Kuinka suojaan sivustoni kybersodalta?

Tietoturvan vahvistamisen
ei tarvitse olla vaikeaa

VALU

Kyberuhkiin varautuminen on ajankohtaisempaa kuin koskaan

Virtuaalisten hyökkäysten rintamalla muutos on juuri nyt nopeaa. Myös Suomessa viranomaiset ovat pyytäneet, että kaikki verkkopalvelujen ylläpitäjät huomioisivat kyberuhkatason selvän nousun. Nyt on oikea hetki tarkastella IT-palveluntarjoajien kanssa tehtyjä sopimuksia ja varmistaa, että oma verkkosivusto on suojattu riittävän hyvin.

Poliittiset jännitteet maailmalla muuttuvat nopeasti, ja yhtä nopeasti muuttuvat verkkohyökkäysten ja hybridivaikuttamisen taktiikat. Uudenlaiset riskit haastavat verkkosivustoja joka päivä.

Tämän oppaan luettuasi tiedät, **miten voit suojata oman verkkosivustosi kyberhyökkäyksiltä nykyistä paremmin**. Opas keskittyy erityisesti WordPress-sivustojen suojaamiseen, mutta se antaa ajattelemisen aihetta minkä tahansa alustan parissa työskentelevälle.

Kyberuhkien torjumisen ei tarvitse olla kallis ja massiivinen projekti. Sen ei tarvitse sitoa kohtuuttomasti organisaatiosi aikaa ja rahaa. Tärkeintä on, että et ohita aihetta olankohautuksella. Kustannukset ja haittavaikutukset voivat sen sijaan kasvaa suuriksi, jos suojautumista lykkää tuonnemmaksi.

Suojautuminen alkaa verkkosivuston kivijalasta. Tekniset ratkaisut on tehtävä tietoturvallisesti, ja ylläpidon käytännöt rakennettava fiksusti. Asiantuntevan verkkosivustokumppanin kanssa perusasioiden voi luottaa olevan kunnossa – mutta minkälaista lisäsuojaa sivustolle kannattaa rakentaa odottamattomien yllätysten varalta?

Opas vastaa esimerkiksi näihin kysymyksiin:

- Millaisia konkreettisia haittoja kyberhyökkäykset aiheuttavat organisaatioille?
- Mikä on hajautettu palvelunestohyökkäys (DDoS) ja miksi se haastaa verkkosivustoja aivan uudella tavalla?
- Miten valita oikeanlainen suojaustaso?

Oppaan sisältö:

Mikä kybersota?

Joskus kyberrikollisia motivoi taloudellisen edun tavoittelu, joskus häiriköinnillä ei ole tunnistettavaa syytä. Viimeistään Venäjän hyökkäyssota Ukrainassa on nostanut poliittiset motiivit ja vaikuttamisyritykset valokeilaan, kun puhutaan organisaatioiden tietoturvasta. **Kybersota ei ole tulevaisuuden skenaario, vaan totta juuri nyt.**

Kyberturvallisuuskeskuksen raportit kertovat, että Suomessakin havaittujen haittaohjelmien, tietojenkalastelukampanjoiden ja palvelunestohyökkäysten takana on ryhmittymiä, joiden jäljet ovat johdettavissa muun muassa Venäjän, Kiinan, Iranin ja Pohjois-Korean hallintojen lähelle.

Vuonna 2022 Kyberturvallisuuskeskus totesi suurimmaksi ajankohtaiseksi kyberuhkaksi sen, että talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen.

Kybersota ei katso valtioiden rajoja

Kybersodassa hyökkääjä pyrkii **vaikuttamaan kohteisiinsa verkon kautta useilla eri keinoilla.** Tavoitteena voi olla vakoilu, tietojärjestelmien tai infrastruktuurin lamauttaminen tai disinformaation levittäminen.

Hyökkäyksillä pyritään myös kolhimaan kohteen mainetta. Tietomurrot tai palvelukatkokset rapauttavat kansalaisten luottamusta verkkopalveluihin ja kokonaisiin instituutioihin.

Valtiot varautuvat tänä päivänä kybersotaan siinä missä perinteiseenkin sodankäyntiin – niin myös Suomessa. Ilmiö on kuitenkin kahdenvälisiä konflikteja ja varusmiesten kouluttamista laajempi. Se ulottuu valtioiden rajojen yli. Siksi myös kyberrikollisuudelta **puolustautuminen kuuluu kaikille verkkosivustojen ja IT-järjestelmien ylläpitäjille.**

Hyökkäysyritykset voivat olla tarkkaan kohdennettuja tai summittaista lukkojen kolistelua. Ne voivat kohdistua yhtä hyvin paikallislehtien, pörssiyritysten kuin julkisten instituutioiden verkkosivustoille. Tänään liikkeellä oleva haittaohjelma voi olla osa verkkohyökkäystä, jonka haitat näkyvät pitkällä viiveellä. Siksi suojautumistoimissa kannattaa olla ennakoiden liikkeellä.

Virtuaalisesti on reaalimaailmaa helpompi piiloutua

Kybersodankäynti on rikollisille **houkutteleva haitanteon muoto, sillä hyökkäysten tekijää ei välttämättä koskaan saada jäljitettyä.** Et saa tietää, onko kyse valtiollisesta vaikuttamisoperaatiosta vai satunnaisesta häirinnästä. Yhtä kaikki, onnistuneen hyökkäyksen jäljissä riittää siivoiltavaa.

IT-palveluntarjoajat seuraavat säännöllisesti maailmalla havaittuja haittaohjelmia ja tietoturvahaavoittuvuuksia. Suomessa Liikenne- ja viestintävirasto Traficom julkaisee seurantadataa ja tilastoja esimerkiksi haittaohjelmahavainnoista. Raportit kertovat trendeistä, mutta niihin ei kannata tuudittautua liiaksi, sillä pinnan alle jää paljon:

- Hyökkäystaktiikat ja haittaohjelmat **kehittyvät niin nopeasti**, että automaattiset skannerit eivät kykene tunnistamaan kaikkia tapauksia. Uudenlainen vahinko huomataan vasta, kun se on jo tapahtunut.
- **Palvelunestohyökkäyksistä** on tullut teknologian kehittymisen myötä aiempaa laajempia ja halvempia toteuttaa. Niiden yleistyminen saattaa vähentää jonkin toisen hyökkäystavan, kuten haittaohjelmien, osuutta.
- Suojauskeinot kehittyvät jatkuvasti. Raportoitujen tapausten määrä pysyy aisoissa, sillä organisaatiot **osaavat varautua** erilaisiin kyberuhkiin päivä päivältä paremmin.

Kyberturvallisuus koostuu neljästä peruspilaristа: tietoturvasta, tietosuojasta, riskienhallinnasta ja toiminnan jatkuvuuden hallinnasta. Asiantuntevan sivustokumppanin kanssa pystyt varautumaan kaikkiin osa-alueisiin, eikä sen tarvitse olla kallis tai vaivalloinen projekti. Varautumatta jättäminen saattaa sen sijaan osoittautua sekä hintavaksi että työlääksi.

Kyberhyökkäyksen haitat organisaatiolle: Kolme näkökulmaa

“Miksi hyökkäys osuisi meihin, emme ole kovinkaan kiinnostava kohde?” Tietyt toimialat – kuten julkinen sektori, pankit, sähköyhtiöt ja muu infrastruktuuri – ovat tyypillisesti rikollisten erityisen huomion kohteena. Poliittisen tilanteen kiristyessä tiedotusvälineiden ja kansainvälisten pörssiyhtiöiden sivustot voivat samoin joutua hyökkääjien luupin alle. Toisaalta kukaan ei ole suojassa toimialansa perusteella: kyberhyökkäysten kohteeksi valikoidutaan myös sattuman kautta.

Tässä luvussa käydään läpi, **mitä riskejä onnistunut kyberhyökkäys tai jopa pelkät hyökkäysyritykset voivat mille tahansa organisaatioille aiheuttaa.**

1. Tietoturvaloukkausten kustannukset

Minkä vuoksi suojautumatta jättäminen voi tulla kalliiksi? Siihen on monia syitä, jotka liittyvät muun muassa ylimääräiseen työaikaan sekä palvelinten kuormitukseen:

- Verkkosivustosi ylläpitokumppani tekee ennakoivaa työtä, jotta kyberhyökkäykset eivät onnistuisi. Riippuu valituista teknisistä ratkaisuista, miten paljon hälytystilanteita esiintyy, ja kuinka paljon ne vaativat ylimääräistä asiantuntijatyöaikaa. Vaikka kaikki näyttäisi päällepäin hyvältä, pelkkä akuuttien kyberuhkien torjuminen ylimääräisenä asiantuntijatyönä saattaa tuottaa lisälaskun.
- Laaja palvelunestohyökkäys voi nostaa palvelintilakustannukset äkillisesti hyvin korkeiksi. Tällaisessa tilanteessa tietoturvallinen perussivusto saattaa kyllä kestää kovaakin painetta, mutta pelkästään käyttökustannusten vuoksi se on ehkä jopa suljettava väliaikaisesti.
- Sekä vakavista läheltä-piti -tilanteista että toteutuneista kyberhyökkäyksistä on raportoitava viranomaisille. Syiden selvittely ja raporttien laatiminen vie aikaa.
- Jos hyökkäys toteutuu, eikä sivusto toimi normaalisti, organisaation asiakaspalvelukanavat ruuhkautuvat. Puhelin-, some- ja sähköpostitiedustelut teettävät ylimääräistä työtä. Kysymykset voivat koskea poikkeustilannetta, tai sitten verkossa normaalisti toimiva itsepalveluasiointi siirtyy muihin kanaviin.
- Kriisiviestintäkoneisto käynnistyy, kun media alkaa selvittää, mistä on kyse. Organisaation oma viestintä siirtyy väliaikaisiin kanaviin tai Twitteriin, ja sitä varten tarvitaan runsaasti työaikaa.
- Verkkokaupoille jokainen tunti ilman toimivaa sivustoa on tunti pois myynnistä.

2. Maine- ja brändihaitat

Yritykset rakentavat brändinsä vetovoimaa jopa vuosia, mutta sen voi menettää yhdessä yössä. Toimintansa jo lopettaneen Psykoterapiakeskus Vastaamon tietovuototapaus ja sen mediahuomio lienee tästä kaikille tuttu esimerkki.

Jos joudut kiristyshaittaohjelman uhriksi, älä maksa lunnaita. Rikollisen sanaan tietojen palauttamisesta ei voi luottaa. Lue Kyberturvallisuus-keskuksen sivuilta lisää tietoa siitä, miten kiristyshaitta-ohjelmatilanteessa tulisi toimia.

Vaikka oman sivuston takana ei edes olisi arkaluontoisia tietoja, joiden vuotaminen olisi katastrofi, toteutunut kyberhyökkäys voi aiheuttaa organisaatiolle pysyviä kolhuja.

Viestinnän teho perustuu **luotettavuuteen**. Jos hyökkääjä onnistuu esittämään sivustolla väärää tietoa, tai linkittää valtaamansa sivuston toiseen osoitteeseen, on se kriisi jo itsessään. Tilanne pystytään ehkä korjaamaan pian, mutta vaikutukset ulottuvat pitkän ajan päähän.

Epävarmuuden lietsomiseksi ei tarvita edes disinformaatiota. Verkkosivusto on yrityksen tai julkisen instituution käyntikortti. Koko organisaation maine kärsii sitä enemmän, mitä pidempään **sivusto on pois käytöstä** esimerkiksi palvelunestohyökkäyksen vuoksi.

3. Luotettavan tiedonsaannin jatkuvuus

Sekä julkisilla tahoilla että yksityisillä yrityksillä voi olla tiedottamiseen liittyviä velvollisuuksia. Verkkosivusto on tänä päivänä se kanava, jossa muun muassa terveydenhuollon ajanvarauspalveluista kerrotaan kootusti. Pörssiyhtiöt julkaisevat sivustoillaan lainsäädännön vaatimia tiedotteita sijoittajille.

Tämän päivän kansalainen ja kuluttaja on tottunut saamaan tietoa nopeasti, kun tilanne on päällä. Esimerkiksi sähköyhtiö haluaa taatusti varmistaa, että sen verkkosivusto kestää horjumatta pystyssä, jotta mahdollisista sähkökatkoista tiedottaminen on sujuvaa.

Yksi kybersodan taktiikoista on pyrkimys vaikuttaa kansalaisten yleiseen mielipiteeseen. Disinformaatio tarkoittaa tahallista väärän tiedon levittämistä ja mielipidevaikuttamista. Sen levittämisessä rikolliset pyrkivät käyttämään hyödyksi juuri tiedotuskanavia ja niiden vakiintuneita yleisöjä. Onnistuessaan tällainen hyökkäys voi aiheuttaa merkittävää haittaa sekä julkisille että yksityisille organisaatioille.

> Kohtuullinen investointi kybersodankestävyyteen on kuin vakuutus, joka ehkäisee kalliita ja työläitä ongelmatilanteita.

Varaudu erilaisiin hyökkäysyrityksiin

Kyberhyökkäysten näkyvät haitat ovat vain jäävuoren huippu. Suurin osa työstä tehdään ennaltaehkäisyn ja suojautumisen parissa. Millaisia verkkosivustoihin kohdistuvat hyökkäysyritykset sitten ovat?

Palvelunestohyökkäykset (DoS ja DDos)

Perinteinen tapa **palvelunestohyökkäyksen (DoS)** tekemiseen on tämä: rikolliset käyttävät muutamaa IP-osoitetta, joista käsin he pyrkivät kuormittamaan kohteensa palvelinta lähettämällä sille lukuisia pyyntöjä yhtä aikaa. Pyynnöt muistuttavat tavallisten kävijöiden vierailuja sivustolla. Kyseessä ei ole murtautuminen tai tietojen urkkiminen, vaan tavoitteena on estää tavallisten kävijöiden pääsy verkkosivustolle. Jos sivustosi olisi tosielämän pankkisali, palvelunestohyökkäys olisi kuin yritys ruuhkauttaa pankin eteinen.

Palvelunestohyökkäyksiin on mahdollista varautua pyyntömäärärajoituksin: kun tietty IP-osoite lähettää tietyn määrän pyyntöjä, se joutuu automaattisesti estetyksi.

Hajautetussa DDoS-palvelunesto-hyökkäyksessä hyödynnetään useimmin bottiverkkoja ja edistynyttä automatiikkaa. Niin kutsutussa volumetrisessa DDoS-hyökkäyksessä pyyntöjä satelee jopa tuhansista eri IP-osoitteista yhtä aikaa. Hyökkääjä voi myös jättää yhteydenmuodostuksen viimeistelemättä, jolloin kertyy nopeasti puoliksi auki olevia yhteyksiä jonka takia tietoliikenneinfrastruktuurin eri komponentit ruuhkautuvat ja palvelu lopulta estyy. Tällaiset hyökkäykset ovat **hyvä esimerkki teknologian nopeasta kehityksestä**, joka näkyy myös kyberrikollisten taktiikoissa. Perinteinen monitorointi ja IP-osoitteiden estäminen ei riitä tällaisen hyökkäyksen torjumiseen. Valu Muuri- ja Headup-ratkaisut (ks. luku 5) sen sijaan huomioivat DDoS-hyökkäysten estämisen jo teknisissä rakenteissaan.

Aiemmin palvelunestohyökkäykset kaatoivat sivustoja nykyistä herkemmin. Skaalautuvien palvelinten myötä sivusto saattaa pysyä pystyssä erittäin suurista pyyntömääristä huolimatta. Jatkuva pyyntöjen pommitus voi kuitenkin nostaa tarvittavan palvelinkapasiteetin ja sen kustannukset äkisti suuriksi.

> Palvelunestohyökkäyksiin varautuminen on kuntapäättäjien mielestä tärkein kriisivalmiuden varautumiskohde heti pitkien sähkökatkojen jälkeen. Lähde: Yle Uutiset

Käyttäjätunnusten kalastelu ja salasanojen arvausyritykset

Salasanojen arvailu (väsytyshyökkäys, brute-force -hyökkäys) tarkoittaa tilannetta, jossa rikollinen ikään kuin kokeilee kepillä jäätä – automaattisesti ja väsymättä. Tavoitteena voi olla esimerkiksi tietomurto, väärän tiedon levittäminen tai haittaohjelmien levittäminen.

Botit pommittavat verkkosivuston ylläpidon kirjautumissivua eri tunnusten ja salasanojen yhdistelmillä. Kun sivustoa ylläpidetään ja monitoroidaan asiantuntevasti, tällainen käyttäytyminen voidaan tunnistaa ja estää hyökkääjien IP-osoitteet saman tien.

Tietojenkalastelu eli phishing tarkoittaa tilannetta, jossa huijari yrittää saada kohdehenkilöiden käyttäjätunnuksia ja salasanoja tietoonsa huijaussähköpostien tai -tekstiviestien avulla. Tunnusten avulla pyritään pääsemään käsiksi verkkosivustojen hallintaan. Tietojenkalasteluyrityksen onnistumiseen riittää yksikin inhimillinen virhe.

Sekä väsytyshyökkäyksen että tietojenkalastelun haittoja voi ehkäistä esimerkiksi:

- käyttäjätunnusten AD-integraatiolla, johon liittyy kaksivaiheinen tunnistautuminen
- IP-osoitteiden rajauksella, jossa verkkosivuston hallintaan pääsee käsiksi vain oman organisaation IP-osoitteista käsin sekä
- Headup-sivustotototeutuksella (ks. luku 5).

Lisäosien haavoittuvuuksien hyödyntäminen
Lisäosat tekevät WordPress-sivustoista erittäin taipuisia ja ketteriä suurtenkin organisaatioiden tarpeisiin. On kuitenkin tärkeää, että WordPress-sivuston toteuttaja- ja ylläpitokumppani tuntee lisäosien tietoturvaan liittyvät riskit ja seuraa ajankohtaisia haavoittuvuuksia huolellisesti. Yksikin päivittämätön lisäosa voi antaa kyberrikollisille keinon päästä käsiksi sivuston ylläpitoon.

Lisäosiin liittyvien ongelmien ehkäisy alkaa jo verkkosivuston rakentamisvaiheessa luotettavien lisäosien valinnasta. Ylläpitovaiheessa jokainen lisäosa on pidettävä jatkuvasti ajan tasalle päivitettynä, aivan kuten WordPressin ydinkin.

Automaattisella skannauksella pystytään tunnistamaan ja estämään haitalliset IP-osoitteet, jotka yrittävät kerätä tietoa tietyn sivuston lisäosista vahingoittamistarkoituksessa.

Palvelinohjelmistoihin liittyvät hyökkäysyritykset

Yleiset verkkohaavoittuvuudet, kuten palvelinohjelmistoihin liittyvät haavoittuvuudet, ovat minkä tahansa verkkosivuston ylläpitoon liittyvä riski. Verkkosivustoilla näihin varaudutaan palomuureilla sekä säännöllisiä palvelinpäivityksiä tekemällä.

Samoin kuin muidenkin hyökkäysyritysten kohdalla, myös palvelinohjelmistoihin murtautumisyritysten kohdalla hyökkäävät IP-osoitteet on mahdollista estää automaattisesti.

Jos haluat olla varma siitä, ettei vakavien hyökkäystilanteiden estämiseen ja selvittelyyn liity ennakoimattomia kustannuksia, sivuston toimintaa kannattaa turvata teknisillä lisävahvistuksilla, joista kerromme seuraavassa luvussa. Silloin varmistat myös, että sivustosi suojakuori ei murru, vaikka useisiin suomalaisiin verkkosivustoihin kohdistuisi yhtä aikaa moderneilla teknologioilla toteutettuja, laajoja verkkohyökkäyksiä.

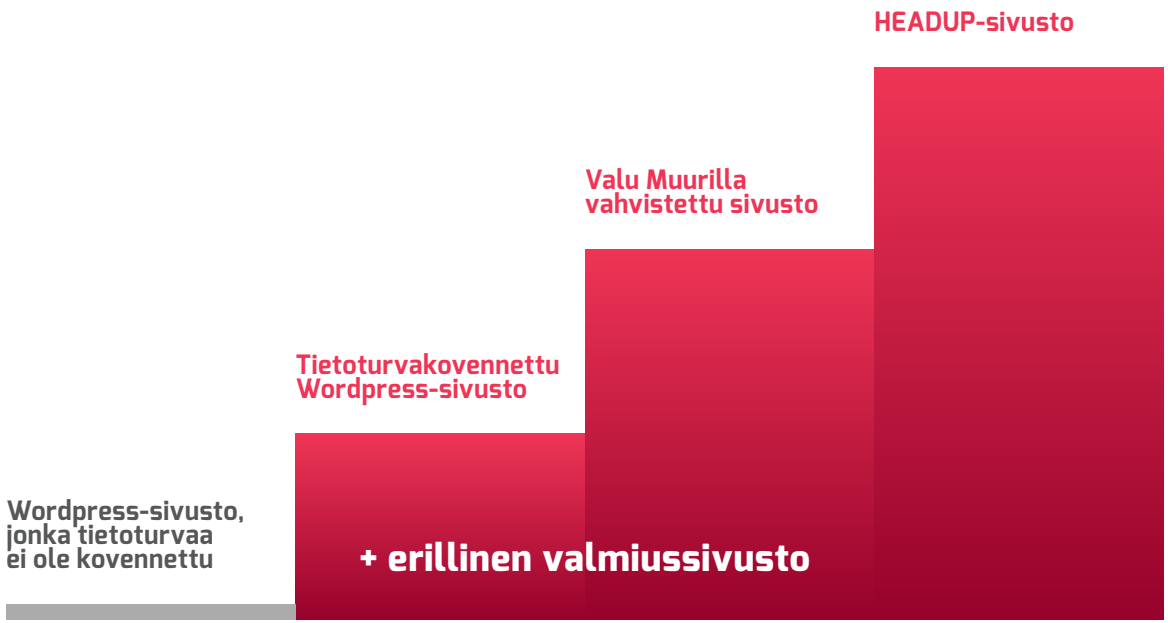
Miten Valu varautuu kyberhyökkäyksiin?

Tietoturva on Valussa yksi toiminnan peruspilareista. Olemme tehneet vuosien ajan säännönmukaista tietoturvatyötä ja toimineet korkean luokan tietoturvaratkaisujen edelläkävijänä WordPress-kentässä. Näin varmistamme verkkosivustojen tietoturvaa:

- Tiedon saatavuuden varmistaminen: Markkinoiden nopein palvelininfrastruktuuri, jossa suorituskyky on helposti skaalattavissa.
- Hyökkäysmahdollisuuksien minimointi: Käyttöjärjestelmien, ohjelmistojen, julkaisujärjestelmien ja lisäosien säännöllinen päivittäminen, lisäosien auditointi ja haavoittuvuuksien seuranta, arkaluontoisen tiedon tallentamisen minimointi.
- Tunkeutumisen vaikeuttaminen: Huolehdimme, että järjestelmästä ja sen käyttäjistä on saatavilla mahdollisimman vähän tietoa. Hämäämme hyökkääjiä väärillä käyttäjätiedoilla ja pysäytämme haitallisen toiminnan ajoissa. Käytämme kaikilla sivustoilla kaksinkertaista palomuuria ja tunkeutumisenestojärjestelmää.
- Vahinkojen minimointi: Ehkäisemme tilanteita, jossa yksi vahinko johtaisi toiseen – esimerkiksi vuotaneen ylläpitotunnuksen avulla ei voi asentaa ylläpidosta haittakoodia, päästä käsiksi palvelimeen tai tyhjentää tietokantaa.
- Vahingoista palautuminen: Varmuuskopioimme automaattisesti tuplana ja käytämme konfiguraationhallintaa, jolla vastaavan ympäristön saa nopeasti pystyyn puhtaalta pöydältä.
- Turvallinen kehittäminen: Hallitsemme SSH-avaimia keskitetysti, jotta pääsyoikeuksien myöntäminen ja poistaminen on mahdollisimman helppoa. Toimistomme verkko on suojattu palomuurilla ja etätyöskentely tapahtuu VPN:n yli. Versioimme koodimuutokset, jotta niitä on mahdollista seurata ja palauttaa. Salaamme työasemat ja varmuuskopiointilevyt vahvalla salauksella.
- Käyttäjästä johtuvien virheiden välttäminen: Käytämme palvelinten hallintaan keskitettyä konfiguraationhallintaa. Käytämme toimintaa automatisoivia ohjelmaskriptejä.
- Kehitämme jatkuvasti tietoturvallisempia ratkaisuja: Valu Muuri ja Headup ovat esimerkkejä teknologioista, jotka suojaavat asiakkaidemme verkkosivustoja.

Minkälainen suojaustaso sopii sivustollesi?

Tietoturvaa ei kannata koskaan laiminlyödä kokonaan. Kun suojaat verkkosivustosi, siirrät samalla hyökkääjän huomion muualle, heikommin varautuneisiin kohteisiin. Se, kuinka järeän varustelun valitset kybersodankäynniltä puolustautumiseen, riippuu siitä, millaisia riskejä organisaatiosi on valmis ottamaan.



Tavanomainen, tietoturvakovennettu Valu-sivusto

Jokaisen Valun asiakkaan WordPress-sivusto on **tietoturvakovennettu WordPress-sivusto**. Tietoturvaa on vahvistettu useilla eri käytännöillä (ks. luku 4). Tilastot kertovat, että nämä sivustot ovat lähes 100 % toimintavarmoja. Tilanne on pysynyt vakaana, vaikka hyökkäysyritysten määrä on jatkuvassa kasvussa.

Tavanomaisiin sivustoihin liittyy kuitenkin tiettyjä **kustannusriskejä**. Verkkosivustojen ylläpitäjinä torjumme suppeampia palvelunestohyökkäyksiä ja erilaisia murtautumisyrityksiä päivittäin. Kyberhyökkäysten yleistyessä yleistyvät myös yksittäiseen sivustoon kohdistuvat poikkeustilanteet. Niiden selvittely ja raportointi asiantuntijoiden tuntityönä voi tuoda ylimääräisiä kuluja sovitun kuukausihinnan päälle.

Toinen odottamaton kuluerä voi liittyä tiedonsiirtoon. Kovennettu sivusto on rakennettu siten, että se kestää korkeitakin kävijäpiikkejä kaatumatta. Sivuston palvelinkapasiteetti mitoitetaan hieman normaalikäyttöä korkeammaksi, ja piikkitilanteista maksetaan erikseen. Jos keskikokoinen palvelunestohyökkäys ajoittuu virka-ajan ulkopuolelle, puhutaan piikin sijaan tuntien tai koko viikonlopun mittaisesta ruuhkatilanteesta. Sivusto kestää ja kestää kaatumatta, mutta pelkästä ylimääräisestä tietoliikennesiirrosta voi kertyä asiakkaalle tuhansien eurojen ylimääräinen lasku.

Valu Muurilla vahvistettu sivusto

Viime aikoina yleistyneet, hajautetut palvelunestohyökkäykset (DDoS) ovat olleet laajuudeltaan ja voimaltaan jopa 500-kertaisia aikaisempaan hyökkäystaktiikkaan verrattuna. Näin laajoihin hyökkäyksiin ei olisi järkevää varautua tavanomaisten WordPress-verkkosivustojen ylläpitosopimuksissa. Palvelunestohyökkäysten aiheuttamat ylläpitokulut voisivat nostaa asiakkaan kuukausikustannukset moninkertaisiksi.

Siksi modernien palvelunestohyökkäysten ehkäisemiseen on tarjolla uudenlainen palvelu: Valu Muuri.

Valu Muuri on verkkosivuston ympärille rakennettu lisäkerros. Se on suodatin, jonka läpi kaikki kyseiseen domain-osoitteeseen liittyvä liikenne kulkee. Sen toiminta perustuu tekoälyyn, joka estää 99 % hajautetuista, useista eri IP-osoitteista tulevista palvelunestohyökkäyksistä. Muuri reagoi haitalliseen liikenteeseen sekunnin kuluessa.

Älykkyys erottaa Valu Muurin perinteisistä palomuureista. Kaikki Valun toteuttamat verkkosivustot on oletusarvoisesti vahvistettu kaksinkertaisen palomuurin lisäksi tunkeutumisenestojärjestelmällä. Vaikka yhdistelmä torjuu monen tyyppisiä hyökkäyksiä tehokkaasti, se ei ehdi reagoida hajautettujen palvelunestohyökkäysten massaan Valu Muurin kaltaisella nopeudella.

Hajautetut palvelunestohyökkäykset perustuvat pitkälle vietyyn automatiikkaan. Siksi ne edellyttävät myös älykästä, automatisoitua puolustusta.

Suodattimen lisäksi Valu Muuriin kuuluu ylimääräinen välimuistituskerros. Taustapalvelinten häiriötilanteissa se tuo jatkuvuutta sivuston toimintaan ja käyttäjille näkyvään kerrokseen.

Tietoturvan vuoksi kehitetty lisäkerros tarjoaa siis lisävakautta ja suorituskykyä myös normaaleihin kävijäpiikkeihin.

Valu Muuri tuo sivuston ylläpitoon kustannussuojan. Kun haitallinen liikenne pysähtyy lisäsuojauskerrokseen, tiedonsiirtokuluja ei muodostu muusta kuin sallitusta, oikeasta kävijäliikenteestä. Näin kuukausittaiset kustannukset ovat tarkasti ennakoitavissa. Valu Muuri -lisäpalvelun kuukausihinta liikkuu sadoissa, ei tuhansissa euroissa, eli säästöt voivat olla huomattavat.

Verkkosivuston kotivara: Valmiussivusto

Valmiussivusto on tavanomaisen sekä Valu Muurilla vahvistetun sivuston “B-suunnitelma”. Se varmistaa, että esimerkiksi tiedotus voi jatkua katkeamattomana, vaikka sivustoon kohdistuisi täysin uudenlainen ja yllättävä kyberhyökkäys.

Käytännössä valmiussivusto on varastoon tehty, mahdollisesti yksinkertaistettu kopio alkuperäisestä sivustosta. Jos normaali sivusto on kriisitilanteessa pois käytössä, valmiussivusto aktivoidaan ja liikenne ohjataan sinne.

Valmiussivusto on saatavilla erillisenä lisätuotteena.

Headup-sivusto

Headup-sivuston tekninen arkkitehtuuri on kybersodan kestävä. Siihen sovelletaan kovennetun WordPress-sivuston tietoturvakäytäntöjä, sitä suojaa Valu Muuri, mutta ennen kaikkea Headup on perustuksiaan myöten erilainen kuin perinteiset WordPress-sivustot.

Headup-sivusto koostuu käytännössä staattisista html-sivuista, jotka voidaan sijoittaa samankaltaisina rajattomalle määrälle palvelimia. Käyttäjä näkee aina häntä lähimmällä palvelimella sijaitsevan sivun. Näin mikään palvelimelle kohdistuva hyökkäys ei pysty estämään sivun näyttämistä.

Headup-sivuston julkisesti näkyvä sivusto on kokonaan erillään WordPress-sisällöntuotantoympäristöstä. Rikolliset eivät pysty etsimään julkaisujärjestelmästä haavoittuvuuksia, sillä se ei ole saavutettavissa julkisen verkon kautta, vaan ainoastaan organisaation omista IP-osoitteista. Ja vaikka julkiselle sivustolle kohdistuisi kuinka paljon kuormaa tahansa, sisällöntuotantoympäristö ei kuormitu.

Kriisitilanteiden uhatessa sivustosta saadaan julkaistua sisällöntuotantoympäristöstä aina uusi versio, joka yksinkertaisesti siirretään aikaisemman version sivulle.

Palvelintason lisäksi muitakaan takaportteja ei kannata jättää auki. Suosittelemmekin kaikille Headup-asiakkaillemme esimerkiksi vahvasti hajautettua nimipalvelinta omalle domainille. Tällöin domain on suojassa kaappauksilta, ja myös maantieteellisesti hajautettu eri palvelinsaleihin.

Valu Muuri vai **Headup**?

Headup on paras vaihtoehto organisaatioille, joilla on ehdoton vaatimus siitä, ettei verkkosivusto saa kaatua. Organisaation toiminta voi olla yhteiskunnan perustoimintojen kannalta kriittistä tai sivuston kaatumisella olisi suoria seurauksia reaalimaailmassa.

Headup-sivustolla uusien sisältöjen siirto sisällöntuotantoympäristöstä julkiseen kerrokseen vie noin 1–5 minuuttia sivuston koosta riippuen. Jos reaaliaikainen, dynaaminen sisällöntuotanto on sivustosi tärkein prioriteetti, saattaa Valu Muurilla vahvistettu tavanomainen sivusto olla paras ratkaisu.

Esimerkkejä erityisen kriittisistä organisaatioista ovat: energiayhtiöt, pankit, terveys- ja turvallisuusviranomaiset, hyvinvointialueet sekä suuret kunnat ja kaupungit.

Jos käytössäsi on tällä hetkellä Valun ylläpitämä WordPress-sivusto, Valu Muurin lisääminen on noin yhden työpäivän mittainen projekti. Headup-toteutus sen sijaan edellyttää sivuston rakentamista uudelleen aina alustaa myöten. Headup-ratkaisu kannattaakin ajoittaa sivustouudistuksen yhteyteen.

Aloita sivustosi vahvistaminen saman tien

Oletko jo Valu Digitalin verkkosivustoasiakas? Asiakkuuspäällikkösi tuntee sivustosi kuin omat taskunsa. Hän voi neuvoa esimerkiksi Valu Muurin käyttöönotossa. Sivustosi on todennäköisesti jo tänään erittäin toimintavarma, mutta paremmin suojautumalla varmistat, ettei hyökkäysten torjuntaan kulu ylimääräisiä resursseja. Valu Muurin pystyttäminen maksaa noin yhden asiantuntijatyöpäivän verran. Palvelun kuukausimaksu liikkuu tällä hetkellä sadoissa, ei tuhansissa euroissa.

Oletko uudistamassa sivustoasi? Verkkosivu-uudistuksen yhteydessä voidaan vaikuttaa teknisiin ratkaisuihin suunnittelusta ja sivuston toimintaperiaatteesta lähtien. Sivuston voi esimerkiksi rakentaa kybersodankestävänä Headup-toteutuksena. Erityisen kestävän sivuston tekemisen ei tarvitse tulla tavanomaista verkkosivustoprojektia kalliimmaksi.

Onko nykyinen sivustosi toisen palveluntarjoajan ylläpitämä? Teemme ulkopuolisia tietoturva-auditointeja verkkosivustoille ja annamme vinkit parempaan suojautumiseen. Voimme myös toteuttaa valmiussivuston kriisitilanteiden varalle erillisenä projektina.

Kun verkkosivusto on asiantuntevissa käsissä, kyberuhkien suhteen ei tarvitse menettää yöuniaan. Ota yhteyttä ja kysy lisää!


VALU