Kui ettevõtet pommitatakse libapäringutega: kaitse teenustõkestusrünnakute vastu on strateegiline äriotsus

15. juuli 2019 - 23:05 Autor: Taavi Talve

Üha digitaalsem maailm ei tähenda ainult tehnoloogilisi võimalusi, vaid ka uusi, sageli üsna leidlikke ohte – küberkurjategijate oskused täiustuvad paralleelselt tehnoloogia arenguga. Andmete varastamise või petujuhtumite kõrval teevad suurt kahju ka teenustõkestusrünnakud. Mida need endast kujutavad ja kuidas ettevõtet kaitsta, kirjutab Telia Eesti IT teenuste juht Taavi Talve.

Distributed Denial of Service ehk DDoS rünnaku käigus üritavad küberkurjategijad sihitud pahatahtlike päringutega häirida ettevõtte veebilehe, e-poe, internetiühenduse või mistahes muu e-lahenduse normaalset toimimist. Sisuliselt saadetakse süsteemi poole erinevatest allikatest tuhandeid päringuid, mis süsteemi üle koormavad. Pättide eesmärk on kas varjata mõnd teist rünnakut või võtta ettevõte „pantvangi“ ja nõuda rünnaku lõpetamise eest lunaraha. Ettevõttel on kaotada väga palju – peamiselt seetõttu, et igapäevane toimimine peatub või on häiritud. Lisaks võib kukkuda toodete või teenuste müük ning ohus on ka ettevõtte usaldusväärsus partnerite ja klientide silmis.

Ka Eestis puutuvad ettevõtted DDoS rünnakutega kokku

Ekslik on arvata, et DDoS rünnaku sihtmärgiks on ainult suured ettevõtted. Tegelikult pole DDoS rünnakute eest kaitstud ükski ettevõte ja sellega puutuvad kokku ka riigiasutused, sh Eestis. Mida rohkem lisandub võrku seadmeid ja andureid, seda enam on võimalusi kellegi ründamiseks. Sealjuures on oluline arvestada, et küberkuritegevus ei pruugi olla juhuslik häkkerite tegutsemine, vaid konkreetse ettevõtte süsteemide sihikindel kahjustamine. Kuna DDoS rünnakuid on võimalik internetis teenusena ka tellida, siis mujal maailmas on selliste rünnakute organiseerimine saanud üha rohkem osaks konkurentsivõitlusest. See tähendab, et aina tavalisemaks muutub olukord, kus ettevõtted tellivad ise rünnakuid konkurentide teenuste, ühenduste või lahenduste häirimiseks.

Telia Eesti võrgus toimub iga päev vähemalt 2-3 DDoS rünnakut, koos teiste võrkudega on rünnakute arv tõenäoliselt suuremgi. Suurema osa Eesti ettevõtete puhul piisab veebiteenuste häirimiseks ainuüksi 1-1,5 Gbits suurusest rünnakust. Kui kasutatav infohulk on veelgi mahukam, näiteks enam kui 20 Gbits, on selliste suurrünnakute vastu ilma DDoS kaitseta võimatu hakkama saada. Ei tasu ka arvata, et rünnak jääb ühekordseks ja teist sellele enam ei järgne. On üsna tavaline, et hõlpsalt kättesaadav lunaraha ahvatleb küberkurjategijaid oma tegu sama ettevõtte suunas kordama.

DDoS kaitse teenus on oluline osa ettevõtte strateegilisest juhtimisest

Kui ettevõte kasutab täna mõnd interneti või pilvelahendust, tasub mõelda DDoS kaitse teenuse peale. Seda eriti siis, kui ettevõtte töövoos on e-poel, heal internetiühendusel, erinevatel veebilehtedel, pilvepõhistel süsteemidel, serverlahendustel või VoIP telefonikeskjaamal oluline roll. DDoS kaitse teenus on oluline ka siis, kui ettevõtte IT süsteemid on üle interneti ühendatud mõne partneri süsteemiga. Viimasel juhul on lisaks IT süsteemide laitmatule toimimisele mängus ka usaldussuhe partneritega ja vastutus nende ees. Sellest vaatest on DDoS kaitse strateegiline äriotsus, mitte enam IT küsimus.

Ettevõtte suurus ei mängi DDoS kaitse vajaduses kõige olulisemat rolli. Kui häiritud veebiteenus toob kaasa märkimisväärse rahalise kahju või mõjutab oluliselt igapäevast toimimist, on DDoS kaitse vajalik. Täpne lahendus sõltub aga konkreetsest ettevõttest.

Alustuseks tasub kaardistada, milliseid eri veebiteenuseid ja lahendusi ettevõte oma töös rakendab ning kas eri partneritel on üle interneti mõnes süsteemis või teenuses kokkupuutepunkte. Ka rahaline aspekt on tähtis, analüüs võimaliku kahju ulatusest ja investeeringust kaitsesse aitab samuti otsust teha.

Kuidas DDoS kaitse teenus töötab?

- Teenuse alustamisel lepitakse kokku ning seadistatakse kliendi poolt määratud süsteemid DDoS kaitse lahenduses
- Esimeste päevade jooksul analüüsib platvorm kliendi internetiliiklust ning paneb paika tavapärase liikluskoormuse
- Teenus jälgib ööpäevaringselt süsteemide liiklust ning DDoS rünnaku tuvastamisel tõkestab rünnaku liikluse automaatselt mõne minuti jooksul
- Sõbralik liiklus toimib ka kaitse rakendumise korral, mis tähendab, et kliendid ja partnerid saavad oma tööd jätkata ka rünnaku korral
- Peale rünnaku lõppu deaktiveeritakse kaitse automaatselt paari minuti jooksul ning tavapärane süsteemide töö jätkub

- Lahendused

- Andmeside
- Turvalisus
- Võrguseadmed