NLCS in vogelvlucht

Burgers en bedrijven moeten ten volle kunnen profiteren van deelname aan de digitale samenleving, veiligheid is hiervoor essentieel. Onze economie, democratie en samenleving zijn afhankelijk van veilige en betrouwbare digitale producten en verbindingen. Deze afhankelijkheid neemt de komende jaren alleen nog maar toe, cybersecurity is een investering in onze toekomst. Met de Nederlandse Cybersecuritystrategie 2022-2028 werkt het kabinet aan een toekomst waarin de scheefgroei tussen digitale dreiging en digitale weerbaarheid zo klein mogelijk is en blijft. Om de visie te realiseren zijn doelen geformuleerd langs vier pijlers.

Pijler I

Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties

Deze pijler ziet toe op de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties. Hierbij gaat het om het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.

Doelen

- Organisaties hebben zicht op cyberincidenten, -dreigingen en -risico's en hoe hiermee om te gaan.
- Organisaties zijn goed beschermd tegen digitale risico's, en nemen hierin hun belang voor de sector en andere organisaties in de keten mee.
- Organisaties reageren, herstellen en leren snel en adequaat op en van cyberincidenten en –crises.

Pijler II

Veilige en innovatieve digitale producten en diensten

Deze pijler focust op de aanbieders en afnemers van digitale producten en diensten en de versterking van cybersecurity kennisontwikkeling en innovatie. Het toewerken naar een veilige en innovatieve digitale economie draagt bij aan de digitale veiligheid en het verdienvermogen van Nederland.

Doelen

- Digitale producten en diensten zijn veiliger.
- Nederland heeft een sterke cybersecuritykennis- en innovatieketen.

Pijler III

Tegengaan van digitale dreigingen van staten en criminelen

Deze pijler richt zich op de nationale en internationale aanpak van kwaadwillende actoren waar een cyberdreiging vanuit gaat. Het vergroten van het zicht op de digitale dreiging om op basis hiervan te handelen. De overheid heeft een speciale verantwoordelijkheid en beschikt over het instrumentarium om de digitale dreiging te adresseren.

Doelen

- Nederland heeft zicht op digitale dreigingen van staten en criminelen.
- Nederland heeft grip op digitale dreigingen van staten en criminelen.
- Staten houden zich aan het normatief kader voor verantwoordelijk statelijk gedrag in de digitale ruimte.

Pijler IV

Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers

Deze pijler richt zich op de mens achter de techniek en de digitale weerbaarheid van burgers. Voor de samenleving als geheel is een belangrijke rol weggelegd om digitale vaardigheden te ontwikkelen, van basiskennis en -vaardigheden tot aan hoogwaardige kennis en specialistische cybersecurityvaardigheden.

Doelen

- Burgers zijn goed beschermd tegen digitale risico's.
- Burgers reageren snel en adequaat op cyberincidenten.
- Leerlingen krijgen onderwijs in digitale vaardigheden gericht op veiligheid.
- De Nederlandse arbeidsmarkt kan voldoen aan de toenemende vraag naar cybersecurity-experts.

Het kabinet investeert daarom in het versterken en transformeren van het digitale ecosysteem waarbij één organisatie of één individu niet langer de zwakste schakel kan zijn. Dit doet het kabinet op basis van deze vijf speerpunten.

Door meer zicht op de dreiging te krijgen zodat we de dreiging kennen en begrijpen.

Om te bepalen hoe en waar onze digitale weerbaarheid versterkt moet worden, is het essentieel scherper zicht te hebben op waar de dreiging vandaan komt en welke specifieke belangen worden bedreigd.

- Uitbreiden capaciteit diensten en defensie

Door te zorgen dat er op de arbeidsmarkt voldoende expertise is zodat we de uitdagingen aan kunnen.

Is nu een groot tekort. Dat merken onze bedrijven, onze kennisinstellingen en onze overheidsorganisaties. Er is concrete actie nodig om meer ICT-specialisten op de arbeidsmarkt te krijgen.

- Digitale veiligheid in het curriculum voor basis en voortgezet onderwijs
- Investeren in opleidingen in het hoger onderwijs en bij- en omscholingsprogramma's

Bewustzijn en kennis van risico's en dreigingen.

De risico's van digitale kwetsbaarheden en dreiging moeten zoveel als mogelijk worden gedragen door de ontwikkelaars en aanbieders van digitale producten en diensten. Er zal echter bijna altijd een restrisico blijven waardoor de burger of MKB ook zelf maatregelen moet nemen. Om deze maatregelen te kunnen nemen moeten burgers en MKB zich allereerst bewust zijn van de risico's en de te nemen maatregelen.

- Voorlichtingscampagnes en onderwijs
- Organiseren van duidelijke informatiepunten voor burgers en bedrijven
- Tijdig notificeren van slachtoffers en/of doelwitten.

Door wet- en regelgeving zodat de kaders helder en toetsbaar zijn.

Een groot deel van de cybersecurity maatregelen die bedrijven nemen zijn momenteel gebaseerd op vrijwillige richtlijnen, handreikingen en kaders. Voor bepaalde organisaties kunnen we, gezien de risico's voor continuïteit, het risico niet lopen dat digitale veiligheid geen prioriteit krijgt. Voor deze organisaties zijn wettelijke kaders nodig. De vrijblijvendheid voorbij. Daarnaast moet bij het ontwikkelen en aanbieden van digitale producten en diensten veiligheid een van de randvoorwaarden worden.

- Uitbreiding van de wettelijke regels en toezicht voor (rijks)overheden en vitale aanbieders (NIS2, WDO etc.).
- Sturen op veilige hard- en software via Europese regelgeving (CRA).
- Meer regie en steviger (politiek-bestuurlijke) sturing op meetbare effecten en resultaten.

Door een herziening van het stelsel zodat capaciteit effectief en efficiënt ingezet wordt.

Het tijdig ontvangen van informatie over dreigingen en kwetsbaarheden op een manier die past bij het volwassenheidsniveau van de organisatie zodat deze organisatie de juiste maatregelen kan nemen, is een van de belangrijkste elementen voor een digitaal weerbaar Nederland. Om dit te realiseren moet de beschikbare capaciteit en expertise zo effectief mogelijk ingezet worden.

- Het NCSC, DTC en CSIRT-DSP worden samengevoegd tot één nationale cybersecurity autoriteit.
- Van de overige schakelorganisaties binnen het cybersecurity informatiedelingsstelsel wordt beoordeeld welke van hun taken centraal (bij de nationale cybersecurity autoriteit) of sectoraal belegd moeten worden.
- Wetswijzigingen om informatiedelen binnen het stelsel te bevorderen.
- Daarom start het kabinet met uitwerken van publiek-privaat platform voor informatie- en kennisdeling.

Bekijk de NLCS online: