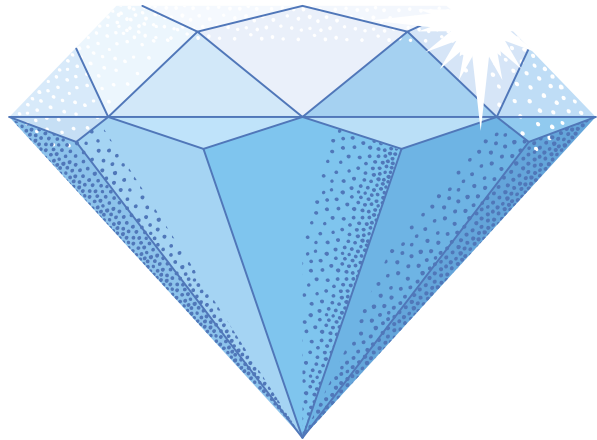




Osa I:

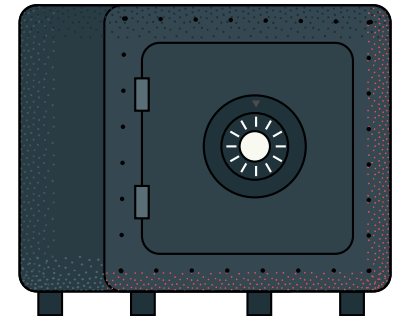
**Mitä ainakin
kannattaa tietää
WordPress-
sivuston
rakentamisesta ja
ylläpidosta?**

1. Tärkeä, tärkeämpi, tietoturva

Verkkosivuston tietoturvassa ei ole kyse vain teknisestä järjestelmästä. Tietojen turvaaminen suojaa ennen kaikkea yrityksen brändiä, liiketoimintaa ja uskottavuutta. WordPress tarjoaa tänä päivänä hyvät puitteet vahvan järjestelmän rakentamiseen. Sivuston tekijöiltä vaaditaan kuitenkin tinkimätöntä asennetta ja määrätietoista työtä.

Moni mieltää verkkosivuston näyteikkunaksi, jossa jokainen sisältö saakin näkyä kenelle tahansa – miksi siis panostaa tietoturvaan?

Mieli voi muuttua nopeasti, jos omalle etusivulle ilmestyy väärennetty pörssitiedote, asiakkaat eivät pääse sivustolle alkuunkaan tai hyökkääjä saa haltuunsa yhteystietoja, joiden ei pitänyt olla saatavilla.



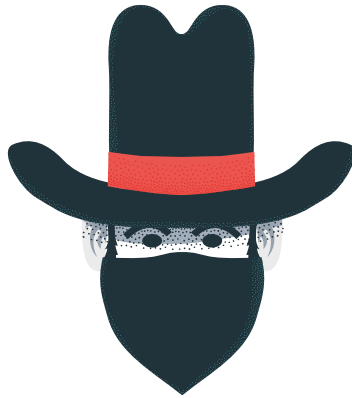
WordPress pysyy jatkuvien päivitysten ansiosta aina uusimmassa versiossa.

- 1) Tiheät päivitykset vahvistavat tietoturvaa, mutta säästävät myös verkkosivuston parissa työskentelevien hermoja.
- 2) Siinä missä kilpailevan, jähmeämmän järjestelmän versiopäivitys on erillinen ohjelmanumero, ei sivuston loppukäyttäjä välttämättä edes huomaa WordPress-päivityksiä.

Onko WordPress kuin reikäjuusto?

Ketteryyden kääntöpuolena on aiemmin sitkeästi elänyt myytti: Onko WordPress tietoturvan kannalta kuin reikäjuusto, jonka kanssa ei isoa sivustoa uskalla tehdä?

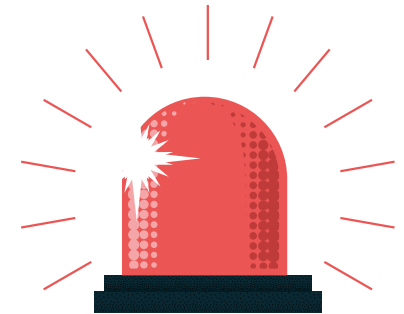
Se ei tänä päivänä pidä paikkaansa. WordPress-sivustosta voi huolehtia yhtä ammattimaisesti kuin mistä tahansa muusta sivustoratkaisusta. Esimerkiksi lisäosien laadun auditoinnit ovat vahvistaneet tietoturvan tasoa huomattavasti. Paikkausaktiivisuus on korkealla, tietoturvapäivityksiä julkaistaan nopealla aikataululla, ja aktiivisen kehittäjäyhteisön lisäksi WordPressin omassa tietoturvatiimissä työskentelee tänä päivänä 25 ammattilaista.



Tietoturva on kuitenkin monisyinen kokonaisuus, jossa heikoin lenkki ratkaisee koko ketjun kestävyyyden. Sen vuoksi erot eri WordPress-toimittajien ja -ylläpitäjien välillä voivat osoittautua suuriksi.

5 kohdan checklist: Varaudu tietoturvauhkiin

- **Vastuullinen WordPress-kumppani** pystyy varmistamaan verkkosivustosi tietoturvan kattavasti. Ota hyvissä ajoin selvää siitä, miten nämä kohdat on huomioitu:
- **Hyökkäysmahdollisuuksien minimointi.** Onko käytössä olevat lisäosat auditoitu? Miten päivitykset toteutetaan? Minne henkilötiedot tallennetaan?
- **Vahinkojen minimointi.** Jos ylläpitotunnus vuotaa rikollisen käsiin, pääseekö sen avulla käsiksi palvelimeen tai tietokantoihin?
- **Tunkeutumisen vaikeuttaminen.** Löytääkö mahdollinen tunkeutuja liian helposti tietoa järjestelmästä sekä sen käyttäjistä?
- **Vahingoista palautuminen.** Takaavatko kattavat varmuuskopiot ja konfiguraationhallinta sen, että vastaavan ympäristön saa puhtaalta pöydältä pystyyn toiseen palvelinsaliin – pian?
- **Tiedon saatavuuden varmistaminen.** Onko suorituskyky nopeasti skaalattavissa?



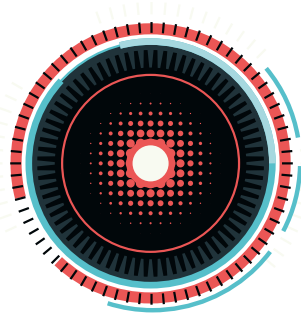
Käytännön esimerkkejä WordPress-sivuston turvaamisesta

”

Emme tee WordPressin ja lisäosien päivityksiä kuukausittain siksi, että saisimme asiakkaan ylläpitokäyttöliittymän hajalle tai hienoja lisäkilkkeitä käyttöön, vaan pitääksemme järjestelmän turvallisena. Tähän käytämme vuositasolla yli 1300 tuntia eli lähes 100 000 euroa.

Varmuuskopioinnin teemme tuplana. Sopimusten mukaisesti teemme tyypillisesti 30 päivän varmuuskopion Nebulan palvelinsaliin, mutta sen lisäksi 7 päivän lisävarmuuskopion Upcloudiin. Näihin varmuuskopioihin Valu investoi yhteensä tuhansia euroja vuodessa.

Käytämme kaksinkertaista palomuuria, jotta voimme mahdollisimman aikaisessa vaiheessa puuttua hyökkäyksiin ja estää haitalliseen liikenteen.



Käytämme asiakaskohtaisia palvelimia, koska haluamme erottaa eri asiakkaiden datan. Osa tietoturvakorjauksista tehdään palvelintasolla, osa taas sovellustasolla oman mallimme, eli erillisen ympäristölisäosan avulla.

Projekteista riippumattomat tietoturvaparannukset ovat kaikille asiakkaillemme yhteisiä. Se tarkoittaa myös sitä, että asiakas saa jo aiemmin kumuloituneen tietoturvatiedon kerralla käyttöönsä, kun siirtää sivustonsa meille.”

Mikko Virenius, teknologiajohtaja, Valu Digital

”

“Uuden sivuston myötä myös tietoturva saatiin pörssiyhtiön tiukkoja vaatimuksia vastaavalle tasolle. Parantunut tietoturva todennettiin myös ulkopuolisen auditoijan toimesta.”

Lue Kojamon asiakastarina: www.valu.fi/asiakastarinat/kojamo/

