NIPV
Nederlands
Instituut
Publieke
Veiligheid

Bestuurlijke Netwerkkaarten Crisisbeheersing

Netwerkkaart 20
Cybersecurity

Nederlandse Academie voor Crisisbeheersing en Brandweerzorg
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.nipv.nl
info@nipv.nl
026 355 24 00

Colofon

Ondanks de aan de samenstelling van de tekst bestede zorg kan de samensteller geen aansprakelijkheid aanvaarden voor schade ontstaan door eventuele fouten c.q. onvolkomenheden in deze publicatie.

Om deze publicatie te kunnen blijven ontwikkelen en verbeteren, ontvangen wij graag commentaar en suggesties ter verbetering. Vragen of opmerkingen kunt u sturen naar info@nipv.nl, onder vermelding van Bestuurlijke Netwerkkaarten.

Auteur(s)	Merijn ten Dam
Contactpersoon	Merijn ten Dam

Datum	2025
Status	handboek
Versie	202504

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.

20 Cybersecurity

Voor telecommunicatie (en providers), zie Bestuurlijke Netwerkkaart telecommunicatie
Voor media/omroepen, zie Bestuurlijke Netwerkkaart media

Crisistypen	>	inbreuk internetveiligheid (cybersecurity)
Bevoegd gezag	>	minister van Justitie en Veiligheid (JenV) (computercriminaliteit, persoonlijke levenssfeer en cybersecurity)
	>	minister Economische Zaken (EZ), minister Infrastructuur en Waterstaat (IenW) (toezicht op cybersecurity van aanbieders van digitale dienstverleners en essentiële diensten)
Soorten maatregelen	>	eigen maatregelen door aanbieders van essentiële diensten en digitale dienstverleners
	>	eigen maatregelen departementen
	>	handhaving jegens digitale dienstverleners en aanbieders van essentiële diensten
	>	waarschuwingen en advisering bij een dreiging of daadwerkelijke inbreuk op internetveiligheid (cybersecurity)

Algemeen

> Bedrijven en instellingen, als ook overheid, zijn zelf verantwoordelijk voor de continuïteit van hun diensten: zij treffen maatregelen om een verstoring zo spoedig mogelijk op te heffen.

Eigen maatregelen

> Grote digitale dienstverleners (online marktplaatsen, clouddiensten, zoekmachines) en zogeheten aanbieders van essentiële diensten zijn verplicht digitale verstoringen zo snel mogelijk te verhelpen en de gevolgen zoveel mogelijk te beperken.

> Aanbieders van essentiële diensten zijn onder meer:
  - de landelijke en regionale elektriciteits- en gasnetbeheerders;
  - (grote) elektriciteitsbedrijven;
  - gasleveranciers, gasopslag en gasraffinage;.
  - de NAM en de Stichting Centraal Orgaan Voorraadvorming Aardolieproducten (COVA);
  - de Rotterdamse Haven
  - luchthaven Schiphol, waaronder de luchtverkeersleiding, Aircraft Fuel Supply B.V., Koninklijke marechaussee en luchtvaartmaatschappijen;
  - drinkwaterbedrijven;
  - ProRail en NS;
  - Rijkswaterstaat (beheer weginfrastructuur)
  - beheerders van digitale infrastructuur, zoals grote internetknooppunten en Stichting Internet Domein Registratie (SIDN), als beheerder van toplevel-

domeinnaam .nl en DNS-dienstverlener.

> De financiële kerninfrastructuur is al op basis van andere regelgeving verantwoordelijk voor de continuïteit van hun diensten (inclusief cyberveiligheid). Zie Bestuurlijke Netwerkkaart Financieel verkeer, onder kopjes Continuïteit betalings- en effectenverkeer en Cybersecurity.
> Voor de rijksoverheid is de Chief Information Security Officer Rijk (CISO Rijk) bevoegd om bij rijksbrede informatiebeveiligingsincidenten en -calamiteiten, namens de Secretaris-Generaal van Binnenlandse Zaken en Koninkrijksrelaties, aanwijzingen te geven met betrekking tot de informatieprocessen van ministeries en maatregelen te laten treffen om de beveiliging daarvan te herstellen en verdere schade te beperken. Per ministerie is de departementale CISO bevoegd.
> De staatsecretaris speelt in dit verband een rol bij de coördinatie van de eigen maatregelen van de rijksoverheid bij grote cyberincidenten.

Toezicht

> Het toezicht is sectoraal belegd:
  – de Rijksinspectie Digitale Infrastructuur (RD), amens minister EZ, voor de grote digitale dienstverleners en beheerders van digitale infrastructuur en de energiesector;
  – de Inspectie Leefomgeving en Transport (namens de minister IenW) voor de drinkwaterbedrijven, transport (spoor en weg), Schiphol en de Rotterdamse haven.
> De toezichthouder kan aanwijzingen geven en spoedbestuursdwang toepassen.

Overheidsinterventie in de ICT-sector

> Een interventie jegens de ICT-sector als zodanig is voorbehouden aan de minister van EZ en kan (ook) plaatsvinden op basis van de Telecommunicatiewet. Het aanbieden van internettoegang valt onder 'het aanbieden van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten' in de zin van de Telecommunicatiewet (zie verder *Bestuurlijke Netwerkkaart Telecommunicatie*).

Cybercrime

> De aanpak van cybercrime valt onder de reguliere opsporingsverantwoordelijkheid van politie en OM. Cybercrime kan leiden tot een digitale verstoring.

Computercrisisteams

> De operationele respons op beveiligingsincidenten en verstoringen met computers of netwerken vindt in veel organisaties plaats in zogeheten CERTs/CSIRTs (Computer Emergency Response Teams/Computer Security and Incident Response Teams), gespecialiseerde computercrisisteams van ICT-professionals. Er zijn CERTs voor grote bedrijven en instellingen, maar ook voor sectoren, zoals de voor de zorgsector (Zorg-CERT). CSIRTs zijn de computercrisisteams met een wettelijke basis.

Nationaal Cyber Security Centrum

> Het Nationaal Cyber Security Centrum (NCSC) valt onder het ministerie van JenV.
> De CSIRTs voor de aanbieders van essentiële diensten en voor de rijksoverheid vallen onder het NCSC. De CSIRT DSP (digitale dienstverleners) valt onder het ministerie van EZ.
> Bij een dreiging of daadwerkelijke inbreuk doet het NCSC waarschuwingen uitgaan en kan het overheden en bedrijfsleven bijstaan en adviseren over te treffen maatregelen.
> Afhankelijk van de dreiging of het incident nemen ICT-experts van vitale aanbieders / sectoren deel in de *ICT Response Board* (IRB) dat door het NCSC wordt gefaciliteerd. De IRB is een publiek-privaat samenwerkingsverband, dat bij elkaar komt wanneer een grote ICT-crisis dreigt of zich voordoet in meerdere sectoren. De

IRB zal indien nodig ook direct waarschuwingen doen uitgaan en adviseert binnen de nationale crisisbesluitvormingstructuur de rijksoverheid (zie verder *Bestuurlijke Netwerkaart Rampenbestrijding algemeen en handhaving openbare orde*).
> Het NCSC onderhoudt contacten met buitenlandse CSIRTs/CERTs en met het Europese ENISA (zie hierna).

Militaire steunverlening cybersecurity

> Militaire steunverlening: op verzoek van de minister van JenV kan Defensie de CSIRT-functie ondersteunen van de NCSC (voor de rijksoverheid en de aanbieders van essentiële diensten). In andere gevallen kan de desbetreffende minister, commissaris van de Koning, dijkgraaf of burgemeester om militaire steun verzoeken.
> In geval van cybercrime kan Justitie en Veiligheid/Openbaar Ministerie ook militaire (politie)bijstand aanvragen ten behoeve van de opsporing.
> Zie verder Bestuurlijke Netwerkkaart Defensie.

Afstemming met veiligheidsregio's

> Samenwerking tussen aanbieders van vitale diensten (vitale sectoren) en veiligheidsregio's is in enkele gevallen vastgelegd in convenanten. *Zie desbetreffende bestuurlijke netwerkkaarten.* De convenanten hebben niet specifiek betrekking op cyberincidenten.
> Op basis van die convenanten kan een liaison van een vitale aanbieder desgevraagd zitting nemen in het regionaal beleidsteam. Dit kan ook anders zijn georganiseerd door een liaison van de veiligheidsregio in het crisisteam van de aanbieder(s).
> In geval van grote cyberverstoringen zal de aanpak van de verstoring op nationaal niveau plaatsvinden, in de nationale crisisstructuur. Het NCC informeert de veiligheidsregio's. Zie verder deel *Nationale afstemming* in *Bestuurlijke Netwerkkaart Rampenbestrijding algemeen en handhaving openbare orde*.

Burgemeester en voorzitter veiligheidsregio

> De burgemeester of voorzitter veiligheidsregio heeft geen invloed op het functioneren van de sector zelf (de continuïteit van de verlening van vitale diensten of de aanpak van een cyberincident als zodanig).
> De burgemeester of voorzitter veiligheidsregio is verantwoordelijk voor aanpak van de effecten voor de openbare orde en de openbare veiligheid.

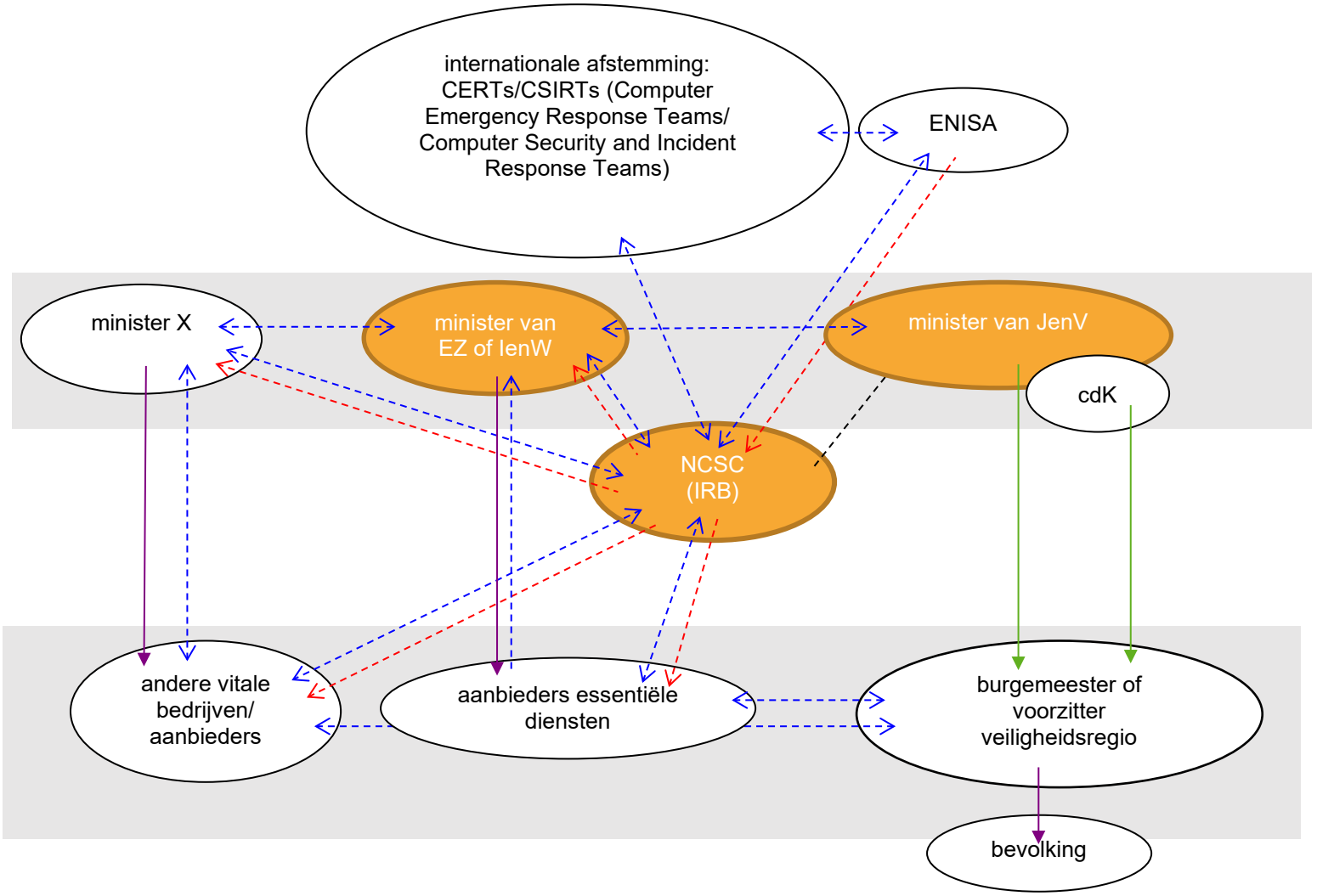
Europese Unie

> Het Europees Agentschap voor netwerk- en informatiebeveiliging/*European Network and Information Security Agency* (ENISA) kan bijstand leveren aan lidstaten bij preventie en preparatie, maar ook bij respons (waaronder leveren van expertise).

functionele ketens vitaal

algemene keten

cybersecurity



- Informatie en afstemming
- Bijstand
- Maatregelen jegens bevolking/bedrijven
- Bestuurlijk toezicht, tevens onderlinge informatie
- Interne lijn

NB 1. Het Nationaal Cyber Security Centrum (NCSC) informeert en adviseert overheden en (vitaal) bedrijfsleven en onderhoudt contacten met buitenlandse zusterorganisaties. Het merendeel van deze contacten is niet expliciet in dit schema weergegeven.

NB 2: Het Agentschap Telecom oefent het toezicht uit namens de minister EZK; ILT oefent het toezicht uit namens de minister van IenW.

NB 3: De digitale dienstverleners zijn voor de overzichtelijkheid niet opgenomen in dit schema. Hun informatielijnen mbt cybersecurity lopen direct naar EZK en niet naar NCSC.

NB 4: De CISO Rijk is voor de overzichtelijkheid niet opgenomen in dit schema; het betreft de interne maatregelen van de rijksoverheid bij cyberincidenten.

NB 5: De AP (Autoriteit persoonsgegevens) vervult geen rol in de responsfase