DDoS-felkészültség nagyvállalati környezetben

Vezetői összefoglaló: mennyire lenne védett a vállalata egy DDoS-támadás esetén?

Egy nagyvállalat digitális szolgáltatásai ma már nem kiegészítő eszközök, **hanem az üzleti működés alapjai.** Ha az ügyfelek nem tudnak belépni az online felületre, nem érik el az ügyfélportált, nem tudnak tranzakciót indítani, rendelést leadni vagy partneri rendszert használni, az nem egyszerű informatikai fennakadás. **Azonnali üzleti, reputációs és működési kockázat.**

A kockázat azonban nem csak az ügyfelek felől jelentkezhet. Egy támadás vagy az arra adott túlzottan durva védelmi reakció – például forgalom teljes korlátozása, régióblokkolás, szolgáltatások ideiglenes lezárása – nemcsak az ügyféloldali felületeket, hanem a belső működéshez szükséges rendszereket is érintheti, mint a levelezés, a vállalati együttműködési platformok, a felhős szolgáltatások vagy a munkatársak számára nélkülözhetetlen digitális munkakörnyezet (pl. Teams, SharePoint, OneDrive, felhős dokumentumtárak, SSO-val elérhető üzleti rendszerek,stb.).

A DDoS-támadás célja nem feltétlenül az adatlopás vagy a rendszer feltörése, hanem az, hogy a cég működése vagy szolgáltatásai lelassuljanak, instabillá váljanak vagy teljesen elérhetetlenek legyenek. **Az ügyfél ebből nem technikai részleteket lát. Azt látja, hogy a cég elérhetetlen, és nem tesz eleget a vállalásainak.**

Ilyenkor nemcsak az ügyfélélmény sérül, hanem maga a napi működés is lassulhat vagy leállhat. Egy rövid kiesés is ügyfélpanaszokat, ügyfélszolgálati terhelést, elmaradó tranzakciókat, negatív sajtóvisszhangot, munkavégzési fennakadást és bizalomvesztést okozhat. Szabályozott iparágakban pedig a digitális működés zavara megfelelési kérdéssé is válhat.

Egy DDoS-támadás tarthat néhány percig, órákig vagy akár visszatérő hullámokban napokig, hetekig is. Vezetői szempontból azonban nem az a fő kérdés, hogy meddig bírja a támadó, hanem hogy a szervezet mennyi ideig tud elfogadható szolgáltatási szinten működni támadás alatt.

A veszély sokszor azért alattomos, mert a szervezet papíron védettnek érzi magát. Van tűzfal, van monitoring, van üzemeltetési csapat, működnek a rendszerek. A valódi kérdés azonban nem ez.

A vezetői kérdés az, hogy:

ha holnap túlterheléses támadás érné a vállalat digitális szolgáltatásait, pontosan tudnák-e, hogy:

- melyik rendszer lassulna vagy állna le, és meddig maradnának elérhetők a kritikus ügyfél- vagy belső munkavégzési felületek?
- ez az incidens milyen elmaradt bevételt, kötbért, ügyfélvesztést, bírságot vagy más közvetlen anyagi veszteséget okozhat?
- ki hoz üzleti és technikai döntést incidens közben?
- hogyan kell kommunikálni az ügyfelek, partnerek, munkatársak vagy hatóságok felé?
- **És ami a legfontosabb: ezt nem feltételezések, hanem tesztelt, dokumentált működés alapján tudnák-e megválaszolni?**

A DDoS-felkészültség lényege, hogy ezekre a kérdésekre ne éles helyzetben kelljen választ keresni. Egy jól felépített felkészültségi vizsgálat megmutatja, **mely digitális szolgáltatások a legkritikusabbak, hol vannak a sebezhető pontok, mekkora terhelést bír el a jelenlegi infrastruktúra, működnek-e a védelmi mechanizmusok, és milyen fejlesztések szükségesek a kockázat csökkentéséhez.**

Az Unicorn Criticaltech célja, hogy a DDoS-felkészültség ne feltételezés, hanem mérhető, dokumentált állapot legyen. Nagyvállalati környezetben vizsgáljuk az üzletileg kritikus rendszereket, a hálózati és biztonsági architektúrát, a monitoringot, a védelmi rétegeket, az incidenskezelési folyamatokat és a kontrollált tesztelhetőséget.

Segítünk felmérni, hogy a jelenlegi működés mennyire ellenálló egy túlterheléses támadással szemben. Szükség esetén kontrollált DDoS-teszttel is igazolható, hogyan reagálna a rendszer valós terhelés alatt. Az eredmény nem elméleti dokumentum, hanem vezetői döntéstámogató anyag: **megmutatja, hol van valódi kockázat, mit kell fejleszteni, és milyen sorrendben érdemes lépni.**

A cél egyszerű: a vállalat ne akkor ismerje meg saját határait, amikor már megtörtént a támadás. Hanem előre, kontrollált körülmények között, mérhető módon.

Ha szeretné gyorsan megtudni, mennyire felkészült a szervezete egy DDoS-helyzetre, az Unicorn Criticaltech szakértői segítenek értelmezni a kockázatokat, felmérni a jelenlegi állapotot, és meghatározni a következő lépéseket.

CTA 1. Konzultációt kérek az Unicorn Criticaltech szakértőivel.

CTA 2. Tovább olvasom a részletes vezetői útmutatót, és megismerem a DDoS-támadások üzleti, technológiai és megfelelési hátterét.

Tartalomjegyzék

Bevezető
Mit kell védeni, és milyen üzleti következménnyel járhat a kiesés?
Vezetői checklist: felkészült a szervezetünk?
Miért lehet bármely szervezet DDoS-célpont?
    Miért kerülhet egy szervezet célkeresztbe?
Hogyan működik egy DDoS-támadás?
Miért nehéz felismerni?
Milyen üzleti károkat okozhat: kiesés, reputáció, bírság, ügyfélbizalom

[DORA és NIS2: miért fontos a bizonyítható digitális ellenállóképesség?](#)
[A korszerű DDoS-védelem rétegei](#)
[DDoS-felkészültségi audit: mit kell felmérni?](#)
[Kontrollált DDoS-teszt: hogyan derülnek ki a valódi gyenge pontok?](#)
[Miért az Unicorn Criticaltech?](#)
[Kérje szakértelmünket!](#)

Bevezető

Ez az útmutató azt mutatja be, hogyan értelmezhető a DDoS-kockázat vezetői, üzleti és technológiai szinten, és milyen lépésekkel mérhető fel egy szervezet valódi felkészültsége.

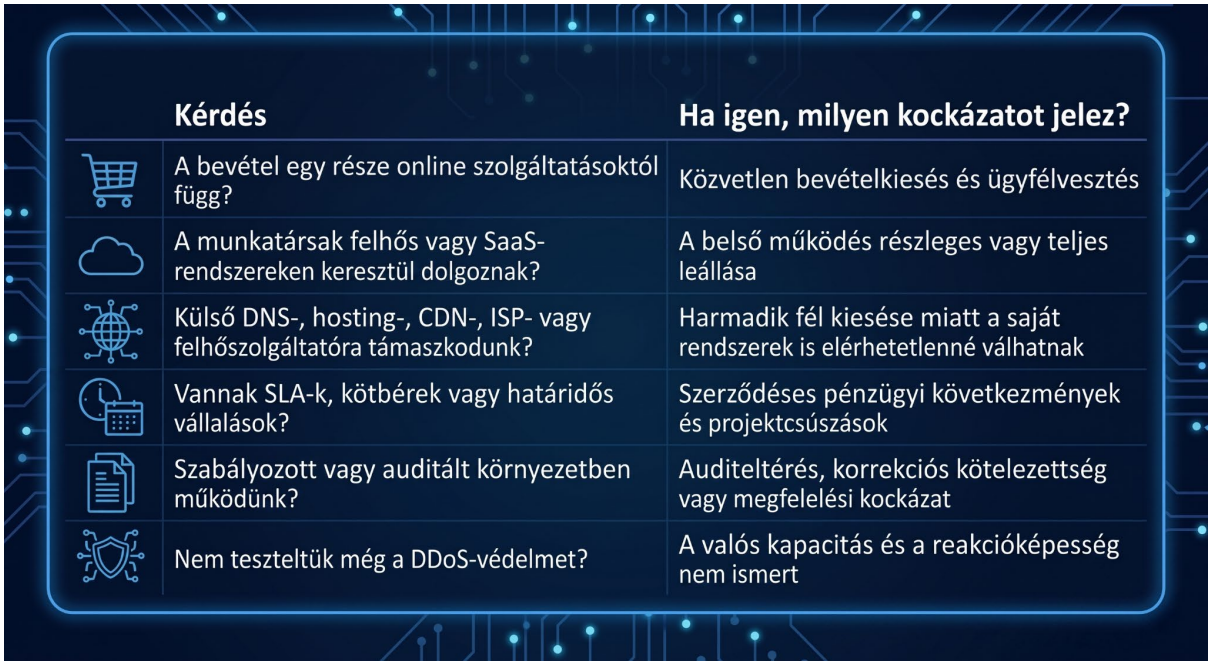
A dokumentum végigvezeti az olvasót azon, mit kell védeni, milyen üzleti következménye lehet egy kiesésnek, miért lehet bármely digitális működésre épülő szervezet célpont, hogyan működik egy túlterheléses támadás, és hogyan segíthet a DDoS-felkészültségi audit vagy a kontrollált teszt a valódi gyenge pontok feltárásában.

Mit kell védeni, és milyen üzleti következménnyel járhat a kiesés?

A DDoS-kockázat nem csak a nyilvános weboldal vagy az ügyfélalkalmazás elérhetőségét érinti. A vállalat ügyfél kiszolgálása, belső működése és beszállítói kapcsolatai egyaránt függhetnek olyan digitális szolgáltatásoktól, amelyek kiesése közvetlen üzleti kárt okozhat.

	Érintett szolgáltatás	Mit akadályozhat a kiesés?	Lehetséges üzleti következmény
	Weboldal, webshop, rendelési felület	Tájékozódás, vásárlás, ajánlatkérés, rendelés	Kieső bevétel, elvesztett ügyfelek, reputációs kár
	Ügyfélportál, mobilalkalmazás	Belépés, ügyintézés, tranzakciók	Ügyfélpanaszok, ügyfélszolgálati túlterhelés, bizalomvesztés
B2B	Partneri API, B2B-integráció	Adatcsere, rendelésfeldolgozás, partneri műveletek	SLA-sértés, kötbér, partneri folyamatok leállása
$	Fizetési szolgáltatás	Fizetés, tranzakció-jóváhagyás, elszámolás	Meghiúsult vagy megszakadt tranzakciók, bevételkiesés
	Microsoft 365 és más SaaS-rendszerek	Levelezés, fájlmegosztás, együttműködés	Munkavégzés lassulása vagy leállása, projektcsúszás
DNS	DNS-, hosting-, CDN- vagy ISP-szolgáltatás	A vállalati rendszerek és online szolgáltatások elérése	Több szolgáltatás egyidejű kiesése
	Felhős infrastruktúra	Alkalmazások, adatbázisok, belső és külső rendszerek	Üzletmenet-megszakadás, helyreállítási költségek
	Kritikus beszállító vagy SaaS-platform	Kiszervezett üzleti vagy technológiai folyamatok	Harmadik fél miatti leállás, szerződéses és megfelelési következmények

Gyors vezetői kitettségi áttekintés

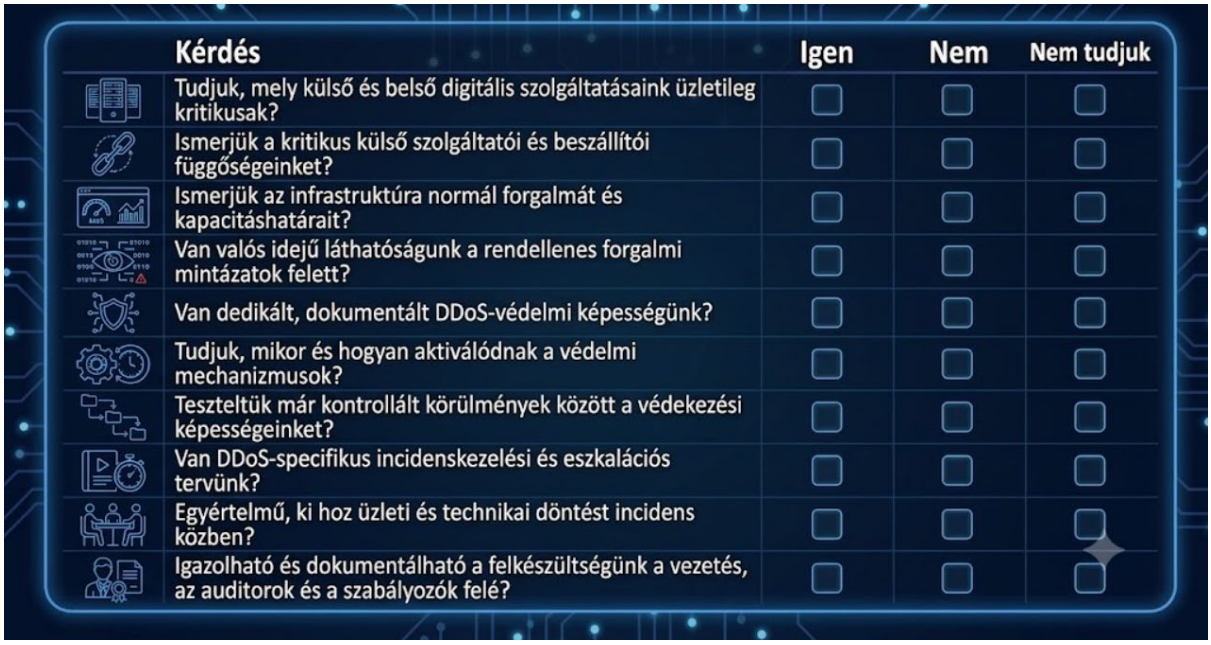


Kérdés	Ha igen, milyen kockázatot jelez?
A bevétel egy része online szolgáltatásoktól függ?	Közvetlen bevételkiesés és ügyfélvesztés
A munkatársak felhős vagy SaaS-rendszereken keresztül dolgoznak?	A belső működés részleges vagy teljes leállása
Külső DNS-, hosting-, CDN-, ISP- vagy felhőszolgáltatóra támaszkodunk?	Harmadik fél kiesése miatt a saját rendszerek is elérhetetlenné válhatnak
Vannak SLA-k, kötbérek vagy határidős vállalások?	Szerződéses pénzügyi következmények és projektcsúszások
Szabályozott vagy auditált környezetben működünk?	Auditeltérés, korrekciós kötelezettség vagy megfelelési kockázat
Nem teszteltük még a DDoS-védelmet?	A valós kapacitás és a reakcióképesség nem ismert

Ha a fenti kérdések közül több is igaz a szervezetre, a DDoS-kockázat nem kizárólag technológiai, hanem közvetlen pénzügyi és működési kérdés.

Vezetői checklist: felkészült a szervezetünk?

Az alábbi checklist megmutatja, hogy a szervezet ismeri-e kritikus függőségeit, tesztelte-e a meglévő védelmet, és tisztázta-e az incidens során szükséges döntéseket.



Kérdés	Igen	Nem	Nem tudjuk
Tudjuk, mely külső és belső digitális szolgáltatásaink üzletileg kritikusak?	☐	☐	☐
Ismerjük a kritikus külső szolgáltatói és beszállítói függőségeinket?	☐	☐	☐
Ismerjük az infrastruktúra normál forgalmát és kapacitáshatárait?	☐	☐	☐
Van valós idejű láthatóságunk a rendellenes forgalmi mintázatok felett?	☐	☐	☐
Van dedikált, dokumentált DDoS-védelmi képességünk?	☐	☐	☐
Tudjuk, mikor és hogyan aktiválódnak a védelmi mechanizmusok?	☐	☐	☐
Teszteltük már kontrollált körülmények között a védekezési képességeinket?	☐	☐	☐
Van DDoS-specifikus incidenskezelési és eszkalációs tervünk?	☐	☐	☐
Egyértelmű, ki hoz üzleti és technikai döntést incidens közben?	☐	☐	☐
Igazolható és dokumentálható a felkészültségünk a vezetés, az auditorok és a szabályozók felé?	☐	☐	☐

Több „Nem” vagy „Nem tudjuk” válasz esetén indokolt a kritikus függőségek részletes felmérése, valamint felkészültségi audit vagy kontrollált DDoS-teszt elvégzése.

Miért lehet bármely szervezet DDoS-célpont?

A DDoS-támadásokkal kapcsolatban több olyan téves feltételezés él, amely hamis biztonságérzetet adhat.

„Nálunk nincs mit ellopni, ezért nem vagyunk célpont.”

A DDoS célja nem feltétlenül az adatlopás. A támadó elérhetetlenné teheti a weboldalt, az ügyfél portált, a rendelési rendszert, a partneri API-t vagy egy belső működéshez szükséges digitális szolgáltatást. Az üzleti kár akkor is jelentkezik, ha egyetlen adat sem kerül illetéktelen kézbe.

„Nem vagyunk elég nagyok vagy ismertek ahhoz, hogy megtámadjanak.”

A támadók számára nem csak a vállalat mérete számít. Célpont lehet minden olyan szervezet, amelynek működése digitális szolgáltatásoktól függ, és amelynél az elérhetetlenség működési, pénzügyi vagy reputációs nyomást okozhat.

„Felhőben tárolunk mindent, ezért ez nem jelent kockázatot.”

A felhő és a SaaS-szolgáltatások csökkenthetnek bizonyos infrastruktúra-kockázatokat, de új függőségeket is teremtenek. Ha a DNS-, hosting-, CDN-, ISP-, Microsoft 365-, felhő- vagy más SaaS-szolgáltatás nem érhető el, a vállalat belső működése akkor is leállhat, ha a saját infrastruktúrája egyébként működőképes.

Miért kerülhet egy szervezet célkeresztbe?

A DDoS-támadás mögött többféle motiváció állhat:

- **zsarolás:** a támadó pénzt kér a támadás leállításáért vagy elkerüléséért;
- **üzleti vagy reputációs károkozás:** a cél a szolgáltatás megbízhatóságának rombolása;
- **versenypiaci nyomásgyakorlás:** egy fontos időszak, kampány vagy értékesítési csúcs megzavarása;
- **ideológiai vagy politikai motiváció:** egy szervezet tevékenységének, ügyfélkörének vagy nyilvános álláspontjának támadása;
- **figyelemelterelés:** a DDoS más támadás, jogosulatlan hozzáférés vagy adatlopási kísérlet elfedésére is szolgálhat;
- **véletlenszerű vagy automatizált célpont választás:** a sérülékeny vagy gyengén védett szolgáltatásokat tömegesen kereső támadásoknál nem feltétlenül történik tudatos vállalat választás.

Hogyan működik egy DDoS-támadás?

A DDoS a **Distributed Denial of Service** rövidítése, magyarul elosztott szolgáltatásmegtagadásos támadást jelent. A támadók ilyenkor nagy mennyiségű forgalmat

irányítanak egy szerver, alkalmazás, weboldal, ügyfélportál vagy más digitális szolgáltatás felé, amíg az már nem képes megfelelően kiszolgálni a valódi felhasználókat.

A cél sokszor nem az adatlopás vagy a rendszerbe való bejutás, hanem az, hogy a szolgáltatás kívülről elérhetetlenné váljon. A háttérrendszer akár működhet is, de ha az ügyfél nem tud csatlakozni hozzá, üzleti szempontból a szolgáltatás kiesett.

Egy DDoS-támadás jellemzően nem egyetlen gépről érkezik. A forgalmat sok ezer vagy akár több millió, földrajzilag szétszórt eszköz generálhatja. Ezek lehetnek fertőzött számítógépek, szerverek, kamerák, routerek, IoT-eszközök vagy más, internetre kapcsolt eszközök, amelyek a tulajdonos tudta nélkül vesznek részt a támadásban. Ezt nevezzük botnetnek.

Miért nehéz felismerni?

Egy DDoS-támadás nem mindig azonnali leállással indul. Sokszor először csak lassulás, válaszidő-növekedés, hibaszám-emelkedés vagy szokatlan forgalmi mintázat látszik. Megfelelő monitoring és forgalomelemzés nélkül ez könnyen összekeverhető hétköznapi teljesítmény problémával, kampány forgalommal vagy infrastruktúra-hibával.

Ezért kulcsfontosságú a normál működés ismerete: ha nem tudjuk, mi számít átlagos forgalomnak, válaszidőnek vagy megszokott terhelési mintázatnak, a támadási mintázatot sem fogjuk időben észrevenni.

A DDoS tehát nem egyszerűen „sok forgalom”. Olyan célzott támadási forma, amely a digitális szolgáltatások rendelkezésre állását veszélyezteti. A védekezéshez ezért nem elég utólag reagálni: előre tudni kell, milyen forgalmat bír el a rendszer, hol vannak a kritikus belépési pontok, és milyen védelmi mechanizmusok lépnek életbe rendellenes terhelés esetén.

Milyen üzleti károkat okozhat: kiesés, reputáció, bírság, ügyfélbizalom

Egy DDoS-támadás üzleti hatása nem merül ki abban, hogy „lassú az oldal” vagy „nem elérhető egy szolgáltatás”. A digitális rendszerek kiesése a szervezet méretétől függetlenül egyszerre érintheti a bevételt, az ügyfélkiszolgálást, a belső működést, a reputációt és adott esetben a szabályozói megfelelést.

A legfontosabb kockázat az üzletmenet-folytonosság megszakadása. Ha egy kritikus rendszer vagy az azt kiszolgáló külső szolgáltató nem érhető el - például ügyfélportál, partneri API, belső üzleti alkalmazás, DNS-, hosting-, CDN-, ISP-, felhő-, fizetési vagy SaaS-szolgáltatás -, akkor nemcsak az IT működése sérül, hanem az üzleti folyamat is.

A pénzügyi veszteség több csatornán keresztül jelentkezhet: elmaradó tranzakciók és kieső bevétel, megnövekedett ügyfélszolgálati terhelés, incidenskezelési és helyreállítási költségek, valamint hosszabb távú ügyfélvesztés formájában. Ehhez társulhatnak a szerződéses kötbérek és SLA-sértésből eredő következmények, a vállalt teljesítések elmaradása, a projektek és szállítások csúszása, a partneri folyamatok megszakadása,

továbbá az auditok vagy megfelelőségi vizsgálatok során feltárt hiányosságokból eredő korrekciós és jogi költségek.

A kár nagysága nemcsak attól függ, hogy mely rendszereket, szerződéses kötelezettségeket és üzleti folyamatokat érinti a támadás, hanem annak időtartamától is. Egy DDoS-incidens nem feltétlenül néhány perces vagy órás esemény: hullámokban visszatérhet, és napokon, heteken vagy akár hosszabb időszakon keresztül is folyamatos védekezést igényelhet. **Ilyenkor a kieső bevétel mellett tartósan növekedhetnek a külső szakértői, infrastruktúra-bővítési, forgalomszűrési, helyreállítási, monitoring- és kommunikációs költségek is.** Minél tovább tart az incidens, annál nagyobb az esélye a szerződéses kötbéreknek, az SLA-k megsértésének, a projektek csúszásának, az ügyfelek elvesztésének és a munkatársak tartós túlterhelésének.

A DDoS-támadás nem feltétlenül jár adatvesztéssel, de a túlterhelés közvetetten adat károsodást is okozhat. Megszakadhat egy fizetési vagy rendelési tranzakció, félbe maradhat egy adatbázisba történő írás, az egyik rendszerben rögzülhet egy művelet, miközben a kapcsolódó rendszerben már nem.

Sikertelen szinkronizáció esetén hiányzó, duplikált vagy egymásnak ellentmondó rekordok keletkezhetnek. További kockázatot jelenthet, ha incidens közben a rendszereket ellenőrzés nélkül, pánikszerűen újraindítják, mert ez a folyamatban lévő műveletek elvesztéséhez vagy az adatok konzisztenciájának sérüléséhez vezethet.

A DDoS emellett figyelem elterelésként is szolgálhat: miközben az üzemeltetési és biztonsági csapat a szolgáltatás helyreállítására koncentrál, a támadók párhuzamosan jogosulatlan hozzáférést, adatkinyerést vagy más behatolási műveletet kísérelhetnek meg. Ezért DDoS-incidens esetén nemcsak a rendelkezésre állást, hanem az esetleges egyidejű behatolási kísérleteket is vizsgálni kell.

A **reputációs veszteség szintén kritikus**. A felhasználók többsége nem technikai incidensként értelmezi a leállást, hanem azt érzékeli, hogy a szolgáltatás nem működik. Ez különösen érzékeny pénzügyi szolgáltatások, telekommunikáció, egészségügy, közmű, e-kereskedelem vagy kritikus B2B szolgáltatások esetén, ahol az ügyfélbizalom központi üzleti érték.

A szabályozói és megfelelési kockázat sem hagyható figyelmen kívül. Ha a szervezet nem tudja bizonyítani, hogy megfelelő felkészültséggel, incidenskezelési folyamattal, üzletmenet-folytonossági tervvel és technológiai védelemmel rendelkezik, akkor egy DDoS-incidens megfelelési kérdéssé is válhat.

Végül vezetői döntési kockázat is jelentkezik: támadás közben gyorsan kell dönteni a forgalomkorlátozásról, kommunikációról, külső védelmi szolgáltató aktiválásáról és az esemény dokumentálásáról. Ha ezek a döntési pontok nincsenek előre tisztázva, a szervezet incidens közben kezd el improvizálni.

Egy DDoS-támadás üzleti hatását ezért nem lehet pusztán technikai mérőszámokkal értékelni. A valódi kérdés az, hogy egy kritikus szolgáltatás kiesése milyen láncreakciót indít el az üzletben.

A DDoS-kockázat tehát nem egyszerűen informatikai probléma. Üzleti folytonossági, pénzügyi, reputációs és megfelelési kérdés, amelyet vezetői szinten is kezelni kell.

DORA és NIS2: miért fontos a bizonyítható digitális ellenállóképesség?

A DDoS-védelem nemcsak technológiai vagy üzletmenet-folytonossági kérdés, hanem egyre inkább megfelelési kérdés is. A nagyvállalatokkal, pénzügyi intézményekkel, telekommunikációs szolgáltatókkal és kritikus működésű szervezetekkel szemben ma már alapvető elvárás, hogy ne csak működtessék digitális rendszereiket, hanem bizonyítani is tudják azok ellenálló képességét.

Ebben a környezetben különösen fontos a **DORA** és a **NIS2** szemlélete.

A **DORA** (Digital Operational Resilience Act) a pénzügyi szektor digitális működési ellenálló képességére helyezi a hangsúlyt. A szabályozás logikája szerint nem elég informatikai rendszereket üzemeltetni: a szervezetnek képesnek kell lennie arra is, hogy felkészüljön a digitális zavarokra, kezelje az incidenseket, tesztelje a védelmi képességeit, és dokumentált módon igazolja a működési ellenállóképességet.

A **NIS2** szintén azt erősíti, hogy a kiberbiztonság nem kizárólag az IT-osztály feladata. A hálózat- és információbiztonsági kockázatok kezelése szervezeti, vezetői és működési felelősség is. Ez különösen igaz olyan vállalatoknál, amelyek kritikus vagy fontos szolgáltatásokat nyújtanak, illetve olyan digitális rendszereket működtetnek, amelyek kiesése szélesebb ügyfélkört, partnereket vagy üzleti folyamatokat érinthet.

A DDoS-támadások ebből a szempontból kiemelt figyelmet érdemelnek, mert közvetlenül a rendelkezésre állást támadják. Egy túlterheléses támadás nem feltétlenül sérti az adatok bizalmasságát, de megbéníthatja a hozzáférést a szolgáltatáshoz. A digitális ellenállóképesség szempontjából ez ugyanúgy kritikus: a rendszernek nemcsak biztonságosnak, hanem elérhetőnek és helyreállíthatónak is kell lennie.

A DORA és a NIS2 irányából nézve a DDoS-felkészültség tehát nem különálló technikai téma. A digitális működési ellenállóképesség része. Olyan terület, amely összekapcsolja az IT-biztonságot, az üzletmenet-folytonosságot, az incidenskezelést, a kockázatmenedzsmentet és a vezetői felelősséget.

Ezért egy DDoS-audit vagy kontrollált DDoS-teszt nem csupán technológiai hasznot ad. **Segít dokumentálhatóvá tenni, hogy a szervezet ismeri a saját kitettségét, tisztában van a kritikus pontokkal, és konkrét lépéseket tesz a digitális ellenállóképesség megerősítésére.**

A korszerű DDoS-védelem rétegei

A hatékony DDoS-védelem nem egyetlen eszközön múlik. Egy nagyvállalati infrastruktúrában a túlterheléses támadások elleni védekezés több, egymásra épülő rétegből

áll. Ezek együtt biztosítják, hogy a szervezet ne csak észlelje a támadást, hanem időben reagálni is tudjon rá.

Fontos különbség, hogy a hagyományos tűzfal önmagában nem DDoS-védelem. A tűzfal alapvetően azt szabályozza, milyen forgalom léphet be a hálózatba, de egy túlterheléses támadásnál gyakran éppen az a probléma, hogy a bejövő forgalom mennyisége bénítja meg a működést. Ilyenkor nem elég egyszerűen „levágni” vagy tiltani a forgalmat, mert azzal a valódi ügyfelek, partnerek vagy munkatársak hozzáférése is sérülhet.

Egyszerű hasonlattal: a tűzfal olyan, mint egy biztonsági kapu, amely eldönti, kit enged be. Egy DDoS-támadásnál viszont nem egyetlen illetéktelen belépővel van gond, hanem azzal, hogy egyszerre ezrek torlódnak fel a kapu előtt. A védelem feladata ilyenkor nemcsak a belépés szabályozása, hanem a torlódás kezelése, a rossz forgalom kiszűrése és a valódi felhasználók kiszolgálásának fenntartása.

Valós idejű forgalom figyelés

Az első réteg a láthatóság. A szervezetnek pontosan tudnia kell, hogyan néz ki a normál működés: milyen forgalom érkezik a kritikus szolgáltatások felé, milyen válaszidők jellemzőek, mikor vannak forgalmi csúcsok, és mely rendszerek számítanak érzékeny belépési pontnak.

Hálózati szintű előszűrés

A támadó forgalmat minél korábban kell azonosítani és kezelni. Ideális esetben nem akkor kezdődik a védekezés, amikor a belső rendszerek már vannak terhelve, hanem már a hálózat peremén vagy azon kívül.

A hálózati szintű előszűrés célja, hogy a nyilvánvalóan rosszindulatú, szokatlan vagy túlzott forgalom ne jusson el változatlan formában a kritikus infrastruktúráig. Ez csökkenti annak esélyét, hogy a támadás a belső rendszereket, tűzfalakat, terhelés elosztókat vagy alkalmazásokat terhelje túl.

Dedikált DDoS-védelmi megoldás

A megfelelő védelem kiválasztása attól függ, hol található a kritikus szolgáltatás, mekkora támadási volumen várható, milyen gyorsan kell beavatkozni, és egyetlen vagy több szolgáltatótól függ-e az internetkapcsolat.



Védelmi megoldás	Mikor lehet megfelelő?	Fő korlát
ISP-alapú DDoS-védelem	Ha a kritikus rendszerek internet forgalma jellemzően egy szolgáltatón keresztül érkezik, és elsősorban nagy volumenű hálózati támadások ellen kell védekezni	A védelem gyakran az adott szolgáltató hálózatához és az általa biztosított kapcsolathoz kötődik
Felhő alapú forgalom tisztítás	Ha nagy támadási kapacitásra, több helyszín vagy internetkapcsolat védelmére, illetve támadás esetén külső forgalomterelésre van szükség	A megfelelő átirányítást, DNS- vagy BGP-folyamatokat előre ki kell alakítani és tesztelni
CDN- és WAF-alapú védelem	Nyilvános weboldalak, webshopok, portálok, API-k és alkalmazásszintű támadások esetén	Nem feltétlenül védi a teljes hálózatot, a nem webes szolgáltatásokat vagy a közvetlenül elérhető infrastruktúrát
Helyszíni DDoS-védelmi eszköz	Ha alacsony késleltetésű, részletes helyi forgalomelemzésre és automatikus beavatkozásra van szükség	A vállalati internetkapcsolat telítődése után önmagában már nem képes a teljes támadó forgalmat kezelni
Hibrid védelem	Kritikus, magas rendelkezésre állást igénylő vagy összetett infrastruktúra esetén, ahol a helyi gyors reagálást nagy kapacitású külső védelemmel kell kombinálni	Összetettebb tervezést, integrációt, tesztelést és üzemeltetést igényel
Menedzselt DDoS-védelmi szolgáltatás	Ha nincs folyamatosan rendelkezésre álló belső szakértői kapacitás, vagy 24/7 észlelésre és incidenskezelési támogatásra van szükség	Pontosan rögzíteni kell az aktiválási időt, az SLA-t, a felelősségeket és a szolgáltatás műszaki határait

Az ISP-alapú védelem különösen akkor lehet célszerű, ha a támadó forgalom már a vállalati internet kapcsolat előtt kiszűrhető. Összetett, több szolgáltatót, felhős rendszert, webalkalmazást vagy több telephelyet érintő környezetben azonban gyakran hibrid modellre van szükség.

A döntés előtt legalább azt kell tisztázni, hogy a megoldás milyen hálózati és alkalmazás szintű támadásokat kezel, mekkora kapacitással rendelkezik, automatikusan vagy manuálisan aktiválódik-e, mennyi az aktiválási idő, biztosít-e 24/7 szakértői támogatást, és hogyan illeszkedik a meglévő ISP-, felhő-, DNS-, CDN-, WAF- és biztonsági környezethez.

Automatikus válasz mechanizmusok

Ezért fontosak az automatikus válasz mechanizmusok: forgalomkorlátozás, IP- vagy régió alapú szűrés, gyanús mintázatok blokkolása, forgalomterelés, riasztás, illetve szükség esetén a védelmi szolgáltatások automatikus aktiválása. Ezeket előre kell megtervezni és tesztelni, mert incidens közben már nincs idő alapvető szabályokat kitalálni.

DDoS-felkészültségi audit: mit kell felmérni?

A DDoS-védelem első lépése nem feltétlenül egy új eszköz beszerzése. Sokkal fontosabb annak megértése, hogy a jelenlegi infrastruktúra milyen kitettséggel működik, hol vannak a kritikus belépési pontok, mely szolgáltatások üzletileg érzékenyek, és milyen gyorsan tudna reagálni a szervezet egy valós támadásra.

Ezt szolgálja a DDoS-felkészültségi audit.

Kritikus szolgáltatások és üzleti prioritások

Elsőként azt kell tisztázni, mely digitális szolgáltatások kiesése okozna azonnali üzleti hatást. Nem minden rendszer azonos fontosságú.

Az audit során ezért meg kell határozni:

- **mely külső és belső rendszerek üzletileg kritikusak,**
- **mely szolgáltatások érhetők el kívülről,**
- **mely felületek támogatják közvetlenül az ügyfélkiszolgálást vagy a belső működést,**
- **mely DNS-, hosting-, CDN-, ISP-, felhő-, fizetési vagy SaaS-szolgáltatóktól függ a működés,**
- **mely rendszerek vagy beszállítók kiesése járna pénzügyi, reputációs vagy megfelelési kockázattal,**
- **milyen rendelkezésre állási elvárások vonatkoznak ezekre.**

Incidenskezelési és döntési folyamat

Egy DDoS-incidens kezelése nem egyetlen technikai csapat feladata. Előre tisztázni kell, hogy az egyes döntési pontoknál ki jogosult intézkedni, kit kell bevonni, és milyen információ alapján történik az eszkaláció.



Incidens fázis	Fő feladat	Elsődleges felelős	Bevonandó területek
Észlelés	Rendellenes forgalom, válaszidő-növekedés, hibaarány vagy kiesés azonosítása	SOC / NOC / üzemeltetés	IT-biztonság, alkalmazásgazda
Első értékelés	Annak megállapítása, hogy támadás, kapacitásprobléma vagy szolgáltatói hiba történt-e	IT-biztonság	Hálózati csapat, alkalmazás üzemeltetés, külső szolgáltató
Incidens aktiválása	Súlyossági szint meghatározása, incidens vezető kijelölése, érintettek riasztása	Incidens vezető / CISO	CIO, üzleti tulajdonos, felsővezetés
Technikai védekezés	Forgalomszűrés, rate limiting, WAF- és DDoS-szabályok aktiválása, forgalomterelés	Hálózati és biztonsági csapat	ISP, CDN-, DNS-, felhő- vagy DDoS-védelmi szolgáltató
Szolgáltatási priorizálás	Kritikus funkciók fenntartása, kevésbé fontos szolgáltatások korlátozása	Üzleti és IT-vezetés	Alkalmazásgazdák, operáció
Párhuzamos fenyegetés vizsgálat	Annak ellenőrzése, hogy a DDoS mellett történt-e behatolási, adatkinyerési vagy jogosultságszerzési kísérlet	SOC / IT-biztonság	IAM-, endpoint-, hálózati és alkalmazás biztonsági szakértők
Üzleti hatásértékelés	Kieső bevétel, SLA-sértés, kötbér, projekt csúszás és ügyfélhatás felmérése	Üzleti tulajdonos / pénzügy	Jogi, compliance, operáció
Kommunikáció	Belső tájékoztatás, ügyfél-, partner-, szolgáltatói és szükség esetén hatósági kommunikáció	Kommunikáció / incidens vezető	Jogi, compliance, ügyfélszolgálat, felsővezetés
Helyreállítás	Szolgáltatások fokozatos visszaállítása, adatintegritás és tranzakciók ellenőrzése	Üzemeltetés	Alkalmazásgazdák, adatbázis- és biztonsági csapat
Incidens lezárása	Naplók, döntések, költségek és tanulságok dokumentálása	Incidens vezető	Minden érintett terület
Utólagos fejlesztés	Küszöbértékek, védelmi szabályok, kapacitások, szerződések és folyamatok módosítása	CISO / CIO	Felsővezetés, beszerzés, szolgáltatók

Ha ezek a felelősségek csak az incidens során kezdenek tisztázódni, a technikai támadás könnyen szervezeti válsággá válhat. A megfelelő védelmi rendszer és az előre tesztelt

playbook csökkenti a manuális döntések számát, gyorsítja a reagálást, és mérsékli a kiesés üzleti költségét.

Tesztelhetőség és dokumentálhatóság

Végül az audit egyik legfontosabb kérdése: tesztelték-e már a védekezési képességeket kontrollált körülmények között?

A DDoS-felkészültségi audit végső értéke az, hogy vezetői és technológiai szinten is tiszta képet ad:

"Milyen szolgáltatásokat kell védeni, milyen kockázatokkal, milyen jelenlegi képességekkel, milyen hiányosságokkal és milyen fejlesztési prioritásokkal."

Kontrollált DDoS-teszt: hogyan derülnek ki a valódi gyenge pontok?

Egy DDoS-felkészültségi audit megmutatja, hogyan épül fel a jelenlegi védelem. A kontrollált DDoS-teszt ennél egy lépéssel tovább megy: valós működési adatok alapján vizsgálja, hogyan viselkedik az infrastruktúra terhelés alatt.

A cél nem az, hogy „megtámadjuk" a saját rendszert, és nem is az, hogy kárt okozzunk. Egy jól megtervezett DDoS-szimuláció kontrollált, előre egyeztetett és fokozatosan felépített terhelési vizsgálat. A cél az, hogy biztonságos körülmények között derüljön ki, hol vannak a rendszer határai, mely komponensek reagálnak először, és a védelmi mechanizmusok valóban úgy működnek-e, ahogyan a szervezet feltételezi.

Mit vizsgál egy DDoS-teszt?

Egy kontrollált teszt során több kérdésre is választ lehet kapni:

- **mekkora forgalmat képes kezelni a jelenlegi infrastruktúra,**
- **mikor kezd nőni a válaszidő,**
- **mely szolgáltatás vagy komponens telítődik először,**
- **működnek-e a riasztások,**
- **aktiválódnak-e az automatikus védelmi szabályok,**
- **el tudja-e különíteni a monitoring a normál terhelést a támadási mintázattól,**
- **van-e olyan pont, ahol manuális döntésre van szükség,**
- **hogyan reagál az üzemeltetési és biztonsági csapat,**
- **milyen üzleti hatása lenne az adott terhelési szintnek.**

Milyen eredményt ad egy DDoS-teszt?

Az eredmény jellemzően tartalmazza:

- **a vizsgált rendszerek és szolgáltatások körét,**
- **a tesztelt terhelési szinteket,**

- **a rendszer válaszidejének és stabilitásának alakulását,**
- **az észlelt szűk keresztmetszeteket,**
- **a védelmi mechanizmusok működésének értékelését,**
- **az incidenskezelési folyamat tapasztalatait,**
- **a rövid, közép- és hosszú távú fejlesztési javaslatokat.**

Egy ilyen teszt ezért nem kockázatvállalás, hanem kockázatcsökkentés. Segít elkerülni, hogy az első valódi nagy terhelés egy éles incidens legyen.

Miért az Unicorn Criticaltech?

Az Unicorn Criticaltech előnye nem önmagában egy technológiai eszköz vagy gyártói megoldás bevezetésében van, hanem abban, hogy nagyvállalati környezetben képes összekapcsolni a hálózati infrastruktúrát, a biztonsági architektúrát, az üzemeltetési folyamatokat és az üzleti kockázati szempontokat.

A DDoS-védelem nálunk nem különálló termékként jelenik meg, hanem egy teljes felkészültségi folyamat részeként: felmérés, tesztelés, kockázati értékelés, védelmi architektúra tervezése, bevezetés és hosszú távú támogatás formájában.

A gyakorlati előny három területen jelenik meg:

- **Nagyvállalati és kritikus infrastruktúra szemlélet:** olyan környezetekben gondolkodunk, ahol a rendelkezésre állás, az üzletmenet-folytonosság és a megfelelőség egyszerre fontos.
- **Technológiai mélység:** a hálózati szintű védelem, a forgalomelemzés, a tűzfalas környezet, a monitoring és a DDoS-specifikus megoldások együttműködését vizsgáljuk, nem csak egyetlen réteget.
- **Mérhető eredmény:** az együttműködés végén az ügyfél nem általános biztonsági javaslatokat kap, hanem konkrét képet arról, mely szolgáltatásai a legkockázatosabbak, hol vannak a szűk keresztmetszetek, milyen védelmi lépések szükségesek, és milyen sorrendben érdemes ezeket megvalósítani.

DDoS-felkészültségi audit

Az első lépés a jelenlegi környezet áttekintése. Az Unicorn szakértői felmérik, mely szolgáltatások üzletileg kritikusak, milyen külső elérési pontok vannak, hogyan épül fel a hálózati és biztonsági architektúra, milyen monitoring működik, és milyen védelmi mechanizmusok állnak rendelkezésre.

Kontrollált DDoS-teszt

A felkészültség valódi szintje csak teszteléssel igazolható. Az Unicorn kontrollált terhelési vizsgálattal segít feltárni, hogyan reagálna az infrastruktúra egy valós túlterheléses helyzetre.

Védelmi architektúra kialakítása

A védelem része lehet a hálózati szintű szűrés, a dedikált DDoS-védelmi technológia, az alkalmazás szintű kontroll, a forgalomterelés, a valós idejű monitoring, az automatikus válasz mechanizmusok és az incidens utáni elemzési folyamat kialakítása.

Az Unicorn olyan gyártói és technológiai háttérre épít, mint például a Netscout Arbor, a Palo Alto Networks, a Cisco és más nagyvállalati hálózatbiztonsági megoldások, de a cél nem önmagában egy eszköz bevezetése. A cél egy olyan összehangolt védelmi rendszer kialakítása, amely a vállalat konkrét működéséhez, kockázataihoz és üzleti prioritásaihoz illeszkedik.

Hosszú távú támogatás és fejlesztés

Az Unicorn hosszú távú partnerként támogatja ügyfeleit a monitoring, az üzemeltetés, az incidens elemzés, a rendszeres felülvizsgálat és a védelmi architektúra fejlesztése területén is.

“A cél egyszerű: a szervezet ne éles támadás közben szembesüljön saját határaival, hanem előre ismerje azokat, és felkészülten tudjon reagálni.”

Kérje szakértelmünket!

Egy DDoS-támadás nem kér engedélyt, és nem akkor érkezik, amikor a szervezetnek kényelmes. A kérdés nem az, hogy érdemes-e felkészülni, hanem az, hogy a jelenlegi infrastruktúra, védelmi rendszer és döntési folyamat hogyan viselkedne egy valódi túlterheléses helyzetben.

Az Unicorn Criticaltech DDoS-felkészültségi audittal, kontrollált terhelési teszttel és nagyvállalati védelmi architektúra kialakításával segít abban, hogy erre ne feltételezések, hanem mérhető válaszok szülessenek.

Tudja meg, hogyan reagálna rendszere egy valódi DDoS-támadásra - még azelőtt, hogy éles helyzetben derülne ki.