Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Afdeling Wbni

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Van:
5.1.2.e

Review:
5.1.2.e
5.1.2.e
5.1.2.e

Datum
13 Oktober2020

Bijlagen
1 grafische weergave stappen
2 RACI-schema

memo

Procedure Risicomodel

Risicobeoordeling (risicomodel) voor het bepalen van thema-inspecties en focus bij reguliere inspecties

Inleiding

In deze memo is het proces "risicomodel" uitgeschreven. Het doel van dit risicomodel is om inzicht te krijgen in het risicobeeld van de AEDs. Dit levert input voor het bepalen van de jaarlijkse onderwerpen voor de thema-inspecties bij de AEDs die opgenomen worden in de jaarplanning. Ook kan het richting geven bij het selecteren van verdiepingsonderwerpen voor de reguliere inspecties of het (laten) uitvoeren van themaonderzoeken.

Het risicomodel/analyse wordt jaarlijks uitgevoerd. Aan het begin van het jaar wordt bepaald en geagendeerd wanneer de risicoanalyse plaats gaat vinden.

Het risicomodel geeft invulling aan informatiegestuurd en risicogericht toezicht, waarbij op basis van informatie en gepercipieerde risico's focus wordt aangebracht in de toezichtwerkzaamheden.[1] Op deze wijze zet Agentschap Telecom de beschikbare middelen zo effectief en efficiënt mogelijk in voor zijn toezichtstaak.

Risicomodel als input voor thema-inspecties, reguliere inspecties en thema onderzoeken

Het doel van de thema-inspectie is om een diepgaand beeld van een onderdeel van de informatiebeveiliging van de essentiële dienst van de AED te verkrijgen. Bij het risicomodel wordt informatie van zowel interne als externe risicofactoren en toekomstige ontwikkelingen verzameld en verwerkt in het risicomodel. Op basis van deze analyse worden mogelijke onderwerpen voor de thema-inspecties bepaald en wordt richting gegeven bij het selecteren van verdiepingsonderwerpen voor de reguliere inspecties. Ook levert het onderwerpen op voor thema-onderzoeken.

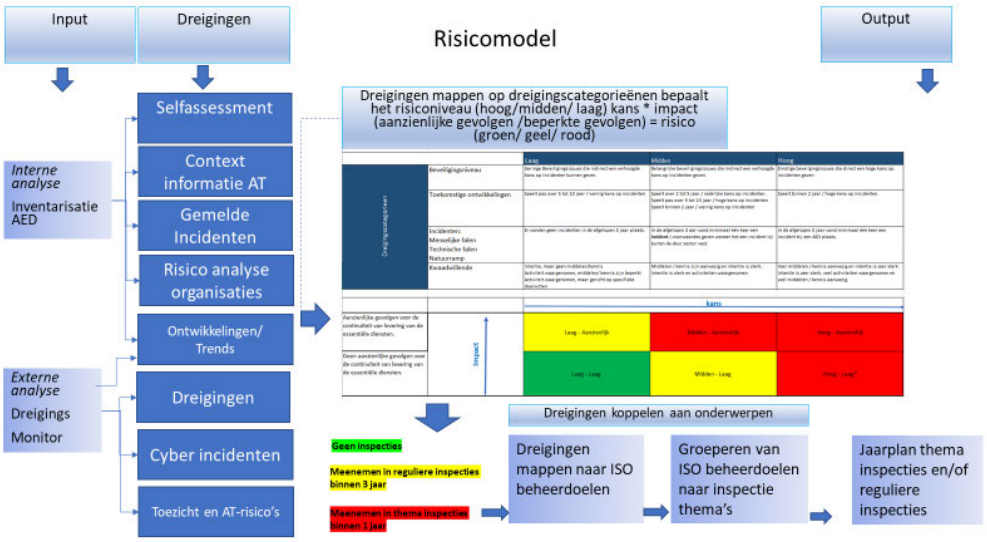
Objecten: per AED-sector wordt een risicoanalyse opgesteld waaronder (niet limitatief):

- Elektriciteit:
  - Regionale distributie elektriciteit Netwerkbeheerders
  - Landelijke transport en distributie elektriciteit: Tennet
  - Beheerders van een (grensoverschrijdende) interconnector
- Gas:

[1] Agentschap Telecom – Jaarplan Toezicht 2020 p. 16

    - Gasproductie, landelijk transport en distributie gas: NAM en opslag Norg
    - Regionale distributie gas
- Energieproducenten;
    - Energiecentrales
    - Zonneparken
    - Windturbines
    - Olievoorziening
- Opslag voorraadvorming Aardolieproducten (COVA)
- Internet en datadiensten 'digitale infrastructuur';
    - Internet Exchange (Ams-ix, NL-IX)
    - .nl top level domain (SIDN)

Hieronder de schematische weergave van het risicomodel:
De uit te voeren risicoanalyse voor het risicomodel bestaat uit de volgende input van informatie bestaande uit interne analyse en externe analyse;



Interne analyse

- Uitgevoerde risicoanalyse(s) van de AED zelf;
- Ontwikkelingen naar aanleiding van gesprekken met AEDs;
- Relevante Incidenten van desbetreffende AEDs;
- Resultaten assessments bij AEDs;
- Contextinformatie AT op basis van inventarisatie bij AEDs;

Externe analyse

- Dreigingen vanuit de dreigingsmonitor;
- Ontwikkelingen/ trends vanuit de dreigingsmonitor
- Incidenten sectorbreed uit dreigingsmonitor.

Aan de hand van workshops wordt met het Wbni-team dreigingen en ontwikkelingen geplot in het risicomodel. De belangrijkste dreigingen worden geplot in de dreigingscategorieën en bepaalt het risiconiveau. Deze kunnen laag, midden en hoog zijn. Vervolgens wordt de impact bepaald deze kunnen verdeeld worden in aanzienlijke of beperkte gevolgen voor de continuïteit. Risiconiveau * Impact = Risico.

Vervolgens wordt samen bepaald welke risico's als hooggekwalificeerd worden. De risico's worden geplot op de ISO-beheerdoelen (control objectives) en worden de ISO-beheerdoelen gegroepeerd naar mogelijke inspectie-onderwerpen. Hoge risico's vragen om aandacht en dienen als input voor onderwerpen voor de thematische inspecties en voor verdiepingsonderwerpen voor de reguliere inspecties, evenals thema-onderzoeken. De beschreven methode is een raamwerk waarbij het gebruik van 'gezond verstand' en vakkundige oordeelsvorming een grote rol blijft spelen.

Richtlijnen voor het toepassen van het risicomodel

1. Inplannen workshop per sector
   Initiator: coördinator per AED sector

Plan per sector een workshop van een dagdeel in met de andere specialistisch inspecteurs die betrokken zijn bij de desbetreffende AED-sector en optioneel de afdelingshoofd Toezicht Digitale Weerbaarheid voor het toepassen van het risicomodel.

2. Aanmaken opslaglocatie en klaarzetten template
   Initiator: coördinator per AED sector

Maak een nieuwe jaarmap (202x) aan op de buiten reikwijdte. Maak vervolgens per AED-sector een map aan. Importeer vervolgens het template risicomodel[2].

3. Voorbereiden interne sectoranalyse t.b.v. workshop
   Initiator coördinator per sector

Eén inspecteur per AED-sector verzamelt uit bestaande documentatie en door navraag bij zijn collega's de risicoanalyses, assessments en relevante informatie die verkregen zijn uit relatiebeheer met de diverse AED en vult de template risicomodel daarmee in.

- Netbeheerder;
- COVA;
- NAM;
- Digitale infrastructuur: Internet Exchange (Ams-ix, NL-IX);
- Digitale infrastructuur: .nl top level domain (SIDN);
- Energieproducenten.

[2] buiten reikwijdte

Vul het template risicomodel in door de tabbladen te vullen

Tabblad uit het template risicomodel	Actie van de coördinator
"Assessment Resultaten"	Gebruik de meest recente assessment resultaten van de diverse AEDs. Vul Assessment onderwerpen met score < 3 in het tabblad. (Maak eventueel gebruik van de gegevens van vorige jaar gebruikte risicomodel en actualiseer het eventueel)
"Context informatie AT"	Vul relevante aanvullende informatie/ constateringen die betrekking hebben op mogelijke risico's over de AEDs die in gespreksverslagen of aantekeningen zijn vastgelegd.
"Incidenten Historie"	Verzamel de gemelde incidenten van AEDs en vul de gemelde incidenten in het tabblad "Incidenten Historie".
"Risicoanalyse"	Gebruik de meest recente risicoanalyse van AEDs die AT tot de beschikking heeft en vul relevante risico's in het risicomodel. (Maak eventueel gebruik van de gegevens van vorige jaar gebruikte risicomodel en actualiseer het)[3]

4. Voorbereiden externe sectoranalyse t.b.v. workshop
   Initiator: coördinator per sector

Eén inspecteur per sector maakt met behulp van de dreigingsmonitor[4] een eerste analyse van de belangrijkste dreigingen, incidenten binnen de sector (wereldwijd) en (toekomstige) ontwikkelingen en zet dit in de template. I

Vul het template risicomodel in door de tabbladen te vullen:

Tabblad uit het template risicomodel	Actie van de coördinator
"Ontwikkelingen Trends"	Selecteer uit de dreigingsmonitor de meest relevante ontwikkelingen, trends voor de desbetreffende AED-sector. Dit is te vinden in het document dreigingsmonitor tabblad " monitor" filter op (toekomstige) ontwikkelingen. Voeg daarnaast ook evt. ontwikkelingen/trends van AED-sector naar aanleiding van informele gesprekken met AED (relatiebeheer).
"Dreigingen"	Selecteer uit de dreigingsmonitor de mogelijke dreigingen voor de desbetreffende AED-sector en leg het vast in het risicomodel. Dit is te vinden in het document dreigingsmonitor tabblad " monitor" filter op dreiging
"Cyber incidenten"	Toelichting: Selecteer uit de dreigingsmonitor de mogelijke dreigingen voor de desbetreffende AED-sector als het gaat om cyberincidenten waar men eventueel rekening moet houden. Dit is te vinden in het document dreigingsmonitor tabblad " monitor" filter op incident
"Toezicht en AT-risico"	Selecteer uit de dreigingsmonitor de Toezicht & AT-risico's wat mogelijk relevant is voor de AED-sector. Dit is te vinden in het document dreigingsmonitor tabblad " Toezicht- & AT-risico's".

[3] Het opvragen van risicoanalyse gebeurd bij een thema inspectie voor de AEDs. Wanneer er sprake is van een reguliere inspectie van de AEDs wordt er geen aanvullende risicoanalyse opgevraagd.

[4] buiten reikwijdte

5. Voer per sector risicoanalyse uit (workshop)
   Initiator: coördinator per sector leidt workshop

Voorbereiding
De aangewezen inspecteur deelt ten minste een week van tevoren het voor zover ingevulde risicomodel met de deelnemers van de workshop.

Uitleg proces workshop
De inspecteur die de workshop leidt, legt het proces voor de workshop uit.

Bespreken interne sectoranalyse
De inspecteurs bespreken de informatie die is opgehaald voor de interne analyse. Dat wil zeggen de assessmentresultaten van AEDs binnen de betreffende sector, de contextuele informatie die AT heeft, de incidenten die geregistreerd zijn. Op basis daarvan worden de belangrijkste risico's in kaart gebracht. Deze worden op de heatmap geplot.

Bespreken externe sectoranalyse
De inspecteurs bespreken de informatie die is opgehaald voor de externe analyse. Op basis daarvan worden de belangrijkste risico's in kaart gebracht. Deze worden op de heatmap geplot.

Bespreken totaalanalyse
De inspecteurs bespreken het totaal van interne en externe sectoranalyse en komen tot een onderbouwde keuze van de belangrijkste risico's en worden geplot in het risicomodel. Vervolgens wordt samen bepaald welke risico's als hooggekwalificeerd worden. Hoge risico's dienen als input voor onderwerpen voor onderzoeken. Let op! Thema's die in voorgaande jaar reeds is onderzocht kan misschien nu nog steeds hoog scoren maar het is niet de bedoeling deze thema's op nieuw te gaan selecteren voor onderzoeken.

6. Bepaal ISO-beheerdoelstellingen aan de hand van het uitgevoerde risicomodel.
   Initiator: coördinator per sector

Maak gebruik van ISO-beheerdoelen (control objectives) om deze belangrijkste risico's te mappen op beheerdoelstellingen (zie NEN ISO IEC 27001 NL.pdf[5]). Sommige benoemde risico's kunnen meerdere ISO-beheerdoelen raken. Leg dit vast in het risicomodel tabblad "totaal analyse". Bepaal aan de hand van de geselecteerde beheerdoelstellingen wat een geschikt overkoepelend thema is. Koppel de resultaten terug aan de deelnemers van de workshop en verifieer of zij de onderwerpen onderschrijven.

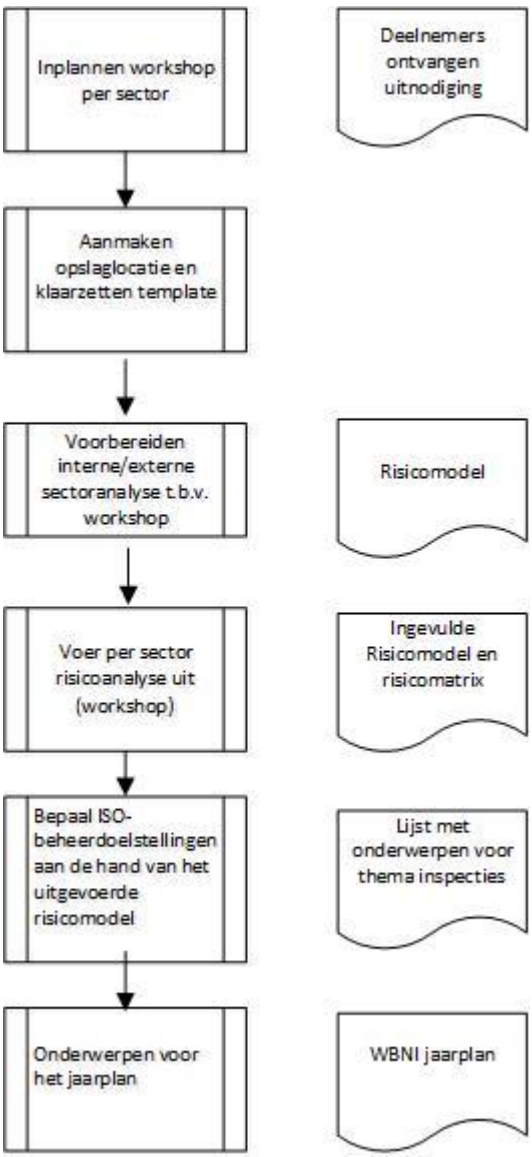
7. Onderwerpen voor het jaarplan
   Initiator: coördinator per sector

Zorg dat de onderwerpen van elke AED-sector is vastgesteld. Bepaal of de onderwerpen aan de hand van thema inspecties of via verdiepingsonderwerpen bij

[5] buiten reikwijdte

de reguliere inspecties worden onderzocht. Eventueel kan er ook gekozen worden om een thema onderzoek uit te voeren.

1. Bijlage: grafische weergave stappen



2. Bijlage RACI-schema

Stap	Taak	Afdelingshoofd Digitale Weerbaarheid	Rol: coördinator per AED sector	Specialistische inspecteur	Coördinerende inspecteur
1	Inplannen workshop per sector	A	R	I	I
2	Aanmaken opslaglocatie en klaarzetten template	A	R		
3	Voorbereiden interne sectoranalyse	A	R	C	I
4	Voorbereiden externe sectoranalyse	A	R	C	I
5	Voer per sector risicoanalyse uit	A	R	R	I
6	Bepaal ISO-beheerdoelstellingen aan de hand van het uitgevoerde risicomodel	A	R	C	I
7	Onderwerpen voor het jaarplan	A	R	I	I

R= Responsible
A= Accountable
C= Consulted
I = Informed

Dreigingmonitor

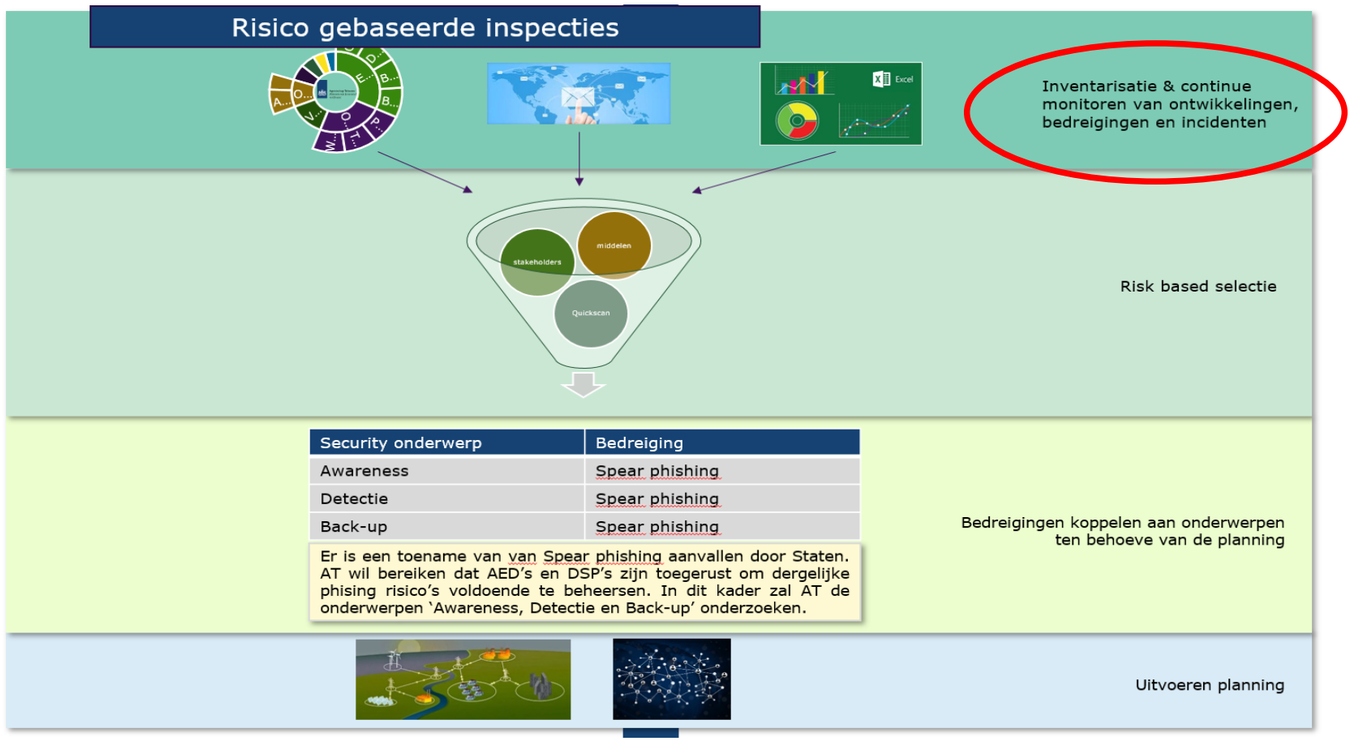
Deze dreigingsmonitor geeft input aan het risicogebaseerde selectiemodel voor het WBNI-toezicht, zoals onderstaand weergegeven.
Het helpt hiermee invulling te geven aan informatiegestuurd en risicogericht toezicht in lijn met het Jaarplan Toezicht 2020.

- Het tabblad "Monitor" bevat:
  - "Incidenten" -> omvat incidenten, zoals aanvallen, storingen of calamiteiten.
  - "Dreigingen" -> omvat relevante dreigingen voor ons toezichtsveld, in het bijzonder t.a.v. kwaadwillenden.
  - "Toekomstige ontwikkelingen" -> omvat (toekomstige) ontwikkelingen.
- Het tabblad "Toezicht- & AT-risico's omvat algemene risico's voor het WBNI-toezicht van AT.
- Het tabblad "Bronnen dreigingsinformatie" omvat digitale bronnen voor dreigingsinformatie.

Het tabblad "Werkblad" bevat het achterliggende datamodel. De "Changelog dreigingsmonitor" omvat een wijzigingslogboek van deze dreigingsmonitor, zodat je kunt zien wat er veranderd is.

Netwerkmaatschappij vraagt om stelseltoezicht
"De rol van de toezichthouder verandert. Toezicht wordt steeds meer één van de spelers in een ingewikkelde waardeketen. De toezichthouder gaat hierbij informatiegestuurd en risicogericht te werk. Hierbij is toezicht minder gericht op het afdwingen van naleving, en meer gericht op de verantwoordelijkheid van de markt. De vraag naar (wetenschappelijke) onderbouwingen van toezicht en het monitoren van effecten neemt toe." (Elektronische Communciatiedomein Radar AT 2019-2024))

Toezichtsmodel WBNI



Specifieke toezichtsinformatie over AEDs waar wij toezicht op houden.
(Deze informatie zit niet in de dreigingsmonitor, maar wordt wel toegepast in de risk-based selectie)

Reguliere inspecties	Interne risicoanalyses AEDs	Context-informatie over AEDs door AT	Incidenten AEDs (gemelde incidenten)

Laag	Midden	Hoog

Begrippenkader en afkortingen

Incident (ISO 27035)
Een of meerdere gerelateerde geidentificeerde inbreuken op informatiebeveiliging die schade kunnen toebrengen aan een organisatie of zijn bedrijfsvoering.

Dreiging (ISO 27005)
Een dreiging heeft de potentie om schade toe te brengen aan assets, zoals informatie, processen, systemen en daarmee organisaties. Dreigingen kunnen een menselijke of natuurlijke oorsprong hebben en kunnen opzettelijk of onopzettelijk zijn.

Toekomstige ontwikkeling
Een ontwikkeling die in de toekomst gevolgen kan hebben voor de continuïteit van essentiële diensten.

Trend
Een trend is een patroon van geleidelijke verandering waarin zich iets ontwikkelt naar een bepaalde richting. Het zijn geen concrete dreigingen of incidenten.

Risico (ISO 31000)
Effect van onzekerheid op (het behalen van) doelstellingen. Dit kan positief of negatief zijn. Risico's worden meestal uitgedrukt in termen van risicobronnen, mogelijke gebeurtenissen, de gevolgen en de waarschijnlijkheid daarvan.

Kwetsbaarheid (ISO 27005)
De kwetsbaarheid van een asset of assets die misbruikt kunnen worden door een of meerdere dreigingen, waarbij een asset alles is wat waarde heeft voor een organisatie, zijn business operations en de continuiteit daarvan, inclusief informatiebronnen die de missie van de organisatie ondersteunen.

OSINT
Open source intelligence - Openbare bronnen voor dreigingsinformatie.

Cyber Threat Intelligence (CTI)
CTI is een ander woord voor

Dreigingsmonitor

Toekomstige ontwikkelingen
(filter in monitor op 'trend' in kolom B)

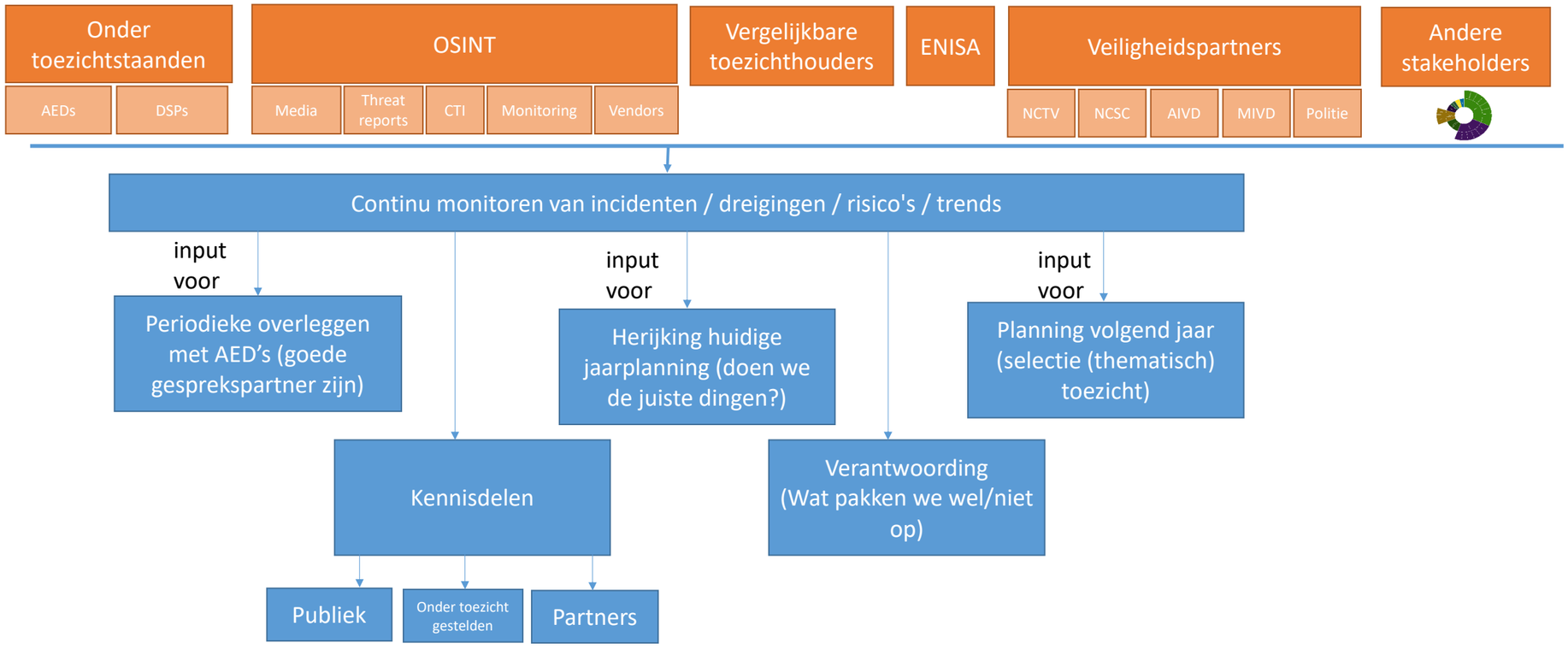
Incidenten en dreigingen
(filter in monitor op oorzaak incident/dreiging in kolom D)

Dreigingscategorieën	Beveiligingsniveau	Laag	Midden	Hoog
	Beveiligingsniveau	Geringe beveiligingsissues die indirect een verhoofde kans op incidenten kunnen geven	Belangrijke beveiligingsissues die indirect een verhoogde kans op incidenten geven	Ernstige beveiligingsissues die direct een hoge kans op incidenten geven.
	Toekomstige ontwikkelingen	Speelt over 5 tot 10 jaar met lage kans op incidenten	- Speelt over 5 tot 10 jaar met hoge kans op incidenten - Speelt over 2 tot 5 jaar met middelgrote kans op incidenten - Speelt binnen 2 jaar met lage kans op incidenten	Speelt binnen 2 jaar met hoge kans op incidenten
	Incidenten: - Falen van systeem - Natuurlijke oorzaak - Menselijke fout - Falen van derde partijen (keten)	In de afgelopen 3 jaar vond er buiten Europa binnen de sector een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond binnen de sector binnen Europa een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond een van de genoemde incident bij een AED in Nederland plaats
	Incidenten en dreigingen door kwaadwillenden	Doelwit is sectoronafhankelijk Kennis/middelen zijn beperkt Activiteit is waargenomen	Doelwit is de sector binnen Europa Kennis/middelen aanwezig Activiteit is waargenomen	Doelwit is de sector in Nederland Kennis/middelen aanwezig
		Kans		
Aanzienlijke gevolgen voor de continuïteit van de levering van de essentiële diensten	Impact	Laag - Aanzienlijk	Midden - Aanzienlijk	Hoog - Aanzienlijk
Geen aanzienlijke gevolgen voor de continuïteit van de levering van de essentiële diensten		Laag - Laag	Midden - Laag	Hoog - Laag Rood *

dreigingsinformatie. De volgende vormen kunnen worden onderscheiden:
- Operationeel (indicators of compromise, zoals URLs, IP's, filehashes etc).
- Tactisch (informatie over intentie, competentie en activiteiten van actoren en andere oorzaken van dreigingen en incidenten)
- Strategisch (Belangrijkste trends en ontwikkelingen qua dreigingen)

Monitoring

Informatiebronnen



Datamodel en taxonomie

Bij een dreigingsmodel is het belangrijk om weldoordachte keuzes te maken qua datamodel en taxonomie. Voor deze dreigingsmonitor is gekozen om zoveel mogelijk aan te sluiten bij bestaande en gangbare datamodellen en taxonomieën. Dit maakt het eenvoudiger om in de toekomst met andere partners samen te werken.

Cybersecurity Incident Taxonomy CG Publication 04/2018 van de NIS Cooperation Group
Deze taxonomie wordt gebruikt voor:
- Sectoren (aangevuld met subsectoren op basis van Annex II van de NIB-richtlijn)
- Oorzaken van incidenten

Cyber Security Beeld Nederland 2019
Deze taxonomie wordt gebruikt voor:
- Actoren
- Typen dreigingen

ENISA Cybersecurity Incident Report and Analysis System
De dreigingmonitor sluit ook zoveel mogelijk aan op het datamodel dat ENISA hanteert voor cybersecurity-incidentstatistieken voor de telecommunicatiesector en vertrouwensdiensten.
https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

STIX 2.1 mapping
Structured Threat Information Expression (STIX™) is de industriestandaard voor het uitwisselen van dreigingsinformatie. STIX heeft een aantal objecttypen (STIX Domain Objects) waarmee informatie gecategoriseerd wordt en van attributen wordt voorzien. Niet alle STIX mogelijkheden zijn op dit moment relevant voor ons toezichtswerk. Echter, om de WBNI dreigingsmonitor toekomstbestendig te maken, zijn nu al de verschillende elementen uit onze dreiginsmonitor op de STIX 2.1 standaard *gemapt*. Zo is het op het later moment eenvoudiger om (geautomatiseerd) dreigingsinformatie te verrijken uit bijvoorbeeld bronnen van partners en andere derden. Ook maakt dit het eenvoudiger om, indien wenselijk, op een later moment gebruik te gaan maken van meer uitgebreide tooling voor het beheren van dreigingsinformatie zoals een (open source) threat intelligence platform.

Zie verder
https://oasis-open.github.io/cti-documentation/stix/intro.html
https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html
https://github.com/freetaxii/libstix2/blob/master/vocabs/vocabs.go

Object	Name	Description
	Attack Pattern	A type of TTP that describe ways that adversaries attempt to compromise targets.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets.
	Course of Action	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to that intelligence.
	Grouping	Explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context).
	Identity	Actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Infrastructure	Represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defence, database servers targeted by an attack, etc.).
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
	Location	Represents a geographic location.
	Malware	A type of TTP that represents malicious code.
	Malware Analysis	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
	Note	Conveys informative text to provide further context and/or to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to.
	Observed Data	Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
	Opinion	An assessment of the correctness of the information in a STIX Object produced by a different entity.
	Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.
	Threat Actor	Actual individuals, groups, or organizations believed to be operating with malicious intent.
	Tool	Legitimate software that can be used by threat actors to perform attacks.
	Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.

Details taxonomie dreigingsmonitor

Actoren (CSBN 2019)
- Staten/staatsgelieerd: Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).
- Criminelen: Actor die aanvallen pleegt met economische of financiële motieven.
- Terroristen: Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angstwil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.
- Hacktivisten: Actor die uit ideologische motieven digitale aanvallen van activistische aard pleegt. Cybervandalen en scriptkiddies
- Insider: Kwaadwillende werknemer of ingehuurde
- Onbekend: Onbekende actor
- Geen: Geen actor

Aard dreigingen / incidenten / trends (CSBN 2019)
- Verstoring: het opzettelijk tijdelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
- Sabotage: het opzettelijk en zeer langdurig aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten, mogelijk leidend tot vernietiging.
- Informatiemanipulatie: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.
- Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
- Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
- Systeemmanipulatie: aantasting van informatiesystemen of -diensten; gericht op de vertrouwelijkheid of integriteit van informatiesystemen of -diensten. Deze systemen of diensten worden daarna ingezet om andere aanvallen uit te voeren.
- Storing/uitval: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
- Lek: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.

Oorzaak incident / dreiging / trend (Cooperation group)
- Falen van systeem: The incident is due to a failure of a system, i.e. without external causes. For example a hardware failure, software bug, a flaw in a procedure, etc. triggered the incident.
- Natuurlijke oorzaak: The incident is due to a natural phenomenon. For example a storm, lightning, solar flare, flood, earthquake, wildfire, etc. triggered the incident.
- Menselijke fout: The incident is due to a human error, i.e. system worked correctly, but was used wrong. For example, a mistake, or carelessness triggered the incident.
- Kwaadwillende: The incident is due to a malicious action. For example, a cyber-attack or physical attack, vandalism, sabotage, insider attack, theft, etc., triggered the incident.

- Falen van derde partijen (keten)The incident is due to a disruption of a third party service, like a utility. For example a power cut, or an internet outage, etc. triggered the incident.

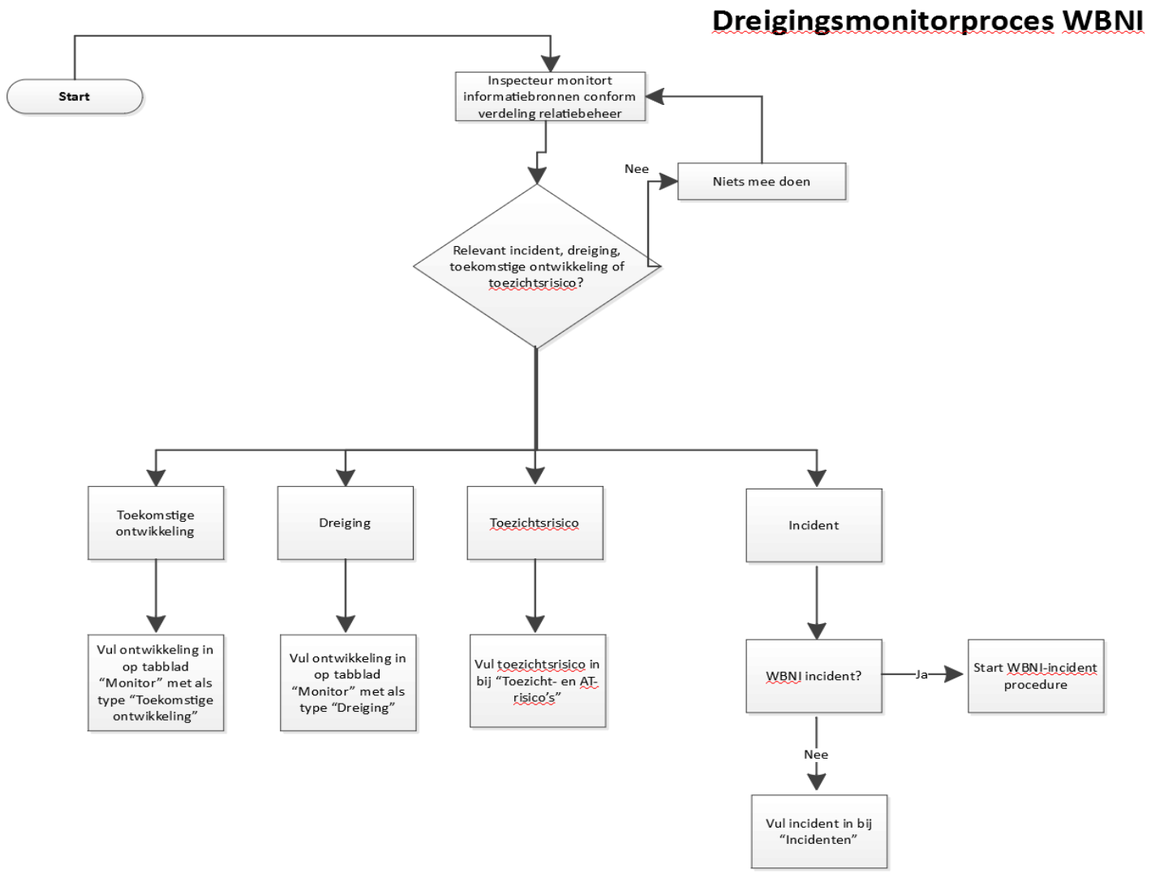
Sectoren (Cooperation group)
- Alle
- Bankwezen
- Digitale infrastructuur - DNS
- Digitale infrastructuur - IX
- Digitale infrastructuur - TLD
- DSP
- Energie - algemeen
- Energie - aardolie
- Energie - elektriciteit
- Energie - gas
- Gezondheidszorg
- Infrastructuur voor de financiele markt
- Levering en distributie van drinkwater
- Nucleair
- Overheid
- Overig
- Telecommunicatie
- Vertrouwensdiensten
- Vervoer - algemeen
- Vervoer - luchtvervoer
- Vervoer - spoorvervoer
- Vervoer - vervoer over de weg
- Vervoer - vervoer over water

Landen
Conform ISO 3166-1 alpha-3

Regio's
Conform STIX 2.1

Verwachte kans op aantasting continuteit AEDs in NL (heatmap risicomodel Wbni AT)
Zie heatmap in deze toelichting om deze beoordeling te doen voor incidenten, dreigingen en trends (toekomstige ontwikkelingen).

Verwachte impact op aantasting continuteit AEDs in NL (heatmap risicomodel Wbni AT)
Zie heatmap in deze toelichting om deze beoordeling te doen voor incidenten, dreigingen en trends (toekomstige ontwikkelingen).



Stapgewijze beschrijving

Dit kader beschrijft stapsgewijs het proces van het bijhouden van de dreigingsmonitor. Het omschrijft niet de processen die gebruik maken van de dreigingsmonitor, zoals het selecteren van onderwerpen voor de thema-inspecties. Deze processen worden afzonderlijk beschreven.

1. Alle inspecteurs monitoren de incidenten, dreigingen, toekomstige ontwikkelingen en toezichtsrisico's van de stakeholders en mediabronnen waar zij verantwoordelijk voor zijn. Deze indeling is te vinden in buiten reikwijdte.

Monitoren houdt in:
- Ontvangen van informatie, bijvoorbeeld via e-mail, nieuwsbrieven, vakliteratuur, lopende trajecten en projecten etc.
- Actief opvragen van informatie bij stakeholders, bijvoorbeeld tijdens periodieke accountgesprekken.

2. Alle inspecteurs vullen relevante incidenten, dreigingen, toekomstige ontwikkelingen en toezichtsrisico's in op de daarvoor aangewezen plek.
- Tabblad "Monitor" voor incidenten, dreigingen en toekomstige ontwikkelingen
- Tabblad "Toezicht- & AT-risico's" voor risico's met betrekking tot ons toezicht. Denk aan onderzoeksrapporten waarin opmerkingen over toezicht worden gemaakt waar we ons tot zullen moeten verhouden op enig moment.

Let op: Bij WBNI-incidenten die aan ons gemeld worden volgen we het aparte WBNI-incidentenproces. Hetzelfde geldt voor AED specifieke toezichtsinformatie. Daarbij volgen we de al bestaande processen en registraties.

3. De dreigingsmonitor gebruiken we periodiek voor:
- Het bepalen van thema-inspecties of de selectie van verdieping in de reguliere inspecties van volgend jaar. Dit loopt in Q3-Q4 van het voorafgaande jaar. Hier volgt een apart proces voor.
- Identificeren en addreseren van toezicht- & AT-risico's. Dit enerzijds input voor het opstellen van het jaarplan in Q3 en Q3 van het voorafgaande jaar. Ook kan het ons huidige jaarplan doen bijstellen.
- Input voor periodiek overleg met AEDs, als achtergrondinformatie over wat er speelt.

Voorbeeld verwerken NCSC maandmonitor

In dit kader volgt een stapsgewijs voorbeeld van hoe de maandelijkse NCSC maandmonitor in de dreigingsmonitor verwerkt kan worden. NCSC maandmonitor juni 2020 wordt als voorbeeld gehanteerd en is te vinden in buiten reikwijdte

buiten reikwijdte

1. De relatiebeheerder primair voor het NCSC ontvangt de NCSC maandmonitor.
2. De inspecteur identificeert de relevante incidenten, dreigingen, toekomstige ontwikkelingen en toezichtrisico's. In dit geval gaat het om:

Incidenten:
-

Dreigingen:
- Volgens de NSA maakt de Russische inlichtingendienst GROe sinds augustus vorig jaar misbruik van een ernstige kwetsbaarheid in de Exim-mailserver (CVE-2019-10149).
De kwetsbaarheid was sinds 2019-06-05 publiekelijk bekend. Er zijn nog veel ongepatchte systemen.
- Software supply chains blijven een bron van kwetsbare kritieke systemen. Productenten maken vaak gebruik van (open source) softwareonderdelen van derde partijen.
20 kwetsbaarheden in de Treck IP stack (Ripple20) werken door in veel producten, o.a. van HP, Schneider Electric, Intel, Rockwell Automation, Caterpillar en Baxter. Niet alle producten krijgen een update.

Toekomstige ontwikkelingen:
- DDoS-aanvallen blijven wereldwijd een stijgende trend vertonen in omvang en complexiteit.

Toezicht- & AT-risico's
- Inspectie IGJ stelt dat de universiteit Maastricht niet volgende voorbereid was op een ransomware-aanval. Er was aandacht voor databeveiliging, maar dat was voornamelijk AVG. In de draaiboeken voor grote incidenten was ransomware niet opgenomen. Er was geen totaal (over)zicht op de it-inrichting en daarmee slechts beperkt zicht op de cyberweerbaarheid van de universiteit als geheel. De interne controle op de uitvoering van het ict-beleid en de opvolging van afspraken was nauwelijks ingericht. In het geval van een ransomware op een onder toezichtgestelde van AT kan AT aangesproken worden op aandacht voor ransomware bij inspecties.

3. De inspecteur vult deze informatie in deze excel in. Niet alle kolommen kunnen altijd ingevuld worden. Deze kun je dan open laten. Je kunt bovenstaande voorbeelden terugvinden inn het tabblad "Monitor".

Sector	Incident, dreiging of (Toekomstige) ontwikkeling	Omschrijving	Oorzaak	Aard	Vermoedelijke actor	Aantasting BIV	Kans op incident
Nucleair	Incident	Aanval op Iraanse nucliaire centrifuges (ICS) met behulp van Stuxnet malware.	Kwaadwillende	Sabotage	Staten/staatsgelieerd	B	
Energie - aardolie	Incident	Aanval op Saudi Aramco met Shamoon malware, waarbij ongeveer 35000 computers van het corporate IT-netwerk onklaar werden gemaakt. Daarnaast werden gegevens buit gemaakt.	Kwaadwillende	Sabotage	Onbekend	BIV	
Energie - algemeen	Incident	Amerikaanse ICS-CERT rapporteert over Havex, een specifieke ICS malware gericht op Europese energiebedrijven. Verspreiding via gecompromitteerde websites van ICS leveranciers (watering-hole) en spear phishing.	Kwaadwillende	Informatiediefstal	Staten/staatsgelieerd	BI	
Energie - elektriciteit	Incident	Stroomuitval in delen van Oekraine door cyberaanval, vermoedelijk met Blackenergy malware	Kwaadwillende	Sabotage	Staten/staatsgelieerd	B	
Energie - elektriciteit	Incident	Stroomuitval in Kiev, Oekraine, door aanval met Industroyer malware	Kwaadwillende	Sabotage	Staten/staatsgelieerd	B	
Energie - aardolie	Incident	Dragos rapporteert over TRISIS/TRITON malware dat zich richt op het onklaar maken van Schneider Electric's SIS (safety instrumentated systems), de Triconex Emergency Shut Down (ESD) systems. Media rapporteren dat hiermee een petrochemische fabriek in Saudi Arabia geraakt zou zijn, waardoor de operatie ervan werd stilgelegd.	Kwaadwillende	Sabotage	Onbekend	B	
Alle	Incident	Trend Micro claimt in een nieuwe analyse dat het meerdere slachtoffers van de USBferry-malware heeft waargenomen, waarbij in ieder geval één militair air-gapped netwerk via het netwerk van militair ziekenhuis besmet raakte	Kwaadwillende	Informatiediefstal	Onbekend	V	
Alle	Dreiging	US-CERT waarschuwt voor Russische cyberactiviteiten tegen Amerikaanse organisaties binnen de sectoren energie, nucliair, water, luchtvaart en vitale maakindustrie, evenals overheidsinstellingen.	Kwaadwillende		Staten/staatsgelieerd		
Alle	Incident	Dragos rapporteert over aangetroffen EKANS/SNAKE-ransomware die ook aangepast lijkt te zijn voor ICS-systemen. De ransomware verwijst naar specifieke ICS processen die afgesloten worden bij infectie, waaronder een ICS data historian. Een mogelijke voorganger van EKANS is MEGACORTEX.	Kwaadwillende	Verstoring	Onbekend	BI	
Energie - algemeen	Incident	Recorded Future meldt een aan Iran geattribueerde campagne gericht op een Europese energiecoordinatie-organisatie waarbij PupyRAT is ingezet.	Kwaadwillende	Spionage	Staten/staatsgelieerd		
Energie - algemeen	Incident	Energias de Portugal (EDP), het grootste energiebedrijf van Portugal, is op tweede paasdag getroffen door RagnarLocker-ransomware. Tegenover Portugese media bevestigt EDP de aanval en stelt dat die geen gevolgen voor de energievoorziening heeft. Wel zijn uit voorzorg verschillende systemen uitgeschakeld.	Kwaadwillende	Verstoring	Onbekend	BI	
Levering en distributie van drinkwater	Incident	Israelische regering bevestigt cyberaanval op watersystemen.	Kwaadwillende	Verstoring	Onbekend	B	
Alle	Dreiging	AIVD stelt dat meerdere staten hebben bewezen de capaciteiten en de bereidheid te hebben om digitale sabotage in te zetten om hun geopolitieke doelstellingen te bereiken. Ook constateert de AIVD al langere tijd dat sommige van deze staten voorbereidingen treffen om digitale sabotage voor toekomstig gebruik mogelijk te maken.	Kwaadwillende	Sabotage	Staten/staatsgelieerd		

Energie - elektriciteit	Incident	De interne systemen van Elexon zijn geraakt door REvil ransomware. Elexon Elexon beheert de Balancing and Settlement Code (BSC) van de electriciteitssector in het VK. De BSC regelt vraag en aanbod op de Britse energiemarkt. BSC en EMR (Electricity Market Reform) waren niet getroffen. De aanvallers persen Elexon af. Anders zullen ze buitgemaakte data openbaar maken.	Kwaadwillende	Verstoring	Onbekend	BI	
Energie - algemeen	Dreiging	ENISA waarschuwt voor dreigingen voor diensten van energiebedrijven die afhankelijk zijn van tijdsynchronisatie. Afhankelijkheid hiervan wordt vergroot door opkomst van smart grids die phasor measurement units (PMUs) gebruiken voor netstabilisatie.	Falen van derde partijen	Systeemmanipulatie	Onbekend		
Energie - elektriciteit	Dreiging	De Amerikaanse overheid ziet grote supply-chain risico's voor het Amerikaanse hoogspanningsnet. Het stelt daarom regels aan "bulk-power electric equipment" in het electriciteitnet van de Verenigde Staten die gemaakt, ontworpen of ontwikkeld worden in het buitenland. De scope is beperkt tot 69 kv en hoger en het geldt niet voor systemen voor lokale distributie van electriciteit.	Falen van derde partijen	Sabotage	Staten/staatsgelieerd		
Alle	Dreiging	WRR signaleert in "Kwetsbaarheid en veerkracht" het belang van digitale infrastructuur in relatie tot COVID-19					
Energie - elektriciteit	(Toekomstige) ontwikkeling	Rijksoverheid verstrekt 5 miljoen subsidie voor slimme laadpleinen. Dit past binnen een bredere ontwikkeling dat de uitrol van laadpalen versneld. Grootschalige uitrol van onveilige laadpalen brengt risico's voor netstabiliteit met zich mee.					Hoog
Alle	(Toekomstige) ontwikkeling	Het risico bestaat dat China de technologische standaarden (5G, kunstmatige intelligentie, kwantumcomputing) voor de toekomst bepaalt, en daarmee afhankelijkheid van Chinese technologie creëert voor de rest van de wereld.			Staten/staatsgelieerd		Midden
Alle	(Toekomstige) ontwikkeling	AI kan nieuwe risico's meebrengen. Op toepassingsniveau zijn de mate van autonoom leren en handelen, de mate van onvoorspelbaarheid, het handelingskader en de invloedssfeer van de AI-toepassing bepalend voor de waarschijnlijkheid en de impact van de additionele risico's. Hier bovenop bestaan in de volledige levenscyclus van een AI-toepassing (planning, dataverzameling, training, testen en validatie en operatie) onverminderd de gangbare risico's ten aanzien van informatiebe-veiliging.					Midden
Alle	Dreiging	buiten reikwijdte	Kwaadwillende	Verstoring	Staten/staatsgelieerd	IV	
Alle	Dreiging	buiten reikwijdte	Falen van derde partijen (keten)			BIV	
Alle	Dreiging	buiten reikwijdte	Kwaadwillende	Verstoring		B	

Alle	Dreiging	FBI waarschuwt voor nieuwe DDOS-amplificatieaanvallen met Jenkins, Apple Remote Management Service, Web Services Dynamic Discovery en Constrained Application Protocol	Kwaadwillende	Verstoring		B	
Alle	Dreiging	U.S. Cybersecurity and Infrastructure Security Agency (CISA) waarschuwt voor misbruik van CVE-2020-5902 mbt F5 Networks' BIG-IP application delivery controller (ADC). Aanvallers misbruiken kwetsbaarheid binnen enkele dagen na PoC.	Kwaadwillende			IV	
Alle	(Toekomstige) ontwikkeling	(Remote) onderhoud aan OT omgevingen wordt steeds vaker uitbesteed. De verantwoordelijke heeft niet altijd zicht op wat de onderhoudende partij doet en of deze wel veilig werkt.	Falen van derde partijen (keten)				
Alle	Dreiging	NSA en CISA waarschuwen voor aanvallen op (internet) connected OT-systemen en geven suggesties voor mitigerende maatregelen	Kwaadwillende	Verstoring		BIV	
Alle	Incident	Injectie van malicious software in open source packages.	Kwaadwillende	Verstoring	Onbekend	BIV	Hoog
Alle	Incident	Malicious Opensource packages met Typo-squatting	Kwaadwillende	Verstoring	Onbekend	BIV	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Informatiediefstal	Onbekend	B	
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Systeemmanipulatie	Criminelen	IV	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Systeemmanipulatie	Criminelen	I	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Verstoring	Onbekend	B	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Verstoring	Criminelen	B	Hoog
Bankwezen	Incident	Ransomware-aanval op Travelex met Sodinokibi/Revil. 5GB persoonlijke data was geexfilteerd en er werd 3 miljoen dollar losgeld geeist. 2.3 miljoen is betaald.	Kwaadwillende	Informatiediefstal	Criminelen	BV	Hoog
Alle	Incident	Ernstige kwetsbaarheid in Citrix wereldwijd misbruikt. Ook in Nederland veel kwetsbare servers.	Kwaadwillende	Informatiediefstal	Onbekend	IV	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Verstoring	Onbekend	B	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Systeemmanipulatie	Criminelen	B	Hoog
Bankwezen	Incident	Cognizant is getroffen door Maze ransomware	Kwaadwillende	Systeemmanipulatie	Criminelen	B	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende	Informatiediefstal	Criminelen	I	Hoog
Bankwezen	Incident	buiten reikwijdte	Kwaadwillende		Criminelen	B	Hoog
Overig	Incident	Universiteit Maastricht is slachtoffer van ransomware-aanval	Kwaadwillende	Systeemmanipulatie	Criminelen	B	Hoog
Energie - elektriciteit	(Toekomstige) ontwikkeling	Minsterie van EZK werkt aan energiewet waarin datauitwisseling binnen de energiesector geregeld wordt. Energiesector gaat steeds verder dataficeren					
Overig	Incident	Garmin, fabrikant van wearables, is slachtoffer van ransomware-aanval	Kwaadwillende	Systeemmanipulatie	Criminelen	B	Hoog
Overig	Incident	Norsk Hydro is slachtoffer van ransomware-aanval. Langdurige uitval van productie.	Kwaadwillende	Systeemmanipulatie	Criminelen	B	Hoog
Energie - algemeen	Incident	Bitdefender schrijft over spearphishing-aanval met tesla spyware op olie- en gasindustrie, waarbij aanvaller zich voordat als bekende engineering contracters	Kwaadwillende	Informatiediefstal	Onbekend	V	Hoog
Alle	Dreiging	Aldus NCTV gaat vanuit het perspectief van nationale veiligheid de dreiging vooral om de risico's van (voorbereidingen voor) sabotage en spionage door statelijke actoren.	Kwaadwillende		Staten/staatsgelieerd	BIV	Midden

Alle	Dreiging	De AIVD en MIVD beschouwen de mogelijke digitale verstoring en sabotage van de vitale infrastructuur als een van de grootste cyberdreigingen voor Nederland en zijn bondgenoten. Meerdere staten hebben bewezen de capaciteiten en de bereidheid te hebben om digitale sabotage in te zetten om hun geopolitieke doelstellingen te bereiken. De AIVD constateert al langere tijd dat sommige van deze staten voorbereidingen treffen om digitale sabotage voor toekomstig gebruik mogelijk te maken. Deze voorbereidingen bestaan uit het zich innestelen in ICT-systemen van onder meer vitale infrastructuur. Ook de MIVD onderkende in 2019 diverse voorbereidende sabotageactiviteiten gericht tegen westerse landen en bondgenootschappelijke belangen. Momenteel ontbreekt het staten aan de intentie om digitale sabotage tegen Nederland in te zetten. Deze intentie is echter veranderlijk en afhankelijk van geopolitieke ontwikkelingen.	Kwaadwillende	Verstoring, Sabotage	Staten/staatsgelieerd		Laag
Alle	Dreiging	Enkele landen gebruiken informatie-operaties als instrument in hybride conflicten. Via die operaties proberen ze verdeeldheid te zaaien over onderwerpen die bij de verschillende doellanden of bondgenootschappelijke organisaties gevoelig liggen.	Kwaadwillende		Staten/staatsgelieerd		Midden
Alle	Dreiging	In 2019 bleek een staatsgelieerde hackersgroep zich bezig te houden met zowel spionage als financieel gemotiveerde operaties. Criminelen gebruiken vaak dezelfde (openbare) middelen als statelijke actoren en vice versa. In het verleden hebben staatsgelieerde actoren uit een ander land zich ook met financieel gemotiveerde aanvallen bezig gehouden.	Kwaadwillende		Staten/staatsgelieerd		
Alle	Dreiging	Steeds vaker wordt waargenomen dat criminele actoren ransomware zodanig inzetten dat zij het slachtoffer onder druk kunnen zetten om tot betaling van losgeld over te gaan. Het gaat de actoren vooral om organisaties die de mogelijkheid hebben om grotere geldbedragen te betalen en/of waarvoor bedrijfscontinuïteit en waardevolle unieke data een belangrijke rol spelen. Kenmerkend voor de werkwijze is de uitgebreide verkenning van het bedrijfsnetwerk. Dit stelt de actor in staat om de waarde van de data en de schade voor het slachtoffer in te schatten en om de ransomware op de meest effectieve wijze te plaatsen. Op basis van dat inzicht varieert het gevraagde losgeld van enkele tienduizenden tot miljoenen euro's. Er lijkt een toename te zijn van ransomware-aanvallen waarbij data niet alleen versleuteld wordt, maar ook gekopieerd. Wanneer een organisatie het losgeld niet wilde betalen, dan publiceerden criminelen in sommige gevallen de data.	Kwaadwillende	Verstoring, informatiediefstal		BV	Hoog
Overheid	Incident	Gemeente Lochem werd aangevallen met ransomware. Aanval was mogelijk door openstaande RDP-server. Het forensisch onderzoek naar het incident toont verder aan dat de gemeente Lochem geen overzicht had van alle it-systemen en de functionaliteiten die daarop draaien.	Kwaadwillende	Afpersing, informatiedie	Criminelen	BV	Hoog
Alle	Dreiging	Kwetsbaarheden in software worden steeds sneller misbruikt, vaak al binnen een dag of enkele dagen. Zeroday of One-day exploits.	Kwaadwillende				
Alle	Dreiging	Cisco waarschuwt voor actief misbruik van lek in Cisco ASA-firewalls. Patch kwam uit op 22 juli. Dag later is een publieke exploit bekend en wordt deze misbruikt.	Kwaadwillende				Hoog
Alle	Dreiging	Er is een hernieuwde interesse aan in het wijzigen van Domain Name System (DNS)-instellingen als aanvalstechniek, ook wel bekend als een DNS-hijack. Door DNS-instellingen van organisaties te wijzigen, bijvoorbeeld via het hacken van een registrar, kan inkomend netwerkverkeer tijdelijk omgeleid en onderschept worden.	Kwaadwillende	Informatiediefstal		BV	
Alle	Dreiging	Toename van phishing via SMS, Whatsapp etc.	Kwaadwillende				
Alle	Dreiging	Leveranciersketen worden misbruikt door gecompromitteerde ICT-producten. Actoren gaan meer op zoek naar de zwakke schakel in ketens waar het beoogde doelwit van afhankelijk is. Dat kan een eenvoudigere manier zijn dan een directe aanval op de organisatie waar ze het op voorzien hebben. Actoren breken bijvoorbeeld in bij een softwareleverancier en modificeren de software, die vervolgens al dan niet met een automatische update gedownload wordt door het doelwit. Voorbeelden: ASUS Live Update, AVAST, MeDoc.	Kwaadwillende				

Energie - algemeen	Dreiging	IBM X-Force schrijft over ZeroCleare, wiper malware gericht op de olie- en gassector in het Midden-Oosten.	Kwaadwillende	Verstoring	Staten/staatsgelieerd	
Alle	Dreiging	Uit onderzoek van de AIVD en MIVD blijkt dat meerdere Nederlandse topsectoren doelwit zijn (geweest) van digitale spionage. Het gaat daarbij vooral om hightech, energie, maritiem en life sciences & health. Doelwitten zijn ook toeleveranciers van Defensie of andere ministeries, vitale sectoren, het verkrijgen van persoonsgegevens en gegevens van andere organisaties, zoals telecomproviders, universiteiten, onderwijsinstellingen, onderzoeksinstituten, denktanks, biotechnologiebedrijven, startups, handel en defensieorderbedrijven	Kwaadwillende	Spionage	Staten/staatsgelieerd	V
Alle	Dreiging	Aldus de NCTV was er in 2019-2020 weer een verdere groei te zien in het aantal kwetsbaarheden in hardware. Bijvoorbeeld DRAM-kwetsbaarheden				
Alle	Dreiging	Het bleek dat veel Nederlandse organisaties hun Fortigate en Pulse VPN systemen nog niet gepatched hadden, ondanks een ernstige kwetsbaarheid.	Kwaadwillende			
Alle	Dreiging	Kwetsbaarheden door ketenafhankelijkheid. Doordat organisaties gebruik maken van diensten en producten van vele andere partijen, kunnen incidenten doorwerken in de keten.				
Alle	Dreiging	Keteneffecten van storingen via of bij grote technologiebedrijven. In 2019 verschenen er berichten in de media over enkele storingen bij wereldwijd opererende grote technologiebedrijven waaronder Cloudflare, Amazon Web Services (AWS) en Google Cloud. Die storingen hadden niet alleen wereldwijde gevolgen voor vele andere organisaties, maar soms ook voor andere grote technologiebedrijven. Zo had volgens media een storing bij Cloudflare, dat (onder andere) bedoeld is om storingen en vertragingen te voorkomen, op 24 juni 2019 gevolgen voor 16 miljoen apps en websites wereldwijd, waaronder in Nederland.	Falen van derde partijen	Verstoring		
Alle	Incident	Een storing bij Tele2 resulteerde in het niet of slecht bereikbaar zijn van overheidsdiensten, gemeenten, de rechtspraak en de RDW en konden personen met enkelbanden niet worden gevolgd	Falen van derde partijen (keten)			
Gezondheidszorg	(Toekomstige) ontwikkeling	De risico's van ICT-uitval in ziekenhuizen moeten beter in beeld worden gebracht. Voor het leveren van goede zorg zijn ziekenhuizen steeds meer afhankelijk van het goed functioneren van de ICT. Die afhankelijkheid kan leiden tot onveilige situaties voor de patiënt, zoals het stellen van een verkeerde diagnose op basis van onvolledige informatie. Aldus de Onderzoeksraad voor Veiligheid.				
Alle	(Toekomstige) ontwikkeling	NCTV schrijft dat er nog steeds zorgen zijn over de afhankelijkheid van buitenlandse partijen, in het bijzonder de continuïteit van maatschappelijke kernprocessen die sterk afhankelijk is geworden van grote buitenlandse aanbieders van digitale voorzieningen.				
Alle	(Toekomstige) ontwikkeling	Verspreiding autonome systemen vergroot digitale kwetsbaarheid, aldus de NCTV. Denk aan zelfrijdende auto's en allerlei internet-of-things producten				
Alle	(Toekomstige) ontwikkeling	Slimme algoritmes hebben positief en negatief effect op digitale veiigheid, aldus de NCTV				
Alle	(Toekomstige) ontwikkeling	Geopolitieke spanningen werken door op mondiale ICT-markt, aldus de NCTV. Zo proberen landen de totstandkoming van nieuwe internetstandaarden te beïnvloeden. Ook zullen veiligheidsbelangen een grotere rol krijgen in keuzes die gemaakt worden rond ICT-infrastructuur. Door oplopende geopolitieke spanningen en het ontstane wantrouwen in hard- en software, producenten en dienstverleners zal het aantal vertrouwde producten en leveranciers per land of regio mogelijk afnemen. Landen veraf en dichtbij zullen pogen om grip te krijgen op de ICT-infrastructuur vanuit veiligheidsbelangen. Daarbij is het denkbaar dat Europa op dit vlak als het ware klem komt te zitten tussen de grote machtsblokken China en de VS. Door de implementatie van nieuwe technologie en de hoge doordringingsgraad van ICT en netwerken zullen risico-afwegingen er anders uitzien dan voorheen.				

Alle	(Toekomstige) ontwikkeling	De dreiging die uitgaat van ideologisch gemotiveerde actorgroepen (hacktivisten en terroristen) en actorgroepen die handelen uit een persoonlijk motief (insiders, cybervandalen en scriptkiddies) is relatief klein. Al jaren zijn vanuit deze actorgroepen geen substantiële aanvallen tegen Nederland of Nederlandse belangen waargenomen. Er is geen aanleiding te veronderstellen dat dit komende jaren anders is. Aldus de NCTV.				
Alle	(Toekomstige) ontwikkeling	Cyberincidenten kunnen zich op verschillende manieren voordoen en ook optreden in samenhang met geheel andersoortige incidenten. Dat komt onder andere door de sterke - veelal internationale - connectiviteit tussen digitale diensten en processen, systemen en het gebruik van generieke hard- en software(componenten). Cyberincidenten kunnen daardoor een onvoorziene kettingreactie in gang zetten waarvan de gevolgen het functioneren van delen van de maatschappij in gevaar kunnen brengen.				
Alle	Dreiging	Phishing was het afgelopen jaar (2019) weer de meest gebruikte (eerste stap) aanvalsmethode.				
Alle	Incident	NotPetya ransomware-aanval. Waarschijnlijk initiële verspreiding via supply chain (MeDoc), daarna via lokaal netwerk (EternalBlue). Leek gericht op Oekraïne. Slachtoffers o.a. Maersk, APM terminals (Nederland), TNT Express, Mars, Merck.	Kwaadwillende	Systeemmanipulatie	Staten/staatsgelieerd	
Alle	Incident	Wannacry ransomware-aanval. Verspreiding via internet via EternalBlue (SMB) kwetsbaarheid. Wereldwijd slachtoffers.	Kwaadwillende	Systeemmanipulatie		
Overig	Incident	Bandenfabriek Apollo Vredestein geraakt door een hack, waardoor productie verstoord werd. Hackers zouden binnen zijn gekomen door oude kwetsbare software verbonden met internet.	Kwaadwillende	Systeemmanipulatie	Onbekend	
Energie - elektriciteit	Incident	Website en e-mailserver van Northwest Territories Power Corporation getroffen door ransomware	Kwaadwillende	Systeemmanipulatie	Onbekend	BI
Energie - Algemeen	Incident	Enel Group interne IT-netwerk is geraakt door EKANS/Snake ransomware	Kwaadwillende	Systeemmanipulatie	Onbekend	BI
Alle	(Toekomstige) ontwikkeling	Google start een (beta) Certificate Authority Service, waarmee organisaties eenvoudig een eigen privé CA kunnen opzetten. In het bijzonder interessant voor IoT. Hiermee zet Google weer een stap om fundamentdiensten voor de digitale economie te leveren.				
Alle	Dreiging	NCSC waarschuwt voor actief misbruik van Cisco ASA-lekken in Nederland	Kwaadwillende		Onbekend	
Overig	Incident	Spie Group, een internationaal technisch dienstverlener, is getroffen door ransomware-aanval en datadiefstal. Bestanden werden gestolen, waarna systemen werden versleuteld.	Kwaadwillende	Systeemmanipulatie	Criminelen	BIV
DSP	Incident	Cloudsoftwarebedrijf Blackbaud was in mei 2020 het doelwit van een ransomware-aanval. Het bedrijf levert o.a. CRM-diensten. Gegevens van o.a. TU Delft en UU werden buitgemaakt.	Kwaadwillende	Systeemmanipulatie	Criminelen	BIV
Alle	Dreiging	FBI en NSA beschuldigen Rusland van gebruik Drovorub-malware, dat gericht is op Linux-systemen. Fancy Bear, Strontium of APT 28 zouden deze gebruiken. Gelieerd aan GRU.	Kwaadwillende	Spionage	Staten/staatsgelieerd	V
Alle	Dreiging	Microsoft waarschuwt gebruikers van Office 365 voor phishingaanvallen via malafide apps, waarbij multifactorauthenticatie wordt omzeild, slachtoffers niet hun inloggegevens op een phishingpagina hoeven in te voeren en het wijzigen van wachtwoorden niet voldoende is om aanvallers de toegang tot het account te ontzeggen. Office 365 staat standaard ongeverfieerde Add-Ins en Apps toe. O.a. SANS is getroffen.	Kwaadwillende	Informatiediefstal	Onbekend	V
Alle	Incident	Aanvallers hebben via een bekend beveiligingslek in de vpn-software van Pulse Secure van meerdere Nederlandse bedrijven de wachtwoorden gestolen. Het gaat onder andere om een dochterbedrijf van het industriële concern VDL, datacenterbedrijf ITB2 en de in kerstversieringen gespecialiseerde groothandel Coen Bakker Decom	Kwaadwillende		Onbekend	
Overig	Incident	De Universiteit van Utah heeft criminelen die de systemen met ransomware infecteerden 457.000 dollar losgeld betaald om te voorkomen dat gestolen data openbaar werd gemaakt,	Kwaadwillende	Systeemmanipulatie	Criminelen	BIV

Overig	Incident	Spearphishingaanvallen op Amerikaanse defensieleveranciers. Gebruik van malafide .docx documenten die CVE-2017-0199 misbruiken. Aanvaller zou Noord-Korea zijn, aldus de VS.	Kwaadwillende		Staten/staatsgelieerd	V
Alle	Incident	Onderzoekers van Kaspersky hebben spionagemalware (Crimson remote access trojan (RAT)) ontdekt die zich via usb-sticks kan verspreiden en wereldwijd honderden systemen heeft besmet, waaronder in Nederland. Aanval begint met spearphishing e-mail met office-document met kwaadaardige macro. Vervolgens infecteert de malware ook USB-sticks.	Kwaadwillende	Spionage	Onbekend	V
Digitale infrastructuur -	Incident	De Amerikaanse internetprovider CenturyLink heeft zondag een grote technische storing gehad nadat een verkeerde configuratie in een van zijn datacenters overal op het internet ravage veroorzaakte. Vanwege de technische aard van de storing - waarbij zowel firewall- als BGP-routering betrokken was - verspreidde de fout zich naar buiten vanaf het netwerk van CenturyLink en had ook invloed op andere internetproviders, waardoor er verbindingsproblemen ontstonden voor veel meer andere bedrijven.	Falen van derde partijen	Verstoring		B
Telecommunicatie	Incident	Verschillende Nederlandse providers hebben last van ddos-aanvallen. Onder andere Online.nl, Tweak, Delta, Caiway, SIgnet en Freedom Internet lagen tijdelijk plat. Ook TV-diensten werkten niet. In België is EDPnet getroffen. In Frankrijk Bouygues Télécom, FDN, K-net en SFR. DDoS werd o.a. uitgevoerd op DNS-servers.	Kwaadwillende	Verstoring		B
DSP	Incident	Website en mailserver van hoster WebReus dagenlang onbereikbaar door DDoS-aanval.	Kwaadwillende	Verstoring		B
Energie - algemeen	(Toekomstige) ontwikkeling	Het deze week opgerichte Zero Emission Services (ZES) maakt het voor binnenvaartschepen mogelijk op verwisselbare accu's te varen. De energiecontainers zijn ontworpen voor meerdere toepassingen, bijvoorbeeld voor het stabiliseren van het elektriciteitsnet of om te voorzien in een lokale tijdelijke vraag naar elektriciteit.				
Energie - elektriciteit	(Toekomstige) ontwikkeling	Meer dan de helft van de datacenters in Europa heeft zorgen over de capaciteit van hun lokale stroomnet en voelt zich niet uitgerust voor temperatuurstijgingen veroorzaakt door klimaatverandering.				
Alle	Dreiging	Emotet-malware zet Nederlandstalige e-mailtemplates in ter verspreiding	Kwaadwillende		Criminelen	
Alle	(Toekomstige) ontwikkeling	MITRE heeft top25 kwetsbaarheden gepubliceerd. CSS staat op 1.				
Alle	(Toekomstige) ontwikkeling	Door economische sancties van de VS krijgt Huawei geen geavanceerde chips meer. Dit brengt de toekomst van het bedrijf in gevaar. Mogelijk zien we in de toekomst meer supply chains die door geopolitieke ontwikkelingen verstoord worden.			Staten/staatsgelieerd	
Overheid	Incident	Veiligheidsregio Noord- en Oost-Gelderland is getroffen door een ransomware-aanval. Interne systemen en e-mail zijn onbeschikbaar.	Kwaadwillende	Systeemmanipulatie		BI
Overig	Incident	Interne systemen van Equinix geraakt door ransomware-aanval	Kwaadwillende	Systeemmanipulatie		BI
Energie - algemeen	(Toekomstige) ontwikkeling	D66 Tweede Kamerlid Matthijs Sienot schrijft in een initiatiefnota dat een Rijksarchitect moet gaan zorgen voor meer regio op de ontwikkeling van het stroomnet. Dit in het kader van de energietransitie.				
Energie - elektriciteit	Incident	Pakistan's stroomleverancier K-Electric is geraakt door een ransomware-aanval. De energievoorziening werd niet geraakt.	Kwaadwillende	Systeemmanipulatie		B
Overheid	Incident	Amerikaanse overheidsinstanties zijn het afgelopen jaar het doelwit geweest van aanvallers die vanuit China opereerden en herhaaldelijk hierbij dezelfde vier kwetsbaarheden gebruikten. F5 Big-IP (CVE-2020-5902), Citrix vpn-appliances (CVE-2019-19781), Pulse Secure vpn-servers (CVE-2019-11510) en Microsoft Exchange (CVE-2020-0688).	Kwaadwillende		Staten/staatsgelieerd	
Alle	Dreiging	Overheden en ondernemers moeten wel voorzichtig omspringen als ze zaken doen met een Chinese partner in de cruciale infrastructuur. "Stel jezelf de vraag of je je op je gemak voelt bij de gedachte dat Chinese technologie in bepaalde delen van de infrastructuur is verwerkt.	Kwaadwillende	Spionage	Staten/staatsgelieerd	BIV

Alle	Dreiging	Iraanse APT Pioneer Kitten misbruikt 1-day kwetsbaarheden in o.a. VPN-apparatuur. Ze zouden opereren in opdracht van de Iraanse overheid ten behoeve van spionage. Ze maken gebruik van webshells. Ook zouden ze toegang tot die apparatuur verkopen op fora op het darkweb.	Kwaadwillende	Spionage	Criminelen	IV
Telecommunicatie	(Toekomstige) ontwikkeling	Nokia breidt geautomatiseerd beheer van mobiele netwerken verder uit. Zijn Self-Organizing Network (SON)-software gebruikt nu machine learning om netwerkproblemen automatisch te ontdekken en zelf op te lossen op basis van een set van vooraf gedefinieerde doelen. Denk daarbij onder meer aan latency- en throughput-niveau's en network slicing. De netwerkbeheersoftware gebruikt ook intelligente inzichten om zichzelf zelfstandig nog meer te verbeteren. Software-upgrades worden nu ook zonder menselijke tussenkomst uitgevoerd.				
Telecommunicatie	Incident	Hardnekkige storing tv en internet bij Online.nl. Vanwege een probleem met de verbinding naar de DNS-server was gebruik van internet met Zyxel modems niet mogelijk.	Falen van systeem			B
Telecommunicatie	Incident	Landelijke storing legt telefoonnummer politie half uur plat		Storing/uitval		B
DSP	Incident	Een 25-jarige Veenendaler die wordt verdacht van afpersing en chantage van bedrijven door zogenoemde DDos-aanvallen op hun websites. Onder de negen aangevallen bedrijven zijn bekende namen als Fleurop, Easytoys en Goossens Wonen.				
Energie - elektriciteit	Dreiging	Onderzoekers beschrijven hoe manipulatie van social-media met nepnieuws ervoor kan zorgen dat veel consumenten in een stad hun elektriciteitsgebruik wijzigen, waardoor het netwerk instabiel kan worden.	Kwaadwillende	Storing/uitval		B
Energie - elektriciteit	(Toekomstige) ontwikkeling	KPN experimenteert met het inzetten van batterijen van de noodstroomvoorzieningen van zijn (wijk)telefooncentrales voor opslag en teruglevering van elektriciteit.				
Alle	(Toekomstige) ontwikkeling	Acht op de tien Nederlandse bedrijven verzuimt alle patches te installeren, aldus onderzoek Panelwizard iov Solvinity.				
Overig	Incident	Tyler software, een belangrijke softwareleverancier voor de Amerikaanse overheid, is geraakt door ransomware. (RansomExx)	Kwaadwillende	Systeemmanipulatie		
Alle	Dreiging	Hackers maken misbruik van de Zerologon Windows Server kwetsbaarheid, aldus Microsoft. Dit enkele weken na bekendwording kwetsbaarheid.	Kwaadwillende			
Energie - elektriciteit	(Toekomstige) ontwikkeling	Volgens ACM houdt op basis van de investeringsplannen van netbeheerders het tekort aan transportcapaciteit in stroomnetten nog 5 tot 10 jaar aan. Netbeheerders moeten flink investeren in infrastructuur				
Energie - elektriciteit	(Toekomstige) ontwikkeling	Amerikaanse FERC (energie toezichthouder, soort ACM) vraagt Amerikaanse energiesector om te rapporteren of ze Huawei of ZTE gebruiken				
Alle	Dreiging	CISCO waarschuwt voor bedreiging van fileless malware voor end-points	Kwaadwillende			
Alle	Dreiging	Standaardconfiguratie Fortigate VPN kwetsbaar voor MITM-aanvallen				
Gezondheidszorg	Incident	Universal Health Services, een ziekenhuisgroep in de VS, is geraakt door een ransomware-aanval. Operaties etc kunnen niet doorgaan.	Kwaadwillende	Systeemmanipulatie		
Overheid	Dreiging	Gemeentemedewerkers vormen grootste risico voor cyberaanvallen, aldus de Informatiebeveiligingsdienst Gemeenten (IBD) in Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten 2021/2022. Dan gaat het niet zozeer om een vergissing, maar om medewerkers met verhoogde toegangsrechten en kwade bedoelingen.	Kwaadwillende			
Telecommunicatie	Dreiging	Onderzoekers tonen op Blackhat Asia 2020 aan dat het zwakke SS7 protocol nog steeds wordt toegepast voor 4G en 5G. Hierdoor zijn nog steeds aanvallen mogelijk, ook op het nieuwere 4G en 5G. Bijvoorbeeld Man-in-the-Middle-aanvallen.	Kwaadwillende			
Alle	(Toekomstige) ontwikkeling	Providers gaan via NBIP bedrijven waarschuwen voor beveiligingslekken, onder andere door informatie van het NCSC door te sturen.				

Alle	Dreiging	Onderzoekers van Kaspersky hebben bij twee organisaties UEFI-images ontdekt die met malware besmet bleken te zijn en een backdoor aan het systeem toevoegden.	Kwaadwillende		Onbekend
Energie - elektriciteit	(Toekomstige) ontwikkeling	Het Amerikaanse Huis van afgevaardigden heeft een aantal wetten aangenomen om het Amerikaanse elektriciteitsnet te beschermen tegen o.a. cyberdreiging.			
Overig	Incident	Internationale Maritieme Organisatie is geraakt door een cyberaanval. De precieze toedracht is onbekend.	Kwaadwillende		Onbekend
Alle	Dreiging	Microsoft meldt in een rapport dat de meeste gedetecteerde staatshacks in de afgelopen twee jaar werden uitgevoerd door groepen uit Rusland, China, Iran en Noord-Korea. De Verenigde Staten zouden het meest voorkomende doelwit zijn van dergelijke hacks.	Kwaadwillende		Staten/staatsgelieerd
Vervoer - vervoer over	Incident	Rrederij CMA CGM is ten prooi gevallen aan ransomware.	Kwaadwillende	Systeemmanipulatie	Criminelen
Alle	Dreiging	Volgens Microsoft duren sommige ransomware-aanvallen van aanval tot versleuteling slechts 45 minuten.	Kwaadwillende		
Alle	(Toekomstige) ontwikkeling	Digital Trust Center ontvangt in 2021 dreigingsinformatie van NCSC			
Alle	(Toekomstige) ontwikkeling	Australië, Canada, India, Japan, Nieuw-Zeeland, het Verenigd Koninkrijk en de Verenigde Staten roepen techbedrijven op om te stoppen met end-to-end encryptie en andere vormen van encryptie waardoor de overheid geen kennis kan nemen van informatie.			
Energie - elektriciteit	(Toekomstige) ontwikkeling	Amerikaanse Department of Energy steekt 7 miljoen om een infrastructuur te ontwikkelen dat het elektriciteitsnet beschermt tegen cyberaanvallen op elektrische voertuigen en laadpalen.			
Alle	Dreiging	APT groepen gebruiken VPN-kwetsbaarheden (Fortigate etc) en Zerologon-kwetsbaarheid om organisatienetwerken en computers over te nemen.	Kwaadwillende		
Overig	Incident	Duitse Software AG slachtoffer Clop ransomware-aanval	Kwaadwillende	Systeemmanipulatie	Onbekend
Alle	Dreiging	Ransomware-aanvallers kopen toegang tot netwerken van organisaties van criminele groepen die eerder toegang hebben verkregen. Prijs tussen $300-$10.000 dollar.	Kwaadwillende	Systeemmanipulatie	Criminelen
Gezondheidszorg	Incident	Storing bij ICTZ zorgt ervoor dat patiëntportalen, beeldbellen en informatiezuilen bij verschillende ziekenhuizen in Nederland niet werken. Aldus ICTZ lag het aan de verbindingsleverancier van het datacenter.	Falen van derde partijen	Storing/uitval	
Energie - elektriciteit	(Toekomstige) ontwikkeling	Een studie stelt voor om de belasting van datacenters te variëren om zo stroompieken of dippen op te vangen in het elektriciteitsnetwerk.			
Energie - elektriciteit	(Toekomstige) ontwikkeling	ENCS en E.DSO publiceren security-vereisten voor RTUs binnen distributie-automatisering			
Alle	Dreiging	Chinese hackers APT-31 maken McAfee-software na met malware en proberen slachtoffers dat te laten installeren.			Staten/staatsgelieerd
Alle	(Toekomstige) ontwikkeling	Onderzoek van Entrust wijst uit dat 83% van de Nederlandse respondenten (tegenover 63% wereldwijd) rapporteert dat er geen duidelijk eigenaarschap is voor het inzetten en beheren van PKI (#1 in de wereld). Daarnaast geeft 62% aan dat er niet genoeg middelen zijn om PKI te implementeren en beheren.			
Telecommunicatie	(Toekomstige) ontwikkeling	Zweden heeft het gebruik van telecomapparatuur van de Chinese techbedrijven Huawei en ZTE bij de aanleg van 5G-netwerken in het land verboden.			
Alle	Dreiging	Nokia waarschuwt voor een toename in aanvallen op Internet of Things (IoT)-apparatuur.	Kwaadwillende		
Alle	Dreiging	Cyberark onderzoekers wijzen op het gevaar van DDoS-aanvallen op LoRaWan netwerken via misbruik van MQTT dat gebruikt wordt voor communicatie tussen de gateways and the network server			
Energie - elektriciteit	(Toekomstige) ontwikkeling	In november 2020 start Smart Solar Charging ism Stedin een nieuw, commercieel systeem voor slim laden voor auto's in Utrecht dat het tijdstip van laden combineert met zowel de elektriciteitsprijs als de wensen van de netbeheerder.			
Alle	Dreiging	Ransomwarevariant RegretLocker gebruikt technieken om virtuele machines (vm's) en open files te versleutelen en op die manier te gijzelen.	Kwaadwillende		

Sector	Risico voor toezicht van AT	Relevantie	Wanneer	Bron	Link	Datum	Opmerkingen	Toegevoegd door
DSP	DSP's zijn niet bekend met het CSIRT-DSP voor actuele cyber intelligence vanuit het NCSC.	Midden	2020	iBestuur	https://ibestuur.nl/weblog/wanneer-is-ict-vitaal	10-4-2020	Opgepakt via DSP communicatie memo	5.1.2.e
Alle	CSR constateert dat niet-vitale processen verweven zijn met vitale infrastructuur en dat IACS vaak indirect gekoppeld zijn aan het internet, waardoor de impact van een intentionele of niet-intentionele verstoring op de gehele keten omvangrijk kan zijn. Het is daarom raadzaam om ons te focussen op vitale sectoren en niet alleen op vitale aanbieders	Hoog	2020	CSR	https://www.cybersecurityraad.nl/binaries/CSR_Advies_IACS_NED_DEF_tcm107-444304.pdf	24-4-2020	Opgepakt via thematisch onderzoek naar ketenafhankelijkheden	5.1.2.e
Alle	Inspectie IGJ stelt dat de universiteit Maastricht niet volgende voorbereid was op een ransomware-aanval. Er was aandacht voor databeveiliging, maar dat was voornamelijk AVG. In de draaiboeken voor grote incidenten was ransomware niet opgenomen. Er was geen totaal (over)zicht op de it-inrichting en daarmee slechts beperkt zicht op de cyberweerbaarheid van de universiteit als geheel. De interne controle op de uitvoering van het ict-beleid en de opvolging van afspraken was nauwelijks ingericht. In het geval van een ransomware op een onder toezichtgestelde van AT kan AT hierop aangesproken worden.	Midden	2020	NCSC Maandmonitor juni 2020		27-7-2020		5.1.2.e
Alle	Een compleet en scherp beeld van de digitale weerbaarheid van vitale processen en bijbehorende systemen ontbreekt (nog).	Hoog	2020	CSBN2020		3-8-2020	Sluit aan bij gezamenlijk inspectiebeeld dat nu opgezet wordt.	5.1.2.e
Alle	De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) wijst op kwetsbaarheid als gevolg van complexe en grensoverschrijdende toeleverings- en productieketens en het gebruik van generieke hard- en software. Dit kan gaan spelen in AT Wbni sectoren.	Hoog	2020	WRR - Voorbereiden op digitale ontwrichting	https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting	3-8-2020		5.1.2.e
Alle	De AIVD vindt het onwenselijk dat Nederland voor de uitwisseling van gevoelige informatie of voor vitale processen afhankelijk is van bedrijven uit landen die een offensief cyberprogramma tegen Nederlandse belangen uitvoeren. Dit kan gaan spelen in AT Wbni sectoren.	Hoog	2020	CSBN2020		3-8-2020		5.1.2.e
Alle	De Europese Centrale Bank maakt zich zorgen over het schrale aanbod van techbedrijven in Europa. De toezichthouder waarschuwt voor concentratierisico's en systeemrisico's nu Amerikaanse bedrijven hier steeds meer de dienst uitmaken. Er is meer samenwerking tussen toezichthouders nodig om de Europese fintechsector te ondersteunen.	Midden	2020	Financieel Dagblad	https://fd.nl/beurs/1355270/ecb-waarschuwt-voor-dominante-positie-amerikaanse-techgiganten	31-8-2020	Opgepakt via thematisch onderzoek naar ketenafhankelijkheden	5.1.2.e
Alle	weerbaarheid, aldus een coalitie van (branche)organisaties die bestaat uit AMS-IX, BTG/TGG, Cyberveilig Nederland, Dutch Data Center Association, DHPA, DINL, FCA, Vereniging ISPConnect en Stichting NBIP	Midden	2020	Security.nl	https://www.security.nl/posting/671696/'Overheid+moet+meer+investeren+in+digitale+weerbaarheid	24-9-2020		5.1.2.e
Energie - algemeen	De FERC/NERC hebben besloten om besluiten/boetes over informatiebeveiligingstekortkomingen bij energiebedrijven niet te publiceren. Dat zou namelijk risico's met zich meebrengen voor de beveiliging.	Midden	2020	Utility Dive	https://www.utilitydive.com/news/nerc-ferc-recommend-public-anonymity-for-utilities-violating-power-system/585934/	29-9-2020		5.1.2.e

2d

Titel threat report	Vindplaats
Cyber Security Beeld Nederland (CSBN) (NCTV)	https://www.nctv.nl
Jaarverslag AIVD	https://www.aivd.nl
Jaarverslag MIVD	https://www.mivd.nl
Internet Organised Crime Threat Assessment (iOCTA) (Europol)	https://www.europol.europa.eu/
Maandmonitor NCSC	T:\AT\RDRDATA\projecten\NIB\26 Literatuur\Threat Reports
Kwartaaldreigingsmonitor NCSC	T:\AT\RDRDATA\projecten\NIB\26 Literatuur\Threat Reports
ENISA Threat Landscape	https://enisa.europe.ec
Dragos Year in Review	https://www.dragos.com/year-in-review/
Fortinet Threat Report	https://www.fortinet.com/blog/threat-research
Accenture Cyber Threatscape Report	https://www.accenture.com/us-en/insights/security/cyber-threatscape-report
Mandiant Security Effectiveness Report	https://www.fireeye.com
Checkpoint Cyber Security Report	https://www.checkpoint.com/
Symantec's Annual Threat Report	https://www.broadcom.com/support/security-center
Crowdstrike Global Threat Report	https://www.crowdstrike.com/resources/reports/
CISCO Threats of the Year	https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html
Sophos Threat Report	https://www.sophos.com
SANS Threat Report	https://www.sans.org/reading-room/whitepapers/threats/
Malpedia	https://malpedia.caad.fkie.fraunhofer.de/library
Council on foreign relations cyber operations tracker	https://www.cfr.org/cyber-operations/#CyberOperations

Graag alle Threat Reports ook opslaan in
buiten reikwijdte

Gebruik aub de gehanteerde syntax voor bestandsnamen.

Websites met actoren	URL
APT Groups and Operations	https://airtable.com/shr3Po3DsZUQZY4we/tblOGNo8GL7Gf4hpA/viwQcgun6Ab0h18KF?blocks=hide
APT Groups and Operations	https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085
MITRE ATT&CK	https://attack.mitre.org/groups/
Malpedia	https://malpedia.caad.fkie.fraunhofer.de/actors

2e

Datum	Wijziging	Door
14-7-2020	Tabbladen "incidenten", "dreigingen" en "trends" geintegreerd in een enkel werkblad genaamd "monitor". Dit maakt het filteren van relevante gegevens eenvoudiger, evenals de aankomende migratie naar Sharepoint. Niet alle kolommen zijn van toepassing op een incident, dreiging of trend, maar we kunnen dan simpelweg de kolommen invullen die wel relevant zijn.	5.1.2.e
14-7-2020	Tabblad "High impact kwetsbaarheden" verwijderd n.a.v. advies van Stan. Dergelijke technische informatie past niet bij principle based toezicht. Bovendien is dergelijke informatie makkelijk van de NCSC website te halen.	5.1.2.e
15-7-2020	Andere informatiebronnen over AEDs toevoegd aan de toelichting, zodat samenhang met risk-based selectie helderder wordt.	5.1.2.e
27-7-2020	Workflow en proces verder uitgewerkt. Voorbeeld ingevoegd. In stakeholder relatiemanagement excelbestand een pagina met open bronnen toegevoegd.	5.1.2.e

Sector	Cybersecurity Incident Taxonomy CG Publication 04/2018 NIS Cooperation Group	STIX 2.1 SDO	STIX 2.1 vocab
Alle		Identity	
Bankwezen	Banking	Identity	Financial-services
Digitale infrastructuur - DNS	Digital infrastructure	Identity	Telecommunication
Digitale infrastructuur - IX	Digital infrastructure	Identity	Telecommunication
Digitale infrastructuur - TLD	Digital infrastructure	Identity	Telecommunication
DSP	Digital services	Identity	Technology
Energie - aardolie	Energy	Identity	Energy
Energie - algemeen	Energy	Identity	Energy
Energie - elektriciteit	Energy	Identity	Energy
Energie - gas	Energy	Identity	Energy
Gezondheidszorg	Health	Identity	Healthcare
Infrastructuur voor de financiele markt	Financial	Identity	Financial-services
Levering en distributie van drinkwater	Drinking water	Identity	Utilities
Nucleair	Energy	Identity	Infrastructure
Overheid	Government	Identity	Government
Overig		Identity	
Telecommunicatie	Communications	Identity	Telecommunication
Vertrouwensdiensten	Trust and identification services	Identity	Technology
Vervoer - algemeen	Transport	Identity	Transportation
Vervoer - luchtvervoer	Transport	Identity	Transportation
Vervoer - spoorvervoer	Transport	Identity	Transportation
Vervoer - vervoer over de weg	Transport	Identity	Transportation
Vervoer - vervoer over water	Transport	Identity	Transportation

Aantasting	Combinaties BIV
Beschikbaarheid	B
Integriteit	BI
Vertrouwelijkheid	BIV
	I
	IV
	BV
	V

Actor	*Actor of oorzaak die in combinatie met een kwetsbaarheid tot een risico leidt. (Naar CSBN en EU 5G toolkit)*	**STIX 2.1 SDO**	**STIX 2.1 vocab**
Staten/staatsgelieerd	Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage).	Threat actor	Nation-state
Criminelen	Actor die aanvallen pleegt met economische of financiële motieven.	Threat actor	Criminal, crime-syndicate
Terroristen	Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolkingsgroepen angstwil aanjagen of politieke besluitvorming probeert te beïnvloeden, door geweld tegen mensen te gebruiken of ontwrichtende schade aan te richten.	Threat actor	Terrorist
Hacktivisten	Actor die uit ideologische motieven digitale aanvallen vanactivistische aard pleegt.	Threat actor	Activist
Cybervandalen en scriptkiddies		Threat actor	Hacker
Insider	Kwaadwillende werknemer of ingehuurde	Threat actor	Insider-disgruntled
Onbekend		Threat actor	Unknown
Geen	Dreigingen door niet opzettelijke fouten van mensen. Bijvoorbeeld misconfiguratie.	Threat actor	

Kwetsbaarheid in	*Kwetsbaarheid dat het risico veroorzaakt. Zie ISO 27005 Annex*
Hardware	Kwetsbaarheid in hardware veroorzaakt risico.
Software	Kwetsbaarheid in software veroorzaakt risico.
Netwerk	Kwetsbaarheid in netwerk veroorzaakt risico.
Organisatie	Kwetsbaarheid in organisatie (afwezigheid processen/procedures/awareness etc) veroorzaakt risico.
Supply chain	Kwetsbaarheid in supply chain veroorzaakt risico.
Fysieke veiligheid	Fysieke kwetsbaarheid veroorzaakt risico. (Bijvoorbeeld vernieling)

Dreigingsselectie ten behoeve van deelwaarnemingen reguliere inspectie 2021

5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e	5.1.2.e
DDoS	Foute medewerkers		Social Engineering / (Spear)phishing	Supply chain / leveranciersmanagement	Supply chain / leveranciersmanagement, o.a. geopolitieke dimensie	Supply chain / leveranciersmanagement	Supply chain / leveranciersmanagement	Hardwarekwetsbaarheden en legacy		Vulnerabilitymanagement, inclusief omgang zeroday en oneday kwetsbaarheden
Hardwarefalen	Sabotage/verstoring door staten		Wachtwoord hergebruik	(Remote) beheer en toegang door leveranciers	Legacy	Social Engineering	Risico's voor Business Continuity Management (BCM)	Supply chain / leveranciersmanagement		Supply chain / leveranciersmanagement
BGP-hijacking	Remote beheer leveranciers		Procedures niet meer up to date door migratie naar de cloud	Afhankelijkheid kennis derde partijen	Risico's voor Business Continuity Management (BCM)	Legacy	Kwetsbaarheden in software, hardware, protocollen	Risico's voor Business Continuity Management (BCM)		Risico's voor Business Continuity Management (BCM)
Afhankelijkheid cloud	Gecompromitteerde software		IT-security van subcontractors	Gebrek aan awareness bij management, inclusief te klein budget		Risico's voor Business Continuity Management (BCM)	Statelijke dreigingen	Disaster recovery		
	Grootschalige onveilige hardware		Eigen medewerkers hebben teveel toegangsrechten				Patchmanagement			
			Offsite backups							
DI	**DI**	**DI**	**DI**	**DI**	**DI**	**DI**	**DI**	**DI**	**DI**	**DI**
DNS-hijacking							Configuratiefouten			
DDoS										
Hardwarefalen										
BGP-hijacking										
Configuratiefouten										
Energie	**Energie**	**Energie**	**Energie**	**Energie**	**Energie**	**Energie**	**Energie**	**Energie**	**Energie**	**Energie**
	Kleine productiepartijen						Legacy	Uitrol onveilige infrastructuur		Uitrol onveilige infrastructuur
	Balancing by the crowd									
	Laadinfrastructuur									
Producenten	**Producenten**	**Producenten**	**Producenten**	**Producenten**	**Producenten**	**Producenten**	**Producenten**	**Producenten**	**Producenten**	**Producenten**

		Overnames							Weinig geneigd tot naleving	
									Gebrek aan awareness bij management, inclusief te klein budget	

Uit bovenstaande komen dreiging t.a.v de volgende onderwerpen naar voren. Per onderwerpen staan als subitem een aantal voorbeelden genoemd:

Top 3

1. Supplychainmanagement / leveranciersmanagement (Hoofdstuk 15 ISO27002: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers)
    - IT-security van subcontractors
    - Remote beheer en toegang leveranciers
    - Afhankelijkheid cloud
    - Afhankelijkheid kennis derde partij
    - Compromitteren van software
    - Onveilige hardware
    - Procedures niet meer up to date door migratie naar de cloud
    - Balancing by the crowd
2. Vulnerabilitymanagement (controleren op, vaststellen, verifiëren, mitigeren en patchen van kwetsbaarheden) (Hoofdstuk 12.6 ISO27002: Benutting van technische kwetsbaarheden voorkomen)
    - Software
    - Hardware
    - Protocollen
    - Omgang met legacy
    - Zero-day en one-day kwetsbaarheden
3. Business continuity management, inclusief disaster recovery (Hoofdstuk 7 ISO27002: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie)
    - Hardwarefalen
    - DDoS
    - BGP-hijacking

Verder vaak genoemd, ter overweging om mee te nemen:

Awareness medewerkers en management
- Aandacht en budget vanuit management
- Risico’s door acties werknemers

Statelijke dreigingen
- Sabotage
- Spionage

Samenvattende longlist dreigingen en ontwikkelingen op basis van dreigingsmonitor 2020

Ontwikkelingen

1) Ivm corona zijn organisaties erg afhankelijk van thuiswerkvoorzieningen/werken op afstand
2) Dreiging van aanvallen door statelijke actoren tbv spionage en (voorbereiding van) sabotage
3) Dataficering energienet; toename (ICT)-automatisering energienet.
4) Decentrale opwekking en afname elektriciteit
5) Producenten elektriciteit hebben mogelijk minder aandacht voor Wbni en security
6) Kleine partijen hebben onvoldoende aandacht en geld voor security
7) Procedures niet meer up to date door migratie naar Cloud
8) Impact van social media / nepnieuws
9) Vraagkant elektriciteit kan gemanipuleerd worden met gevolgen voor het net
10) Marktontwikkeling elektriciteitssector
    a) Uitbreiding Balancing Service Provider
    b) Aggregators
11) Openbare informatie die misbruikt kan worden om kwetsbaarheden in essentiële diensten te vinden.
12) Politieke keuzes kunnen risico's voor continuïteit essentiële diensten met zich meebrengen.
13) AEDs/producenten actief in meerder EU-landen, mogelijk conflict van normen

Aanvalsvectoren

14) Afhankelijkheden centrale onderdelen in het elektriciteitssysteem
    a) EPEX (European Power Exchange voor spot market)
    b) ENTSO-E Transparency Platform (Load, Generation, Transmission, Balancing, Outages and Congestion Management)
    c) ENTSOE European Awareness System (realtime systeem voor uitwisseling van informatie tussen TSOs, o.a. frequentie en interconnectors)
15) Gecompromitteerde useraccounts/credentials
16) Toegang tot systemen op afstand door leveranciers
17) Toegang met laptop tot OT door monteurs
18) Koppeling ICS aan internet
19) Kwetsbaarheden
    a) Softwarekwetsbaarheden
    b) Hardwarekwetsbaarheden
    c) Hardwarekwetsbaarheden die niet verholpen kunnen worden
    d) Kwetsbaarheid en afhankelijkheid tijdsynchronisatie
    e) Legacy protocollen
20) Supplychainrisico / ketenafhankelijkheid
    a) Geopolitiek / gebruik apparatuur landen met offensief cyberprogramma
    b) Leveranciers / onderaannemers
    c) Onveilige producten geleverd door leveranciers
    d) Aanvallen op ketenpartners die belangrijk zijn voor leveren essentiële dienst
    e) Gecompromitteerde softwaredistributiekanalen
    f) Vendor lock-in
    g) Capaciteit stroomvoorziening
21) Software

a) Gebruik kwetsbare softwareonderdelen
b) Secure Software Development
c) Versiebeheer
d) Deployment

22) Grootschalige uitrol (mogelijk) onveilige infrastructuur met invloed op elektriciteitsnet
a) Laadpalen
b) Smart Grid
c) IoT

23) Verstoren communicatie
24) Shadow IT (gebruik van ICT-middelen die geen bedrijfsmiddelen zijn)

Aanvalsmethoden

25) Malware
26) Ransomware
27) Social Engineering
a) (Spear)phishing
b) Caller-ID spoofing
c) Misbruiken authenticatiemethoden clouddiensten
d) Business email compromise
e) Hoax

28) Authenticatie
29) DNS-hijack
30) BGP-hijack
31) Zeroday en one-day-aanvallen
32) DDoS
33) Insider threat

Omgang met (onbedoelde) verstoringen

34) Configurationmanagement
a) BGP-routeringsfouten
b) Software Defined Networking
c) Standaard kwetsbare configuratie
d) Beheer PKI-omgeving
e) Beheerfouten
f) Configuratiefouten
g) Hardwarefalen

Met opmerkingen 5.1.2.e **]:** Gerelateerd aan ISO -> Assetmanagement en CMBD

35) BCM
a) Geen controle op werkende backups

36) Menselijke fouten
37) Niet geautomatiseerd deployen

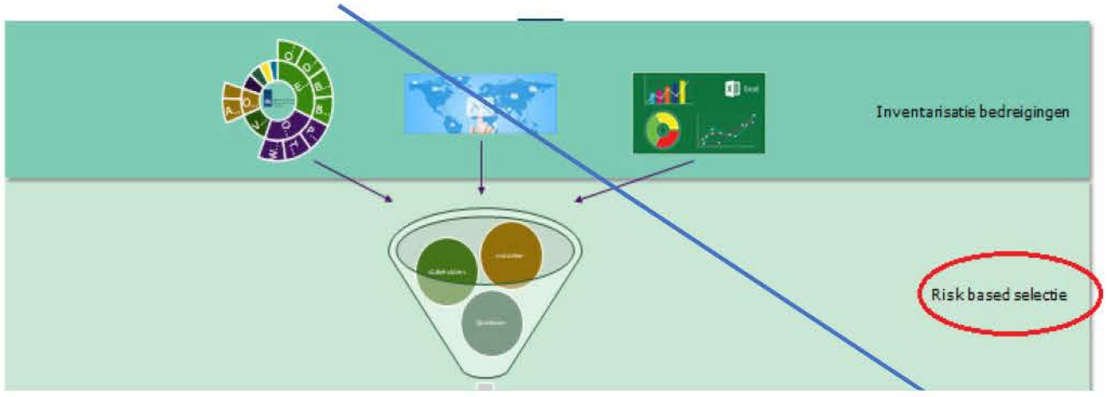
Risicomodel: identificatie van risico's aan de hand van dreigingen en vervolgens analyseren en beoordelen in hoeverre het een relevante risico is op basis van het risicomodel.
Het doel van dit risicomodel is om inzicht te krijgen in het risicobeeld van de AEDs. Dit levert input voor het bepalen van de jaarlijkse onderwerpen voor de thema-inspecties bij de AEDs die opgenomen worden in de jaarplanning. Ook kan het richting geven bij het selecteren van verdiepingsonderwerpen voor de reguliere inspecties of het (laten) uitvoeren van themaonderzoeken.

Onderstaande is een toelichting van het risicomodel template die gebruikt gaat worden. Voor het uitvoeren van het risicomodel kan er gebruikt wordt van de procedurebeschrijving buiten reikwijdte waarbij de afzonderlijke stappen binnen het proces zijn beschreven.

Toezichtsdoel: Aanbieders (essentiële diensten en digitale dienstverleners) treffen adequate maatregelen om de cyberweerbaarheid van vitale infrastructuren te borgen.
Risico: Onvoldoende cyberweerbaarheid in de keten van vitale infrastructuren.
AT voert als toezichthouder naast regulier inspecties o.a. thematische onderzoeken uit om de afhankelijkheid, samenhang en overlap van een essentiële dienst en digitale dienstverlener te beoordelen. Het doel van de thema-inspectie is om een diepgaand beeld van een onderdeel van de informatiebeveiliging van de essentiële dienst van de AED te verkrijgen. Op basis van een risicomodel wordt bepaald welke onderwerpen in de jaarlijkse thematische onderzoeken wordt uitgevraagd.
Dit excel document is een template waarbij de interne als de externe risicofactoren (Dreigingsmonitor) worden verzameld en verwerkt in een risicomatrix.
Uit de risicomatrix wordt vervolgens bepaald wat de mogelijke thema inspecties voor de komende jaar kunnen zijn. Het risicomodel wordt als input gebruikt uiteindelijk wordt in een workshop met de betrokken specialistische inspecteurs bepaald wat de meest relevante onderwerpen zijn voor de thematische onderzoeken. Let op dit is een kwalitatieve risicoanalyse en geen exacte wetenschap op detail niveau, gebruik van 'gezond verstand' en vakkundige oordeelsvorming blijft een grote rol spelen.
Objecten: per AED-sector wordt een risicoanalyse opgesteld waaronder (niet limitatief):
•Gas:
oGasproductie, landelijk transport en distributie gas: NAM en opslag Norg
oRegionale distributie gas
•Energieproducenten;
oEnergiecentrales
oZonneparken
oWindturbines
oOlievoorziening
•Opslag voorraadvorming Aardolieproducten (COVA)
•Internet en datadiensten 'digitale infrastructuur';
oInternet Exchange (Ams-ix, NL-IX)
o.nl top level domain (SIDN)

Input vanuit de interne en externe risicofactoren zijn uitgewerkt in onderstaande tabbladen:
-het tabblad "Assessment Resultaten" omvat de opgeleverde resultaten van de AED.
-het tabblad "Context informatie AT" omvat aantekeningen /opmerkingen / bijvangst naar aanleiding van gesprekken met AED.
-het tabblad "Incidenten historie" omvat gemelde incidenten bij AT of incidenten van AED.
-het tabblad "Risico analyse" omvat de uitgevoerde risicoanalyse door AED
-het tabblad "Ontwikkelingen en trends " omvat relevante informatie die uit accountmanagement gesprekken met AED, relevante trends.
-het tabblad "Dreigingen" omvat relevante dreigingen voor ons toezichtsveld.
-het tabblad "Cyber incidenten sector breed" omvat gebeurtenissen zoals aanvallen, storingen en calamiteiten.
-het tabblad "Toezicht en AT-risico's" omvat algemene risico's voor het WBNI-toezicht van AT.
-het tabblad "**Totaal analyse**" omvat alle informatie uit bovenstaande tabbladen die meegenomen worden in de risico matrix. Vervolgens worden hoge risico's meegenomen in thema inspecties deze worden vergeleken met de ISO beheersdoelstellingen. Tot slot worden de ISO beheerdoelen gegroepeerd naar inspectie thema's en hierna volgt een planning uit voort na prioritering.

Hieronder zie je het totale Toezichtsmodel waarbij dit document een template betreft voor het risicomodel (zie tabblad totaal anayse).



Begrippenkader en afkortingen

Incident (ISO 27035)

Een of meerdere gerelateerde geidentificeerde inbreuken op informatiebeveiliging die schade kunnen toebrengen aan een organisatie of zijn bedrijfsvoering.

Dreiging (ISO 27005)

Een dreiging heeft de potentie om schade toe te brengen aan assets, zoals informatie, processen, systemen en daarmee organisaties. Dreigingen kunnen een menselijke of natuurlijke oorsprong hebben en kunnen opzettelijk of onopzettelijk zijn.

Trend

waarin zich iets ontwikkelt naar een bepaalde richting.

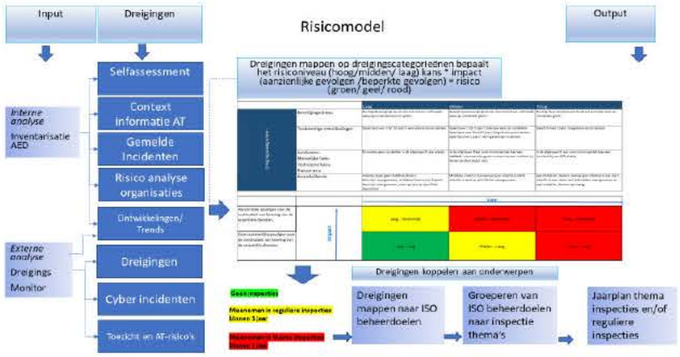
Risico (ISO 31000)

Effect van onzekerheid op (het behalen van) doelstellingen. Dit kan positief of negatief zijn. Risico's worden meestal uitgedrukt in termen van risicobronnen, mogelijke gebeurtenissen, de gevolgen en de waarschijnlijkheid daarvan.

Kwetsbaarheid (ISO 27005)

De kwetsbaarheid van een asset of assets die misbruikt kunnen worden door een of meerdere dreigingen, waarbij een asset alles is wat waarde heeft voor een organisatie, zijn business operations en de continuiteit daarvan, inclusief informatiebronnen die de missie van de organisatie ondersteunen.

Hieronder visuele weergave van het proces voor het risicomodel



zie tabblad totaal analyse voor toelichting

		Laag	Midden	Hoog
orieen	Beveiligingsniveau	Geringe Beveiligingsissues die indirect een verhoogde kans op incidenten kunnen geven.	Belangrijke beveiligingsissues die indirect een verhoogde kans op incidenten geven.	Ernstige beveilgingsissues die direct een hoge kans op incidenten geven.
	Toekomstige ontwikkelingen	Speelt pas over 5 tot 10 jaar / weinig kans op incidenten	Speelt over 2 tot 5 jaar / redelijke kans op incidenten. Speelt pas over 5 tot 10 jaar / hoge kans op incidenten Speelt binnen 2 jaar / weinig kans op incidenten	Speelt binnen 2 jaar / hoge kans op incidenten.

Dreigingscategorie				
	Incidenten: Menselijke falen Technische falen Natuurramp	Er vonden geen incidenten in de afgelopen 3 jaar plaats.	In de afgelopen 3 aar vond minimaal één keer een **incident** (voorwaardes geven waneer het een incident is) buiten de deur sector vast.	In de afgelopen 3 jaar vond minimaal één keer een incident bij een AED plaats.
	Kwaadwillende	Intentie, maar geen middelen/kennis Activiteit waargenomen, middelen/ kennis zijn beperkt Activiteit waargenomen, maar gericht op specifieke doelwitten	Middelen / kennis zijn aanwezig en intentie is sterk. Intentie is sterk en activiteiten waargenomen.	Veel middelen / kennis aanwezig en intentie is zeer sterk. Intentie is zeer sterk, veel activiteiten waargenomen en veel middelen / kennis aanwezig.
		kans →		
Aanzienlijke gevolgen voor de continuïteit van levering van de essentiële diensten.	Impact ↑	Laag - Aanzienlijk	Midden - Aanzienlijk	Hoog - Aanzienlijk
Geen aanzienlijke gevolgen voor de continuïteit van levering van de essentiële diensten.		Laag - Laag	Midden - Laag	Hoog - Laag*

*Hoewel de impact behorende bij deze inschatting geen aanzienlijke gevolgen heeft voor de continuïteit van de levering van de essentiële dienst, krijgt deze toch kleur ‘Rood’ vanwege het maatschappelijk belang dat er kan zijn indien de bedreiging of het risico zich voordoet.

Uitgevoerde Assessment onderwerpen met laagste score < 3 voor desbetreffende AED-sector			
Toelichting: Gebruik de meest recente assessment resultaten van de diverse AEDs. Vul Assessment onderwerpen met score < 3 in het tabblad. Je kunt ook de AED de huidige selfassessment resultaten vergelijken met de vorige resultaten. Wat valt op en wat is mogelijk interessant om als onderwerp te nemen voor de deelwaarneming.Een voorbeeld kan zijn dat een onderwerp in 2021 veel hoger scoort t.o.v. 2019, dit kan een aanleiding zijn om dit onderwerp in de deelwaarneming te betrekken.			
Onderwerp	Score	Opmerkingen	Dreiging
1			

Context informatie AT : omvat aantekeningen /opmerkingen / bijvangst naar aanleiding van gesprekken met AED wat niet direct te relateren is aan het toetsingskader	
Toelichting: Vul relevante aanvullende informatie/ constateringen die betrekking hebben op mogelijke risico's over de AEDs die in gespreksverslagen of aantekeningen zijn vastgelegd.	
Algemeen Beeld	Dreiging

Historisch overzicht incidenten laatste 3 jaar (sector)					
Toelichting: Verzamel de gemelde incidenten van AEDs en vul de gemelde incidenten in het tabblad zie hieronder als voorbeeld					
sector	Datum	Boven melddrempel	Soort Incident	Oorzaak	Omschrijving

Risico Analyse van bedrijf

Toelichting: Gebruik de meest recente risicoanalyse van AEDs die AT tot de beschikking heeft en vul relevante risico's in het risicomodel. (Maak eventueel gebruik van de gegevens van vorige jaar gebruikte risicomodel en actualiseer het). Het opvragen van risicoanalyse gebeurd bij een thema inspectie voor de AED's. Wanneer er sprake is van een reguliere inspectie van de AED's wordt er geen aanvullende risico analyse opgevraagd.

Categorie	Dreiging	Risk Level	evt. Commentaar
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		
nvt	nvt		

Dreigingen

Toelichting: selecteer uit de dreigingsmonitor de mogelijke dreigingen voor de desbetreffende AED-sector en leg het vast in het risicomodel. Dit is te vinden in het document dreigingsmonitor tabblad " monitor" filter op dreiging. Zie hieronder een voorbeeld

Sector	dreiging	Omschrijving	Oorzaak	Aard	Vermoedelijke actor	Aantasting BIV	Kans op incident	Aanzienlijke gevolgen voor continuïteit essentiële dienst	Regio (s)	Land (en)	Jaar waarin - incident plaatsvond - dreiging geconstateerd werd - (Toekomstige) ontwikkeling naar verwacht doorbreekt	Bron	MITRE ATT&CK link	MITRE ATT&CK ICS link	Toegevoegd door	
		Ter voorbereiding van de workshop hebben we van tevoren een aantal mogelijk relevante trends,dreigingen en incidenten, toezicht risico geindentificeerd uit de dreigingsmontitor [20201109 - Dreigingsmonitor.xlsx] en vastgelegd in een longlist [20201111 - Samenvattende longlist dreigingen 2020]. Tijdens de workshop hebben de deelnemers de volgende onderstaande trends/ dreigingen/ incidenten het vaakts benoemd [20201111 - Dreigingsselectie ten behoeve van deelwaarnemingen reguliere inspectie 2021.docx]	20201109 - Dreigingsmonitor.xlsx 20201111 - Samenvattende longlist dreigingen												
Alle		Onvoldoende beheersing van het Supplychainmanagement (SCM)/ leveranciersmanagement risico waaronder •IT-security van subcontractors •Remote beheer en toegang leveranciers •Afhankelijkheid cloud •Afhankelijkheid kennis derde partij •Compromitteren van software •Onveilige hardware •Procedures niet meer up to date door migratie naar de cloud •Balancing by the crowd	20201111 - Dreigingsselectie ten behoeve van												
		Onvoldoende beheersing van het vulnerabilitymanagement (controleren op, vaststellen, verifiëren, mitigeren en patchen van kwetsbaarheden) •Software •Hardware •Protocollen •Omgang met legacy •Zero-day en one-day kwetsbaarheden												
		Onvoldoende beheersing van Business Continuity Management (BCM) •Hardwarefalen •DDoS •BGP-hijacking												

Ontwikkelingen sector adhv informele gesprekken met AED (relatiebeheer), Trend en Toezicht & AT risico				
Toelichting: Selecteer uit de dreigingsmonitor de meest relevante ontwikkelingen, trends voor de desbetreffende AED-sector. Dit is te vinden in het document dreigingsmonitor tabblad " monitor" filter op (toekomstige) ontwikkelingen.				
Voeg daarnaast ook evt. ontwikkelingen/trends van AED-sector naar aanleiding van informele gesprekken met AED (relatiebeheer).				
Sector	(Toekomstige) ontwikkeling	Omschrijving	Oorzaak	Aard
	Ter voorbereiding van de workshop hebben we van tevoren een aantal mogelijk relevante (toekomstige) ontwikkelingen, incidenten , toezicht risico en dreigingen geindentificeerd uit de dreigingsmonitor en vastgelegd in een longlist. Tijdens de workshop hebben de deelnemers bepaald welke relevante punten opgenomen moet worden als mogelijk risico voor de AED's/ sector. Zie tabblad ***dreigingen*** *voor de uitwerkingen.*			

Vermoedelijke actor	Aantasting BIV	Kans op incident	Aanzienlijke gevolgen voor continuïteit essentiële dienst	Regio (s)	Land (en)	Jaar waarin - incident plaatsvond - dreiging geconstateerd werd - (Toekomstige) ontwikkeling naar verwacht doorbreekt	Bron

MITRE ATT&CK link	MITRE ATT&CK ICS link	Toegevoegd door	

Cyber incidenten

Ter voorbereiding van de workshop hebben we van tevoren een aantal mogelijk relevante (toekomstige) ontwikkelingen, incidenten , toezicht risico en dreigingen geindentificeerd uit de dreigingsmonitor en vastgelegd in een longlist. Tijdens de workshop hebben de deelnemers bepaald welke relevante punten opgenomen moet worden als mogelijk risico voor de AED's/ sector. Zie tabblad dreigingen voor de uitwerkingen.

Sector	Incident, dreiging of (Toekomstige) ontwikkeling	Omschrijving	Oorzaak	Aard	Vermoedelijke actor	Aantasting BIV	Kans op incident	Aanzienlijke gevolgen voor continuïteit essentiële dienst	Regio (s)	Land (en)	Jaar waarin - incident plaatsvond - dreiging geconstateerd werd - (Toekomstige) ontwikkeling naar verwacht doorbreekt	Bron	MITRE ATT&CK link	MITRE ATT&CK ICS link	Toegevoegd door

5h

"Toezicht en AT-risico's" omvat algemene risico's voor het WBNI-toezicht van AT.	
Ter voorbereiding van de workshop hebben we van tevoren een aantal mogelijk relevante (toekomstige) ontwikkelingen, incidenten , toezicht risico en dreigingen geindentificeerd uit de dreigingsmonitor en vastgelegd in een longlist. Tijdens de workshop hebben de deelnemers bepaald welke relevante punten opgenomen moet worden als mogelijk risico voor de AED's/ sector. Zie tabblad dreigingen voor de uitwerkingen.	

Sector	Risico voor toezicht van AT	Relevantie	Wanneer relevant	Bron	Link	Datum	Opmerkingen	Toegevoegd door

Totaalanalyse

Toelichting: relevante dreigingen uit de voorgaande tabbladen worden hierin geimporteerd

Op basis van de workshop van 9 november 2020 heeft er een prioritering plaats gevonden voor de externe analyse

Document

	Totaaloverzicht van dreigingen uit verschillende bronnen							
	A. Assessment	B.Context informatie AT	I. (gemelde) Incidenten	R. Risico analyse	O. Ontwikkelingen Trends zie kolom G 'Dreigingen' samengevat	D. Dreigingen	C. Cyberincidenten sectorbreed zie kolom G 'Dreigingen' samengevat	T. Toezicht en AT-Risico's zie kolom G 'Dreigingen'samengevat
1	0 A1	0 B1	Buiten reikwijdte I1	nvt	0	Onvoldoende beheersing van het Supplychainmanagement (SCM)/ leveranciersmanagement risico waarond D1 •IT-security van subcontractors •Remote beheer en toegang leveranciers •Afhankelijkheid cloud •Afhankelijkheid kennis derde partij •Compromitteren van software •Onveilige hardware •Procedures niet meer up to date door migratie naar de cloud •Balancing by the crowd	0	0
2	0 A2	0 B2	Buiten reikwijdte I2	nvt	0	Onvoldoende beheersing van het vulnerabilitymanagement (controleren op, vaststellen, verifiëren, mitigeren en patchen van kwetsbaarheden) •Software •Hardware •Protocollen •Omgang met legacy •Zero-day en one-day kwetsbaarheden D2	0	0
3	0 A3	0 B3	Buiten reikwijdte I3	nvt	0	Onvoldoende beheersing van Business Continuity Management (BCM) •Hardwarefalen •DDoS •BGP-hijacking D3	0	0
4	0 A4	0 B4	Buiten reikwijdte I4	nvt		0 D4		
5	0 A5	0 B5	Buiten reikwijdte I5	nvt		0		

Mappen van dreigingen naar risiconiveau door de bolletjes te plotten op het risicomodel (dit wordt gezamelijk gedaan in een workshop)

hieronder een aantal dreigingen uitgewerkt als voorbeeld

Dreigingscategorieën		Laag	Midden	Hoog
	Beveiligingsniveau	Geringe beveiligingsissues die indirect een verhoofde kans op incidenten kunnen geven	Belangrijke beveiligingsissues die indirect een verhoogde kans op incidenten geven	Ernstige beveiligingsissues die direct een hoge kans op incidenten geven.
	Toekomstige ontwikkelinge	Speelt over 5 tot 10 jaar met lage kans op incidenten	- Speelt over 5 tot 10 jaar met hoge kans op incidenten - Speelt over 2 tot 5 jaar met middelgrote kans op incidenten - Speelt binnen 2 jaar met lage kans op incidenten	Speelt binnen 2 jaar met hoge kans op incidenten
	Incidenten: - Falen van systeem - Natuurlijke oorzaak - Menselijke fout - Falen van derde partijen (keten)	In de afgelopen 3 jaar vond er buiten Europa binnen de sector een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond binnen de sector binnen Europa een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond een van de genoemde incident bij een AED in Nederland plaats
	Incidenten en dreigingen door kwaadwillenden	Doelwit is sectoronafhankelijk Kennis/middelen zijn beperkt Activiteit is waargenomen	Doelwit is de sector binnen Europa Kennis/middelen aanwezig Activiteit is waargenomen	Doelwit is de sector in Nederland Kennis/middelen aanwezig
			Kans	
Aanzienlijke gevolgen voor de continuïteit van de levering van de essentiële diensten	Impact	Laag - Aanzienlijk	Midden - Aanzienlijk	Hoog - Aanzienlijk D3 D2 D1

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

5.1.2.e
Cc Wbni-team

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Van
5.1.2.e
5.1.2.e
5.1.2.e
5.1.2.e

Datum
2 september 2021

Bijlagen
-

memo

Onderwerpkeuze 2022 op basis van risicoanalyse

Aanleiding

Conform het Wbni toezichtsmodel en bijhorende risicomodel kiest Agentschap Telecom informatie- en risicogebaseerd de onderwerpen die bij inspecties en andere toezichtactiviteiten extra aandacht behoeven.[1] Voor de thema-inspecties 2022 en andere activiteiten dienen deze onderwerpen te worden vastgesteld.

Voorstel

Eind 2020 heeft een workshop plaatsgevonden wat resulteerde in een *longlist* en *shortlist* van relevante risico's en dreigingen voor de Wbni sectoren waar AT toezicht op houdt. De shortlist betrof:

- Business Continuity management
- Supply Chain Management
- Vulnerability Management

16 augustus 2021 zijn deze bevindingen in klein comité besproken.[2] Zij kwamen op basis van de bijgewerkte dreigingsmonitor en aanvullende publicaties zoals het Cyber Security Beeld Nederland tot de conclusie dat de risico's en dreigingen ten opzichte van eind 2020 niet wezenlijk zijn veranderd.

Het voorstel is daarom om voor de thema-inspectie aan te sluiten bij de uitkomsten van de eerdere analyse en niet nogmaals het volledige risicomodelproces te doorlopen. Het voorstel is om te kiezen voor Business Continuity Management als thema voor de thema inspectie 2022. De reden voor deze keuze is dat dit onderwerp het aspect 'continuïteit' van de essentiële dienst het meest raakt. Bovendien dekken we hiermee een nieuw BBNI-domein af, namelijk herstel.[3]

Daarnaast is het voorstel om het onderwerp Supply Chain Management ook een plek te geven in de planning voor 2022. Dit in de vorm van thematisch toezicht, waarbij bijvoorbeeld gewerkt wordt aan een publicatie, dialoogsessie etc.

[1] Zie de memo 'procedure risicomodel' voor meer informatie.
[2] Aanwezig: 5.1.2.e , 5.1.2.e , 5.1.2.e
[3] In 2020 vond de thema-inspectie Detectie Monitoring en Logging plaats, waar het BBNI-domein detectie centraal stond.

Omwille van capaciteit en belasting voor de AEDs is het voorstel om Vulnerability Management op te pakken in een later jaar (2023) op te pakken.

De onderwerpkeuze betreft het reguliere toezichtproces voor AED en DSP. Voor het thematische toezicht is reeds een onderwerpkeus gemaakt in een overzicht van doelen en acties, op basis van meerdere sessies met een externe partij. Tezamen vormt dit de programmering voor het toezicht Wbni voor 2022.

Gevraagd besluit[4]

- Instemmen met het niet nogmaals volledig doorlopen van het risicomodel, gezien de ongewijzigde omstandigheden.
- Instemmen met het selecteren van Business Continuity Management als onderwerp van onderzoek voor de thema inspectie 2022.
- Instemmen met het selecteren van Supply Chain Management als onderwerp voor thematisch toezicht 2022
- Instemmen met de voorlopige globale planning (de onderwerpen genoemd in voorliggende memo zijn in de paarse velden weergegeven):

<table>
<tr><th>Q1</th><th>Q2</th><th>Q3</th><th>Q4</th></tr>
<tr><td>Uitloop reguliere inspectie Netbeheer</td><td></td><td></td><td></td></tr>
<tr><td>Uitloop inventarisatie Producenten</td><td>Samenvatting inventarisatie Producenten</td><td rowspan="2">Account gesprekken & terugkoppeling Producenten</td><td></td></tr>
<tr><td></td><td>Account gesprekken Netbeheer & DI</td><td>Account gesprekken Netbeheer & DI</td></tr>
<tr><td>Opstellen Kader BCM</td><td>Aankondigingsbrief thema inspectie BCM Netbeheer & DI*</td><td>Plannen en voorbereiden thema inspectie BCM Netbeheer & DI</td><td>Uitvoeren thema inspectie BCM Netbeheer & DI</td></tr>
<tr><td></td><td></td><td colspan="2">Thematisch toezicht SCM</td></tr>
<tr><td>Toezicht DSP</td><td>Toezicht DSP</td><td>Toezicht DSP</td><td>Toezicht DSP</td></tr>
<tr><td>Overig</td><td>Overig</td><td>Overig</td><td>Overig</td></tr>
</table>

*Dit betreft de formele aankondiging. In Q4 worden de AED's al geïnformeerd over de onderwerpen en het proces op hoofdlijnen.

[4] Akkoord 5.1.2.e d.d. 1-9-2022.

Toezicht op de Wbni door Agentschap Telecom

Deelonderzoek binnen het VO EZK

(Conceptnota van bevindingen)

Conceptversie 25 februari 2022

Inhoud

Vooraf

In ons jaarlijkse verantwoordingsonderzoek beoordelen wij de jaarverslagen die de ministers op Verantwoordingsdag aanbieden aan de Staten-Generaal, onderzoeken we de bedrijfsvoering van de ministeries gedurende het begrotingsjaar, en doen we onderzoek naar de beleidsinformatie. Deze nota van bevindingen betreft ons onderzoek naar de bedrijfsvoering.

In ons onderzoek naar de bedrijfsvoering van de ministeries onderzoeken wij of het begrotingsbeheer, het financieel beheer, de materiële bedrijfsvoering en de daartoe bijgehouden administraties van het Rijk voldoen aan de normen van doelmatigheid, rechtmatigheid, ordelijkheid, controleerbaarheid en betrouwbaarheid. De minister is er voor verantwoordelijk dat de verantwoording en de bedrijfsvoering voldoen aan de daaraan te stellen kwaliteitseisen.

Als we vinden dat een onderdeel van de bedrijfsvoering onvoldoende beheerst verloopt, noemen wij dat een ‘onvolkomenheid’ of een ‘ernstige onvolkomenheid’. In onze rapporten geven we niet alleen informatie over de onvolkomenheden, maar ook over belangrijke risico’s en aandachtspunten.

Een uitgebreide methodologische verantwoording over ons jaarlijkse verantwoordingsonderzoek staat op onze website: https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/over-dit-onderzoek

Deze nota van bevindingen is onderdeel van het Verantwoordings-onderzoek (VO) EZK 2021 door de Algemene Rekenkamer en bevat bevindingen over het beleid en de uitvoering van het toezicht op de Wet

beveiliging netwerk- en informatiesystemen door het Ministerie van EZK, met de focus op Agentschap Telecom.

Deze nota is géén onderzoeksrapport en bevat geen bestuurlijke conclusies. Op basis van de conceptnota, de ontvangen reactie en eventuele aanvullende informatie vormt de Algemene Rekenkamer haar bestuurlijke oordeel dat via een conceptrapport voor bestuurlijke reactie wordt voorgelegd aan de verantwoordelijke minister.

De conceptnota is voor ambtelijk hoor en wederhoor op 25 februari 2022 naar het Ministerie van EZK verstuurd. De ambtelijke reactie hebben wij op datum ontvangen. De reactie van het ministerie is verwerkt en de nota is definitief gemaakt.

1 Inleiding

1.1 Aanleiding voor het onderzoek

De Nederlandse vitale infrastructuur

Bepaalde processen zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur.[1] Bij de herijking van de vitale infrastructuur uit 2015[2] is de categorie 'Digitale overheid' aan de vitale infrastructuur toegevoegd. 'Vitale aanbieders' zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving.

Toezicht op de vitale sectoren

Sinds 9 november 2018 is de Wet beveiliging netwerk- en informatie-systemen[3] (Wbni) van kracht. De Wbni is erop gericht de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. Vitale aanbieders[4] en digitaledienstverleners[5] (DSP's) moeten aan de Wbni voldoen. Ze moeten maatregelen nemen om incidenten te voorkomen en incidenten met aanzienlijke gevolgen melden. Agentschap Telecom (AT) is toezichthouder op de Wbni voor de vitale sectoren 'Energie' en 'Digitale infrastructuur' en voor de digitaledienstverleners. [6]

[1] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/documenten/publicaties/2018/02/01/factsheet-weerbare-vitale-infrastructuur.
[2] Tweede Kamer, vergaderjaar 2014–2015, 30 821, nr. 23.
[3] https://wetten.overheid.nl/BWBR0041515/2021-08-01.
[4] Volgens de definitie in de Wbni art. 5 lid 1, dit zijn (categorieën) aanbieders van een essentiële dienst of (categorieën) andere vitale aanbieders.
[5] Dit zijn online marktplaatsen, zoekmachines en cloudcomputerdiensten, zie ook Wbni art. 1
[6] Staatscourant 2018 nr. 63334 7 november 2018 (https://wetten.overheid.nl/BWBR0041524/2018-11-09).

Kader van de Wbni

De richtlijn netwerk- en informatiebeveiliging (NIB-richtlijn)[7] is een 'cybersecurity-wet' op Europees niveau. Het uitgangspunt van deze richtlijn is het tot stand brengen van een hoog gemeenschappelijk niveau van beveiliging van netwerk en informatiesystemen die essentieel zijn voor de instandhouding van kritieke maatschappelijke en economische activiteiten (zoals energie, het bankwezen en de gezondheidszorg) in de Europese Unie.[8] Dit moet zorgen voor meer eenheid in beleid over netwerk- en informatiebeveiliging. Nederland heeft de NIB-richtlijn geïmplementeerd in de Wbni en het Besluit beveiliging netwerk- en informatiesystemen[9] (Bbni) zoals ze in werking zijn getreden op 9 november 2018 respectievelijk 1 januari 2019.

Deelonderzoek binnen het VO 2021

In ons Verantwoordingsonderzoek (VO) 2021 bij het Ministerie van EZK hebben we onderzocht of het Ministerie van EZK/AT voldoende invulling geeft aan het toezicht op de naleving van de Wbni. Dit deelonderzoek is in § 1.2 van het overkoepelende projectvoorstel VO EZK 2021 aangekondigd.

1.2 Leeswijzer

Voor de indeling van deze nota van bevindingen volgen we de onderzoeksvragen uit ons plan van aanpak. De nota is als volgt ingedeeld:

- Hoofdstuk 2: Hier beschrijven we de opzet van ons onderzoek.
- Hoofdstuk 3: Hier beschrijven we het beleidsterrein voor het toezicht op de Wbni op hoofdlijnen.
- Hoofdstuk 4: Hier beschrijven we de opzet van het toezicht op de Wbni bij het Ministerie van EZK.

[7] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194). Naar deze wet wordt ook wel verwezen als 'NIS', dat is de Engelstalige verwijzing. In deze nota gebruiken we beide termen.
[8] Gebaseerd op de Wbni, onder andere overweging 20.
[9] https://wetten.overheid.nl/BWBR0041520/2021-05-01.

- Hoofdstuk 5: Hier beschrijven we een aantal praktijkcases van de uitvoering van het toezicht op de Wbni door AT.

In bijlage 1 hebben we een overzicht opgenomen van de gebruikte afkortingen.

2 Onderzoeksopzet

In dit hoofdstuk geven we een toelichting op de onderzoeksopzet: de doel- en probleemstelling (§ 2.1), de onderzoeksvragen (§ 2.2), de gebruikte normen (§ 2.3) en de onderzoeksaanpak (§ 2.4).

2.1 Doel- en probleemstelling

Doelstelling

De minister van EZK heeft Agentschap Telecom aangewezen als toezichthouder zoals bedoeld in de Wbni. We willen met dit deelonderzoek nagaan hoe AT dit toezicht in de praktijk uitvoert, hoe de communicatie met de andere toezichthouders verloopt en of hier verbeteringen mogelijk zijn.

Probleemstelling

De probleemstelling voor dit onderzoek is:

- In hoeverre is het toezicht op de naleving van de Wbni voldoende geregeld voor de (vitale) sectoren die onder de verantwoordelijkheid van de minister van EZK vallen?

2.2 Onderzoeksvragen

Het onderzoek bestaat uit de volgende hoofdvragen:

I. Hoe ziet het beleidsterrein van EZK er op hoofdlijnen uit als het gaat om het toezicht ingevolge de Wbni?
II. Hoe is het toezicht door AT ingevolge de Wbni georganiseerd? (Opzet)
III. Hoe is het toezicht door AT in een aantal praktijkgevallen uitgevoerd? (Werking)
IV. Welke verbeteringen zijn er eventueel mogelijk?

We hebben deze hoofdvragen als volgt uitgewerkt:

I Beschrijving van het beleidsterrein:

1. Voor welke (categorieën van) aanbieders van diensten geldt de Wbni?
2. Wat zijn de rechten en plichten van deze aanbieders?
3. Welke actoren zijn betrokken bij het toezicht op de Wbni?
4. Wat zijn de taken en bevoegdheden van de toezichthouders op de Wbni (bijvoorbeeld audits, handhaving etc.)?

II Invulling van het toezicht door AT

1. Op welke wijze voeren AT en EZK de risicoanalyse en prioritering uit voor het toezicht op de Wbni en hoe leggen ze dit vast, bijvoorbeeld:
    - Op welke gronden en door wie zijn de Aanbieders van Essentiële Diensten (AED's) en Andere Aangewezen Vitale Aanbieders (AAVA's) aangewezen, en hoe worden deze keuzes geactualiseerd?
    - Hoe houdt AT zicht op de digitaledienstverleners (aangezien deze niet individueel worden aangewezen)?
    - Wat zijn de overwegingen voor het uitvoeren van een actief danwel reactief toezichtsbeleid op bepaalde aanbieders?
    - Heeft AT een meerjarenplan voor het toezicht op de Wbni opgesteld?
2. Welke normen worden gehanteerd door AT, en door wie worden deze normen vastgesteld, bijvoorbeeld:
    - Is er een 'drempelwaarde' vastgesteld voor het melden van een incident?
    - Wat zijn de normen voor 'bijna-ongelukken', (hoe) is dat geoperationaliseerd?
3. Hoe wordt vastgesteld of vitale aanbieders alle incidenten melden die gemeld zouden moeten worden?

4. Hoe wordt beoordeeld of door de aanbieders aan de zorgplicht is voldaan?
5. In hoeverre er overlap is met andere wet- en regelgeving op dit beleidsterrein en hoe wordt hiermee omgegaan? (bijvoorbeeld overlap met de Telecommunicatiewet en de Algemene verordening gegevensbescherming)[10]
6. Op welke wijze wordt door AT samengewerkt en kennis gedeeld met andere toezichthouders?
7. In hoeverre slaagt AT er in om voldoende gekwalificeerd personeel vrij te maken voor de toezichthoudende taak?
8. Wat zijn de eerste resultaten van het toezicht na de inwerkingtreding van de Wbni?

III Praktijk voor een aantal casussen

1. Hoe is het toezicht in de praktijk vormgegeven bij een aantal verschillende typen aanbieders (AED's, AAVA's en digitale-dienstverleners)?
2. Hoe heeft AT in de praktijk gereageerd op incidenten bij/meldingen door de verschillende typen aanbieders, bijvoorbeeld:
    - Welke acties zijn ondernomen richting de aanbieder naar aanleiding van het incident/de melding?
    - (Hoe) is met andere betrokken toezichthouders gecommuniceerd over het incident/de melding?

Bij het casusonderzoek hebben we ons gericht op het toezicht door AT, we geven geen oordelen over de dienstverleners zelf.

IV Welke verbeteringen zijn er eventueel mogelijk?

Deze nota van bevindingen bevat geen bestuurlijke conclusies. Eventuele aanbevelingen zullen worden opgenomen in ons conceptrapport.

[10] Zie ook: Tweede Kamer, vergaderjaar 2017-2018, 34 883, nr. 3 (blz. 11 en 17).

2.3 Normen

Onze normen/uitgangspunten baseren we op binnen het Rijk geaccepteerde normen, zoals de Kaderstellende visie op toezicht[11]. Verder baseren we ons op de geldende wet- en regelgeving (in het bijzonder de Wbni en de Bbni). We toetsen alleen aan normen die aansluiten bij onze onderzoeksvragen. In bijlage 2 hebben we een overzicht opgenomen van de normen die we in ons onderzoek gebruiken.

2.4 Aanpak

Dit deelonderzoek is uitgevoerd door middel van bestudering van onder andere:

- Wet- en regelgeving;
- Relevante Kamerstukken;
- Beleidsdocumenten;
- Afspraken tussen de toezichthouders;
- Verantwoordingsinformatie;
- Dossiers van meldingen en toezichtsactiviteiten van AT.

Daarnaast is een aantal interviews gehouden met medewerkers van de betrokken beleidsdirectie, van AT en van andere betrokken actoren:

- Een gesprek met medewerkers van Agentschap Telecom: Afdeling Toezicht-Digitale weerbaarheid, team Wbni (november 2021);
- Een gesprek met medewerkers van de Directie Digitale Economie van het Ministerie van EZK (november 2021);
- Een gesprek met medewerkers van het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (december 2021);
- Een gesprek met het voor de Wbni verantwoordelijke MT-lid bij Agentschap Telecom (december 2021);

[11] Kaderstellende Visie op Toezicht: Minder last, meer effect. Zes principes van goed toezicht (Tweede Kamer, vergaderjaar 2005–2006, 27 831, nr. 15).

- Een gesprek met medewerkers van Agentschap Telecom: Afdeling Toezicht-Digitale weerbaarheid team Wbni, in combinatie met dossieronderzoek (januari 2022).

Naast een beschrijving van het toezicht door AT op de Wbni hebben we bij AT een aantal dossiers van het toezicht op AED’s en DSP’s nader onderzocht. We hebben hierbij gekeken hoe AT de in opzet beschreven procedures voor toezicht heeft toegepast, waarbij we aandacht hebben besteed aan zowel het reguliere toezicht als de acties na meldingen.

Afbakening

We hebben ons met dit deelonderzoek gericht op het toezicht op de Wbni. Dit betekent dat we niet hebben gekeken naar de cybersecurity van de niet-vitale sectoren die niet onder de Wbni vallen.

3 Beschrijving beleidsterrein

In dit hoofdstuk geven we een beschrijving van het beleidsterrein van EZK op hoofdlijnen als het gaat om het toezicht ingevolge de Wbni.
We beantwoorden hiermee onze onderzoeksvragen I.1 t/m I.4:

1. Voor welke (categorieën van) aanbieders van diensten geldt de Wbni?
2. Wat zijn de rechten en plichten van deze aanbieders?
3. Welke actoren zijn betrokken bij het toezicht op de Wbni?
4. Wat zijn de taken en bevoegdheden van de toezichthouders op de Wbni (bijvoorbeeld audits, handhaving etc.)?

Verder geven we een vooruitblik op de mogelijke aanpassing van de NIB-richtlijn, die ook gevolgen zal hebben voor de Wbni.

3.1 Scope van de Wbni en Bbni (vraag I.1)

Onderzoeksvraag

- Voor welke (categorieën van) aanbieders van diensten geldt de Wbni?

Bevindingen

Dienstverleners waarvoor de Wbni geldt zijn:

1. Aanbieders van essentiële diensten (AED's);
2. Andere aangewezen vitale aanbieders (AAVA's);
3. Digitaledienstverleners/Digital Service Providers (DSP's).

In het Bbni is vastgelegd welke (categorieën van) aanbieders zijn aangewezen als AED of als AAVA. In dit deelonderzoek beperken we ons tot de aanbieders die onder de (toezichts-)verantwoordelijkheid van de minister van EZK vallen (zie bijlage 3).

Aanbieders essentiële diensten

AED's zijn vitale aanbieders in de sectoren die zijn genoemd in bijlage II van de NIB-richtlijn. [12] Het gaat om onder andere de sectoren vervoer en energie.[13] De Nederlandse AED's zijn aangewezen in het Bbni. Sommige AED's worden met name genoemd, bijvoorbeeld de NAM en Schiphol. Andere AED's moeten door de verantwoordelijke minister worden aangewezen middels een besluit, bijvoorbeeld 'aangewezen exploitanten van oliepijpleidingen' (door de minister van EZK) en 'aangewezen wegenautoriteiten' (door de minister van IenW).[14] De AED's in de sectoren 'Energie' en 'Digitale infrastructuur' vallen onder de (toezichts-) verantwoordelijkheid van de minister van EZK.
Hoe het Ministerie van EZK uitvoering heeft gegeven aan het aanwijzen van AED's beschrijven we onder vraag II.1.

Andere aangewezen vitale aanbieders

De NIB-richtlijn geeft een limitatief aantal sectoren waarbinnen AED's kunnen worden aangewezen (zie hiervoor). Nederland beschouwt echter meer sectoren als vitaal, en wijst daarbinnen de zogenoemde AAVA's aan. De AAVA's zijn ook door de verantwoordelijke ministers aangewezen in het Bbni. [15] Het gaat hier bijvoorbeeld om aanbieders van processen in de digitale infrastructuur die onderdeel zijn van de digitale gegevens-verwerking tussen overheidsorganisaties en tussen overheidsorganisaties en burgers, en die zo belangrijk zijn voor de Nederlandse samenleving dat uitval of verstoring leidt tot ernstige maatschappelijke ontwrichting en een bedreiging vormt voor de nationale veiligheid. Voorbeelden van vitale digitale voorzieningen zijn DigiD en het Handelsregister van de Kamer van Koophandel (KVK).[16] Het gaat hier dus om processen in sectoren die *niet*

[12] NIB-richtlijn art. 5 lid 1.
[13] Alle sectoren die in de bijlage worden genoemd zijn: Energie, Vervoer, Bankwezen, Infrastructuur voor de financiële markt, Gezondheidszorg, Levering en distributie van drinkwater, Digitale infrastructuur.
[14] Bbni (https://wetten.overheid.nl/BWBR0041520/2021-06-01).
[15] Staatsblad 2021 nr. 160, blz. 27.
[16] Bbni, Staatsblad 2021 nr. 160, blz. 27.

worden genoemd in bijlage II van de NIB-richtlijn. De aanwijzing van de *andere vitale aanbieders* (art. 3 Bbni) in Nederland staat los van de Europese NIB-richtlijn.[17]

DSP's

Digitaledienstverleners (Digital Service Providers/DSP's) zijn aanbieders van digitale diensten (dit zijn online marktplaatsen, zoekmachines en cloudcomputerdiensten)[18]. Lidstaten hoeven niet te achterhalen wie de individuele DSP's zijn, omdat de richtlijn van toepassing is op alle DSP's die binnen de definitie van de NIB-richtlijn vallen.[19] Aanbieders van digitale diensten worden geacht zelf te achterhalen of ze onder de NIB/Wbni vallen (zie ook § 4.1).

De NIS2-richtlijn

Op 16 december 2020 heeft de Europese Commissie (EC) het voorstel gedaan voor de vervanging van de huidige NIS-richtlijn: de NIB2/NIS2[20]. Met de invoering van NIS2 zal de EC waarschijnlijk gaan bepalen wie worden aangewezen als 'belangrijke' of 'essentiële' aanbieders. In de praktijk blijkt dat er nu soms grote verschillen bestaan tussen de verschillende lidstaten. In Nederland is bijvoorbeeld de gezondheidszorg (waaronder de ziekenhuizen) niet als vitale sector aangewezen[21], en zijn er dus geen AED's binnen deze sector aangewezen. In bijvoorbeeld België, Finland en Frankrijk is de gezondheidszorg wel als vitaal aangemerkt[22]. In de Nederlandse implementatie van de nieuwe richtlijn zal moeten worden uitgewerkt welke van deze belangrijke en essentiële aanbieders als vitaal

[17] Staatsblad 2021 nr. 160, blz. 9.
[18] NIB-richtlijn art. 5 punt 5 en 6, en bijlage III.
[19] Tweede Kamer, vergaderjaar 2017-2018, 34 883, nr. 3 (blz. 2) en de NIB-richtlijn overweging 57.
[20] Voorstel voor een RICHTLIJN VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 (https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52020PC0823&qid=1609770678546).
[21] Staatsblad 2021 160 blz. 27 en Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021 tabel a blz. 16.
[22] Onderzoek Cybersecurity voor Industrial Automation en Control Systems, Gartner, 21 augustus 2021, Uitgebracht aan het Ministerie van JenV (https://www.cybersecurityraad.nl/documenten/rapporten/2019/08/21/csr-advies-iacs---onderzoeksrapport-gartner).

worden beschouwd. 'Vitaal' is overigens een Nederlands begrip, dit volgt niet uit de NIB-richtlijn.
Het is nog niet zeker wanneer de NIS2 in werking zal treden, vooralsnog wordt uitgegaan van 2024.[23]

Nederland heeft een fiche[24] opgesteld voor de NIS2 en stelt hierin een aantal kritische kanttekeningen bij het voorstel van de EC, waar we in deze nota van bevindingen verder niet inhoudelijk op ingaan.

Samengevat
De Wbni geldt voor vitale dienstverleners (AED's, AAVA's) en DSP's. De AED's zijn aanbieders van vitale diensten in de sectoren die worden genoemd in de NIB-richtlijn. Bij de AAVA's gaat het om sectoren die niet worden genoemd in de NIB-richtlijn. De AED's en de AAVA's worden aangewezen in het Bbni. De DSP's worden niet individueel aangewezen.

3.2 Rechten en plichten van aanbieders (vraag I.2)

Onderzoeksvraag

- Wat zijn de rechten en plichten van de aanbieders die onder de Wbni vallen?

Bevindingen
Dienstverleners die onder de Wbni vallen hebben een 'meldplicht' voor incidenten en een 'zorgplicht' om incidenten te voorkomen.[25] Daarnaast hebben ze recht op ondersteuning hierbij van het Nationaal Cyber Security Centrum (NCSC). In het Bbni is nader uitgewerkt welke beveiligings-maatregelen door deze dienstverleners moeten worden genomen (de zorgplicht) en welke incidenten gemeld moeten worden (de meldplicht).

[23] Zie Offerte Agentschap Telecom Toezichtstaken 2022, blz. 24.
[24] Tweede Kamer, vergaderjaar 2020–2021, 22 112, nr. 3053.
[25] NIB-richtlijn art. 14 en § 2 en § 3 van de Wbni.

Voor sommige typen aanbieders geldt alleen de meldplicht en voor andere aanbieders geldt zowel de meldplicht als de zorgplicht (zie hierna).

Meldplicht

Het NCSC is op grond van de Wbni als Computer Security Incident Response Team (CSIRT) aangewezen voor AED's en AAVA's[26]. Dit betekent dat organisaties in vitale sectoren verplicht zijn om ernstige digitale veiligheidsincidenten op het terrein van cybersecurity te melden bij het NCSC.

AED's moeten op grond van de Wbni de volgende incidenten melden[27]:

- Incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende dienst (meldplicht bij het NCSC en bij AT);
- Inbreuken op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kunnen hebben ('bijna-ongelukken') voor de continuïteit van de verleende dienst (alleen meldplicht bij het NCSC, niet bij AT).

De AAVA's moeten de hiervoor genoemde incidenten alleen melden bij het NCSC, niet bij AT.[28]

Voor DSP's is er een aparte CSIRT: het CSIRT-DSP, onderdeel van het Ministerie van EZK[29]. Bij DSP's kan er sprake zijn van een vrijwillige of een verplichte melding. In het geval er sprake is van een verplichte melding moet het incident ook gemeld worden bij AT.[30] Voor de verplichte meldingen stelt de minister van EZK de melddrempels vast (zie § 4.2).

[26] https://www.ncsc.nl/over-ncsc/wettelijke-taak (geraadpleegd 16 augustus 2021) en Staatsblad 2018 nr. 388 (o.a. blz. 18).
[27] Zie art. 10 van de Wbni.
[28] Zie art. 10 van de Wbni.
[29] https://www.agentschaptelecom.nl/actueel/nieuws/2019/01/21/csirt-beschikbaar en https://www.csirtdsp.nl/.
[30] https://www.csirtdsp.nl/hoe-kunt-u-melden en Wbni art. 10 en 16.

Zorgplicht

AED's en DSP's hebben naast de *meldplicht* voor incidenten op grond van de Wbni ook een *zorgplicht*[31]. Die zorgplicht betekent samengevat dat de aanbieders passende maatregelen moeten nemen om risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen, om incidenten te voorkomen en om de gevolgen van eventuele incidenten zoveel mogelijk te beperken. Voor AAVA's geldt deze zorgplicht niet.

Rechten van aanbieders

Vitale aanbieders (AED's en AAVA's) en DSP's hebben recht op: [32]

- Bijstand van het CSIRT bij het treffen van maatregelen om de continuïteit van hun dienst te waarborgen en te herstellen bij incidenten;
- Verstrekking van vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten door het CSIRT.

De bijstand die het CSIRT biedt valt buiten de scope van ons onderzoek.

Samengevat

AED's en DSP's hebben een zorgplicht, en ze hebben een meldplicht bij de sectorale toezichthouder en het NCSC respectievelijk het CSIRT-DSP's.
AAVA's hebben een meldplicht bij het NCSC. AAVA's hebben geen zorgplicht op grond van de Wbni en ook geen meldplicht bij de sectorale toezichthouder, deze houdt dan ook geen toezicht op de AAVA's.
Alle vitale aanbieders kunnen voor advies en ondersteuning een beroep doen op het NCSC. DSP's kunnen hiervoor terecht bij het CSIRT-DSP's.

[31] Wbni art. 7 en 8.
[32] Wbni art 3 lid 1 en https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/vitale-aanbieders en https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/voor-wie-geldt-de-wbni/digitale-dienstverleners (geraadpleegd 16 augustus 2021).

3.3 Betrokken actoren bij (toezicht op) de Wbni (vraag I.3)

Onderzoeksvraag

- Welke actoren zijn betrokken bij het toezicht op de Wbni?

Bevindingen

Coördinatie totstandkoming en uitvoering Wbni

Er zijn vele actoren betrokken bij de weerbaarheid van de vitale infrastructuur: de aanbieders zelf, de verantwoordelijke vakdepartementen en de veiligheidsregio's. De minister van Justitie en Veiligheid (JenV) is verantwoordelijk voor de coördinatie van de totstandkoming en uitvoering van de Wbni.

Aanwijzing vitale aanbieders door vakdepartementen

De vakdepartementen zijn primair verantwoordelijk voor de vraag welke aanbieders beschouwd moeten worden als vitaal. De meeste vitale aanbieders worden in of op grond van het Bbni aangewezen als aanbieder van een essentiële dienst (AED) of als aanbieder van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving (AAVA). Vitale aanbieders worden door het vakdepartement hierover geïnformeerd.[33] (zie ook § 3.1 over de aanwijzing van AED's en AAVA's)

Toezicht op de Wbni door EZK

De minister van EZK is in de Wbni aangewezen als 'bevoegde autoriteit' voor de vitale sectoren Energie en Digitale infrastructuur, en voor de digitaledienstverleners. Dat betekent dat de minister van EZK voor deze sectoren en dienstverleners verantwoordelijk is voor het monitoren van de toepassing van de NIB-richtlijn op nationaal niveau. De minister van EZK heeft Agentschap Telecom aangewezen als toezichthouder op de

[33] Zie https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen.

Wbni voor de sectoren energie, digitale infrastructuur en voor digitale diensten.[34]

Melding en monitoring van incidenten

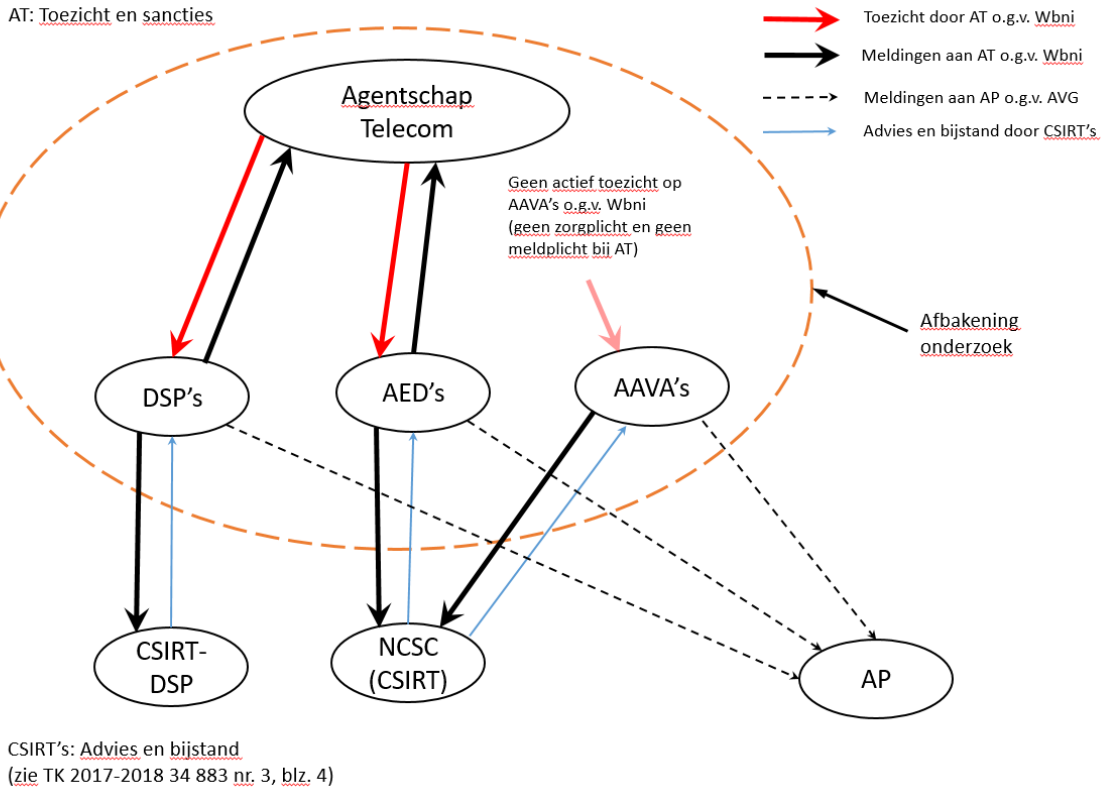
Als er sprake is van een dreiging of een incident in netwerk- en informatiesystemen van vitale aanbieders, van onderdelen van het Rijk of van digitaledienstverleners, dan zijn er computercrisisteams die hulp kunnen verlenen. In de Wbni wordt zo'n team een Computer Security Incident Response Team (CSIRT) genoemd. Het Nationaal Cyber Security Centrum (NCSC, onderdeel van het Ministerie van JenV) is in de Wbni aangewezen als CSIRT voor de AED's en AAVA's[35]. Daarnaast moeten AED's de incidenten ook melden bij hun sectorale toezichthouder, in het geval van EZK is dat AT. DSP's moeten incidenten melden bij AT en bij het CSIRT-DSP[36], dat onder het Ministerie van EZK valt. DSP's hoeven incidenten niet bij het NCSC te melden. Er is een scheiding tussen toezicht en sancties (door de toezichthouders) en advies en bijstand (door de CSIRT's).[37]

De Autoriteit Persoonsgegevens (AP) is ook een van de betrokken toezichthouders, maar neemt een relatief bijzondere positie in ten opzichte van de toezichthouders op de Wbni. De AP houdt namelijk op grond van de Algemene Verordening Gegevensbescherming (AVG) toezicht op álle organisaties, publiek of privaat, die persoonsgegevens verwerken. Onder deze organisaties vallen ook de vitale aanbieders, voor zover zij hierbij persoonsgegevens verwerken.

In figuur 1 staat een schema met de belangrijkste actoren binnen de scope van ons onderzoek. Er is voor het toezicht een overlap tussen de Wbni en de Telecommunicatiewet, dit beschrijven we in § 4.5.

[34] Staatscourant 2018 nr. 63334 7 november 2018 (https://wetten.overheid.nl/BWBR0041524/2018-11-09).
[35] Zie Staatsblad 2018 388 (blz. 6).
[36] https://www.agentschaptelecom.nl/actueel/nieuws/2019/01/21/csirt-beschikbaar en https://www.csirtdsp.nl/.
[37] Tweede Kamer, vergaderjaar 2017–2018, 34 883, nr. 3, blz. 4.

Figuur 1: Betrokken actoren bij het toezicht op de Wbni



In bijlage 4 hebben we een totaaloverzicht opgenomen van de vitale processen in Nederland met hun toezichthouders.

Samengevat

De minister van JenV is verantwoordelijk voor de coördinatie van de totstandkoming en uitvoering van de Wbni. De vakdepartementen zijn primair verantwoordelijk voor de vraag welke aanbieders beschouwd moeten worden als vitaal en informeren deze aanbieders ook hierover. De verantwoordelijke ministers wijzen toezichthouders aan voor het toezicht op de Wbni. Naast het toezicht door de toezichthouders is er ook sprake van ondersteuning en advies door de CSIRT’s.

3.4 Taken en bevoegdheden van de toezichthouders (vraag I.4)

Onderzoeksvraag

- Wat zijn de taken en bevoegdheden van de toezichthouders op de Wbni (bijvoorbeeld audits, handhaving etc.)?

Bevindingen

De minister van EZK is in de Wbni (art. 4) aangewezen als 'bevoegde autoriteit' voor de sectoren Energie en Digitale infrastructuur. De toezichtswerkzaamheden die volgen uit de Wbni heeft EZK gemandateerd aan AT.[38] AT is een rijksinspectie en werkt binnen de kaders van aanwijzingen inzake de rijksinspecties.[39]

De bevoegdheden van de toezichthouder(s) met betrekking tot de Wbni zijn vastgelegd in hoofdstuk 6 'Handhaving' van de Wbni. De toezichthouder kan een aanbieder bijvoorbeeld de verplichting opleggen om door een onafhankelijke deskundige te laten vaststellen of aan de zorgplicht is voldaan (Wbni art. 26). Verder is vastgelegd dat er bestuurlijke boetes kunnen worden opgelegd bij overtreding van de Wbni, en wat de maximale hoogtes van deze boetes zijn (Wbni art. 29). [40]

Samengevat

AT is door de minister van EZK aangewezen als toezichthouder op de Wbni. De benodigde bevoegdheden voor de handhaving zijn vastgelegd in de Wbni en in de Mandaatregeling van EZK.

[38] art. 25 Wbni en Besluit mandaat, volmacht en machtiging EZK 2019 (onder XVII 2g), https://wetten.overheid.nl/BWBR0041776/2019-01-01.
[39] Uit mail van AT d.d. 12 oktober 2021, https://wetten.overheid.nl/BWBR0037073/2022-01-01.
[40] Zie ook: https://www.nctv.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/wie-doet-wat/bevoegde-autoriteiten.

4 Opzet van het toezicht op de Wbni

In dit hoofdstuk beschrijven we hoe het toezicht door AT ingevolge de Wbni is georganiseerd. We beantwoorden hiermee onze onderzoeksvragen II.1 t/m II.8:

1. Op welke wijze voeren AT en EZK de risicoanalyse en prioritering uit voor het toezicht op de Wbni en hoe leggen ze dit vast?
2. Welke normen worden gehanteerd door AT, en door wie worden deze normen vastgesteld?
3. Hoe wordt vastgesteld of vitale aanbieders alle incidenten melden die gemeld zouden moeten worden?
4. Hoe wordt beoordeeld of door de aanbieders aan de zorgplicht is voldaan?
5. In hoeverre er overlap is met andere wet- en regelgeving op dit beleidsterrein en hoe wordt hiermee omgegaan? (bijvoorbeeld overlap met de Telecommunicatiewet en de Algemene verordening gegevensbescherming)
6. Op welke wijze wordt door AT samengewerkt en kennis gedeeld met andere toezichthouders?
7. In hoeverre slaagt de AT er in om voldoende gekwalificeerd personeel vrij te maken voor de toezichthoudende taak?
8. Wat zijn de eerste resultaten van het toezicht na de inwerkingtreding van de Wbni?

4.1 Risicoanalyse en prioritering (vraag II.1)

Onderzoeksvraag

- Op welke wijze voeren AT en EZK de risicoanalyse en prioritering uit voor het toezicht op de Wbni en hoe leggen ze dit vast?

Bevindingen

Aanwijzing en risicoanalyse AED's

Het aanwijzen van de AED's gebeurt onder verantwoordelijkheid van de minister van EZK bij het DG Bedrijfsleven en Innovatie / Directie Digitale Economie. Voor de beoordeling of er sprake is van een 'essentiële dienst' bevat de *NIS directive* criteria (zie art. 5.2 en 6.1 NIS), zoals '*een entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten*'. Verder moet er een afhankelijkheid bestaan van netwerk- en informatiesystemen en zou een incident aanzienlijke verstorende effecten hebben voor de verlening van de dienst. Voor het bepalen van het verstorend effect moeten de lidstaten onder andere rekening houden met het aantal gebruikers, het marktaandeel van die entiteit en de gevolgen die incidenten kunnen hebben voor economische en maatschappelijke activiteiten of de openbare veiligheid. EZK voert hiervoor per sector een risicoanalyse uit. EZK gebruikt voor deze risicoanalyse geen vast format of procedure, maar bepaalt per sector welke analyses nodig zijn. EZK had bijvoorbeeld wat minder zicht op de datacenters en heeft daar daarom extern onderzoek[41] naar laten uitvoeren.

De lijst met aangewezen AED's wordt periodiek door EZK geëvalueerd en geactualiseerd.[42] Afgelopen zomer (2021) zijn bijvoorbeeld de energie-producenten als AED aangewezen. EZK stelde daarvoor een lijst op van producenten die onder toezicht zouden worden gesteld en kondigde dat aan in een brief naar de producenten. AT heeft een kopie van deze brieven ontvangen, ten behoeve van het toezicht dat AT moet houden op deze producenten.[43] AT voert na zo'n aanwijzing door EZK een risicoanalyse uit op de ondertoezichtgestelde partijen (OTG's) en stelt de prioriteiten in het toezicht.

[41] Bijlage bij Tweede Kamer, vergaderjaar 2020–2021, 26 643, nr. 772.
[42] Zie bijvoorbeeld Staatsblad 160 20.
[43] Zie brief d.d. 25 oktober 2018 aan netbeheerders en overzicht AED's (ontvangen van AT).

AT heeft ook een signalerende functie naar EZK, zo heeft AT de risico’s gesignaleerd die spelen bij de laadpaaldienstverlening, en hierbij ook suggesties gedaan voor mogelijke oplossingsrichtingen.[44]

Naast de ‘reguliere’ inspecties voert AT ook thematische onderzoeken uit, om een diepgaand beeld van een bepaald onderdeel van de informatiebeveiliging van de essentiële dienst van de AED te verkrijgen. Op basis van een risicomodel wordt bepaald welke onderwerpen in de jaarlijkse thematische onderzoeken aan de orde komen. AT verzamelt hiervoor interne en externe risicofactoren (de Dreigingsmonitor) en verwerkt deze in een risicomatrix. Uit de risicomatrix wordt vervolgens bepaald wat de mogelijke thema inspecties voor het komende jaar kunnen zijn. Het risicomodel wordt door de betrokken specialistische inspecteurs als input gebruikt voor het bepalen van relevante onderwerpen voor de thematische onderzoeken. Het gaat hier om een kwalitatieve risicoanalyse waar volgens AT gebruik van ‘gezond verstand’ en vakkundige oordeelsvorming een belangrijke rol spelen.
Voor de AED’s stelt AT per sector een overkoepelende risicoanalyse op ten behoeve van het toezicht. Op basis van dit overkoepelende beeld worden de algemene onderwerpen voor het komende jaar geselecteerd. Dit kan vervolgens worden aangevuld met AED-specifieke risico's.

De Algemene Rekenkamer heeft voorbeelden van risicoanalyses ontvangen die zijn uitgevoerd volgens de hiervoor beschreven systematiek. Ook is de werking hiervan door medewerkers van AT toegelicht aan de hand van dossiers[45].

[44] Zie brief 21 januari 2021 van AT aan EZK, kenmerk AT-EZK/8139488.
[45] Werkbezoek aan AT d.d. 26 januari 2022.

Aanwijzing en risicoanalyse AAVA's

De minister die eerstverantwoordelijk is voor een digitale voorziening beoordeelt of deze voorziening moet worden beschouwd als een 'andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving'.[46] Het aanwijzen van de AAVA's op het beleidsterrein van EZK gebeurt, net als de aanwijzing van de AED's, bij het DG Bedrijfsleven en Innovatie / Directie Digitale Economie. Voor het Ministerie van EZK zijn de KVK (voor het Handelsregister) en 'vitale telecomaanbieders'[47] aangewezen als AAVA's. Deze aanbieders hebben op grond van de Wbni/het Bbni een meldplicht bij het NCSC voor incidenten.

AAVA's vallen niet onder het Wbni-toezicht van AT. Bij sommige AAVA's is er echter wel toezicht op grond van andere wet- en regelgeving:

- De zorgplicht, de meldplicht en het toezicht door AT voor telecomaanbieders volgt uit de Telecommunicatiewet. Voor de (vitale) telecomaanbieders geldt er daarmee een zorgplicht, een meldplicht en een toezichtsregime dat vergelijkbaar is met dat van de Wbni. De Telecommunicatiewet geldt overigens voor alle telecomaanbieders; deze wet maakt geen onderscheid tussen vitaal en niet-vitaal.
- Voor de KVK is er geen zorgplicht en geen meldplicht bij AT op grond van de Wbni, en dit is ook niet in andere wet- en regelgeving geregeld. AT houdt dus geen toezicht op de KVK. De KVK is een Zelfstandig bestuursorgaan (zbo) en een Rechtspersoon met een wettelijke taak (rwt). Vanuit die hoedanigheid houdt het Ministerie van EZK toezicht op de KVK. Het Ministerie van EZK geeft aan dat er sinds kort een nieuwe afdeling eigenaarsadvisering is gestart bij FEZ, waarbij ook aandacht is voor IT en cybersecurity. Er vinden volgens EZK reguliere gesprekken plaats tussen de pSG (eigenaar) en het hoofd van dienst van de KVK. Als daar aanleiding toe is, wordt cybersecurity daar

[46] Zie Staatsblad 2021 160 blz. 27, Wbni art. 5, eerste lid onder b en Bbni art. 3.
[47] Een aanbieder van een elektronisch communicatienetwerk of een elektronische communicatiedienst die een netwerk of infrastructuur beheert dat of die direct of indirect wordt gebruikt ten behoeve van het verlenen van een telefoon-, sms- of internettoegangsdienst aan minimaal 1.000.000 eindgebruikers (art. 3 Bbni).

geagendeerd. Daarnaast zijn er 2 keer per jaar gesprekken tussen de Chief Information Security Officer (CISO) EZK en de CISO KVK. Ook neemt de CISO KVK regelmatig deel aan het Integraal Beveiligings-platform, een gremium voor alle CISO's en beveiligingscoördinatoren binnen de ministeries van EZK en LNV. Verder is een traject opgestart om ook één keer per jaar een reguliere rapportage van de KVK aan de CISO van EZK in te stellen over cybersecurity en privacy.[48] Deze rapportages zijn nu nog niet opgesteld.

De minister van EZK heeft, als eerstverantwoordelijke voor het Handelsregister, geoordeeld dat dit proces moet worden aangemerkt als 'andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving'. Echter de sector 'Digitale overheidsprocessen' valt onder de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Dit betekent dat het Handelsregister *als vitaal proces* onder de verantwoordelijkheid van de minister van BZK valt. Voor de Digitale overheidsprocessen is nog geen toezichthouder aangewezen als het gaat om het toezicht op de cybersecurity (zie bijlage 4). In Nederland wordt overwogen de Wbni te wijzigen, zodat er geen verschil meer zit tussen de plichten van AED's en AAVA's. Met dat traject was in juni 2021 nog niet begonnen.[49] De verantwoordelijkheid voor dit wetswijzigingstraject Wbni ligt bij het Ministerie van JenV. AT liet ons weten dat op ambtelijk niveau inmiddels voorbereidingen worden getroffen voor deze wetswijziging.[50] Als deze wetswijziging een feit is zal er een toezichthouder moeten worden aangewezen voor de Digtale overheidsprocessen, waaronder het Handelsregister.

[48] Samengevat uit mail van EZK d.d. 31 januari 2022.
[49] Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021, blz. 14 en 41.
[50] Zie mail van AT d.d. 17 februari 2022.

Aanwijzing van Digitaledienstverleners

DSP's hoeven niet individueel te worden aangewezen door de lidstaten.[51] DSP's in Nederland moeten met behulp van een 'beslisboom Digitale Diensten'[52] zelf checken of ze onder de Wbni vallen.

Voor de DSP's wordt vanwege de ex post aanpak (incident gedreven) door AT geen risicomodel toegepast. AT onderneemt wel actie om DSP's zoveel mogelijk bewust te maken van het feit dat ze in bepaalde gevallen een meldplicht en een zorgplicht hebben. Hiertoe worden door AT de DSP-doelgroepen in kaart gebracht en worden Communicatieprogramma's opgesteld voor het communiceren van de verwachtingen van AT naar de DSP's. Met het NCSC worden afspraken gemaakt om bij incidenten bij DSP's hun te wijzen op de Wbni-meldplicht voor DSP's.

Toezichtsregime voor de verschillende aanbieders

Zoals in de NIB-richtlijn is voorgeschreven houdt AT *reactief* toezicht op de DSP's. Inspecties vinden dan plaats op basis van signalen en incidenten. [53] AED's vallen onder een *actief* toezichtbeleid van AT. Dat betekent dat er geplande inspecties plaatsvinden die zijn gericht op opzet, bestaan en werking van het risicomanagementproces en het treffen van passende beheersings-maatregelen.

Rolverdeling EZK-AT bij de prioritering in het toezicht

De aanwijzing inzake de rijksinspecties biedt handvatten om de relatie tussen departement en inspecties vorm te geven. AT gaat als inspectie zelf over prioritering. AT legt het Jaarwerkplan toezicht voor aan de beleidsdirectie. Die kan hierop reageren. AT kan de reacties betrekken in het definitieve jaarwerkplan. De aanwijzingen inzake de Rijksinspecties bieden ook de mogelijkheid aan een minister om specifiek aandacht te

[51] Zie NIB-richtlijn overweging 57.
[52] https://www.agentschaptelecom.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen.
[53] https://www.agentschaptelecom.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/documenten/videos/2019/05/15/video-wbni en overweging 60 van de NIB-richtlijn.

vragen voor bepaalde onderwerpen, bijvoorbeeld ransomware. Op basis van de informele contacten weet AT meestal al wat er speelt en wat de risico's zijn. Al die inzichten worden meegenomen in de afwegingen die AT maakt om haar toezichtactiviteiten te programmeren.[54] Het toezichtsplan wordt aan de Tweede Kamer toegezonden. De verantwoording aan EZK gebeurt via een jaarrapportage.

Samengevat

Het aanwijzen van de AED's in de sectoren 'Energie' en 'Digitale infrastructuur' gebeurt door de betrokken beleidsdirectie bij EZK onder verantwoordelijkheid van de minister van EZK. Dit gebeurt op basis van een risicoanalyse. Voor deze risicoanalyse is geen vast format of procedure, EZK bepaalt per sector welke analyses nodig zijn. De lijst met aangewezen AED's wordt periodiek door EZK geëvalueerd en geactualiseerd. De door EZK aangewezen AED's vallen onder een *actief* toezichtbeleid van AT. Dat betekent dat er geplande inspecties plaatsvinden die zijn gericht op opzet, bestaan en werking van het risicomanagementproces en het treffen van passende beheersings-maatregelen.

Zoals in de NIB-richtlijn is voorgeschreven houdt AT *reactief* toezicht op de DSP's. Inspecties vinden dan plaats op basis van signalen en incidenten. AT onderneemt wel actie om DSP's zoveel mogelijk bewust te maken van het feit dat ze in bepaalde gevallen een meldplicht en een zorgplicht hebben. AAVA's op het beleidsterrein van EZK worden onder verantwoordelijkheid van de minister van EZK aangewezen. Ze hebben geen zorgplicht en meldplicht op basis van de Wbni en vallen niet onder het toezicht van AT. In sommige gevallen is er wel zorgplicht en meldplicht voor incidenten op basis van andere wetgeving.

[54] Gesprek met AT d.d. 22 december 2021.

4.2 Normen bij het toezicht (vraag II.2)

Onderzoeksvraag

- Welke normen worden gehanteerd door AT, en door wie worden deze normen vastgesteld?

Bevindingen

Normen voor de zorgplicht

De normen voor de zorgplicht liggen vast in artikel 7 en 8 de Wbni. De Wbni stelt dat een AED 'passende en evenredige organisatorische en technische maatregelen' dient te treffend om de continuïteit van de dienstverlening te waarborgen. De Wbni schrijft niet exact voor welke maatregelen dit dienen te zijn. (Zie verder § 4.4 Beoordeling toereikendheid van de zorgplicht). Het afgelopen jaar (in 2021) is de zorgplicht via het Bbni nader ingevuld. Hiervoor heeft EZK tezamen met AT tekstvoorstellen gedaan om daar invulling aan te geven.

Ter uitvoering van de zorgplicht moet de AED (samengevat) ten minste de volgende maatregelen nemen[55]

1. De aanbieder werkt volgens een risicogebaseerde aanpak.
2. Organisatie van netwerk- en informatiebeveiligingsbeheer: De aanbieder heeft een informatiebeveiligingsbeleid en -strategie en past deze actief toe.
3. Incidenten voorkomen: De aanbieder heeft een gelaagde beveiligingsstrategie die is gebaseerd op de risico's die volgen uit de risicoanalyse. Wanneer hij door relevante instanties (zoals leveranciers of betrokken overheidsinstanties) geattendeerd wordt op beveiligingsadviezen en dreigingsinformatie, beoordeelt hij of aanvullende maatregelen noodzakelijk zijn om geïdentificeerde risico's te verkleinen.
4. Detectie en respons: De aanbieder heeft de beveiliging van zijn netwerk- en informatiesystemen zodanig ingericht dat hij daarmee

[55] Samengevat uit bijlage van het Bbni.

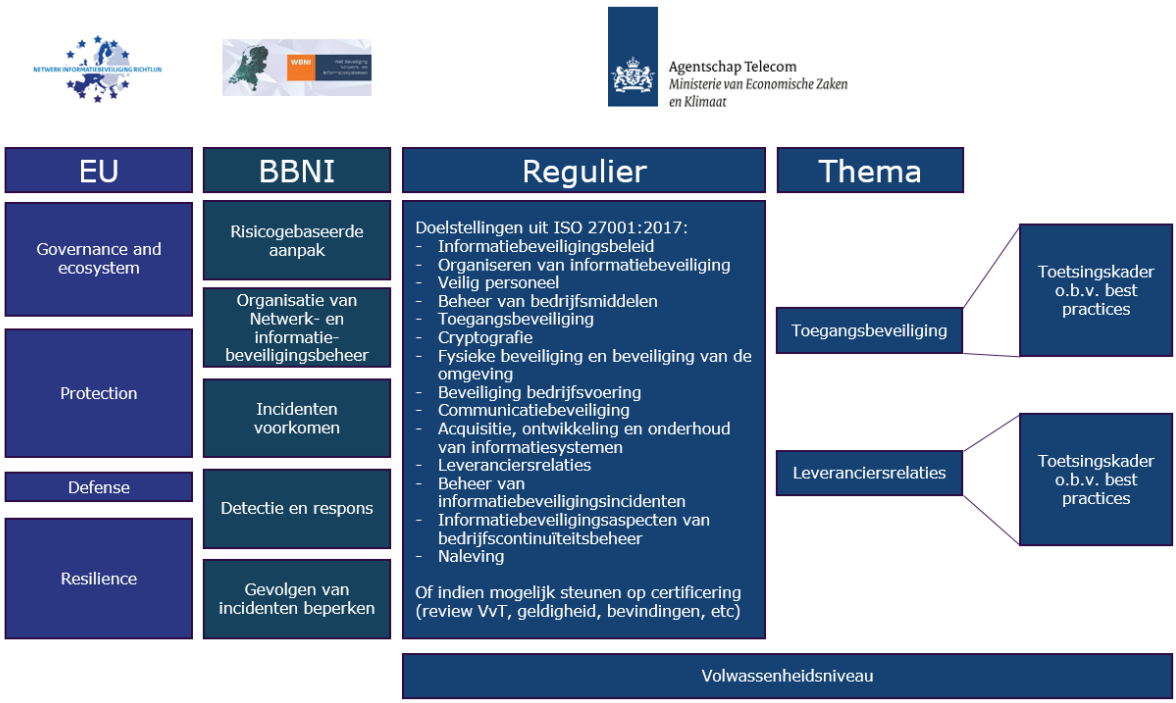
incidenten kan detecteren, analyseren en vastleggen en de gevolgen daarvan zo veel mogelijk kan beperken. Hij hanteert procedures omtrent het optreden bij incidenten.

5. Gevolgen van incidenten beperken: De aanbieder stelt een bedrijfscontinuïteitsbeleid en crisismanagementbeleid op voor de netwerk- en informatiesystemen, met in ieder geval een plan om de essentiële dienst zo spoedig mogelijk te herstellen na een incident.

Voor het toezicht op de zorgplicht hanteert AT diverse in het vakgebied erkende normen, zoals de ISO 27001 en IEC 62443[56]. AT geeft aan dat er een AT-EZK projectteam op medewerkersniveau bestaat, waarin onder meer het toezicht op de Wbni, en verschillende toekomstige acties hieromtrent, worden besproken. AT geeft in deze overleggen bijvoorbeeld reflecties op de Wbni toezichtstaak die zij uitoefenen.

[56] Internationale standaard voor informatiebeveiliging en cybersecurity. Zie ook mail van AT d.d.

AT heeft hun toezichtsmodel als volgt schematisch weergegeven:[57]



Normen voor de meldplicht

Voor de meldplicht staan in de Wbni open normen. AED’s moeten volgens de NIB en Wbni ‘incidenten met aanzienlijke gevolgen voor de continuïteit van de door hem verleende dienst’ melden bij het NCSC en de bevoegde autoriteit (AT). Om te bepalen of een incident aanzienlijke gevolgen heeft voor de continuïteit van de essentiële dienst worden in ieder geval in aanmerking genomen:[58]

- Het aantal gebruikers dat wordt getroffen;
- De duur van het incident;
- De omvang van het geografische gebied dat is getroffen.

Voorgenoemde punten worden niet verder uitgewerkt in de Wbni of het Bbni. EZK stelt voor de AED’s die onder dit ministerie vallen de

[57] Ontvangen in mail van AT d.d. 17 februari 2022.
[58] Zie Wbni art. 10.

melddrempels vast: bijvoorbeeld voor energieproducenten ligt de melddrempel op 100 megawatt[59]. Sommige buitenlandse toezichthouders hebben die drempel lager liggen, bijvoorbeeld Duitsland heeft hem op 35 megawatt. AT geeft dat soort signalen door aan EZK. Het is vervolgens aan EZK om deze drempelwaarden eventueel aan te passen. Op dit moment loopt er bij AT een project om de interventiestrategie voor de Wbni verder uit te werken.

Communicatie over de melddrempels

De aanwijzing van AED's gebeurt in het Bbni. EZK is verantwoordelijk voor dit proces. De identificatie en aanwijzing als AED gebeurt door EZK, en daar hoort een melddrempel bij. Deze informatie krijgt een AED in een brief van EZK. AT wordt hierbij betrokken en krijgt van EZK de informatie over melddrempels ten behoeve van het toezicht. De melddrempels worden ook gedeeld met het NCSC. De Algemene Rekenkamer heeft een voorbeeld ontvangen van een brief aan de netbeheerders over de aanwijzing van de netbeheerders met meer informatie over de meldplicht en de achtergrond van de Wbni.[60]

Bredere blik dan meldingen

AT is er geen voorstander van om voor inzichten alleen te focussen op de meldplicht. Daarvoor vindt AT de melddrempel te hoog en de frequentie van meldingen te laag. Voor goede inzichten en analyses vindt AT dat er een breder en representatiever veld aan data over incidenten nodig is. Voor het leereffect zou AT liever ook willen vragen om een incidentenlog, waarbij aan de organisatie wordt gevraagd welke incidenten een leereffect hebben. Dit brengt AT dan ook aan de orde tijdens de inspecties en de accountgesprekken.

[59] AT heeft ons een document gestuurd waarin de melddrempel voor de energiesector nader toegelicht wordt (1.2).
[60] Brief d.d. 25 oktober 2018 van DG Energie, Telecom & Mededinging met afschrift aan o.a. AT.

Meldplicht voor 'Bijna-ongelukken'

Aangewezen vitale aanbieders, inclusief AED's, moeten ook inbreuken melden die aanzienlijke gevolgen kúnnen hebben voor de continuïteit van vitale dienstverlening ('bijna-ongelukken'), maar dergelijke inbreuken hoeven alleen te worden gemeld bij het NCSC. Het staat aanbieders vrij om deze inbreuken op vrijwillige basis ook bij de bevoegde autoriteit te melden.[61] Dit betekent dus dat EZK/AT geen normen hoeft te hebben voor wat 'bijna-ongelukken' zijn. Het NSCS valt buiten de scope van ons onderzoek.

Samengevat

De normen voor de zorgplicht en de meldplicht liggen vast in de Wbni en het Bbni. Melddrempels worden vastgesteld door EZK, en de beleidsdirectie van EZK brengt de aanbieders op de hoogte van de melddrempels. AT houdt toezicht op basis van de vastgestelde normen. Daarnaast kijkt AT breder dan alleen het toetsen aan de normen, om een breder en representatiever beeld te hebben van het veld en om relevante ontwikkelingen naar de beleidsdirectie te kunnen signaleren ten behoeve van het beleid.

4.3 Volledigheid van de meldingen (vraag II.3)

Onderzoeksvraag

- Hoe wordt vastgesteld of vitale aanbieders alle incidenten melden die gemeld zouden moeten worden?

Bevindingen

Incidenten worden in eerste instantie gemeld bij het NCSC. Daarna moet een tweede melding worden gedaan bij AT als het incident voldoen aan de melddrempel. AT gaat als toezichthouder pas na het incident (na het

[61] Tweede Kamer, vergaderjaar 2017–2018, 34 883, nr. 3 (blz. 4).

crisisproces) kijken: Waar komt dit uit voort, wat betekent het voor de zorgplicht, en wat kan er in de toekomst beter? Dat zijn dus twee gescheiden trajecten. Er worden in principe geen meldingen gedeeld tussen de toezichthouders, behalve in uitzonderlijke gevallen waar de nationale veiligheid in het geding is (zie verder § 4.6 Samenwerking en kennisdeling toezichthouders).
Om de volledigheid van meldingen te bevorderen besteedt AT bij het toezicht aandacht aan de registratie van incidenten bij de AED's. Dit was eerder een aandachtspunt bij een van de thema-inspecties.

DSP's staan onder reactief toezicht, dus AT komt pas in actie bij een incidentmeldingen. De DSP's moeten AT dus weten te vinden. Om die reden is AT ook bezig zich bekend te maken via relevante netwerken en communiceert aan deze partijen wat AT van ze verwacht (zie ook § 4.1). AT ziet dat incidenten worden aangemeld en ziet hier ook een toename van gemelde 'incidenten' (lees: verstoringen). Deze verstoringen zijn overigens niet allemaal meldingsplichtig. Bij de DSP's zijn er ongeveer 3 incidenten per jaar.[62]
AT controleert bij vermoedens van incidenten altijd eerst of de aanbieder een DSP is of niet. Hier is een verschil tussen AED en DSP's: AT mag AED's zelf actief benaderen, voor DSP's is een aanleiding nodig.

Samengevat
Om de volledigheid van meldingen te bevorderen besteedt AT bij het toezicht aandacht aan de registratie van incidenten bij de AED's. Dit was bijvoorbeeld een aandachtspunt bij een van de thema-inspecties.
DSP's staan onder reactief toezicht, dus AT komt pas in actie bij een incidentmeldingen. AT communiceert via de relevante netwerken aan de DSP's wat er van ze wordt verwacht op dit punt.

[62] Uit gesprek met AT d.d. 2 november 2021.

4.4 Beoordeling toereikendheid van de zorgplicht (vraag II.4)

Onderzoeksvraag

- Hoe wordt beoordeeld of door de aanbieders aan de zorgplicht is voldaan?

Bevindingen

Beoordeling van de zorgplicht door AT

AT werkt in het toezicht via twee lijnen: (1) Over de breedte, door middel van zelfassessment de volwassenheid van de organisatie te toetsen, en (2) in de diepte, meer op onderwerp geselecteerd. Omdat er bij een inspectie altijd wel bevindingen zijn geeft dit volgens AT veel inzicht. Daarbij kan het soms de vraag zijn of een bevinding een overtreding is van de zorgplicht of niet. Daarover gaat AT dan in gesprek met de OTG, waarbij wordt aangegeven wat AT belangrijk vindt en waar partijen een verbeterslag kunnen maken. Dat wordt vervolgens door AT gemonitord in de accountgesprekken. Indien noodzakelijk kan AT een strengere interventiestrategie hanteren. De uiteindelijke keuze voor het soort interventie, van gesprek tot waarschuwing tot sanctie, maakt deel uit van de interventiestrategie van AT. Die wordt op dit moment ontwikkeld aan de hand van inzichten vanuit een inspectietraject in de Telecomsector, het interne AT-programma Kwaliteitstoezicht en het overkoepelend beleidskader van AT.

AT wil met het toezicht vooral aan de voorkant zitten en daarmee de incidenten voor zijn. AT voert hiertoe proactief toezicht uit: Heeft de onderzochte organisatie een goede invulling en uitvoering gegeven aan de zorgplicht? AT onderzoekt middels 'principle-based auditing' of de maatregelen om aan de zorgplicht te voldoende passend en evenredig zijn. De maatschappelijke opgave van AT is een veilig verbonden Nederland[63]. Het Wbni team vertaalt dit naar het digitaal weerbaarder

[63] https://www.agentschaptelecom.nl/over-agentschap-telecom.

maken van Nederland. Hiermee heeft volgens AT het Wbni-team/AT in feite hetzelfde doel als de AED zelf.
AT voert de inspectiewerkzaamheden op de zorgplicht risico-gebaseerd uit (regulier en thematisch), bijvoorbeeld op basis van de Dreigingsmonitor: Wat voor ontwikkelingen ziet AT op dit moment, wat voor incidenten spelen in de sector? (zie ook § 4.1) AT deed bijvoorbeeld in 2020 een thema-inspectie: 'Is de monitoring door de aanbieders/OTG's zo ingericht dat je incidenten kunt zien?' Meldingsplichtige incidenten moeten uiteraard bij AT worden gemeld. Daarnaast stuurt AT wel aan op een 'Just Culture'[64]: een partij moet open zijn over fouten om hiervan te leren. In de vertrouwensrelatie wil AT dat partijen zichzelf vrij voelen om te melden als er een incident is.

Naarmate meer inspecties worden gedaan, verwacht AT wel een minimum niveau aan volwassenheid van de organisatie[65]. Als daar dan niet aan wordt gedaan, kan AT handhavend optreden door bijvoorbeeld boetes op te leggen. Dit sluit aan op de bestaande AT-processen. Team Wbni heeft voor de Wbni nog geen ervaring met sanctioneren, aangezien hier tot op heden geen aanleiding voor is geweest. Het Wbni team heeft permanente ondersteuning uit de afdeling juridische zaken die monitoren op de vraag of dossiers 'juridisch' voldoende zijn opgezet voor een eventueel sanctietraject.[66]

AT heeft 14 incidentmeldingen ontvangen in de periode van 2019 tot en met november 2021. AT heeft naar eigen zeggen in die periode een veelvoud aan (proactieve) inspecties uitgevoerd, met de nadruk op

[64] Just Culture is een begrip uit de luchtvaart. Dit is een cultuur waarin geleerd wordt van fouten doordat mensen veilig incidenten kunnen melden. In de luchtvaart is het voorkomen van ongevallen namelijk cruciaal. (https://www.ncoi.nl/blog/techniek-en-veiligheid/just-culture-bereid-zijn-om-te-leren-van-fouten.html).
[65] Het gaat om de volwassenheidsniveaus volgens CMMI. CMMI geeft aan op welk niveau de softwareontwikkeling van een organisatie zit. Je kunt het ook de volwassenheid van de organisatie noemen. Het model onderscheidt vijf niveaus, waaronder sturing op incidenten en sturing op verbetering.
[66] Gebaseerd op gesprek met AT d.d. 2 november 2021. Tijdens het dossieronderzoek d.d. 26 januari 2022 bleek de inzet van juristen in voorkomende gevallen.

preventie. AT gebruikt daarbij een toetsingskader gebaseerd op ISO processen-risicomanagement. Dat wordt gebruikt om bij een incident door het gehele proces heen te gaan met gerichte vragen. Daarin hanteert AT 'open normen'[67] om te toetsen hoe de onderzochte partij zijn analyses uitvoert.
In hoofdstuk 5 beschrijven we hoe het toezicht door AT in de praktijk wordt uitgevoerd.

In het geval van DSP's houdt AT geen actief toezicht op de zorgplicht. Als er een incidentmelding is wordt wel gekeken in hoeverre aan de zorgplicht is voldaan en wordt de ontwikkeling gemonitord bij volgende inspecties.

Samengevat
AT voert de inspectiewerkzaamheden op de zorgplicht risico-gebaseerd uit (regulier en thematisch). Daarnaast stuurt AT wel aan op een vertrouwensrelatie waarin partijen zichzelf vrij voelen om te melden als er een incident is, om ervan te kunnen leren. Als het nodig is kan AT handhavend optreden door bijvoorbeeld boetes op te leggen. Het Wbni team heeft permanente ondersteuning uit de afdeling juridische zaken die monitoren op de vraag of dossiers 'juridisch' voldoende zijn opgezet voor een eventueel sanctietraject.
Bij DSP's wordt de zorgplicht alleen beoordeeld na een incidentmelding.

4.5 Overlap Wbni met andere regelgeving (vraag II.5)

Onderzoeksvraag

- In hoeverre er overlap is met andere wet- en regelgeving op dit beleidsterrein en hoe wordt hiermee omgegaan? (bijvoorbeeld overlap met de Telecommunicatiewet en de Algemene verordening gegevensbescherming)[68]

[67] Van AT ontvangen informatie: 1.1 Open norm toezicht flyer AT.pdf.
[68] Zie ook: Tweede Kamer, vergaderjaar 2017-2018, 34 883, nr. 3 (blz. 11).

Bevindingen

Overlap met andere wet- en regelgeving

Er is overlap in wetgeving. Een telecomaanbieder kan bijvoorbeeld ook een DSP of een AAVA zijn. AT heeft op dit moment bijvoorbeeld een incident dat wordt onderzocht door de Afdeling Toezicht-Veiligheid team Telecom Security. Afdeling Toezicht-Digitale weerbaarheid team Wbni wordt dan wel betrokken, maar is niet "in de lead".

Verder is er een overlap met de AVG. Er kan in bepaalde gevallen een meldplicht zijn op grond van de Wbni, en als er persoonsgegevens bij betrokken zijn is er tevens een meldplicht bij de AP.

Volgens AT gaat er ook een toekomstige overlap ontstaan met de *Network Code on Cybersecurity*, een Europese aanpassing van de energiewetgeving, die naast de NIB-richtlijn extra regels en taken inzake cybersecurity introduceert in de elektriciteitssector. Deze regelgeving is in korte tijd ontwikkeld en landt in Nederland via de werking van de Energiewet. Dit brengt volgens AT een grote voorbereidingsdruk met zich mee en maakt het toezicht van AT in de elektriciteitssector in de toekomst ingewikkelder vanwege de verschillende wettelijke kaders, en het feit dat sommige dienstverleners onder beide regimes kunnen vallen.[69]

Samengevat

Er is overlap tussen de Wbni en andere wet- en regelgeving. AT heeft voor de huidige situatie intern een taakverdeling hiervoor. Er wordt echter meer Europese wet- en regelgeving op het gebied van cybersecurity verwacht, die naar verwachting van AT vooral het toezicht in de elektriciteitssector ingewikkeld kan maken.

[69] Zie reactie van AT in mail d.d. 7 februari 2022.

4.6 Samenwerking en kennisdeling toezichthouders (vraag II.6)

Onderzoeksvraag

- Op welke wijze wordt door AT samengewerkt en kennis gedeeld met andere toezichthouders?

Bevindingen[70]

Meldingen

In de Wbni is er een scheiding tussen toezicht en advies/bijstand. Bij het NCSC komen meldingen binnen van incidenten en verzoeken om bijstand. Het NCSC kan de aanbieders wijzen op de meldplicht bij andere instanties (zoals de sectorale toezichthouder of de Autoriteit Persoonsgegevens), en doet dat ook. Het NCSC gaat vertrouwelijk om met meldingen, dit is vastgelegd in de Wbni. Er is wel een uitzondering op deze regeling, namelijk als de nationale veiligheid in het geding is en/of als er risico bestaat op maatschappelijke onrust. Dan heeft het NCSC de taak de melding door te geven aan de toezichthouder of betrokken minister (Wbni art. 20 lid 4). Die drempel ligt echter hoog en het is volgens het NCSC in de praktijk nog niet voorgekomen. Over de individuele meldingen is geen overleg met de toezichthouders. Er is wel een toezichthoudersoverleg op tactisch niveau.

Verschillen tussen de toezichthouders

In een gesprek met medewerkers van het NCSC en de NCTV wordt AT getypeerd als een van de voorlopers in het veld als het gaat om toezicht op de Wbni. Bij AT was al op dat terrein al relatief veel kennis aanwezig. Er waren bijvoorbeeld ook toezichthouders die eerder niet veel te maken hadden met toezicht op cybersecurity. De wijze waarop toezichthouders invulling geven aan het toezicht op de Wbni kan afhankelijk zijn van het niveau van kennis dat de toezichthouder heeft, de toezichtscultuur en het

[70] Uit gesprek met NCSC/NCTV d.d. 2 december 2021 en met AT d.d. 2 november 2021.

niveau van volwassenheid. Als er veel kennis is kan het toezicht dieper gaan dan bijvoorbeeld het werken met een checklist.

Samenwerking en kennisdeling

Op inspecteursniveau heeft AT regelmatig contact met collega's bij onder andere de ILT en de ANVS. AT vervult verder het voorzitterschap van het 'toezichthoudersoverleg cybersecurity vitale processen'[71][72]. Dit overleg is ontstaan in de periode in aanloop naar de inwerkingtreding van de Wbni en kent geen oprichtingsbesluit, maar heeft ondertussen wel een vaste status en wordt betrokken in beleidsmatige afstemmingsprocessen.
In dit toezichthoudersoverleg worden verschillende werkgroepen ingesteld. Binnenkort start bijvoorbeeld de derde 'inspectiebeeld werkgroep'. Dit algemene inspectiebeeld gaat uit van de vitale processen, en de Wbni is een van de wetten die toeziet op die vitale processen. Het *Samenhangend inspectiebeeld*[73] wordt uitgebracht namens alle betrokken toezichthouders. De Inspectie Justitie en Veiligheid coördineert dit proces, in nauwe samenwerking met AT.
AT heeft samenwerkingsovereenkomsten met ACM en AP. AT is bezig met opstellen van nieuwe overeenkomsten en het herzien van de bestaande samenwerkingsafspraken met DNB, AP en ANVS. In de offerte 2022 staat verder dat AT in samenwerking met EZK en ACM voorbereidingen treft voor de mogelijke impact van de Netwerkcode cybersecurity elektriciteit (onder andere een impactanalyse t.a.v. de capaciteit, samenwerking met ACM en de gevolgen voor de toezichtstrategie).

Samengevat

In de Wbni is er een scheiding tussen toezicht en advies/bijstand. AT houdt toezicht, en het NCSC verleent op verzoek bijstand in geval van incidenten. Het NCSC gaat vertrouwelijk om met incidentmeldingen,

[71] Met de toezichthouders AT, DNB, ANVS, AP, IJ&V, IGJ en ILT.
[72] Zie offerte AT Toezichtstaken 2022 blz. 25.
[73] Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021 (https://www.inspectie-jenv.nl/Publicaties/rapporten/2021/06/29/rapport-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2020-2021), bijlage bij Tweede Kamer, vergaderjaar 2020–2021, 26 643, nr. 769.

behalve als de nationale veiligheid in het geding is en/of als er risico bestaat op maatschappelijke onrust. Over de individuele meldingen is geen overleg tussen de toezichthouders. Er is wel een toezichthouders-overleg op tactisch niveau over de cybersecurity van vitale processen.

4.7 Beschikbaarheid expertise voor de toezichtstaak (vraag II.7)

Onderzoeksvraag

- In hoeverre slaagt AT er in om voldoende gekwalificeerd personeel vrij te maken voor de toezichthoudende taak?

Bevindingen

Mogelijke gevolgen van aanpassing van wet- en regelgeving

In § 3.1 hebben we de komende aanpassingen van de wet- en regelgeving op het gebied van de Wbni beschreven. Het is nog niet bekend wat de gevolgen hiervan zullen zijn voor de toezichtstaken van AT, maar de taken zullen waarschijnlijk wel gaan toenemen. Dit geldt zowel voor het aantal aanbieders dat onder het toezicht gaat vallen als voor de eisen die aan het toezicht worden gesteld. AT voert nu met J&V en EZK gesprekken over de mogelijke omvang en scope van de nieuwe regelgeving. Er wordt geprobeerd een inschatting te maken van wat er nodig is, bijvoorbeeld qua capaciteit. Er is nu nog geen indicatie van de sectoren en de omvang van die sectoren die onder het toezicht gaan vallen. Daar heeft AT een signaal over afgegeven naar EZK[74], zodat in er ieder geval rekening mee kan worden gehouden dat er mogelijk extra inspecteurs nodig zullen gaan zijn. AT merkt op dat hier geen oneindige stijging aan zit, je zult dus ook moeten kiezen voor een toezichtsstrategie. [75]

[74] Zie offerte Toezichtstaken 2022.

[75] Uit gesprek met AT d.d. 22 december 2021.

Mogelijke gevolgen voor de toezichtstrategie

AT brengt jaarlijks een offerte uit aan de SG van het Ministerie van EZK. Daarin staat onder andere voor de Wbni toegelicht wat de doelstelling en de activiteiten voor het komende jaar zijn. Ook wordt er een overzicht gegeven van de ontwikkelingen en trends. Voor de Wbni is voor 2022 een totaalbudget begroot van ruim 4,2 miljoen euro. Op basis van de halfjaarrapportages maken EZK en AT afspraken maken over de wijze waarop met de onder-uitputting of overschrijding van het budget wordt omgegaan. AT geeft aan dat er nu (begin 2022) voldoende capaciteit is om toezicht te houden op de Wbni, op de wijze die volgens AT toegevoegde waarde heeft (dat is principle-based, zie § 4.4). In het geval er meer toezichttaken bij zouden komen verwacht AT dat er meer inspecteurs bij moeten komen om toezicht te houden op de Wbni, of dat er andere keuzes gemaakt moeten worden in de toezichtstrategie (bijvoorbeeld meer naar 'rule-based' en/of een andere frequenties voor het uitvoeren van inspecties in combinatie met het risicoprofiel van de OTG). Dan is er minder ruimte over om met de OTG in gesprek te gaan over mogelijke verbeteringen, terwijl de huidige werkwijze juist door de OTG's als constructief wordt ervaren[76].

Omdat er nog zo veel onzeker is heeft AT nog geen specifieke scenario's ontwikkeld voor de mogelijke nieuwe toezichtstaken. AT geeft aan wel extra claims bij EZK te hebben ingediend voor de extra projectcapaciteit die nodig is om alle voorbereidende activiteiten op te zetten. Deze inzet zal volgens AT ook de scenario-inzichten moeten opleveren voor het nieuwe toezichtsveld. AT merkt in dit verband op dat het verwachtingen-management richting bestuur en politiek belangrijk is, je kunt immers niet *alles* onderzoeken en ook niet voorzien. AT geeft in hun offerte voor de toezichtstaken 2022 bijvoorbeeld aan dat er bij risicogericht toezicht altijd sprake is van een restrisico, waarbij risicoaanvaarding een belangrijk onderwerp is in de dialoog met de stakeholders. Het gaat hier volgens AT

[76] Agentschap Telecom onderzoekt SIDN | Domeinnamen | SIDN.

vooral om het besef dat hoogwaardig en diepgaand onderzoek naar de cybersecurity van een vitale organisatie veel tijd kost. In het *Samenhangend inspectiebeeld* (blz. 9) staat een vergelijkbare kanttekening:
'Een gewijzigde NIB-richtlijn zal mogelijk een substantiële impact hebben op het aantal en de omvang van de sectoren en het toezicht daarop. Extra financiële middelen zijn in dat geval noodzakelijk. Tevens neemt de aard van dreigingen en digitale risico's toe, zoals blijkt uit diverse rapportages, zoals het CSBN. Als de prioritering in beleid ten aanzien van digitalisering en cybersecurity in de komende kabinetsperiode toeneemt, zal dat, gezien de voorgaande conclusies een opdrijvend effect hebben op de verwachtingen richting toezichthouders.'

AT geeft een voorbeeld van hoe zij hun toezichtstrategie op dit moment invullen: AT kijkt naar de elektriciteitssector, en daarbinnen naar netbeheerders. Die netbeheerders moeten continue elektriciteitstransport kunnen waarborgen. Daarachter zit een maatschappelijke opgave: het net moet blijven functioneren. AT zag hier risico's die niet binnen het bereik van de verantwoordelijkheid van de netbeheerders lagen, zoals laadpalen. Die worden in zulke hoge aantallen aangesloten dat ze de balans van het elektriciteitsnet kunnen verstoren. AT signaleert dat, en geeft dit aan bij EZK.[77] EZK kan hier vervolgens over in gesprek gaan met I&W. Als AT hier straks toezicht op moet gaan houden, moet dat samen worden gedaan met de ILT. Daarvoor is het nodig om over verschillende domeinen heen het toezicht te gaan programmeren, en is het nodig om te coördineren tussen toezichthouders, wat ook weer extra capaciteit kost. [78]
De staatssecretaris van IenW geeft in antwoord op Kamervragen aan dat er overleg is tussen de ministerie van EZK en van IenW over cybersecurity

[77] Zie brief 21 januari 2021 van AT aan EZK, kenmerk AT-EZK/8139488.
[78] Uit gesprek met AT d.d. 2 november 2021.

en laadinfrastructuur, en dat ze verwacht het overleg over dit onderwerp ook de komende tijd verder te continueren.[79]

Opbouw van de toezichtstaak Wbni

AT licht toe dat het opbouwen van een toezichttaak in een 'greenfield' omgeving (een nieuwe omgeving) een complex en gelaagd traject is. Het gaat hier om:

- Een geheel nieuwe organisaties voor de toezichthouder;
- een nieuw inhoudelijk veld;
- inspecteurs met kennis van de inhoud, maar de toezichts-ervaring moet nog worden opgebouwd;
- afwezigheid van toezichtdata (die bouw je pas in de eerste jaren op door inspecties, pas daarna kun je daadwerkelijk aan goed toezichtbeleid gaan werken).

In zo'n greenfield omgeving wordt in feite elk jaar een laag extra op het toezicht opgebouwd, waardoor het toezicht rijker, gerichter en relevanter kan worden. Vooralsnog verloopt de ontwikkeling van de stappen in het Wbni-toezicht wat AT betreft naar wens: het veld is in beeld, er is kennis van het veld ontwikkeld, inspecteurs hebben ervaring opgebouwd en er is een eerste databestand opgebouwd. De eerstvolgende grote stap is om de inzichten van de afgelopen opbouwjaren te vertalen naar goede interne beleidskaders, 'de volgende laag'.

Strategisch personeelsplan

AT geeft aan dat er een grote aanzet is gemaakt met een strategisch personeelsplan. Dit is tijdelijk stopgezet toen is besloten tot een reorganisatie die op dit moment (februari 2022) nog aan de gang is. Zodra de reorganisatie is afgerond wordt dit proces weer opgepakt, in samenhang met de ontwikkelopdrachten van de nieuwe directies.

[79] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2020Z21236&did=2021D02855

Voor de benodigde capaciteit baseert AT zich op empirische gegevens van het toezicht op de Wbni en toezichtsvelden die vergelijkbaar zijn met de Wbni. AT noemt het een uitdaging om voldoende gekwalificeerd personeel te vinden. Een paar jaar geleden was dat makkelijker dan nu. AT geeft aan veel contacten te hebben met opleidingen om aandacht te vragen voor de combinatie IT + toezichten en om het toezichtsvak meer te promoten.[80]

Samengevat

AT geeft aan op dit moment voldoende capaciteit te hebben om 'principle-based' toezicht te houden op de Wbni. Er worden echter aanpassingen in de wet- en regelgeving verwacht die mogelijk zullen leiden tot meer toezichtstaken voor AT. In overleg met EZK zullen dan mogelijk keuzes moeten worden gemaakt om de toezichtstrategie aan te passen.

4.8 Eerste resultaten van het toezicht op de Wbni (vraag II.8)

Onderzoeksvraag

- Wat zijn de eerste resultaten van het toezicht na de inwerkingtreding van de Wbni?

Bevindingen

Evaluaties en rapportages over het toezichtsproces

AT geeft aan dat de thema-inspecties inmiddels zijn afgerond, dit ziet AT als een goed basisproces. Over de thema-inspecties is gerapporteerd in het *Samenhangend inspectiebeeld*. Voor AT is bijvoorbeeld gerapporteerd over de thema-inspecties 'Detectie, logging en monitoring'. In het Samenhangend Inspectiebeeld wordt beschreven dat de AED's in de sectoren Energie en Digitale Infrastructuur zich bewust zijn van het belang van preventieve en detectieve maatregelen om hun essentiële dienst te

[80] Uit gesprek met AT d.d. 22 december 2021.

beveiligen, en dat ze hiervoor passende en evenredige maatregelen hebben getroffen. Verder signaleerde AT dat de AED's de drive hebben zich steeds verder te verbeteren. Dit uitte zich onder meer in meer ISO 27001[81]-certificeringen, effectievere monitoring door het toevoegen van nieuwe risicoscenario's en het inschakelen van externe expertise.

AT evalueert met het Wbni-team elk jaar het toezichtsproces. Op basis daarvan kunnen templates en dergelijke voor de reguliere inspecties worden aangepast. AT heeft zelf ook periodieke evaluaties aan het einde van inspectierondes, om daar ook van te leren. We hebben van AT een document[82] ontvangen waarin de verschillende vormen van toezicht staan, waarin te zien is hoe en waarom AT het toezicht vormgeeft.

Focus op preventie en herstellend vermogen
AT ziet een maatschappelijke uitdaging om met risico's om te gaan. Misschien gaan incidenten in de toekomst wel vaker voorkomen, en niet alles kan worden voorkomen. Daarom moet er volgens AT aandacht zijn voor zelfredzaamheid en bedrijfscontinuïteit: Als er iets fout gaat, wat wil je dan geregeld hebben? Dus niet alleen aan de voorkant kijken, maar ook naar het herstellend vermogen.
AT stuurt met het toezicht wel op de voorkant en de preventie, maar intervenieert ook waar dat nodig is. Er wordt dus ook achteraf ingegrepen als blijkt dat er verwijtbaar iets fout is gegaan. Dit ligt in elkaars verlengde. Je bent effectiever als je stuurt op de gehele keten als toezichthouder en niet alleen 'end-of-pipe' optreedt. Ook vanuit de open norm, sturen op interventies. Dit is volgens AT heel effectief, maar moeilijk te meten (preventie-paradox). Je kunt succesvol zijn maar dat niet uit kunnen drukken in kwantiteiten. [83]

[81] ISO 27001 is een internationale standaard voor informatiebeveiliging.
[82] Document 5.3, op 1 november 2021 ontvangen van AT via Client portaal.
[83] Gesprek met AT d.d. 22 december 2021.

Informatievoorziening EZK-AT

AT legt met de jaarrapportage verantwoording af aan EZK over het gehele toezicht. Verder is er periodiek overleg tussen AT en EZK op MT-niveau. Daarin kan indien nodig ook de Wbni worden geagendeerd. AT heeft daarnaast overleggen met de pSG en de SG. Die zijn respectievelijk de eigenaar en de formele opdrachtgever voor de toezichthouder. AT speelt voor de beleidsdirectie ook een belangrijke signalerende rol; AT kan vroegtijdig signaleren hoe de wetgeving in de praktijk uitwerkt, bijvoorbeeld straks met de implementatie van de NIS2, die zal leiden tot aanpassing van de Wbni.

Samengevat

Er wordt rijksbreed gerapporteerd over de resultaten van het toezicht op de Wbni in het *Samenhangend inspectiebeeld*. Voor de AED’s die onder het toezicht van AT vallen is het beeld dat deze AED’s zich bewust zijn van het belang van de beveiliging van hun essentiële diensten, en dat er continu wordt gewerkt aan verdere verbetering. Tegelijk geeft AT aan dat het lastig is om het resultaat van het toezicht op de Wbni kwantitatief uit te drukken. AT stuurt vooral op preventie, en het effect daarvan is moeilijk te meten.

5 Praktijkcases toezicht op de Wbni

We hebben onderzocht hoe het toezicht door AT in een aantal praktijkgevallen is uitgevoerd. We hebben ons hierbij gericht op het toezicht door AT, we geven geen oordelen over de dienstverleners zelf. We beantwoorden hiermee onze onderzoeksvragen III.1 en 2.

Onderzoeksvragen

- Hoe is het toezicht in de praktijk vormgegeven bij een aantal verschillende typen aanbieders (AED's, AAVA's en digitale-dienstverleners)?
- Hoe heeft AT in de praktijk gereageerd op incidenten bij/meldingen door de verschillende typen aanbieders, bijvoorbeeld:
    - Welke acties zijn ondernomen richting de aanbieder naar aanleiding van het incident/de melding?
    - (Hoe) is met andere betrokken toezichthouders gecommuniceerd over het incident/de melding?

5.1 Toezicht in de praktijk AED's (vragen III.1 en 2)

Bevindingen

Algemeen

We hebben bij AT een aantal dossiers bekeken van inspecties die waren afgerond. Dat was nog niet voor alle AED's het geval, bijvoorbeeld voor de COVA. We hebben in de AED-dossiers voorbeelden gezien van de verslaglegging van accountgesprekken en de communicatie over incidenten.

AT heeft een mailbox waar incidentmeldingen binnenkomen. Dit gaat via een formulier dat AT online laat invullen door de meldingsplichtigen. Op basis daarvan volgt een gesprek met de meldingsplichtigen.

AT heeft een toetsingskader dat wordt gebruikt om op basis van gesprekken en documenten de gecontroleerde partij te beoordelen. Daarbij wordt geen uitspraak gedaan of iets 'goed' is of niet, maar er wordt op basis van elk onderwerpje een 'bevinding' gedaan. Op basis van de bevindingen worden met de gecontroleerde partijen 'acties' afgesproken. Als deze acties niet worden opgevolgd, nadat AT dat meermaals heeft nagevraagd, dan zal op een bepaald moment het dossier worden overgedragen aan het sanctiebureau. Soms loopt juridische zaken ook direct mee bij meldingen (zie § 4.4). De AR heeft deze werkwijze gezien in de dossiers van AT.[84]

Voorbeeld toezichtopbouw netbeheerders:[85]

- AT heeft in 2019 kennis gemaakt met de netbeheerders. Er is toen een quick scan gemaakt voor de beeldvorming. Dit was nog geen zwaar toezicht, maar om een beeld te vormen van informatie over risico's die er bij de partijen zelf aanwezig was.
- De volgende stap die AT zette was in 2020 om dieper op een onderwerp in te zoomen: detectie, monitoring en logging. AT wilde weten in hoeverre partijen bestand waren tegen bijvoorbeeld DDOS aanvallen en ransomware.
- Dit jaar (2021-2022) voert AT een reguliere inspectie uit (op basis van de ISO): een uitbreiding van de quick scan. AT wil een volwassenheids-analyse uitvoeren: op basis van vijf deelwaarnemingen zien of de self-assessment juist en volledig is uitgevoerd.

5.2 Toezicht in de praktijk AAVA's (vragen III.1 en 2)

Bevindingen

In ons projectvoorstel was opgenomen dat we ook een praktijkcasus zouden beschrijven van toezicht op een AAVA, bijvoorbeeld de KVK/het

[84] Werkbezoek d.d. 26 januari 2022.
[85] Gesprek met AT d.d. 2 november 2021.

Handelsregister. Het Handelsregister is door de minister van EZK aangemerkt als AAVA, dat wil zeggen als 'een dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving'. Het Handelsregister wordt beschouwd als 'een proces van de digitale infrastructuur die zo belangrijk is voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid'.[86] Er wordt echter geen toezicht gehouden op de KVK op basis van de Wbni (zie §4.1).

5.3 Toezicht in de praktijk DSP's (vragen III.1 en 2)

Bevindingen

DSP's staan onder reactief toezicht van AT. Als er aanleiding toe is, kan AT inspecties uitvoeren bij de DSP's. Een aanleiding is over het algemeen als er een verstoring is. Er zijn ongeveer 40 AED's en ongeveer 1000 DSP's. Daarom kan AT niet bij alle DSP's langsgaan om na te gaan hoe zij hun zorgplicht uitvoeren, daarnaast is dit vanuit de wet niet mogelijk, DSP's zijn niet individueel aangewezen (ex-post toezicht).[87]

We hebben bij AT een aantal dossiers gezien van meldingen door een DSP en de opvolging daarvan. Er was bijvoorbeeld een incidentmelding over een IT-bedrijf. Dit was geen meldingsplichting incident, maar was voor AT wel aanleiding om onderzoek te (kunnen) gaan doen naar de zorgplicht. Op basis van de bevindingen heeft AT een brief geschreven aan het bedrijf met aanbevelingen voor verbetering.

Er is ook samenwerking tussen de lidstaten als het gaat om toezicht op DSP's. Dit toezicht gebeurt in principe door 1 lidstaat, en dat is de lidstaat waar de betrokken DSP zijn hoofdvestiging heeft.[88] We hebben tijdens het

[86] Staatsblad 2021 160, blz. 27.
[87] Gesprek met AT d.d. 2 november 2021.
[88] NIB-richtlijn, overweging 64.

dossieronderzoek bij AT voorbeelden gezien van onderlinge informatie-uitwisseling. Zo is Nederland door Duitsland op de hoogte gesteld van een incident bij een DSP met een hoofdvestiging in Nederland. AT heeft op zijn beurt een melding van een incident bij een DSP doorgespeeld aan Ierland.

Bijlage 1 Afkortingen en begrippen

AAVA	Andere Aangewezen Vitale Aanbieder
AED	Aanbieder Essentiële Dienst
ANVS	Autoriteit Nucleaire Veiligheid en Stralingsbescherming
AP	Autoriteit Persoonsgegevens
AT	Agentschap Telecom
AVG	Algemene Verordening Gegevensbescherming
Bbni	Besluit beveiliging netwerk- en informatiesystemen
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CSIRT	Computer Security Incident Response Team
CSIRT-DSP	Computer Security Incident Response Team voor Digital Service Providers
DNB	De Nederlandse Bank
DSP	Digital Service Provider
EECC	Europese Elektronische Communicatie Code
EZK	Ministerie van Economische Zaken en Klimaat
IGJ	Inspectie Gezondsheidszorg en Jeugd
IJenV	Inspectie Justitie en Veiligheid
ILT	Inspectie Leefomgeving en Transport
IenW	Ministerie van Infrastructuur en Waterstaat
ISO	International Organization for Standardization
IT	Information technology
JenV	Ministerie van Justitie en Veiligheid
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NIB-richtlijn	Netwerk- en informatieveiligheid richtlijn
Wbni	Wet beveiliging netwerk- en informatiesystemen
Wgmc	Wet gegevensverwerking en meldplicht cybersecurity

Bijlage 2 Normen

Onze normen/uitgangspunten baseren we op binnen het Rijk geaccepteerde normen, zoals de Kaderstellende visie op toezicht[89]. Verder baseren we ons op de geldende wet- en regelgeving (in het bijzonder de Wbni en de Bbni). We toetsen alleen aan normen die aansluiten bij onze onderzoeksvragen.
Hierna volgt een overzicht van de normen die we in ons onderzoek gebruiken. Met 'toezichthouder' bedoelen we hier AT. Waar we spreken over 'lidstaten' kan dit gaan om de minister van EZK of om AT.

I: Risicoanalyse en prioritering

1. Toezichthouders maken in hun toezichtplannen gebruik van risicoanalyse en prioritering.
2. Toezichthouders maken hun keuzes in toezicht inzichtelijk.
3. Toezichthouders wegen kosten en baten van overheidstoezicht af en maken deze inzichtelijk.
4. Toezichthouders beschikken over capaciteit en bevoegdheden om risico's te managen en doelen te prioriteren.

II: Uitvoering en samenwerking met andere toezichthouders

1. Toezichthouders en ministeries leggen afspraken tot samenwerking vast in meerjarenplannen.
2. Toezichthouders baseren hun handhaving op de te realiseren beleidsdoelen.
3. Toezichthouders geven soort en aard van de interventie op maat vorm, evenals de grens tussen naleving stimuleren en hard ingrijpen.

[89] Kaderstellende Visie op Toezicht: Minder last, meer effect. Zes principes van goed toezicht (Tweede Kamer, vergaderjaar 2005–2006, 27 831, nr. 15).

4. Toezichthouders brengen hun gegevenshuishouding[90] in kaart, waarbij overlap met andere toezichthouders zoveel mogelijk wordt vermeden.
5. Toezichthouders stemmen hun handhavingsplannen, risicoprofielen en meerjarenplannen af op die van andere toezichthouders met dezelfde te realiseren beleidsdoelen of identieke objecten van toezicht.

III: Beleidsinformatie

1. De toezichthouder verantwoordt zich achteraf over de effectiviteit en doelmatigheid van de gemaakte keuzes en over de wijze waarop zij het afgelopen jaar heeft gefunctioneerd.

IV: Specifieke normen gebaseerd op de Wbni/Bbni

1. De lidstaten (bevoegde autoriteiten) dienden uiterlijk op 9 november 2018 de AED's te hebben aangewezen in de sectoren die zijn genoemd in bijlage II van de NIB-richtlijn. [91]
2. De lidstaten zorgen ervoor dat de bevoegde autoriteiten over de nodige bevoegdheden en middelen beschikken om de naleving van de meldplicht en zorgplicht van de aanbieders van essentiële diensten te beoordelen.[92]
3. De lidstaten zorgen ervoor dat aanbieders van essentiële diensten passende en evenredige technische en organisatorische maatregelen nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen die zij bij hun activiteiten te gebruiken te beheersen. [93]
4. Het is de verantwoordelijkheid van de AED om passende beveiligingsmaatregelen te nemen en deze maatregelen periodiek

[90] In dit deelonderzoek richten we ons hierbij met name op de meldingen van incidenten, die meestal bij meerdere toezichthouders worden gedaan.
[91] Tweede Kamer, vergaderjaar 2017-2018, 34 883, nr. 3 (blz. 2) en NIB-richtlijn artikel 5 lid 1.
[92] Afgeleid uit NIB-richtlijn artikel 15 lid 1.
[93] NIB artikel 14 lid 1.

te evalueren. Het is aan de toezichthouder om vast te stellen of de AED hiermee aan de zorgplicht voldoet. [94]

5. De lidstaten zorgen ervoor dat aanbieders van essentiële diensten incidenten met aanzienlijke gevolgen voor de continuïteit van de door hen verleende essentiële diensten onverwijld aan de bevoegde autoriteit of het CSIRT te melden. [95]

[94] Staatsblad 2021 160 (blz. 29).
[95] NIB artikel 14 lid 3.

Bijlage 3 Overzicht AED's en AAVA's

AED's die onder Wbni-toezicht van de minister van EZK/AT vallen[96]:

Als aanbieders van een essentiële dienst of categorieën van zodanige aanbieders worden aangewezen:

Sector	*Aanbieder*	*Essentiële dienst*
Energie: elektriciteit	De netbeheerder van het landelijk hoogspanningsnet, aangewezen op grond van artikel 10, tweede lid, of 14 van de Elektriciteitswet 1998	Transmissie en distributie van elektriciteit
	De regionale netbeheerders, aangewezen op grond van artikel 10, negende lid, 13, eerste lid, of 14 van de Elektriciteitswet 1998	
	BritNed Development Ltd.	Transmissie van elektriciteit (landsgrensoverschrijdend)
	Een elektriciteitsbedrijf als bedoeld in Bijlage II van de NIB-richtlijn, dat één of meerdere productie-installaties als bedoeld in artikel 1, eerste lid, onder ah, van de Elektriciteitswet 1998, beheert met een cumulatief nominaal vermogen van ten minste 100 MegaWatt	Productie van elektriciteit
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen elektriciteitsbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Levering of aankoop van elektriciteit
Energie: gas	De netbeheerder van het landelijk gastransportnet, aangewezen op grond van artikel 2, eerste lid, of 5 van de Gaswet	Transmissie en distributie van gas
	De regionale netbeheerders, aangewezen krachtens artikel 2, achtste lid, of 5 van de Gaswet	
	De Nederlandse Aardolie Maatschappij B.V.	Het opsporen en winnen van gas op basis van de concessie voor de aardgaswinning uit het Groningenveld op grond van het koninklijk besluit van 30 mei 1963, nr. 39 (Stcrt. 1963, 126) Het opslaan van gas op basis van de opslagvergunning «Norg» van 31 maart 2003 (Stcrt. 2003, 68)
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen leveringsbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Levering van gas
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen opslagsysteembeheerders, als bedoeld in Bijlage II van de NIB-richtlijn	Opslag van gas

[96] https://wetten.overheid.nl/BWBR0041520/2021-06-01 (geraadpleegd 21 februari 2022).

	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen LNG-systeembeheerders, als bedoeld in Bijlage II van de NIB-richtlijn	Het vloeibaar maken van aardgas of de invoer, de verlading en de hervergassing van LNG
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aardgasbedrijven, als bedoeld in Bijlage II van de NIB-richtlijn	Productie of aankoop van aardgas, met inbegrip van LNG
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van voorzieningen voor de raffinage en behandeling van aardgas, als bedoeld in Bijlage II van de NIB-richtlijn	Raffinage of behandeling van aardgas
Energie: aardolie	Stichting Centraal Orgaan Voorraadvorming Aardolieproducten	Het beheren van strategische olievoorraden
Energie: aardolie	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van oliepijpleidingen, als bedoeld in Bijlage II van de NIB-richtlijn	Beheer van oliepijpleidingen
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen exploitanten van voorzieningen voor de productie, opslag, transport, raffinage en behandeling van olie, bedoeld in Bijlage II van de NIB-richtlijn	Productie, opslag, transport, raffinage, of behandeling van olie
Digitale infrastructuur	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aanbieders van internetknooppunten, bedoeld in bijlage II van de NIB-richtlijn	Het faciliteren van het internet- en dataverkeer
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aanbieders van registers voor topleveldomeinnamen, als bedoeld in bijlage II van de NIB-richtlijn	Het beheren en registreren van domeinnamen onder een topleveldomein
	De bij besluit van Onze Minister van Economische Zaken en Klimaat aangewezen aanbieders van DNS-dienstverleners, als bedoeld in bijlage II van de NIB-richtlijn	Het verlenen van DNS-diensten

AT heeft ons een overzicht verstrekt van de door de minister van EZK aangewezen AED’s die onder het Wbni-toezicht van AT vallen.[97]

[97] Ontvangen van AT d.d. 1-11-2021.

Andere Aangewezen Vitale Aanbieders (AAVA’s) op het terrein van EZK zijn:

Sector	*Andere vitale aanbieder*	*Dienst*
Elektronische communicatienetwerken en -diensten/ICT	Een aanbieder van een elektronisch communicatienetwerk of een elektronische communicatiedienst die een netwerk of infrastructuur beheert dat of die direct of indirect wordt gebruikt ten behoeve van het verlenen van een telefoon-, sms- of internettoegangsdienst aan minimaal 1.000.000 eindgebruikers	Het verlenen van een telefoon-, sms- of internettoegangsdienst
Digitale overheid	De Kamer van Koophandel, bedoeld in artikel 2 van de Wet op de Kamer van Koophandel	Het handelsregister, bedoeld in artikel 2 van de Handelsregisterwet 2007

Deze aanbieders vallen niet onder het Wbni-toezicht van AT. De telecomaanbieders vallen wel onder het toezicht van AT op grond van de Telecommunicatiewet.

Bijlage 4 Toezichthouders op vitale processen

Hieronder staat een overzicht van de processen die in Nederland als vitaal beoordeeld zijn en wie de toezichthouders zijn.[98]

Vitaal proces	sector	grondslag			Toezichthouder
		NIB	Wbni		
			AED[1]	AAVA[2]	
Landelijk transport en distributie elektriciteit	Energie	*	*		AT
Regionale distributie elektriciteit	Energie	*	*		AT
Gasproductie, landelijk transport en distributie gas	Energie	*	*		AT
Regionale distributie gas	Energie	*	*		AT
Olievoorziening	Energie	*	*		AT
Internet en datadiensten	ICT/Telecom	*	*		AT
Internettoegang en dataverkeer	Digitale infra-structuur	EECC			AT
Spraakdienst en SMS	ICT/Telecom	EECC			AT
Plaats- en tijdsbepaling middels GNSS					-
Drinkwatervoorziening	Drinkwater	*	*		ILT
Keren en beheren waterkwantiteit	Water			*	- +
Vlucht- en vliegtuigafhandeling	Transport	*	*		ILT
Scheepvaartafwikkeling		*	*		ILT
Vervoer van personen en goederen over (hoofd)spoorweginfrastructuur	Transport	*			ILT++
Vervoer over (hoofd)wegennet	Transport	*			ILT++
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	Chemie				Nnb +++
Opslag, productie en verwerking nucleair materiaal	Nucleair			*	ANVS
Toonbankbetalingsverkeer	Financieel	*	*	*	DNB
Massaal giraal betalingsverkeer	Financieel	*	*	*	DNB
Hoogwaardig betalingsverkeer tussen banken	Financieel	*	*	*	DNB
Effectenverkeer	Financieel	*	*	*	DNB
Communicatie met en tussen hulpdiensten middels 112 en	OOV	EECC			AT en IJenV

[98] Bron: Samenhangend Inspectiebeeld cybersecurity vitale processen, blz. 15 Tabel a.

Inzet politie	OOV				IJenV
Basisregistraties personen en organisaties	Digitale overheids-processen				onbekend
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)					-
Elektronisch berichtenverkeer en informatieverschaffing aan burgers					-
Identificatie en authenticatie van burgers en bedrijven	Vertrouwens-diensten	eIDAS			AT
Inzet defensie	Defensie				-

[1] AED: Aanbieder Essentiële Dienst. Hiervoor geldt de Wbni-zorgplicht en -meldplicht waarop toezicht wordt gehouden.

[2] AAVA: Andere Aangewezen Vitale Aanbieder. Hiervoor geldt alleen een Wbni-meldplicht bij het NCSC en hierop wordt geen toezicht gehouden.

\+ Nog geen toezichthouder aangewezen.
++ Deze processen zijn (inmiddels) door het betrokken vakdepartement als vitaal aangemerkt; daarbinnen worden de AED’s aangewezen. Dit vindt plaats in 2021.
+++ Chemie: Omgevingsdiensten zijn toezichthouder, ILT is tweedelijns toezichthouder. Voor cybersecurity is echter (nog) geen toezichthouder aangewezen..

Geen vitaal proces in NL					
Gezondheidszorg ++++		*			IGJ

++++ De sector gezondheidszorg waar de IGJ toezicht op houdt, is wel Europees NIB-vitaal maar in het kader van de Wbni tot op heden niet vitaal verklaard en er zijn ook geen AED’s in de zorg aangewezen. Het ministerie van VWS gaat opnieuw beoordelen wat er van de zorg of delen van de zorg vitaal verklaard zal worden. Het is nu nog niet duidelijk welke consequenties dat gaat hebben voor het toezicht van de IGJ en dat van anderen als bepaalde delen van de zorg vitaal worden verklaard.

We hebben van AT per mail[99] uitleg gekregen waarom ‘Internettoegang en dataverkeer’ en ‘Spraakdienst en SMS’ wel onder de NIB staat, maar niet onder de Wbni: In Overweging 7 van de NIB-richtlijn staat dat de aanbieders van deze diensten onder de Richtlijn 2002/21/EG[100] vallen. Verder staat de KVK niet in dit overzicht als AAVA omdat dit overzicht is gebaseerd op de vitale processen zoals gedefinieerd door de NCTV.[101] Hierin wordt het Handelsregister/KVK niet genoemd.

[99] Mail van AT d.d. 22 februari 2022.
[100] Een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en –diensten.
[101] https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.

Risk based selectie

Risicomodel

Input

Interne analyse

Inventarisatie AED

Externe analyse

Dreigings monitor

Dreigingen

- Selfassesment
- Context informatie AT
- Gemelde incidenten
- Interne risico analyse AED
- Ontwikkelingen Trends
- Dreigingen
- Cyber Incidenten
- Toezicht en AT risico's

Dreigingen plotten op dreigingscategorieën bepaalt het risiconiveau (hoog/midden/laag). Kans * Impact (aanzienlijke gevolgen/ beperkte gevolgen) = Risico (groen/geel/rood)

Dreigingscategorieën		Laag	Midden	Hoog
	Beveiligingsniveau	Geringe beveiligingsissues die indirect een verhoofde kans op incidenten kunnen geven	Belangrijke beveiligingsissues die indirect een verhoogde kans	Ernstige beveiligingsissues die direct een hoge kans op incidenten geven.
	Toekomstige ontwikkelin	Speelt over 5 tot 10 jaar met lage kans op incidenten	- Speelt over 5 tot 10 jaar met hoge kans op incidenten - Speelt over 2 tot 5 jaar met middelgrote kans op incidenten - Speelt binnen 2 jaar met lage kans op incidenten	Speelt binnen 2 jaar met hoge kans op incidenten
	Incidenten: - Falen van systeem - Natuurlijke oorzaak - Menselijke fout - Falen van derde partijen (keten)	In de afgelopen 3 jaar vond er buiten Europa binnen de sector een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond binnen de sector binnen Europa een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond een van de genoemde incident bij een AED in Nederland plaats
	Incidenten en dreigingen door kwaadwillenden	Doelwit is sectoronafhankelijk Kennis/middelen zijn beperkt Activiteit is waargenomen	Doelwit is de sector binnen Europa Kennis/middelen aanwezig Activiteit is waargenomen	Doelwit is de sector in Nederland Kennis/middelen aanwezig
		Kans		
Aanzienlijke gevolgen voor de continuïteit van de levering van de essentiële diensten	Impact	Laag - Aanzienlijk (A1)	Midden - Aanzienlijk	Hoog - Aanzienlijk (A2, I1, I2)
Geen aanzienlijke gevolgen voor de continuïteit van de levering van de essentiële diensten		Laag - Laag (A3)	Midden - Laag	Hoog - Laag Rood *

- Geen Inspecties
- Meenemen in reguliere inspecties binnen 3 jaar
- Meenemen in thema inspectie/reguliere inspectie thema onderzoeken

Dreigingen koppelen aan onderwerpen

Dreigingen mappen evt. naar ISO beheerdoelen

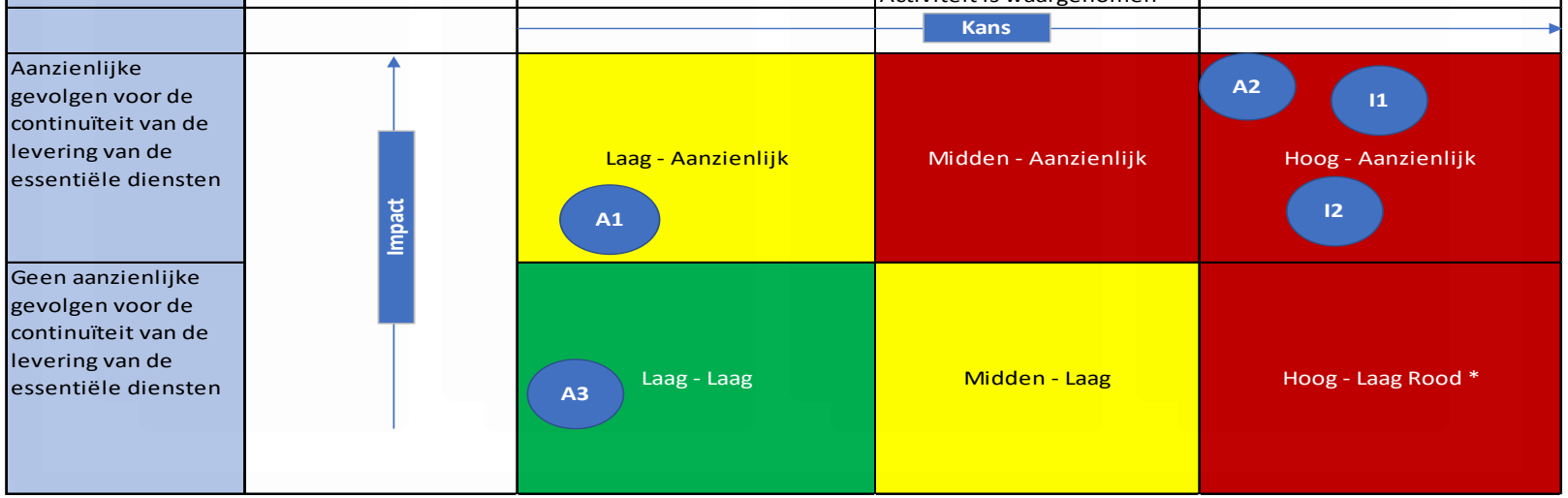
Groeperen van ISO beheerdoelen naar inspectie thema's

Output

Jaarplan thema inspecties / reguliere inspecties/ thema onderzoeken

Beveiligingsniveau		Laag	Midden	Hoog
Toekomstige ontwikkelingen		Speelt pas over 5 tot 10 jaar	Speelt over 2 tot 5 jaar	Speelt binnen 2 jaar
Incidenten: - Falen van systeem - Natuurlijke oorzaak - Menselijke fout - Falen van de derde partijen (keten)		Er vonden geen incidenten in de afgelopen 3 jaar plaats.	In de afgelopen 3 jaar vond minimaal één keer een incident buiten de sector plaats.	In de afgelopen 3 jaar vond minimaal één keer een incident bij een AED geleid plaats.
Incidenten en dreigingen door kwaadwillende		Intentie, maar geen middelen/kennis Activiteit waargenomen, middelen/kennis zijn beperkt Activiteit waargenomen, maar gericht op specifieke doelwitten	Middelen/kennis zijn aanwezig en intentie is sterk Intentie is sterk en activiteiten waargenomen	Veel middelen/kennis aanwezig en intentie is zeer sterk Intentie is zeer sterk, veel activiteit waargenomen en veel middelen/kennis aanwezig.
Aanzienlijke gevolgen voor de continuïteit van levering van de essentiële diensten		Laag – Aanzienlijk	Midden - Aanzienlijk	Hoog - Aanzienlijk
Geen aanzienlijke gevolgen voor de continuïteit van levering van de essentiële diensten		Laag – Laag	Midden - Laag	Hoog – Laag Rood*

		Laag	Midden	Hoog
	Beveiligingsniveau	Geringe beveiligingsissues die indirect een verhoofde kans op incidenten kunnen geven	Belangrijke beveiligingsissues die indirect een verhoogde kans	Ernstige beveiligingsissues die direct een hoge kans op incidenten geven.
Dreigingscategorieën	Toekomstige ontwikkelin	Speelt over 5 tot 10 jaar met lage kans op incidenten	- Speelt over 5 tot 10 jaar met hoge kans op incidenten - Speelt over 2 tot 5 jaar met middelgrote kans op incidenten - Speelt binnen 2 jaar met lage kans op incidenten	Speelt binnen 2 jaar met hoge kans op incidenten
	Incidenten: - Falen van systeem - Natuurlijke oorzaak - Menselijke fout - Falen van derde partijen (keten)	In de afgelopen 3 jaar vond er buiten Europa binnen de sector een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond binnen de sector binnen Europa een van de genoemde incidenten plaats	In de afgelopen 3 jaar vond een van de genoemde incident bij een AED in Nederland plaats
	Incidenten en dreigingen door kwaadwillenden	Doelwit is sectoronafhankelijk Kennis/middelen zijn beperkt Activiteit is waargenomen	Doelwit is de sector binnen Europa Kennis/middelen aanwezig Activiteit is waargenomen	Doelwit is de sector in Nederland Kennis/middelen aanwezig



Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Aanpak Inspectie

Opgemaakt door

Bijlagen
-

Onderwerp:	Xxx
AED/DSP:	Xxx
Contact persoon AED/DSP:	Xxx
Inspecteurs:	Xxx
Datum:	Xxx

Aanleiding & Context:
<Licht kort toe waarom deze inspectie uitgevoerd wordt>

Scope, reikwijdte en diepgang:
<Waar heeft de inspectie betrekking op>

Aanpak:
<Beschrijf de werkwijze en de hanteren beheerdoelstellingen>

Planning:
<Maak een inschatting over de benodigde uren en doorlooptijd>

Gespreksverslag

Opgemaakt door
<naam>

Bijlagen
-

Onderwerp:	Interview Incident inspectie	
AED:	<naam>	
Datum bespreking:	<datum>	
Deelnemers AED:	<naam>	RDI: <naam>
Afwezig:	<naam>	

1 Gespreksonderwerp

Interview incident inspectie.

2 Besprekingsverslag

3 Actiepunten

Incident Analyse

Onderwerp		Vragen	Toelichting	
1 Aard van het incident				
	1.1	Welke services zijn getroffen door het incident?		
	1.2	Hoe lang waren deze services niet beschikbaar?		
2 Impact van het incident (DSP criteria)				
	2.1	Hoeveel gebruikers zijn er getroffen door dit incident?		
	2.2	Was er een risico voor verlies van levens als gevolg van dit incident?		
	2.3	Was er een risico voor de openbare veiligheid, of de openbare beveiliging als gevolg van dit incident?		
	2.4	Heeft het incident geleid tot een verlies aan integriteit, authenticiteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens?		
	2.5	Heeft het incident materiële schade veroorzaakt voor een of meerdere gebruikers?		
	2.6	Zijn er van gebruikers/klanten klachten ontvangen?		
3 Oorzaak van het incident				
	3.1	Wat was de oorzaak van het incident?		
	3.2	Is er al een post incident report door de DSP opgesteld?		
	3.3	Zijn er al Post Mortem analyses ontvangen van de betrokken leveranciers?		
4 Bestrijding van het incident				
	4.1	Zijn er al maatregelen opgesteld n.a.v. dit incident?		
	4.2	Zijn deze maatregelen al (deels) geimplementeerd?		
4 Organisatie van de informatiebeveiliging				
	5.1	Welke personen zijn verantwoordelijk voor informatiebeveiliging en hoe is hun positie binnen de organisatie?		
	5.2	Is er een Information Security Management System proces binnen de organisatie geimplementeerd en wordt er een bepaald information security control framework gehanteerd?		
	5.3	Heeft de organisatie een Information Security certificering zoals ISO27001?		

Toetsingskader op basis van ISO27001					In te vullen door de inspecteur												
Onderwerp	**Subonderwerp**		**Doelstelling**	**Goodpractice (ISO27002)**	Aandachtspunten voor de inspecteur	Interview	Eigen waarneming	Beleid, procedure of instructie	Schermafdruk	Documentatie	Deelwaarneming	Interview verslag	Verslag overige evidence (eigen waarneming, beleid, procedure of instructie, schermafdruk en documentatie)	Afgerond?	Afgestemd met AED	Volwassenheid volgen inspecteur	Eventuele acties naar aanleiding van de inspectie
6.1 Risico management				**Ga bij de beoordeling van deze doelstelling ten minste in op:**													
	6.1.1	Algemeen	Bij het plannen voor het managementsysteem voor informatiebeveiliging moet in de context van de organisatie de risico's en kansen worden vastgesteld en aangepakt**.**	1. de wijze waarop cyber security maatregelen om de risico's te beperken en kansen te benutten tot stand komen (methodiek). 2. de wijze waarop de cyber security maatregelen in het bestaande risicomanagement proces zijn geïntegreerd (proces). 3. de wijze waarop de doeltreffendheid van deze cyber security maatregelen worden geëvalueerd (evaluatie).	1. Vraag na welke best practice wordt gebruikt (bv COSO) 2. Welke cyber security risico's zijn onderkend? 3. Met welke frequentie wordt het risicobeeld geactualiseerd? Opvragen laatste 3 actualisaties. 4. Opvragen beleid en procedures.											
	6.1.2	Risicobeoordeling van informatiebeveiliging	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen**.**	1. Risicocriteria voor cyber security zijn vastgesteld en worden onderhouden. 2. Risico's voor cyber security zijn onderkend en een risico eigenaar hebben. 3. Risico's voor cyber security zijn gecategoriseerd op basis van kans en impact. 4. Risico's voor cyber security zijn geprioriteerd voor risicobehandeling.	1. Risicocriteria: hoe vindt risico acceptatie plaats? 2. Risicocriteria: hoe vindt risico beoodeling plaats?											
	6.1.3	Behandeling van informatiebeveiligingsrisico's	De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen.	1. Maatregelen voor de beheersing van het risico ten aanzien van cyber security zijn vastgelegd. 2. Een behandelplan voor de beheersing van het cyber security risico is vastgelegd. 3. De risico eigenaren keuren het behandelplan goed en accepteren de restrisico's.	1. Vraag na welk systeem wordt gebruikt voor de risicobeheersing (bv Bwise)? 2. Opvragen 3 behandelplannen.											
16.1 Beheer van informatiebeveiligingsincidenten				**Ga bij de beoordeling van deze doelstelling ten minste in op:**													
	16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen	Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.	16.1.1 Verantwoordelijkheden en procedures: - verantwoordelijkheden - Is er een incidentmanagement proces geïmplementeerd en worden incidenten ook gerapporteerd? - Zijn er procedures om informatie over incidenten met aanzienlijke gevolgen naar toezichthouders en CSIRTs te communiceren (b.v. melden bij AT en CSIRT-DSP) - Zijn er crisis procedures/draaiboeken voor hoe te handelen bij incidenten met aanzienlijke impact, b.v. welke communicatiekanalen te gebruiken en welke informatie te verstrekken aan klanten en relaties betreffende oorzaak, impact voor getroffenen, workarounds, voortgang incidentonderzoek, etc.	Opvragen Incident management procedure(s) Checken of melding aan AT en andere toezichthouders is opgenomen in procedures Walkthrough van het incident waarbij gecheckt wordt of het incident conform opzet van de procedure is afgehandeld Checken of de procedure effectief is gebleken bij de afhandeling.											
				16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen: - Zijn er procedures voor het rapporteren van informatiebeveiligingsgebeurtenissen en het contactpunt waaraan de gebeurtenissen behoren te worden gerapporteerd?	Hoe verloopt de communicatie betreffende afhandeling van het incident (directie, IT beheer, etc.)? Wordt de informatie van dit incident meegenomen in trend en management rapportages?											
				16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging: - Zijn er procedures voor medewerkers betreffende het rapporteren van in systemen of diensten waargenomen of vermeende zwakke plekken in informatiebeveiliging?	Hoe lopen de rapportagelijnen voor meldingen over zwakke plekken die mogelijk tot incidenten kunnen leiden (voor zover van toepassing)?											
				16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen: - Zijn er procedures voor het classificeren en prioriteren van incidenten en het bepalen van de impact en omvang van incidenten?	Hoe ziet de escalatie procedure eruit? (op welke criteria wordt prioriteit toegekend en wordt besloten tot opschalen)											
				16.1.5 Respons op informatiebeveiligingsincidenten: - Is er vastgelegd hoe te handelen bij incidenten (melden, escalatie, containment, bewijs veiligstellen, herstel, verslaglegging, etc.)	Is het incident conform de opzet van de procedure afgehandeld? Wat is het communicatieplan i.g.v. incidenten (communicatie naar Directie, interne stakeholders, klanten)											
				16.1.6 Lering uit informatiebeveiligingsincidenten: - Wordt kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen (b.v. updaten van risico analyse)?	Worden de learnings van dit incident vertaald naar concrete verbeteringsmaatregelen? Worden de learnings van dit incident ook meegenomen in het risico management proces (evaluatie van de risicoanalyse)?											

				16.1.7 Verzamelen van bewijsmateriaal: Is er een loggingpolicy waarin is vastgelegd per systeem/applicatie welke gegevens gelogd moeten worden voor het detecteren en analyseren van incidenten? Zijn er procedures voor het identificeren en veilig stellen van incidentinformatie die als bewijs kan dienen?	Is er een procedure voor het veilig stellen van logdata, zorgen voor geldig forensisch bewijs? identificeren, verzamelen, bewaren.											
17.1	**Business Continuity Management**			**Ga bij de beoordeling van deze doelstelling ten minste in op:**												
	17.1	Informatiebeveiligingscontinuïteit	Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.	17.1.1 Plannen - Is informatiebeveiligingscontinuïteit ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie? - Worden er bedrijfsimpactanalyses uitgevoerd voor informatiebeveiligingsaspecten om de informatiebeveiligingseisen vast te stellen die van toepassing zijn op ongunstige situaties?	- Is er een BCM beleid? (wie is verantwoordelijk hiervoor, welke scenario's zijn binnen scope, is ook disaster recovery onderdeel hiervan) - Zijn er BIAs uitgevoerd, raakt dit incident aan de reeds uitgevoerde BIAs											
				17.1.2 Implementeren - Is er een BCM plan opgesteld waarin de belangrijkste bedrijfsprocessen zijn geidentificeerd (middels BIA's) en waarvoor de eisen voor continuïteit (RTO/RPO) zijn vastgesteld? - Is in het BCM plan een crisismanagement organisatie voorzien die is voorbereid op een verstorende gebeurtenis en erop reageert met personeel dat beschikt over de nodige autoriteit, ervaring en competentie?	- Is er een BCM plan opgesteld? - Teams en capaciteiten (wie & wat) - Training medewerkers voor crisisafhandeling - Handboeken voor specifieke casussen - Communicatie naar stakeholders (prepared statements)											
				17.1.3 Verifiëren, beoordelen en evalueren - Worden onderdelen van het BCM plan regelmatig getest op het handhaven van het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie (Disaster Recovery / Uitwijktesten) en wordt het BCM plan bijgesteld op basis van de uitkomsten van deze tests ?	- BCM training en testen - Op vragen resultaten eerdere BCM testen - Updaten BCM plan aan de hand van resultaten eerdere BCM testen											
	17.2	Redundante componenten	Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.	17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten - Zijn er voor systemen en applicaties eisen voor redundantie opgesteld op basis van de beschikbaarheidseisen?	- Beleid t.a.v. redundantie (afweging tussen kosten en beschikbaarheid, risk appetite van de organisatie) - Inzicht in opzet en architectuur voor redundantie (uitwerking van beleid, redundante componenten, uitwijkfaciliteiten)										

Good practice:	1. de wijze waarop cyber security maatregelen om de risico's te beperken en kansen te benutten tot stand komen (methodiek). 2. de wijze waarop de cyber security maatregelen in het bestaande risicomanagement proces zijn geïntegreerd (proces). 3. de wijze waarop de doeltreffendheid van deze cyber security maatregelen worden geëvalueerd (evaluatie). 1. Risicocriteria voor cyber security zijn vastgesteld en worden onderhouden. 2. Risico's voor cyber security zijn onderkend en een risico eigenaar hebben. 3. Risico's voor cyber security zijn gecategoriseerd op basis van kans en impact. 4. Risico's voor cyber security zijn geprioriteerd voor risicobehandeling. 1. Maatregelen voor de beheersing van het risico ten aanzien van cyber security zijn vastgelegd. 2. Een behandelplan voor de beheersing van het cyber security risico is vastgelegd. 3. De risico eigenaren keuren het behandelplan goed en accepteren de restrisico's.
Aandachtspunten:	1. Vraag na welke best practice wordt gebruikt (bv COSO) 2. Welke cyber security risico's zijn onderkend? 3. Met welke frequentie wordt het risicobeeld geactualiseerd? Opvragen laatste 3 actualisaties. 4. Opvragen beleid en procedures. 1. Risicocriteria: hoe vindt risico acceptatie plaats? 2. Risicocriteria: hoe vindt risico beoodeling plaats? 1. Vraag na welk systeem wordt gebruikt voor de risicobeheersing (bv Bwise)? 2. Opvragen 3 behandelplannen.

Datum:		
Gesproken met:		
Inspecteurs:		

Samenvatting gesprek:		**Evidence:**		**Walkthrough:**
Bevindingen inspecteur:				

Good practice:	16.1.1 Verantwoordelijkheden en procedures: - verantwoordelijkheden - Is er een incidentmanagement proces geimplementeerd en worden incidenten ook gerapporteerd? - Zijn er procedures om informatie over incidenten met aanzienlijke gevolgen naar toezichthouders en CSIRTs te communiceren (b.v. melden bij AT en CSIRT-DSP) - Zijn er crisis procedures/draaiboeken voor hoe te handelen bij incidenten met aanzienlijke impact, b.v. welke communicatiekanalen te gebruiken en welke informatie te verstrekken aan klanten en relaties betreffende oorzaak, impact voor getroffenen, workarounds, voortgang incidentonderzoek, etc. 16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen: - Zijn er procedures voor het rapporteren van informatiebeveiligingsgebeurtenissen en het contactpunt waaraan de gebeurtenissen behoren te worden gerapporteerd? 16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging: - Zijn er procedures voor medewerkers betreffende het rapporteren van in systemen of diensten waargenomen of vermeende zwakke plekken in informatiebeveiliging? 16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen: - Zijn er procedures voor het classificeren en prioriteren van incidenten en het bepalen van de impact en omvang van incidenten? 16.1.5 Respons op informatiebeveiligingsincidenten: - Is er vastgelegd hoe te handelen bij incidenten (melden, escalatie, containment, bewijs veiligstellen, herstel, verslaglegging, etc.) 16.1.6 Lering uit informatiebeveiligingsincidenten: - Wordt kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen (b.v. updaten van risico analyse)? 16.1.7 Verzamelen van bewijsmateriaal:
Aandachtspunten:	Opvragen Incident management procedure(s) Checken of melding aan AT en andere toezichthouders is opgenomen in procedures Walkthrough van het incident waarbij gecheckt wordt of het incident conform opzet van de procedure is afgehandeld Checken of de procedure effectief is gebleken bij de afhandeling. Hoe verloopt de communicatie betreffende afhandeling van het incident (directie, IT beheer, etc.)? Wordt de informatie van dit incident meegenomen in trend en management rapportages? Hoe lopen de rapportagelijnen voor meldingen over zwakke plekken die mogelijk tot incidenten kunnen leiden (voor zover van toepassing)? Hoe ziet de escalatie procedure eruit? (op welke criteria wordt prioriteit toegekend en wordt besloten tot opschalen) Is het incident conform de opzet van de procedure afgehandeld? Wat is het communicatieplan i.g.v. incidenten (communicatie naar Directie, interne stakeholders, klanten) Worden de learnings van dit incident vertaald naar concrete verbeteringsmaatregelen? Worden de learnings van dit incident ook meegenomen in het risico management proces (evaluatie van de risicoanalyse)? Is er een procedure voor het veilig stellen van logdata, zorgen voor geldig forensisch bewijs? identificeren, verzamelen, bewaren.

Datum:			
Gesproken met:			
Inspecteurs:			

Samenvatting gesprek:		**Evidence:**		**Walkthrough:**	
Bevindingen inspecteur:					

Good practice:	17.1.1 Plannen - Is informatiebeveiligingscontinuïteit ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie? - Worden er bedrijfsimpactanalyses uitgevoerd voor informatiebeveiligingsaspecten om de informatiebeveiligingseisen vast te stellen die van toepassing zijn op ongunstige situaties? 17.1.2 Implementeren - Is er een BCM plan opgesteld waarin de belangrijkste bedrijfsprocessen zijn geidentificeerd (middels BIA's) en waarvoor de eisen voor continuïteit (RTO/RPO) zijn vastgesteld? - Is in het BCM plan een crisismanagement organisatie voorzien die is voorbereid op een verstorende gebeurtenis en erop reageert met personeel dat beschikt over de nodige autoriteit, ervaring en competentie? 17.1.3 Verifiëren, beoordelen en evalueren - Worden onderdelen van het BCM plan regelmatig getest op het handhaven van het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie (Disaster Recovery / Uitwijktesten) en wordt he 17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten - Zijn er voor systemen en applicaties eisen voor redundantie opgesteld op basis van de beschikbaarheidseisen?
Aandachtspunten:	- Is er een BCM beleid? (wie is verantwoordelijk hiervoor, welke scenario's zijn binnen scope, is ook disaster recovery onderdeel hiervan) - Zijn er BIAs uitgevoerd, raakt dit incident aan de reeds uitgevoerde BIAs - Is er een BCM plan opgesteld? - Teams en capaciteiten (wie & wat) - Training medewerkers voor crisisafhandeling - Handboeken voor specifieke casussen - Communicatie naar stakeholders (prepared statements) - BCM training en testen - Op vragen resultaten eerdere BCM testen - Updaten BCM plan aan de hand van resultaten eerdere BCM testen - Beleid t.a.v. redundantie (afweging tussen kosten en beschikbaarheid, risk appetite van de organisatie) - Inzicht in opzet en architectuur voor redundantie (uitwerking van beleid, redundante componenten, uitwijkfaciliteiten)

Datum:		
Gesproken met:		
Inspecteurs:		

Samenvatting gesprek:		**Evidence:**		**Walkthrough:**
Bevindingen inspecteur:				

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Team Wbni

Van

5.1.2.e
5.1.2.e

T

Datum
1 december 2022

Bijlagen
1: flowchart
2: versiebeheer

memo

Procesbeschrijving incident inspectie

In deze memo is het proces "incident inspectie" uitgeschreven. Dit proces is zowel van toepassing op AED's als DSP's. Om deze inspecties uit te voeren wordt gebruik gemaakt van het dummy dossier, bestaande uit:

- Dummy dossier;
- Template intake
- Template aanpak
- Template aankondiging incident inspectie;
- Template toetsingskader incident inspectie;
- Template gespreksverslag;
- Template rapport.

Overige relevantie informatie:

- Brochure Wbni – meldplicht
- Brochure Wbni – Meldplicht DSP
- Wbni mailbox (ontvangst meldingen)
- Centrale registratie meldingen van de coördinator
- https://www.agentschaptelecom.nl/documenten/formulieren/2018/november/8/melden-van-incident-onder-de-wet-beveiliging-netwerk--en-informatiediensten
- Checklist start inspectie DSP

De inspecties worden bij voorkeur door twee inspecteurs uitgevoerd: één inspecteur met auditachtergrond en de andere met een IB-achtergrond. Stem per duo af wie welke taken voor zijn rekening neemt. Meldingen dienen te allen tijde zo spoedig mogelijk te worden opgepakt en afgehandeld. In de bijlage worden de stappen grafisch weergegeven.

Definities

- Vrijwillige melding:
    - Een melding van een dreiging waarbij de OTG maatregelen heeft getroffen. Bijvoorbeeld: vanwege de LOG4J dreiging heeft een OTG haar IT en OT losgekoppeld. Deze maatregel heeft geen impact op de essentiële dienst gehad.
    - Een melding van een incident (near miss) waarbij de melddrempel niet is gehaald. Dit incident heeft dus wel impact op de essentiële dienst gehad.
- Meldplichtig incident: een incident waarbij de melddrempel is gehaald
- Signaal: een melding van een derde partij of eigen waarneming dat een OTG mogelijk niet aan de zorgplicht voldoet. Deze signalen kunnen afkomstig zijn van een derde partij of uit eigen analyse. Uit een eigen analyse kan bijvoorbeeld blijken dat een OTG meerdere keren een incident heeft gehad, waarbij de melddrempel niet is gehaald.
- Incident inspectie: een onderzoek op basis van:
    - Vrijwillige meldingen
    - Meldplichtige incidenten
    - Signalen over het mogelijk niet voldoen aan de zorgplicht
- Melding: dit betreft een:
    - Vrijwillige melding
    - Meldplichtig incident
    - Signaal over het mogelijk niet voldoen aan de zorgplicht

Scope

Binnen de scope:

- Vrijwillige meldingen
- Meldplichtig incident
- Signaal dat een OTG mogelijk niet aan de zorgplicht voldoet.

Buiten de scope:

- Vragen die via de Wbni mailbox binnenkomen.
- Crisis/uitwijktesten van OTG’s waarbij een melding bij het Wbni team wordt gemaakt.
- Nationale crisis: meerdere essentiële diensten zijn niet beschikbaar. In een dergelijke situatie kan AT vragen van andere overheidsinstanties verwachten. AT heeft geen actieve rol. Nadat de diensten weer beschikbaar zijn, onderzoekt AT de crisis als zijnde meldplichtige incidenten.

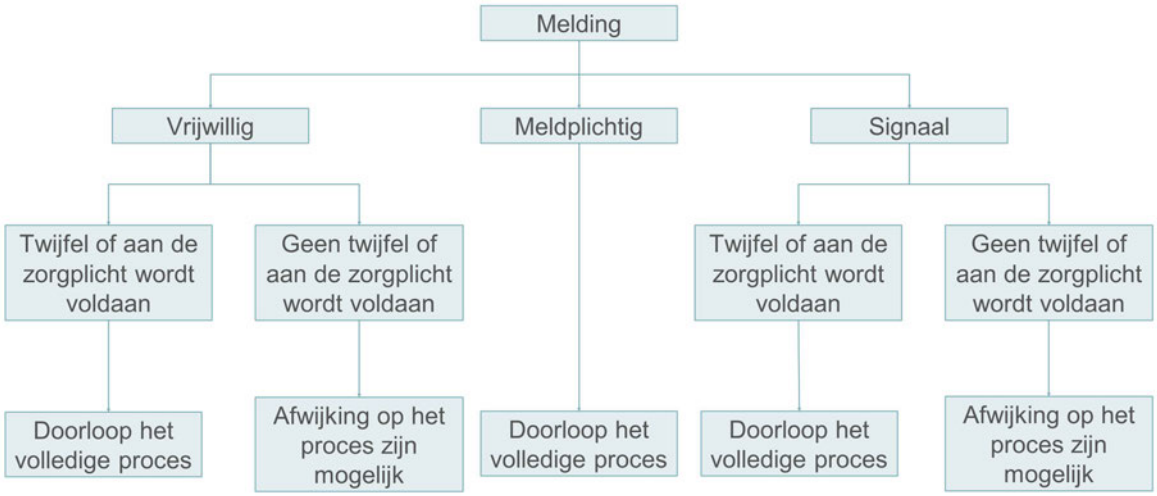
Uitgangspunten

Uitgangspunten:

- Incident inspecties voeren wij pas uit, zodra het incident en/of de acute dreiging door de OTG verholpen is.
- Wij geven nooit adviezen. Deze rol is weggelegd voor de CSIRT's (zoals NCSC).
- Voor iedere melding (vrijwillig, meldplichtig, signaal) voeren wij een intake uit. Deze intake is onderdeel van het dossier.
- Voor ieder meldplichtig incident voeren wij een incident inspectie uit. Dit houdt o.a. in dat er altijd een aankondigingsbrief en inspectie rapport wordt opgesteld.
- Voor iedere vrijwillige melding of ieder signaal maken wij een afweging of wij een incident inspectie uitvoeren of niet. De onderbouwing leggen wij vast. Mocht het leiden tot een incident inspectie dan volgt er altijd een aankondigingsbrief en een inspectie rapport en wordt het toetsingskader gebruikt.
- De aanpak van een melding kan per type verschillen. Meldplichtige meldingen dienen te allen tijde formeel te worden opgepakt. Dit wil zeggen een formele aankondiging en inspectie rapport (beiden met RP nummer en handtekening). De overige meldingen kunnen van deze formele aanpak afwijken. Dit dient echter wel te worden onderbouwt in het dossier. De mogelijkheden per type melding zijn in onderstaande tabel weergegeven.

Type melding	Intake	Uitvoeren inspectie	Beschrijven aanpak	Aankondigingsbrief	Toetsingskader	Rapport	Review
Vrijwillig	Ja	Optioneel	Ja	Optioneel	Optioneel	Optioneel	Optioneel
Meldplichtig	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Signaal	Ja	Optioneel	Ja	Optioneel	Optioneel	Optioneel	Optioneel

De volgende tabel kan helpen bij de onderbouwing van de keuzes. Met volledig proces wordt bedoelt dat alle templates worden gebruikt (aankondigingsbrief, toetsingskader, rapport en de twee review documenten).



Ontvangst melding (vrijwillig, meldplichting, signaal)
Meldingen van AED's en DSP's komen in principe binnen in de Wbni-mailbox. Indien meldingen via een andere route binnen komen (telefonisch of in persoonlijke mailboxen), dient de melder verzocht te worden om het meldformulier op de website in te vullen en deze op een veilige manier (bv infoportal) te sturen naar de Wbni-mailbox. Het klant contact centrum is op de hoogte van de werkwijze. Op deze manier hebben wij een centrale registratie van meldingen die binnen komen. De ondersteunend medewerk(st)er van het Wbni team bewaakt de Wbni-mailbox. Deze persoon informeert de contactpersonen van de OTG indien er een melding in relatie tot een AED is ontvangen. Bij een incident waar mogelijk een DSP bij betrokken is, wordt de coördinator betrokken bij de toebedeling van de melding aan een duo van inspecteurs.

Aanmaken dummy dossier
Maak een directory aan op de buiten reikwijdte[1] waar alle stukken van de inspectie worden opgeslagen. Zet in de directory een kopie van het dummy dossier[2] en pas ze aan voor de inspectie (hernoemen conform naamgevingsconventies)[3]. Let op dat de originele documenten ongewijzigd blijven. Zorg er voor dat ook de melding van het incident in het dossier is opgenomen.

[1] buiten reikwijdte
[2] buiten reikwijdte
[3] buiten reikwijdte

Intake
Niet altijd dient een AED, DSP of derde partij direct een incidentmelding in. Mogelijk start het proces met het indienen van een vraag. Om te bepalen wat voor een type (Vrijwillige melding, Meldplichtig incident, Signaal over het mogelijk niet voldoen aan de zorgplicht) melding het betreft, voer je een intake uit. Dit kan bijvoorbeeld door aanvullende vragen per mail of telefonisch te stellen. Op basis van de intake bepalen de inspecteurs het vervolgtraject.

Afronden indien er geen inspectie volgt
Indien er geen incident inspectie wordt uitgevoerd, informeer je de melder hierover en archiveer je de mails in de Wbni-mailbox en het dossier.

Verzoek om melding te maken
Indien het een meldplichtig incident betreft en er nog geen meldformulier is ingevuld, dien je de OTG te verzoeken om een formele melding in te dienen[4]. Deze situatie kan erop duiden dat er sprake is van een overtreding van de meldplicht. Afhankelijk van het geval kan het een overweging zijn om met deze overtreding iets te doen. Overleg in dit geval met de coördinator en één van de lead auditors. Daarnaast zijn de melddrempels voor DSP's complexer in de toepassing dan die voor de AED's. Gebruik de Checklist Start Inspectie DSP om na te gaan of de Melddrempel mogelijk is geraakt. Overleg bij twijfel met de coördinator.

Informeer de coördinator over de uitkomst van de intake
Informeer de coördinator over de melding die is gemaakt en hoe het vervolgtraject er uit zal zien. De coördinator zorgt voor een centraal overzicht van meldingen.

Aankondigen van incident inspectie en beschrijven aanpak
Stel op basis van de templates uit het dummy dossier de aanpak op. De aanpak hoeft niet verzonden te worden. Dit is een intern dossierstuk.

Indien een inspectie plaatsvindt op basis van het toetsingskader en indien je een formele rapportage gaat maken, stel je ook een aankondigingsbrief op. De aankondigingsbrief dient te zijn voorzien van een RP nummer en handtekening van de manager Wbni. Sla de brief op als PDF en verstuur deze naar de betreffende AED of DSP. Plaats in het dossier ook de mail waaruit blijkt dat de brief is verzonden. Tip: licht de komst van de brief eerst mondeling toe.

Een aankondigingsbrief is te allen tijde verplicht bij een meldplichtig incident. Voor overige meldingen is dit optioneel. Dit wil zeggen: als er geen toetsing op basis van een toetsingskader plaatsvindt, is een aankondiginsbrief niet nodig. Leg de onderbouwing vast in het dossier. Indien je geen aankondigingsbrief verstuurt (het betreft dus in ieder geval geen meldplichtig incident), dien je wel de OTG te informeren over de aanpak en het doel.

[4] Deze aanpak hanteren wij tot dat er een interventiestrategie beschikbaar is, waarin nader is uitgewerkt hoe we om gaan met OTG's die geen melding van een meldplichtig inc dent doen.

Uitvoeren incident inspectie
Neem contact op met de contactpersoon van de OTG om het doel van de inspectie toe te lichten. Licht het proces toe, maak werkafspraken en leg dit vast.

Doel van de incident inspectie op basis van het toetsingskader is:
- Stel vast of de OTG de oorzaak en het gevolg van het incident juist en volledig heeft onderzocht;
- Stel vast of de OTG adequate verbetermaatregelen heeft getroffen of gepland;

Concludeer of de OTG in gebreke is geweest bij het vervullen van de zorgplicht Maak een inschatting of je de kant van sanctioneren op wil. Bespreek dit met de lead auditors.

Indien bij vrijwillige meldingen of signalen geen toetsingskader wordt gebruikt, kan het doel anders zijn. Dit doel moet duidelijk terug te vinden zijn in het dossier, bijvoorbeeld in de intake of de beschrijving van de aanpak en in ieder geval bij het informeren van de OTG over de aanpak en het doel.

Leg het onderzoek vast. Het onderzoeksdossier bestaat uit evidence en afgestemde gespreksverslagen (inclusief de correspondentie over hoor en wederhoor) en een ingevuld toetsingskader (optioneel). Zorg er voor dat bevindingen te allen tijde aantoonbaar zijn afgestemd met de OTG. Maak afspraken met de OTG over eventuele acties en leg deze vast.

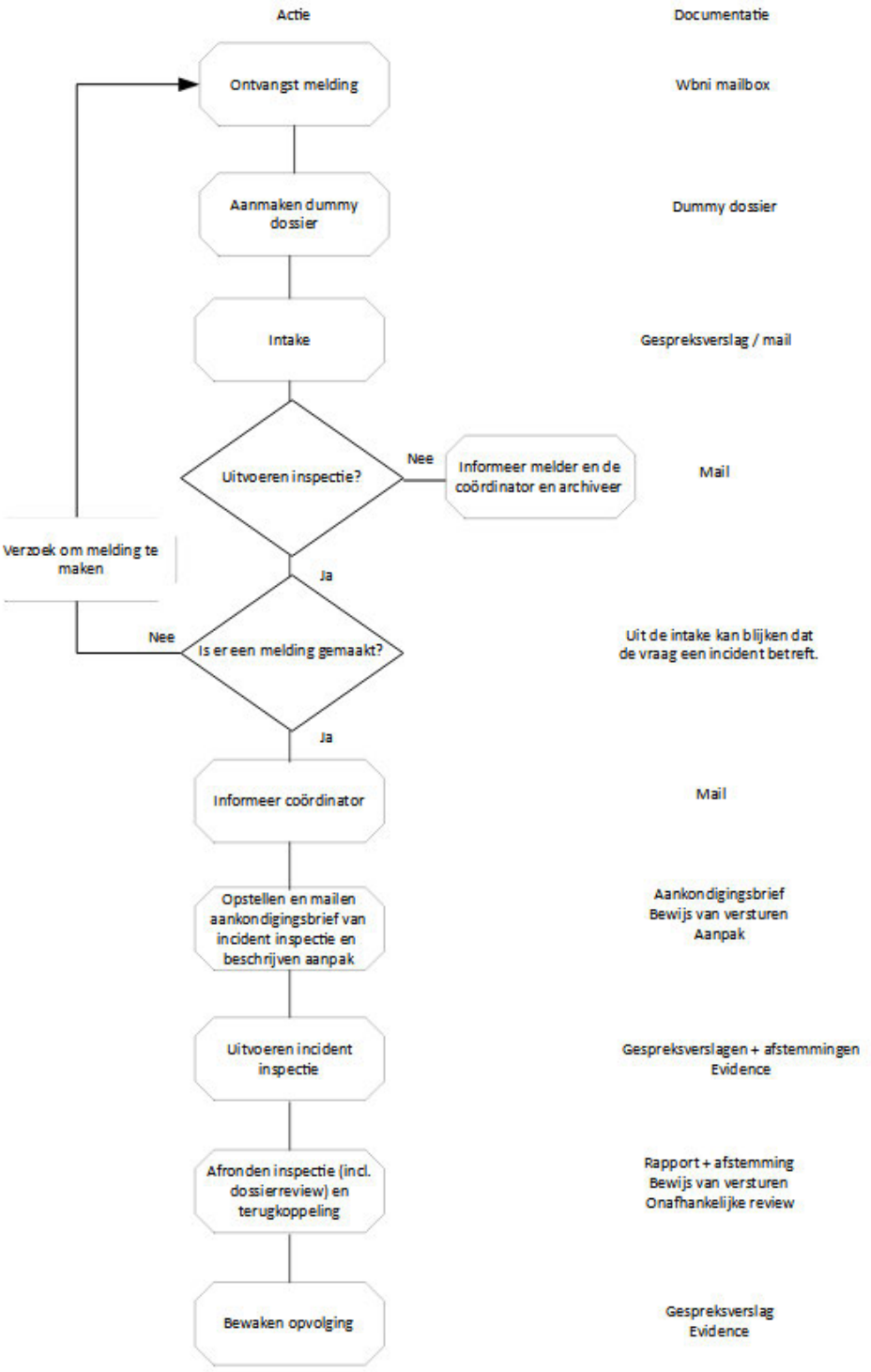
Afronden inspectie (inclusief dossierreview) en terugkoppeling
Stel op basis van de template uit het dummy dossier de eindrapportage op. Stem deze af met de OTG. Leg de afstemming vast in het dossier. Verwerk eventuele opmerkingen in een nieuwe versie.

Laat een dossierreview uitvoeren door de lead auditors. Zij kijken zowel naar de volledigheid van het dossier als de inhoud. Verwerk eventuele vragen en opmerkingen. Na goedkeuring kan je de brief laten ondertekenen door de manager Wbni via de ondersteunende medewerk(st)er. Deze rapportage dient te zijn voorzien van een RP nummer.

Sla alle afstemmingen en bewijzen van versturen documenten op in het dossier. Denk ook aan print screens inclusief datum van verzending en toelichting van via de infoportal verstuurde en ontvangen stukken.

Bewaken opvolging
Bewaak conform afspraak de opvolging van acties. Leg de opvolging vast in het dossier door middel van afgestemde gespreksverslagen en evidence. Dit kan bijvoorbeeld door een follow-up map (004 Follow-up) aan te maken in het dossier.

Bijlage: grafische weergave stappen



Bijlage: versiebeheer

Versie	Datum	Wijzigingen door	Gewijzigd
0.1	30-6-2021	5.1.2.e en 5.1.2.e	Eerste opzet
1.1	13-04-2022	5.1.2.e en 5.1.2.e	Aanpassing nav evaluatie (intake fase aangescherpt)
1.2		5.1.2.e en 5.1.2.e	Aanpassingen nav teamoverleg 4-7-2022
1.4	8-11-2022	5.1.2.e	Review eerdere aanpassingen en aanvullingen
1.5	1-12-2022	5.1.2.e en 5.1.2.e	Verwerken review opmerkingen op versies 1.2 en 1.4

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken
en Klimaat

<INSP>,<INSP>

BEVINDINGEN EN VERVOLGAANPAK
Thematische Inspectie <ONDERWERP>

<DATUM>

Agenda

Afgeronde onderwerpen

- <norm nr/hfdstuk> <norm>

Onderwerpen waarbij nadere toelichting nodig is

- <norm nr/hfdstuk> <norm>

Onderwerpen met bevindingen

- <norm nr/hfdstuk> <norm >

Reactie bevindingen en vervolgaanpak

- Reactie op bevindingen
- Acties en planning
- Vervolg

Afgeronde onderwerpen

- <norm nr/hfdstuk> <norm naam>
- <norm nr/hfdstuk> <norm naam>

Voor deze inspectie hebben we geen openstaande vragen meer op deze onderwerpen.

Onderwerpen nadere toelichting nodig

<norm nr/hoofdstuknr><norm>
Vraag 1
Vraag 2

<norm nr/hoofdstuknr><norm>
Vraag 1
Vraag 2

Bevindingen

<norm nr/hoofdstuknr><norm>

- <Punt 1>
- <Punt 2>

Feedback	
Actie:	<In te vullen door AED>
Planning:	<In te vullen door AED>

<norm nr/ hoofdstuknr><norm>

- <Punt 1>
- <Punt 2>

Feedback	
Actie:	<In te vullen door AED>
Planning:	<In te vullen door AED>

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken
en Klimaat

Vervolgstappen

1. RDI: Updaten presentatie en mailen naar <AED>
2. <AED>: Invullen feedback in presentatie en mailen naar RDI
3. RDI: Opstellen eindrapportage en mailen naar <AED>

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Bedrijfsnaam B.V.
T.a.v. de heer/mevrouw xxx
Straatnaam
Postcode Plaats

Hoofdafdeling Toezicht
Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (050) 587 74 44
www.agentschaptelecom.nl

Contactpersoon
<naam van de inspecteur>
<functie>
Toezicht Wbni
T 06-<nummer>

Datum
xx-xx-20xx

Ons kenmerk
AT-
xx-20xx-xI-x

Met opmerkingen [5.1.2.e]: Opvragen bij 5.1.2.e

Bijlagen
-

Betreft: Bevindingen inspecties xxx

Geachte heer/mevrouw

<Bedrijfsnaam> is een aangewezen aanbieder van essentiële diensten (hierna: AED) / digital service provider (hierna: DSP) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op deze wet. Op xx-xx-xxx heeft u een incident betreffende <omschrijving> gemeld. Dit incident onderzochten wij in de periode xx-xx-xxxx tot en met xx-xx-xxxx. De betreffende inspectie is aangekondigd op xx-xx-xxxx, zie onze brief met kenmerk AT-EZ/<RP2000 nummer> xx-20xx-xI-x. Hierbij rapporteren wij onze bevindingen.

Wat zijn onze bevindingen?
<Omschrijf hier de bevindingen>

Met opmerkingen [5.1.2.e]: Maak een inschatting of het sanctiebureau moet worden ingeschakeld. Dit zal het geval zijn indien er aanzienlijke risico's ten aanzien van de levering van de essentiële dienst worden geconstateerd. Het sanctiebureau kan afdwingen dat opvolging moet plaatsvinden. Neem de zorgplicht mee in je overwegen. In het geval er geen opvolging plaatsvindt, kan het sanctiebureau op later moment worden ingeschakeld.

Wat is het vervolg?
<Omschrijf hier het vervolg/eventuele afspraken>

Vragen?
Mocht u naar aanleiding van dit schrijven vragen hebben, kunt u zich wenden tot onze inspecteurs:
- de heer/mevrouw <naam> <functie> en/of
- de heer/mevrouw <naam> <functie>.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Met opmerkingen [5.1.2.e]: Stem het rapport af met 5.1.2.e of 5.1.2.e.
5.1.2.e zorgt voor een handtekening.

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

> Retouradres

Bedrijfsnaam B.V.
T.a.v. de heer/mevrouw xxx
Straatnaam
Postcode Plaats

Contactpersoon
<naam van de lead inspecteur>
<functie>
Toezicht Wbni
T 06-<nummer

Ons kenmerk
RDI-EZK/ /<RP2000
num
xx-20xx-xI-x

Met opmerkingen [5.1.2.e]: Opvragen bij 5.1.2.e

Uw kenmerk
-

Bijlagen
-

Datum <datum>
Betreft Aankondiging incident inspectie 20xx

Geachte heer/mevrouw,

<Bedrijfsnaam> is een aangewezen aanbieder van essentiële diensten (hierna: AED) / digital service provider (hierna: DSP) en valt hierdoor onder de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Agentschap Telecom (hierna: AT) is vanaf 9 november 2018 toezichthouder op deze wet. Op xx-xx-xxx heeft u een incident betreffende <omschrijving> gemeld. In dit kader kondigen wij met deze brief een inspectie naar dit incident aan.

Incident inspectie
Een incident inspectie valt onder incident gestuurd toezicht. Deze vorm van toezicht omvat het uitvoeren van onderzoeken naar aanleiding van meldingsplichtige incidenten. Dit zijn onvoorziene en niet geplande onderzoeken. De focus van deze onderzoeken ligt op de wijze waarop de onder toezichtgestelde organisatie de oorzaak en het gevolg van het incident heeft onderzocht en hoe verbetermaatregelen tot stand zijn gekomen en geïmplementeerd danwel gepland zijn. Met deze onderzoeken stimuleren wij het systeemleren en dragen we bij aan het voorkomen van toekomstige verstoringen.

Op korte termijn nemen wij contact met u op om afspraken te maken over de planning en uitvoering van de inspectie.

Vragen?
Mocht u naar aanleiding van dit schrijven vragen hebben, kunt u zich wenden tot onze inspecteurs:
- de heer/mevrouw <naam> <functie> en/of
- de heer/mevrouw <naam> <functie>.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

Met opmerkingen [5.1.2.e]: Stem het rapport af met 5.1.2.e of 5.1.2.e.
5.1.2.e zorgt voor een handtekening.

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Intake Inspectie

Opgemaakt door
<NAAM>

Bijlagen
-

Onderwerp:	Melding
OTG:	<NAAM>
Contactpersoon OTC:	<NAAM>
Contactpersoon intern:	<NAAM>
Inspecteurs:	<NAAM>
Datum:	<DATUM>

Aanleiding & Context:

<BESCHRIJF WANNEER DE MELDING IS ONTVANGEN EN WELKE STAPPEN JE HEBT ONDERNOMEN OM TE BEPALEN WELKE TYPE INCIDENT HET BETREFT. ONDERBOUW DE KEUZE VOOR HET VERVOLGTRAJECT>

Aanpak:

<BESCHRIJF HET VERVOLGTRAJECT>


Inventarisatie
Tell me / Trust me
Beeld vormen
Inspectie
Show me / prove me
Compliance
Standaard rapport
Indien ernstige bevinding overleg met 5.1.2.e
Indien nodig haken we vervolgens ATS aan
Analyse en algemene terugkoppeling
5.1.2.e
Planning algemeen en maatwerk voor uitzonderingen

Kennismakingsgesprek ENEXIS - Agentschap Telecom 02 -05-2019

Agenda

1. Voorstelrondje (Allen)
2. Introductie (AT)
3. ENEXIS Organisatie, achtergrond, visie, toekomst (ENEXIS)
4. Uitleg WBNI, toezicht en meldplicht (AT) preso en film
5. Organisatie Cybersecurity binnen ENEXIS (ENEXIS)
6. Hoe verder? (AT)

Toelichting Agendapunten:

2) Korte inleiding van Agentschap Telecom over het doel en verwachtingen van het gesprek.

3) Hierbij is Agentschap Telecom vooral geïnteresseerd om het verhaal achter ENEXIS te horen, wat zijn de onderscheidende kenmerken van ENEXIS ten opzichte van andere spelers, wat is de toekomstvisie van ENEXIS qua ontwikkelingen in de markt, internetconnectiviteit, etc. Daarnaast willen we ook graag horen hoe ENEXIS denkt over zijn rol als Aanbieder van Essentiële Diensten en wat dit betekent voor de ENEXIS organisatie.

4) Dit is een korte presentatie van onze kant over de Wbni, de doelstellingen van de wet, wat toezicht inhoudt en de rol van Agentschap Telecom.

5) Hierbij willen we graag van ENEXIS weten hoe op bestuursniveau met cybersecurity wordt omgegaan, hoe dit is vertaald naar de organisatie, etc. Het is niet de bedoeling om diep in de details te duiken, dat komt later in het toezichttraject nog wel aan bod.

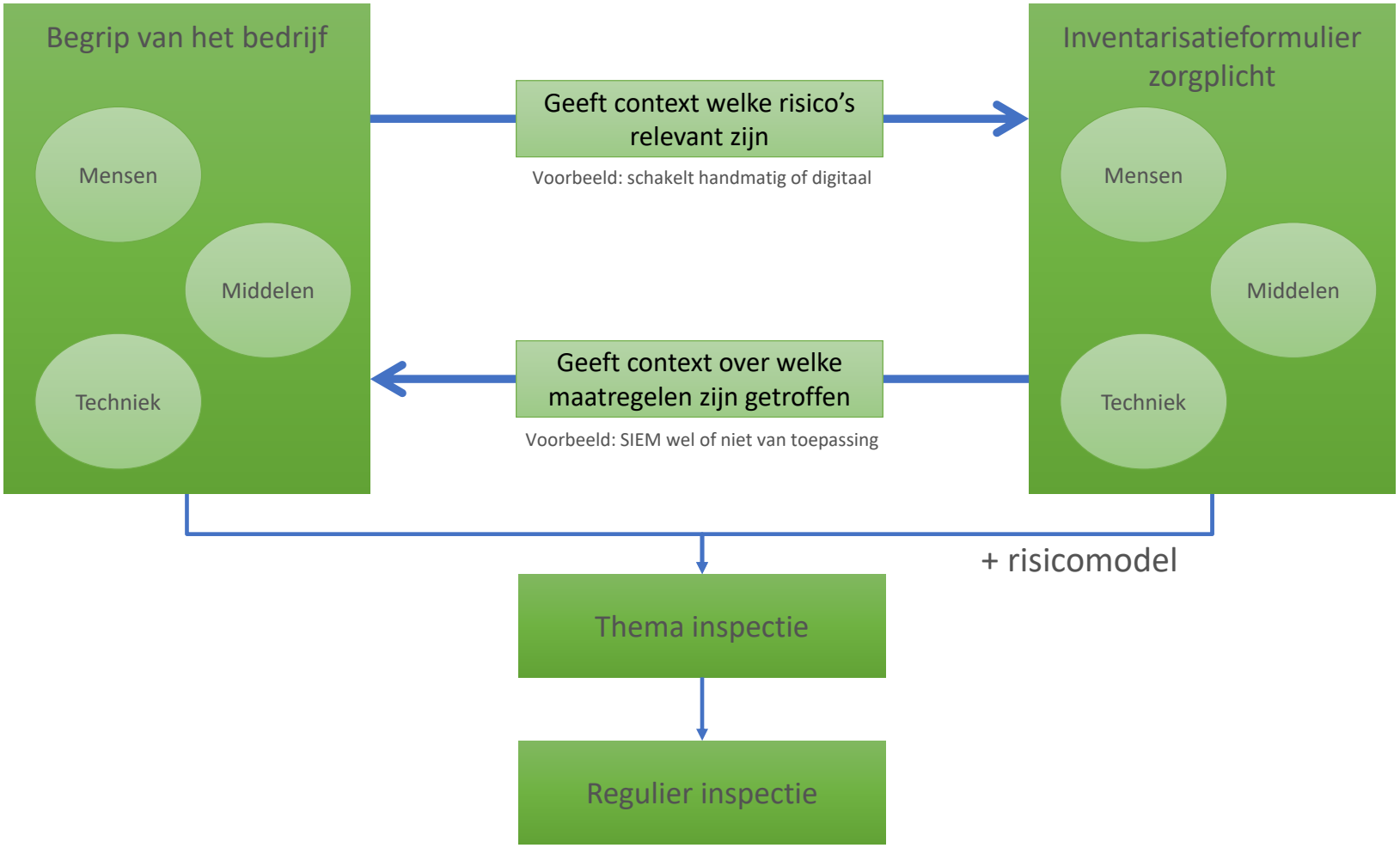
6) Ter afsluiting van het gesprek zal Agentschap Telecom inzicht geven in het verdere verloop van het toezicht traject en zullen we met elkaar afspreken hoe we verder contact houden.

Vraag	Antwoord
Kennisniveau organisatie	
Hoe vaak heeft cybersecurity op de bestuursagenda gestaan afgelopen jaar?	
Wat ziet u als het grootste cybersecurityrisico voor uw organisatie?	
Zijn er targets verbonden aan cybersecurity?	
Heeft u de informatiebijeenkomsten bijgewoond?	
Heeft u hier vragen over? (Denk aan rol van AT als toezichthouder of over toezicht in het algemeen)	
Verantwoordelijkheden	
Hoe is cybersecurity georganiseerd in uw organisatie?	
Hoe heeft u ervoor gezorgd dat de beheersing van de (bij de risicoanalyse vastgestelde) risico's zijn belegd in de organisatie?	
Is de verantwoordelijkheid voor cyberrisico's eenduidig en expliciet belegd binnen de organisatie? (Welke rollen zijn te onderscheiden, organogram etc.)	
Heeft een directielid cybersecurity in zijn portefeuille?	
Heeft de organisatie een RvC / RvT en zit daar iemand met cyberkennis?	
Heeft de organisatie een interne auditdienst, en waar is deze gepositioneerd?	
(Worden externe audits uitgevoerd?)	
(Welk normenkader wordt hiervoor gebruikt?)	
Risicomanagement	
Voert uw organisatie regelmatig corporate risicoanalyses[1] uit?	

[1] Bij kleinere organisaties zal dit niet altijd gestructureerd plaatsvinden

Wordt het onderwerp cybersecurity meegenomen in de corporate risicoanalyse?	
Wat is de 'risk appetite' van uw organisatie op het gebied van cybersecurity?	
Wat is er geïnvesteerd en georganiseerd om de risico's die uit de analyse volgen te beheersen?	
Heeft het bedrijf in beeld welke processen en systemen van vitaal belang zijn en worden deze voldoende gemonitord?	
Meldplicht	
Heeft de organisatie recent succesvol een cyberaanval afgeslagen?	
Heeft uw bedrijf een procedure voor het melden, oplossen en opvolgen van beveiligingsincidenten?	
Vervolgafspraken	
Met wie kunnen wij een vervolgafspraak maken voor het tweede gesprek?	
Wie is onze contactpersoon en kan deze ook de assessment invullen?	

Relatie instrumenten nieuwe producten met inspecties



Eerste gesprek: begrip van het bedrijf	Doel: verkrijgen globale indruk en kenmerken AED en kunnen vergelijken van lijsten van AED’s.	Werkwijze: op basis van meerkeuzevragen, bepalen welke vragen je nader toegelicht wilt krijgen (open vragen).
Tweede gesprek: inventarisatie zorgplicht	Doel: verkrijgen globale brede indruk van getroffen maatregelen en kunnen vergelijken van lijsten van AED’s.	Werkwijze: op basis van gesloten vragen, bepalen welke vragen je nader toegelicht wilt krijgen (open vragen). Het resultaat wordt meegewogen om de verdere aanpak in de vorm van thema inspecties te bepalen.

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Kennismaking
Enexis

Wet beveiliging netwerk- en informatiesystemen

16-05-2019

Onderwerpen

1. Voorstellen
2. Toezicht
3. Toezicht in de praktijk
4. Tot slot

1. Voorstellen...

Agentschap Telecom
Ministerie van Economische Zaken

Agentschap Telecom staat voor de beschikbaarheid en betrouwbaarheid van IT- en communicatie netwerken, zodat Nederland veilig verbonden is.

Video

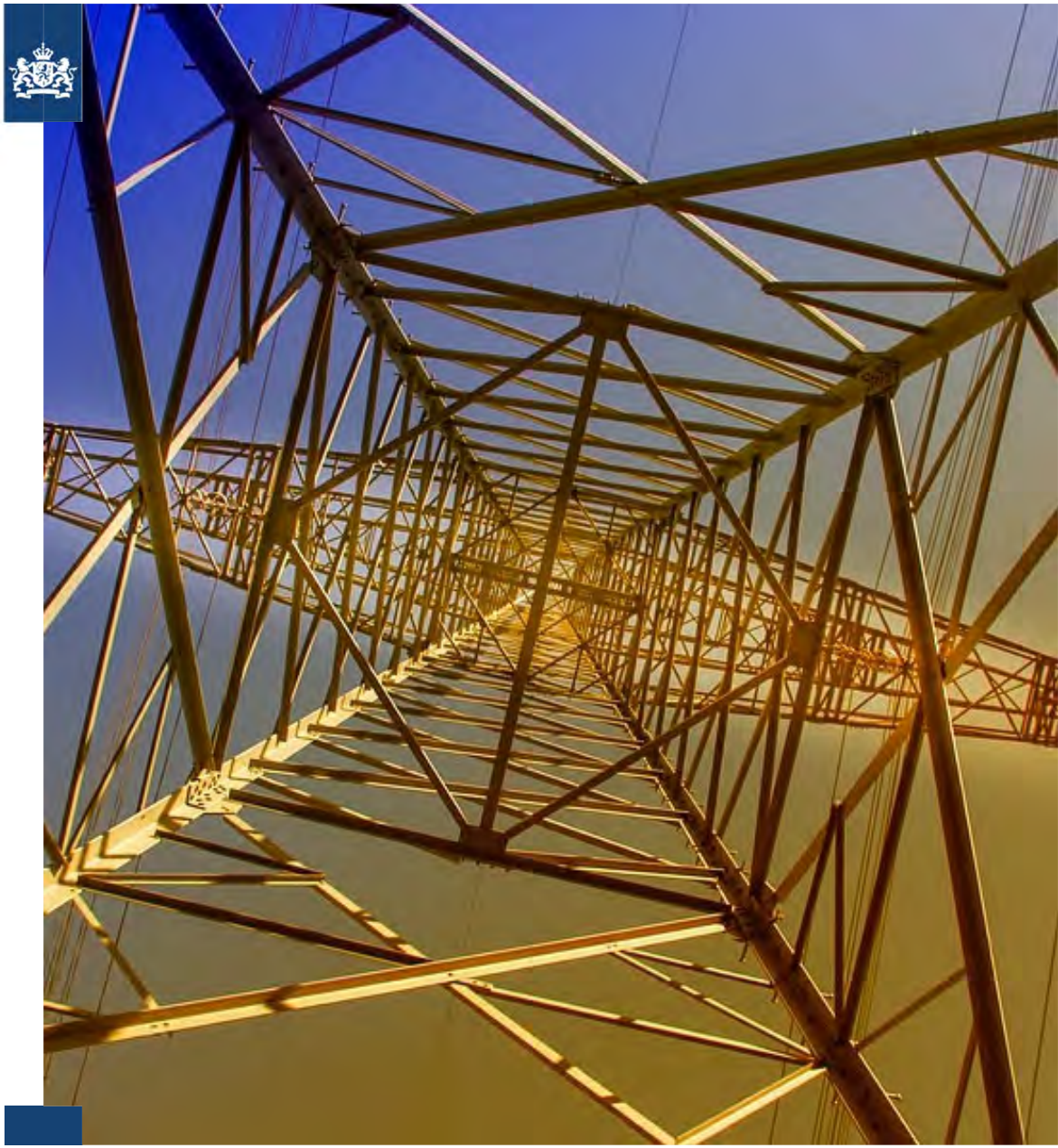
Youtube

Agentschap Telecom
Ministerie van Economische Zaken

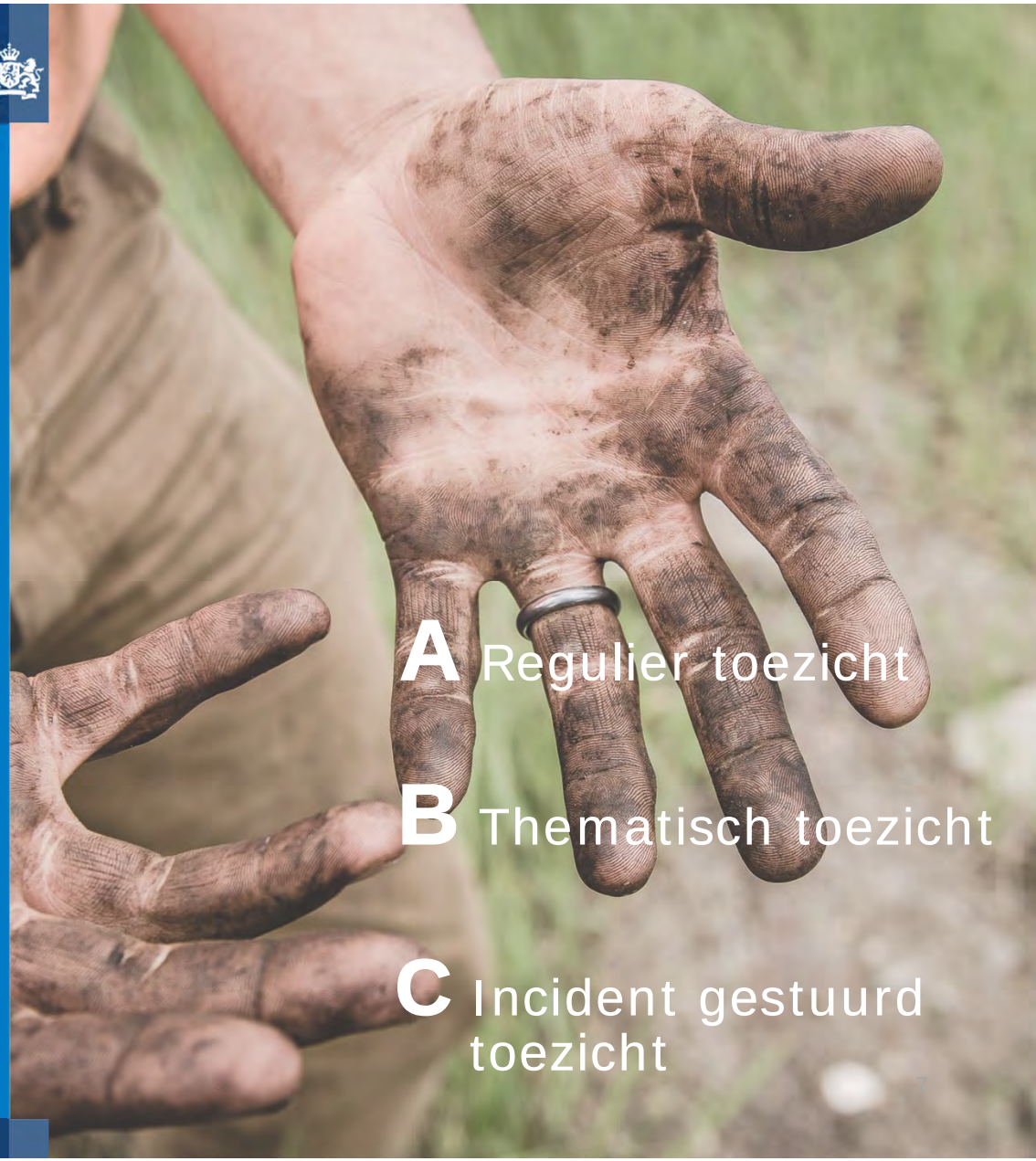
2. Toezicht

Toezicht is meer dan handhaven

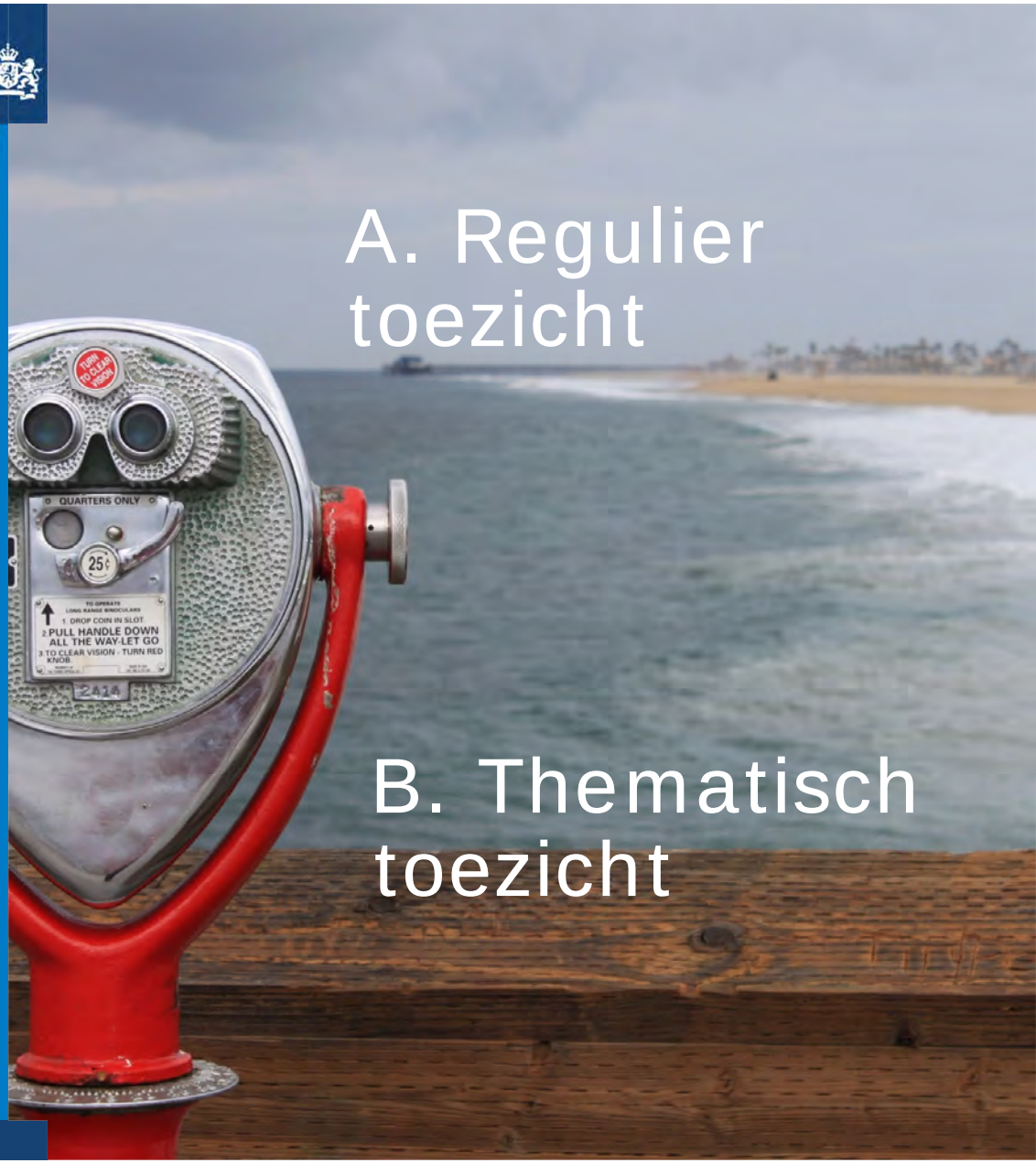
- Informatiegestuurd en risicogericht
  - Analyseren en leren van incidenten en inspecties
  - Normen ontwikkelen
- Effectief
  - Samenwerkend en in verbinding met de omgeving
  - Bevordert naleving
- Efficiënt:
  - Proportioneel
  - Interventie is ook informeren en verbinden
- Reflectief
  - Signaleren van (nieuwe) ontwikkelingen, dreigingen en risico's
  - Agenderend



3. Toezicht in de praktijk



- Informeren over wettelijk kader en zorgplicht
- Bevorderen naleving zorgplicht
- Inspecties
- Stimuleren meldingsbereidheid en wil om te leren
- Stimuleren zelfregulering en normering in een branche
- Just culture



Wettelijk kader

EU **Directive**: Netwerk- en Informatiebeveiliging (NIB) richtlijn

Wbni: Nederlandse implementatie van de NIB

Open norm

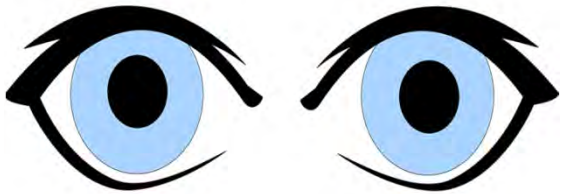
De wetgever zegt:

De aanbieder van een essentiële dienst neemt passende en evenredige technische en organisatorische maatregelen

De wetgever zegt niet:

De aanbieder van een essentiële dienst neemt de volgende maatregelen om de risico's voor de beveiliging van hun netwerk- en informatie-systemen te beheersen.

Hoe houd je dan toezicht?



Systeemtoezicht

al het toezicht waarbij de opzet, reikwijdte en werking van (kwaliteits)systemen en bedrijfsprocessen bij organisaties wordt vastgesteld. Dit door auditachtige onderzoeken met realitychecks uit te voeren.”

Met welk oog kijkt de toezichthouder?

- Wettelijk kader (zorgplicht)
- Niet één geldende norm
- Geaccepteerde standaarden (ISO, ETSI, NIST et cetera)
- Brancherichtlijnen, best practices
- Ervaring en kennis toezichthouder
- Uitleg en documentatie organisatie zelf

Geaccepteerde standaarden

Uit: reference document on security measures for operators of essential services (NIS coorporation group)

1. • Governance / ecosystem (Risico's)
2. • Protection (Preventieve maatregelen)
3. • Defense (Detectieve maatregelen)
4. • Resilience (Repressieve en correctieve maatregelen)

Domeinen

1. Governance / ecosystem (Risico's)
2. Protection (Preventieve maatregelen)
3. Defence (Detectieve maatregelen)
4. Resilience (Repressieve en correctieve maatregelen)

Type maatregelen

- 1: Security governance & risk management; ecosystem management
- 2: IT security architecture; IT security administration; IAM; security maintenance; physical security
- 3: Detection, Incident management
- 4: Continuity and crisis management

C. Incident gestuurd toezicht

- Melding van een incident
- Vermoeden of aanwijzing van een incident

Meldplicht

- Een AED moet een incident met “aanzienlijke gevolgen” voor de dienstverlening melden.
- Bij twijfel: gewoon melden
- Niet automatisch handhaven
- Een melding leidt niet tot verhoogde verwijtbaarheid, integendeel
- NCSC geeft geen meldingen door aan toezichthouder (AT), daarom dubbel melden.
- Het Ministerie EZK stelt de drempelwaarden voor een sector vast

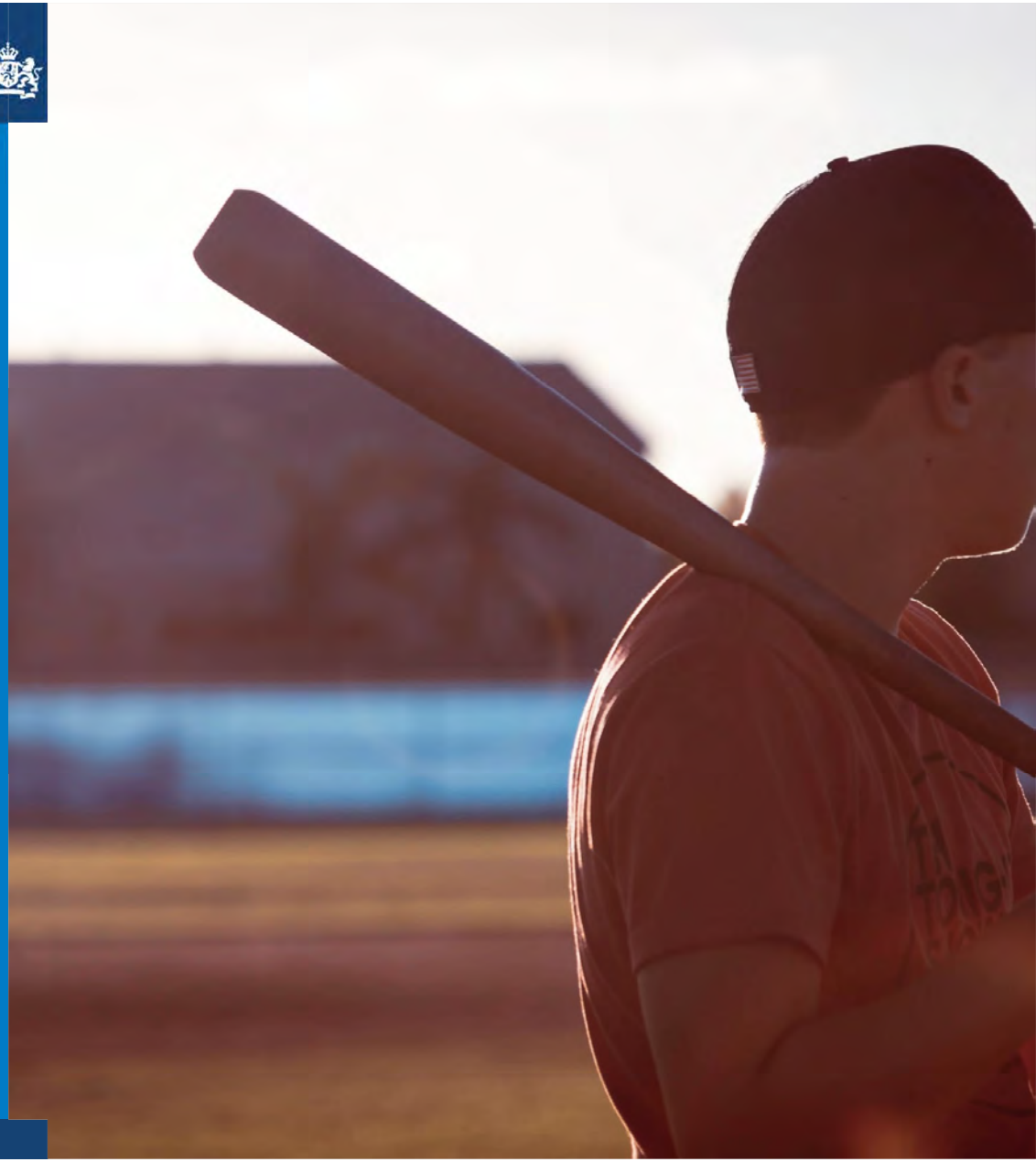
4. Tot slot

In simpel proza

- Ken je netwerk- en informatiesystemen die je essentiële dienst mogelijk maken
- Ken de risico's voor die netwerk- en informatiesystemen
- Zorg voor een adequate beheersing van die risico's
- Wijs iemand aan die verantwoordelijk is voor het signaleren en melden van incidenten
- Zorg ervoor dat je netwerk- en informatiesystemen na een incident z.s.m. weer beschikbaar zijn.

End game?

- meldingsbereidheid en lerend effect
- ontstaan van branchebrede normen en voorzieningen
- ontwikkeling van richtsnoeren (waaronder security frameworks, risico analyses, etc.)
- self assessments, quick scans
- delen van informatie
- ‘just culture’



Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Een veilig verbonden Nederland

Daar staat Agentschap Telecom voor

Meer informatie of een vraag?

Kijk op **agentschaptelecom.nl/wbni** of

stuur een e-mail naar **wbni@agentschaptelecom.nl**

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Team Wbni

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Van
5.1.2.e
5.1.2.e
5.1.2.e

T

Datum
December 2022

Bijlagen
1 Versiebeheer

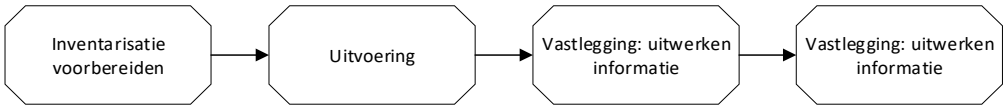
memo

Procesbeschrijving inventarisatie nieuwe AED's

In deze memo is het proces "inventarisatie nieuwe AED's" uitgeschreven. De inventarisatie wordt uitgevoerd bij iedere AED die voor het eerst met de Wbni te maken heeft. Voordat de inventarisatie wordt uitgevoerd heeft een kennismaking op directieniveau plaatsgevonden. Voor documenten van de kennismaking zie map kennismakingsgesprek van de desbetreffende AED[1].
Tijdens de kennismaking is de inventarisatie aangekondigd. Om de inspectie uit te voeren wordt gebruik gemaakt van het dummy dossier en de volgende documenten[2]:

- Vragenlijsten 'begrip van het bedrijf' en 'inventarisatie zorgplicht',
- Vastlegging gespreksverslagen 'begrip van het bedrijf' en inventarisatie 'zorgplicht'.

De volgende stappen worden doorlopen om de inventarisatie uit te voeren:



De inventarisatie heeft als doel om een eerste indruk te krijgen van het bedrijf en inventariseren welke maatregelen de organisatie heeft genomen voor informatiebeveiligingsrisico's.
Let wel, het gaat hier om een inventarisatie. Er is dus nog geen sprake van een oordeel van AT en derhalve dient er ook geen evidence te worden opgevraagd. Daarnaast dient dit gesprek voor een nadere kennismaking: een logisch vervolg op het eerdere gesprek. Het is het tweede formele contactmoment tussen AT en de AED.

[1] buiten reikwijdte

[2] buiten reikwijdte

Inventarisatie voorbereiden
Voer een interne analyse om het gesprek voor te bereiden. Hierbij kan gebruik worden gemaakt van al uitgevoerde inventarisatiedocument van de desbetreffende AED[3].

Er dient 1 of 2 inventarisatiegesprekken (in overleg met AED) ingepland te worden met de AED.
Het eerste gesprek betreft 'begrip van het bedrijf'. Doel hiervan is het verkrijgen van globale indruk en kenmerken van de AED en kunnen vergelijken van lijsten van AED's. Van tevoren wordt een meerkeuzevragenlijst 'begrip van bedrijf' inclusief handleiding opgestuurd en wordt gevraagd om het in te vullen en te retourneren. Het retourneren zal via onze Client Portal AT gaan. Voeg de AED contactpersoon op in de Client Portal en stuur ook de handleiding Client Portal Agentschap Telecom[4] naar de desbetreffende persoon.
Op basis van de ingevulde vragenlijst wordt bepaald welke vragen je nader toegelicht wilt krijgen (open vragen) tijdens het inventarisatiegesprek.

Het tweede gesprek betreft 'inventarisatie zorgplicht'. Het doel hiervan is het verkrijgen van een globale brede indruk van getroffen maatregelen en kunnen vergelijken van lijsten van AED's. Net als bovenstaande wordt een vragenlijst 'inventarisatie zorgplicht' opgestuurd dit kan op hetzelfde moment verzonden worden. Op basis van de ingevulde vragenlijst wordt bepaald welke vragen je nader toegelicht wilt krijgen (open vragen) tijdens het geplande gesprek. Het resultaat is input voor de verdere invulling van onze toezichtstrategie.

Zorgen wegnemen bij AED
Bij de communicatie met de AED zal duidelijk worden gemaakt wat we met dit instrument willen bereiken. Het gaat slechts om een eerste indruk van de getroffen maatregelen. Een inventarisatie kan door de AED als beoordeling worden ervaren, waar mogelijk negatieve gevolgen aan zitten. Het is niet mogelijk om de AED te beloven dat zij gevrijwaard zijn van handhaving,[5] echter, het doel van het assessment is niet om op basis van de uitkomsten handhavend op te treden. Een andere zorg van de AED kan zijn dat de inventarisatie wordt gezien als de vinklijst waarmee AT het toezicht gaat uitvoeren. Dit is nadrukkelijk niet het geval, de inventarisatie kan *niet* worden gezien als een invulling van de open norm.

Uitvoering
Tijdens de inventarisatiegesprekken kan er uitleg en vragen gesteld worden naar aanleiding van de opgestuurde vragenlijsten. Het doel van de gesprekken is een eerste indruk krijgen van het bedrijf en inventariseren hoe risico's worden beheerst (zorgplicht). Behandel minimaal de opvallende antwoorden (bv. afwijkingen t.o.v. van andere partijen). Vraag door totdat jij vindt dat het de formulieren een juist en volledig beeld weergeven. Eventueel kun je met een collega sparren over de diepgang.

[3] buiten reikwijdte [redacted]
[4] buiten reikwijdte [redacted]
[5] Je kunt een onder toezichtstaande partij in geen enkel geval toezeggen dat er niet gehandhaafd gaat worden.

De focus ligt op de 5 BBNI-onderwerpen en inzicht te krijgen welke processen en objecten van de AED binnen de essentiële dienst valt.

1. Risico gebaseerde aanpak
2. Organisatie van netwerk- en informatiebeveiligingsbeheer
3. Incidenten voorkomen
4. Detectie en respons
5. Gevolgen van incidenten beperken

Vastlegging: uitwerken informatie
Na afloop wordt door de inspecteurs verslag gemaakt van het gesprek. Gebruik de informatie die uit het gesprek is gekomen. Stuur het verslag op naar de contactpersoon bij de AED, vraag om een reactie en verwerk zijn commentaar in het verslag.

Afronding
Verwerk alle gevraagde informatie en verwerk alle bevindingen en zorg ervoor dat alle bestanden worden opgeslagen in de daarvoor bestemde directory.[6] Stuur ter afsluiting een eindrapportage[7] naar de AED waarin wordt gemeld dat deze fase afgesloten is. Gebruik hiervoor de rapportage template uit het dummy dossier. Uitgangspunt is om de gehele inventarisatie binnen 2 maanden na het kennismakingsgesprek af te ronden.

Laat een dossierreview uitvoeren door de lead auditors. Zij kijken zowel naar de volledigheid van het dossier als de inhoud. Verwerk eventuele vragen en opmerkingen. Na goedkeuring kan je de brief laten ondertekenen door de manager Wbni via de ondersteunende medewerk(st)er. Deze rapportage dient te zijn voorzien van een RP nummer.

Sla alle afstemmingen en bewijzen van versturen documenten op in het dossier. Denk ook aan print screens inclusief datum van verzending en toelichting van via de infoportal verstuurde en ontvangen stukken.

[6] buiten reikwijdte
[7] buiten reikwijdte

Bijlage: versiebeheer

Versie	Datum	Wijzigingen door	Gewijzigd
1.1	September 2021	5.1.2.e en 5.1.2.e	Eerste opzet
1.2	Januari 2022	5.1.2.e en 5.1.2.e	Toegevoegd gebruik van rapportage template. Besluit in teamoverleg 10-1-2022.
1.3	November 2022	5.1.2.e , 5.1.2.e en 5.1.2.e	Aanpassingen nav gas en olie aanwijzing