Eidsiva bredband – DDOS-beskyttelse, DDOS mitigering

Produkt - introduksjon

Eidsiva Bredband tilbyr 24/7-beskyttelse mot volumetriske DDOS-angrep, basert på et generelt regelsett.

Eidsiva Bredband tilbyr løsninger for IDP, basert på utstyr fra Fortinet.

Produktene kan bestilles som tilleggstjeneste til alle internettabonnement for bedriftskunder, og etablering skjer i samråd med Kunden.

DDOS og andre angrep via internett

HVA ER ET ANGREP?

Alt som er tilkoblet internett, vil på et eller annet tidspunkt kunne bli mål (eller utilsiktet offer) for en eller annen type angrep.

Det finnes flere varianter av angrep, og de kategoriseres ofte etter selve hensikten med angrepet:

1) Tjeneste-nekt og volumetriske angrep
2) Snik-angrep/e-spionasje
3) «Social engineering»

I kategori 1) finner vi typiske DDOS-angrep. Disse kjennetegnes ofte ved at angrepstrafikken kommer fra mange steder på en gang (Distributed), og hensikten er som regel å utarme en ressurs, være seg båndbredde/kapasitet, CPU og/eller andre maskinvare-ressurser, i den hensikt å gjøre ressursen utilgjengelig for andre (Denial of Service).

I kategorien 2) finner vi utnyttelse av sikkerhetshull, hvor hensikten kan være den samme som i 1), eller å omgå visse sikkerhetsmekanismer for å få tilgang på digitalisert informasjon som ellers ville vært utilgjengelig.

I kategorien 3) finner vi eksempelvis epost/SMS/telefoni/SoMe-meldinger hvor mottageren blir lurt til å oppgi konfidensiell informasjon, initiere en penge-transaksjon, installere en skadevare, eller tvinges via eskalerende trusler til å begå handlinger som mottageren i utgangspunktet ikke ville gjennomført.

HVORDAN ØKE RESISTANS MOT ANGREP?

For angrep i kategorien 3) gjelder alt fra intern opplæring, vask/filtrering av epost og meldinger, og andre tiltak for å bevisstgjøre eller beskytte sluttbruker, eksempelvis deltagelse på «Nasjonal Sikkerhetsmåned» i regi av NoRSIS.

For angrep i kategorien 2) må en strategisk tilnærming til informasjonssikring legges til grunn. Dette inkluderer blant annet fortløpende tetting av sikkerhetshull / fjerne kjente sårbarheter, men også bevisstgjøring knyttet til hvilken informasjon som lagres hvor, og på hvilket format / kryptering.

For 24/7-overvåkning av internett-trafikk finnes det flere muligheter

- systemer for IDP (Intrusion Detection and Prevention) analyserer nettverkstrafikk, og identifiserer og varsler/stopper angrep med gjenkjennbare trafikkmønstre
- systemer for adferds-analyse - identifisere og varsler/stopper angrep basert på nye trafikkmønstre. Disse systemene kan stoppe angrep hvor angrepsvektoren ikke er beskrevet

For angrep i kategorien 1) (DDOS-angrep):

Disse angrepene utnytter protokoller som i utgangspunktet er legale, hvis tilstedeværelse er en grunnleggende forutsetning for bruk av internett, og dermed er «åpne».

Hensikten med disse angrepene kan være en eller flere.
De vanligste variantene er:

1) Overbelaste en internett-tilbudt tjeneste – eksempelvis en web-tjeneste - slik at denne blir utilgjengelig for andre
2) Overbelaste en linje/kapasitet, for å gjøre denne kapasiteten (med bakenforliggende tjenester) utilgjengelig for den tiltenkte bruken

I tillegg kan slike angrep ha flere hensikter:

3) Overbelaste en internett-tilbudt tjeneste, for å finne svakheter i bakenforliggende infrastruktur
4) Få tilgang på informasjon som til vanlig er utilgjengelig eller beskyttet
5) Som «røykteppe» for å ta vekk oppmerksomhet fra annen type og parallelt angrep

DDOS-angrep utnytter som nevnt svakheter i IP-protokollen, kombinert med vårt behov for kapasitet og tilgjengelighet.

DDOS TCP-SYN-angrep er rettet mot tjenester som er allment tilgjengelig på internett. Dette kan være web/http-baserte tjenester, systemer for innlogging, «remote desktop» m.m. Angrepene er pr definisjon ikke volumetriske, men utarmer en tjenesteressurs ved å initiere mange parallelle bruker-sesjoner mot en og samme ressurs, inntil ressursen ikke kan håndtere flere sesjoner.
TCP-SYN-angrep utnytter en svakhet i TCP-protokollen, og effekten av angrepet kan vesentlig reduseres ved enkle hjelpemidler, for eksempel geografisk begrensning for tilgang til tjeneste (GeoIP).

DDOS UDP-angrep benytter åpne protokoller, hvis tilstedeværelse er avgjørende for at internett skal fungere. Angrepet har sjelden noen annen hensikt enn å «fylle opp linker» ved at angrepstrafikken i volum er større enn linje-kapasiteten.

ANBEFALT INNFØRINGSMETODIKK:

Effekten av angrep kan vesentlig reduseres/elimineres ved å følge rådene som gjengitt ovenfor:

1) Intern kompetanseheving
2) I samråde med tjeneste-tilbyder/ISP: Etablere en ekstern beskyttelse mot volumetriske angrep (DDOS-UDP)
3) I samråd med valgt utstyrs- eller tjenesteleverandør, etablere en intern IDP-beskyttelse
4) I samråd med utstyrs-, tjeneste- eller sky-leverandør, etablere en sesjons-beskyttelse for tjeneste-trafikken (DDOS-TCP)

EIDSIVA BREDBANDS VOLUMETRISKE DDOS-FILTER, TEKNISK BESKRIVELSE

Basert på vår kunnskap om trafikkmønstre i volumetriske DDOS-angrep, har vi etablert en relativt enkel metode for å identifisere og begrense trafikken som utgjør disse angrepene.

1. Volumetriske DDOS-angrep følger kjente protokoller og porter (UDP: NTP, SSDP, CHARGEN, SNMP, DNS, UDP-fragments mm).
2. Når trafikk av denne typen ankommer EBs nett, identifiseres den, og merkes med en prioritet.
3. Internt i EBs nett begrenses denne trafikken, slik at summen av våre kunder ikke blir skadelidende
4. Mot hver enkelt sluttkunde kan vi begrense den identifiserte trafikken til en %-andel av total båndbredde for sluttkunden.

Det vil til enhver tid være både legal og illegal trafikk som blir fanget opp og merket ihht metoden.
Når vi begrenser den identifiserte trafikken (ved hjelp av «policere») setter vi grenseverdiene slik at trafikken i en normal-situasjon ikke blir påvirket.
Ved et angrep, vil derimot all identifisert trafikk bli begrenset, og da også en prosentandel av den legale trafikken.
Implementeringsprosessen pr kunde inkluderer spesialtilpasninger utover standard-metoden.