



Digiturva³⁶⁵

Digitaalinen kivijalka turvaan – Verkkokaupan ja kotisivujen suojaaminen hyökkäyksiltä

Onko digitaalinen kivijalkasi todella suojattu? Käytännön opas yrityksille

- Mikko Kivinen, Digiturva365 / Scene Group Oy
- Verkkosivujen ja -kauppojen uhkakuvat sekä moderni suojaus

Miksi verkkosivusto tai verkkokauppa on jatkuva kohde?

Kyberrikollisuus ei valikoi – automaatio haravoi verkkoa 24/7



Automaattiset botit ja skannerit

Etsivät avoimia haavoittuvuuksia verkosta massana ja kohdistavat hyökkäyksiä löydettyihin, haavoittuviin kohteisiin.



Arvokas saalis

Verkkokauppojen tietokannat ja maksuliikenne ovat rahanarvoista saalista kyberrikollisille.



Iskun seuraukset

Maineen menetys, myynnin pysähtyminen, tietojen vuotaminen, toimintahäiriö ja hakukonenäkyvyyden romahdus.

1. Haavoittuvuudet, 0-dayt & SQL-injektiot

Sovellustason yleisimmät tietoturva-aukot ja korttitietojen kaappaus

01

Tunnetut ja nollapäivähaavoittuvuudet

Lisäosien ja teemojen (WordPress, Magento) korjaamattomat aukot. Suurin osa murroista hyödyntää jo tunnettuja aukkoja, joihin korjaus olisi saatavilla.

02

SQL-injektiot (SQLi)

Haitallisen tietokantakoodin syöttäminen lomakkeiden kautta (koko tietokannan vuoto).

03

E-skimming / Magecart

Huomaamaton haitallinen JavaScript maksusivulla, joka varastaa luottokorttitiedot lennossa kassan läpi kulkiessa. Kyberturvallisuuskeskus on saanut useita ilmoituksia Magecart-hyökkäyksistä suomalaisiin verkkokauppoihin.

Sovellustasolla yleisin reitti sisään ovat vanhentuneet lisäosat. E-skimming on erityisen vaarallinen, koska kauppa toimii normaalisti: British Airways 2018 – skimmeri toimi maksusivulla kaksi kuukautta huomaamatta, noin 430 000 asiakkaan tiedot vuotivat ja seurauksena oli 20 miljoonan punnan sakko.

2. Botnetit, Brute Force & Credential Stuffing

Kun tuhannet saastuneet laitteet iskevät kirjautumissivullesi



Credential Stuffing

Vuodettujen tunnus-salasanaparien automaattinen kokeilu verkkokaupan, sivuston tai sovelluksen hallintapaneeliin.



Brute Force -hyökkäykset

Salasanojen järjestelmällinen arvaaminen valtavalla volyymilla.



Roskaposti- ja huijausbotit

Kommenttispammi, lomakkeiden saastuttaminen, SEO-töhrintä ja turhan palvelinkuorman aiheuttaminen.

Saastuneista laitteista koostuvat botnetit testaavat valtavia määriä tunnusyhdistelmiä. Vaikka murto ei onnistuisi, pelkkä yritysten määrä voi kuormittaa palvelinta tai laukaista rajoitukset, jolloin myös oikeat asiakkaat kärsivät.

3. DDoS, Sivuston töhrminen & Kryptolouhinta

Palvelun lamauttaminen, sivuston töhrminen ja resurssikaappaus



DDoS (Distributed Denial of Service)

Verkkosivusto kaadetaan tulvimalla palvelimelle miljoonia kyselyitä. Suomeen kohdistuu tuhansia palvelunestohyökkäyksiä päivässä.



Sivuston töhrminen (Defacement)

Etusivun korvaaminen rikollisten omalla viestillä (välitön mainehaitta).



Kryptolouhinta & Troijalaiset

Saastunut palvelin valjastetaan kryptovaluutan louhintaan tai jatkohyökkäyksiin.

DDoS tukkii verkkokaupan kaistan juuri sesongin kynnyksellä. Defacement tuhoaa luottamuksen välittömästi. Kryptolouhijat taas pyörivät taustalla hidastaen palvelinta.

4. Nimipalvelut (DNS) & Toimitusketjut

Kun liikenne ohjataan valesivulle tai luotettu koodi vuotaa



DNS Hijacking / Spoofing

Liikenne ohjataan väärään paikkaan väärentämällä DNS-vastauksia, kaappaamalla reitityksiä (BGP) tai – yleisimmin – murtautumalla rekisteröijän tai DNS-palvelun hallintapaneeliin. Kävijät päätyvät valesivustolle ilman, että pääpalvelimeen kosketaan.



Toimitusketju- ja koodiriskit

Hyökkääjä saastuttaa kolmannen osapuolen seurantaskriptin, chat-widgetin tai lisäosan kehittäjän päässä, ja haitallinen koodi suoritetaan luotettuna asiakkaan selaimessa. Esimerkki: polyfill.io 2024 – kaapattu skriptipalvelu syötti haittakoodia yli 100 000 sivustolle.



API-haavoittuvuudet

Taustajärjestelmien (ERP, CRM) rajapintojen puutteellinen tunnistautuminen tai syötteen suodatus. Hyökkääjät ohittavat verkkokaupan käyttöliittymän ja hyödyntävät suoria API-kutsuja datan varastamiseen.

Vaikka oman sivustosi koodi olisi kunnossa, nimipalvelinkaappaus (DNS) tai saastuneet kolmannen osapuolen riippuvuudet ohittavat sovellustason suojaukset ja vaarantavat käyttäjien tiedot.

1. Cloudflare, Bunny.net & DNSSEC – Liikenteen reunasuojaus

Estä DDoS-hyökkäykset ja suojaa nimipalvelut ennen kuin ne saavuttavat palvelimesi



CDN & Anycast-verkko (Cloudflare, Bunny.net)

Pysäyttää laajat DDoS-hyökkäykset ja suodattaa haitallisen liikenteen reunaverkossa – kunhan palvelimen oikea IP-osoite on piilotettu ja liikenne sallitaan vain CDN:n kautta.



DNSSEC (DNS Security Extensions)

Digitaalinen allekirjoitus DNS-vastauksille: estää väärennetyt vastaukset ja välimuistimyrkytyksen. Hallintapaneelin kaappausta vastaan tarvitaan lisäksi MFA ja verkkotunnuksen siirtolukko.



Suorituskyky & Nopeus

Suojauksen lisäksi välimuistitustoiminnot nopeuttavat verkkokauppaa merkittävästi.

Cloudflaren tai Bunny.netin kaltainen reunapalvelu imee DDoS-hyökkäyksen ennen kuin se pääsee palvelimellesi. DNSSEC estää DNS-vastausten väärentämisen – ja MFA rekisteröijän tunnuksissa suojaa domainia kaappaukselta.

2. WAF & Virtuaalipaikkaus (WP Guardian, Patchstack)

Pysäytä SQL-injektiot ja paikkaa reiät ilman välitöntä koodimuutosta



Web Application Firewall (WAF)

Suodattaa HTTP-liikennettä sovellustasolla (OWASP Top 10, ModSecurity / Cloudflare WAF).



Virtuaalipaikkaus (WP Guardian, Patchstack)

Kun lisäosan haavoittuvuus tulee tietoon, kohdennettu suojaussääntö estää sen hyödyntämisen – usein jo ennen kuin virallinen korjaus on saatavilla. WP Guardian toimii palvelintasolla: kysy palveluntarjoajaltasi.



Aikasäästö & Turva

Antaa kehittäjille aikaa päivittää lisäosat turvallisesti ilman, että sivusto on haavoittuvainen.

WAF tutkii kaiken liikenteen. Virtuaalipaikkaus lisää WAF:iin kohdennetun säännön heti, kun uusi haavoittuvuus tulee tietoon – ennen kuin virallinen päivitys ehditään koodata, julkaista ja asentaa.

3. Palvelintason torjunta (Imunify360, CrowdSec)

Proaktiivinen haittaohjelmaskannaus ja yhteisöpohjainen IP-estolistaus



Imunify360

Automaattinen palvelintason suojaus (haittaohjelmien reaaliaikainen siivous ja verkkopalomuuuri). Palveluntarjoaja ottaa sen käyttöön palvelimella – kysy, onko se käytössä.



CrowdSec

Yhteisöpohjainen IP-reputatioverkko ("Naapurivahti verkossa") – jakaa tietoa hyökkäävistä boteista ja estää ne globaalisti.



Perinteiset palomuurit & HIDS

Perinteiset palomuurit, ModSecurity ja murronhavaitsemisjärjestelmät (IDS/HIDS, kuten Wazuh) tarjoavat perussuojan, mutta vaativat ylläpitoa ja erikoisosaamista.

Perinteinen palomuuuri ja murronhavaitsemisjärjestelmä (IDS) saavat rinnalleen nykyaikaisen automaation: Imunify360 siivoaa haittaohjelmat ja CrowdSec estää hyökkäykset kollektiivisen älyn avulla.

4. Zero Trust & Sisäiset järjestelmät

Kuka pääsee käsiksi versiohallintaan, hallintapaneeliin tai laskutukseen?



Nollaluottamus (Zero Trust)

Älä luota kehenkään oletuksena – edes sisäverkossa. Jokainen käyttäjä, laite ja pääsypyyntö todennetaan ja valtuutetaan aina erikseen.



Tarkan pääsynhallinnan periaate

Tarvitseeko koko tiimi pääsyn versiohallintaan, tietokantaan tai laskutukseen? Entä onko tarvetta päästä järjestelmiin kaikkialta maailmasta, vai kannattaako pääsy rajata esimerkiksi vain Suomen alueelle?



Suojatut rajapinnat

IP-rajoitukset, SSO/MFA-pakotus ja Zero Trust Network Access (ZTNA) sisäisiin työkaluihin julkisen verkon sijaan.

Onko yrityksenne intranet, versiohallinta tai laskutusjärjestelmä avoinna koko maailmalle pelkän salasanan takana? Zero Trust -malli sulkee sisäiset järjestelmät julkisesta verkosta.

5. Cloudflare WARP & Access – Suojaa sisäiset järjestelmät

Ei avoimia portteja internetiin: tunnistautuminen tapahtuu ennen kuin verkkosivu edes latautuu



1. WARP-asiakasohjelmisto (valinnainen)

Kevyimmillään Access toimii pelkällä selaimella. Työntekijän laitteelle asennettava WARP-client tuo lisäksi laitetarkistuksen: pyyntö hyväksytään vain yrityksen hallinnoimalta päätelaitteelta.



2. Väliintulo reitillä

Kun työntekijä avaa suojatun osoitteen (esim. intranet.yritys.fi, hallintapaneeli tai laskutus), ruudulle pamahtaa ensin Cloudflare Access -tunnistautumissivu.



3. Kertakäyttökoodi (OTP)

Käyttäjä syöttää sähköpostiinsa saapuvan vahvistuskoodin (tai tunnistautuu M365/SSO-tunnuksillaan). Vasta hyväksynnän jälkeen varsinainen verkkosivu latautuu näkyviin.



4. Täydellinen piilotus

Ulkopuoliselle hyökkääjälle tai botille itse taustajärjestelmää ei ole edes olemassa – he näkevät vain Cloudflaren suojamuurin.

Cloudflare WARP & Access luo saumattoman Zero Trust -suojauskeinojen: sisäiset järjestelmät pysyvät täysin piilossa julkiselta verkolta ja pääsy todennetaan aina ennen yhteyden muodostamista.

6. CMS-lisäosat, Kontitus & Staattiset sivut

CMS-tason sovellussuojaus ja hyökkäyspinnan minimointi



CMS-tietoturvalisäosat (Wordfence, Solid Security)

Sovelluksensisäinen palomuuuri, MFA
ylläpitäjille ja kirjautumisvalvonta.



Eristäminen & Kontitus (Docker / LXC)

Eristetään verkkokauppa ja muut
sovellukset omiin kontteihinsa
mahdollisten tartuntojen tai
tietomurtojen leviämisen estämiseksi.



Staattiset sivustot (Jamstack / SSG)

Kun sivustolla ei ole tietokantaa eikä
julkisessa verkossa olevaa
sisällönhallintaa, hyökkäyspinta on
murto-osa (Ei tietokantaa = Ei SQLi!).
Hosting-tunnukset, DNS ja ulkoiset
skriptit on silti suojattava.

Kontitus rajoittaa hyökkäyksen leviämistä palvelimella. Esittelysivustoille staattinen SSG-malli on erinomainen suoja: kun tietokantaa tai julkista sisällönhallintaa ei ole, hyökkääjällä on huomattavasti vähemmän kaapattavaa.

Mistä aloittaa omassa yrityksessä?

Toimenpiteet riippuvat siitä, kuka ylläpitää verkkokauppaasi



Käytätkö SaaS-verkkokauppaa? (esim. Shopify, MyCashflow)

- Ota MFA käyttöön kaikille ylläpitäjille
- Kysy toimittajalta: WAF, DDoS-suojaus ja varmuuskopiot
- Käytä maksupalvelun omaa maksusivua (esim. Paytrail, Stripe Checkout)
- Karsi turhat ulkoiset skriptit ja lisäosat



Ylläpidätkö omaa WordPressiä / WooCommercea?

- Automaattiset päivitykset, poista käyttämättömät lisäosat
- Virtuaalipaikkaus (Patchstack / WP Guardian) ja WAF
- CDN-reunasuojaus ja palvelimen IP-osoite piiloon
- Testatut offsite-varmuuskopiot
- MFA ylläpitoon, rekisteröijään ja DNS:ään

Kysy palveluntarjoajaltasi: mitkä näistä on jo hoidettu puolestani?

Tarkistuslista: Suojaa digitaalinen kivijalkasi

Viisi konkreettista askelta verkkopalvelun ja verkkokaupan turvaamiseksi



1. CDN & DNSSEC

Laita Cloudflare/Bunny.net ja DNSSEC kuntoon (suojaa nimipalvelut ja torju DDoS-hyökkäykset).



2. WAF & Virtuaalipaikkaus

Ota käyttöön WAF & virtuaalipaikkaus (Cloudflare / Bunny.net / WP Guardian / Patchstack).



3. Palvelintason suojaus

Varmista palvelintason suojaus (Imunify360 / CrowdSec) haittaohjelmia ja bottihyökkäyksiä vastaan.



4. MFA & Zero Trust

Ota MFA käyttöön kaikissa ylläpito-, rekisteröijä- ja DNS-tunnuksissa. Sulje sisäiset työkalut ja hallintapaneelit julkisesta verkosta.



5. Varmuuskopiot & CMS

Huolehdi varmuuskopioista & CMS-päivityksistä (automaattiset päivitykset ja testatut varmuuskopiot muualla).

Digitaalinen kivijalka pysyy pystyssä kerroksittaisella suojauksella: reunalla (Cloudflare/Bunny.net), sovelluksessa (WAF/Patchstack), palvelimella (Imunify360) ja pääsynhallinnassa (MFA & Zero Trust) – ja testatut varmuuskopiot pelastavat, kun kaikki muu pettää.

Kiitos osallistumisesta!



Koulutuksen järjestäjä

Prizztech Oy

www.prizz.fi



Kouluttaja & Asiantuntijatuki

**Scene Group Oy /
Digiturva365**

Mikko Kivinen



Oppaat ja lisämateriaalit

asiakaspalvelu@digiturva365.fi

myynti@digiturva365.fi

**www.digiturva365.fi
www.scenegroup.fi**