# WordPress – õnnistus ja nuhtlus

Kaido Kikkas

(Algselt avaldatud ajakirjas "30 pluss" septembris 2016, siin ilmub kokkuleppel toimetusega)

2003. aastal panid Matt Mullenweg ja Mike Little aluse tarkvaraprojektile, millest sai vaba tarkvara suurimaid edulugusid. Algselt ajaveebide loomiseks mõeldud WordPress arenes järgnevate aastate jooksul täismõõdus sisuhaldussüsteemiks (tarkvara, mis lihtsustab veebisisu avaldamist), mille põhjal saab luua väga erinevaid veebilehti. Veebitehnoloogialehe W3Techs.com andmetel oli juulis 2016 üle 26% kõigist veebilehtedest ehitatud WordPressi kasutades. Eestiski on see kasutatavaim sisuhaldussüsteem, millel põhineb eri hinnangutel umbes viiendik Eesti veebist.

WordPress on saadaval kahes peamises variandis – allalaetava tarkvarakomplektina kogukonnaportaalist wordpress.org ning valmiskujul veebiteenusena aadressilt wordpress.com. Viimane konkureerib kasutatavuselt päris edukalt Google Bloggeri ehk blogspot.com -teenusega tavainimesele jõukohase veebiloomise paigana. Valmisteenuse eeliseks on haldamise mure jätmine WordPressi meeskonna õlgadele, samas ei saa seda nii laialdaselt kohandada kui enda serverisse paigaldatavat varianti.

## Edu võtmed

Esmalt võiks WP puhul mainida sama asja, mida taipasid omal ajal nii Bill Gates kui Steve Jobs – massidesse minev tarkvara peab olema lihtne. WP kasutajaliides on mugav ja arusaadav nii väljast- (lugeja/külastaja vaade) kui seestpoolt (autori/halduri vaade). Ka enda serverisse paigaldamine on lihtne. Tõsi, see eeldab mõningaid lisategevusi nagu andmebaasi seadistamine – aga nende oskusteta inimene vaevalt serverisse tarkvara paigaldamisega tegeleb.

Eelmise jätkuna tuleks eraldi mainida rahvusvahelisust – WordPress on eri määral tõlgitud üle 200-sse keelde ja dialekti. Siinkirjutaja on juba pikka aega olnud WordPressi üks põhieestindajaid.

Teine suur eelis on väga suur lisamoodulite ehk pluginate ökosüsteem WordPressi ümber. Kui algselt olid need mõeldud väikeste täienduste tegemiseks ajaveebidele (kalendri lisamine vms), siis tänaseks on mitmed WordPressi pluginad täiesti omaette suured tarkvarasüsteemid – vaid mõne näitena võiks mainida sündmusteplaneerijat Event Organiser, fotogaleriid NextGEN, muusikamängijat Cue ja e-poodi WooCommerce. Enamik neist kasutab *freemium*-ärimudelit, s.t. lihtsam versioon on vabalt leviv, võimsam aga tasuline. Pluginate autorid on väga erinevad ning neil ei ole otsest seost WordPressi põhiosa tegijatega.

Lisaks pluginatele on saadaval terve hulk erinevaid teemasid ehk kujunduspakette. WordPressi vaikimisi kujundused on alates 2010. aastast kandnud väljalaskeaasta nime (seega praegune on „Twenty Sixteen"), lisaks on aga kerge vaevaga võimalik paigaldada täiesti erinev kujundus. Mõni teema on lihtne, mõni teine aga selline, mille taga ehk isegi Matt Mullenweg WordPressi ära ei tunneks. Olgu ka mainitud, et nii teemade kui pluginate paigaldamine käib reeglina mugavalt WordPressi enda haldusliidese kaudu.

Märkusena – enamik teemasid on (nagu arvata) ingliskeelsed, teiste keelte tugi varieerub. Seega kui eestikeelne veebileht vajab uut ja uhket kujundust, siis tuleb see sageli ise ära tõlkida (mis ei ole tegelikult väga keeruline).

## Nõrgad kohad

Nüüd aga jõuame WordPressi nõrgemate külgede juurde. Mõned neist tulenevad sarnaselt näiteks MS Windowsiga suurest kasutajaskonnast, mõned on seotud väliste asjaoludega, mõned on aga ka otseselt tarkvara enda praak.

Nagu öeldud, WordPress on tänaseks levinuim sisuhaldussüsteem ja sellisena ka suurim märklaud erinevatele kaakidele. On loodud terve rida vahendeid, mis võimaldavad leida veebist WordPressi kasutavaid lehti ning nendes teadaolevaid turvaauke rünnata. Siinkohal meenutagem kohe kurjavõitu tõdemust kahest mehest, kes lõvi eest pagevad – vaja pole tingimata joosta kiiremini kui lõvi, piisab teisest mehest kiirem olemisest... Helgema poole pealt võib nentida, et suure osa kaakide eemalhoidmiseks ei ole alati vaja tippturvalisust – piisab mõistlikust tasemest, kuna lihtsamaid ohvreid on netis palju (ja kahjuks pole eriti lootust, et olukord paraneks).

Teine ohuallikas on WordPressi „all" töötav tarkvara – operatsioonisüsteem (enamasti on selleks Linux või mõni muu Unixi perekonna süsteem), veebiserver, SQL andmebaas (enamasti MySQL) ja PHP skriptikeel. Eriti kahe viimasega on seotud mitmed ründevõimalused – ent piisab ka Linuxi süsteemist, mida pole poolteist aastat keegi uuendanud ja kus selle aja peale on leitud mitmed turvaaugud.

Kolmandaks suureks ohuvektoriks on needsamad pluginad, mida eespool mainiti ühe suurima plussina. Natuke sarnaselt eespooltoodud esimese punktina on ka WordPressi pluginate „turg" tänaseks niivõrd lai, et kaakidel tasub neid sihtima hakata. Ja kui WordPressi põhisüsteemi uuendamine on tegijate poolt regulaarne ning kasutaja jaoks lihtne (sageli saab seda seada automaatseks), siis pluginate puhul sõltub see igast autorist eraldi. Nii võib tekkida olukord, kus majal on ees tohutu turvauks, aga keldriaken pärani lahti.

Järgmine turvarisk tuleneb paradoksaalselt paigaldamise lihtsusest. Veebis on hulgaliselt WordPressi lehti, mille haldur on saanud hakkama vaikimisi paigaldusega, kuid ei tea või ei oska edasisi samme. Seega ikka ja jälle tuleb mainida suurt kurjajuurt - „tihendit klaviatuuri ja tooli vahel" ehk võhiklikku kasutajat (või haldurit).

## Mida tuleks teha?

Olgu, meil on olemas Linuxi server, oleme edukalt WordPressi alla laadinud, lahti pakkinud ja lihtsa paigaldusprotsessi läbi teinud. Veebilehitseja näitab tuttuut serverit WordPressi vaikimisi avalehega. Mis edasi?

Esimene asi on tuttav mitmest eelnevast kirjatükist – tarkvara tuleb uuendada. WordPressi on võimalik seadistada uuenema automaatselt, mis mõnelgi juhul on hea variant. Aktiivsemalt hallatava lehe puhul võib lasta lihtsalt saadaolevast uuendusest märku anda ja jätta selle tegemine halduri hooleks. Eraldi tuleb mainida vajadust uuendada kasutatavaid pluginaid ja teemasid – need ei uuene koos põhisüsteemiga ja uuendada tuleb eraldi (see käib sama lihtsalt, kuid lihtsalt omaette sammuna).

Teiseks on hea idee saada lahti algsest „admin"-nimelisest kasutajast. Kuna WordPress ei võimalda seda ümber nimetada, on selleks kõige lihtsam viis luua uus kasutaja, anda sellele halduriõigused, logida välja, seejärel uue kasutajana sisse ning vana „admin" kustutada.

Kolmandaks tasub (taas kord) üle vaadata paroolid. Ükski süsteem ei ole piisavalt turvatud, kui halduri parooliks on „123456”.

Neljandaks tasub hästi läbi mõelda kasutajate süsteem – kes vajab milliseid õigusi. Reeglina ei vajata WordPressi lehe lugemiseks kasutajaks registreerumist (tõsi, seda saab seadistada) ja kasutajaõigused tuleb määrata vaid neile, kes lehte haldavad ja/või sinna sisu loovad. WordPressil on viis kasutajataset, seega tuleks igaühele anda minimaalne õigustekomplekt, mida kasutaja tööks vajab – kõigile maksimumõiguste andmine ei ole kindlasti hea idee.

Nagu eespool öeldud, on WordPressi pluginate ja teemade valik äärmiselt lai ja nende paigaldamine on lihtne. Kindlasti aga tasuks teha enne mõne uue lisamist taustakontrolli (kasvõi guugeldada näiteks „WordPress plugin pluginanimi”). Tasub ka tähelepanu pöörata sellele, millal konkreetset pluginat või teemat on viimati uuendatud – mõni on niivõrd „sammaldunud”, et ei pruugi uuema WordPressiga üldse töötada või osutub turvariskiks.

Pluginatest tasuks eraldi mainida mõnda, mille lisamine aitab WordPressi turvalisust üksjagu tõsta:
* WordFence – võimekas turbetarkvara, täidab sisuliselt sama rolli kui tulemüür arvutis. Kasutab *freemium*-mudelit, kuid reeglina piisab tasuta versiooni võimalustest.
* Akismet – juba päris pikaealine, ent siiani elujõuline rämpspostifilter, mis rämpskommentaatorite punnitused suuresti tühja saadab.
* Limit Login Attempts – tõhus abinõu toore jõuga ründajate vastu, kes üritavad kõikvõimalikke kasutajanimesid ja paroole läbi proovida (see käib tänapäeval suuresti automaatselt) – kui kasutaja ei ole näiteks 3 korraga suutnud end identifitseerida, rakendub mingiks ajaks ligipääsupiirang. Sama funktsionaalsus on olemas ka WordFence’is.

## Jutu kokkuvõtteks

WordPress on asjalik ja laialt levinud veebitööriist. Iga tööriista aga tuleb osata käsitseda sihipäraselt ja turvaliselt – seetõttu tasuks igal ajaveebnikul või mõnel muul veebisepal end peamiste turvavõtetega kurssi viia.