CTRL

TÚLTERHELÉSES TÁMADÁS ELLENI VÉDELMI SZOLGÁLTATÁSOK A MAGYAR TELEKOMTÓL

Ahogy egy modern vállalat szolgáltatásai és kommunikációja egyre inkább a kibertérbe helyeződik át a hagyományos csatornák helyett, úgy válik mind fontosabbá a szolgáltatásokat futtató infrastruktúra magas rendelkezésre állása és megfelelő kapacitásának biztosítása.

E két tényezőt támadják azok a bűnözők is, akik a szolgáltatások leállását vagy lassulását előidéző Distributed Denial of Service (DDoS) módon próbálják a szolgáltatást blokkolni. A DDoS egy olyan támadás, amelyet nagyszámú, akár több százezer kliensről összehangoltan indítanak, és elsődleges célja, hogy a támadott szerver a túlterhelés következtében ne tudja ellátni feladatát.

CYBER THREAT RESILIENCE TEAM

CTRL

A Menedzselt Anti-DDoS szolgáltatási csomagján belül egy új, a vállalati szintű védekezésnél sokkal hatékonyabb, központi anti-DDoS megoldást kínál ügyfeleinek.

A túlterheléses támadás elleni védelmi szolgáltatásaink alapja egy központi, nagy teljesítményű védelmi rendszer, amely képes egyidejűleg több ügyfél védelmét biztosítani. A központi védelmi eszközpark a Magyar Telekom gerinchálózatára épül. Ezzel képessé válik az egyes vállalatok és intézmények internetsávszélesség-igényénél nagyságrendekkel nagyobb sávszélességet kezelni.

A védelmi szolgáltatást igénybe vevő ügyfeleink internetes forgalma időszakosan (pl. támadás esetén) vagy állandó jelleggel halad át védelmi eszközparkunkon. E forgalom állandó monitorozása mellett a szolgáltatás képes érzékelni és manuális vagy automatikus módon kiszűrni a támadásokat, miközben ügyfeleink létfontosságú legitim forgalma a támadások ideje alatt továbbra is zavartalanul folyik.

DDoS-CÉLPONTOK ÉS -TRENDEK

A DDoS-támadások növekedését számos felmérés igazolja, és ez a tendencia hazánkban is megfigyelhető. Ezek a támadások akár több órára megbénítják a szervezetek működését, az ügyfelek kiszolgálásának elmaradása pedig akár milliárdos károkkal járhat.
Ennek a kockázatnak az emelkedése egyetlen gazdálkodó szervezetnél vagy kormányzati intézményben sem hagyható figyelmen kívül.

A DDoS-támadások leggyakoribb célpontjai:

- pénzügyi szolgáltatók, bankok, kormányzati szervek;
- nagyvállalatok;
- nonprofit (civil és politikai) szervezetek, webáruházak;
- távmunkát alkalmazó szervezetek.

A támadások jellegét és volumenét illetően az alábbi trendekkel kell számolni:

- Növekszik a gazdasági indíttatású támadások száma és aránya, illetve növekszik a célzott támadások száma.
- A botnetek – melyek az utóbbi időben a rendkívül megszaporodott, de rendkívül gyengén védett IoT-eszközöet is célozzák – és a róluk indított DDoS-támadások könnyen elérhető, olcsó, néhány dolláros (!), mindenki számára megvásárolható „szolgáltatássá” váltak.
- A látszólag legitim forgalmat generáló támadások megnehezítik a valós idejű detektálást és védekezést.
- Növekszik a volumetrikus támadások aránya és a támadásonként generált forgalom mértéke.
- A támadások bit/s-ban kifejezhető „erőssége” évente növekedik, a 2020-as évekre meghaladta az 500 Gbps-ot, és ennek mértéke folyamatosan növekszik.

A DDoS-TÁMADÁSOK FAJTÁI ÉS A VÉDEKEZÉS LEHETŐSÉGEI

A támadások jellegét és volumenét illetően az alábbi trendekkel kell számolni:

- Sávszélességet felemésztő (volumetrikus) támadások: az a céljuk, hogy telítsék a szerver hálózati kapcsolatát vagy túlterheljék az azt kiszolgáló hálózati eszközöket.
- Kapcsolatalapú támadások: a csak kezdeményezett vagy ténylegesen megnyitott, de nem használt kapcsolatok nyilvántartása foglalja le az erőforrásokat. Szerveren kívül célpontja lehet tűzfal vagy terheléselosztást végző eszköz is.
- Alkalmazásszintű támadások: nagyszámú lekéréssel kötik le a szerver erőforrásait (processzor, memória), speciális változata lehet a DNS- vagy egyéb kiszolgálószolgáltatást megbénító támadás.

A vállalati felhasználásra kínált DDoS védelmi eszközök inline megoldások, amelyek az internetszolgáltató által biztosított adatvonalba beépülve monitorozzák és szükség esetén szűrik a kártékony forgalmat.

Az előfizetői oldali megvalósítás hátránya, hogy bár képes a támadás detektálására, és meg tudja akadályozni a támadó forgalom eljutását a célba vett szerverre, de volumetrikus támadások esetén nem képes védeni az adott szervert a vonalkapacitás (sávszélesség) elfogyása ellen. A védett szerver ugyan nem áll le, de gyakorlatilag elérhetetlen, így a támadó elérte a célját.

Éppen ezért szolgáltatói oldalon célszerű implementálni a DDoS-védelmet, amely így egyidejűleg alkalmas a támadó forgalom észlelésére, szűrésére, valamint az

CTRL

ügyfél sávszélességének megőrzésére. A támadó jellegű forgalom kiszűrése mellett a legitim forgalom továbbra is eljut a kiszolgálóhoz, tehát a védelem sikeres.

A CTRL Menedzselt Anti-DDoS termékünk központosított szolgáltatást kínál az ügyfeleknek. A központi védelmi eszközpark egyszerre több ügyfél védelmét teszi lehetővé. A forgalmakat már az internetszolgáltató központban szűrik, ezzel tehermentesítve ügyfeleink internet-sávszélességét.

AJÁNLATI CSOMAGJAINK ÁTTEKINTÉSE

SZOLGÁLTATÁSELEMEK	BRONZE CSOMAG	SILVER CSOMAG	GOLD CSOMAG	PLATINUM CSOMAG	PLATINUM+ CSOMAG
Kinek ajánljuk?	költséghatékony védelem	komplex védelmi szolgáltatás	nagyvállalati és több telephellyel rendelkező ügyfelek számára	üzletkritikus alkalmazásokat üzemeltetők számára	auditált nagyvállalati ügyfeleinknek
Szolgáltatásba bevont internetkapcsolatok száma	1 db	2 db	korlátlan	korlátlan	korlátlan
További internetkapcsolatok bevonása a szolgáltatásba	igen, külön díj ellenében	igen, külön díj ellenében	korlátlan	korlátlan	korlátlan
Védelem beállítása	template alapú	ügyfélre szabott	ügyfélre szabott, rendszeresen finomhangolva	ügyfélre szabott, rendszeresen finomhangolva	ügyfélre szabott, rendszeresen finomhangolva
Rendelkezésre állás	7x24 óra	7x24 óra	7x24 óra	7x24 óra	7x24 óra
Manuális beavatkozás megkezdése	nem	nem	4 óra	30 perc (proaktív üzemeltetés)	30 perc (proaktív üzemeltetés)
Műszaki konzultáció, finomhangolás havonta	nem	nem	igen	igen	igen
Incidenselemzés	nem	nem	igen	igen	igen
Rendszeres riport	negyedévente, elemzés nélkül	negyedévente, elemzés nélkül	negyedévente, elemzés nélkül	havonta, elemzéssel	havonta, elemzéssel
Online portál (read-only elérés)	nem	nem	igen, külön díj ellenében	igen	igen
DDoS-tesztelés és részletes jegyzőkönyv	nem	nem	igen, külön díj ellenében	igen, külön díj ellenében	igen
Inline csomag lehetősége	nem	nem	nem	igen, külön díj ellenében	igen, külön díj ellenében
Éves rendelkezésre állás	99,9%	99,9%	99,9%	99,9%	99,9%
Havidíj	**54 900 Ft**	**113 600 Ft**	**309 700 Ft**	**677 200 Ft**	**767 500 Ft**

A csomagárak nem tartalmazzák a 27%-os áfát.

TOVÁBBI INFORMÁCIÓÉRT FORDULJON ÜGYFÉLMENEDZSERÉHEZ, VAGY ÍRJON SZAKÉRTŐINKNEK A **CTRL_SOLUTIONS@TELEKOM.HU** E-MAIL CÍMRE!

CYBER THREAT RESILIENCE TEAM