CENTER FOR CYBERSIKKERHED

Sådan kan du imødegå DDoS-angreb

Center for Cybersikkerhed har udarbejdet en vejledning i, hvordan truslen om DDoS-angreb kan imøde-gås.

Beskrivelse af DDoS
DDoS er et angreb, hvor angriberen kalder en tjeneste, for eksempel en hjemmeside, med typisk en så stor intensitet, at hjemmesidens infrastruktur ikke kan klare belastningen. Resultatet er, at hjemmesiden bliver utilgængelig for den legitime trafik. Et DDoS-angreb kræver store ressourcer (også hos angriberen, eksempelvis i form af penge eller angrebskapacitet) og er derfor altid tidsbegrænset. Angrebet vil således typisk ophøre efter et antal timer.

Basal beskyttelse
Der findes nogle basale foranstaltninger, som kan hjælpe til at opdage og modvirke et angreb. Du bør:

- sikre, at alle netværkskomponenter, herunder firewall og spamfiltre, er opdateret til seneste patch level
- sørge for opdateret dokumentation af netværkstopologi, og overvej eventuelle afledte konse-kvenser af et DDoS-angreb på en hjemmeside eller anden offentligt anvendt tjeneste, f.eks.
    - om et DDoS-angreb på hjemmesiden kan overbelaste en firewall eller router og dermed afbryde eller forstyrre adgang til VPN eller e-mail
    - om et DDoS-angreb på hovedpostkassens e-mailadresse kan påvirke organisationens mu-lighed for at anvende e-mail internt på grund af en overbelastet mailserver.
- Aktivere relevant logning på alle it-systemer og sikre, at logning ikke har et unødvendigt stort performance overhead. Logningen er et redskab for myndighederne til at konstatere uregelmæs-sigheder
- monitorere netværk og applikationer for hurtigt at kunne erkende et angreb, herunder have et normalt billede af båndbredde (tilgængeligt og brugt)
- sikre, at alle relevante personer er bekendt med beredskabsplanen, herunder at den indeholder kontakter i Center for Cybersikkerhed og kontakt til og aftaler med internetleverandør (ISP).

Aktive tiltag
Udover de basale foranstaltninger findes der en række aktive tiltag, du kan indføre på baggrund af en konkret risikovurdering. Tiltagene er listet med de (forventeligt) billigste først:

1. Forbered nødforside på hjemmesiden, der fylder så lidt som muligt.
2. Undersøg, hvilke DDoS-forsvarsmidler din internetleverandør (ISP) stiller til rådighed – eventuelt som tilkøbsydelse

3. Indkøb eller lav aftale om ekstra IP-adresser, som kan bruges, hvis din primære IP-adresse bliver blokeret
4. Indkøb eller lav aftale om ekstra, separate internetadgange, som kan bruges, hvis din primære internetadgang bliver blokeret
5. Forbered alternativ hostet forside/informationsside og overvej eventuelt anvendelse af cloud-hosting af hjemmesiden (vær opmærksom på prismodel)
6. Lad netværksadministratorer gøre sig bekendt med eller uddanne sig i routere og andre net-værkskomponenters mulighed for at beskytte sig mod de mest almindelige angreb som:

    - SYN flood
    - ICMP flood
    - UDP flood
    - Smurf og Fraggle Attack
    - E-mail bombing

7. Optimér netværk for ydelse og gennemfør ydelsestest. Alt efter løsning kan dette inkludere:

    - Redundans i opbygningen
    - Separation af indgående og udgående internettrafik
    - Fysisk separation af intern kritisk infrastruktur og eksterne servere
    - Separat e-mailserver til de primære eksternt kommunikerede e-mailadresser, fx hoved e-mail-adressen

8. Optimér applikationer for ydelser og gennemfør ydelsestest, herunder sikre applikation mod de mest almindelige angrebsformer som:

    - Malformed data
    - SQL injection
    - User locking
    - Regular expression attacks

9. Installér dedikerede netværkskomponenter til at imødegå angreb. Lav aftale med ISP'en eller eksterne udbydere af løsninger til at imødegå angreb. Det kan fx være løsninger, som benytter sig af:

    - Mailscreen
    - Traffic scrubbing
    - Anycast.