VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Panu Dahlqvist

LUOVUTETTU KARJALA SIVUSTON PÄIVITTÄMINEN TIETOTURVAN NÄKÖKULMASTA

Liiketalous
2024

VAASAN AMMATTIKORKEAKOULU
Tietojenkäsittely

TIIVISTELMÄ

Tekijä	Panu Dahlqvist
Opinnäytetyön nimi	Luovutettu Karjala sivuston päivittäminen tietoturvan näkökulmasta
Vuosi	2024
Kieli	suomi
Sivumäärä	42
Ohjaaja	Tero Ulvinen

Tämän opinnäytetyön aiheena oli Luovutettukarjala.fi -verkkosivuston päivittäminen modernimman näköiseksi WordPress -sisällönhallintatyökalua käyttämällä ja lisätä sen turvallisuutta. Sivuston alkuperä on jo 1990-luvun lopulta ja sen visuaaliseen ilmeeseen ei juurikaan ollut puututtu sen jälkeen.

Opinnäytetyössä keskitytään verkkosivun tietoturvaratkaisuihin. Teoriaosuudessa käydään läpi, mitä on tietoturva, mikä on WordPress ja mitkä ovat WordPressin yleisimmät turvallisuusuhat. Projektin toteutusvaiheessa käydään läpi vanhaa sivustoa ja sitä, miten otin huomioon tietoturvaa lisäävät asiat sivustoa päivittäessä.

Projektin lopputuloksena saatiin päivitetty visuaalinen ilme Luovutettu Karjala -sivustolle ja sivustosta tuli käyttäjälle selkeämpi. Sivustosta myös saatiin turvallinen käyttäjälle ja ylläpitäjälle.

Avainsanat tietoturva, WordPress, luovutettukarjala

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Tietojenkäsittely

ABSTRACT

Author	Panu Dahlqvist
Title	Updating the Luovutettu Karjala website from the point of view of information security
Year	2024
Language	Finnish
Pages	42
Name of Supervisor	Tero Ulvinen

The subject of this thesis was updating the Luovutettukarjala.fi website to look more modern by using the WordPress content management tool as well as to enhance its security. The site originated in the late 1990s, and its visual appearance has seen little change since then.

In addition to updating the visual appearance of the website, the thesis focuses on cyber security. The theoretical section discusses what cyber security is, what WordPress is, and what the most common security threats to WordPress are. In the implementation phase of the project, the old site was reviewed, and attention was given to factors that enhance security as part of the update process.

As a result of the project, the Luovutettu Karjala website received an updated visual look, and we made it clearer for users. The site also became secure for both users and administrators.

Keywords Cyber security, WordPress, Luovutettukarjala

SISÄLLYS

KUVA- JA TAULUKKOLUETTELO

1 JOHDANTO

Valitsin Luovutettu Karjala- sivuston päivittämisprojektin opinnäytetyön aiheeksi, koska se oli ajankohtainen toimeksiantajalle ja halusin tutustua tarkemmin WordPressin ominaisuuksiin, sekä miten sillä saadaan luotua turvallinen sivusto. Sivuston päivitykset on luotu ryhmätyönä, mutta olen ollut itse vastuussa tietoturvaan liittyvissä asioissa.

Projektin tarkoituksena on päivittää Luovutettu Karjala-sivuston ulkoasua WordPress -sisällönhallintajärjestelmällä, sekä saada sivustosta käyttäjälle selkeämpi ja turvallinen käyttökokemus. Sivusto sisältää paljon linkkejä ja kuvia, joita oli tarve yhdistää. Projektin tarkoituksena oli myös saada sivustosta turvallinen niin käyttäjälle, kuin ylläpitäjälle.

1.1 Toimeksiantaja

Projektin toimeksiantajan toimii Karjalaliitto ry:n entinen puheenjohtaja Seppo Rapo. Karjalaliitto ry:n ensisijainen tarkoitus on luovutetun Karjalan perinteen ja kulttuurin tallentaminen ja siitä tiedottaminen. Karjalaliiton tehtävänä on karjalaisen perinteen ja kulttuurin siirtäminen tuleville sukupolville sekä karjalaisten ja heidän jälkeläisten yhteenkuuluvuuden lisääminen ja heidän etujensa valvominen.

1.2 Opinnäytetyön tavoite

Projektin tavoitteena oli rakentaa toimeksiantajalle nykyaikaiset sekä responsiiviset verkkosivut WordPress -sisällönhallintajärjestelmää käyttäen. Projekti alkoi marraskuussa 2023 ja tavoitteena oli sivuston valmistuminen kesällä 2024. Tavoitteena oli myös syventyä WordPress -sisällönhallintajärjestelmän työkaluihin ja sen tietoturvaan. Opinnäytetyön tutkimuskysymyksenä on, kuinka kehitetään Luovutettu Karjala verkkosivustosta käyttäjäystävällinen, nykyaikainen ja turvallinen WordPressin avulla.

2 TIETOTURVAN PERUSTEET

Tietoturva tarkoittaa kaikkia niitä toimenpiteitä, joiden avulla suojataan tiedot, järjestelmät ja verkot erilaisilta uhilta, kuten luvattomalta käytöltä, tietovuodoilta, vahingoittamiselta tai muokkaamiselta. Se on välttämätöntä, jotta tiedot pysyvät luottamuksellisina, eheinä ja ovat käytettävissä, kun niitä tarvitaan. (Kyberturvallisuuskeskus 2019.) Tietoturvan perusteiden omaksuminen on tärkeää, jotta niitä pystyy hyödyntämään erilaisissa ympäristöissä.

2.1 Tietoturvan osa-alueet

Tietoturva on laaja käsite ja kattaa monia osa-alueita. Se ei koske pelkästään teknisiä ratkaisuja, kuten palomuureja tai virustorjuntaohjelmia, vaan se sisältää myös hallinnollisia ja käyttäytymiseen liittyviä tekijöitä. Tietoturvan tavoitteena on suojata sekä henkilökohtaiset tiedot sekä organisaatioiden ja yritysten kriittiset tiedot.

2.1.1 Hallinnollinen tietoturva

Hallinnollinen tietoturva tarkoittaa työyhteisön riittävää tietoturvaosaamista. Tällä estetään se, ettei kukaan pääse tuhoamaan tai kopioimaan tietoja oman osaamisen, taloudellisen hyödyn tai pahantahtoisuuden vuoksi. Hallinnollinen tietoturva sisältää käyttäjien koulutusta, tiedottamista ja erilaisten käyttösopimusten tekemistä. (Savelan 2023.) Tätä on myös uusittava ajoittain, koska asian tärkeys unohtuu käyttäjiltä pikkuhiljaa. Käyttäjien on ymmärrettävä, että käyttäjätunnus ja salasana ovat vain omaan käyttöön, eikä niitä tule antaa muiden käyttöön. Näin voidaan aina tarvittaessa tunnistaa, kuka on vastannut tehdyistä toimenpiteistä.

2.1.2 Fyysinen tietoturva

Fyysinen tietoturva tarkoittaa laitteistojen fyysistä lukitsemista niin, ettei asiaan kuulumattomat pääse käsittelemään tietokoneita, tallennustiloja tai servereitä.

Tämä myös tarkoittaa fyysisten verkkojen suojaamista, etteivät ulkopuoliset henkilöt pääse kopioimaan tai lukemaan tietoliikennettä. Fyysisessä tietoturvassa tulee myös varautua erilaisiin luonnonilmiöihin ja tulipaloihin, etteivät ne pääse vahingoittamaan tiedostoja. (Seclion 2021.) Tähän on monenlaisia ratkaisuja, kuten kulunvalvonta, tilojen lukitseminen sekä riittävä paloilmoitinjärjestelmä. Myös tietokoneita ja verkkoja pystytään vartioimaan erilaisilla ohjelmilla ja tiedostoja voidaan salata. On myös tärkeää muistaa varmuuskopiointi ja varmuuskopioiden säilytyksestä on pidettävä huolta.

2.1.3 Laitteistoturvallisuus

Laitteistoturvallisuus tarkoittaa kaikkien yrityksen teknisten laitteiden suojaamista. Varsinkin tietoturvan kannalta erittäin tärkeitä kohteita ovat kannettavat tietokoneet, palvelimet, tulostimet ja matkapuhelimet. Suojamekanismien käyttöönotto tulisi aina kirjata laitteistodokumentaatioon ja henkilöstön olisi hyvä tutustua laitteistoihin ja niiden ohjeisiin. Moni ei myöskään tiedä sitä, ettei hajonneen tietokoneen kovalevylle välttämättä käy mitään koneen hajoamisessa ja se on vielä luettavissa. Tämän kaltaisia asioita on siis tärkeä käydä läpi yrityksissä, etteivät tiedot ja tiedostot joudu vääriin käsiin. Yrityksen on siis tärkeää selvittää, mitä laitteita on yrityksen käytössä ja miten niitä tulisi suojata. Jos yritys tarjoaa kannettavat tietokoneet työtekijöille, heillä ei pitäisi olla mitään tarvetta tuoda omaa konetta työpaikalle, sillä omasta tietokoneesta voi levitä haittaohjelmia yrityksen verkkoon ja se voi olla suuri riski yritykselle. Laitteiden sijainnilla on myös vaikutus tietoturvaan ja laitteistot tulisi aina säilyttää lukittujen ovien takana, eikä niitä kannata sijoittaa poistumisteiden läheisyyteen. Vaikka työntekijöitä olisikin paikalla, voi varkauksia olla vaikea huomata. (Techtarget 2022.)

2.1.4 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus tarkoittaa tietojärjestelmässä käytettävien lisenssien ja ohjelmistojen hallintaa. Tähän sisältyvät sekä työpöytä- että palvelinohjelmistot. Li-

senssien hallinta on tärkeää, sillä puutteet voivat johtaa tietoturvariskeihin. Esimerkiksi virustorjuntaohjelmiston lisenssin vanheneminen saattaa vaikuttaa koko ohjelmiston toimivuuteen. Tällaiset ongelmat voidaan estää tehokkaalla hallinnalla ja seurannalla. Kaikki tärkeät yrityksen ohjelmistoihin liittyvät asiat ovat tärkeää listata tietoturvaperiaatteisiin. Erityisesti varmuuskopiointikäytäntöjen ja tietoturvallisten toimintatapojen ohjeistamiseen kannattaa käyttää aikaa. Henkilöstön on myös tiedettävä, mitä ohjelmistoja heillä on lupa käyttää työkoneillaan. Kaikkein tärkeintä ohjelmistoturvallisuuden kannalta on ohjelmien ja järjestelmien luvattoman käytön estäminen.

Yleisin tapa suojautua luvattomalta käytöltä on käyttäjän todentaminen käyttäjätunnuksella ja salasanalla. Yrityksen tietoturvaohjeistuksiin kannattaa lisätä kohta, jossa kerrotaan turvallisten ja monimutkaisten tunnusten luomisesta. Tietyn tyyppiset salasanat ovat helposti murrettavissa normaalin tietokoneen avulla. Kaikki yrityksen työntekijät eivät välttämättä ole tietoisia tästä, joten ohjeistuksen tekeminen on suotavaa. Ohjelmistoihin saattaa ilmestyä vikoja samalla tavalla kuin laitteisiinkin. Syy voi olla esimerkiksi virheellisissä järjestelmäpäivityksissä. Nämä viat saattavat estää ohjelman päivittäisen käytön. Ylläpito- ja huoltosopimukset ovat hyvä tapa siirtää vastuuta myös muille osapuolille. (Kyberturvallisuuskeskus 2023.)

2.1.5 Tietoaineistoturvallisuus

Tietoaineiston turvallisuus tarkoittaa asiakirjojen, tietueiden ja tiedostojen luottamuksellisuuden vaarantamisen estämistä, sekä estämään tietojen tuhoutumista ja tahatonta muuttumista. Tietoaineiston turvallisuuden kannalta on oleellista myös tallenteiden suojaaminen ja oikeanlainen säilyttäminen. Tähän liittyvät tiedon jatkuva varmistaminen, asianmukainen säilytys ja hävittäminen. Tietoaineistot voidaan kategorisoida myös turvaluokkiin aineiston tärkeyden perusteella: julkiset eli kaikkien työntekijöiden saatavilla olevat tiedot, luottamukselliset eli vain tiedot, jotka halutaan vain jonkun osan työntekijöiden saavan esille, salaiset tiedot, jotka koskevat henkilöiden omia tietoja ja paljastuessaan voi aiheuttaa vaaraa ihmiselle

ja uhkaavat tiedot, jotka sisältävät valtion tietoja. Tämän takia on hyvä luokitella se, mitä kukin käyttäjä voi lukea tai tuhota. (Tietoturvariskienarviointi n.d.)

2.1.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus tarkoittaa keinoja ja laitteita, joilla pyritään suojaamaan dataverkossa liikkuvan tiedon eheys, luottamuksellisuus ja saatavuus. Dataverkoiksi lasketaan tässä tapauksessa kaikki ne tiedonsiirtokanavat, joita yritys käyttää sähköisen informaation liikuttamiseen paikasta toiseen. Yksi tyypillisimmistä yrityksen käytössä olevista tietoliikenneyhteyksistä on Internet. Menetelmät, joilla Internetiä käytetään, vaihtelevat runsaasti. Pienemmät yritykset saattavat turvautua vain matkapuhelimen kautta käytettävään yhteyteen, kun taas suuremmat voivat ostaa kokonaisia valokuituyhteyksiä toimipisteisiinsä. Tietoliikenneratkaisuja hankkiessaan yrityksen kannattaa tutustua tarjontaan ja valita itsellensä sopivin ja tietoturvallisin vaihtoehto. Laitetasolla verkkojen tietoturvaa on parannettavissa esimerkiksi reitittimillä, kytkimillä ja palomuureilla. Näiden laitteiden avulla voidaan rakentaa fyysisesti tai virtuaalisesti eri verkkoja ja rajoittaa niissä liikkuvaa dataa. Mikäli yrityksessä käytetään langattomia tekniikoita, on tietoliikenneturvallisuudesta vastaavan henkilön tiedettävä myös niistä aiheutuvat riskitekijät. (Organisaationtietoturva 2015.)

2.1.7 Henkilöstöturvallisuus

Elinkeinoelämän keskusliiton (2022.) mukaan henkilöstöturvallisuus tarkoittaa yrityksen työntekijöiden työturvallisuuteen ja työhyvinvointiin liittyvien riskien hallintaa. Ihmisten käyttäytymisellä ja toiminnalla eri prosesseissa on merkittävä vaikutus tietoturvan tasoon. Yrityksen työntekijöiden on osattava toimia oikein erilaisissa tilanteissa, kuten epäilyttävien tiedostojen kohdalla. Henkilöstöturvallisuuteen liittyvillä toimenpiteillä pyritään ehkäisemään työntekijöistä ja sidosryhmistä aiheutuvia tietoturvariskejä. Työntekijöiltä vaadittava tietoturvaosaaminen määräytyy heidän työtehtäviensä mukaan. IT-osastolta edellytetään teknistä osaamista, kun taas yritysjohdon tulee hallita hallinnollisen tietoturvan periaatteet.

Kaikkia työntekijöitä yhdistävät yhtenäiset toimintatavat, ja erillisillä tietoturvakoulutuksilla voidaan jakaa parhaita käytäntöjä tasapuolisesti kaikille. Ohjeistamisen ja koulutuksen merkitystä ei saa aliarvioida. On myös tärkeää, että työntekijät noudattavat ohjeita käytännön tilanteissa. Inhimilliset virheet voivat antaa rikollisille mahdollisuuden aiheuttaa yritykselle merkittäviä taloudellisia haittoja. Jos esimerkiksi yritysjohdon työntekijä avaa haittaohjelman sisältävän sähköpostiliitteen, rikolliset voivat saada laajat käyttöoikeudet tietojärjestelmiin ja päästä käsiksi muun muassa liikesalaisuuksiin.

2.1.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan yrityksen päivittäisten toimintojen ja rutiinien suojaamista. Tämä osa-alue kattaa kaikki suojatoimet, jotka liittyvät sekä manuaaliseen että automaattiseen tiedonkäsittelyyn, kuten salasanojen hallinnan ja järjestelmien valvonnan. Käyttöturvallisuutta pidetään toisinaan erillisenä, kahdeksantena tietoturvan osa-alueena sen erityispiirteiden vuoksi. Yritys voi itse päättää, haluaako esimerkiksi salasanojen hallintakäytännöt dokumentoida kahdessa eri osa-alueessa, sekä ohjelmisto- että käyttöturvallisuudessa tai vain toisessa. (ekurssit n.d.)

2.2 Tietoturva pilvipalveluissa

Pilvipalveluiden tietoturva on monipuolinen ja tärkeä osa-alue, koska pilvipalvelut ovat yhä laajemmin käytössä organisaatioissa ja yksityishenkilöillä. Pilvipalveluiden tietoturva kattaa menetelmät ja toimenpiteet, joilla suojataan pilvessä olevat tiedot ja resurssit. Pilvipalveluiden tietoturvassa on huomioitava erityisesti jaetut vastuut, eli mitä palveluntarjoaja ja palvelun käyttäjä vastaavat tietoturvan osalta (Microsoft n.d.b.). WordPressillä tuotetut sivustot usein toimivat eri pilvipalveluiden kautta niiden helpon ylläpidon takia.

2.2.1 Tietoturvan vastuun hallinta

Kriteeristössä esitetyt vaatimukset kohdistuvat useimmissa tapauksissa perustellusti pilvipalveluntarjoajan vastuulle kuuluviin osiin, toisinaan sekä pilvipalveluntarjoajan että asiakkaan vastuulle ja joissain tapauksissa yksinomaan asiakkaan vastuulla oleviin osiin. Joidenkin suojausten toteuttamisessa voi olla perusteltua hyödyntää sekä asiakkaan vastuulla olevan asiakasjärjestelmän, että pilvipalveluntarjoajan vastuulla olevan pilvipalvelualustan toiminnallisuuksia. Kriteeristön tarkoituksenmukainen käyttö edellyttää riittävää osaamista turvallisuuden arvioijalta, pilvipalveluntarjoajalta ja pilvipalvelun asiakkaalta. (Wallenius consulting 2022.)

2.2.2 Fyysinen tietoturva pilvipalveluissa

Pilvipalvelun fyysisellä ympäristöllä on suuri merkitys palvelun turvallisuuteen ja jatkuvuuteen. Hyvin suojattu ja valvottu on vähemmän altis vahingoille, kuin huonosti valvottu. Kulun valvonta ja lukitut konesalit ovat siis välttämättömyys pilvipalvelun tarjoajalle. (Wallenius consulting 2022.)

2.2.3 Käyttöoikeuksien hallinta ja käyttäjätunnistus

Microsoft kertoo sivuillaan (n.d.a.), että käyttöoikeuksien hallinnalla pyritään varmistumaan siitä, että oikeutetulla käyttäjällä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattuun tietoon. Käyttäjä oikeudet tulee rajata vain sellaisiin sovelluksiin verkkoihin ja laitteisiin, joita käyttäjä tarvitsee työssään. Liian laajat käyttöoikeudet ovat tietoturvariski. Käyttäjäoikeuksien hallinnalla ehkäistään tahattomia ja tahallisia riskejä. Käyttäjän tunnistuksessa on tärkeää, että kaikilla on henkilökohtaiset käyttäjätunnukset ja salasanat, jotka luokitellaan riittävän vahvaksi suojattavaan tietoon nähden. Myös ylläpitäjien tunnukset tulisi olla henkilökohtaisia.

2.2.4 Järjestelmäkovennus

Järjestelmäkovennus tarkoittaa järjestelmän asetusten muuttamista siten, että haavoittuvuuspinta-alaa saataisiin pienemmäksi. Järjestelmiin otetaan vain välttämättömimmät laitteet, palvelut ja toiminnot käyttöön ja automaattisille ominaisuuksille annetaan vain ne tiedot ja oikeudet käyttöön, joita ne välttämättä tarvitsevat (Kyberturvallisuuskeskus 2020.).

2.2.5 Tietojen ja laitteistojen turvallinen hävittäminen ja uusiokäyttö

Tietojen ja laitteistojen hävittämisessä tulee huolehtia, että tiedot on oikeasti tuhottu eivätkä ne ole helposti palautettavissa. Laitteiston rikkoutuminen ei myöskään aina vaikuta siihen, saako tiedot vielä käyttöön (Kyberturvallisuuskeskus 2022.).

2.2.6 Tiedon erottelu

Jos samaa laitteistoa käytetään useiden asiakkaiden tiedon käsittelyyn samanaikaisesti, tulee varmistua siitä, että tietojen erottelu on riittävän turvallinen, eikä asiakkaan tietoihin ole pääsyä muilla asiakkailla. Erottelu on toteutettava riittävän luotettavasti käyttämällä joko loogisia, fyysisiä, tai molempia erottelumenetelmiä. (Metropolia 2024.)

2.2.7 Tietojen turvallisuusluokitus TL I, TL II, TL III, TL IV

Luokitustasot määrittelevät, kuinka kriittisiä tiedot ovat ja millaisia suojaustoimenpiteitä niiden käsittely edellyttää.

Taulukko 1 Tietoturvaluokitukset

Luokitus	Tarkoitus	Esimerkki
Turvallisuusluokitus 1	Erittäin salaista tietoa.	Valtion asiakirjoja.
Turvallisuusluokitus 2	Salaista tietoa.	Henkilötietoja ja potilastietoja.

Turvallisuusluokitus 3	Luottamuksellista tietoa.	Yrityksen tietoja.
Turvallisuusluokitus 4	Käyttöä on rajoitettu.	Käyttö tilit eri sovelluksiin.

2.2.8 Tiedon ja palveluiden sijainti

Pilvipalveluissa käsiteltävien tietojen käsittely, säilytys, sekä pilvipalvelun tuottamiseen liittyvät ylläpito- ja muut hallinnointitoimet voivat sijaita eri maissa. Erilaisiin sijainteihin voi liittyä erilaisia riskejä. Maiden väliset sopimukset voivat kuitenkin aiheuttaa riskejä. Sijaintiin liittyviä riskien arvioinnissa suositellaan huomioitavaksi myös se, että yleiset pilvipalveluihin soveltuvat salaustekniset suojaukset eivät tuo merkittävää lisäsuojaa lainsäädäntöjohdannaisia riskejä vastaan (Digi ja väestötietovirasto 2022.).

2.3 Pilvipalvelun toteuttamisen vaihtoehdot

Yksityisen pilven hankkiminen on mahdollista konesalipalveluntarjoajalta. Tällaiseen palveluun kuuluu konesalitila, tietoliikenneyhteydet, fyysiset palvelimet ja levyjärjestelmät (Digi ja väestötietovirasto 2022). Palvelun tarjoajia on markkinoilla paljon ja heillä on erilaisia paketteja. Pilvipalveluja on myös mahdollista luoda itse ja silloin sitä kutsutaan Premise- ratkaisuksi. Pilvipalvelun itse tuottaminen on kuitenkin kallista, koska ylläpitäjän pitää itse huolehtia kulunvalvonnasta ja muusta valvonnasta, sekä kaikki laitteet ovat omakustanteisia.

Pilvipalveluiden käyttämä verkko voi olla joko yksityinen tai julkinen, mutta niiden välistä löytyy myös yhdistelmäratkaisuita, jotka pyrkivät hyödyntämään molempien parhaita puolia. Palvelun tyyppi määräytyy käyttäjän tarpeiden mukaan.

Yksityinen pilvi eli privaattipilvi tarkoittaa yrityksen yksityistä pilviympäristöä, joka sijaitsee joko omassa tai palveluntarjoajan omistamassa konesalissa. Samalla se

tarjoaa poikkeuksellisen korkeaa tietoturvaa sekä häiriötöntä ja verkkoliikenteestä riippumatonta tiedonsiirtokapasiteettia. (Digi ja väestötietovirasto 2022.)

Yhdistelmä pilvi tarkoittaa palvelua, joka yhdistää yksityisen pilven ja julkisen pilven palveluita. Tällainen palvelu voi sijaita yrityksen omassa konesalissa, mutta sitä voidaan täydentää julkisesta pilvestä hankittavilla palveluilla. (Digi ja väestötietovirasto 2022.)

Julkinen pilvi tarkoittaa palvelua, joka on julkisesti tarjolla ja hankittavissa henkilöstä riippumatta. Tällaista palvelua tuotetaan lähes poikkeuksetta palveluntarjoajan konesalista ja sen takia siihen kohdistuu enemmän tietoturva hyökkäyksiä. (Digi ja väestötietovirasto 2022.)

2.4 Pilvipalvelujen palvelumallit

Yleiset pilvipalveluiden palvelumallit ovat IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ja SaaS (Software as a Service). Nämä palvelumallit tarjoavat erilaisia ratkaisuja käyttäjän tarpeisiin, helpottaen tietoteknillisten rakenteiden hallintaa ja parantaen kustannustehokkuutta.

IaaS-palvelussa palveluntuottaja tarjoaa infrastruktuuria palveluna asiakkaalle tyypillisesti niin, että asiakkaan käyttöön tarjotaan web-pohjainen hallintaliittymä, jonka kautta voi itse perustaa tarvittavia palvelimia sekä hallinnoida palvelimen kapasiteettia, verkkoyhteyksiä ja palomuureja. (Google cloud n.d.)

PaaS:ista puhutaan, kun palveluntuottaja tarjoaa palveluna sovellusalustoja, jotka ovat paketoitu helposti käyttöön otettavaan muotoon. Sovellusalustoja tarjotaan yleisesti ottaen ohjelmistokehityksen käyttöön ja tarpeisiin. (Google cloud n.d.). Käytännössä palvelunkäyttäjä voi tilata sopivan alustan, maksaa joustavasti käyttöön perustuen ja siirtää sovelluksensa palveluun.

SaaS-palvelut tarjoavat kokonaisuudessa ohjelmiston palveluna, tästä hyvänä esimerkkinä toimii sähköpostipalvelu. SaaS-palvelussa palveluntuottaja vastaa kokonaisvaltaisesti koko ohjelmistosta. Tyypillisesti SaaS-palveluita käytetään web-selaimen kautta. (Google cloud n.d.)

2.5 Tietoturvallisuutta lisäävät ohjelmat

Tietoturvaa lisäävät ohjelmat ovat ohjelmistoja, joiden tarkoituksena on suojata tietokoneita, mobiililaitteita ja verkkoja erilaisilta uhkilta, kuten haittaohjelmilta, tietomurroilta ja tietojen kalastelulta. Myös on olemassa ohjelmistoja, joiden tarkoituksena ei ole suoranaisesti laitteen turvaaminen, mutta käyttäjä pystyy itse seuraamaan esimerkiksi tietoliikennettä.

2.5.1 Palomuuri

Tietotekniikassa palomuurilla tarkoitetaan ohjelmistoa, joka asennetaan tietokoneelle suojaamaan sitä haitalliselta verkkoliikenteeltä. Palomuuri estää haitallisten ja epäilyttävien IP-osoitteiden pääsyn laitteeseen ja suojelee tietokonetta muun muassa viruksilta. Se valvoo myös laitteesta lähtevää liikennettä ja tarvittaessa estää sen, jos havaitsee mitään epäilyttävää.

Palomuuria voi ajatella suodattimena tietokoneen ja internetin välissä tai vartijana, joka tarkastaa kaikkien yhteyksien luotettavuuden. Kannettavat tietokoneet ja kotiverkot eivät yleensä vaadi ulkoisten laitteiden yhdistämistä, joten tällaisissa tapauksissa palomuuri toimii erityisen hyödyllisenä turvakeinona (F-Secure n.d.b.).

Monissa laitteissa on jo valmiina jonkinlainen palomuuri, joka on kytkettävä päälle, jotta se alkaa suojata verkkoliikennettä. Useissa tietokoneissa palomuuri on oletuksena päällä suojaamassa käyttäjää. Pelkkä palomuuri ei kuitenkaan riitä suojaamaan kaikkia verkkouhkia vastaan, joten sen rinnalla tarvitaan myös virustorjuntaohjelma. Toisin kuin palomuurit, virustorjuntaohjelmat eivät kuitenkaan kuulu automaattisesti kaikkiin laitteisiin.

Palomuurin toiminta perustuu ennalta määriteltyihin sääntöihin, jotka järjestelmänvalvojat ovat asettaneet. Näiden sääntöjen avulla palomuuri tunnistaa haittaohjelmat ja estää niitä pääsemästä laitteelleseen verkon kautta. Jos palomuuri havaitsee jotain epätavallista, se pysäyttää liikenteen automaattisesti.

Palomuureja on monia eri tyyppejä, ja ne on suunniteltu erilaisiin käyttötarkoituksiin. Tietyt palomuurit sopivat parhaiten yksittäisiin laitteisiin, kun taas toiset on kehitetty toimimaan tehokkaasti suurissa verkostoissa.

2.5.2 Kaksivaiheinen tunnistautuminen

Kaksivaiheinen tunnistautuminen tuo ylimääräisen turvatason käyttäjätilillesi kirjautuessa. Pelkän käyttäjätunnuksen ja salasanan lisäksi käyttäjän on varmistettava henkilöllisyytesi toisella tavalla. Tämä toinen tapa voi olla esimerkiksi puhelimeesi saapuva tekstiviestikoodi, henkilökohtainen turvakysymys, sormenjälkitunniste tai mobiilisovellus.

Kaksivaiheinen tunnistautuminen kannattaa ottaa käyttöön mahdollisimman monella tilillä. Kaikki palvelut eivät kuitenkaan vielä tue tätä ominaisuutta, jolloin turvallisuus perustuu vahvojen ja yksilöllisten salasanojen käyttöön. Verkkorikolliset ja huijarit kehittävät jatkuvasti uusia tapoja päästä käsiksi tileihin, joten on tärkeää huolehtia, että vain sinä voit kirjautua omiin tunnuksiisi. (F-Secure n.d.a.)

Kaksivaiheinen tunnistautuminen on itse asiassa helpompaa kuin usein ajatellaan. Se on yksinkertainen, vaivaton ja vieläpä maksuton keino lisätä turvallisuutta verkossa.

Kertakäyttöinen vahvistuskoodi on kertaluontoinen koodi, jota käytetään ylimääräisenä varmistuksena kirjautumisen tai maksutapahtuman yhteydessä. Se on keskeinen osa kaksivaiheista tunnistautumista, ja sen tarkoitus on parantaa tilisi turvallisuutta. Koodin avulla varmistetaan, että kirjautuja ei ole vain joku, joka tietää salasanasi, vaan hänellä on myös pääsy johonkin toiseen tunnistautumiskeinoon, esimerkiksi puhelimeesi.

Kasvojentunnistus on tunnistautumismenetelmä, jossa henkilön kasvot toimivat salasanan korvikkeena tai lisätunnisteena, erityisesti mobiililaitteissa ja joissain tietokoneissa. Teknologian avulla käyttäjän kasvot skannataan ja analysoidaan, ja tämä data verrataan laitteen muistiin tallennettuihin kasvojen piirteisiin. Kasvojentunnistusta käytetään sekä kirjautumiseen että lisäturvakeinona, esimerkiksi sovellusten avaamiseen tai maksujen hyväksymiseen.

Sormenjälkitunnistus on biometrinen tunnistautumismenetelmä, jossa käyttäjä tunnistetaan sormenjälkensä avulla. Tämä menetelmä on suosittu älypuhelimissa, tietokoneissa ja tietyissä turvallisissa käyttöympäristöissä, sillä se on nopea ja vaivaton tapa todentaa henkilöllisyys.

QR-koodi on tunnistautumismenetelmä, jossa käyttäjä käyttää QR-koodia henkilöllisyytensä varmistamiseen. QR-koodit ovat kaksidimensionaalisia viivakoodeja, jotka voidaan skannata kameralla, ja ne sisältävät tietoa, jota käytetään turvalliseen kirjautumiseen tai maksutapahtumiin. Tunnistautumisessa QR-koodit tarjoavat nopean, turvallisen ja kätevän vaihtoehdon erityisesti mobiililaitteilla.

Vaikka kaksivaiheinen tunnistautuminen lisää suojaa käyttäjätileille ja vaikeuttaa murtautumista, verkkorikolliset ja hakkerit voivat silti kiertää sen. Joissakin tapauksissa tämä tapahtuu huijaamalla käyttäjää, kun taas toisissa hyödynnetään palveluiden heikkouksia. (Winnova 2024.)

2.5.3 VPN

Virtual private network eli virtuaalinen erillisverkko on tehokas työkalu yksityisyyden suojaamiseksi netissä. VPN on palvelu, joka varmistaa internetyhteytesi turvallisuuden ja pitää tietosi yksityisinä. Se tekee tämän luomalla salatun tunnelin, jonka kautta tiedot kulkevat, piilottaen samalla IP-osoitteesi ja suojaten henkilöllisyytesi. Näin voit käyttää esimerkiksi julkisia Wi-Fi-verkkoja turvallisemmin (NordVPN n.d.).

Kun käytät VPN:ää, et muodosta yhteyttä suoraan internetiin, vaan liikenteesi kulkee ensin VPN-palvelimen kautta. Tällöin verkkopalvelut näkevät ainoastaan VPN-palvelimen IP-osoitteen, eivät omaasi. Tämä auttaa pitämään todellisen sijaintisi salassa, jolloin esimerkiksi internetpalveluntarjoajasi tai vierailemasi verkkosivustot eivät pysty seuraamaan, miten käytät nettiä (F-Secure n.d.c.).

2.5.4 Wireshark

Wireshark kertoo sivuillaan, että se on suosittu avoimen lähdekoodin työkalu verkkoliikenteen analysointiin ja diagnosointiin. Sen tarkoituksena ei ole suojata tietokonetta, mutta sen avulla pystyy analysoimaan tietoliikennettä. Wireshark on erityisen suosittu IT-ammattilaisten, kuten järjestelmänvalvojien, tietoturva-asiantuntijoiden ja verkkoinsinöörien keskuudessa, koska se auttaa tunnistamaan verkon ongelmia, havaitsemaan mahdollisia tietoturvauhkia ja selvittämään suorituskykyongelmia.

Wireshark kerää ja näyttää kaiken sieppaamansa verkkoliikenteen, kuten lähettäjä- ja vastaanottajaosoitteet, liikenteen protokollat ja tiedonsiirron sisällön. Koska ohjelma näyttää verkkoliikenteen hyvin tarkasti, sitä voi käyttää myös väärin, ja siksi sen käyttö edellyttää lupaa verkonvalvojalta tai organisaatiolta, jonka verkkoa analysoidaan (Wireshark n.d.).

Wireshark on tehokas työkalu verkkoliikenteen syväanalyysiin, ja se soveltuu sekä organisaatioiden että yksittäisten käyttäjien käyttöön erityisesti vianmäärityksessä ja tietoturvan parantamisessa.

3 WordPress

3.1 Mikä on WordPress?

WordPress on avoimen lähdekoodin blogityökalu, julkaisualusta ja sisällönhallintajärjestelmä, joka on vakiinnuttanut asemansa maailman suosituimpana CMS-järjestelmänä (Content Management System). Se hallitsee noin 60 % kaikista CMS-pohjaisista verkkosivustoista ja kattaa noin 28 % kaikista internetin sivustoista. Alun perin blogialustaksi kehitetty WordPress on vuosien varrella kasvanut monipuoliseksi ja joustavaksi alustaksi, joka soveltuu kaikenlaisten verkkosivujen rakentamiseen ja ylläpitoon. (Fissiomedia 2023.)

WordPressin vahvuuksia ovat sen laajennettavuus ja avoin lähdekoodi, mikä mahdollistaa jatkuvan kehityksen ja sivuston omistajan riippumattomuuden yksittäisestä palveluntarjoajasta. Monipuoliset ominaisuudet ja laaja valikoima laajennuksia tekevät siitä erinomaisen vaihtoehdon niin pienille blogeille kuin suurille, runsaasti liikennettä keräävälle verkkosivustoille. Lisäksi WordPressin suorituskyky on optimoitavissa riittävillä palvelinresursseilla ja asianmukaisilla toteutuksilla, mikä takaa luotettavuuden myös suurten kävijäpiikkien aikana. (Zoner 2021.)

Alustan jatkuvat päivitykset ja kehitykset ovat muovanneet WordPressistä monipuolisen ja tehokkaan työkalun, joka on kasvanut yksinkertaisesta blogityökalusta täysiveriseksi sisällönhallintajärjestelmäksi, tarjoten kattavat ratkaisut erilaisten verkkosivustojen tarpeisiin.

3.2 WordPressin turvallisuus

WordPressin turvallisuus voidaan varmistaa monella eri tavalla verkko-, palvelin- ja sovellustasolla. Sovellustasolla, eli itse WordPress-järjestelmässä, erilaiset tietoturvalisäosat ja verkkosovelluspalomuurit ovat keskeisiä suojaamassa sivustoa verkkohyökkäyksiltä ja haavoittuvuuksilta.

Turvallisuuslisäosat, kuten Wordfence ja Sucuri Security, tarjoavat tehokkaita toimintoja, kuten haittaohjelmien skannausta, kirjautumisyritysten seurantaa sekä reaaliaikaista uhkien tunnistusta. Näiden työkalujen avulla on mahdollista havaita ja käsitellä tietoturvaongelmia nopeasti. Lisäksi ne tarjoavat ratkaisuja käyttäjien tunnistautumisen ja pääsynhallinnan vahvistamiseen, mikä lisää sivuston suojaa. (Fissiomedia 2023.)

Verkkosovelluspalomuurit kuten Cloudflare, toimivat suojamuurina sivuston ja potentiaalisten hyökkääjien välillä. Ne suodattavat saapuvan liikenteen ja estävät haitalliset pyynnöt, sekä tunnetut uhat ennen kuin ne voivat vahingoittaa sivustoa. Yhdessä turvallisuuslisäosien kanssa nämä palomuurit tarjoavat monikerroksisen suojan, joka parantaa WordPress-sivuston kokonaisvaltaista tietoturvaa ja tuo mielenrauhaa sekä sivuston omistajille että käyttäjille.

3.3 Tyypilliset turvallisuusuhat

WordPressin ydin on suunniteltu erittäin turvalliseksi, ja sen turvallisuudesta pidetään jatkuvasti huolta. Kuitenkin tavallisimmat uhat sivustoille johtuvat vanhentuneista teemoista ja lisäosista sekä heikoista käyttäjätunnuksista ja salasanoista. Myös palvelimen haavoittuvuudet voivat aiheuttaa ongelmia, etenkin jaetussa hosting-ympäristössä, jossa sivusto voidaan kaapata toisen sivuston kautta, jos tämä sivusto on murrettu. (Fissiomedia 2023.)

Yksi yleisimmistä hyökkäyksistä on Brute force -hyökkäys, jossa hyökkääjät yrittävät arvata kirjautumistunnuksia kokeilemalla systemaattisesti erilaisia käyttäjänimiä ja salasanoja. Tämän uhan torjumiseksi on tärkeää käyttää vahvoja, uniikkeja salasanoja ja rajoittaa kirjautumisyritysten määrää. (NordVPN 2022.)

Vanhentuneet ohjelmistot ovat toinen suuri riski. WordPressin ydin, teemat ja lisäosat voivat sisältää tietoturva-aukkoja, jos niitä ei päivitetä säännöllisesti. Tämä tekee sivustosta haavoittuvaisen hyökkäyksille, joissa hakkerit voivat käyttää hy-

väkseen näitä tunnettuja heikkouksia päästäkseen luvatta sisään tai manipuloidakseen sivuston sisältöä. Siksi on ehdottoman tärkeää pitää sekä WordPress-asennus että siihen liittyvät komponentit aina ajan tasalla.

Haittaohjelmat muodostavat jatkuvan uhan WordPress-sivustoille. Näitä voi päästä sivustolle haavoittuvien lisäosien, teemojen tai huonosti suojattujen lomakkeiden kautta, mikä voi johtaa tietojen varastamiseen, sivuston turmeltumiseen tai luvattomaan pääsyyn (Fissiomedia 2023.). Haittaohjelmien riskiä voidaan vähentää käyttämällä tietoturvalisäosia, jotka skannaavat ja poistavat haitallista koodia, auttaen pitämään sivuston turvallisena.

Kolmannen osapuolen lisäosat ja teemat ovat myös riskitekijöitä. Kaikki kehittäjät eivät noudata tiukkoja tietoturvakäytäntöjä, ja huonosti koodatut laajennukset voivat altistaa sivuston vakaville tietoturvaongelmille. Tämän välttämiseksi on tärkeää valita lisäosat ja teemat luotettavista lähteistä ja varmistaa, että ne päivitetään säännöllisesti, jotta tietoturva-aukot pysyvät tukittuna. (Fissiomedia 2023.)

4 Luovutettu karjala sivuston tietoturvan parantaminen

Luovutettu Karjala verkkosivu on alun perin Seppo Rapon luoma sivusto, joka käsittelee karjalan historiaa. Hän loi ensimmäisen version Luovutettu Karjala sivustosta jo 1990-luvun lopussa ja on päivittänyt sivuston ilmettä aina tarpeen vaatiessa. Sivusto ja Luovutettu Karjala aiheena on Rapolle tärkeä, koska hänen sukunsa on sieltä kotoisin ja hän on myös toiminut Karjala Liitto ry:ssä monissa luottamus toimissa vuosia. (Luovutettu Karjala 2022.)

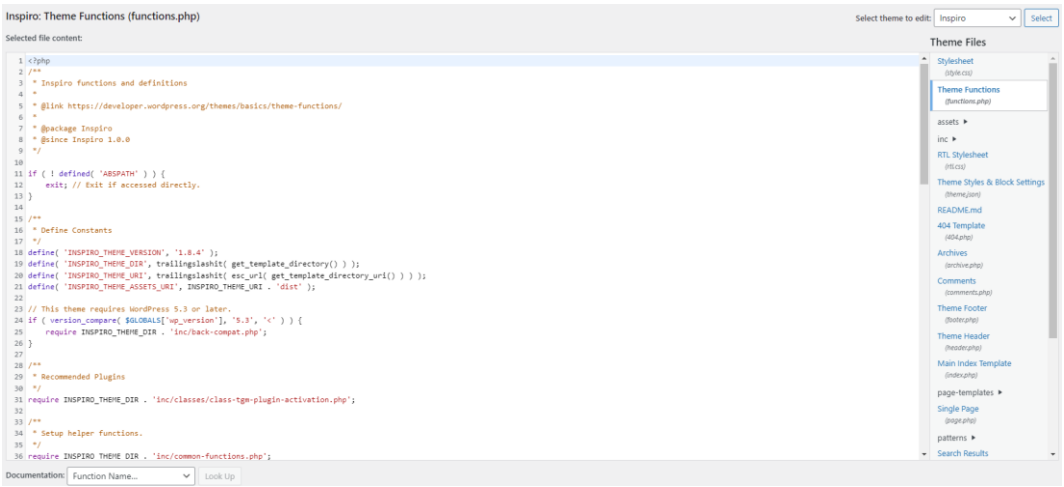
Sivusto kuitenkin alkaa jo näyttämään vanhanaikaiselta ja Rapo pyysikin Vaasan ammattikorkeakoululta apua sivuston päivittämisessä. Ensimmäisessä palaverissa kävimme läpi minkälaista ilmettä hän sivustolle halusi ja mitkä asiat pitäisi muuttaa. Rapolla on myös toinen sivusto nimeltä lumivaara.fi ja hän oli antanut sivuston päivittämisen aikaisemmille vuosikurssin opiskelijoille ja oli tyytyväinen sivuston ulkonäköön, joten meidän tavoitteemme oli lähteä tekemään samankaltaiselta näyttävää sivustoa unohtamatta karjalalle tuttuja värejä ja logoja. Ensimmäisessä palaverissa tuli myös ilmi, että alkuperäinen sivusto oli aikaisemmin kaapattu ja tästä aiheutui paljon pään vaivaa Rapolle. Sivustosta tulisikin tehdä niin turvallinen, ettei se joutuisi helposti uudestaan hakkereiden hallintaan.

Kuva 1. Sivuston alkuperäinen ulkonäkö

4.1 Projektin alku

Projektin alussa loimme toisen WordPress -sivuston, johon siirsimme nykyisessä tilassa olevan sivuston sisällön, jotta voisimme tarkastella ja muokata sivustoa vaikuttamatta alkuperäisen sivuston toimintaan.

Tärkeimmät tiedostot siirrettyämme, aloitimme luotettavan teeman valinnalla. Teeman valinta kriteereinä oli luotettavuus, ilmainen käyttö sekä helppo muokattavuus. Teemoja oli kuitenkin paljon, mutta suurin osa niistä oli maksumuurin takana, tai niiden muokkaaminen ei ollut mahdollista, joten päädyimme käyttämän samaa teemaa, kuin lumivaara.fi sivustossa oli käytetty. Teeman nimi on Inspiro ja sen tekijöinä toimii luotettava WPZOOM-palvelu, joka tuottaa WordPress sivustolle paljon teemoja ja lisäosia, jotka ovat ilmaisessa käytössä, mutta niissäkin on osa ominaisuuksista maksumuurin takana. Luotettavuutta myös lisää avoin lähdekoodi, jota tarkastelemalla käyttäjä pystyy tarkistamaan, ettei siellä ole piilotettuina viruksia tai muita haittaohjelmia.



Kuva 2. Teeman lähdekoodi

Teeman valinnan jälkeen jatkoimme tiedon ja kuvien siirtämistä sivustolle, joka vei paljon aikaa, koska jokaisessa pitäjässä oli oma kartta ja vaakuna, jotka pitivät manuaalisesti tuoda oikeaan paikkaan ja varmistaa, ettei sivustolle tule virheellisiä kuvatiedostoja.

4.2 Tietoturvaan syventyminen

Tiedostojen siirron jälkeen jatkoimme projektia lisäämällä suosittuja ja turvallisia laajennuksia sivustolle, jotka tekevät sivustosta turvallisemman ja samalla miellyttävämmän käyttökokemuksen sivuston käyttäjälle.

4.2.1 Lisäosat

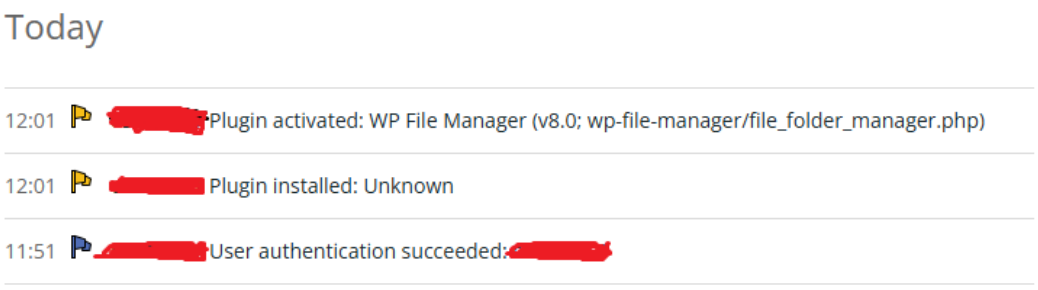
Ensimmäisenä lisäsimme Easy HTTPS (SSL) Redirection nimisen lisäosan, jonka tarkoituksena on muuttaa sivuston osoite HTTPS-muotoon. Tämä salaa liikenteen käyttäjänselaimen ja palvelimen välillä parantaen tietoturvaa (Tips and Tricks HQ n.d.).

Tämän jälkeen lisäsimme Limit login attempts reloaded lisäosan, jonka tarkoituksena on estää hyökkäyksiä, jotka arvaavat käyttäjätunnus- ja salasanapareja. Lisä-

osa rajoittaa sivustolle kirjautumisyrityksiä, jotta hakkerit eivät saisi montaa yritystä kirjautumiseen. Lisäosan avulla pystyy myös estämään tietystä IP-osoitteesta kirjautumisen, tai sallia vain kirjautumisen tietystä IP-osoitteesta (Limit login attempts n.d.).

Kuva 3. Kirjautumisyritysten seuranta

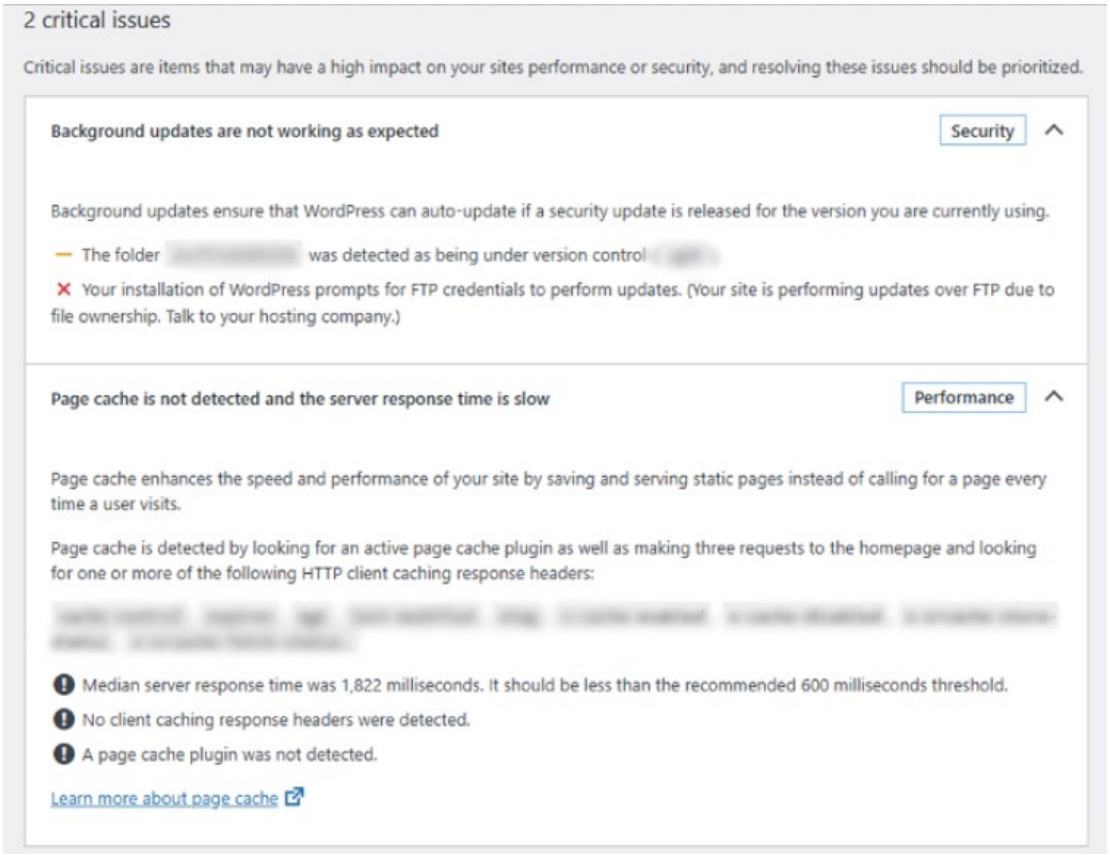
Sivuston lisäosien turvallisuuden tarkastamiseen käytimme Sucuri security ohjelmaa, jonka tarkoituksena on tarkastaa lisäosien turvallisuus, haittaohjelmien tarkistus sekä lisäosa myös lähettää ilmoituksen, kun se huomaa sivustolla haitallista toimintaa. Sucuri myös pitää huolta kirjautumisyrityksistä sekä piilottaa WordPressin versionumeron.



Kuva 4. Sucurin seurantapaneeli

Sivustolle on lisäksi asennettu muita lisäosia, kuten WP Coder ja Advanced iFrame, jotka mahdollistavat sivuston helppokäyttöisemmän muokkauksen ja parantavat sen käyttäjäystävällisyyttä. Näiden lisäosien avulla on myös mahdollista muokata lisäosien ominaisuuksia, jotka ovat muutoin maksumuurin takana, kuten sivuston yläosassa sijaitsevien alasvetovalikoiden värejä ja tekstin fonttia.

WordPressillä on kuitenkin käytössään jo valmiiksi tietoturvaa lisääviä ominaisuuksia, jotka kertovat sivuston ylläpitäjälle tärkeää tietoa, kuka sivustoa on muokannut ja mitä he ovat tehneet, sekä kertoo myös, onko sivuston suorituskyvyssä ongelmia (Wordpress n.d.).



Kuva 5. WordPressin hallintapaneeli

Tärkeää on myös muistaa poistaa käyttämättömät teemat ja lisäosat sivustolta, koska jokainen niistä lisää tietoturvariskiä ja niistä voi löytyä aukkoja, joita hakkerit hyödyntävät.

4.2.2 Tiedostojen ja hakemistojen suojaaminen

WordPress-sivuston tiedostojen suojaaminen on tärkeää, koska tiedostot sisältävät keskeisiä tietoja ja toiminnallisuuksia, jotka liittyvät sivuston käyttöön ja hallintaan.

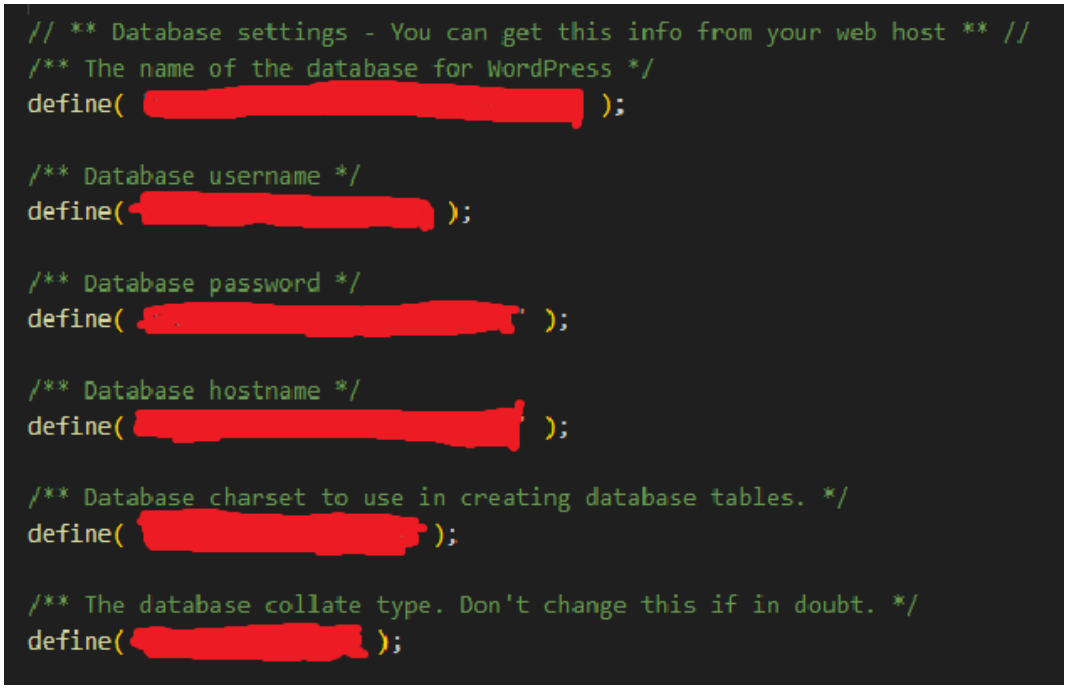
Käyttöoikeuksien määrittämisellä on suuri merkitys sivuston turvallisuuden kannalta, mutta sivustollamme ei ole muita käyttäjiä, kuin sivuston ylläpitäjät, joten kaikilla on ylläpitäjien oikeudet käytössään. Tätä olisi kuitenkin tärkeää rajoittaa, jos sivustolla olisi enemmän käyttäjiä. Yleisiä käyttöoikeuksien rajoituksia voisi olla esimerkiksi pääsyn estäminen eri hakemistoihin sekä htaccess ja wp-config tiedostoihin, jotka sisältävät kaiken tarvittavan sivuston perusasetusten hallintaan.

4.2.3 Tietokantojen suojaaminen

WordPress-sivuston tietokannan suojaaminen on kriittinen osa sivuston tietoturvaa, sillä tietokanta sisältää kaiken sisällön, käyttäjätiedot ja asetukset. Oletuksena WordPress luo tietokannat käyttäen wp- etuliitettä ja tämä on hyökkääjien tiedossa ja sen vaihtaminen parantaa turvaa SQL- injektiohyökkäyksiä vastaan (WPservices 2024.).

4.2.4 Wp-config- tiedosto

wp-config- tiedosto on WordPressin keskeinen konfiguraatiotiedosto, joka sisältää kaikki tarvittavat asetukset, jotta WordPress-sivusto toimii oikein. Se sijaitsee WordPress-asennuksen juurihakemistossa, ja sen kautta määritellään tärkeitä tietoja, kuten tietokantayhteydet ja turvallisuusasetukset. Tämän tiedoston tärkeyden takia sen luku- ja kirjoitusoikeudet on vain sivuston pääkäyttäjillä. Wp-config tiedosto sijaitsee julkisessa kansiossa oletuksena, joka tarkoittaa kansioon pääsyä oikealla linkillä. Tiedoston voi kuitenkin laittaa hakemistossa yhden kansion juureen päin ja tämä estää sisältöön käsiksi pääsemisen selaimen kautta.



Kuva 6. Wp-config- tiedoston sisältöä

4.2.5 Käyttäjätilien hallinta

Käyttäjätilien hallinta on tärkeä osa tietoturvaa ja jokaisella käyttäjälle pitäisi olla vain heidän tehtäviinsä sopivat oikeudet. Oikeanlaiset oikeudet estävät tiettyjä käyttäjiä lukemasta tai muokkaamasta tiedostoja ja tietoturvallisuusriskejä (WPopas n.d.). käyttäjillä olisi myös tärkeää olla hyvä ja yksilöity käyttäjätunnus ja vahva salasana sen tueksi. Salasanaa olisi myös hyvä päivittää muutaman kuukauden välein.

4.2.6 Lisäosien päivittäminen

Teemojen ja lisäosien päivittäminen on myös tärkeää, sillä päivitysten myötä lisäosista ja teemoista tulee parempia ja turvallisempia, sekä niihin voi tulla uusia ominaisuuksia, jotka helpottavat niiden käyttöä. Teemoissa ja lisäosissa kannattaakin käyttää automaattista päivitystä.

4.2.7 Palvelin suojaus

Palveluntarjoajamme on luotettava OVHcloud niminen yritys. OVHcloud on ranskalainen pilvipalvelujen tarjoaja, joka tarjoaa yrityksille ja yksityishenkilöille laajan valikoiman palveluja, kuten virtuaalipalvelimia, tietovarastoja, verkkosivustojen isännöintiä ja muita pilvipohjaisia infrastruktuuriratkaisuja. OVHcloud on yksi Euroopan suurimmista pilvipalveluiden tarjoajista, ja se tunnetaan erityisesti keskittymisestään tietoturvaan, suorituskykyyn ja ympäristöystävällisiin käytäntöihin. (OVHCloud 2024.)

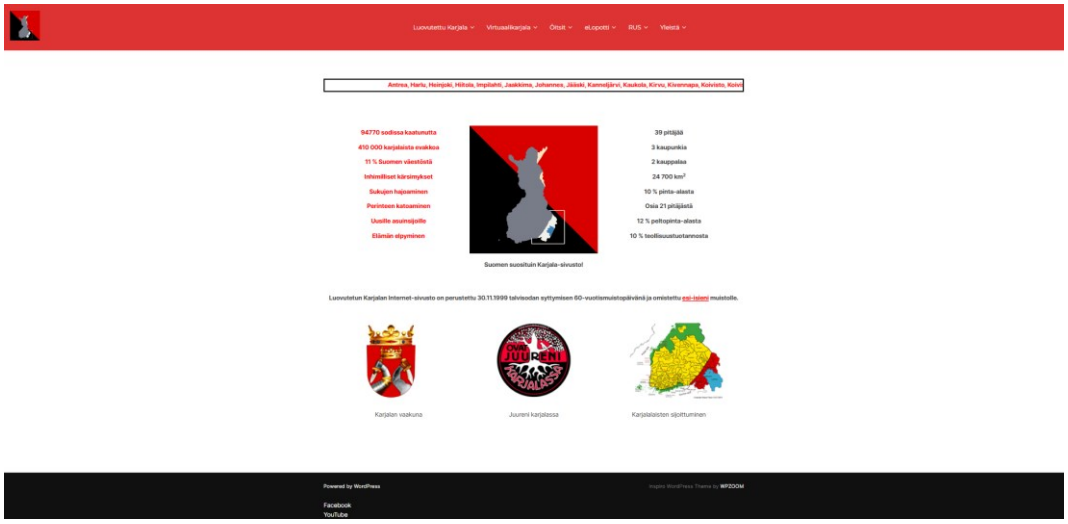
OVHcloud on tunnettu infrastruktuurinsa suorituskyvystä ja tietoturvasta. Heillä on myös oma tietokeskusverkosto, joka takaa hyvän hallinnan ja valvonnan tietojen säilyttämisessä sekä korkeatasoiset tietoturvakäytännöt, kuten DDoS-suojaus. OVHcloud myös pitää huolta verkkosivujen varmuuskopioinneista.

4.2.8 Kirjautumistietojen seuranta

Lokiseuranta auttaa havaitsemaan ja ehkäisemään mahdollisia uhkia ennen kuin ne muuttuvat ongelmiksi. Se tarjoaa arvokasta tietoa sivuston toiminnasta, käyttövalvonnasta ja turvallisuudesta, ja erityisesti sivustoilla, joissa on useita käyttäjiä tai herkkiä tietoja, se on tärkeä osa WordPressin tietoturvaa (Sucuri n.d.). Säännöllinen lokitietojen tarkastelu auttaa havaitsemaan sivuston toimintaan liittyvät poikkeavuudet. Erityisesti suuremmilla sivustoilla on hyödyllistä käydä lokitiedot läpi esimerkiksi kerran viikossa tai kuukaudessa. Meidän tapauksessamme lokitietojen seurantaa suoritetaan Sucuri nimisellä lisäosalla, joka kertoo uusista osoitteista tehdyistä kirjautumisyrityksistä.

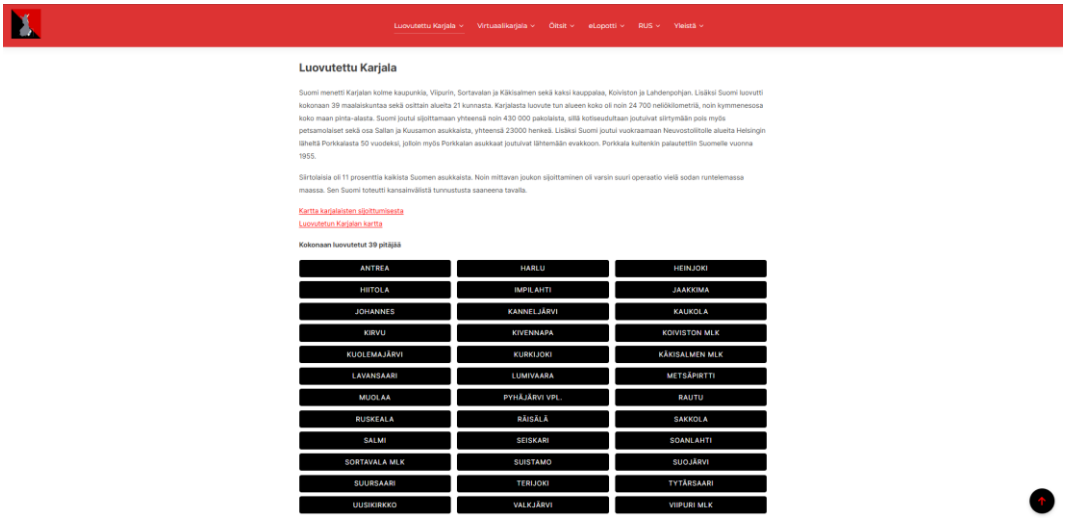
5 LOPPUTULOS

Lopputuloksena saatiin tuotettua toimivat ja modernin näköiset sivut, joita on helppo käyttää.



Kuva 7. Sivuston päivitetty ulkonäkö

Sivuston ulkonäkö on aika yksinkertaistettu ja navigointivalikosta pääsee tutkimaan sivuston sisältöä tarkemmin. Sivuston teemana on myös pidetty tutut värit vanhoilta sivuilta toimeksiantajan pyynnöstä. Myös Karjalan vaakuna, juureni karjalassa ja karjalan kartta on pidetty etusivulla.



Kuva 8. Pitäjät sivun päivitetyt linkit

Pitäjät -sivu koki suurimman muutoksen. Sieltä löytyy nyt painike jokaiseen pitäjään ja painike avaa sivulle pitäjän vaakunan, tietoa pitäjästä, linkin kuvagalleriaan sekä kartan.

Kuva 9. Pitäjät linkkien sisältö

Näiden alta löytyy vielä Karjala-lehden pitäjäliitteet, jotka ovat liitteitä vanhoista Karjala-lehdistä.

Öitsit -kohdasta löytyy tietopeli. Peli on tuotu suoraan vanhalta sivustolta ja sen toiminta jää hieman keskeneräiseksi. Tietopeli toimii muuten hyvin, mutta jokaiseen kysymys- ja vastaussarakkeeseen käyttäjä pystyy itse kirjoittamaan, sekä manipuloimaan vastauksia

Kuva 10. Karjala-aiheinen tietopeli

RUS-valikosta löytää karjalan historiaa venäjäksi.

Toteutetut tietoturvatoimet ja lisäosien käyttöönotto olivat keskeisiä sivuston turvallisuuden, vakauden ja käyttäjäkokemuksen parantamisessa. Näkyvin muutos käyttäjälle on, että kaikki käyttäjäliikenne on suojattu SSL-salauksella ja mahdollisilta hyökkäyksiltä suojataan monitasoisin menetelmin. Käyttäjän näkökulmasta sivusto toimii turvallisesti ja luotettavasti.

Sivuston ylläpitäjän kannalta tietoturva ja hallittavuus ovat ensiarvoisen tärkeitä. Automatisoitu lokitietojen seuranta ja käyttäjätilien hallinta antavat ylläpitäjille mahdollisuuden hallita ja valvoa sivustoa tehokkaasti ilman merkittävää manuaalista työtä. Vain ylläpitäjillä pääsy on tärkeimpiin tiedostoihin, kuten wp-config-tiedostoon, mikä vähentää riskejä, jos lisäkäyttäjiä lisätään.

Kokonaisuutena, nämä ratkaisut eivät vain turvaa sivustoa, vaan tekevät siitä käyttäjäystävällisen ja helppokäyttöisen sekä vierailijoille että ylläpitäjille.

6 JOHTOPÄÄTÖKSET

Projektin tavoitteena oli päivittää ja rakentaa toimeksiantajille nykyaikaiset, responsiiviset sekä turvalliset verkkosivut WordPress-sisällönhallintajärjestelmällä. Projektin toimeksiantaja halusi saada vanhalle LuovutettuKarjala.fi-sivustolle modernimman ja uudemman ilmeen, joka kuitenkin kunnioittaisi toimeksiantajan toiveita ja Luovutetun Karjalan muistoa. Opinnäytetyön tutkimuskysymyksenä oli, kuinka kehittää Luovutettu Karjala verkkosivustosta nykyaikainen ja turvallinen käyttäjälle ja ylläpitäjälle.

Vanha LuovutettuKarjala-sivusto oli ilmeeltään vanhanaikainen ja yksinkertainen, sekä sen käytettävyys oli huonoa linkkien paljouden takia. Toimeksiantajan asettamana ehtona oli, että kaikki vanhan sivuston sisältö siirretään uuteen sivustoon, ja tämä tavoite saavutettiin. Uudelle sivustolle saatiin siirrettyä kaikki vanha tieto, samalla muokaten sen visuaalista ilmettä. Sivustolle luotiin moderni ilme, nykyaikainen rakenne, ja responsiivisuutta, mikä mahdollisti vaivattoman selailun mobiililaitteilla. Sivuston tietoturvallisuus myös parani huomattavasti.

6.1 Pohdinta

Projektia tehdessä suurin ongelma oli tiedon siirtäminen toiselle palvelimelle. Vanhalla sivustolla oli paljon tietoa eri pitäjistä, mutta esimerkiksi kuvien linkit olivat toisella sivulla ja niiden yhdistäminen vei paljon aikaa. Projekti eteni välillä aika hitaasti, mutta lopputulokseen olen tyytyväinen.

Ennen projektin alkua olin tehnyt harjoitus mielessä yhdet sivut WordPressillä, joten sen käyttäminen oli jokseenkin tuttua. Oma mielenkiintoni kuitenkin on tietoturvan puolella, ja sen takia halusin opinnäytetyössäni tuoda esille. Oli mielenkiintoista tutustua tähän aiheeseen ja päästä hyödyntämään oppimaani.

WordPress sivuston tietoturvan lisääminen oli vaivatonta, koska tietoa aiheesta löytyi paljon ja eri lisäosista pystyi lukemaan käyttäjien arvioita. Ymmärsin myös,

miten vaivatonta sivuston kaataminen tai haltuun ottaminen on osaavalle hakkerille, jos tietoturvalle ei ole juurikaan tehty mitään. Esimerkiksi WordPressin versionumeron piilottaminen tuntui aluksi turhalta, mutta eri foorumeita selattuani ja nähtyäni erilaisia aukkoja eri versioissa kaikkien nähtävillä, tajusin, kuinka tärkeää sen piilottaminen on.

LÄHTEET

Digi- ja väestötietovirasto 2022. Tietosuoja pilvipalveluissa. Viitattu 11.9.2024. https://dvv.fi/documents/16079645/110183105/Tietosuoja+pilvipalveluissa+-+VAHTI+hyv%C3%A4t+k%C3%A4yt%C3%A4nn%C3%B6t+-tukimateriaali.pdf/e7d9e55f-eaa5-ea6a-685d-756c5992a0e3/Tietosuoja+pilvipalveluissa+-+VAHTI+hyv%C3%A4t+k%C3%A4yt%C3%A4nn%C3%B6t+-tukimateriaali.pdf?t=1667993950041

Ekurssit (n.d.) Käyttöturvallisuus. Viitattu 11.9.2024. http://www.ekurssit.net/kurssit/tietoturvallisuus/kayttoturvallisuus.php

F-Secure (n.d.a.) Mikä on kaksivaiheinen tunnistautuminen (2FA)? Viitattu 6.11.2024. https://www.f-secure.com/fi/articles/what-is-two-factor-authentication

F-Secure (n.d.b.) Mikä on palomuuri? Viitattu 6.11.2024. https://www.f-secure.com/fi/articles/firewall

F-Secure (n.d.c.) Mikä on VPN? Viitattu 6.11.2024. https://www.f-secure.com/fi/articles/what-is-a-vpn

Google cloud (n.d.) PaaS vs. IaaS vs. SaaS vs. CaaS: How are they different? Viitattu 14.9.2024. https://cloud.google.com/learn/paas-vs-iaas-vs-saas

Hjorth K. Organisaationtietoturva (2015) Organisaation tietoturva -kurssi. Viitattu 6.9.2024. https://organisaationtietoturva.wordpress.com/

Huttunen K. 2021. Mikä on WordPress? Viitattu 13.9.2024. https://www.zoner.fi/wordpress/mika-on-wordpress/

Jurvanen L. (2023) Mitä tarkoittaa hallinnollinen tietoturva? Viitattu 4.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Kiravuo T, Timlin P, Kemppainen K, Eronen J, Seppänen S. (2023) Ohjelmistoturvallisuudentila 2023. Viitattu 5.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjelmistoturvallisuuden%20tila%202023.pdf

Koskinen A. (2023) Mikä on WordPress? Viitattu 13.9.2024. https://www.fissiomedia.fi/wordpress/mika-on-wordpress/

Kyberturvallisuuskeskus(n.d.). (2019). Luottamuksen lähteillä. Viitattu 4.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Limit login attempts reloaded (n.d.) The only plugin you need for login protection. Viitattu 14.10.2024. https://www.limitloginattempts.com/

Metropolia (n.d.a.) 2024 tietojen luokittelu ja tallennus turvallisesti. Viitattu 10.9.2024. https://wiki.metropolia.fi/display/tietohallinto/Tietojen+luokittelu+ja+tallennus+tietoturvallisesti

Microsoft (n.d.b.) Mitä on käyttöoikeuksien hallinta? Viitattu 9.9.2024. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-access-control

Microsoft (n.d.c.) Mitä pilvipalvelujen tietoturva on? Viitattu 9.9.2024. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-cloud-security

NordVPN (n.d.) Mikä on VPN? Viitattu 6.11.2024. https://nordvpn.com/fi/what-is-a-vpn/

OVHCloud (n.d.) Why choose OVHcloud? Viitattu 22.10.2024. https://www.ovhcloud.com/en/

Rajamäki M. (2022) Yritysturvallisuus. Viitattu 6.9.2024. https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/

Rapo S. 2022. Luovutettu Karjala sivuston tekijä. Viitattu 21.10.2024. https://www.luovutettukarjala.fi/

Seclion (n.d.). (2021). Mitä on fyysinen tietoturvallisuus? Viitattu 4.9.2024. https://blog.seclion.fi/turvallisuus/fyysinen-tietoturvallisuus

Sucuri (n.d.) Clean and protect your website fast. Viitattu 14.10.2024. https://sucuri.net/

Tietoturvariskienarviointi (n.d.). (2023) Yleistä tietoturvariskeistä. Viitattu 6.9.2024. https://www.tietoturvariskienarviointi.fi/

Tips and Tricks HQ (n.d.) WordPress easy HTTPS redirection plugin. Viitattu 15.10.2024. https://www.tipsandtricks-hq.com/wordpress-easy-https-redirection-plugin

Traficom (n.d.a) (2022) pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) Viitattu 10.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Traficom (n.d.b) (2022) Äly- ja digilaitteetkin kuuluvat kierrätykseen. Viitattu 10.9.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/aly-ja-digilaitteetkin-kuuluvat-kierratykseen

Vittaniemi N. (n.d.) Näin tarkkailet WordPress-käyttäjiä. Viitattu 14.10.2024. https://wpopas.fi/nain-tarkkailet-wordpress-kayttajia/

Wallenius N. (2022) Miten pilvipalvelujen tietoturva eroaa perinteisestä tietoturvasta? Viitattu 9.9.2024. https://niklaswallenius.fi/pilvipalvelun-tietoturva-erilainen/

Winnova (n.d.) Monivaiheinen tunnistautuminen. Viitattu 6.11.2024. https://www.winnova.fi/wp-content/uploads/2024/05/Monivaiheinen-tunnistautuminen.pdf

Wireshark (n.d.) What is Wireshark? Viitattu 6.11.2024. https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

WordPress (n.d.) Keep your site safe and secure. Viitattu 15.10.2024. https://wordpress.com/support/security/

WPservices (2024) (n.d.) WordPressin suosituimmat tietoturvauhat ja niiden torjuminen. Viitattu 21.10.2024. https://www.wpservices.com/fi/top-wordpress-security-threats-and-how-to-counter-them-wordpress-security-service/

Yasar K. Hardware security (2022). Viitattu 5.9.2024. https://www.techtarget.com/searchitoperations/definition/hardware-security

Zieniūtė U. (2022) Mikä on brute force -hyökkäys eli väsytyshyökkäys? Viitattu 21.10.2024. https://nordvpn.com/fi/blog/vasytyshyokkays/