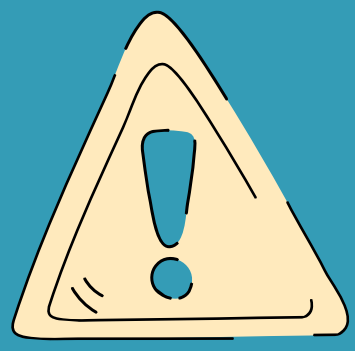
SI TË MBRONI KOMPANINË/INSTITUCIONIN TUAJ NGA SULMET DDOS



ÇFARË JANË SULMET DDOS?

Sulmet DDoS janë një lloj sulmi kibernetik ku shumë pajisje kompromentuese (të quajtura botnet) përdoren për të mbingarkuar një sistem, rrjet ose shërbim të caktuar me trafik të madh të të dhënave.

MASAT PARANDALUESE

1 MONITORONI DHE EKZAMINONI TRAFIKUN NË RRJET PËR AKTIVITETE TË PAZAKONSHME

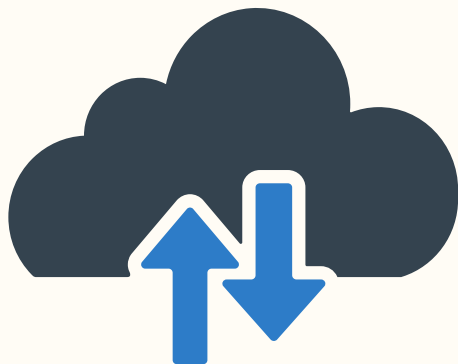
Monitoroni vazhdimisht trafikun që hyn duke konfiguruar pajisjet e rrjetit (p.sh. *firewall*-et) për të zbuluar llojet e trafikut anormal, mbingarkesat e kapacitetit të sistemit dhe pajisjet mashtruese të lidhura në rrjet. Mbani të përditësuar sistemet tuaja të të dhënave, rregulloni firewall-et e aplikacionit tuaj në web dhe programet e tjera të sigurisë së rrjetit.

2 PRAKTIKONI BAZAT E HIGJIENËS KIBERNETIKE

Ka disa hapa të thjeshtë që çdo biznes mund të marrë për të siguruar një nivel bazë sigurie kundër kërcënimeve DDoS. Këto përfshijnë praktikat më të mira të tilla si: përdorimi i fjalëkalimeve komplekse, detyrimi i rivendosjes së fjalëkalimit çdo tre muaj dhe shmangia e mbajtjes shënim të fjalëkalimeve. Këto mund të duken të parëndësishme, por është alarmante se sa shumë biznese janë të rrezikuara nga neglizhenca e higjienës bazë të sigurisë.

3 PËRDORNI ZGJIDHJET E BAZUARA NË CLOUD

Cloud ofron më shumë shpërndarje *(bandwidth)* dhe burime në krahasim me rrjetet private. Qendrat e të dhënave cloud mund të tërheqin trafikun keqdashës dhe t'i shpërndajnë ato në zona të tjera duke i penguar ata të arrijnë objektivat e synuara.



4 PËRDORNI NJË CDN (CONTENT DELIVERY NETWORK)

Meqenëse sulmet DDoS funksionojnë duke mbingarkuar një server pritës *(hosting server)*, CDN-të mund të ndihmojnë duke ndarë ngarkesën në mënyrë të barabartë në një numër serverësh që janë të shpërndarë gjeografikisht dhe më afër përdoruesve. Në këtë mënyrë, nëse një server nuk funksionon, do të ketë serverë të tjerë që janë ende funksionalë.