

SAVONIA

ammattikorkeakoulu

OPINNÄYTETYÖ - AMMATTIKORKEAKOULUTUTKINTO
TEKNIIKAN JA LIIKENTEEN ALA

TYÖELÄMÄN TIETOTURVAN JA KY- BERTURVALLISUUDEN OSAAMISEN TUKEMINEN

TEKIJÄT Roope Lappeteläinen
Panu Kiminki

Koulutusala Tekniikan ja liikenteen ala			
Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma			
Työn tekijä(t) Roope Lappeteläinen ja Panu Kiminki			
Työn nimi Työelämän tietoturvan ja kyberturvallisuuden osaamisen tukeminen			
Päiväys	1.2.2024	Sivumäärä/Liitteet	31
Toimeksiantaja/Yhteistyökumppani(t) Savonia-ammattikorkeakoulu			
<p>Tiivistelmä</p> <p>Opinnäytetyön tavoitteena oli tutkia tieto- ja kyberturvallisuutta pääasiassa työelämän näkökulmasta. Lisäksi tavoitteena oli suunnitella ja kehittää muistipeli, joka tukisi työelämässä olevien henkilöiden tieto- ja kyberturvallisuus osaamista. Tavoitteena oli myös tarkastella tieto- ja kyberturvallisuuden käsitteitä, analysoida tietoturvallisuuden tilannetta Suomessa sekä käsitellä yrityksen ja työntekijän rooleja tietoturvassa. Lisäksi käydä läpi yleisimmät kyberuhat ja niiden torjuntakeinot.</p> <p>Muistipeli toteutettiin web-sovelluksena käyttäen JavaScriptiä ja React-kirjastoa käyttöliittymässä. Palvelinpuoli rakennettiin Node.js-ympäristössä, ja tietokantana käytettiin MariaDB:tä. Ohjelmiston ja tietokantapalvelimen välille luotiin REST API -rajapinta, joka suorittaa käyttöliittymältä saadut tietokantakyselyt. REST API toteutettiin käyttäen Node.js-ympäristöä ja Express-kehystä, ja ohjelmointikielenä käytettiin JavaScriptiä.</p> <p>Tilaajan suunnitelman mukainen muistipeli toteutettiin, jonka tarkoitus on tukea työelämässä olevien henkilöiden tieto- ja kyberturvallisuus osaamista. Valmiiksi markkinoille sopivaa web-sovellusta ei ollut tavoitteena tuottaa, vaan toimiva perusta luotiin, jota voidaan halutessa jatkokehittää tulevaisuudessa.</p>			
Avainsanat Tietoturva, kyberturvallisuus, muistipeli, web-sovellus, Vite, React, Node.js, MariaDB			

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Information Technology	
Author(s) Roope Lappeteläinen and Panu Kiminki	
Title of Thesis Supporting Information Security and Cyber Security Competence in Working Life	
Date 1 February 2024	Pages/Appendices 31
Client Organisation /Partners Savonia University of Applied Sciences	
<p>Abstract</p> <p>The aim of the thesis was to study information and cyber security from the perspective of working life. Another aim was to design and develop a memory game that would support the information and cyber security skills of people in working life. The goal was to examine information and cyber security concepts, analyze the information security situation in Finland and discuss the roles of companies and employees in information security. In addition, the goal was to go through the most common cyber threats and ways to combat them.</p> <p>The memory game was implemented as a web application using JavaScript and the React library in the user interface. The server side was built in a Node.js environment and MariaDB was used as the database. A REST API interface was created between the software and the database server, which performs database queries received from the user interface. The REST API was implemented using the Node.js environment and the Express framework, and JavaScript was used as the programming language.</p> <p>A memory game was implemented in accordance with the client's plan, which supports the information and cyber security skills of people in working life. The goal was not to produce a web application suitable for the market, but to create a functional base that can be further developed in the future, if desired.</p>	
<p>Keywords</p> <p>Data security, Cyber security, Memory game, Web-app, Vite, React, Node.js, MariaDB</p>	

SISÄLTÖ

1	JOHDANTO	8
2	TIETO- JA KYBERTURVALLISUUS.....	10
2.1	Tietoturvallisuus.....	10
2.2	Kyberturvallisuus	10
3	ORGANISAATIOIDEN TIETOTURVA.....	12
3.1	Tietoturvallisuus suomessa	12
3.2	Yrityksen rooli tietoturvassa	12
3.3	Työntekijänrooli tietoturvassa	14
4	YLEISIMMÄT KYBERUHAT	15
4.1	Kiristysohjelmat	15
4.2	Palvelunestohyökkäykset	15
4.3	Tietokonevirukset.....	16
4.4	Tietokonemadot.....	16
4.5	Troijalaiset	16
4.6	Käyttäjän manipulointi.....	17
4.7	Vakoiluohjelmat	17
5	UHKIEN TORJUNTA	18
5.1	Miten parantaa työntekijöiden tietoturvaosaamista?	18
5.2	Miten tunnistaa tietoturvauhat?	18
5.3	Perinteiset torjuntakeinot	18
5.3.1	Virustorjuntaohjelmisto	18
5.3.2	Palomuuuri.....	19
5.3.3	Vahvat salasanat ja kaksivaiheinen tunnistautuminen	19
5.3.4	Ohjelmistojen päivitykset	20
5.3.5	Varmuuskopiot	20
5.3.6	Käyttöoikeuksien hallinta.....	20
6	MUISTIPELI TIETOTURVAN/KYBERTURVALLISUUDEN TUKEMISEKSI	22
6.1	Muistipeli koulutuskäytössä.....	22
6.2	Projektin kuvaus	22
6.3	Projektin suunnittelu	22
7	SOVELLUKSEN ARKKITEHTUURI JA TEKNIIKAT.....	23

7.1 Käyttöliittymä	23
7.2 Palvelinpuoli	23
7.3 Tietokanta	24
8 ULKOASUT JA NÄKYMÄT	25
8.1 Etusivu	25
8.2 Kirjautuminen	26
8.3 Kirjautunut käyttäjä	26
8.4 Hallinta	27
8.5 Lisäys ja muokkaus lomake	27
9 YHTEENVETO.....	29
LÄHTEET	30

KUVALUETTELO

Kuva 1. Poliisin tietoon tullut kyberrikollisuuden määrä Suomessa vuosina 2000–2020 (Elinkeinoelämän tutkimuslaitos 2020)	9
Kuva 2. Sovelluksen arkkitehtuuri.....	23
Kuva 3. Tietokanan ER-kaavio.....	24
Kuva 4. Sovelluksen etusivu.....	25
Kuva 5. Pelikortit.....	25
Kuva 6. Korttipari.	26
Kuva 7. Sovelluksen kirjautuminen.	26
Kuva 8. Sovelluksen etusivu kirjautuneella käyttäjällä.	27
Kuva 9. Korttien hallinta sivu.	27
Kuva 10. Korttiparin lisäys lomake.....	28

KÄYTETYT TERMIT JA LYHENTEET

Wi-Fi	Langaton lähiverkko.
Fakeupdates	Haittaohjelma, joka tallentaa haitalliset hyötykuormat levyille ennen niiden suorittamista.
Remcos	Etäkäyttötroijalainen, joka kykenee saamaan etäyhteyden uhrin järjestelmään, varastamaan arkaluontoista tietoa ja tunnistetietoja sekä suorittamaan haitallista toimintaa käyttäjän tietokoneella.
Snatch	Haittaohjelma, joka toimii kaksinkertaisella kiristysmallilla, jossa se sekä varastaa että salaa uhrin tietoja kiristystarkoituksessa.
Ducktail	Windows-haittaohjelma, jota käytetään varastamaan Facebook-tilejä, selaimen tietoja ja kryptovaluuttalompakoita.
Viking	Itsestään monistuva haittaohjelma, joka käyttää tietokoneverkkoa lähettääkseen kopioita itsestään muihin solmupisteisiin, ja se voi tehdä sen ilman käyttäjän suostumusta tai tietoa.
SSL	Secure Sockets Layer, on palvelimille ja selaimiin asennettava salausprotokolla. Se salaa verkkoliikenteen luotettavasti ja estää verkkosivustojen luomisen muiden nimissä.
Pimeä verkko	joukko piilotettuja Internet-sivustoja, joita ei löydy perinteisellä hakukoneella ja joihin ei pääse käsiksi ilman erityisiä ohjelmia.
JavaScript	Ohjelmointikieli, jota käytetään erityisesti web-sovellusten kehittämisessä. Se mahdollistaa dynaamisten ja interaktiivisten ominaisuuksien lisäämisen verkkosivuille.
HTML	Standardoitu merkintäkieli, jota käytetään dokumenttien struktuurin ja sisällön kuvaamiseen verkkosivuilla.
CSS	Kieli, jolla määritetään verkkosivustojen ulkoasuja.
Vite	Paikallinen kehitystyökalu, joka tarjoaa nopeampaa kehitystä.
Sass	CSS-kieleen perustuva tyylien esikäsittelijä. Se on ohjelmiston avulla luotu työkalu, joka mahdollistaa monipuolisemman ja tehokkaamman CSS-koodin kirjoittamisen.

Http	Protokolla, jota käytetään tiedon siirtämiseen ja kommunikointiin WWW-palvelimien kanssa.
State-objekti	JavaScript-objekti, joka sisältää erilaisia arvoja tai tilanmuuttujia, jotka liittyvät komponenttiin, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon.
Node.js	Avoimen lähdekoodin alustariippumaton ajoympäristö JavaScript-koodin suorittamiseen palvelimella.
Express.js	Kevyt, avoimen lähdekoodin web-sovelluskehys Node.js-ympäristölle.
MySQL	Relaatiotietokantaohjelmisto.
CORS	Cross-Origin Resource Sharing on web-turvamekanismi, joka säätelee, miten verkkosivustot voivat tehdä HTTP-pyyntöjä toisille verkkotunnuksille.
Body-parser	Express.js käytetty väliohjelmisto, joka auttaa käsittelemään HTTP-pyyntöjen rungon (body) tiedot.
bcrypt	Salausalgoritmi, jota käytetään tyypillisesti salasanojen turvalliseen tallentamiseen tietokannoissa.
MariaDB	Kehittäjäyhteisön kehittämä MySQL:ään pohjautuva relaatiotietokantajärjestelmä.
InnoDB	Tallennusmoottori MySQL:n.

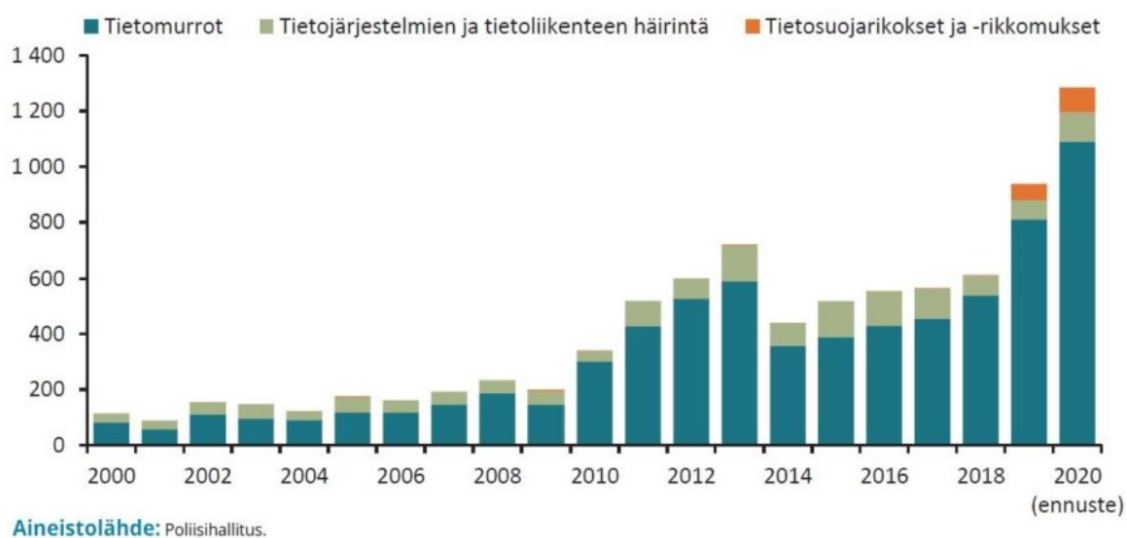
1 JOHDANTO

Tietoturvallisuus ja kyberturvallisuus ovat tärkeitä osa-alueita nykypäivän digitaalisessa ympäristössä, jossa teknologia kehittyy jatkuvasti, kun samalla verkossa piilevät uhkat kasvavat ja yleistyvät. Yritykset ja organisaatiot ovat alttiina erilaisille tietoturvariskeille ja kyberhyökkäyksille, jotka usein aiheuttavat merkittäviä taloudellisia menetyksiä ja mainehaittaa.

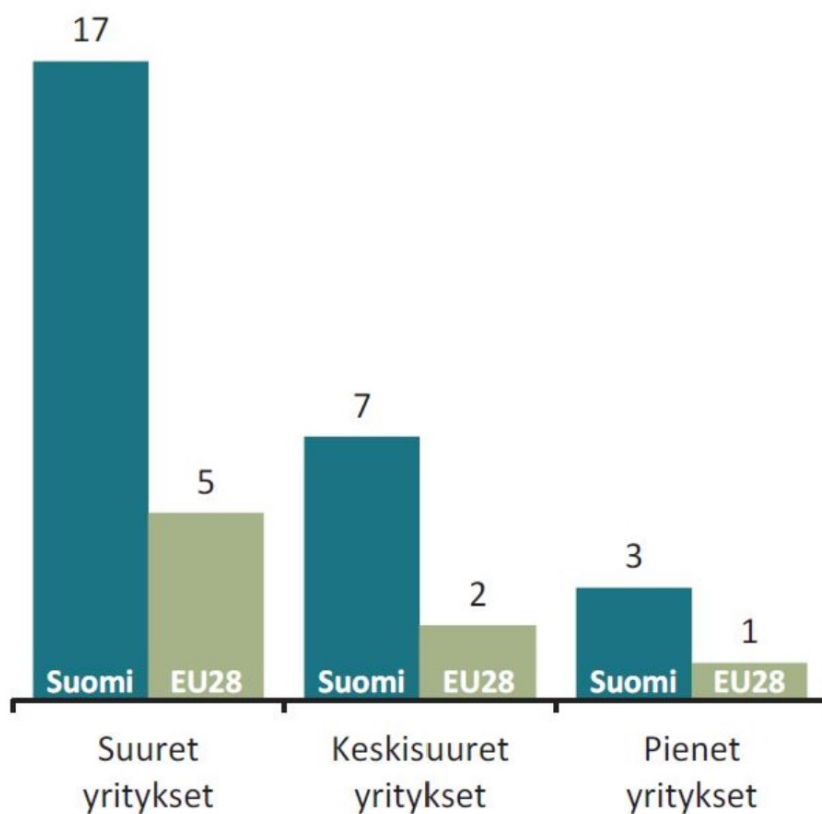
Tutkimukset osoittavat, että suomalaiset yritykset joutuvat verkkorikollisuuden kohteeksi huomattavasti useammin kuin muualla Euroopassa. Vuonna 2019 peräti 42 prosenttia suomalaisista suuryrityksistä ilmoitti kohdanneensa kyberturvaongelmia, kun vastaava luku koko EU:ssa oli vain 23 prosenttia. Lisäksi tietovuotoja raportoitiin Suomessa kolme kertaa enemmän kuin Euroopassa keskimäärin (STT 2020). Vuonna 2018 suomessa kirjattiin 477 tietomurtoa ja vuonna 2021 määrä oli jo 1467 (Mäntysalo 2022).

Yrityksille ja yhteiskunnalle aiheutuvat kustannukset kyberhyökkäysten seurauksena kasvavat edelleen huimaa vauhtia. Tietoturvayhtiö McAfee ja ajatushautomo CSIS arvioin mukaan vuonna 2018 globaalin kyberrikollisuuden kokonaiskustannukset olivat noin 600 miljardia euroa. Tämä vastasi noin 0,8 prosenttia maailman vuotuisesta bruttokansantuotteesta. Vuonna 2019 isoille yrityksille aiheutuneet kustannukset keskimäärin kyberhyökkäyksen kohteeksi joutumisen seurauksena olivat noin 3,8 miljoonaa euroa, mikä merkitsi yli 50 prosentin kasvua verrattuna vain vuotta aikaisempaan (Elinkeinoelämän tutkimuslaitos 2020).

Tämän opinnäytetyön tarkoituksena oli perehtyä tieto- ja kyberturvallisuuteen ja käydä läpi, miten voitaisiin tukea työelämässä olevien henkilöiden tieto- ja kyberturvallisuus osaamista. Tarkoitus oli myös luoda muistipeli, jonka avulla voisi opetella tietoturvallisuuden ja kyberturvallisuuden perusteita. Pelillä pyritään lisäämään tietoisuutta erilaisista uhkista, haavoittuvuuksista ja sekä mahdollisista parhaista käytännöistä, joilla voidaan suojautua haavoittuvuuksilta. Pelin avulla pelaajat voivat oppia tunnistamaan tietoturvariskejä, välttämään huijauksia ja suojaamaan omia sekä yrityksen tietoja paremmin.



Kuva 1. Poliisin tietoon tullut kyberrikollisuuden määrä Suomessa vuosina 2000–2020 (Elinkeinoelämän tutkimuslaitos 2020).



Lähde: Mattila et al. (2020), perustuen Eurostatin tietoihin.

Kuva 2. Tietovuodon kohteeksi joutuneet yritykset kokoluokittain 2019, % (Elinkeinoelämän tutkimuslaitos 2020).

2 TIETO- JA KYBERTURVALLISUUS

2.1 Tietoturvallisuus

Tietoturvallisuus, eli tietoturva, on olennainen osa digitaalista toimintaa, joka liittyy tietojen käsittelyyn ja säilyttämiseen. Se koskee laajasti erilaisia digitaalisia alustoja, kuten henkilökohtaisia tietokoneita, älypuhelimia, verkkopalveluita, julkisten organisaatioiden tietojärjestelmiä ja yritysten tietoverkkoja.

Tietoturvallisuus tarkoittaa tilannetta, jossa tietojasi voi käyttää ja muuttaa sinun lisäksi ainoastaan ne, joilla on siihen erityisoikeudet. Tietoturva pyrkii varmistamaan, että tietosi pysyvät suojattuina ja etteivät ne joudu väärin käsiin. Samalla kuitenkin varmistetaan, että tietoihin on helppo päästä käsiiksi silloin, kun niitä tarvitaan (Suomi.fi julkaisuaika tuntematon).

Tietoturvallisuus kattaa joukon toimenpiteitä ja käytäntöjä, joiden tavoitteena on suojata tietojärjestelmiä, tietokoneita, verkkoja ja niiden käyttäjiä erilaisilta tietoturvaongelmilta ja uhilta. Keskeisenä päämääränä on estää luvaton pääsy, muokkaus tai varastaminen. Tämä saavutetaan käyttämällä monipuolisesti teknisiä ja hallinnollisia toimenpiteitä.

Tietoturvassa korostetaan perinteisten uhkien, kuten luvattoman käytön, muokkauksen ja varastamisen, torjuntaa. Tärkeitä käytäntöjä ovat vahvat salasana, kaksivaiheinen tunnistautuminen, säännölliset päivitykset tietokoneille ja ohjelmistoille, haittaohjelmien torjunta sekä systemaattiset varmuuskopiot.

Käyttäjien tietoisuuden lisääminen on myös keskeinen osa tietoturvaa. Tämä sisältää esimerkiksi koulutusta haitallisten sähköpostiviestien ja linkkien tunnistamiseksi, ohjeistuksia varovaisuudesta sosiaalisessa mediassa sekä neuvontaa arkaluonteisten tietojen salassapidosta verkossa. Tietoturva ei ole pelkästään yksittäisten käyttäjien vastuulla, vaan se edellyttää myös organisaatioiden, yritysten ja valtioiden osallistumista tietoturvan kokonaisvaltaiseen turvaamiseen.

2.2 Kyberturvallisuus

Kyberturvallisuus keskittyy erityisesti suojaamaan tietojärjestelmiä ja verkkoja ulkoisilta hyökkäyksiltä, kuten haittaohjelmilta, tietomurroilta ja tietomurtoyrityksiltä. Kyberturvallisuus laajentaa näkökulmaa käsittämään digitaalista ympäristöä ja sen moninaisia uhkia. Tärkeimpänä tavoitteena on varmistaa, että tieto säilyy luottamuksellisena ja on saatavilla ainoastaan oikeutetuille käyttäjille. Kyberturvallisuudessa korostetaan digitaalisen toiminnan suojelua kaikenlaisilta mahdollisilta kyberuhilta.

Sähköiset ja internetistä riippuvaliset toiminnot ovat nykyään arkipäivää, ja merkittävä osa valtioiden kriittisestä infrastruktuurista perustuu näihin palveluihin. Siksi kyberturvallisuuden merkitystä ei voi liikaa korostaa. Voi vain kuvitella mitä tapahtuisi, jos yhteiskunnan kannalta elintärkeät palvelut lakkaisivat toimimasta äkillisesti esimerkiksi kyberhyökkäyksen seurauksena (F-Secure julkaisuaika tuntematon).

Kyberturvallisuus sisältää kaikki tietoturvakäytännöt, mutta painottaa erityisesti digitaalista puolta, kuten verkkoturvallisuutta, tietoverkkojen suojaamista ja kyberhyökkäysten torjuntaa. Organisaatioiden tulee käyttää luotettavia tietojärjestelmiä, suojata tietojaan asianmukaisesti ja kouluttaa henkilöstöään kyberturvallisuuteen liittyvissä asioissa.

Suomessa kyberturvallisuuden parissa työskentelee vuonna 2014 perustettu Kyberturvallisuuskeskus, joka toimii Liikenne- ja viestintävirasto Traficom alaisuudessa (F-Secure julkaisuaika tuntematon). Kyberturvallisuuskeskuksen tehtävänä on kehittää ja valvoa viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Lisäksi keskus tuottaa tietoturvallisuuden tilannekuvaa (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus julkaisuaika tuntematon).

3 ORGANISAATIOIDEN TIETOTURVA

3.1 Tietoturvallisuus suomessa

Vuoden 2023 aikana yksityishenkilöihin kohdistuneiden huijausten määrä on kasvanut. Lisäksi yrityksiä uhkaavien kiristyshaittaohjelmien käyttö on yleistynyt. Erityisen huolestuttavaa on se, että huijaukset ovat muuttuneet entistä hankalammiksi tunnistaa, ja tietojärjestelmien haavoittuvuuksia hyödynnetään aiempaa nopeammin (Tauriainen 2023).

Lokakuun 2023 alussa teleoperaattoreille asetettiin velvoite estää puhelinnumeroiden väärentäminen, mikä on johtanut puhelin- ja tekstiviestihuijausten määrän merkittävään vähenemiseen Suomessa. Se takia noin 80 % ulkomaan puhelinliikenteestä estettiin, koska ne olivat huijauspuheluita, jonka jälkeen puheluiden määrät Suomeen romahtivat. Puheluita soittaneet rikolliset lakkauttivat Suomeen kohdistuvat hyökkäyksensä, huonon menestymisen takia (Tauriainen 2023).

Mutta samoihin aikoihin Suomen suojelupoliisi varoitti, että Suomessa on ilmennyt useita tapauksia, joissa kotiverkon laitteita on käytetty välineenä vakoilussa. Esimerkiksi hyökkääjä, joka on yhteydessä ulkomailta, voi käyttää kodin verkkolaitteita peittääkseen alkuperänsä ja naamioida verkkoliikenteen tulevan Suomesta, joka sitten vaikeuttaa hyökkäyksen tunnistamista. Tyypillisesti kaikki verkkoliikenne kulkee yhden reitittimen ja saman verkon kautta, mikä tarkoittaa sitä, että kodin elektroniikka ja esimerkiksi työpaikan kannettava tietokone ovat todennäköisesti samassa verkossa. Tämä luo potentiaalisia haavoittuvuuksia ja lisää riskiä tietoturvaloukkauksille. Rikollisia ja vakoojia harvemmin kiinnostaa ne älyjääkaapit vaan niiden kiinnostuksen kohteita ovat esimerkiksi työtietokoneet ja niiden sisältö (Tauriainen 2023).

Suomessa on jopa joissain tapauksissa saatu tuotantolaitosten tuotanto seisautettua kiristyshaittaohjelmien voimin. Jos jokin kriittinen järjestelmän osa on salattu tai muutoin saatu pois käytöstä, tämä voi aiheuttaa yritykselle massiivisia vahinkoja. Vuoden 2023 lopussa Suomessa ilmeni ongelmia muutamissa yritysten järjestelmissä, johtuen kiristyshaittaohjelmahyökkäyksistä, joissa lunnaita ei voinut maksaa. Luultavammin taustalla oli joko vakoilu tai tietojen tuhoaminen. Yksi mahdollinen syy tietojen tuhoamiseen voi olla esimerkiksi yrityksen kehitystyön pysäyttäminen (Tauriainen 2023).

Tietoturvayhtiö Check Point mukaan marraskuussa 2023 viisi yleisintä haittaohjelmaa suomessa olivat Fakeupdates, Remcos, Snatch, Ducktail ja Viking. JavaScript-latausohjelma FakeUpdates nousi Suomen yleisimmäksi ja maailman toiseksi yleisimmäksi haittaohjelmaksi sen jälkeen, kun se oli hetken aikaa poissa yleisimpien haittaohjelmien listalta. Lokakuussa 2023 kyseinen haittaohjelma oli Suomessa kolmanneksi yleisin (Lehtiniitty 2023).

3.2 Yrityksen rooli tietoturvassa

Yrityksen rooli tietoturvassa on merkittävä, ja sen tulisi sitoutua suojaamaan liiketoimintaansa, asiakkaitaan ja työntekijöitään tietoturvariskeiltä. Sen tulisi kattaa kaikki toimet, joilla pyritään varmistamaan tietojen luottamuksellisuus, eheys ja saatavuus.

Jokaisen yrityksen on tärkeää olla tietoinen siitä, mitä vaatimuksia tietosuojalainsäädäntö asettaa heidän liiketoiminnalleen. GDPR (General Data Protection Regulation), eli EU:n yleinen tietosuojalainsäädäntö.

asetus, on luotu suojaamaan henkilötietoja ja vahvistamaan yksilöiden oikeuksia heitä koskevan datan käsittelyssä. Samalla se edistää jokaisen yrityksen tietosuojavaatimuksia. Huonosti toteutettu tietoturva voi altistaa yrityksen asiakastietojen pääsyn väärin käsiin, mikä aiheuttaa merkittävää mainehaittaa. Sen lisäksi siitä voi myös seurata suuria sanktioita esimerkiksi suuret sakot tai jopa vankeustuomio tietosuojarikoksesta. Yrityksen tulee siis tarkastella huolellisesti, miten ja missä he säilyttävät asiakkaidensa henkilötietoja ja varmistaa, että he täyttävät tietosuoja-asetuksen asettamat vaatimukset (Yrittäjät julkaisuaika tuntematon).

Yrityksen on nimettävä tietosuojavastaava, jos henkilötietojen käsittely on olennainen osa yrityksen liiketoimintaa, rekisteröityjen toimintaa seurataan säännöllisesti ja järjestelmällisesti tai jos arkaluonteisia tietoja käsitellään laajalti. Tietosuojavastaavaa voidaan nimittää myös tilanteissa, joissa tietosuoja-asetus ei sitä suoraan edellytä. Tehtävän ei välttämättä tarvitse olla yrityksen oman työntekijän vastuulla, vaan sen voi myös ulkoistaa. Huolimatta siitä, tuleeko tietosuojavastaava yrityksen sisältä vai ulkopuolelta, organisaation johdon vastuulla on lopulta varmistaa henkilötietojen käsittelyn lainmukaisuus (Yrittäjät julkaisuaika tuntematon).

Yrityksen tehtävä on huolehtia uusimmat päivitykset yrityksen laitteisiin ja että ne ovat jokaiselle asennettuna. Yrityksessä tulisi edistää kulttuuria, jossa on itsestään selvää ja velvollisuus pitää laitteet, kuten puhelimet ja tietokoneet päivitettyinä aina uusien päivitysten saapuessa tai viimeistään muutaman päivän kuluessa päivitysilmoituksen saamisesta. On tärkeää, että yritys perustelee työntekijöilleen, miksi tämä on olennaista. Lisäksi yrityksessä tulisi aina olla nimetty henkilö, joka ottaa vastuun yrityksen tietoturvasta ja pystyy auttamaan käytännön tietoturvakysymyksissä (Yrittäjät julkaisuaika tuntematon).

Yrityksen on myös tärkeä kouluttaa työntekijöistä tietoturvan osaajia. On olennaista kertoa ja perustella selkeästi, miksi tietyt tietoturvasäännöt ovat välttämättömiä työpaikalla. Tietämätön tai ajattelematon henkilö on usein tietoturvan heikoin lenkki. Lisäksi on tärkeää, että yritys on sopinut selkeästi työlaitteiden käytöstä ja verkkosivujen selailusta työntekijöiden kanssa. Esimerkiksi yrityksen kannattaa rajoittaa mitä sovelluksia pystyy lataamaan työpuheliin sovelluskaupasta ja kertoa miksi yrityksen kannettava tietokonetta, tablettia tai älypuheliin ei kannata yhdistää tuntemattomaan avoimeen verkkoon (Yrittäjät julkaisuaika tuntematon).

Yrityksen tehtävä on myös huolehtia omat verkkosivut kuntoon. Esimerkiksi, jos verkkosivustolla ei ole SSL-salausta, sen verkkoliikennettä ei ole suojattu. SSL-sertifikaatin käyttö auttaa vähentämään esimerkiksi haittaohjelmien leviämistä. Suosituimmat selaimet esim. Google Chrome, Mozilla Firefox ja Microsoft Edge, merkitsevät kaikki verkkosivustot, jotka toimivat ilman SSL-suojausta turvatomiksi ja varoittavat käyttäjiä tästä. Tämä voi vaikuttaa merkittävästi liiketoimintaan ja sivuston löydettävyyteen Googlen hakutuloksissa (Yrittäjät julkaisuaika tuntematon).

Suurin tietoturvaus on ihminen. Siksi on tärkeää, että yritys pitää eri järjestelmien ja ympäristöjen käyttäjätiedot sekä käyttöoikeudet ajan tasalla. On olennaista varmistaa, että poistuneiden työntekijöiden tilit ja oikeudet käsitellään asianmukaisesti, jotta he eivät voi enää päästä käsiksi yrityksen järjestelmiin. Myös kulkulupien kanssa yrityksen pitää olla tarkkana. Palvelinhuoneeseen ei tulisi

myöntää kulkulupaa kaikille työntekijöille, vaan ainoastaan niille, jotka tarvitsevat pääsyn, koska palvelimet sisältävät yleensä yrityksen arkaluonteisia tietoja (Yrittäjät julkaisuaika tuntematon).

3.3 Työntekijänrooli tietoturvassa

Työntekijöillä on merkittävä rooli organisaation tietoturvassa. Yritykset voivat omaksua useita käytäntöjä ja sääntöjä, mutta työntekijöiden sitoutuminen ja aktiivinen osallistuminen ovat keskeisiä onnistuneen tietoturvan varmistamiseksi.

Ihmisten käyttäytymisen ja toiminnan vaikutus tietoturvasuhteeseen on merkittävä. Siksi on tärkeää, että yrityksen työntekijät ymmärtävät, miten toimia erilaisissa tilanteissa, kuten epäilyttävien tiedostojen käsittelyssä. Henkilöstöturvallisuuden toimenpiteillä pyritään ehkäisemään tietoturvariskejä, jotka voivat johtua työntekijöistä ja sidosryhmistä (Laakso julkaisuaika tuntematon).

Työntekijältä vaadittava tietoturvaosaaminen vaihtelee työtehtävien perusteella. Yrityksen IT-osastolta vaaditaan teknistä tietämystä, kun taas yritysjohtajalla on tunnettava hallinnollinen tietoturva. Kaikkia kuitenkin yhdistävät yhtenäiset toimintatavat. Erottamalla erillisiä tietoturvakoulutuksia voidaan tehokkaasti jakaa parhaita käytäntöjä kaikille tasavertaisesti. Ohjeistamisen ja kouluttamisen tärkeyttä ei koskaan saa unohtaa. Näiden lisäksi työntekijöiden on vielä muistettava toimia, kuten ohjeissa kerrotaan (Laakso julkaisuaika tuntematon).

Yrityksissä työskentelee usein sellaisia henkilöitä, joiden tietoturvaton toimintatavat voivat vaarantaa koko yrityksen liiketoiminnan. Tällainen henkilö voi olla esimerkiksi tietojärjestelmien pääkäyttäjä tai ylimmän johdon työntekijä. Heitä yhdistää pääsy kriittisiin tietoihin, kuten henkilötietoihin tai palvelinhuoneisiin (Laakso julkaisuaika tuntematon).

4 YLEISIMMÄT KYBERUHAT

4.1 Kiristysohjelmat

Kiristysohjelma on haittaohjelma, joka salaa käyttäjän tiedostoja tai estää käyttäjän pääsyn tietoihin jollain tavalla. Tämän jälkeen hyökkääjä vaatii yleensä lunnaita tiedostojen tai järjestelmän palauttamiseksi. Yleensä lunnaiksi halutaan kryptovaluuttoja koska niitä on vaikeampi jäljittää verrattuna pankkisiirtoon ja näin olleen kiinni jäämisen riski on pienempi. Lunnaat ovat tavallisesti noin 300–500 dollarin arvoiset ja ne vaaditaan yleensä bitcoinkryptovaluuttana. Yleisimmin kiristysohjelmien tartunta saadaan vierailemalla haitallisilla verkkosivuilla, suojaamattomassa Wi-Fi-verkossa, lataamalla haitallinen sähköposti liitetiedosto, tai lataamalla laiteelle vahingossa tai toisen haittaohjelman kautta (F-Secure julkaisuaika tuntematon).

Kun kiristysohjelma on asennettu tietokoneelle, se käynnistää tiedostojen salauksen ja näyttää käyttäjälle viestin, jossa vaaditaan lunnaita, jotka pitää maksaa tiettyyn päivämäärään mennessä. Uhkana voi myös olla, että uhanalaisia tietoja julkaistaan verkkoon kaikkien saataville tai lähetään kaikille käyttäjän sähköposti kontakteille tai tuhotaan tiedostoja, jos lunnaita ei makseta. Lunnaita ei kannata maksaa missään nimessä koska se ei takaa, että rikolliset todella tekevät sen mitä lupaavat ja saatavat vaan sen jälkeen vaatia lisää rahaa (F-Secure julkaisuaika tuntematon).

4.2 Palvelunestohyökkäykset

Palvelunestohyökkäys on verkkohyökkäys, jossa pyritään saamaan tietokonejärjestelmä tai verkkopalvelu pois käytöstä ylikuormittamalla sitä. Tämä tapahtuu yleensä siten, että suuri määrä tietokoneita tai muita laitteita, usein eri puolilta maailmaa, yhdistetään ja niitä käytetään lähettämään valtavia määriä pyyntöjä kohdejärjestelmälle tai vaihtoehtoisesti hyökkääjä voi lähettää sellaista liikennettä, joka aiheuttaa kohde laiteelle normaalia suuremman kuormituksen muisti- tai laskentaresursseja vaativien tehtävien käsittelyyn, ilman että liikenteen määrän tarvitsee olla erityisen suuri. Tämän tyyppiset hyökkäykset eivät välttämättä näy liikennemäärän poikkeuksellisenä kasvuna. Tällainen massiivinen tietoliikenteen määrä voi ylittää kohteen resurssit, kuten verkkokaistan leveyden, palvelimen suorituskyvyn tai muut resurssit, mikä johtaa sen hidastumiseen tai jopa kaatumiseen (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus 2022).

Hyökkääjät hyödyntävät yleisesti bottiverkkoja, jotka muodostuvat lukuisista internetiin kytketyistä laitteista, jotka on kaapattu laitteiden omistajien tietämättään hyökkäyksiä varten. Palvelunestohyökkäyksiin ei tarvita nykyisin laajaa teknistä asiantuntemusta, sillä niitä voidaan ostaa edullisesti esimerkiksi pimeästä verkosta. (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus 2022).

Tällaiset hyökkäykset voivat olla haitallisia yrityksille ja organisaatioille, koska ne voivat aiheuttaa palvelukatkoja, liiketoimintahäiriöitä ja muita vakavia ongelmia. Usein tällaisia hyökkäyksiä tehdään myös kiristuksen, kiusanteon tai ideologisen motiivin vuoksi (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus 2022).

4.3 Tietokonevirukset

Tietokonevirus on haittaohjelma, joka leviää ja tarttuu muihin ohjelmiin tai tiedostoihin. Virus voi aiheuttaa vahinkoa tietokoneelle, kuten tietojen tuhoutumista, hidastaa laitteen käyttöä, ohjelmistojen toimintahäiriöitä tai muita haittavaikutuksia (F-Secure julkaisuaika tuntematon).

Viruksille ominaista on, että ne tarvitsevat isännän, johon ne voivat tarttua. Käyttäjät voivat saada viruksen esimerkiksi lataamalla tartunnan saaneita tiedostoja internetistä, avaamalla saastuneita sähköpostiliitteitä tai käyttämällä tartunnan saaneita ulkoisia tallennusvälineitä. Kun käyttäjä avaa viruksesta saastuneen tiedoston tai ohjelman, virus aktivoituu ja leviää. Siihen saakka virus pysyy piilossa, odottaen käyttäjän toimia (F-Secure julkaisuaika tuntematon).

4.4 Tietokonemadot

Tietokonemato on toinen tyyppinen haittaohjelma, joka eroaa viruksista toimintatapansa suhteen. Madot ovat itsenäisiä ohjelmia, jotka kykenevät itsenäiseen leviämiseen ja lisääntymiseen tietokoneverkoissa ilman isäntäohjelman tai tiedoston tarvetta. Tällä tavoin se myös leviää muihin tietokoneisiin samassa verkossa. Toisin kuin virukset, madot eivät välttämättä liitä itseään olemassa oleviin ohjelmiin tai tiedostoihin (F-Secure julkaisuaika tuntematon).

Madot voivat levitä hyödyntämällä tietoturva-aukkoja ja haavoittuvuuksia tietokonejärjestelmissä. Ne voivat kopioitua itsestään ja levitä tietokoneesta toiseen esimerkiksi sähköpostiliitteiden, piiloutumalla pikaviestipalveluissa lähetettyihin viesteihin, verkkoliikenteen tai muiden tietoverkkojen kautta. Madot voivat aiheuttaa haittaa tietojärjestelmille, kuten hidastaa verkkoliikennettä, varastaa tietoja tai asentaa muita haittaohjelmia (F-Secure julkaisuaika tuntematon).

4.5 Troijalaiset

Trojialainen on haittaohjelma, joka naamioituu näyttämään hyödylliseltä tai vaarattomalta ohjelmistolta, mutta sen todellinen tarkoitus on suorittaa haitallisia toimintoja tietokoneella ilman käyttäjän lupaa tai tietämystä. Trojialainen voi esimerkiksi seurata näppäimistön painalluksia ja siepata salasanonoja sekä muita henkilökohtaisia tietoja asentamalla vakoiluohjelmia laitteelle. Troijalaiset eivät yleensä leviä itsestään, kuten virukset tai matot, vaan käyttäjän on tahattomasti asennettava ne tietokoneelleen. Trojialainen voi esimerkiksi naamioitua tietokoneen ohjelmaksi, päivitykseksi, sähköpostin liitteeksi tai muuksi mahdolliseksi ominaisuudeksi, ja mahdollinen uhri houkutellessaan avaamaan se tietokoneella. Troijalaiset eivät tartu vain tietokoneisiin. Ne voivat myös tarttua vaivihkaa älypuheliin, joissa ne voivat esimerkiksi piiloutua tekstiviesteihin (Lorentsen 2023).

Nimi "trojialainen hevonen" viittaa antiikin tarinaan, jossa kreikkalaiset käyttivät puista hevosta piilottaakseen joukon sotilaita hevosen sisään. Troijalaiset uskoivat, että kreikkalaiset olivat luovuttaneet ja jättäneet heille lahjaksi valtavan puuhevosen. He avasivat kaupungin portit, vetivät hevosen Troijan muurien sisään ja lopulta sotilaat tulivat ulos hevosen sisältä ja valtasivat kaupungin. Periaatteessa virusta muistuttava trojialainen toimii samalla tavalla, ja nimi tulee siitä (Lorentsen 2023).

Troijalaiset voivat suorittaa monenlaisia haitallisia toimintoja, kuten tietojen varastamista, vakoilua, tietokoneen kaappaamista, haittaohjelmien asentamista tai muiden haitallisten toimintojen mahdollistamista. Niiden tarkoituksena on usein jäädä huomaamatta ja toimia taustalla keräten tietoja tai mahdollistaen laajemman hyökkäyksen (Lorentsen 2023).

4.6 Käyttäjän manipulointi

Käyttäjän manipuloinnissa yksilön tai ryhmän tarkoituksena on manipuloida ja harhauttaa ihmisiä paljastamaan luottamuksellista tietoa. Se perustuu enemmän psykologiaan ja ihmisen käyttäytymiseen kuin tekniseen taitotietoon (Euroopan unionin neuvosto 2023).

Käyttäjän manipuloinnissa hyökkääjä usein esittäytyy luotettavana henkilönä tai lähteenä saavuttaakseen uhrin luottamuksen. Hyökkääjällä on erilaisia keinoja kuten tekeytyminen toiseksi henkilöksi, taivuttelu tai hämäys, joilla hän yrittää saada tärkeitä tietoja esim. salasanoja, taloudellisia tietoja tai pääsyn järjestelmään tai verkkoon. Hyökkääjä saattaa esim. lähettää sähköpostia yrityksen työntekijöille ja tekeytyä IT-tukihenkilöksi ja tämän varjolla kalastaa yrityksen arkaluonteisia tietoja (Euroopan unionin neuvosto 2023).

Käyttäjän manipuloinnissa hyökkäykset voivat vaihdella muodoltaan. Se ei välttämättä aina tapahdu digitaalisessa ympäristössä vaan voi myös ilmetä fyysisessä ympäristössä. Tarkoituksena on hyödyntää inhimillistä haavoittuvuutta hyökkääjän tavoitteiden saavuttamiseksi, olipa kyse sitten luvattomasta pääsystä taikka datan tai rahan varastamisesta (Euroopan unionin neuvosto 2023).

4.7 Vakoiluohjelmat

Vakoiluohjelma on haittaohjelma, joka tartuttaa laitteen ja vakoilee sitä. Se siirtää sitten tiedot hallinnoijilleen. Monet ohjelmat keräävät tietoja käyttäjästä, mutta vakoiluohjelma tekee sen ilman lupaa ja käyttäjän tietämättä. Ja yleensä pahat mielessä. Tyypillisimpiä vakoiluohjelmien varastamia tietoja ovat luottokorttitiedot, salasanat, käyttäjänimet, verkkopankkien tunnistetiedot ja tiedot käyttäjän toimista verkossa. Rikolliset voivat käyttää näitä tietoja tilien valtaamiseen ja identiteettivarkauksiin. Valtionhallinnot, mainostajat ja rikolliset voivat käyttää vakoiluohjelmia myös seurantaan (F-Secure julkaisuaika tuntematon).

Vakoiluohjelmat osoittavat tyypillisesti monipuolisia haitallisia vaikutuksia, jotka eivät rajoitu ainoastaan vakoilutoimintaan. Näillä ohjelmilla tunnusomaista on usein järjestelmän ja verkkoyhteyden hidastuminen. Ne voivat myös muuttaa laitteen tietoturva-asetuksia ja mahdollistaa muiden haittaohjelmien lataamisen. Lisäksi laitteeseen ja selaimeen saattaa ilmestyä enemmän mainoksia ja ponahdusikkunoita (F-Secure julkaisuaika tuntematon).

Yleensä vakoiluohjelmat leviävät tartuttamalla käyttäjän tietokoneen haitallisten liitetiedostojen, sähköpostiviestien, vioittuneiden verkkosivustojen avulla. Vakoiluohjelma voi myös olla usein troijalainen, joka pääsee laitteeseen, kun asentaa jonkin toisen ohjelman. Vakoiluohjelma voi käyttää myös etenkin selaimissa olevia ohjelmistohaavoittuvuuksia sisäänkäyntiin. Jos laitteessa on vakoiluohjelma, siinä on todennäköisesti myös muita haittaohjelmia (F-Secure julkaisuaika tuntematon).

5 UHKIEN TORJUNTA

5.1 Miten parantaa työntekijöiden tietoturvaosaamista?

”Yrityksen tietoturva on yhtä heikko, kuin sen heikoin lenkki”. Tästä syystä olisi hyvä parantaa työntekijöiden tietoturvaosaamista. Työntekijöiden tietoturvaosaamisen parantamiseen on yksinkertaisia keinoja, kuten tutustuttamalla yrityksen tietoturvakäytäntöihin ja kertomalla vastuut selkeästi. Tulisi myös ohjeistaa työntekijöitä käyttämään vahvoja salasanoja ja päivittämään niitä säännöllisesti ja lisäksi käyttämään kaksivaiheista tunnistautumista aina kun mahdollista. Näiden lisäksi on hyvä kertoa miten jakaa tiedostoja turvallisesti ja miten tarkistaa asiakirjojen oikeus luokitukset, kuten yksityinen, luottamuksellinen ja julkinen.

Työntekijöille pitäisi olla selkeät toimintatavat ja ohjeet eri tilanteita varten. Työntekijöille pitäisi järjestää säännöllisiä tietoturvakoulutuksia ja -tietoiskuja, jotka käsittelevät ajankohtaisia uhkia ja hyökkäystapoja. Työntekijöille voi myös järjestää tietoturvaharjoituksia, jotta työntekijät voivat harjoitella oikeissa tilanteissa toimimista. Työntekijöille olisi hyvä tarjota avoimia viestintäkanavia, joiden kautta työntekijät voivat ilmoittaa epäilyttävistä tapahtumista tai kysyä neuvoa tietoturvallisista käytännöistä. Työntekijöitä voi myös palkita hyvistä tietoturvakäytännöistä ja asettaa selkeät seuraamukset tietoturvasääntöjen rikkomisesta.

5.2 Miten tunnistaa tietoturvauhat?

Tietoturvauhat voivat ilmetä monin eri tavoin, ja niiden tunnistaminen voi olla välillä haastavaa, koska ne voivat vaihdella suuresti ja nykyisin kyberrikolliset ovat ovelia mutta aina kannattaa muistaa, että jos joku asia on liian hyvää ollakseen totta, se ei todennäköisesti ole totta. Eli jos saapuneessa sähköpostiviestissä ilmoitetaan mahdollisuudesta saada miljoona perintönä tuntemattomalta henkilöltä, mutta vastaanottajalta vaaditaan ensin maksamaan asianajajan kulut, tulisi tässä vaiheessa herätä epäily.

Suomen kielen avulla on myös hyvä tunnistaa tietoturvauhkia koska Suomen kieli on aika haastava ja maailman väkilukuun nähden aika harva puhuu Suomea. Näin ollen on pienempi todennäköisyys, että Kyberrikolliset puhuisivat Suomea. Silloin yleensä kyberrikolliset joutuvat turvautumaan kääntäjään lähettääkseen Suomen kielellä esimerkiksi tietojenkalasteluviestin ja kun Suomen kieli on aika haastavaa, niin kääntäjä tekee siinä aika helposti virheitä eli jos tulee esimerkiksi epäilyttävä tekstiviesti Suomen poliisilta ja se on kirjoitettu huonolla Suomella niin silloin pitäisi herätä epäilykset. On tärkeää tiedostaa, että osa kyberrikollisista hallitsee myös Suomen kielen, ja viime aikoina tekoäly on kehittynyt nopeasti, osaten jo melko hyvin Suomen kieltä. Tätä osaamista voi hyödyntää kuka tahansa.

5.3 Perinteiset torjuntakeinot

5.3.1 Virustorjuntaohjelmisto

Virustorjuntaohjelmistot havaitsevat ja poistavat haittaohjelmia, kuten viruksia, matoja ja troijalaisia, joiden tarkoituksena on vahingoittaa tietokonejärjestelmiä. Virustorjuntaohjelmisto olisi hyvä ainakin asentaa kaikkiin Windows ja macOS käyttöjärjestelmiin sekä Android puhelimiin sekä tabletteihin. Kun taas iPhoneille sekä iPadille virustorjunta ei ole välttämätön hankinta koska virukset eivät ole

järin merkittävä tietoturvaus niille (F-Secure julkaisuaika tuntematon). Myöskään Linux käyttöjärjestelmään sitä ei ole välttämättä pakko asentaa koska Linuxiin vaikuttavat virukset ovat edelleen hyvin harvinaisia (Ubuntu julkaisuaika tuntematon).

5.3.2 Palomuuuri

Palomuuuri on ohjelmisto, jonka tarkoitus on estää haitallista verkkoliikennettä tietokoneessa. Palomuuuri estää häiritsevien ja sopimattomien IP-osoitteiden pääsyn laitteeseen ja suojaa tietokonetta muun muassa haittaohjelmilta. Palomuuuri tarkkailee myös laitteestasi lähtevää liikennettä ja tarvittaessa puuttuu peliin, jos se havaitsee mitään epäilyttävää (F-Secure julkaisuaika tuntematon).

Useimmissa tietokoneissa on valmiiksi jonkinlainen palomuuuri, joka on yleensä oletuksena päällä valvomassa verkkoliikennettä. Windows käyttöjärjestelmässä, se on nimeltään Windows Defender Firewall ja se on siinä oletuksena päällä. Palomuuuri ei kuitenkaan tarjoa yksinään riittävää suojaa verkon vaaroja vastaan, vaan sen tueksi tarvitaan yleensä virustorjuntaohjelma (F-Secure julkaisuaika tuntematon).

5.3.3 Vahvat salasanat ja kaksivaiheinen tunnistautuminen

Hakkerit murtavat salasanoja ohjelmilla, jotka testaavat miljoonia eri vaihtoehtoja sekunnissa. Tästä huolimatta riittävän monimutkaisen salasanan murtaminen voi viedä miljoonia vuosia eli hyvää salanaa kannattaa miettiä tarkkaan (F-Secure julkaisuaika tuntematon).

Salasana tulisi olla mahdollisimman pitkä koska mitä pidempi salasana on, sitä vaikeampi se on arvata tai murtaa. Hyvä salasana myös sisältää monenlaisia merkkejä, kuten isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Tämä tekee salasanasta vielä monimutkaisemman. Mutta helposti arvattavia tietoja, kuten syntymäpäiviä, nimiä ja muita henkilökohtaisia tietoja tulisi välttää salassana. Tällaiset tiedot voivat olla helposti saatavilla tai arvattavissa. Myöskään peräkkäisiä numeroita tai kirjaimia, kuten "12345" tai "abcde" tulisi välttää, koska ne ovat helppoja arvata. Samaa salanaa ei tulisi käyttää useilla eri tileillä koska, jos salasana paljastuu hakkeri todennäköisesti, kokeilee sitä salanaa myös muihin tileihin ja pääsee myös niihin käsiksi. Salasana tulisi myös päivittää säännöllisin väliajoin.

Salasanan lisäksi olisi hyvä olla käytössä kaksivaiheinen tunnistautuminen. Silloin ei pelkkä käyttäjätunnus ja salasana riitä vaan lisäksi on todistettava henkilöllisyys jollain toisella tavalla ennen pääsyn myöntämistä tiettyyn järjestelmään, palveluun tai tilille. Toinen tapa tunnistautua voi olla esimerkiksi puhelimeen tekstiviestillä lähetettävä koodi, henkilökohtainen turvakysymys, sormenjälki tai mobiilisovellus (F-Secure julkaisuaika tuntematon).

Kaksivaiheisen tunnistautumisen tarkoituksena on lisätä turvallisuutta, sillä pelkän salasanan varassa oleva tunnistautuminen voi olla haavoittuvainen esimerkiksi tietomurroille tai haittaohjelmille. Vaikka salasana paljastuisi, hyökkääjällä olisi silti vaikeampaa päästä tietoihin käsiksi ilman toista tunnistusvaihetta. Monet verkkopalvelut, kuten sähköpostit, pankit ja sosiaalisen mediat, tarjoavat mahdollisuuden käyttää kaksivaiheista tunnistautumista ja nykyisin jopa vaativat sen käyttöä.

5.3.4 Ohjelmistojen päivitykset

Ohjelmistojen päivittäminen on erittäin tärkeä osa tietoturvaa koska julkittuluiden haavoittuvuuksien hyväksikäyttö on ollut kasvava trendi jo pidemmän aikaa. Kun valmistajat julkaisevat ohjelmistopäivityksiä, rikolliset iskevät nopeasti niihin kohteisiin, joita ei ole vielä ehditty päivittää. Päivitykset sisältävät usein korjauksia tunnistettuihin haavoittuvuuksiin ja parannuksia tietoturvaan. Siksi on tärkeää päivittää kaikki ohjelmistot heti kun niihin tulee uusi päivitys. Tärkeää olisi päivittää esimerkiksi käyttöjärjestelmä, virustorjunta, selain, kaikki asennetut ohjelmat. Myös modeemi ja reititin tulisi aina päivittää (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus 2020).

Kun ohjelmisto tai laite tulee elinkaarensa päähän, valmistaja ei enää tuota siihen päivityksiä. Tässä vaiheessa laite tai ohjelmisto pitää uusia täysin sellaiseen versioon, jonka kehitystä ja turvallisuutta valmistaja tukee jatkossakin. Esimerkiksi tietokoneissa, joissa käyttöjärjestelmä on Windows 8, suositellaan päivittämään se Windows 10:een, sillä Microsoft ei enää tarjoa tukea Windows 8:lle. Jos päivitys Windows 10:een ei ole mahdollinen, suositellaan harkitsemaan uuden tietokoneen hankintaa tai vaihtoehtoisesti toisen käyttöjärjestelmän, kuten Linuxin, asentamista (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus 2020).

Useimmat ohjelmat tarjoavat automaattisia päivityksiä, jolloin päivityksiä ei itse tarvitse etsiä verkosta. Samalla voit olla varma, että käyttämäsi ohjelmistot ovat ajan tasalla eivätkä päivitykset unohdu. Yleensä automaattinen päivitys on oletuksena päällä. Myös yrityksen tulisi tarjota automaattiset päivitykset, että työntekijän ei tarvitse niistä huolehtia ja yrityksen laitteet pysyvät aina ajan tasalla (Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus 2020).

5.3.5 Varmuuskopiot

Varmuuskopiointi on prosessi, jossa tietoja tallennetaan toiseen sijaintiin tai välineeseen turvallisuuden varmistamiseksi ja mahdollisen tietojen menetyksen välttämiseksi ja näin ollen se on tärkeä osa tietoturvaa. Tietojen menetys voi johtua monista syistä, kuten laitteiston vioista, viruksista, inhimillisistä virheistä tai varkaudesta. Varmuuskopiointi auttaa palauttamaan tärkeät tiedot, jos jotain tällaista tapahtuu.

Varmuuskopiointi voi toteutua monin eri tavoin, ja valittu strategia riippuu käyttäjän tarpeista ja resursseista. Yksi yleinen käytäntö on säännölliset varmuuskopiot, jotka varmistavat, että kaikki tärkeät tiedot ovat turvassa. On olemassa myös automaattisia varmuuskopiointiohjelmia, jotka helpottavat prosessia, kun ei tarvitse itse tehdä manuaalisesti varmuuskopioita.

Tiedon varmuuskopiointiin voidaan käyttää erilaisia tallennusvälineitä, kuten ulkoisia kiintolevyjä tai pilvipalveluita. Ulkoiset kiintolevyt tarjoavat fyysisen vaihtoehdon, kun taas pilvipalvelut mahdollistavat tiedon tallentamisen verkkoon, mikä tarjoaa helpon ja laajan saatavuuden tiedoille. Fyysinen vaihtoehto on hyvä, jos ei halua luovuttaa arkaluonteista tietoa kolmansille osapuolille.

5.3.6 Käyttöoikeuksien hallinta

Käyttöoikeuksien hallinta keskittyy siihen, miten organisaatiot hallinnoivat käyttäjien pääsyä tietojärjestelmiin ja -resursseihin. Sen tarkoituksena on varmistaa, että oikeat ihmiset pääsevät oikeisiin resursseihin ja että organisaation tiedot pysyvät turvassa.

Käyttöoikeuksien hallinta estää haitallisia toimijoita ja valtuuttamattomia käyttäjiä pääsemästä käsiinsä luottamuksellisiin tietoihin, kuten asiakastietoihin. Samalla se vähentää riskiä, että työntekijät siirtävät tietoja luvattomasti ja torjuu verkkopohjaisia uhkia. Suurin osa organisaatioista, jotka painostavat tietoturvaan, hyödyntää käyttäjätietojen ja käyttöoikeuksien hallintaratkaisuja sen sijaan, että hallitsisivat oikeuksia manuaalisesti (Microsoft julkaisuaika tuntematon).

Yksinkertaisimmassa muodossaan käyttöoikeuksien hallinta tarkoittaa, että käyttäjä tunnistetaan hänen tunnistetietojensa perusteella, ja kun hänet on todennettu, hänelle annetaan sopivan tasoiset käyttöoikeudet. Tunnistetietoja ovat esimerkiksi salasanat, PIN-koodit ja sormenjäljet. Sitten kun käyttäjän henkilöllisyys on todennettu, käyttöoikeuksien hallinnan käytännöt antavat tietyt käyttöoikeudet ja valtuuttavat käyttäjän jatkamaan tarkoittamallaan tavalla (Microsoft julkaisuaika tuntematon).

6 MUISTIPELI TIETOTURVAN/KYBERTURVALLISUUDEN TUKEMISEKSI

6.1 Muistipeli koulutuskäytössä

Muistipeli voi olla erinomainen apuväline myös koulutuskäytössä, erityisesti kun halutaan kehittää muistia, keskittymistä ja ongelmanratkaisutaitoja. Muistipeli vaatii lyhytkestoista työmuistia, mutta toistamalla asioita tarpeeksi monta kertaa ne siirtyvät pitkäkestoiseen säilömuistiin. Toistojen ansiosta muistipelin aiheet jäävät paremmin mieleen. Lisäksi pitkäkestoinen harjoittelu auttaa asioiden mieleen painamisessa (Jylhäsalmi 2018). Jotkut ihmiset säilyttävät mielenkiintonsa paremmin harjoittelussa, kun voivat tehdä sen konkreettisesti verrattuna teoreettiseen opiskeluun lukemisen kautta. Tästä syystä esimerkiksi muistipeli voi sopia toisille paremmin koulutuksen tueksi.

Koulutuksellisessa kontekstissa muistipeli voi olla erityisen hyödyllinen oppimismenetelmä, kun halutaan vahvistaa käsitteiden ja käytännön taitojen oppimista. Pelin avulla voidaan luoda vuorovaikutteisia oppimistilanteita, jotka tekevät koulutuksesta mielenkiintoisempaa ja tehokkaampaa. Lisäksi muistipelissä käytettävät aiheet voivat räätälöidä koulutusta vastaamaan tiettyjä oppimistavoitteita tai teemoja.

6.2 Projektin kuvaus

Tarkoituksena oli kehittää web-sovellus, jonka kohderyhmänä ovat työelämässä olevat henkilöt, ja joka mahdollistaa tietoturvan ja kyberturvallisuuden perusteiden opiskelun. Toimeksiantaja ei asettanut oikeastaan muita rajoitteita, joten meillä oli aika lailla vapaat kädet toteuttaa sovellus.

Projektin lopputuloksena on toimiva muistipeli, jonka korttiparit muodostuvat kysymyksistä ja niihin vastauksista. Valittavana on kolme eri vaikeusastetta ja teemaa. Projektin kehitys ajaksi arvioitiin kaksi ja puoli kuukautta.

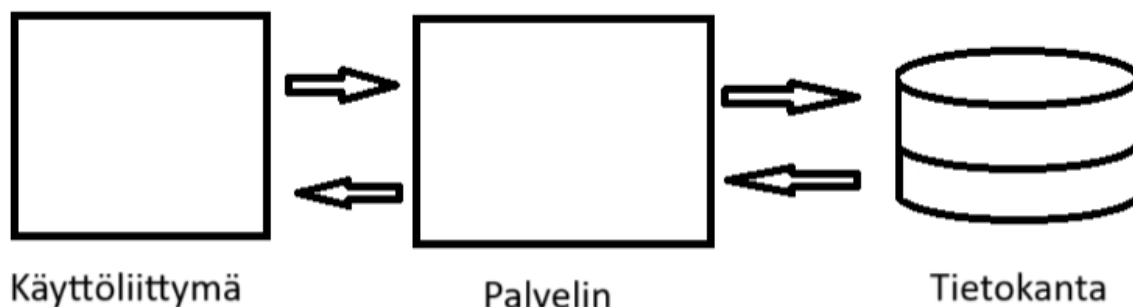
6.3 Projektin suunnittelu

Suunnittelutyössä keskityttiin luomaan monipuolisia ja laadukkaita kysymyksiä tietoturvan ja kyberturvallisuuden liittyen, jotka kattavat tietoturva-alan perusteet. Käyttäjä harjoittelisi ja opettelisi tieto- ja kyberturvallisuutta muistipelin muodossa, mutta Peli eroaa perinteisestä pareja etsivästä logikasta, sillä käyttäjien tehtävänä on yhdistää riski ja siihen liittyvä torjuntakeino.

Suunnittelussa päädyttiin tarjoamaan käyttäjälle erilaisia vaikeustasoja ja teemoja, jotta käyttäjät voivat valita itselleen sopivan haasteen. Helpolla vaikeustasolla olisi kuusi paria, normaalilla kaksitoista paria ja vaikealla kaksikymmentäneljä. Teemoina olisi tietoturvan ja kyberturvallisuuden peruskäsitteet, verkkoturvallisuus ja älylaitteiden turvallisuus. Käyttäjällä olisi mahdollisuus kirjautua sisään, minkä jälkeen hän voisi muokata, lisätä ja poistaa korttipareja.

7 SOVELLUKSEN ARKKITEHTUURI JA TEKNIIKAT

Muistipeli on web-sovellus, joka on luotu hyödyntäen JavaScript-ohjelmointikielen kirjastoa. Sovellus on jaettu kolmeen pääkomponenttiin, jotka vaihtavat tietoja keskenään. Käyttöliittymä kommunikoi palvelinpuolen kanssa käyttäen REST-rajapintaa, kun taas palvelinpuoli vuoro vaikuttaa tietokannan ja käyttöliittymän kanssa.



Kuva 3. Sovelluksen arkkitehtuuri (Kiminki 2024).

7.1 Käyttöliittymä

Web-sovelluksen käyttöliittymä toteutettu React JavaScriptin-kirjastolla. Kirjaston avulla verkkoselain renderöi käyttäjälle näkyviin käyttöliittymän, joka koostuu JavaScriptistä, HTML:stä ja CSS:stä. Reactin luomisessa käytettiin Vite-kehitystyökalua. Ulkoasun tyylien luomisessa käytimme SASS-komentosarja kieltä, jossa on monia ominaisuuksia esim. muuttujat, joita pystyt jakamaan tyylietiedostojen välillä. Käyttöliittymän ja palvelinpuolen tiedonvälitys tapahtuu http-pyyntöillä.

Käyttöliittymä otti saamansa tiedot sisään rakennettuun state-objekteihin, joista tiedot välitettiin oikeille komponenteille käytettäväksi. Hallinta puolella otimme käyttöön keksit (cookies), jolla saadaan käyttäjä pidettyä sisällä. Sivustolla liikkuminen on luotu yleisimmällä navigointi kirjastolla reactissa eli React-Router.

7.2 Palvelinpuoli

Web-sovelluksen palvelinpuoli on toteutettu Node.js-toteutusympäristöllä ja se käyttää Express.js verkkosovelluskehystä, joka on yksinkertainen ja kevyt. Se toteuttaa monipuolisen palvelinpuolen logiikan muistipelin korttien hallinnassa ja käyttäjien kirjautumisessa sekä rekisteröitymisessä. Sovellus hyödyntää MariaDB-tietokantaa korttien ja käyttäjätietojen tallentamiseen. Palvelinpuolen koodissa on selkeä rakenne, ja se käyttää useita moduuleja, kuten Express, CORS, MySQL, Body-parser ja Bcrypt, tarjoten näin tehokkaan ja laajennettavan ratkaisun.

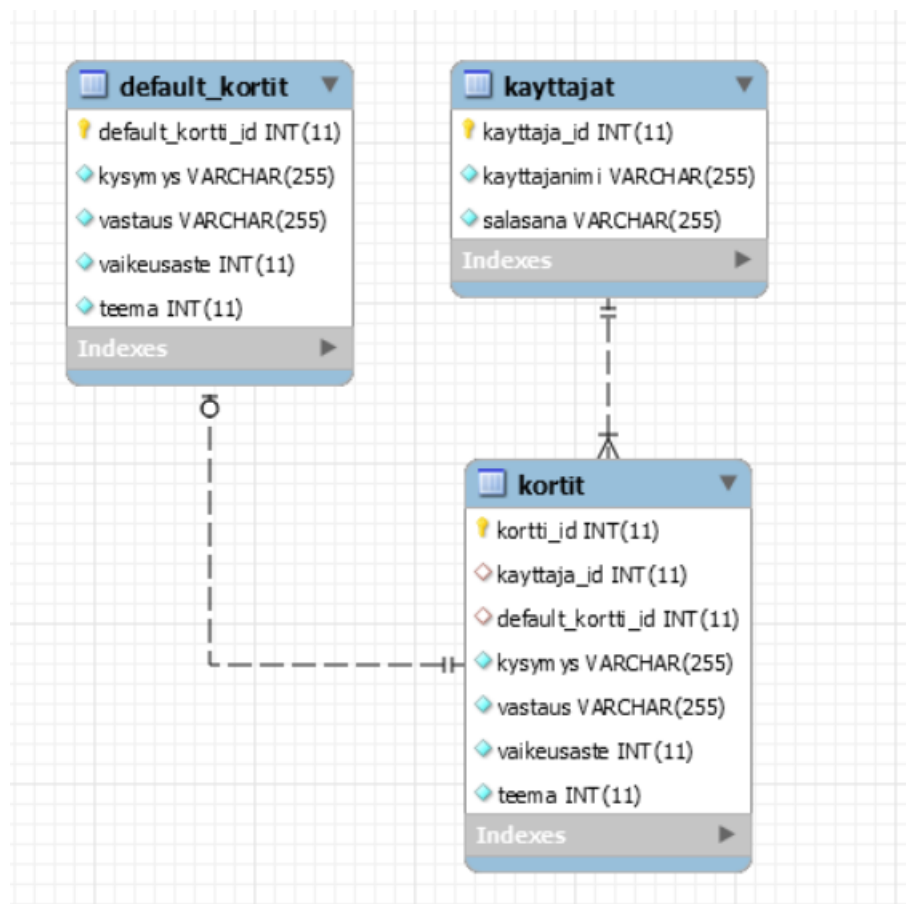
Sovellus tarjoaa lukuisia reittejä, jotka mahdollistavat erilaisten toiminnallisuuden suorittamisen. Sovellus käsittelee HTTP-pyyntöjä, jotka liittyvät korttien hakuun, lisäämiseen, muokkaamiseen ja poistamiseen. Lisäksi se hoitaa käyttäjän kirjautumisen ja rekisteröitymisen turvallisesti salaten ja tarkistaen salasanat Bcrypt-moduulin avulla.

Palvelinpuolen koodi sisältää myös huolellista virheiden käsittelyä eri vaiheissa, mikä parantaa sovelluksen luotettavuutta. Esimerkiksi se palauttaa asianmukaiset HTTP-vastaukset ja virheilmoitukset

eri tilanteissa. Palvelinpuoli on suunniteltu tarjoamaan selkeän ja tehokkaan rajapinnan muistipelin korttien sekä käyttäjätietojen hallintaan.

7.3 Tietokanta

Tietokanta toteutettiin paikallisilla MariaDB:llä ja tietokantamoottorina toimi InnoDB. Sovelluksen käyttämät tiedot tallentuvat yhteen tietokantaan. Tiedot on jaettu kolmeen eri tauluun, jotka ovat liitetty toisiinsa avaimilla. Tauluja ei pysty sovelluksen kautta itsessään muokkaamaan, poistamaan tai lisäämään, mutta tauluissa olevia tietoja voidaan muokata. Tietokannan tauluihin kaikki muut tiedot tallentuvat selkokieლისinä paitsi salasana. Salasana tallennetaan kryptattuna, jolloin voitaisiin estää mahdollinen käyttäjätilin väärin käyttö.



Kuva 4. Tietokannan ER-kaavio (Kiminki 2024).

8 ULKOASUT JA NÄKYMÄT

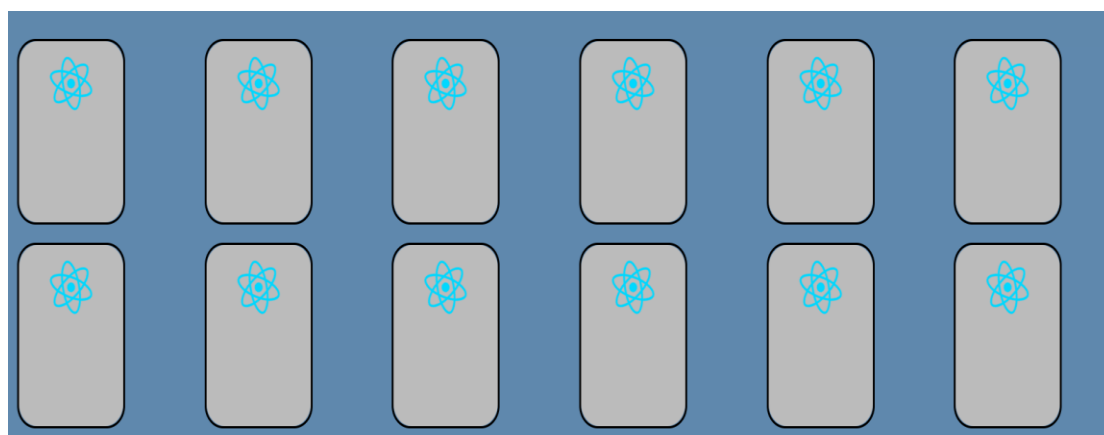
8.1 Etusivu

Sivustolle tultaessa käyttäjä voi joko kirjautua sisään hallinta puolelle ”Kirjaudu”-painiketta painamalla tai päättää vaikeusasteen ja teeman ja aloittaa pelaamisen ”Aloita Peli”-painiketta painamalla. Jos käyttäjä ei valitse vaikeusastetta tai teemaa hakee peli kaikista korteista satunnaisella arvonnalla kuusi paria. Vaikeusasteet määrittävät kuinka monta korttiparia otetaan peliin ja kuinka hankalia kysymyksiä. Teema puolestaan määrittää korttiparien aiheen.

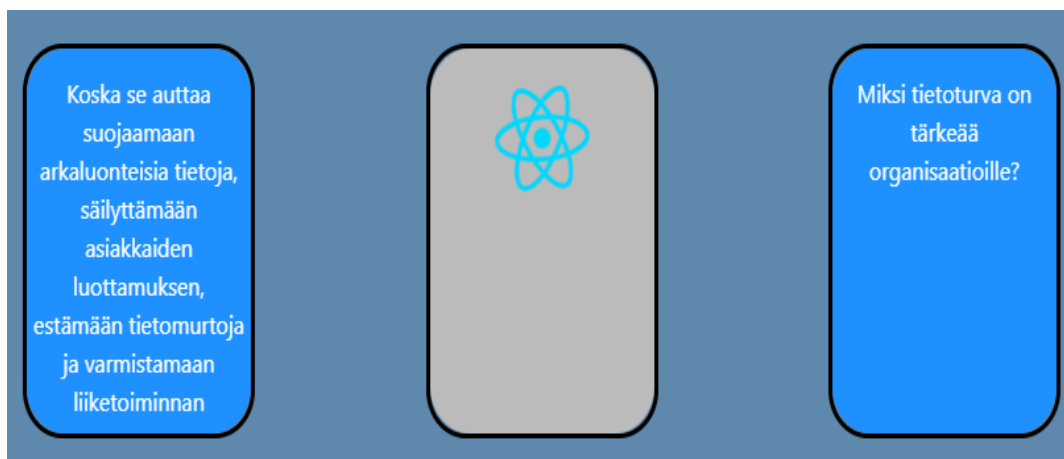


Kuva 5. Sovelluksen etusivu (Kiminki 2024).

”Aloita Peli”-painiketta painamalla hakee sovellus kortit palvelinpuolen kautta tietokannasta ja tulostaa ne käyttäjälle pelattavaksi. Joissain korteissa voi olla pitkäkin vastaus, jolloin laittamalla hiiren kortin tekstin päälle avautuu mahdollisuus vierittää tekstiä kortin sisässä.



Kuva 6. Pelikortit (Kiminki 2024).



Kuva 7. Korttipari (Kiminki 2024).

8.2 Kirjautuminen

”Kirjaudu”- painiketta painaessa avautuu sisään kirjautumisen mahdollistava lomake ja tausta tummenee, jolloin käyttäjä tajuaa kohdistaa. Lomake on hyvin yksinkertainen, jossa kentät käyttäjä nimelle ja salasana. Lomakkeen voi myös sulkea painamalla oikeassa yläkulmassa olevaa raksia. Jos käyttäjätunnus ja salasana ovat oikein tulee käyttäjälle ilmoitus ponnahdusikkunana.



Kuva 8. Sovellukseen kirjautuminen (Kiminki 2024).

8.3 Kirjautunut käyttäjä

Kirjautuneelle käyttäjälle avautuu muuten samankaltainen näkymä, mutta pienillä muutoksilla, jotka ovat ”Hallinta”- ja ”Kirjaudu ulos”-painikkeet. Kirjautunut käyttäjä voi suoraan alkaa pelaamaan käyttäjän omilla korteilla valitsemalla vaikeusasteen ja teeman ja painamalla ”Aloita Peli”-painiketta. Vaikeussateen ja teeman valitseminen ei ole pakollinen, jolloin kone valitsee itse kaikista käyttäjän korteista oletuksena kuusi paria.



Kuva 9. Sovelluksen etusivu kirjautuneella käyttäjällä (Kiminki 2024).

8.4 Hallinta

Hallinta sivustolla avautuu näkymä, jossa käyttäjä voi tarkastella korttipareja. Korttipareista näytetään kysymys kysymykseen vastaus vaikeusaste ja teema. Käyttäjä voi myös lisätä kortteja "Lisää kortteja"- painikkeella, muokata kortteja "Muokkaa"-painikkeella tai poistaa korttiparin "Poista"-painikkeella. Käyttäjä pääsee pelaamaan omilla korteillaan oikeassa yläkulmassa olevalla "Pelaamaan" painikkeella, joka ohjaa käyttäjän takaisin etusivulle.

Korttien hallinta					
Pelaamaan					
Lisää kortteja					
Kysymys	Vastaus	Vaikeusaste	Teema		
Miksi tietoturva on tärkeää organisaatioille?	Koska se auttaa suojaamaan arkaluonteisia tietoja, säilyttämään asiakkaiden luottamuksen, estämään tietomurtoja ja varmistamaan liiketoiminnan jatkuvuuden.	Helppo	Tieturva/kyberturvallisuuden peruskäsitteet	Muokkaa	Poista
Mikä on haittaohjelma?	Se on ohjelmisto, joka on suunniteltu vahingoittamaan tietokonejärjestelmiä, varastamaan tietoja tai suorittamaan muita haitallisia tehtäviä	Helppo	Tieturva/kyberturvallisuuden peruskäsitteet	Muokkaa	Poista
Kuinka voi suojautua haittaohjelmilta?	Pidä käyttöjärjestelmät päivitettyinä ja ohjelmistot päivitettyinä. Ota varmuuskopiot. Suhtaudu sähköpostiliitteisiin ja sähköposteissa esiintyviin linkkeihin terveellä maalaisjärjellä. Käytä virusorjuntaohjelmaa ja palomuuria.	Normaali	Tieturva/kyberturvallisuuden peruskäsitteet	Muokkaa	Poista
Mitä on salaus tietoturvan näkökulmasta?	Se on tietoturvaan liittyvä menetelmä, jossa tieto muunnetaan koodiksi siten, että se on ymmärrettävää vain niille, joilla on oikea salausavain. Tämä suojaaa tietoa, kun se siirtyy verkossa tai tallennetaan laitteisiin.	Vaikea	Tieturva/kyberturvallisuuden peruskäsitteet	Muokkaa	Poista
Miksi tietosuojaa on tärkeää verkkopalveluissa?	Se suojaaa käyttäjien henkilökohtaisia tietoja ja estää niiden väärinkäyttöä.	Helppo	Verkkoturvallisuus	Muokkaa	Poista
Mitä ovat tyypillisiä turvallisuushuolia älylaitteille?	Niitä ovat tietovuodot, haittaohjelmat, etähyökkäykset, laitteen fyysinen varastaminen ja heikko laitteiston tai ohjelmiston suojaus.	Helppo	Älylaitteiden turvallisuus	Muokkaa	Poista

Kuva 10. Korttien hallinta sivu (Lappeteläinen 2024).

8.5 Lisäys ja muokkaus lomake

Lisäys- ja muokkauslomake ovat ulkonäöltään muuten samat, mutta otsikossa ja napeissa vaihtuu teksti. Lisäksi muokkaa lomakkeessa kentät täyttyvät automaattisesti valitun kortin tiedoilla. Käyttäjä voi lisätä/muuttaa korteista melkein kaikkia käyttäjälle näkyviä arvoja, kuten kysymykset, vastaukset, vaikeusasteet ja teemat. Vaikeusasteita ja teemoja on molempia kolme kappaletta. Vaikeusasteina ovat "Helppo", "Normaali" ja "Vaikea". Teemat vaihtoehdot ovat "Tieturva/kyberturvallisuuden peruskäsitteet", "Verkkoturvallisuus" ja "Älylaitteiden turvallisuus".

Lisää korttipari

Kysymys

Kirjoita kysymys tähän

Vastaus

Kirjoita vastaus tähän

Vaikeusaste

Helppo ▾

Teema

Tieturva/kyberturvallisuuden peruskäsitteet ▾

Lisää korttipari

Peruuta

Kuva 11. Korttiparin lisäys lomake (Kiminki 2024).

9 YHTEENVETO

Tieto- ja kyberturvallisuuden osaamisen ylläpitäminen on tärkeää, koska uhat uusiutuvat hetki toisensa jälkeen ja tietomurrot ovat Suomessa kasvussa. Uhkien torjunnassa on tärkeää, että laitteet ja ohjelmat ovat päivitettyjä, ja käytössä on päivitetty virustorjuntaohjelma sekä palomuuuri. Jotta käyttäjä tileihin ei päästäisi niin helposti hyökkäämään suositeltavaa olisi käyttää vahvoja salasanoja ja kaksivaiheista tunnistautumista. Viimeisimmäksi, mutta ei lainkaan vähäisimmäksi kannattaa harkita avaako kaikkien sähköpostiviestien mukana tulleita linkkejä.

Opinnäytetyön tavoitteena oli luoda web-ohjelma, jonka avulla tukea työelämässä olevien henkilöiden tietoturva- ja kyberturvaosaamista. Ohjelman kehitys pysyi aikataulussaan ja, toimeksiantaja ja kehittäjät ovat sovelluksen nykyiseen tilaan tyytyväisiä. Tämänhetkisessä sovelluksessa käyttäjä pysyy pelaamaan oletus tai omilla korteilla joko satunnaisesti valittuna kaikista korteista tai valitun vaikeusasteen ja teeman mukaan, kirjautua sisään, lisätä-, muokata-, poistaa korttipareja.

Ohjelmalle asetetut tavoitteet tuli saavutettua. Ohjelman luomisen aikana ei ilmennyt merkittäviä yllätyksiä. Eniten kehitystyössä aikaa vei päivittynyt navigointi, joka jouduttiin opettelemaan uudelleen ja se, että kirjastosta ei ohjelman alusta löytänyt heti mitä navigoinnin omassa dokumentissa oli mainittu.

Tarpeellisia jatkokehitys ideoita ohjelmalle voisi olla esimerkiksi: käyttäjän rekisteröityminen, suoriutus merkinnän lisääminen pelin läpäisseelle käyttäjälle ja muokattuihin pelikortteihin voisi luoda avaimen millä toiset käyttäjät pääsisivät pelaamaan kohdistetuilla korteilla. Lisäksi löydetyn korttiparin erottaminen muista esim. taustavärillä voisi auttaa tunnistamaan mitkä asiat kuuluvat yhteen. Sivustosta voisi tehdä myös responsiivisen, jolloin ohjelma skaalautuisi paremmin myös puhelimelle ja tabletille.

LÄHTEET

Elinkeinoelämän tutkimuslaitos 2020. Kyberrikollisuus yleistyy ja Suomi kompuroi tietoturvassa – osaamispula jarruttaa kehitystä. Etla: <https://www.etla.fi/ajankohtaista/kyberrikollisuus-yleistyy-ja-suomi-kompuroi-tietoturvassa-osaamispula-jarruttaa-kehitysta/>. Viitattu 12.12.2023.

Euroopan unionin neuvosto 2023. Kyberturvallisuus: käyttäjän manipulointi. Consilium.europa: <https://www.consilium.europa.eu/fi/policies/cybersecurity/cybersecurity-social-engineering/>. Viitattu 12.1.2024.

F-Secure julkaisuaika tuntematon. Mikä on kaksivaiheinen tunnistautuminen (2FA)? F-Secure: <https://www.f-secure.com/fi/articles/what-is-two-factor-authentication>. Viitattu 16.1.2024.

F-Secure julkaisuaika tuntematon. Mikä on palomuuuri? F-Secure: <https://www.f-secure.com/fi/articles/firewall>. Viitattu 16.1.2024.

F-Secure julkaisuaika tuntematon. Mikä on ransomware? F-Secure: <https://www.f-secure.com/fi/articles/what-is-a-ransomware-attack>. Viitattu 3.1.2024.

F-Secure julkaisuaika tuntematon. Mikä on tietokonemato? F-Secure: <https://www.f-secure.com/fi/articles/computer-worm>. Viitattu 11.1.2024.

F-Secure julkaisuaika tuntematon. Mikä on tietokonevirus? F-Secure: <https://www.f-secure.com/fi/articles/what-is-a-computer-virus>. Viitattu 11.1.2024.

F-Secure julkaisuaika tuntematon. Mitä on kyberturvallisuus? F-Secure: <https://www.f-secure.com/fi/articles/what-is-cyber-security>. Viitattu 17.1.2024.

F-Secure julkaisuaika tuntematon. Mitä ovat vakoiluohjelmat? F-Secure: <https://www.f-secure.com/fi/articles/what-is-spyware><https://www.f-secure.com/fi/articles/what-is-a-computer-virus>. Viitattu 12.1.2024.

F-Secure julkaisuaika tuntematon. Tarvitseeko Mac, iPad tai iPhone virustorjuntaa? F-Secure: <https://www.f-secure.com/fi/articles/do-macs-iphones-and-ipads-need-antivirus>. Viitattu 6.1.2024.

F-Secure julkaisuaika tuntematon. Tiesitkö tämän salasanoista? F-Secure: <https://www.f-secure.com/fi/password-generator>. Viitattu 16.1.2024.

Jylhäsalmi, Anu 2018. Tehoa opiskeluun! Oppa: <https://oppa.onedu.fi/zine/31/article-986>. Viitattu 24.1.2024.

Laakso, Matti julkaisuaika tuntematon. Henkilöstöturvallisuus. Tietojesiturvaksi: <https://tietojesiturvaksi.fi/tietoturvasuunnitelma/henkilostoturvallisuus>. Viitattu 7.1.2024.

Lehtiniitty, Markus 2023. Nämä olivat yleisimmät haittaohjelmat marraskuussa – ”hyökkääjät ohittavat perinteiset suojaukset petollisen yksinkertaisin menetelmin”. Mobiili: <https://mobiili.fi/2023/12/13/nama-olivat-yleisimmat-haittaohjelmat-marraskuussa-hyokkaajat-ohittavat-perinteiset-suojaukset-petollisen-yksinkertaisin-menetelmin/>. Viitattu 5.1.2024.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020. Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen! Kyberturvallisuuskeskus: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen>. Viitattu 16.1.2024.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2022. Toimintaohje – Palvelunestohyökkäys. Kyberturvallisuuskeskus: <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf>. Viitattu 10.1.2024.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus julkaisuaika tuntematon. Etusivu. Kyberturvallisuuskeskus: <https://www.kyberturvallisuuskeskus.fi/fi>. Viitattu 17.1.2024.

Lorentsen, M 2023. Mikä on troijalainen ja mitä se voi tehdä? Kotimikro: <https://kotimikro.fi/tietoturva/haittaohjelmat/mika-on-trojalainen-ja-mita-se-voi-tehda>. Viitattu 11.1.2024.

Microsoft julkaisuaika tuntematon. Mitä on käyttöoikeuksien hallinta? Microsoft: <https://www.microsoft.com/fi-fi/security/business/security-101/what-is-access-control>. Viitattu 16.1.2024.

Mäntysalo, Jesse 2022. Tietomurtoja tapahtuu nyt enemmän kuin koskaan, mutta rikollisia ei saada kiinni – viime vuonna 96 prosenttia tapauksista jäi selvittämättä. Yle: <https://yle.fi/a/3-12596198>. Viitattu 12.12.2023.

STT 2020. Yritykset kärsivät verkkorikollisuudesta selvästi useammin Suomessa kuin muualla Euroopassa. Yle: <https://yle.fi/a/3-11695621>. Viitattu 12.12.2023.

Suomi.fi julkaisuaika tuntematon. Tietoturva. Suomi: <https://www.suomi.fi/kansalaiselle/oikeudet-ja-velvollisuudet/turvallisuus-ja-jarjestys/opas/tietoturva>. Viitattu 17.1.2024.

Tauriainen, Antti 2023. Netthuijaukset ovat koko ajan nopeampia ja vaikeampia tunnistaa – näistä ilmiöistä vuosi 2023 muistetaan. Yle: <https://yle.fi/a/74-20065352>. Viitattu 5.1.2024.

Ubuntu julkaisuaika tuntematon. Tarvitsenko virustentorjuntaohjelman? Ubuntu: <https://help.ubuntu.com/stable/ubuntu-help/net-antivirus.html.fi>. Viitattu 6.1.2024.

Yrittäjät julkaisuaika tuntematon. Tietoturva. Yrittäjät: <https://www.yrittajat.fi/tietopankki/turvaayrittamiseen/tietoturva/#paivitykset-ajan-tasalle>. Viitattu 6.1.2024.