu

	€Hinta 100Gb/kk *
SpiderOak	7,14
Dropbox	14,29
ADrive	9,97
Cloud Backup	21,44
Jungle Disk	10,72
OnlineBackupVault	53,58
PerfectBackup	204,52
BackupRight	42,83

* Valuutat muunnettu 3.7.2009

Riittävän kattava hintavertailu on tarpeellista tehdä, koska palveluntarjoajien välillä on suuriakin eroja hinnoissa. Esimerkiksi Taulukosta 2 löytyvä 100Gb:n kuukausihintavertailussa on kalleimman ja halvimman vaihtoehdon välillä eroa lähes 200 euroa. Kaikki yllä kuvatut yritykset tarjoavat palveluitaan myös Linux-käyttöjärjestelmälle. Tämä on yritykselle tärkeää, koska yrityksen palvelimessa on Linux-Ubuntun palvelinversio.

Loppujen lopuksi päädyttiin online-ratkaisuun, koska tämä vaihtoehto tarjoaa paremman hinta-laatusuhteen, helppokäyttöisyyden sekä yksinkertaisen tavan varastoida äärimmäisen suuria määriä tietoa. Täysin ongelmallisena ei tätä ratkaisua kuitenkaan voi pitää. Suurimpana uhkana voidaan pitää palveluntarjoajan konkurssia, joka aiheuttaisi pahimmassa tapauksessa tietojen menetyksen. Kyseisen ongelman voi kuitenkin kiertää käyttämällä useampia online-vaihtoehtoja.

Suunnitelman soveltaminen lähitulevaisuuteen

Kyseessä olevan yrityksen keskeisenä tarkoituksena on modernia teknologiaa hyödyntävien lihastoiminnan mittaus- ja harjoituslaitteiden kehittäminen kaupallisiksi tuotteiksi sekä kotimaan että ulkomaiden markkinoille. Vientitoiminta on suunniteltu aloitettavaksi vuoden 2011 aikana. Tätä tavoitetta tukee yrityksen osallistuminen usean kuopiolaisyrityksen yhteishankkeeseen, jonka tähtäimenä on luoda kansainvälisille terveystuotteille hyvinvoinnin ja terveyden mittaamiseen, ohjeistukseen ja seurantaan tarkoitettu klinikkatoimintamalli.

Kun otetaan huomioon, että kyseisellä pk-yrityksellä ei ole vielä asiakkaita, mutta parin vuoden kuluttua tilanne on toinen, onkin järkevää jo tässä vaiheessa kirjata suunnitelmaan ylös asiakastietojen käsittelyä koskevat ohjeistukset. Eivätkä asiakassuhteiden solmimiset ole ainoa asia joka tulee lähitulevaisuudessa ajankohtaiseksi. Mahdollisen laajentumisen myötä sellaiset seikat kuten langaton verkko ja älypuhelin suojaus pitää ottaa tietoturvan kannalta huomioon.

Puutteelliset ohjeistukset

Kun vierailija ensimmäisen kerran saapuu ulko-ovesta sisään, voi hän huomata tärkeitä dokumentteja lojumassa pöydillä, suoran pääsyn tuotekehitystiloihin ja pöytäkoneita ilman salasanasuojasta. Tämä tarkoittaa sitä, että paljon on korjattavaa ennen kuin voidaan sanoa kyseessä olevan yrityksen välttävän teollisuusvakoilun.

Vastaisuudessa tämäntapaiset tapaukset pyritään välttämään jokaiselle työntekijälle tarkoitettulla ohjeistuksella, jossa kerrotaan miten huolehtia omasta, että yrityksen tietoturvasta. Tällä tavoin sekä sähköisessä, että fyysisessä muodossa olevan tiedon päätyminen väärin käsiin tehdään mahdollisimman hankalaksi.

Asiat, jotka jokaisen työntekijän tulisi ottaa ohjeistuksesta huomioon:

- Salasanapolitiikka
- Fyysinen tiloihin pääsy
- Yrityksen tietojen käsittely julkisissa tiloissa
- Paloturvallisuus
- Sähköturvallisuus
- Salassapitosopimusten noudattaminen
- Tietoliikennelaitteiden fyysinen suojaus
- Omien tietojen turvallinen käyttö

9.1. Fyysinen tietoturva

Kaikki tietoturvan osa-alueet eivät ole tietokoneisiin liittyviä. Jos ei huolehdi tapaturmien ennaltaehkäisystä, tietoliikenteen turvaaminen on vahingon sattuessa ehkä turhin toimenpide, mitä siinä tilanteessa voisi kuvitella. Fyysiseen tietoturvaan voidaan luokitella kuuluvaksi muun muassa erilaiset suojamekanismit sähköisille laitteille, henkilöstön tiedonkulun valvominen ja ulkopuolisten pääsyn rajoittaminen.

Kaikkia mahdollisia fyysisen tietoturvan menetelmiä ei ole mahdollista ottaa huomioon sellaisenaan. Esimerkkinä mainittakoon palohälyttimen puuttuminen tuotteiden valmistus-tilasta, mikä johtuu tuotekehitystyön aiheuttamasta silloin tällöin ilmenevästä savusta.

9.1.1. Kulunvalvonta

Tällä hetkellä yrityksen sisällä ei suoriteta minkäänlaista kulunvalvontaa, mikä altistaakin yrityksen mahdolliselle teollisuusvakoilulle. Positiivisena seikkana mainittakoon, että ovet sentään pysyvät lukittuina työajan ulkopuolella. Videovalvontaan siirtyminen olisi näin pienen yrityksen kannalta hyvinkin kyseenalaista. Kaikkihan tuntevat toisensa ja näin ollen tuntemattomat henkilöt erotettaisiin helposti joukosta.

Sivulla 31 olevassa pohjapiirroksessa (Kuva 9) näkyy myös kuinka helposti ulko-ovesta pääsee täysin huomaamatta lähimpänä olevaan työhuoneeseen vilkaisemaan mitä kaikkea yrityssalaisuuksia sieltä löytyykään. Tällaisten tapausten välttämiseksi on järkevää hankkia edes jonkinlainen kulunvalvontajärjestelmä, vaikka se olisikin niin yksinkertainen kuin ovikello.

Myös henkilökunnan osuus on otettava kulunvalvonnassa huomioon. Jos kuka tahansa pääsee yrityksen tiloihin ilman, että kukaan huomioisi tätä, vika on enemmänkin asenteissa kuin puutteellisessa valvonnassa. Tulevaisuudessa olisikin hyvä, että joku joka on paikalla, voisi pikaisesti vilkaista kuka sieltä ulko-ovesta tulikaan.

Eräs tärkeimmistä fyysisen tietoturvan osa-alueista on ehdottomasti avainten hallinta. Tällä tarkoitetaan sitä, että henkilöstön vakiojäsenten hallussa pidettävät avaimet ovat yrityksen omaisuutta ja siten niiden kopioiminen ulkopuolisille on määriteltävä kielletyksi. Edellä mainitun kaltainen skenaario voisi pahimmassa tapauksessa aiheuttaa merkittävän taloudellisen tappion.

9.1.2. Laitteiden suojaus

UPS-laitteen hankinta on tuonut lisää varmuutta työntekoon johtuen sen tuomasta turvallisuuden tunteesta. Ennen kuin kyseinen laite oli hankittu, sähkökatkon ilmetessä kaikki työt mitä sillä hetkellä oltiin tekemässä, menetettiin. UPS:n käytössä on kuitenkin pidettävä mielessä se, että se ei ole varavirtageneraattori vaan sen tuoma virta on vain lyhytaikaista.

Sähkövikojen lisäksi on hyvä varautua tulipaloihin asianmukaisella välineistöllä. Tällä hetkellä ei toimistolla ole minkäänlaista palohälytintä puhumattakaan edes jonkinlaisesta sammutusratkaisusta. Esimerkiksi varmuuskopiointi voi osoittautua varsin hyödyttömäksi jos useiden kuukausien aikana kerätyt full- tai incremental-backupit menetetään kokonaisuudessaan tulipalossa.

Sähköpalon ollessa kyseessä täytyy ehdottomasti tietää mitä tekee. Tavallinen vesi olisi huonoin ratkaisu sähkölaitteista alkaneisiin tulipaloihin, se itse asiassa vain pahentaa tilannetta. Kaikkein viisainta olisi hankkia jauhesammutin tai sammutuspeite tai parhaassa tapauksessa molemmat.

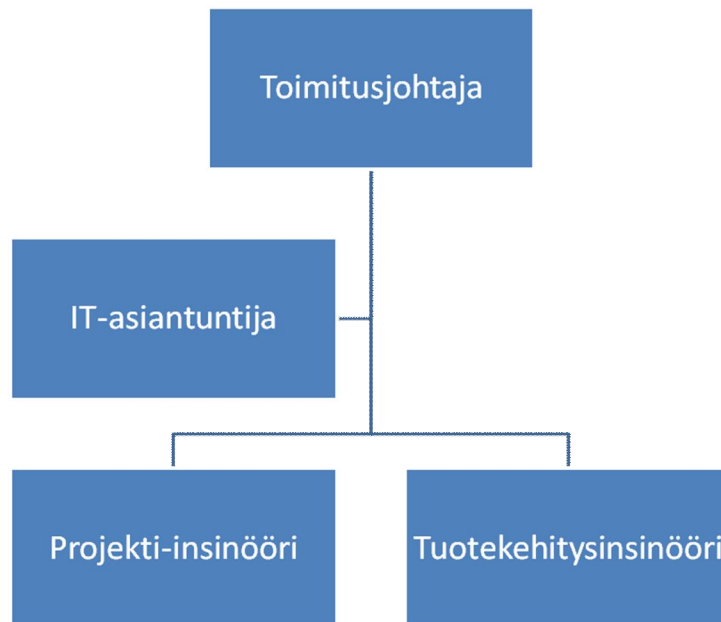
Pöly on se minkä kanssa elektroniikkalaitteet eivät saisi joutua kosketuksiin. Syy tähän löytyy siitä, että se aiheuttaa ongelmia komponentteihin sekä virtakaapeleiden - ja johdinten kontakteihin. Seuraukset tästä ovatkin sitten vähemmän toivottuja: toimintahäiriöitä ja virran sammumista.

Tulostimen sijoittamisen tärkeyttä ei sovi unohtaa, kun mietitään asiakirjojen näkyvyyttä kriittisillä hetkillä, kuten yritysvierailujen yhteydessä. Tällöin on syytä varautua siihen, että mikäli tulostin on sijoitettuna näkyvälle paikalle, todennäköisyys tietojen leviämiseen on hyvinkin suuri. Tästä syystä kaikkein järkevin sijainti tulostimen lopulliseksi sijoituspaikaksi olisi sellainen, joka ei ole vierailijoille automaattisesti tavoitettavissa mutta samalla se olisi henkilökunnalle lyhyen matkan päässä.

9.1.3. Vastuuhenkilöt

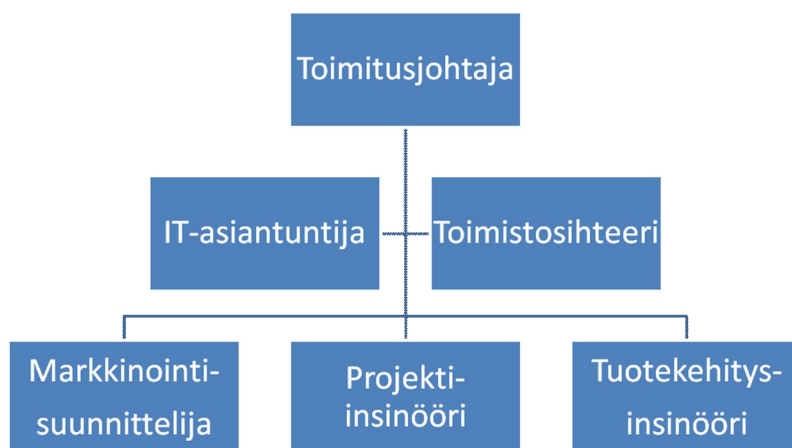
Liian monen henkilön ollessa vastuussa yhdestä tietystä asiasta, voi johtaa väärinkäsityksiin ja konflikteihin. Tätä asiaa pystytään välttämään määräämällä erilliset vastuuhenkilöt ja annetaan heille riittävät valtuudet luottamustehtäviensä kelvolliseen suorittamiseen. Hyvänä esimerkkinä toimii palvelimen kanssa toimiminen. Kahden henkilön toimiessa näinkin tärkeässä tehtävässä, pahimmassa tapauksessa voi ilmetä jopa ylimääräisiä kustannuksia. Yksi tällainen tapaus voisi olla varmuuskopioinnin suorittaminen kahteen kertaan. Jos kovalevyt täyttyvät liian nopeaan tahtiin, uusien ostaminen voi pitkällä aikavälillä käydä todella kalliiksi.

Sen lisäksi, että vastuuhenkilöt ovat vastuussa heille määrätystä tehtävästä, he ovat myös velvollisia huolehtimaan omaan työkäyttöön tarkoitettujen tietokoneiden ja älypuhelinien tietoturvasta. Sähköpostin suojausta ei myöskään pidä unohtaa kun halutaan ylläpitää korkeaa tietoturvan tasoa omalla henkilökohtaisella panostuksella.



Kuva 7 Tämänhetkinen organisaatiorakenne

Kuvan 7 mukaisesti järjestetty organisaatio on tällä hetkellä varsin toimiva ratkaisu ja henkilökunnalla on jo entuudestaanakin tietty rajattu vastuualue, jonka he hoitavat parhaan kykynsä mukaan. Tämä ei välttämättä tulevaisuudessa riitä, mikäli asiakaskunta ja yhteistyökumppaneiden määrä kasvaa merkittävän suureksi.



Kuva 8 Mahdollinen organisaatorakenne lähitulevaisuudessa

Kun myytävä tuote on siinä vaiheessa, että sitä voidaan alkaa myymään ja markkinoimaan, alkuperäisen henkilökunnan osaaminen ei kata riittävästi kyseisiä business-maailman osa-alueita. Tämän asia on ratkaistu kuvassa 8, jossa on lisätty alkuperäiseen henkilöstöön uutta potentiaalia.

9.2. Tietoliikenneyhteydet

Oleellinen osa riittävää tietoturvaa on tietoliikenneyhteyksien suojaaminen. Tämä opinnäytetyön tilannut yritys on ratkaissut tämän siten, että kaikki verkossa liikkuva tieto kulkee palomuurin kautta. Tämän lisäksi roskapostista on turha huolehtia, koska ulkoiselle palveluntarjoajalle delegoitu sähköpostipalvelimen ylläpito pitää huolen siitä, että suodatus toimii nyt ja jatkossa.

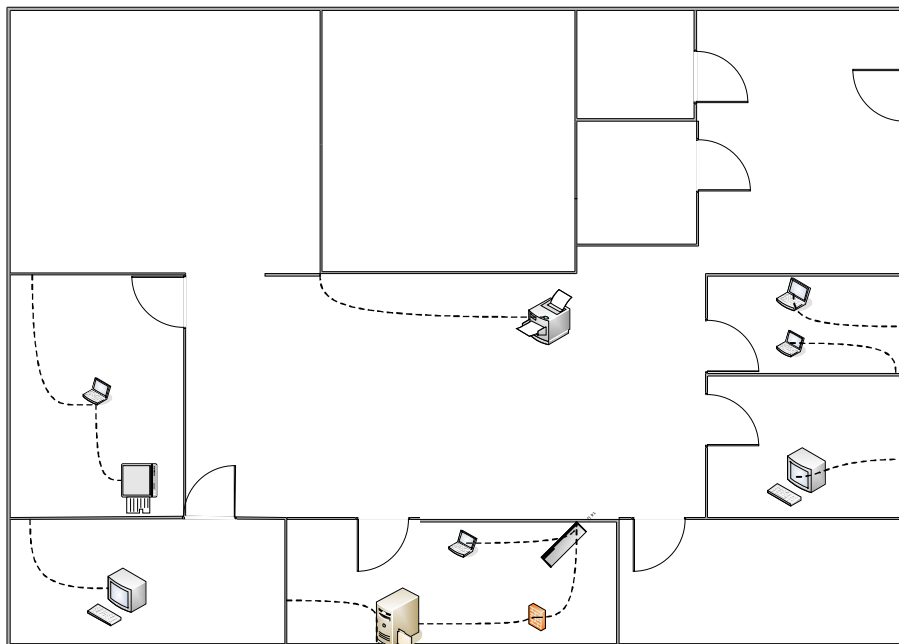
Yhteistyö kyseisen palveluntarjoajan kanssa jatkuu varmasti pitkäänkin, koska WMHost on toiminut jo vuodesta 2001. Jopa tuhannet asiakkaat saavat rahoilleen vastineeksi muun muassa webhotelli-, palvelinhotelli-, ja tietoturvapalveluita. Näiden lisäksi WMHost tarjoaa kattavaa konsultointiapua moniin tietoteknisiin ongelmiin. Ja jos tarve vaatii, heidän kauttaan voi myös rekisteröidä oman fi-päätteisen verkkotunnuksen.

Kuten kuvasta 9 voidaan todeta, suuria määriä tietoliikennelaitteita ei ole järkevää hankkia, koska niistä saatava hyöty olisi varsin vähäinen pienen tietokonemäärän vuoksi. Myöskään langattomille verkoille ei löydy tarvetta ainakaan tässä vaiheessa yrityksen elinkaarta. Minimaalisen henkilökunnan takia kaikki tärkeä tieto mahtuu helposti palvelimen kovalevyille talletettavaksi.

Hankitut tietoliikennelaitteet

Palvelin, joka tullaan ottamaan käyttöön, on HP Proliant ML310 G5, Intel Quad Core Xeon X3210, 1GB – tornipalvelin, joka on varustettu neliydin – prosessorilla ja siinä sekä virtalähde, että kiintolevyt ovat lennosta vaihdettavissa. Palvelimen lisäksi tullaan hankkimaan ainakin UPS (APC Smart-UPS SC 1000VA 2U) ja kytkin (HP ProCurve Switch Gigabit 1400-8G). Ensimmäinen suojaa palvelimen sähkökatkojen ja ukkosten aiheuttamilta tuhoilta ja jälkimmäinen tarjoaa riittävän määrän tietoliikenneportteja, jotta kaikki tarvittavat tietokoneet & muut laitteet saadaan kytkettyä lähiverkkoon. Turvallisuuden takia erillisen palomuurin hankinta tulee ajankohtaiseksi silloin, kun palvelimella sijaitsee yrityksen

kannalta kriittistä tietoa. Palomuuuri, joka hankitaan, on Netgear Prosafe FVS336G, josta löytyy vakiona vpn-toiminto.



Kuva 9 Pienyrityksen tietoliikennelaitteiden sijainnit

Tietoliikennelaitteiden hankkimisessa on sekä hyvät että huonot puolensa. Selkeästi positiivisiin seikkoihin lukeutuu yleisen tietoturvan tason nousu, mutta tämä toteutuu vain ja ainoastaan jos pätevät henkilöt ovat osanneet asentaa laitteet valmistajien vaatimien spesifikaatioiden mukaan. Toisaalta, jos tehtaalta suoraan tullut pakkaus puretaan ja laitetaan käyttövalmiiksi ilman mitään virittelyä, voi tämänkaltaisen toiminta johtaa pitkällä aikavälillä vähintään lisääntyneeseen tietokonevirusongelmaan.

Mobiilitietoliikenne

Luonnollisestikin kaikkein nopein ja kätevin tapa tavoittaa työyhteisön jäsenet kiireellisissä tilanteissa on käyttää matkapuhelinta. Jotta kilpailevien yritysten teollisuusvakoilu ei olisi liian helppoa, työpuhelimien käyttö julkisilla paikoilla ja kulkuneuvoilla on rajattava minimiin.

On sanomattakin selvää, että matkapuhelin on helpompi varastaa kuin kannettava tietokone johtuen sen huomattavasti pienemmästä koosta. Tästä syystä jokainen matkapuhelin, jota käytetään pääasiassa yrityksen sisäisten asioiden kommunikointiin, täytyy salata riittävän vaikeasti murrettavalla PIN-koodilla, jotta katoamis- tai varastamistilanteessa ei menettäisi arvokkaita tietoja kilpailevien yritysten haltuun.

Koska matkapuhelin on nykyisin tietoliikennelaitte, ei myöskään viruksilta voi välttyä. Onneksi niiden kulkeutuminen omaan puhelimeen on helppo estää. Mobiilivirukset kulkevat bluetooth-yhteyden avulla suojaamattomasta laitteesta toiseen. Suojautuminen tämänkaltaisilta hyökkäyksiltä onnistuu kätevästi sulkemalla oman matkapuhelimen bluetooth-yhteyden kokonaan.

9.2.1. Palvelin

Kaikki tietoliikenne, oli se sitten ulospäin menevää tai sisäänpäin tulevaa, kulkee DHCP-palvelimen kautta. Kyseinen palvelin toimii myös kaikkein salaisimpien tuotekehitystietojen säilytyspaikkana. Tämä siksi, koska kannettavilla laitteilla ei ole turvallista säilyttää liikesalaisuuksia, helpon varkauden vuoksi.

Koska palvelimella sijaitsee yrityksen kannalta tärkeää tietoa, on järkevää huolehtia kyseisen tietoliikenne laitteen luotettavuudesta. Se onnistuu parhaiten suojaamalla laite fyysisesti esimerkiksi UPS-laiteella ja ohjelmallisesti suojaus tapahtuu asianmukaisella virustorjuntaohjelmalla.

Yksi yrityksen kannalta merkittävistä tietoturvan edistäjistä on ehdottomasti palvelimella sijaitseva wiki-sivusto. Tämän perimmäinen tarkoitus on edistää sujuvaa tiedonvälitystä henkilökunnan jäsenten välillä. Eikä sovi myöskään unohtaa kyseisen sivuston luotettavuutta. Tämä johtuu pääasiassa siitä, että tietojen siirtelyyn muistitikkujen sijaan käytetäänkin keskitettyä palvelua kyseisen asian hoitamiseen. Näin vältetään ikäviltä jälkiseurauksilta, jotka voisivat päättää kyseessä olevan yrityksen liiketoimet pahimmassa tapauksessa kokonaan.

Käyttöjärjestelmänä kyseisellä palvelimella toimii Linux-Ubuntun palvelinversio. Tietoturvan kannalta tämä onkin viisas ratkaisu, koska Linux-käyttöjärjestelmässä ei ole niin paljon hyödynnettävissä olevia tietoturva-aukkoja kuin Windows-käyttöjärjestelmässä. Tämän lisäksi Linux on huomattavasti Windowsia kevyempi, joten tiedon siirron nopeus ei tule olemaan palvelimesta kiinni.

9.2.2. Palomuuuri

Yrityksille on yksityishenkilöitä tärkeämpää oman työpisteen turvallisuuden säilyttäminen. Varsinkin siinä tapauksessa, kun tietomurtoon kykenevillä henkilöillä on mahdollisuus kiristää yrityksen johtoa tiedoilla, jotka ovat olleet täysin vailla suojaa. Niinpä yrityksen johtoporrasakin on hankkinut palomuurin välttääkseen tällaisia uhkia.

```
Microsoft Windows XP [versio 5.1.2600]
(C) Copyright 1985 - 2001 Microsoft Corp.

C:\Documents and Settings\new>cd..
C:\Documents and Settings>cd..
C:\>tracert 62.241.198.246

Jäljitetään reitti isäntään resolver2.dnaip.fi [62.241.198.246]
käyttäen enintään 30 siirrantäväliä:

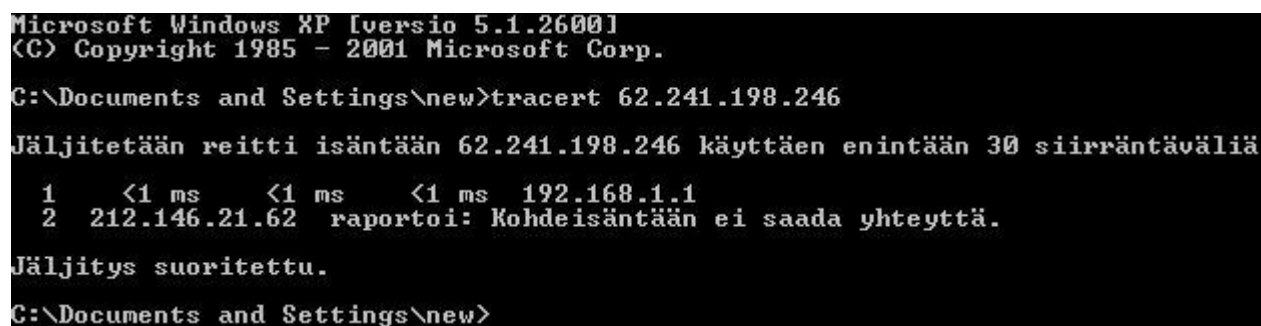
 1  <1 ms      <1 ms      <1 ms      192.168.1.1
 2  10 ms      10 ms      10 ms      212-146-21-1.bb.dnainternet.fi [212.146.21.1]
 3  15 ms      14 ms      14 ms      holi-tr1.dnaip.fi [62.78.105.114]
 4  14 ms      14 ms      14 ms      kuo1-tr1.dnaip.fi [62.78.107.29]
 5  15 ms      14 ms      14 ms      kuo1-er1.dnaip.fi [62.78.105.251]
 6  14 ms      14 ms      14 ms      resolver2.dnaip.fi [62.241.198.246]

Jäljitys suoritettu.
C:\>
```

Kuva 10 Reitti DNA:n nimipalvelimelle

Kuvasta 10 nähdään reititys pk-yrityksen palveluntarjoajan nimipalvelimelle silloin kun palomuuuri toimii niin kuin sen pitääkin. Aina eivät asiat ole näin hyvin. Palomuuuri, aivan

kuten muutkin tietoliikennelaitteet, on insinöörin suunnittelema. Tästä voidaankin todeta, että nettiyhteyden pätkiminen silloin tällöin ei yllätä ketään. Kun tämä tapahtuu, reititys DNA:n nimipalvelimelle on vain kaukainen haave. Tracert-komennon jälkeen ei palomuuria pidemmälle päästä, vaan ruudulle ilmestyy teksti: ”Kohdeisäntään ei saada yhteyttä”. Kuten kuvasta 11 voidaan todeta.



```
Microsoft Windows XP [versio 5.1.2600]
(C) Copyright 1985 - 2001 Microsoft Corp.

C:\Documents and Settings\new>tracert 62.241.198.246

Jäljitetään reitti isäntään 62.241.198.246 käyttäen enintään 30 siirrantäväliä

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2  212.146.21.62  raportoi: Kohdeisäntään ei saada yhteyttä.

Jäljitys suoritettu.

C:\Documents and Settings\new>
```

Kuva 11 Epäonnistunut reititys

9.2.3. Extranet

Kansainvälisten asiakkaiden kanssa toimiessa on otettava huomioon erilaiset käytännöt tietoturvan suhteen verrattuna Suomeen. Tästä syystä onkin kiinnitettävä erityistä huomiota tietoliikenneyhteyksiin asiakkaiden välillä. Tietysti materiaalia on oltava verkosta ladattavissa muun muassa käyttöohjeiden ja päivityspakettien muodossa. Nämä hoidetaan kuitenkin ilman oman sisäverkon vaarantumista. Yhteistyökumppanien ja asiakkaiden kanssa kommunikoidessa voidaan ottaa käyttöön yrityksen lähiverkosta irrallinen palvelu: Extranet.

Jotta tämä palvelu olisi yhtä aikaa sekä tehokas, käytännöllinen ja turvallinen, palomuurin VPN-ominaisuutta tullaan hyödyntämään parhaan mahdollisen lopputuloksen aikaansaamiseksi. Asiakkaat, yhteistyökumppanit ja henkilökunta tulevat kaikki kirjautumaan sisään omilla henkilökohtaisilla tunnuksillaan kryptattua yhteyttä käyttäen.

Extranetin käytännön turvallisuus on tulevaisuudessa ratkaistavissa siten, että kaikki kyseessä olevaa palvelua käyttävät henkilöt, jotka eivät yhteyden muodostamisen aikaan kuulu yrityksen vakituiseen henkilökuntaan, saavat käyttöönsä kertakäyttöiset salasana. Tällä toimenpiteellä halutaan ehkäistä esimerkiksi identiteettivarkauksien syntymistä, joka olisi mahdollista, koska on hyvin todennäköistä, että kaikkialla ei huolehdita tietoturva-asioista tarpeeksi hyvin.

Oli sitten kyseessä pelkkä yrityksen sivusto tai laajempi kokonaisuus lisättynä sähköisen kaupankäynnin ominaisuudella, pelkkä käyttäjiin kohdistuva valvonta ja fyysinen palomuri ei riitä, jos itse sivustossa on haavoittuvuuksia. Yksi tällainen on huolimattomasti laaditusta tietokannasta löytyvä SQL-injektio. Jotta nämä voitaisiin välttää, sivusto voidaan skannata siihen erikoistuneella ohjelmalla.

Yksi suurimmista syistä Extranetin käyttöönotolle on mahdollinen verkkokaupan avaaminen. Tällöin yrityksen puolelta olisi löydyttävä riittävät resurssit asiakkaiden kaupankäynnin turvaamiseksi. Tämä onnistuu siten, että kaikki rahaliikenteeseen liittyvä verkkoaktiivisuus suojataan erittäin vahvoilla salauksilla.










9.2.4. Työasemat

Palvelinta lukuun ottamatta kaikkien yrityksen työasemien käyttöjärjestelmänä toimii Windows XP. Tietoturvan kannalta tämä onkin varsin toimiva ratkaisu, kunhan muistaa säännöllisin väliajoin päivittää Windows update-palvelusta uusimmat tietoturvapäivitykset. Ei pidä myöskään unohtaa XP:n vähäisiä tai jopa olemattomia yhteensopivuusongelmia eri laitteiden kanssa.

Yhteensopivuusongelmista eritoten täytyy mainita Linux-palvelin, jonka kautta täytyisi järjestää keskitetty tiedonkulku Microsoftin Active Directoryn tapaan. Onneksi UNIX-maailmasta löytyy tähänkin ratkaisu: SAMBA-serverin viimeisin versio tarjoaa mahdollisuuden kytkeä päälle niin sanottu Active Directory-moodi.

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	File System	Not all hard drives are using the NTFS file system. What was scanned Result details How to correct this
	Automatic Updates	Updates are not automatically downloaded or installed on this computer. What was scanned How to correct this
	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation, the computer is restarted. What was scanned How to correct this
	Windows Firewall	Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Autologon	This check was skipped because the computer is not joined to a domain. What was scanned
	Password Expiration	This check was skipped because the computer is not joined to a domain. What was scanned

Kuva 12 Microsoft Baseline Security Analyzer-ohjelman tulokset

Tämän opinnäytetyön tekemisen ajaksi sain käytettäväkseni kannettavan tietokoneen, jossa käyttöjärjestelmänä on XP:n Media Center Edition. Viruksista tai haittaohjelmista ei ollut ongelmia, koska ennen töiden alkamista tähän koneeseen asennettiin Avast!-virustorjuntaohjelma. Microsoft Baseline Security Analyzer-ohjelmalla (Kuva 12) saatiin selville käyttöjärjestelmän haavoittuvuudet ja suurimpana uhkana ohjelma pitää sitä, että recovery-osion tiedostojärjestelmä on FAT32.

Virustorjuntaohjelmien välillä ei huomattu kovinkaan suurta eroa siinä, oliko kyseinen ohjelmisto maksullinen vai täysin ilmaiseksi ladattavissa ohjelmien tekijöiden omilta kotisivuilta. Juurikin tästä syystä yrityksen johdon päätöksellä, kaikilla sisäverkon työasemilla käytetään ilmaisia virustorjuntaohjelmia kustannusten säästämiseksi.

Tietomurtojen ehkäisemiseksi kaikkiin työasemiin, joissa on käyttöjärjestelmänä Windows XP, kirjautuminen tapahtuu tästä lähtien sellaisilla tunnuksilla, joissa ei ole järjestelmänvalvojan oikeuksia. Syy tällaiselle menettelylle löytyy Windowsin haavoittuvuudesta. Kun XP:tä käytetään suurilla oikeuksilla, annetaan siinä tapauksessa järjestelmään tunkeutujille mahdollisuus kaapata tietoja haltuunsa.

Yrityksen sisäverkossa käytettävien työasemien käytössä huomioitavia asioita ovat muun muassa:

- virusturvan pitäminen ajan tasalla
- pölyn määrän minimoiminen
- muistitikkujen poistaminen käytön jälkeen
- epäluotettavien sivustojen välttäminen
- turvallisten yhteyksien käyttäminen
- tiedostojen alkuperän varmentaminen

Verkkoratkaisu

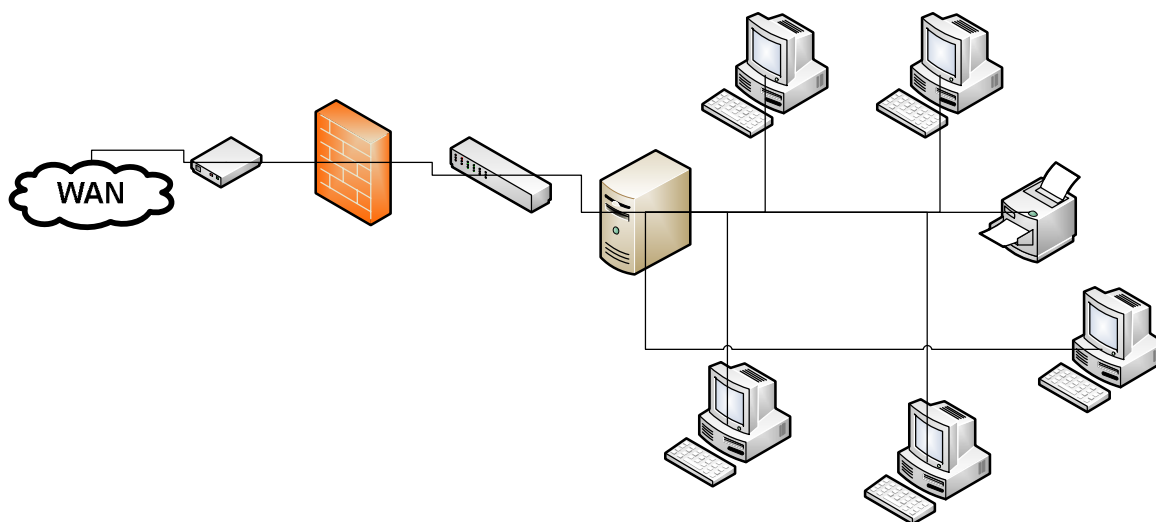
Pääasiallinen asetus on joka tapauksessa se, että liikenne sisältä ulos on sallittu ja toiseen suuntaan estetty lukuun ottamatta VPN-tunnelia.

VPN-ratkaisuna käytetään palomuurin tarjoamaa SSL-VPN – pohjaista ratkaisua. Käytännössä homma toimii siis niin, että navigoidaan laitteen palvelemalle websivulle, jonne kirjaututaan sisään omilla VPN-tunnuksilla. Kirjautumisen jälkeen sivulta ladataan NetGearin oma SSL-VPN -asiakasohjelma (käytännössä activeX-komponentti), joka huolehtii liikenteen tunneloimisesta firman sisäverkkoon. SSL-VPN-ratkaisu on kevyempi kuin perinteiset VPN:t.

Ongelmana tuossa on esimerkiksi nimipalvelut, jolloin sisäverkon koneiden nimet eivät päivitty VPN-asiakkaan tietoon, vaan niihin pääsee käsiksi vain yrityksen sisäverkon IP-osoitteiden avulla. Koska sisäverkko on pieni ja muistettavia osoitteita näin varsin rajatusti, ei tätä pidetä suurena ongelmana. Samoin yhteys tuntuu toimivan luotettavasti vain Internet Explorerilla. Muilla alustoilla (Mac) ja selaimilla toiminta on ollut konekohtaista, joillakin toimii, joillakin ei.

NetGear tarjoaisi myös perinteisen VPN:n erillisellä asennettavalla asiakasohjelmalla, mutta yritys ei toistaiseksi ole kokenut tarvetta alkaa asennella tuota kenenkään koneille. Suorituskyky olisi ehkä hieman parempi, mutta vastaavasti asiakasohjelman asennuksessa ja konfiguroinnissa on melkoinen työ.

Asennusvaiheessa huomattiin, että palomuuuri ei ole kaikkein vakain, vaan heitteli Zyxelin ADSL-modeemin kanssa yhteyttä poikki vähän väliä. Zyxelin tilalle vaihdettu A-linkin modeemi ratkaisi tämän ongelman. Samoin VPN:n konfiguroinnin kanssa oli kaikenlaisia pieniä vaikeuksia, mutta tämä ratkesi NetGearin puhelintuen avulla. Lähinnä kyse oli vääristä konfiguroinneista, syynä olivat huonot ohjeet ja huolimaton ohjeiden lukeminen IT-asiantuntijan taholta.



Kuva 13 Yrityksen sisäverkon looginen kuva

Kuvassa 13 ADSL-modeemi siltaavassa tilassa (tämä ei siis näy verkossa mitenkään), palomuri (kiinteä ulkoverkon osoite + NAT, VPN), kytkin ja sisäverkko (palvelin (DHCP), tulostin ja työasemat).

9.3. Kriittisen tiedon käsittely

Kaikki tieto mikä tuotetaan yrityksissä, ei ole sellaista, jota voisi julkisesti esitellä kenelle vain. Tästä syystä mainitun kaltaisissa tilanteissa on hyvä tehdä suunnitelma miten ja kuka tällaista informaatiota pääsee kontrolloimaan? Väärinkäytösten välttämiseksi on ensiarvoisen tärkeää huomioida jo tiedonluontivaiheessa oikeanlainen menettelytapa myöhempää käyttöä varten.

Millainen tieto sitten määritellään kriittiseksi? Ainakin siihen kategoriaan voisi laskea helposti ainakin tuotekehitystiedot, asiakastiedot, henkilöstötiedot ja vastaavat. Nämä olisi suositeltavaa määritellä salaisiksi ja lukuoikeudet sallittaisiin vain ja ainoastaan henkilöille, jotka niitä oikeasti tarvitsevat.

Salaiseksi määrittelemisen lisäksi on tärkeää kiinnittää huomiota siihen, kuinka hyvin ulkomaalaisten yhteistyökumppaneiden ja asiakkaiden kanssa solmitut sopimukset suojaavat tärkeitä tietoja. Tällöin niin sanotut salassapitosopimukset tulevat kyseeseen. Jokainen yritys, joka vaatii salassapitosopimuksen allekirjoittamista, antaa itsestään hyvän kuvan tietoturvastaan huolehtivana yrityksenä.

Tiedon käsittely sosiaalisissa medioissa

Vaikka henkilökunnan käyttäytymistä Facebookissa tai Twitterissä ei varsinaisesti valvotaan, niin yhteisen edun vuoksi olisi suotavaa, jos yrityksen ylimpään johtoon kuuluvien henkilöiden yhteystietoja ei leviteltäisi tätä kautta. Hyvin suurella todennäköisyydellä joku ulkopuolinen voisi laittaa profiilisivulta löytämänsä sähköpostiosoitteen roskapostilistalleen. Henkilöstön negatiivista käyttäytymistä sosiaalisissa mediassa, ei luonnollisestikaan suositella, koska yksittäinen henkilö voi tällaisella käytöksellä aiheuttaa epäsuorasti vahinkoa kyseessä olevalle yritykselle.

Asian toinen puoli on nykyisin kovaa vauhtia etenevä yksityisen ja julkisen sektorin vahva esiintulo Facebookin kautta tavallisten ihmisten tietoisuuteen. Tätä kautta voidaan varmistaa, ettei yritys jää pimentoon kun kilpailijat ovat jo luoneet merkittävän osan markkinaosuudesta ilman, että olisivat käyttäneet siihen ollenkaan taloudellisia resurssejaan.

Negatiivisena puolena mainittakoon vielä se, että kyseisten palvelujen tietoturvan tasosta ei ole minkäänlaisia takeita. Joissakin vastaavanlaisissa palveluissa sivustojen haavoittuvuudet ovat aikaansaaneet sen, että tunkeutuja on saanut haltuunsa kyseisen sivuston käyttäjien tunnukset ja salasanat. Tämän vuoksi on äärimmäisen tärkeää, että yrityksen henkilökunta ei käytä samoja tunnuksia yrityksen sisäverkossa ja sosiaalisissa medioissa.

Ennen kuin sivustolle ollaan kirjautumassa, olisi syytä ottaa selville, että kyseessä on todellakin palveluntarjoaja johon ollaan ottamassa yhteyttä. Aina voi olla se riski, että taitavasti laadittu huijaussivusto on päässyt yllättämään kokeneen web-selaajan, joten liian varovainen ei voi olla.

9.3.1. Tiedon säilytys

Hyvään tiedonsäilytyspolitiikkaan kuuluu ehdottomasti palvelimen käyttö tuotekehitystietojen säilyttämisessä. Jotta tämä skenaario hoituisi ilman suurempia vahinkoja, on käytettävä riittävää suojausta, johon kuuluu rautapuolen lisäksi antivirus- ja haittaohjelmienpoisto-ohjelmat.

Negatiivisena puolena mainittakoon palvelimen kovalevyjen kapasiteetin äärimmilleen vieminen. Tämä ei kuitenkaan tule olemaan mikään ylitsepääsemätön este, sillä nykyaikaisen ”hot swap”-tekniikan ansiosta sekä virtalähde, että kiintolevyt ovat vaihdettavissa kun niissä on vielä virta päällä.

9.3.2. Tiedon tuhoaminen

Aivan kaikkia asiakirjoja ja dokumentteja ei ole kovin viisasta säilyttää loputtomiin, varsinkin jos ne sisältävät: henkilöstö-, asiakas- tai projektitietoja. Sellaisissa tapauksissa joissa roskakoriin tai paperinkeräykseen vieminen olisi riskialtista, on kannattavaa hankkia silppuri.

Tässä raportissa jo aiemmin mainittu yritys on ratkaissut edellä mainitun ongelman hankkimalla Peach 35X-asiapaperituhoojan. Laitteen ominaisuuksiin kuuluu muun muassa mahdollisuus tuhota luottokortteja, kolmen taitetun paperin samanaikainen tuhoaminen sekä luonnollisestikin silppuriastia. Kyseinen laite soveltuu parhaiten kodin ja pienen toimiston käyttöön. Fyysiset mitat ovat: leveys 21 cm, pituus 15 cm ja syöttöaukon leveys on 11,4 cm.

Nykyisessä tietoyhteiskunnassa on kuitenkin todennäköistä, että suurin osa tiedosta on digitaalisessa muodossa. On epäolennaista minkälaisessa digitaalisessa muodossa yrityksen kannalta käyttökelpoton tieto on säilytetty. Kaikki kovalevyt ja siirrettävät tiedon arkistointilaitteet, joita ei enää tarvita on ehdottomasti tehtävä lukukelvottomaksi. CD-levyjen kohdalla tilanne on helppo, jos esimerkiksi silppurista löytyy ominaisuus näiden tuhoamiseen. Kovalevyistä pääsee eroon fyysisesti tuhoamalla tai niin sanotulla ”uudelleenkirjoittamisella”. Tässä on kyse siitä, että estetään riittävän pätevää henkilöä onnistumasta

oikeilla menetelmillä saamaan formatoidun kovalevyn tiedot haltuunsa. Prosessin voi toistaa niin monta kertaa kuin turvallisuus vaatii.

Valitettavasti ”uudelleenkirjoittaminen” ei ole täysin varma tapa tietojen tuhoamiseen. Kyseisen prosessin voi kääntää aina ympäri niin monta kertaa, että tiedot saadaan näkyville. Onneksi tämäkin tehtävä on nykyään helppo ulkoistaa tähän erikoistuneille yrityksille. Systeemi toimii seuraavalla tavalla: kun haluat päästä eroon vanhoista kovalevyistäsi, otat yhteyttä niitä tuhoavaan yritykseen, siellä päässä levyt tuhotaan turvallisilla ja ekologisilla menetelmillä käyttäen.

Haitallisen tiedon tuhoaminen

Mikäli henkilökunnan jäsen havaitsee, että palvelimen tai työaseman levytila on huomattavasti kasvanut tai tuntemattoman nimisiä tiedostoja on alkanut ilmestyä ilman minkäänlaisia syytä, ensimmäisenä asiana täytyy välttää panikointia. Sillä tavalla ei ainakaan helpoteta uhkaavaa tilannetta. Jos haitallisten tiedostojen poistaminen ei onnistu yksin, siinä tapauksessa on parasta kutsua asiantuntija apuun. Mikäli et jostain syystä saa asiantuntijaa tavoitettua, kirjoita paperille ylös kaikki tietokoneessa ilmenevä epäilyttävä toiminta. Tällä tavoin kaikki tärkeimmät asiat ovat tiedossa kun apua on saatavilla.

9.4. Suunnitelman käyttöönotto

Tämän kyseessä olevan tietoturvasuunnitelman ei ole tarkoitus jäädä vain ajatuksen tasolle, vaan koko yrityksen henkilökunta sitoutuu noudattamaan uusia ohjeita yrityksen tulevaisuuden turvaamiseksi. Ne ohjeistukset, jotka koskevat vasta lähitulevaisuutta, luonnollisestikin otetaan käyttöön sitten, kun yrityksen tilanne sen vaatii.

Luonnollisestikin tekniikka kehittyy ja he sen mukana. Ne turvajärjestelyt, jotka toimivat nyt, eivät ole välttämättä riittäviä muutaman vuoden päästä. Tästä syystä tietoturvasuunnitelma, joka otetaan käyttöön, päivitetään vastaamaan sen hetkistä tilannetta. Jotta edellä kuvattu skenaario toteutuisi, on jokaisen yrityksen työntekijän sitouduttava noudattamaan annettuja velvoitteita ja ilmoitettava löytämistään tietoturva-aukoista välittömästi.

Lähtötilanne ennen käyttöönottoa

Ennen kuin aloitin opinnäytetyöni tekemisen, työpaikan yleisen tietoturvan taso oli sen hetkiseen tilanteeseen nähden riittävä. Tämä ei tosin riittäisi lähitulevaisuudessa, koska suojeltavan tiedon ja yhteistyökumppaneiden määrä lisääntyisi, mikä tarkoittaisi tarkempaa huolehtimista yrityssalaisuuksien pitämisessä omana tietona.

Puutteita silti löytyi, etenkin salasanoiden osalta. Joissain työasemissa ne olivat käytössä, joissain taas ei. Muuta korjattavaa löytyi muun muassa palohälyttimen ja sammutusjärjestelmän puuttumisen muodossa. Ennen palvelimen käyttöönottoa tärkeitä tuotekehitystietoja sekä muita liikesalaisuuksia kuljetettiin salaamattomilla usb-tikuilla, mutta nykyisin ne sijaitsevat palvelimen kovalevyillä.

9.4.1. Ohjeistus v. 2011 ja sen jälkeen

Koska myyntitoiminta ei käynnisty ennen vuotta 2011, on pidettävä huolta siitä, että sitten kun vienti alkaa vetämään mahdolliset uudet työntekijät on perehdytetty ”talon tapoihin”. Ehkäpä kaikkein tärkeimpänä näistä voisi olla asiakastietojen oikeaoppinen käsittely. Eihän kukaan voi olettaa, että rekrytointivaiheessa henkilö tietäisi jo ennalta kaikki mahdolliset yhteistyökumppanit ja heidän protokollansa.

Sen lisäksi, että omat työntekijät pitävät tietoturvan tason korkeana, asiakaspuoleen täytyy myös kiinnittää huomiota. Jos käy niin, että asiakas aiheuttaa taloudellista tai muunlaista vahinkoa itse yritykselle, riittäviin toimenpiteisiin on ryhdyttävä. Riippuen siitä, onko aiheutettu vahinko tahallinen vai tahoton, oikea menettelytapa on joko korvausvaatimus tai molemminpuolinen sopiminen.

Asiakkaat eivät ole ainoa ulkopuolinen ryhmä, joka täytyy ottaa huomioon tietoturvasuunnitelmaa laatiessa. Myös yhteistyökumppanit voivat olla huolimattomia, eivätkä ota huomioon kaikkea mitä pitäisi, esimerkiksi tietoliikenneyhteyksissä. Yhteisten pelisääntöjen luominen lisää turvallisuutta ja ehkäisee vahinkoja syntymästä.

Muita huomionarvoisia seikkoja

Kun asiakaskunta kasvaa ja liikevaihto kasvaa voidaan olettaa, että myös henkilökunta kasvaa. Henkilöstömuutoksien takia on myös varauduttava toimitilojen muutoksiin. Tällaisissa tapauksissa yleensä on tapana tehdä vähintäänkin pienimuotoisia muutoksia yrityksen sisäiseen tietoverkkoon. Ja jos kyse ominaisuuksien lisäyksestä, niin silloin on hyvin tavallista, että jos langatonta verkkoa ei ole vielä käytössä uusissa toimitiloissa ainakin on.

Erittäin tärkeänä asiana voidaan pitää uusien työntekijöiden tekniikan tuntemuksen puutteellisuus. Osa on todennäköisesti saanut humanistisen tai vastaavan koulutuksen ja näin ollen ei todennäköisesti ymmärrä kaikkia tietokoneisiin liittyviä tietoturvariskejä. Tästä syystä lopulliseen tietoturvasuunnitelmaan lisätään mahdollisimman tarkat selvennökset kaikista tarvittavista teknisistä termeistä, jotka eivät aivan totaaliselle maallikolle avautuisi.

Langattoman verkon turvallisuudesta voidaan olla montaa mieltä, mutta oikeilla menetelmillä sille saadaan riittävä suojaus. Ainoa turvallinen vaihtoehto on valita WPA2:n Enterprise-moodi. Tavallisessa kotikäytössä riittää pienempikin suojaus, mutta kun on kyse Pk-yrityksestä, ei turvallisuudesta kannata tinkiä.

Organisaatiomuutokset voivat tietysti tarkoittaa henkilökunnan kasvun lisäksi myös entisten työntekijöiden poistumista yrityksestä. Tällaisissa tapauksissa korrekti tapa olisi pitää huolta siitä, että arvokkaita tai muuten yritykselle merkityksellisiä tietoja ei vietäisi kilpaleviin yrityksiin. Jotta tämä skenaario ei toteutuisi, siihen voidaan valmistautua vaatimalla jokaista henkilöstöön kuuluvaa jäsentä allekirjoittamaan salassapitosopimus, jolla pyritään ennaltaehkäisemään tietovuotoja sekä ylläpitämään yrityksen toiminta jatkossakin kannattavana.

9.4.2. Hyötynäkökulma sujuvasta ohjeistuksesta

Ilman uusille työntekijöille tehtävää kattavaa perehdytystä yrityksen tietoturvan osalta, ei voida olettaa tuotekehitys- tai asiakastietojen pysyvän kovinkaan pitkään ulkopuolisilta salassa. Pidempään työskennelleet hyötyvät hyvästä ohjeistuksesta myös, kun mahdollisesti uusia turvallisuusmenetelmiä otetaan käyttöön.

Taloudellinen hyöty on myös huomattava, koska esimerkiksi ajattelematon työntekijä voisi vahingossa kadottaa avaimensa ja yrityksen turvallisuusvastaava joutuisi uusimaan lukot. Toinen skenaario voisi olla varmuuskopioinnin puuttuminen. Jos sitä ei ole, silloin pahimmassa tapauksessa viimeisimmät töiden tulokset häviäisivät ja mahdollisesti asiakkaat niiden mukana.

10. Yhteenveto

Tämän insinöörityön tarkoituksena oli luoda hyvinvointiteknologiaan erikoistuneelle Pk-yritykselle tietoturvasuunnitelma, jossa on otettu huomioon tulevaisuudessa tapahtuvat muutokset yrityksen sisällä.

Ennen kuin aloitin tämän opinnäytetyön tekemisen, kaikkein olennaisimmista aiheista oli syytä pitää palaveri yrityksen IT-asiantuntijan kanssa, joka toimi myös tämän projektin valvojana heidän puoleltaan. Merkittävimpiin asioihin kuului ehdottomasti tulevaisuuden tietoturvaasteiden ennakoiminen.

Yhteisymmärryksen löydyttyä sovimme, että hän ottaa hoitaakseen suurimman osan teknisistä tehtävistä ja minä voisin keskittyä itse tärkeimpään eli tietoturvasuunnitelman laatimiseen. Ennen kirjoittamisen aloittamista oli kuitenkin syytä tutustua tarkemmin yrityksen tietoturvan nykytilaan.

Sen verran sain selville, että varmuuskopiointia ei ollut, ovesta pääsi kulkemaan kuka tahansa keskellä päivää, tärkeitä ja ajankohtaisia tietoja säilytettiin useissa eri paikoissa (muistitikuilla, sähköpostilla ja työasemilla).

Suunnitelman kirjoitusvaiheessa sain toimitusjohtajalta parannusehdotuksia edistymistahdin mukaan. Yksi oleellisimmista oli perusteellisemmat selitykset kaikkein teknisimmistä termeistä, jotta vähemmän tekniikkaan orientoituneet henkilöt ymmärtäisivät suunnitelmasta olennaisimman.

Todelliseen testiin tietoturvasuunnitelma joutuu vasta vuonna 2011, koska silloin ensimmäiset asiakaskontaktit saadaan myyntitoiminnan alkamisen vuoksi. Tästä syystä tekemäni työn merkitys yrityksen tulevaisuuden kannalta jäänee ainakin tässä vaiheessa arvoitukseksi.

Lähdeluettelo

- [1] Tipton. Harold F. & Krause. Micki, *Information security management handbook*. Auerbach Publications. 2006.
- [2] Zhan. Xue Ping, *Network security in a small company*. Thesis. Degree programme in information technology. Savonia university of applied sciences. 2005.
- [3] Stokes, Todd H. Torrance, JT. Li, Henry and Wang, May D. *ArrayWiki: an enabling technology for sharing public microarray data repositories and meta-analyses*, BMC Bioinformatics. vol 9. suppl 6. 2008.
- [4] Klobas, Jane. *Wikis: Tools for information work and collaboration*, Chandos Publishing. 2006.
- [5] Lucas. Mark, Singh. Abhishek & Cantrell. Chris, *Firewall policies and vpn configuration*, Syngress Publishing. 2006.
- [6] Egele. Manuel, Wurzinger. Peter, Kruegel. Christopher & Kirda. Engin, *Defending Browsers against Drive-by Downloads: Mitigating Heap-Spraying Code Injection Attacks*, DIMVA 2009 July 9th. 2009.
- [7] Bertino, Elisa. Shay, Richard. Bhargav-Spantzel, Abhilasha. *Password policy simulation and analysis*, Proceedings of the 2007 ACM workshop on Digital identity management. 2007.
- [8] Miettinen, Juha E. *Yritysturvallisuuden käsikirja*, Kauppakaari. 2002.
- [9] Van Heerden, Francois. *Social Engineering The dark art of persuasion*, Showcase Ontario 2008 September 8 – 10. 2008.
- [10] Ferguson P. and Huston G. *What is a vpn?* [verkkodokumentti]. 1998 [viitattu 28.5.2009]. Saatavissa: <http://www.potaroo.net/papers/1998-3-vpn/vpn.pdf>
- [11] Narasimhan Raghavan, Rajat Gopal, Sashidhar Annaluru, Shasidhar Kura. *Virtual Private Networks and Their Role in E-Business*, Bell Labs Technical Journal, vol 6, nro 2, s. 99-115. 2002.
- [12] Sun. Rong, *Virtual private networks*. Thesis. Degree programme in information technology. Savonia university of applied sciences. 2004.
- [13] Drake, Jeff S. *Data Backup and Recovery Options*. [verkkodokumentti]. 2007 [viitattu 12.6.2009]. Saatavissa: http://www.infosecwriters.com/text_resources/pdf/Backup_JDrake.pdf
- [14] Dodescu, Gheorghe. *Firewall Technologies*, Informatica Economică, nro 4, s. 119 – 121. 2007.
- [15] Singh, U.K. ; Ramani, A.K. ; Chaudhari, N.S. *On analysis and design of the enhanced firewall for Intranet security*, Journal of Computer Science. vol 1, nro 2, s. 290-295. 2005.

- [16] Welch-Abernathy, Dameon D. *Essential Check Point FireWall-1 NG : an installation, configuration, and troubleshooting guide*. Addison-Wesley. 2004.
- [17] The Hong Kong University of Science and Technology *Guide to Firewall Configuration* [verkkodokumentti]. 1997 [viitattu 17.6.2009]. Saatavissa: <http://www.cyber.ust.hk/handbook4/hb4main.html>
- [18] S.A.Z. Murad, M.N.Md. Isa and N.A. Rahman. *Monitoring System for Uninterruptible Power Supply*. American Journal of Applied Sciences. vol 4, nro 3, s. 181-183. 2007.
- [19] Pacific Gas and Electric Company *Uninterruptible Power supply* [verkkodokumentti]. 2000 [viitattu 22.6.2009]. Saatavissa: <http://www.pge.com/includes/docs/pdfs/mybusiness/customerservice/energystatus/powerquality/ups.pdf>
- [20] Järvinen, Petteri *Tietoturva & yksityisyys*. Docendo. 2002.