Landelijke actoren in Cyber Weerbaarheid

Wie is verantwoordelijk?

Bedrijven en instanties zijn zelf verantwoordelijk voor informatie-beveiliging en uitwijkmogelijkheden.

De VR (met brandweer), politie (met meldkamer), GHOR en gemeente zijn dus zelf verantwoordelijk. In 2020 werd VNOG getroffen door gijzelsoftware

Bedrijven en instanties hebben zelf een aantal functionarissen in dienst

- CISO: Chief Information Security Officer. Deze functionaris is eindverantwoordelijk voor informatie-beveiliging binnen een organisatie.
- Functionaris Gegevensbescherming. Rol voorgeschreven vanuit de AVG. Gaat dus alleen maar over de bescherming van privacy-gevoelige gegevens.

Het Computer Emergency Response Team

Als er een cyber aanval is kan een “Computer Emergency Response Team” (CERT) actief worden. Zo’n CERT wordt vaak gezamenlijk georganiseerd in een branche. Zo zijn er bijvoorbeeld:

- NREN CERT voor onderwijs
- Informatie beveiligingsdienst (IBD) van de VNG
- Stichting Z-CERT voor zorginstellingen
- CSIRT-DSP: “Cyber Security Incident Response Team voor digitale dienstverleners”. Dat zijn leveranciers van digitale diensten zoals een cloud service of een zoekmachine.

Een CERT kan ook een rol spelen bij het beschermen en voorbereiden. En het is een platform voor het uitwisselen van kennis of een actueel dreigingsbeeld.

Soms is er in plaats van een CERT alleen maar een “lnformation Sharing and Analysis Centre” (ISAC). Dat houdt zich alleen bezig met informatie-uitwisseling en is niet gericht op het daadwerkelijk optreden bij een cyber-aanval.

Daarnaast is er op initiatief van het ministerie van economische zaken het “digital trust center” (DTC) opgericht om ondernemers te ondersteunen.

Het Nationaal cyber security centrum

Het Nationaal cyber security centrum (NCSC) is de CERT voor de rijksoverheid en vitale aanbieders. Vitale aanbieders worden door een departement aangewezen. Een actueel overzicht: Overzicht vitale processen | Vitale infrastructuur | Nationaal Coördinator Terrorismebestrijding en Veiligheid

Het NCSC onderhoudt ook contact met haar zusterorganisaties in de EU en alle verschillende CERT's in Nederland. En zij krijgt informatie van de veiligheidsdiensten voor een actueel dreigingsbeeld.

Al deze informatie is samengebracht in een plaatje van het landelijk dekkend stelsel.

In dit plaatje zie je bovendien nog de "OKTT":

Het NCSC erkent dat sommige organisaties "objectief kenbaar tot taak" hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten. De organisaties worden "OKTT's" genoemd. Als daar aanleiding voor is verstrekt het NCSC informatie aan een OKTT zodat deze haar doelgroep kan informeren.

Wettelijke eisen

Er kunnen wettelijke eisen gesteld worden aan de cyber-security van overheden en vitale aanbieders. De Cyberbeveiligingswet (Op basis van de EU Nis 2 richtlijn) geldt voor de sector Energie, Vervoer, Digitale diensten, Gezondheidszorg, Maakindustrie van een bepaalde omvang.

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Had voorheen iedere overheidslaag zijn eigen baseline, nu is er met gezamenlijke inspanning 1 BIO voor de gehele overheid.

Kijk eens naar de Operationele kennisproducten BIO - bio-overheid . Op welke cascades van het cyber-cacsademodel zijn deze kennisproducten gericht?