FELHŐ ALAPÚ DDOS VÉDELEM

Mi a DDoS támadás?

A DDoS (Distributed Denial of Service) egy szolgáltatásmegtagadással járó támadás, vagy más néven túlterheléses támadás.

Célja, hogy telítse a szerver hálózati kapcsolatát vagy túlterhelje az azt kiszolgáló hálózati eszközöket. Ezáltal a megtámadott szolgáltatás elérhetetlenné válik, ami veszélyezteti az üzletfolytonosságot.

A DDoS támadások **száma** és **összetettsége** folyamatosan **növekszik**; mérettől függetlenül, bármely vállalat potenciális **célpont lehet**. Egy ilyen akció nem csak hosszabb-rövidebb távú **üzemkiesést**, de jelentős **üzleti kárt** és **presztízsveszteséget** is okozhat.

Az Invitech megoldása

Az általunk kínált védelmi megoldás keretében a DDoS szolgáltatás monitoring rendszere felügyeli és mintavételezés útján elemzi az internet forgalmat, 10 percen belül, bekapcsol a blokkolás, azt követően, hogy fenyegető forgalomnövekedést észlel.

- A központi szűrő rendszer a beérkező káros forgalmat blokkolja, **de a legitim forgalom továbbra is elérhető marad**.
- A támadás így **nem jut el a megcélzott szerverig** és **nem csökkenti a vállalat internet sávszélességét** sem

Világszerte nő a túlterheléses támadások **száma és összetettsége**

Az Invitech DDoS elleni védelmi szolgáltatása biztosítja az **adatforgalom tisztítását**

Hatékony védelem a **folyamatos üzletmenetért**

A szolgáltatás három változatban vehető igénybe:

1. DDoS folyamatos védelem:

Támadás esetén az ügyfelek forgalma áthalad az Invitech hálózatán belül elhelyezett központi szűrő rendszeren, mely véd a 20Gbps – 30Gbps méretű támadások ellen, **eseti díj felszámítása nélkül, így költségei előre kiszámíthatóvá válnak**.

2. Felhő alapú DDoS védelmi szolgáltatás:

Az Invitech internet uplink vagy saját forgalom tisztító kapacitását meghaladó támadások esetére az Arbor Cloud szolgáltatással további védelmi szintet tudunk biztosítani ügyfeleink számára. - A felhő alapú szűrés csak szükség esetén kerül bekapcsolásra a 20-30 Gbps sávszélességet meghaladó támadások esetén. A felhős védelem szűrőrendszerének kapacitása nagyságrendileg 11 Tbps.

3. „Sensor" védelem a third-party telekommunikációs vonalakra:

Annak érdekében, hogy a DDoS támadások elleni védekezés egy szolgáltató rendelkezésre állásával valósulhasson, az Invitech hardver appliance-ek (AED) elhelyezését javasolja az idegen szolgáltató által nyújtott telekommunikációs vonalakra. A külső vonalakra elhelyezett eszközök már önmagukban képesek védelmi szolgáltatás ellátására, illetve „szenzorként" jelezni tudnak a központi feldolgozó egység számára, ha a kapacitásukat meghaladó, volumetrikus támadás történik. Támadás esetén a forgalom az Invitech központi szűrőrendszere felé kerül átirányításra.

Szolgáltatás előnyei

- **Folyamatos üzletmenet** – támadás esetén is zavartalan internetforgalom
- **Költséghatékony**, jól skálázható megoldás
- **Havidíjas** konstrukció
- **Állandó rendszerfelügyelet,** monitoring és mintavételezés
- **Testre szabható** riportok, statisztikák
- Az egyidejűleg több ügyfél védelmét is biztosító központi rendszerbe való bekötéssel, illetve az Arbor Cloud szolgáltatására való egyidejű előfizetéssel nem fordulhat elő, hogy a támadások elérhetetlenné teszik ügyfeleink internetes szolgáltatásait.

Opcionális szolgáltatások

- Tűzfal megoldások
- Végpontvédelmi szolgáltatások
- Logmenedzsment
- WAF, SOC

További információkért látogassa meg weboldalunkat.

invitech