Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Verdedigbaar Netwerk
Hoe doe je dat?

Aanpak voor **cybersecurity**

Statelijke actoren ontzien jouw sector niet

Hoe voorkom je dat jouw organisatie stil komt te liggen door een cyberaanval? En hoe voorkom je dat de voordeur wel op slot zit, maar aan de achterkant nog een raam openstaat?

Door de digitalisering van onze samenleving worden veel infrastructuren groter en ingewikkelder. Aanvallers maken misbruik van deze ontwikkeling om data te stelen. Jouw systemen staan voortdurend bloot aan opportunistische basisaanvallen. Een aanvaller hoeft maar één ingang te vinden, terwijl jij keuzes moet maken voor de beveiliging van je hele organisatie. Wat is daarin belangrijk en wat doe je eerst? De cybersecurityaanpak van de Unit Weerbaarheid helpt je deze keuzes te maken en deze te onderbouwen.

Wat is de Unit Weerbaarheid?

De Unit Weerbaarheid (uWBH) van de AIVD heeft als doel om Nederland digitaal veilig te maken tegen statelijke dreigingen en Advanced Persistent Threats (APT's). Wij zijn uniek doordat wij specialistische beveiligingskennis combineren met de inlichtingenpositie die we hebben als onderdeel van de AIVD. We werken nauw samen met onze veiligheidspartners MIVD, NCTV en NCSC. Gezamenlijk helpen we de Rijksoverheid, kennisinstellingen, vitale- en topsectoren om gevoelige informatie, -processen en -systemen te beschermen.

De uWBH-cybersecurityaanpak helpt jouw organisatie met:
- Het beveiligen van gevoelige informatie en kritische processen.
- Het maken van gefundeerde risico-inschattingen.
- Het kiezen van de juiste digitale beveiligingsmiddelen.

Hoe werkt het?

Met onze cybersecurityaanpak kun je snel zelf de juiste focus en kernpunten vinden bij risico's in het cyberdomein. Het geeft je houvast bij het maken van een moderne informatiebeveiligings-strategie en geeft structuur aan ingewikkelde beveiligingsdiscussies. Deze aanpak is gegroeid uit onze klantcontacten rond incidentafhandeling, risicomanagement en beveiligingsadvies.

Verbeter je IT-infrastructuur tegen cyberaanvallen

Een integrale en organisatiebrede aanpak, waarbij elk bedrijfsproces en onderdeel van de infrastructuur het gewenste beveiligingsniveau krijgt maakt het krachtig. Hiermee voorkom je keuzes voor te smalle puntoplossingen. Cybersecurity is breder dan alleen techniek. Voorkom keuzes voor een standaard- of te smalle oplossing. Streef naar wendbaarheid in de weerbaarheid van jouw organisatie. Cyberaanvallen zijn namelijk voortdurend aan verandering onderhevig.

Wat levert de uWBH-cybersecurityaanpak jouw organisatie op?

- Hogere weerbaarheid tegen (statelijke) cyberaanvallen.
- Goede bescherming van je vitale processen en vertrouwelijke en gerubriceerde informatie.
- Een plan van aanpak om de schade zoveel mogelijk te beperken als het toch misgaat.

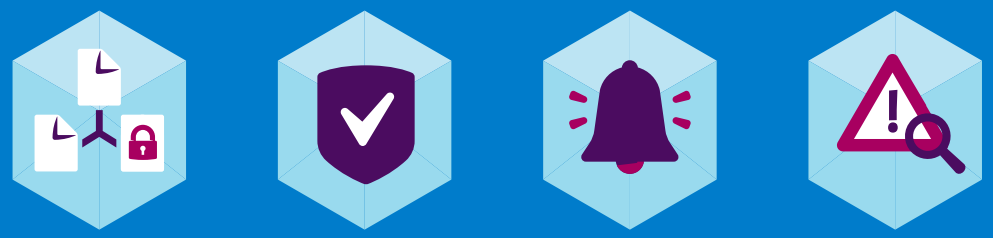
Deze aanpak van de AIVD sluit naadloos aan bij de praktijk én de bestaande normenkaders, zoals de BIO, het VIRBI, de ABRO en het NkBR. Deze aanpak is in lijn met de verschillende factsheets van het NCSC[1] om de weerbaarheid van je organisatie te vergroten.[2]

Heb je vragen?
Heb je bij het beveiligen van je bijzondere en gevoelige informatie vragen over de dreiging vanuit staten of andere APT's? Bel ons op 079-3205050 en vraag naar de uWBH. We helpen je graag om jouw organisatie digitaal weerbaarder te maken.

[1] www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid

[2] BIO = Baseline Informatiebeveiliging Overheid, VIRBI = Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie, ABRO= Algemene Beveiligingseisen Rijksoverheid Opdrachten (Vervangt ABDO per 2025), NkBR = Normenkader Beveiliging Rijkskantoren.

Onze cybersecurityaanpak is gebaseerd op **drie principes en vier ondersteunende pijlers**



De drie principes

Risicodenken

Met risicodenken bepaal je waar de grootste risico's zitten in je organisatie en hoe je de weerbaarheid van je organisatie verhoogt. Het is een wijze van risicoreductie waarbij je keuzes maakt in de mate van de bescherming van je infrastructuur en streeft naar een acceptabel restrisico.

Assume breach

Met het *assume breach*-principe ga je ervan uit van het feit dat je ooit slachtoffer wordt van een cyberaanval. Het is een 'mindset' die zorgt voor het creëren van de noodzakelijke scheiding van toegang. Hiermee verklein je de schade in een zo'n beperkt mogelijk deel van de organisatie en daarmee de impact op de gehele organisatie.

De Unit Weerbaarheid van de AIVD heeft uniek inzicht in de werkwijze van statelijke actoren. Op basis hiervan bepalen we de effectiviteit van maatregelen tegen deze dreiging en geven we advies hierover.

Continue verbetering

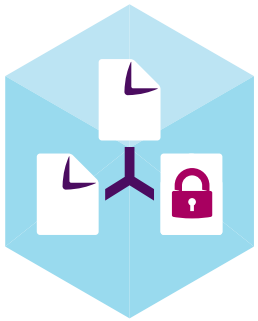
De wereld om ons heen verandert continu en deze veranderingen volgen elkaar ook steeds sneller op. Het is belangrijk dat organisaties hierop anticiperen en zich aanpassen. De digitalisering van de maatschappij zorgt voor een grote verscheidenheid, complexiteit en dynamiek van infrastructuren. Dit zal in de toekomst nog verder toenemen. Belangrijke trends zijn bijvoorbeeld de toename van public clouddiensten (en de integratie daarvan), *artificial intelligence, automation,*[3] *Post Quantum Cryptografie (PQC) en Internet of Things (IoT).*

Tegelijkertijd verandert de cyberdreiging op infrastructuren constant.[4] Actoren ontwikkelen nieuwe cyberaanvallen met onbekende kwetsbaarheden in software of systemen. Zelfs bij nieuwe leveranciers verandert het speelveld, omdat organisaties via hun toeleveringsketen indirect kunnen worden aangevallen door statelijke actoren. Ook verschuivende geopolitieke verhoudingen zorgen voor een ander dreigingslandschap.

[3] Gerelateerd aan IaC (Infrastructure as code), automate for efficiency en security automation.

[4] Op nctv.nl vind je de publicatie 'Cybersecuritybeeld Nederland'. In de publicatie lees je meer over de actuele digitale dreigingen en de belangen die daardoor kunnen worden aangetast. De publicatie wordt jaarlijks vernieuwd.

De vier ondersteunende pijlers



1 Contextanalyse

Met een contextanalyse beslis je voor je organisatie waar hoge weerbaarheid essentieel is en waar een lagere weerbaarheid acceptabel is. Op deze manier kunnen schaarse middelen efficiënt worden ingezet en kan je het remmende effect van IT-beveiliging op het functioneren van je organisatie beperken.

Belangrijk voor contextanalyse zijn:

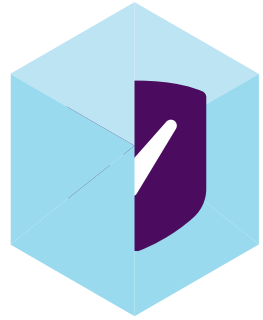
Inzicht in de kroonjuwelen
Je organisatie weet welke gegevens, toepassingen en (industriële) controlesystemen vitaal, vertrouwelijk of gerubriceerd zijn. Ook weet je welke informatie juist als open wordt gezien.

Inzicht in de dreiging
Je organisatie weet welke actoren belangstelling hebben voor je kroonjuwelen. Je weet welke aanvalspaden en aanvalsscenario's het meest waarschijnlijk zijn, zodat je prioriteiten kunt stellen.

Inzicht in de infrastructuur
Je organisatie weet hoe de eigen infrastructuur is opgebouwd, welke koppelingen met ketenpartners er zijn en waar de kroonjuwelen staan. Het is bekend welke systemen aanwezig zijn, waar de speelruimte van je *legacy* zit, hoe systemen zich normaal gedragen, wie de eigenaar is, wie de beheerder is en wie welke verantwoordelijkheden heeft bij een incident.

Inzicht in de organisatie
Je hebt een goed beeld van de beschikbare expertise. Die expertise kan liggen bij goed getrainde eigen medewerkers, of bij een dienstverlener. Daarnaast is de governance helder; je hebt op alle niveaus goede afspraken over verantwoordelijkheden en waar beslissingen gemaakt mogen worden.

Methode voor risicoanalyse
Je organisatie gebruikt een beproefde, objectieve en reproduceerbare methode voor risicoanalyse, die past bij de eigen cultuur en infrastructuur.



2 Weerstand

Voor een goede weerstand tegen cyberaanvallen moet je preventieve maatregelen nemen. Hiermee blokkeer of vertraag je cyberaanvallen en ontmoedig je aanvallers.

Belangrijk voor weerstand zijn:

Geëvalueerde producten
Kroonjuwelen met een hoog dreigingsrisico moeten goed beveiligd worden. Hiervoor zijn verschillende producten geëvalueerd door de uWBH (deze vind je op aivd.nl). Deze producten kunnen gebruikt worden met een inzetadvies.

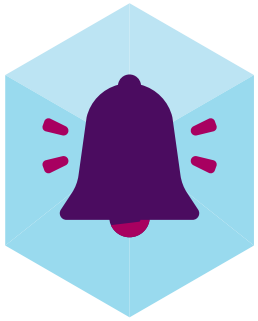
Identity & Access Management
Gebruikers, processen en systemen krijgen doelgericht toegang tot andere systemen, functies of gegevens met een sterke digitale identiteit. Deze digitale identiteit wordt verleend via een betrouwbaar proces van authenticatie/autorisatie in een goed ingericht systeem, en wordt betrouwbaar geregistreerd en beheerd. Je gebruikt bij voorkeur het least privilege access-principe.

Segmentering en afscherming
Waar mogelijk is de infrastructuur gesegmenteerd, zodat de kroonjuwelen extra zijn afgeschermd van de minder kritieke delen van de infrastructuur. Segmentering beperkt het aanvalsoppervlak van de kroonjuwelen flink, waardoor de schade van een geslaagde aanval beperkt wordt. Denk hierbij ook aan het toepassen van microsegmentatie en zero trust-architecturen.

Hardening
De infrastructuur is beveiligd en gehardend op het gekozen (preventieve) beveiligingsniveau. Waar nodig wordt gebruikgemaakt van software of hardware. Dit houdt bijvoorbeeld in dat producten van vertrouwde leveranciers worden gebruikt, systemen up-to-date zijn en dat alle hard- en software juist geconfigureerd is. Op alle geïdentificeerde aanvalspaden naar de kroonjuwelen toe zijn passende maatregelen genomen.

Beveiligingsbewustzijn
Naast technische maatregelen is beveiligingsbewustzijn en veilig gedrag belangrijk voor een goed beveiligingsniveau. Belangrijk hierbij is dat gebruikers en beheerders gemotiveerd zijn om veilig te werken, dat zij voldoende training, capaciteit en mogelijkheden hebben om veilig te werken en dat de IT-omgeving veilig gebruik en beheer ondersteunt.

Periodiek testen van de weerstand
Beveiligingsmaatregelen kunnen hun effectiviteit verliezen door verandering van de dreiging, nieuw ontdekte kwetsbaarheden, veranderingen in de IT-omgevingen en menselijke fouten in het beheer. Dit kun je voorkomen met periodieke testen middels pentesten en *red teaming*.



3 Detectie

Monitoring en detectie zijn bedoeld om aanvallen tijdig te ontdekken. Zeker gezien de toegenomen dreiging is het verlagen van de Mean Time to Detect (MTTD) steeds belangrijker. Dit bereik je onder andere door een detectievriendelijke infrastructuur, een zo volledig mogelijke logging en goed opgeleide professionals.

Belangrijk voor detectie zijn:

Network-based detectie
Dit is detectie op netwerkverkeer. Hiervoor is het nodig om chokepoints te maken op de randen van netwerken of tussen netwerksegmenten. Denk hierbij ook aan je cloudinfrastructuur. Detectie op het netwerkverkeer kan gaan om zowel statische detectie al detectie op afwijkingen. Omdat steeds meer netwerkverkeer versleuteld is, kan het nodig zijn om (in een gecontroleerde context) aan TLS-interceptie te doen.

Endpointdetectie
Met detectie op servers en end user-devices met logging of geheugenanalyse kan op individuele systemen (zowel fysiek als virtueel) nauwkeurige detectie plaatsvinden. De AIVD heeft voor Windows endpoints een Windows eventlogging-configuratiebaseline gepubliceerd. Gebruik deze.[5]

Active defence
Met honeypots, tokens en andere mechanismen kun je detectie uitlokken. Dit verhoogt de kans om ook aanvallers die voorzichtig te werk gaan op te sporen.

Correlatie en detectie ongebruikelijk gedrag
Afzonderlijke handelingen van een actor kunnen onschuldig lijken, maar in onderling verband wijzen op verdacht gedrag. Door correlatie en detectie van ongebruikelijk gedrag kan verdacht gedrag opgespoord worden met modellen van technieken, tactieken en procedures (TTP's) van de actor.

Alerte medewerkers
Ook spontane oplettendheid van beheerders en (andere) medewerkers op verdachte gebeurtenissen helpt bij detectie. Op deze manier kun je incidenten ontdekken die anders niet zouden opvallen. Zorg daarom voor een intern meldpunt waar medewerkers melding kunnen doen.

Hunting
Voor het verhogen van de weerbaarheid tegen statelijke actoren is het belangrijk om een continu huntingproces in te richten. Daarbij maak je niet alleen gebruik van bestaande detectiemiddelen, maar zoek je ook met intelligence over bijvoorbeeld de TTP's van de aanvallers naar verdacht gedrag.

[5] https://github.com/jscu-nl/logging-essentials

De Unit Weerbaarheid van de AIVD heeft indicatoren uit inlichtingenbronnen die zorgen voor een verbeterde detectie en detectiemethoden van met name statelijke actoren. De Unit Weerbaarheid neemt deel aan het Nationaal Detectie Netwerk (NDN).

4 Schadebeperking

Een organisatie moet adequaat kunnen reageren op een geslaagde cyberaanval en het hieruit volgende beveiligingsincident. Daarom is het belangrijk om digitaal onderzoek te laten doen en herstelwerkzaamheden in gang te zetten. De plannen hiervoor moeten al klaar liggen. Oefen hier ook mee.

Belangrijk voor schadebeperking zijn:

Incident respons proces
Het is belangrijk dat verantwoordelijkheden en mandaten vooraf duidelijk zijn, er concrete communicatielijnen zijn en er een centraal meldpunt is voor incidenten. Hier worden de incidenten geregistreerd en afgehandeld volgens vooraf afgesproken doorlooptijden, waarbij de voortgang voortdurend wordt bijgehouden. Er moet analysecapaciteit met voldoende kennis en middelen beschikbaar zijn om te analyseren wat er aan de hand is. Afspraken met interne en externe beheerders moeten vooraf gemaakt zijn. Het is cruciaal dat het incidentresponsproces aansluit op het crisismanagementproces, en de verantwoordelijkheden duidelijk belegd zijn.

Incident recovery plan
Met een passend recoveryplan kun je de continuïteit van bedrijfsprocessen en/of vitale functies garanderen, de schade beperken en zo snel mogelijk terugkeren naar de reguliere bedrijfsvoeringsprocessen. Voor deze processen en assets is het belangrijk dat je een passende back-upstrategie maakt en deze ook test.

Forensic readiness
Forensic readiness betekent dat bij een incident de juiste informatie, middelen en procedures beschikbaar zijn. Logging is hierin belangrijk. Zorg dat duidelijk is welke informatie nodig is om goed onderzoek te doen en zorg dat deze informatie wordt verzameld op een toegankelijke plek. In de praktijk blijken veel organisaties niet voorbereid te zijn op een incident, waardoor er uiteindelijk geen hoogwaardig onderzoek kan worden gedaan. Dit heeft als gevolg dat een organisatie niet weet wat er precies is gebeurd en daarom moet uitgaan van het worstcasescenario. *Forensic readiness* zorgt voor een kortere doorlooptijd van een onderzoek, waardoor normale bedrijfsvoeringsprocessen sneller kunnen worden hervat.

Heb je vragen?

Heb je vragen over het beveiligen van je vitale processen, vertrouwelijke en gerubriceerde informatie? Bel ons op 079-3205050 en vraag naar de Unit Weerbaarheid. We helpen je graag om jouw organisatie digitaal weerbaarder te maken.

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 Den Haag
Aivd.nl

Augustus 2024