Nederlandse securitycentra

NCSC

Het Nationaal Cyber Security Centrum (NCSC) is, met het oog op het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en -incidenten en het versterken van de digitale weerbaarheid van de samenleving, belast met:

a. het informeren, adviseren en bijstaan van de rijksoverheid en vitale aanbieders in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen;

b. het informeren van anderen;

c. het verrichten van analyses en technisch onderzoek naar aanleiding van cyberdreigingen en -incidenten;

d. het aan anderen verstrekken van analyses verkregen informatie over dreigingen en incidenten betreffende andere netwerk- en informatiesystemen;

e. de taken van het centraal contactpunt, bedoeld in de Wet beveiliging netwerk- en informatiesystemen;

f. het bevorderen en voeren van het secretariaat van de publiek-private samenwerking op het gebied van cybersecurity.

DTC

Het DTC waarschuwt niet-vitale bedrijven wanneer er sprake is van specifieke, ernstige cyberdreigingen. Dit zijn actuele cyberaanvallen of kwetsbaarheden in bedrijfsapplicaties die een grote kans op misbruik hebben en potentieel veel schade kunnen aanrichten.

Het DTC en NCSC vormt samen met verschillende sectorale computercrisisteams en schakelorganisaties het groeiende *Landelijk Dekkend Stelsel (LDS)* van cybersecurity- samenwerkingsverbanden

CSIRT

De taken van een Computer Security Incident Response Teams zijn onder andere:

- reageren op incidenten die vrijwillig of verplicht worden gemeld;
- incidenten op nationaal niveau monitoren, aanbieders vroegtijdig waarschuwen en informatie over risico's en incidenten verspreiden;
- deelnemen aan het internationale netwerk van CSIRT's en
- op samenwerking gerichte contacten onderhouden met de particuliere sector.

Het *CSIRT*-DSP is het nationale Cyber Security Incident Response Team voor digitale dienstverleners.

CERT

Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt een CERT zich ook op preventie en preparatie.

Er is een aantal sectorale CERT's: Z-CERT voor zorginstellingen, SURFcert voor onderwijsinstellingen, IBD voor gemeenten en WM-CERT voor waterschappen.
Daarnaast bestaan er Organisaties die Kenbaar Tot Taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's)

SOC

Een Security Operations Center (SOC) is een eenheid, die binnen de organisatie monitort om inzicht en grip te hebben op de digitale infrastructuur binnen uw organisatie en op wat daarbinnen allemaal gebeurt. Vanuit applicaties en apparaten wordt loginformatie verzameld en onderzocht op mogelijke aanvallen. Door correlatie van gegevens wordt bepaald of er afgeweken wordt van de standaard. De loginformatie is afkomstig van verschillende bronnen zoals servers, firewalls, (web)applicaties, infrastructurele componenten en endpoint-protectiesystemen.

SIEM

Een hulpmiddel dat onlosmakelijk verbonden is met een SOC is een Security Information & Event Management (SIEM) systeem. Het betreft software die in staat is om loginformatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten.