Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Verdedigbaar Netwerk
Hoe doe je dat?

Aanpak voor **cybersecurity**

Statelijke actoren vallen óók overheidsinstanties aan

Hoe voorkom je dat jouw organisatie stil komt te liggen door een cyberaanval? En de spreekwoordelijke voordeur goed op slot zit, terwijl 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 (gevoelige) data te kunnen stelen. 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? Onze NBV-cybersecurityaanpak helpt je om zelf keuzes te maken voor je organisatie en deze te onderbouwen.

Wat is het NBV?

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) heeft als doel om Nederland digitaal veilig te maken tegen statelijke dreigingen en andere Advanced Persistent Threats (APT's). Wij zijn uniek doordat wij onze specialistische beveiligingskennis combineren met de bijzondere inlichtingenpositie die we hebben als onderdeel van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). We werken nauw samen met onze veiligheidspartners MIVD, NCTV en NCSC. Gezamenlijk helpen we de Rijksoverheid en vitale sectoren om bijzondere en gevoelige informatie zoals staatsgeheimen te beschermen.

De NBV-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 informatiebeveiligingsstrategie en geeft structuur aan ingewikkelde beveiligings-discussies. Deze aanpak is het resultaat van jarenlange expertise en in de praktijk bewezen informatiebeveiliging en risicomanagement.

Verbeter je IT-infrastructuur tegen cyberaanvallen

De kracht zit in de organisatiebrede aanpak, waarbij elk bedrijfsproces en onderdeel van de infrastructuur het gewenste beveiligingsniveau krijgt. Hiermee voorkom je keuzes voor standaard- en of te smalle puntoplossingen. Cybersecurity is breder dan alleen techniek. Voorkom keuzes voor een standaard- of te smalle oplossing.

Wat levert de NBV-cybersecurityaanpak op voor jouw organisatie?

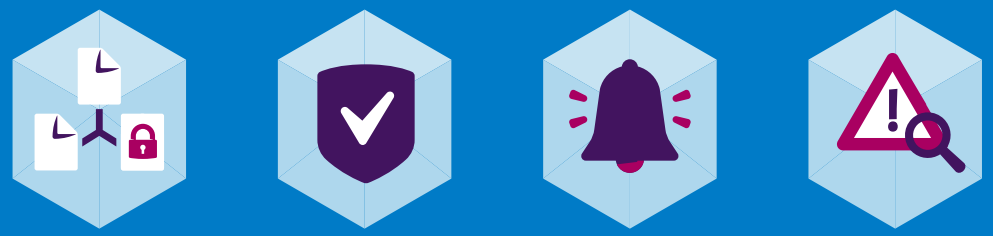
- ✓ Hogere weerbaarheid tegen statelijke cyberaanvallen.
- ✓ Goede bescherming van je vitale processen, vertrouwelijke en gerubriceerde informatie.
- ✓ Een plan van aanpak om de schade zoveel mogelijk te beperken voor als het toch misgaat.

Deze aanpak van de AIVD sluit naadloos aan bij de praktijk én de bestaande normen-kaders, zoals de *BIO, het VIRBI, de ABDO en het NKBR. Deze aanpak is in lijn met de verschillende factsheets van het NCSC (kijk op ncsc.nl) om de weerbaarheid van je organisatie te vergroten.

Heb je vragen?
Loop je bij het beveiligen van je gerubriceerde informatie tegen vragen aan? Bel ons op: 079-3205050 en vraag naar het NBV. We helpen je graag om jouw organisatie digitaal weerbaarder te maken.

*BIO = Baseline Informatiebeveiliging Overheid, VIRBI = Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie, ABDO = Algemene Beveiligingseisen Defensie Opdrachten, NKBR = Normenkader Beveiliging Rijkskantoren

Onze cybersecurityaanpak is gebaseerd op drie principes en vier ondersteunende pijlers



De drie principes

Risicodenken

Met risicodenken bepaal je hoe de juiste weerbaarheid de juiste plek krijgt in je organisatie. Waarbij afscherming en goede beveiliging van je kroonjuwelen natuurlijk een must is. Daarom moet je keuzes maken in de mate van de bescherming van je infrastructuur, waarbij je streeft naar een acceptabel restrisico.

Assume breach

Met *assume breach* bereid je je erop voor dat een cyberaanval slaagt, zodat je de duur en de schade van het beveiligingsincident beperkt. Het is voorstelbaar dat je ooit te maken krijgt met een beveiligingsincident waarbij een actor toegang heeft tot het netwerk van je organisatie.

Continue verbetering

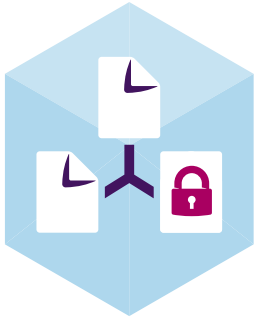
De wereld om ons heen verandert continu. Daarom is het belangrijk dat organisaties hierop anticiperen en zich aanpassen. De digitalisering van de maatschappij zorgt voor een grote verscheidenheid, complexiteit en dynamiek van infrastructuren die nog verder zal toenemen. Belangrijke trends zijn bijvoorbeeld de virtualisatie van systemen en netwerken, het thuiswerken, de toename van het gebruik van publieke clouddiensten en het *internet of things* (IoT).

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

Het NBV 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.

* Op nctv.nl vind je de publicatie 'Cybersecurity Beeld Nederland' uit 2021. Hierin lees je meer over digitale dreigingen en de belangen die daardoor kunnen worden aangetast.

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

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

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, hoe zij zich normaal gedragen, wie de eigenaar is, wie de beheerder is en wie welke verantwoordelijkheden heeft bij een incident.

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 hoge dreiging moeten goed beveiligd worden. Hiervoor zijn verschillende producten geëvalueerd door het NBV (deze vind je op aivd.nl). Deze producten kunnen gebruikt worden met een inzetadvies.

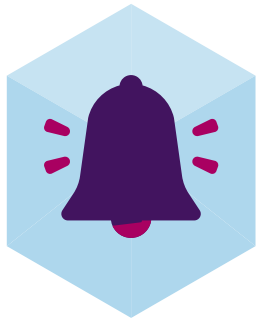
Identity & Access Management
Gebruikers, processen en systemen krijgen doelgericht toegang tot andere systemen, functies of gegevens met een sterke digitale identiteit. Deze digitale identiteit wordt verleend via een betrouwbaar proces van authenticatie/autorisatie in een goed ingericht systeem, en wordt betrouwbaar geregistreerd en beheerd.

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 beveiligingsoplossingen (zie geëvalueerde producten op aivd.nl). 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 beveiligings-bewustzijn en veilig gedrag een belangrijke maatregel 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 een 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 door periodieke testen.



3 Detectie:

Monitoring en detectie is bedoeld om aanvallen tijdig te ontdekken. Een detectievriendelijke infrastructuur heeft zogenaamde chokepoints. Dit zijn centrale knooppunten in de infrastructuur, zoals bijvoorbeeld cloud access security brokers (CASB) of netwerkkoppelvlakken waar logging- en netwerkdata gemonitord worden.

Belangrijk voor detectie zijn:

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

Endpoint-detectie
Detectie op servers en end-user-devices met logging of geheugenanalyse. Hiermee kan op individuele systemen (zowel fysiek als virtueel) nauwkeurige detectie plaatsvinden.

Detectie
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. Met deze methode kan verdacht gedrag opgespoord worden met modellen van technieken, tactieken en procedures (TTP's) van de actor.

Alerte medewerkers
Spontane oplettendheid van medewerkers en beheerders op verdachte gebeurtenissen kan aanvullend gebruikt worden voor detectie. Op deze manier kunnen incidenten ontdekt worden die anders niet op zouden vallen. 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.

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

4 Schadebeperking:

Een organisatie moet adequaat kunnen reageren op een geslaagde cyberaanval en het hieruit volgende beveiligings-incident. Daarom is het belangrijk om digitaal onderzoek te (laten) doen en herstelwerkzaamheden in gang te zetten.

Belangrijk voor schadebeperking zijn:

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

Incident recovery plan
Met een passend recovery plan 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-up-strategie maakt en deze test.

Forensic readiness
Met forensic readiness zijn de juiste informatie, middelen en procedures beschikbaar bij een incident. 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. Met als gevolg dat een organisatie niet weet wat er precies is gebeurd en moet uitgaan van het *worst case scenario*. Forensic readiness zorgt voor een kortere doorlooptijd van een onderzoek, waardoor normale operaties sneller hersteld kunnen worden.

Heb je vragen?

Loop je bij het beveiligen van je gerubriceerde informatie tegen vragen aan? Bel ons op: 079-3205050 en vraag naar het NBV.
We helpen je graag om jouw organisatie digitaal weerbaarder te maken.

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010 | 2500 EA Den Haag
T (079) 320 50 50

oktober 2021