Tampereen yliopisto

Anna Kunnas

”CDN, MIKSI VÄLITTÄISIN?”

Sisällönjakeluverkon rooli sivustokehityksessä

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Elokuu 2022

TIIVISTELMÄ

Anna Kunnas: ”CDN, miksi välittäisin?” – Sisällönjakeluverkon rooli sivustokehityksessä
Kandidaattitutkielma
Tampereen yliopisto
Tietotekniikan tutkinto-ohjelma
Elokuu 2022

Sisällönjakeluverkko (Content Delivery Network, CDN) on monien suurten yritysten käyttämä palvelu, jolla pyritään nopeuttamaan verkkosivujen sisällön jakoa eri käyttäjien kesken. Erityisesti finanssi- ja verkkokauppa-alalla jopa lyhyillä häiriöajoilla voi olla suuret vaikutukset yrityksen tulokseen. Tutkielman tavoitteena on selvittää mitä hyötyjä ja haittoja sisällönjakeluverkon käytöllä voidaan olettaa olevan ja millaisia tietoturvauhkia tähän palveluun kohdistuu.

Tutkielma jakautuu kolmeen osaan. Ensimmäisessä osassa käydään läpi sisällönjakeluverkon rakennetta ja suurimpia toimijoita. Toisessa osassa perehdytään odotettuihin hyötyihin sekä siihen, miten sisällönjakeluverkko eroaa muista sisällönjakelumetodeista. Kolmannessa osassa selvitetään yleisimmät sisällönjakeluverkkoon kohdistuvat tietoturvauhkat, mutta ei perehdytä tarkemmin siihen, miten eri palveluntarjoajat ovat varautuneet näihin.

Tutkielman lopputuloksena voidaan todeta, että sisällönjakeluverkon käyttö ei automaattisesti korjaa verkkosivun nopeusongelmia tai poista palvelimiin liittyviä tietoturvauhkia, vaan on parhaimmillaan hyvin suunnitellulla ja toteutetulla verkkosivulla. Sisällönjakeluverkoilla on myös yleisesti enemmän resursseja suurien liikennemäärien käsittelyyn, mikä vähentää verkkosivun ylikuormittumisen riskiä. Sisällönjakeluverkkojen käyttöä hiertää kuitenkin edelleen kysymys yksityisyydestä ja yleisen tietosuoja-asetuksen noudattamisesta.

Avainsanat: sisällönjakeluverkko, CDN, tietoturva

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

AWS	Amazon Web Services
CCPA	California Consumer Privacy
CDN	Content Delivery Network
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DPI	Deep Packet Inspection
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
LAN	Local Area Network
Mbps	Megabits per second (megabittiä sekunnissa)
MIT	Massachusetts Institute Technology
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
QoS	Quality of Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
UDP	User Data Protocol
URL	Uniform Resource Locator
WAF	Web Application Firewall
WWW	World Wide Web
XSS	Cross-Site Scripting

1 JOHDANTO

World Wide Web, tai lyhyemmin WWW, on dokumentteja palvelimilta hakeva järjestelmä, joka mahdollistaa vierailut verkkosivustoilla. WWW kehitettiin Euroopan hiukkasfysiikan tutkimuskeskuksessa CERNissä brittiläisen tutkijan Tim Berners-Leen toimesta ja julkaistiin vuonna 1989. WWW hyödyntää prosessissaan Internetiä, joka on palvelimien ja protokollien muodostama verkko. Vaikka Internetin historia ulottuu 60-luvulle, jolloin Massachusetts Institute of Technologyssa (MIT) kehitettiin ensimmäinen sähköpostijärjestelmä, ei sen käyttö ollut vuosikymmeniin kovinkaan suurta. Arvioiden mukaan noin 0,5 % maailman populaatiosta käytti Internetiä vuonna 1990 ja vuoteen 2016 mennessä määrä oli kasvanut yli 3,4 miljardiin, eli noin 45,9 %:iin. Pääasiallinen kasvu tapahtui kuitenkin vuosien 2000–2016 välillä, suurilta osin erilaisten verkkosovellusten ja sosiaalisen median syntymisen myötä. (Roser et al., 2015) Vuoden 2016 jälkeen trendi on ollut alati kasvava ja yhä useammat ihmiset ympäri maailmaa käyttävät Internettiä. Vaikka Internet mahdollistaa WWW:lle sen tarvitseman infrastruktuurin ja WWW toimii sen päällä omana palvelunaan, nykypäivänä näitä kahta termiä käytetään usein toistensa synonyymina. Esimerkiksi englanninkielinen sana website käännetään usein (varsinkin puhekielessä) muotoon nettisivu, minkä etuosa viittaa Internettiin. Tästä terminologisesta ristiriidasta huolimatta nettisivu on vakiinnuttanut paikkansa suomen kielessä.

Nykypäivänä Internet nähdään osana ihmisoikeutta. Esimerkiksi Suomessa vuonna 2009 Liikenne- ja viestintäministeriö määritteli niin kutsutun yleispalvelulaajakaistan minimitasoksi yhden megabitin sekunnissa (Mbps). Myöhemmin tämä korotettiin kahteen megabittiin ja lopulta viiteen megabittiin vuonna 2021. Lakiasetuksen myötä jokaisella taloudella tulee olla mahdollisuus liittyä Internettiin, vaikka alueella ei olisi riittävästi kaupallista tarjontaa. (LVM, 2009, 2021) Tällaisilla asetuksilla jokaiselle yksilölle pyritään saamaan yhtäläiset oikeudet Internetin käyttöön, mutta samaan aikaan kun käyttäjien määrä kasvaa ja Internetin käyttö asettuu osaksi jokapäiväistä elämää, myös vaatimukset sen nopeuden ja tehokkuuden suhteen kiristyvät. Nykypäivänä verkkosivuilta ja -sovelluksilta odotetaan paljon: sisällön tulee latautua nopeasti ja käytön tulee olla sulavaa, aiheuttaen painetta palveluntarjoajille.

Sisällönjakeluverkko, joka tunnetaan paremmin kirjainyhdistelmästä CDN, on nimensä mukaisesti verkko, jonka tehtävänä on jakaa sisältöä hajautetusti mahdollisimman lähellä loppukäyttäjää. Verkkosivujen sisältöä on mahdollista jakaa monella tapaa, mutta sisällönjakeluverkon ideana on jakaa sisältöä mahdollisimman nopeasti, tehokkaasti ja luotettavasti. Ciscon vuonna 2019 tehdyn ennusteen mukaan sisällönjakeluverkko on tänä päivänä vastuussa 72 % Internet-

liikenteestä, kun vuonna 2017 se oli 56 % (Cisco, 2019). Sisällönjakeluverkon käyttö on siis nopeasti kasvava osa sivustokehitystä.

Kandidaattitutkielmassa perehdytään tarkemmin siihen mikä sisällönjakeluverkko on ja mitä hyötyjä se tuo sivustokehitykseen, sekä selvitetään, onko sisällönjakeluverkon käyttö kaikissa tilanteissa suotavaa ja mitä haittoja sen käyttöön saattaa liittyä.

Tutkielma on jäsennelty seuraavasti: luvussa 2 käydään läpi tutkimusmenetelmää ja sitä, mistä ja millä tavoin tietoa on etsitty. Luku 3 perehtyy tarkemmin siihen mikä sisällönjakeluverkko on, mistä se koostuu ja miten se eroaa toimintatavaltaan muista sisällönjakelumetodeista. Luvussa 4 päästään varsinaisiin sisällönjakeluverkon hyötyihin. Luku 5 puolestaan selvittää ovatko edellisessä kappaleessa mainitut hyödyt kaikissa tilanteissa haittoja suuremmat ja luku 6 tuo esiin vastakkaisia näkemyksiä alalta.

2 TUTKIMUSMENETELMÄ

Kandidaattitutkielman taustamateriaali pohjautuu pääosin aiempiin tutkimuksiin sekä alan ammattilaisen haastatteluun. Aineistoa on kerätty eri tietokannoista (Andor, ACM Digital Library) ja hauissa on käytetty muun muassa seuraavia hakusanoja:

- *cdn OR “content delivery network”*
- *website AND (cdn OR “content delivery network”)*
- *website AND speed AND (cdn OR “content delivery network”)*
- *speed AND (cdn OR “content delivery network”)*
- *security AND (cdn OR “content delivery network”)*

Koska sisällönjakeluverkon käyttö ei rajoitu ainoastaan verkkosivuihin, vaan sitä voidaan hyödyntää myös muun muassa videopeliteollisuudessa, hakusanat, jotka eivät sisältäneet sanaa ”website”, antoivat jonkin verran kandidaattitutkielman kannalta epäolennaisia tuloksia. Vapaammat hakukriteerit mahdollistivat kuitenkin laajemman otannan eri tietolähteitä.

Tutkimusaineiston lisäksi kandidaattitutkielmassa on käytetty Internetistä löytyviä artikkeleita, ottaen kuitenkin huomioon, etteivät ne ole vertaisarvioituja. Tämän vuoksi artikkeleita on valittu harkiten niin, että kirjoittajana on yleensä ollut iso ja tunnettu yritys tai yhdistys, mikä lisää sisällön luotettavuutta. Artikkeleiden valinnassa on myös huomioitu mahdollinen puolueellisuus, eikä joukkoon ole valittu esimerkiksi sellaista sisältöä, joka selkeästi mainostaisi yrityksen tarjoamien palvelujen ylivertaisuutta. On kuitenkin huomioon ottamisen arvoista, että kandidaattitutkielmassa on käytetty paljon Cloudflaren tarjoamaa dokumentaatiota ja

materiaalia sen selkeyden, helppolukuisuuden ja kattavuuden vuoksi. Valittu dokumentaatio on kuitenkin ollut yleistä tietoutta lähinnä tietoturvaan liittyen, eikä se ole sisältänyt varsinaista mainostekstiä Cloudflaren osalta.

3 SISÄLLÖNJAKELUVERKKO

3.1 Määritelmä ja historia

Sisällönjakeluverkko on nimensä mukaisesti verkko, jonka tehtävä on jakaa (lähinnä staattista) verkkosivujen sisältöä loppukäyttäjille mahdollisimman tehokkaasti ja nopeasti.

Sisällönjakeluverkon toiminta perustuu ympäri maailmaa sijoitettuihin palvelinklustereihin muodostaen verkon, jonka jokaisella palvelimella on kopio haetun verkkosivun tiedostoista. Palvelimen läheisyys pienentää tiedonsiirron viivettä ja mahdollistaa tiedostojen nopean jakamisen loppukäyttäjälle. Mikäli kopiota ei kuitenkaan löydy, haetaan se alkuperäiseltä palvelimelta. Tiedostojen kopioiminen palvelimille voi tapahtua joko loppukäyttäjän pyynnön yhteydessä tai ”puskemalla” ne verkkoon etukäteen. Kyseessä ei kuitenkaan ole globaali, kaikkien saatavilla oleva yhtenäinen verkko, vaan kaupallistettu palvelu, josta useimmiten maksetaan palveluntarjoajalle. Jokaisella palveluntarjoajalla on oma verkostonsa, jonka resursseja ne jakavat palvelun käyttäjille.

Sisällönjakeluverkon historia ulottuu 90-luvulle, jolloin MIT:n tutkimusryhmä yritti löytää ratkaisua verkkosivujen liikennepiikkeihin. Tästä syntyi vuonna 1998 Akamai, joka on edelleen yksi suurimmista sisällönjakeluverkkopalveluja tarjoavista yrityksistä. Ensimmäiset sisällönjakeluverkot keskittyivät vain staattisen sisällön jakamiseen, mutta nykypäivän modernit sisällönjakeluverkot pyrkivät jakamaan myös dynaamista sisältöä. Dynaamisella sisällöllä viitataan käyttäjään henkilökohtaisesti mukautuvaan verkkosisältöön. (Buyya et al., 2008)

3.2 Rakenne

Sisällönjakeluverkko on yksinkertaisuudessaan edustapalvelin (engl. reverse proxy), joka välittää HTTP-pyyntöjä ja -vastauksia asiakaskoneen ja kohdepalvelimen välillä (Cloudflare, 2022c). HTTP (Hypertext Transfer Protocol) on verkkoselaimien ja verkkopalvelimien väliseen viestintään suunniteltu protokolla, joka mahdollistaa hypermediadokumenttien kuten HTML-tiedostojen lähettämisen (MDN, 2022). Sisällönjakeluverkon tapauksessa välissä toimiva edustapalvelin lisäksi tallentaa välittämäänsä sisältöä välimuistiin, josta sitä on helppo ja nopea jakaa seuraaville, samaa sisältöä pyytäville asiakaskoneille. Tietoliikenteen viiveiden minimoimiseksi palvelimet tulee tuoda mahdollisimman lähelle loppukäyttäjiä, mikä vaatii palveluntarjoajalta laajalle hajautetun palvelininfrastruktuurin.

3.3 Suurimmat toimijat

Suurimpia CDN-toimijoita ovat tällä hetkellä Cloudflare, Amazon Web Services ja Akamai. Intricatelyn tuottamassa raportissa analysoitiin 2,6 miljoonaa yritystä, joista noin miljoona käytti Cloudflarea, 190 000 AWS:ää, 50 000 Akamaita ja loput muita, pienempiä toimijoita. Vaikka Akamailla on näistä kolmesta vähiten käyttäjiä, sen liikevaihto kattaa suuren osan koko alan liikevaihdosta. Akamai on ensimmäinen sisällönjakeluverkkopalveluja tarjoava yritys, jolla on vahva jalansija suurten ja tunnettujen yritysten keskuudessa. Cloudflaren asiakaskunta koostuu enimmäkseen pienistä ja keskisuurista yrityksistä, sillä yritys on yksi harvoista CDN-toimijoista, joka tarjoaa palveluaan myös ilmaiseksi. Tämä tekee Cloudflaresta houkuttelevan vaihtoehdon muun muassa startupeille. (Intricately, 2020)

4 SISÄLLÖNJAKELUVERKON HYÖDYT

4.1 Nopeus

Data kulkee valokuidussa noin 31 % hitaammin kuin valonnopeus, eli noin 207 miljoonaa metriä sekunnissa (Poletti et al., 2013). Toisin sanoen viesti Kiinan itärannikolta Argentiinan veisi ideaalista reittiä pitkin noin 90 millisekuntia. Puhutaan siis latenssista tai viiveestä, joka datalla kestää kulkea paikasta A paikkaan B. Tällainen viive ei välttämättä kuulosta pahalta, mutta Akamain vuonna 2017 tehdyn tutkimuksen mukaan verkkosivujen latausnopeuksista puhuttaessa jopa millisekunnit ovat kriittisiä.

- 100 millisekunnin viive verkkosivun lataamisessa huonontaa konversioarvoa 7 prosentilla. Konversioarvolla viitataan siihen, kuinka moni potentiaalisista asiakkaista saadaan vuorovaikuttamaan sivuston kanssa. Vuorovaikutus voi liittyä esimerkiksi suoritettuun ostotapahtumaan tai lomakkeen täyttämiseen.
- Kahden sekunnin viive verkkosivun lataamisessa nostaa poistumisprosenttia 103:lla. Poistumisprosentilla viitataan prosentuaaliseen osuuteen niistä loppukäyttäjistä, jotka vierailevat sivulla, mutta poistuvat ilman vuorovaikutusta.
- 53 prosenttia mobiilikäyttäjistä poistuu sivulta, mikäli lataaminen kestää enemmän kuin kolme sekuntia.
- Poistumisprosentti oli suurin mobiilikäyttäjillä ja pienin tablettikäyttäjillä.

Tutkimusdataa kerättiin yhden kuukauden ajan SOASTA:n toimesta (nykyään osa Akamaita) ja se sisälsi noin 10 miljardia anonyymia verkkovierailua suurimpien verkkokauppiaiden sivustoilla. (Akamai, 2017) Tämän vuoksi monet yritykset luottavat sisällönjakeluverkkojen kykyyn tarjoilla sisältöä asiakkailleen nopeasti.

CDNPerf kerää ja analysoi päivittäin yli 300 miljoonaa testiä, joilla seurataan eri palveluntarjoajien suorituskykyä. Suorituskykytestissä tarkastellaan HTTP-pyyntöjen kyselyaikojen mediaaneja eri palveluntarjoajilla, kun käyttäjä lataa 500 bitin kuvan. Cloudflarella, AWS:llä ja Akamailla tämä vaihteli kesäkuussa 25–30 ms välillä (CDNPerf, 2022). Kyse on siis yhdestä HTTP-pyynnöstä, mutta kokonaisen verkkosivun lataamiseksi HTTP-pyyntöjä on yleensä tehtävä enemmän. Kuvitellaan yksinkertaistettu tilanne, jossa Kiinan itärannikolla sijaitseva käyttäjä haluaa tarkastella Argentiinassa sijaitsevaa verkkosivua, joka sisältää kolme lisätiedostoa (esimerkiksi kuvia):

1. Kiinassa olevan asiakaskoneen on ensin muodostettava TCP/IP-yhteys Argentiinassa olevan kohdepalvelimen kanssa, joka vaatii yhteensä kolme matkaa kohteiden välillä: **90 ms + 90 ms + 90 ms = 270 ms**.
2. Tämän jälkeen asiakaskone lähettää varsinaisen HTTP-pyynnön: **270 ms + 90 ms = 360 ms**.
3. Kohdepalvelin vastaa asiakkaalle, sisältäen listan kaikista muista tarvittavista tiedostoista: **360 ms + 90 ms = 450 ms**.
4. Asiakaskone pyytää kohdepalvelimelta loput tarvittavat tiedostot: **450 ms + 90 = 540 ms**.
5. Kohdepalvelin lähettää loput tiedostot asiakaskoneelle asynkronisesti (samanaikaisesti): **540 ms + 90 ms = 630 ms**.

Koko prosessi verkkosivun lataamiseksi vie siis 630 ms, sillä datan on matkustettava jokaisessa välissä maapallon toiselle puolelle. Saatu tulos ei ole tavaton, sillä kokonaisen verkkosivun lataaminen voi viedä useamman sekunnin. Esimerkissä käytettiin kuitenkin aikaa, joka datalla kestää kulkea häiriöttömästi äärettömän kaistanleveyden omaavassa valokuidussa, jossa tiedostojen koko ei vaikuta tiedonsiirtonopeuteen. Todellisuudessa matka-aikaan vaikuttaa kuitenkin lähiverkon (LAN) liikenne, solmujen määrä ja niiden ruuhkautuminen, palvelimen vasteaika, reitin todellinen pituus sekä suurten tiedostojen kohdalla kaistanleveys (Cloudflare, 2022d). Mikäli käytössä olisi ollut sisällönjakeluverkko, jonka palvelin sijaitsisi esimerkiksi keskellä Intiaa, olisi lopputulos ollut huomattavasti nopeampi. Matka-aika Kiinan itärannikon ja Intian välillä on noin 2 ms. Kun aiemmin mainittuihin kaavoihin sijoittaa 90 ms tilalle 2 ms, lopputulokseksi saadaan 14 ms. CDNPerfin tulosten perusteella tällainen nopeus ei ole realistinen, mutta kuvastaa millainen teoreettinen vaikutus lähempänä sijaitsevalla palvelimella on, kun verkkosivun koko ja tiedostojen määrä kasvaa. Kun HTTP-pyyntöjä on tehtävä enemmän, myös kokonaismatka-aika kasvaa nopeasti.

Sisällönjakeluverkot myös tallentavat tietoa välimuistiin ottaen huomioon, kuinka suositusta sivustosta on kyse: suosituimpien sivustojen sisältö tallennetaan muistiin ja vähemmän suosittujen pidemmän vasteajan kiintolevylle, josta ne haetaan tarpeen tullen (Ghaznavi et al., 2021).

4.2 Saatavuus

Välimuistin hyödyntäminen sisällönjakeluverkkojen palvelimissa mahdollistaa verkkosivulla vierailun silloinkin, kun alkuperäinen palvelin on hetkellisesti alhaalla. Esimerkiksi Cloudflare tarjoaa palveluilleen 100 % saatavuuden, eli mikäli verkkosivu ei ole saatavilla CDN:n käytöstä huolimatta ja katkos ei aiheudu asiakkaasta, asiakas voi hakea korvauksia menetetyltä ajalta (Cloudflare, 2022a). 100 % saatavuuden tarjoaminen on jokseenkin poikkeuksellista, sillä monilla palveluntarjoajilla vastaava luku on 99,50–99,90 %.

Välimuistin osumatarkkuus kertoo prosentteina, kuinka usein haettu sisältö löytyy suoraan välimuistista. Tämä on sisällönjakeluverkoille tärkeä suorituskykyindikaattori, joka vaihtelee pääosin staattisilla verkkosivuilla yleensä 95–99 % välillä. Mitä suurempi kyseinen luku on, sitä tehokkaammin palvelimet kykenevät tarjoilemaan sisältöä loppukäyttäjälle. (Cloudflare, 2022h)

4.3 Skaalautuvuus

Suunniteltaessa verkkosivustoa on tärkeää analysoida mahdollisia loppukäyttäjiä ja tulevaisuuden kasvutarpeita. Tulevatko loppukäyttäjät todennäköisimmin yhdeltä tietyltä alueelta vai ympäri maailmaa? Onko mahdollista, että loppukäyttäjien määrä kasvaa huomattavasti tulevaisuudessa? Sisällönjakeluverkko tarjoaa käyttäjilleen automaattisesti skaalautuvan palvelun, jolloin loppukäyttäjät ympäri maailmaa pyritään palvelemaan mahdollisimman pienellä viiveellä.

Sisällönjakeluverkon skaalautuvuus mahdollistaa verkkosivun nopean ja tehokkaan tarjoilun loppukäyttäjille riippumatta siitä, missä loppukäyttäjät sijaitsevat ja kuinka monta heitä on. Tämä puolestaan vähentää kotipalvelimen kuormaa sekä sivustonkehittäjän tarvetta suunnitella palvelun skaalautumista itse.

4.4 Verkkohyökkäysten torjunta

Koska sisällönjakeluverkot ovat tänä päivänä vastuussa hyvinkin suuresta määrästä verkkoliikennettä, niiden tulee olla valmiita reagoimaan mahdollisiin tietoturvauhkiin, kuten DDoS-hyökkäyksiin (Distributed Denial-of-Service), XSS-hyökkäyksiin (Cross-Site Scripting) ja SQL-injektioihin (Structured Query Language). Erityisesti taloudellisesta näkökulmasta hyökkäyksiltä suojautuminen on äärimäisen tärkeää. Ponemon Instituutin vuonna 2016 tekemän tutkimuksen mu-

kaan suurin osuus häiriöajan aiheuttamista kuluista liittyi yrityksen mainevaurioihin ja asiakkaiden vaihtuvuuteen. Tämän jälkeen tulivat varsinainen tulojen menetys sekä loppukäyttäjän ja yrityksen sisäisen tuottavuuden heikentyminen. Suurimmat tappiot kohdistuivat finanssialan yrityksiin ja jokainen minuutti vastasi keskimäärin 9000 dollarin menetystä. (Ponemon, 2016)

Yksi sisällönjakeluverkkojen etu on niiden massiivinen verkkokapasiteetti, joka puolestaan on hyödyksi erityisesti DDoS-hyökkäyksiltä suojautumisessa. Distributed Denial-of-Service viittaa hajautettuun palvelun saatavuuden estämiseen. DDoS-hyökkäyksen tarkoituksena on kaataa verkkosivu ohjaamalla siihen mahdollisimman paljon liikennettä hyvin lyhyen ajan sisällä, jolloin yksittäisellä palvelimella ei ole mahdollisuutta reagoida kaikkiin pyyntöihin, aiheuttaen palvelussa ”tukoksen”. (Cloudflare, 2022b)

DDoS-hyökkäyksiä on montaa eri tyyppiä, jotka kohdistuvat OSI-mallin kolmeen eri kerrokseen: verkko- (3), kuljetus- (4) tai sovelluskerrokseen (7) (Cloudflare, 2022b). OSI-malli kuvaa seitsemää eri kerrosta, joita tietokoneet käyttävät kommunikoidessaan Internetin välityksellä.

- Sovelluskerroksen tehtävänä on tarjota protokollia, joiden avulla sovellus voi lähettää ja vastaanottaa dataa, sekä välittää oleellista tietoa käyttäjälle. Yleisimpiä protokollia ovat muun muassa HTTP, FTP (tiedostojen siirto palvelimelta toiselle), SMTP (sähköpostin välittäminen) ja DNS (käännös verkkotunnuksen ja IP-osoitteen välillä).
- Kuljetuskerroksen tehtävänä on pilkkoa dataa lohkoihin lähetystä varten ja koota ne yhteen vastaanottavassa päässä, sekä vastata tietovuonohjauksesta ja virheiden hallinnasta. Kuljetuskerros varmistaa, että dataa lähetetään sopivalla taajuudella suhteessa vastaanottavaan laitteeseen ja vastaanotettu data on virheetöntä.
- Verkkokerroksen tehtävänä on pilkkoa kuljetuskerroksen datalohkot pienempiin verkkopaketteihin lähetystä varten ja koota ne yhteen vastaanottavassa päässä, sekä valita paras (nopein) fyysinen reitti niiden kuljetusta varten. (Imperva, 2022)

Hyökkäykset voivat olla yhtä tyyppiä tai monen tyypin yhdistelmä. Yleisiä DDoS-hyökkäyksiä ovat muun muassa HTTP flood, SYN (synchronization) flood, UDP (User Datagram Protocol) flood ja ICMP (Internet Control Message Protocol) flood.

- Sovelluskerroksen hyökkäykset liittyvät HTTP GET ja HTTP POST metodien käyttöön. Hyökkäyksen tarkoituksena on ylikuormittaa palvelimen pisteeseen, jossa se ei enää kykene reagoimaan jokaiseen pyyntöön, aiheuttaen verkkosivun kaatumisen.

- Kuljetuskerroksen toimintaa voidaan häiritä SYN floodilla tai UDP floodilla. SYN flood hyödyntää kahden laitteen välistä yhteyttä muodostettaessa tapahtuvaa kättelyä, jolla varmistetaan osapuolten valmius tiedonsiirtoa varten. Normaalissa kättelyssä asiakaskone lähettää palvelimelle SYN-paketin pyytäen yhteyden muodostamista. Palvelin vastaa tähän pyyntöön SYN/ACK-paketilla (synchronization/acknowledgement), jääden odottamaan asiakaskoneelta lopullista ACK-pakettia, jonka jälkeen yhteys on muodostettu. SYN floodissa hyökkääjä lähettää jatkuvasti uusia SYN-paketteja ilman viimeistä ACK-pakettia, avaten uusia portteja yhteyspyynnön käsittelyä varten, kunnes palvelimella ei ole enää vapaita portteja muita yhteyksiä varten. UDP floodissa hyökkääjä hyödyntää palvelimen toimintatapaa, jossa jokaista vastaanotettua UDP-pakettia kohden palvelimen täytyy erikseen tarkistaa, kuunteleeko jokin sovellus annettua porttia. Koska kyseessä on hyökkäys, tarkistukset ovat luonnollisesti turhia ja vievät resursseja palvelimelta. Kun pyyntöjä tulee tarpeeksi, palvelin ei enää kykene vastaamaan jokaiseen niistä. (Cloudflare, 2022e, 2022f)
- Verkkokerroksen hyökkäys voidaan toteuttaa ICMP floodilla, joka tunnetaan myös nimellä ping flood. ICMP flood hyödyntää echo-request ja echo-reply viestejä, joilla normaalisti diagnosoidaan verkkolaitteen yhteyttä ja tilaa. Jokaista lähetettyä echo-requestia kohden palvelin lähettää yhden echo-reply viestin, joka vaatii sekä palvelinresursseja että kaistanleveyttä. (Cloudflare, 2022g)

Koska DDoS-hyökkäyksen ja aidon liikennepiikin erottaminen voi olla haastavaa, myös torjuntatapojen tulee olla hienostuneita. Liikenteen katkaiseminen kokonaan liikennepiikin ilmaantuessa tai liikenteenteen rajoittaminen tiettyyn määrään tiettyä aikaikkunaa kohden voi toimia pienillä sivustoilla, mutta esimerkiksi uusien tuotteiden aiheuttama asiakasryntäys verkkokauppasivustolle tulisi pyrkiä sallimaan samalla, kun palvelu valvoo mahdollisia DDoS-hyökkäyksiä. Eri palveluntarjoajilla on omat ratkaisunsa DDoS-hyökkäyksiltä suojautumiseen, eikä tässä kandidaattitutkielmassa perehdytä niihin tarkemmin.

4.5 Helppous

Verkkosivustojen rakentaminen on nykypäivänä helppoa erilaisten selaimessa toimivien graafisten käyttöliittymien ansiosta. Tunnetuimpia näistä lienevät Wix, Shopify, Squarespace ja WordPress. Sivustokehittäjältä ei siis välttämättä vaadita kovinkaan vahvaa teknistä osaamista, jolloin myös laitteisto- ja tietoturvakysymykset voidaan haluta ulkoistaa kolmannelle osapuolelle. Tähän sisällönjakeluverkko soveltuu hyvin, sillä palvelimet on konfiguroitu tarjoilemaan verkkosivuja

mahdollisimman nopeasti ja tehokkaasti, ottamalla samalla huomioon mahdolliset tietoturvakysymykset.

4.6 Erot muihin sisällönjakelumetodeihin

Verkkosivujen sisältöä on mahdollista jakaa käyttäjille monella eri tavalla, mutta sisällönjakeluverkko nähdään usein helpoimpana vaihtoehtona niin kehittäjän kuin loppukäyttäjänkin näkökulmasta. Vuonna 2015 kirjoitetussa artikkelissa vertailtiin sisällönjakeluverkkoa muihin tekniikoihin, joilla kaikilla oli jotain yhteistä sisällönjakeluverkon kanssa.

Palvelinklusteri on joukko palvelimia, jotka on yhdistetty samaan välittäjäpalvelimeen. Välittäjäpalvelimen tehtävä on välittää siihen saapuvat HTTP-pyynnöt eri palvelimille. Yleensä jokainen näistä palvelimista sisältää saman sisällön, jolloin yksittäisen palvelimen häiriöt eivät vaikuta verkkosivun toimivuuteen, sillä pyynnöt voidaan ohjata toisille palvelimille. Ratkaisu lisää systeemin saatavuutta sekä luotettavuutta ja klusterointi on usein kustannustehokkaampi vaihtoehto kuin yksittäinen tehokas palvelin. Palvelinklustereiden käyttö ei kuitenkaan vähennä latenssia, sillä palvelimet sijaitsevat yleensä vain tietyllä maantieteellisellä alueella.

Asiakaspuolen välimuistia voidaan hyödyntää tallentamalla verkkosivun sisältöä suoraan verkkoselaimen välimuistiin. Vaikka ratkaisu vähentää latenssia ja kaistanleveyden tarvetta, vaatii se myös välimuistin rajallisen määrän takia tehokkaita välimuistin korvausalgoritmeja. Ratkaisu myös tyydyttää vain yksittäisen asiakkaan tarpeet, välimuistin osumatarkkuus voi vaihdella, eikä sisällöntarjoajilla ole keinoa hallita mitä välimuistiin tallennetaan.

Välimuistipalvelimen välimuistia voidaan hyödyntää tallentamalla verkkosivun sisältöä suoraan palvelimen välimuistiin. Ratkaisu vähentää latenssia ja tyydyttää asiakaspuolen välimuistista poiketen useamman asiakkaan tarpeet, mutta myös tässä osumatarkkuus voi vaihdella eikä sisällöntarjoajalla ole keinoa hallita mitä välimuistiin tallennetaan. Lisäksi välimuistipalvelimessa esiintyvät häiriötilat estävät kokonaan pääsyn verkkosivulle.

Peilauksessa alkuperäisen palvelimen sisältö kopioidaan täydellisenä toiseen, lähempänä asiakasta sijaitsevaan palvelimeen. Ratkaisu on siis hyvin samanlainen kuin sisällönjakeluverkko, sillä se parantaa latenssia, mutta vaatii suuren infrastruktuurin. Identtisten kopioiden ylläpito saattaa kuitenkin olla aikaa vievää ja kallista suhteessa saatuun hyötyyn.

Multihomingissa yksi palvelin muodostaa yhteyden Internetiin useammalla yhteydellä. Tämä voidaan toteuttaa joko yhdellä Internet-palveluntarjoajalla, jolla on useita yhteyksiä, tai usealla Internet-palveluntarjoajalla. Ratkaisulla mahdollisestaan yhteyksille useampia reittejä, jolloin yhden epäonnistuminen ei vaikuta

koko yhteyden onnistumiseen. Tämä puolestaan parantaa vasteaikaa ja suorituskykyä. Ongelmana on kuitenkin sisällön sijaitseminen yksittäisellä palvelimella, mahdollinen päällekkäisyys eri Internet-tarjoajien reiteissä sekä useamman yhteyden ylläpitokustannukset.

Vertailun perusteella näiden tekniikoiden suurimmiksi ongelmiksi muodostuivat latenssi sekä huono skaalautuvuus ja hinta-laatusuhde. (Gupta et al., 2015)

5 OIKOTIE ONNEEN?

Vuonna 2022 sisällönjakeluverkon markkina-arvoksi arvioitiin 19,2 miljardia dollaria ja vuonna 2027 mennessä sen odotetaan nousevan 34,5 miljardiin dollariin. Lisääntynyt kysyntä rikkaalle sisällölle, jatkuvasti lisääntyvä käyttäjien määrä sekä digitalisaation kasvu organisaatioissa lisäävät väistämättä sisällönjakeluverkon kysyntää sekä kasvattavat sen markkina-arvoa. (MarketsandMarkets, 2022) Samalla kuitenkin huoli sisällönjakeluverkon kyvystä vastata tietoturvauhkiin ja muun muassa Euroopan Unionin asettamaan yleiseen tietosuoja-asetukseen kasvaa. Esimerkiksi vuonna 2017 Cloudbleed nimen saanut haavoittuvuus aiheutti salasanojen ja yksityisviestien vuotamisen kolmansille osapuolille. Kokonaisuudessaan tietoturvaongelma vaikutti 120 000 verkkosivuun, joiden joukossa oli isoja yrityksiä kuten Uber, Fitbit ja OKCupid. (Anon, 2017)

Sisällönjakeluverkkoja tarjoavien yritysten negatiivisia puolia ja tietoturvakysymyksiä ei ole juurikaan tutkittu, mikä herättää luonnollisestikin huolen siitä, onko esimerkiksi arkaluonteisen materiaalin luovuttaminen näihin verkkoihin turvallista. Vuonna 2021 julkaistussa artikkelissa selvitettiin sisällönjakeluverkkoihin mahdollisesti kohdistuvia tietoturvauhkia sekä niiden vaikutuksia palveluntarjoajan verkostoon, palvelun tilaajan palvelimeen sekä loppukäyttäjään (Ghaznavi et al., 2021).

5.1 Yleisiä uhkia

Sisällönjakeluverkot varautuvat yleisiin sovelluskerroksen tietoturvauhkiin muun muassa kieltämällä kokonaan HTTP POST -metodin käytön, asettamalla epäilyttäviä käyttäjiä väliaikaiselle sulkulistalle ja/tai turvautumalla palomuuriin, jonka tehtävänä on tutkia jokainen lähetetty HTTP-pyyntö ja -vastaus. Palomuurin suodatinkonfiguraatio perustuu usein OWASPin (Open Web Application Security Project) vapaasti tarjoamaan 10 kriittisimmän tietoturvariskin mukaiseen listaan. Tietyn HTTP-metodin kieltäminen kokonaan vähentää sisällönjakeluverkon joustavuutta ja HTTP-pyyntöjen sekä -vastausten tarkastelu puolestaan vaatii pakettien syvällisempää tutkimista (Deep Packet Inspection, DPI), vieden resursseja, kasvattaen viivettä sekä nostaen esiin huolen loppukäyttäjien yksityisyydestä ja

mahdollisesta tietojen myymisestä markkinointiyrityksille. Lisäksi palomuurin asentaminen jokaiseen sisällönjakeluverkon palvelimeen vie osaltaan resursseja itse verkolta. (Ghaznavi et al., 2021)

5.2 Haitallisen koodin piilotus salattuun liikenteeseen

Nykypäivänä suuri osa Internetissä tapahtuvasta liikenteestä on tavalla tai toisella salattua. Salatun viestin purku tapahtuu salaisen avaimen avulla. Ilman salaista avainta sisällönjakeluverkko pystyy tutkimaan ja analysoimaan ainoastaan liikenteen ei-salattuja osioita ja tekemään tämän perusteella päätöksiä siitä, onko sisältö mahdollisesti haitallista. Jotta sisällönjakeluverkon olisi mahdollista tutkia myös salatun liikenteen sisältöä, on palvelun käyttäjän luotettava palveluntarjoajaan salaisen avaimen luovuttamiseksi. Tämä antaa palveluntarjoajalle käytännössä mahdollisuuden toimia niin sanottuna mies välissä -hyökkääjänä, kuunnellen kaikkea liikennettä asiakaskoneen ja kohdepalvelimen välissä. Sisällönjakeluverkkojen on siis hyvin vaikeaa tarjota samanaikaisesti sekä suojaa että yksityisyyttä, joka noudattaa muun muassa GDPR:n (General Data Protection Regulation) ja CCPA:n (California Consumer Privacy) asettamia vaatimuksia. (Ghaznavi et al., 2021)

5.3 Välimuistin saastuttaminen

Sisällönjakeluverkon koko idea perustuu hyvin toimivaan välimuistiin, jonka osumatarkkuussuhde on mahdollisimman suuri. Välimuistin saastuttamisessa hyökkääjän tavoitteena on korvata suosittu sisältö epäsuositulla sisällöllä, huonontaen näin palvelimen osumatarkkuussuhdetta ja sisällönjakeluverkon palvelun laatua (Quality of Service, QoS). Palveluntarjoajat pyrkivät estämään tällaisia hyökkäyksiä seuraamalla erinäisten kynnysarvojen täyttymistä. Koska kynnysarvot saattavat kuitenkin täyttyä myös aidoilla käyttäjillä, on tärkeää, että tästä aiheutuvat toimenpiteet ovat väliaikaisia. (Ghaznavi et al., 2021)

5.4 Välimuistin myrkyttäminen

Verkkosivun hakeminen välimuistista tapahtuu välimuistiavaimen avulla. Kun asiakaskone pyytää palvelimelta tiettyä verkkosivua, palvelin tarkistaa, vastaako HTTP-pyynnön otsikot välimuistissa olevia välimuistiavaimia. Mikäli kyllä, palvelin tarjoilee asiakaskoneelle suoraan välimuistissa olevan tallennetun vastauksen. Muussa tapauksessa palvelin hakee vastauksen alkuperäiseltä palvelimelta. Välimuistiavain perustuu yleensä muutamaan otsikkoon, joiden yhdistelmä muodostaa avaimen. Välimuistin myrkyttämisessä hyökkääjä hyödyntää niitä otsikoita, jotka eivät kuulu välimuistiavaimeen, sillä palvelin ei tarkista niiden oikeellisuutta. Hyökkääjä voi lisätä ylimääräiseen otsikkoon esimerkiksi skriptin, joka tallentuu

HTTP-pyynnön ohella välimuistiin. Kun seuraava asiakaskone pyytää samaa verkkosivua, hänelle tarjoillaan suoraan välimuistista hyökkääjän myrkyttämä vastaus. Välimuistin myrkyttämiseltä voidaan suojautua esimerkiksi käyttämällä välimuistiavaimessa tunnettuja myrkytyksessä käytettäviä otsikoita. Samalla pidemmät välimuistiavaimet vievät kuitenkin enemmän tilaa palvelimilla. (Ghaznavi et al., 2021)

5.5 Välimuistin huijaus

Välimuistin huijauksessa hyökkääjä huijaa loppukäyttäjän pyytämään staattista sisältöä arkaluontoiselta verkkosivulta URL-osoitteesta, jota ei ole olemassa, esimerkiksi www.pankki.fi/profiili/foo.jpg. Mikäli verkkosivua ei ole toteutettu käsittelemään odottamattomia URL-osoitteita esimerkiksi palauttamalla HTTP 404 tai estämällä välimuistiin tallentamisen kokonaan, kohdepalvelin palauttaa arkaluontoiset tiedot osoitteesta www.pankki.fi/profiili. URL-osoitteen päätteen vuoksi välissä toimiva sisällönjakeluverkon palvelin pitää pyyntöä normaalina staattisen sisällön pyyntönä ja tallentaa vastauksen välimuistiin. Tämän jälkeen hyökkääjä lähettää palvelimelle pyynnön samalla URL-osoitteella kuin uhri, saaden suoraan pääsyn arkaluontoisiin tietoihin. Hyökkäyksen torjunnassa myös palveluntarjoajalla on vastuu olla tallentamatta välimuistiin arkaluontoista sisältöä. (Ghaznavi et al., 2021)

5.6 HTTP-salakuljetus

Riippuen konfiguraatioista palomuuri (WAF) ja sisällönjakeluverkon palvelin saattavat käsitellä HTTP-pyyntöjen otsikoita eri tavalla. Tällöin hyökkääjän on mahdollista salakuljettaa yksittäisen HTTP-pyynnön sisällä toinen HTTP-pyyntö hyödyntämällä Content-Length ja Transfer-Encoding otsikoita. Content-Length kertoo (biteissä) pyynnön varsinaisen datan pituuden. Transfer-Encoding ja sen kanssa käytetty chunked avainsana puolestaan kertoo, että varsinainen data lähetetään paloina, joista jokainen on tietyn pituinen, ja koko data päättyy nollaan. Esimerkiksi jos HTTP-pyyntö sisältää kaksi eriävää Content-Length otsikkoa (0 ja 45), WAF saattaa priorisoida näistä suuremman. Tällöin haitallinen HTTP GET -pyyntö kulkeutuu WAFin ohi toisen HTTP-pyynnön datana. Kun pyyntö saavuttaa sisällönjakeluverkon palvelimen, palvelin saattaa priorisoida kahdesta Content-Lengthistä pienemmän, jolloin se tulkitsee molemmat HTTP-pyynnöt erillisiksi (nolla tarkoittaa, että pyynnöllä ei ole varsinaista dataa). Haitallinen HTTP-pyyntö pääsee siis palomuurin ohi kohdepalvelimelle, ja palvelin palauttaa hyökkääjälle ensimmäistä pyyntöä vastaavan (ei-haitallisen) vastauksen. Kun seuraava henkilö pyytää samaa verkkosivua kuin hyökkääjä, palvelin palauttaa vastauksena salakuljetetun haitallisen pyynnön vastauksen. Mikäli kaikki HTTP-

pyyntöjä käsittelevät osapuolet noudattaisivat RFC 7230 -standardia, ongelmia ei syntyisi. (Ghaznavi et al., 2021) Esimerkiksi kun Transfer-Encoding otsikko on käytössä, Content-Length otsikkoa ei tulisi huomioida, tai kun HTTP-pyyntö sisältää kaksi eriävää Content-Length otsikkoa, koko HTTP-pyyntö tulisi hylätä (Fielding & Reschke, 2014).

Yllä mainitut ovat vain osa sisällönjakeluverkkoihin kohdistuvista tietoturvauhkista, eikä tässä kandidaattitutkielmassa ole lähdetty selvittämään tarkemmin, miten jokainen palveluntarjoaja on varautunut kyseisiin ongelmakohtiin. On kuitenkin hyvä tiedostaa, että suurista infrastruktuureista ja resursseista huolimatta myös sisällönjakeluverkot ovat alttiita kyseisille hyökkäyksille, eikä sisällönjakeluverkon käyttö ole automaattinen oikotie onneen.

6 ALAN AMMATTILAISEN NÄKÖKULMA

Kandidaattitutkielmaa varten haastateltiin Seravo Oy:n teknologiajohtajaa Ville Korhosta. Seravo tarjoaa maailman nopeinta hosting-palvelua WordPress-sivustoille, mutta ei hyödynnä tekniikassaan sisällönjakeluverkkoa (Viscomi, 2022). Halusin selvittää, miksi näin on ja miten alan ammattilainen näkee sisällönjakeluverkot ja niiden tarpeellisuuden: onko sisällönjakeluverkon hyödyntäminen kaikissa tilanteissa kannattavaa ja mitä haittapuolia näiden palvelujen käytöllä mahdollisesti on.

Korhosen mukaan verkkosivujen nopeuteen liittyvä pullonkaula aiheutuu useimmiten huonosti toteutetusta verkkosivusta, jota sisällönjakeluverkon käyttö ei korjaa. Tällöin palvelimen sijainnilla ei juurikaan ole väliä, sillä latenssin suhde itse verkkosivun toimintanopeuteen on pieni. Sisällönjakeluverkko on parhaimmillaan hyvin toteutetulla verkkosivulla, joka sisältää paljon staattista sisältöä. Tämä kuitenkin on nykypäivänä entistä harvinaisempaa, sillä monet verkkosivut mukautuvat esimerkiksi maantieteellisiin sijainteihin ja siihen, onko käyttäjä kirjautunut sisään vai ei. Korhosen myös huomauttaa, että käytettäessä sisällönjakeluverkkoa kaikki liikenne kulkee palveluntarjoajan kautta, jolloin mahdollisissa häiriötilanteissa hosting-yrityksen mahdollisuudet tilanteen selvittämiseksi ja korjaamiseksi ovat rajalliset. Lisäksi välimiespalvelimen vuoksi loppukäyttäjä tai hosting-yritys eivät voi varmistua siitä, että tieto kulkisi koko matkan salattuna.

Seravon tarjoaman palvelun nopeus perustuu WordPress-sisällönhallintajärjestelmään optimoituun infrastruktuuriin, joka ei hyödynnä olemassa olevien teknologiajättien pilvipalveluita, vaan omassa hallinnassa olevia tehokkaita palvelintietokoneita. Välistä on siis pyritty karsimaan turhat välikädet. Tämän lisäksi

Seravon palveluun on kuulunut HTTP-tason välimuisti jo vuodesta 2014. Esimerkki tehokkaasti onnistuneesta sisällönjaosta oli Koronavilkkuun liittyvä verkkosivu, jolla vieraili yhden päivän aikana 935 000 kävijää. Suurin liikennepiikki osui iltapäivään, jolloin tunnin aikana sivustolla vieraili 150 000 kävijää.

Korhosen mukaan sisällönjakeluverkon tekniikka ei ole uutta, vaan sen toiminta perustuu samaan kuin minkä tahansa muun palvelimen. Palveluna modernit sisällönjakeluverkot kuitenkin tarjoavat suuren infrastruktuurin ja lisäpalveluita, joiden toteuttaminen itse voidaan kokea hankalana. Erityisesti kokemattoman sivustokehittäjän näkökulmasta nopeusoptimointiin liittyvien palvelujen tilaaminen yhdeltä ja samalta palveluntarjoajalta voidaan nähdä kustannustehokkaana ja vaivattomana ratkaisuna.

Sisällönjakeluverkon kysyntä kasvoi suuresti erityisesti koronapandemian aikana etätyövelvoitteen ja suoratoistopalvelujen suosion kasvamisen myötä. Tämä tarkoitti samalla verkkoliikenteen keskittymistä yhä suuremmassa osin muutamille tunnetuille CDN-toimijoille, joka Korhosen mukaan vähentää verkkoliikenteen hajautusta. On siis entistä todennäköisempää, että yksittäisen palveluntarjoajan ongelmat vaikuttavat merkittävästi koko maailman verkkoliikenteeseen. Kysymys kuuluukin, kannattaako palvelun tilaajan turvautua erilliseen sisällönjakeluverkkoon vai etsiä hosting-palvelu, joka tarjoilee sisältöä nopeasti ilman ylimääräisiä välikäsiä? (V. Korhonen, haastattelu, 25.7.2022)

7 YHTEENVETO

Modernit sisällönjakeluverkot ovat väistämättä kasvava osa sivustokehitystä, sillä pelkästään niiden tarjoamat lisäpalvelut ovat monelle houkutteleva motivaattori niiden käyttöön. Hyvin suunnitellulla ja toimivalla verkkosivulla sisällönjakeluverkon käyttö voi olla perusteltua, mutta huonoa koodia nekään eivät valitettavasti pelasta. Mikäli kyseessä on suuria liikennemääriä vastaanottava verkkosivu, voi sisällönjakeluverkon tarjoama verkkokapasiteetti kuulostaa järkevältä ratkaisulta. Usean palvelimen muodostama kokonaisuus kykenee palvelemaan samanaikaisesti ympäri maailmaa tulevat ”käyttäjäryntäykset” sekä toimimaan tehokkaasti mahdollisia tietoturvahyökkäyksiä vastaan. Sisällönjakeluverkon kyky skaalautua liikennemäärien mukaan tekee verkkosivusta kestävämmän, mutta resursseista huolimatta yksikään sisällönjakeluverkko ei ole täysin immuuni erinäisille tietoturvauhkille.

Kun kaikki liikenne kulkee välikäden kautta, häiriötilanteen syntyessä sivuston ylläpitäjällä ei välttämättä ole muuta vaihtoehtoa kuin nostaa kädet pystyyn. Sisällönjakeluverkon käytössä onkin mietittävä suhdetta kontrollin ja helppouden välillä sekä luottoa palvelua tarjoavaan yritykseen. Jos kyseessä on esimerkiksi

Suomen sisällä toimiva suomenkielinen verkkokauppa, mikä sisältää paljon dynaamista sisältöä, voi laadukkaan hosting-palvelun käyttöönotto olla sisällönjakeluverkkoa parempi vaihtoehto. Tietyissä tilanteissa ulkomaalaisen sisällönjakeluverkon käyttö saattaa jopa huonontaa suomalaisen verkkosivun nopeutta, mikäli lähin palvelin löytyy esimerkiksi Ruotsista.

Sisällönjakeluverkko ei siis ole automaattisesti oikotie onneen, eikä sen käyttöä tulisi pitää oletuksena. Harkitessaan palvelun käyttöönottoa sivustokehittäjän tulisikin miettiä omaa teknistä osaamista, punnita palvelun ja eri palveluntarjoajien hyötyjä ja haittoja sekä analysoida tulevien loppukäyttäjien tarpeita.

LÄHDELUETTELO

Anon. (2017). Cloudbleed security breach threatens thousands of sites. Web User, 418, 8–8.

Akamai. (2017). Akamai Online Retail Performance Report: Milliseconds Are Critical. Akamai Technologies, Inc. https://www.ir.akamai.com/news-releases/news-release-details/akamai-online-retail-performance-report-milliseconds-are (Haettu 24.6.2022)

Buyya R., Pathan, M., & Vakali, A. (2008). Content Delivery Networks. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-77887-5

Cisco. (2019). Cisco Visual Networking Index: Forecast and Trends, 2017–2022. Cisco Systems, Inc. https://twiki.cern.ch/twiki/pub/HEPIX/TechwatchNetwork/HtwNetwork-Documents/white-paper-c11-741490.pdf (Haettu 24.6.2022)

Cloudflare. (2022a). Business Service Level Agreement. Cloudflare, Inc. https://www.cloudflare.com/business-sla (Haettu 20.7.2022)

Cloudflare. (2022b). What is a DDoS attack?. Cloudflare, Inc. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack (Haettu 24.6.2022)

Cloudflare. (2022c). What is a reverse proxy?. Cloudflare, Inc. https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy (Haettu 24.6.2022)

Cloudflare. (2022d). What is a round-trip time?. Cloudflare, Inc. https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt (Haettu 20.7.2022)

Cloudflare. (2022e). What is a SYN flood attack?. Cloudflare, Inc. https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack (Haettu 19.7.2022)

Cloudflare. (2022f). What is a UDP flood attack?. Cloudflare, Inc. https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack (Haettu 19.7.2022)

Cloudflare. (2022g). What is a Ping (ICMP) flood attack?. Cloudflare, Inc. https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack (Haettu 19.7.2022)

Cloudflare. (2022h) What is a cache hit ratio?. Cloudflare, Inc. https://www.cloudflare.com/learning/cdn/what-is-a-cache-hit-ratio/ (Haettu 27.7.2022)

Fielding, R., & Reschke, J. (2014). Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc7230 (Haettu 25.7.2022)

Ganti, V. & Yoachimik, O. (2020). Network-layer DDoS attack trends for Q3. CloudFlare, Inc. https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q3-2020/ (Haettu 20.7.2022)

Ghaznavi, Jalalpour, E., Salahuddin, M. A., Boutaba, R., Migault, D., & Preda, S. (2021). Content Delivery Network Security: A Survey. IEEE Communications Surveys and Tutorials, 23(4), 2166–2190. https://doi.org/10.1109/COMST.2021.3093492

Gupta, M. & Garg, A. (2015). A Comparative Analysis of Content Delivery Network and Other Techniques for Web Content Delivery. International Journal of Service Science, Management, Engineering and Technology, 6(4), 43–58. https://doi.org/10.4018/IJSSMET.2015100104

Imperva. (2022). Osi Model. Imperva. https://www.imperva.com/learn/application-security/osi-model/ (Haettu 19.7.2022)

Intricately. (2022). CDN Industry: Trends, Size, And Market Share. Intricately, Inc. https://blog.intricately.com/cdn-industry-trends-market-share-customer-size (Haettu 19.7.2022)

LVM. (2019). Kaikille mahdollisuus vähintään yhden megan nettinopeuteen 1.7. Liikenne- ja viestintäministeriö. https://www.lvm.fi/-/kaikille-mahdollisuus-vahintaan-yhden-megan-nettinopeuteen-1-7-773301 (Haettu 24.6.2022)

LVM. (2021). Yleispalvelulaajakaistan nopeudeksi 5 Mbit/s. Liikenne- ja viestintäministeriö. https://www.lvm.fi/-/yleispalvelulaajakaistan-nopeudeksi-5-mbit/s-1550306 (Haettu 24.6.2022).

MarketsandMarkets. (2022). Content Delivery Network Market. MarketsandMarkets. https://www.marketsandmarkets.com/Market-Reports/content-delivery-networks-cdn-market-657.html (Haettu 27.7.2022)

MDN. (2022). HTTP. MDN Web Docs. https://developer.mozilla.org/en-US/docs/Web/HTTP (Haettu 20.7.2022)

PerfOps. (2022). CDN Performance – Analytics & Comparison. CDNPerf. https://www.cdnperf.com/#!performance,world,2022-06-01 (Haettu 20.7.2022)

Poletti, Wheeler, N. V., Petrovich, M. N., Baddela, N., Numkam Fokoua, E., Hayes, J. R., Gray, D. R., Li, Z., Slavík, R., & Richardson, D. J. (2013). Towards high-capacity fibre-optic communications at the speed of light in vacuum. Nature Photonics, 7(4), 279–284. https://doi.org/10.1038/nphoton.2013.45

Ponemon. (2016). Cost of Data Center Outages. Ponemon Institute. https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf (Haettu 20.7.2022)

Roser, M., Ritchie, H., & Ortiz-Ospina, E. (2015). Internet. https://ourworldindata.org/internet (Haettu 24.6.2022)

Viscomi, R. (2022). Is my host fast yet? Ismyhostfastyet. https://ismyhostfastyet.com/ (Haettu 25.7.2022)