Ministerie van Infrastructuur
en Waterstaat

HOOFDDIRECTIE BESTUURLIJKE EN JURIDISCHE ZAKEN

Regeling van de Minister van Infrastructuur en Waterstaat, van ....., nr. IENW/BSK-, houdende nadere regels voor de beveiliging van netwerk-en informatiesystemen van aanbieders van essentiële diensten in de sectoren op het terrein van infrastructuur en waterstaat (Regeling beveiliging netwerk- en informatiesystemen IenW)

VERSIE TEN BEHOEVE VAN DE INTERNETCONSULTATIE

De Minister van Infrastructuur en Waterstaat,

Na overleg met de Minister van Justitie en Veiligheid;

Gelet op artikel 3a van het Besluit beveiliging netwerk- en informatiesystemen;

BESLUIT:

Paragraaf 1 Begripsbepalingen

Artikel 1 Begripsbepalingen

In deze regeling wordt verstaan onder:
AED: aanbieder van een essentiële dienst;
besluit: Besluit beveiliging netwerk- en informatiesystemen;
ISMS: Information Security Management System als bedoeld in artikel 3, tweede tot en met vierde lid;
risicoanalyse: risicoanalyse als bedoeld in onderdeel 1 van de bijlage bij artikel 3a, eerste lid, van het besluit;

Paragraaf 2 Reikwijdte

Artikel 2 Reikwijdte

1. Deze regeling is van toepassing op elke AED in de sectoren drinkwater en vervoer, onderdelen luchtvervoer en vervoer over water, voor zover het de netwerk- en informatiesystemen betreft die gebruikt worden voor de essentiële dienst.
2. Bij het nemen van de maatregelen, opgenomen in onderdelen 1 tot en met 5 van de bijlage bij artikel 3a van het besluit, past de AED de paragrafen 3 tot en met 9 toe.

Paragraaf 3 ISMS en risicoanalyse

Artikel 3 ISMS

1. De AED hanteert een ISMS.
2. Het ISMS stelt de AED in staat om maatregelen te nemen uit te voeren en waar nodig die bij te stellen met als doel om op een structurele wijze risico’s terug te brengen tot een acceptabel niveau.
3. Het ISMS omvat omschrijvingen van het beleid, de processen en procedures, gericht op de maatregelen bedoeld in de paragrafen 4 tot en met 8.
4. Het ISMS ondersteunt de AED bij het toepassen van de continue verbetercyclus, bedoeld in artikel 5.
5. De AED beschikt over een document waarin is vastgelegd op welke wijze uitvoering is gegeven aan het eerste lid.

Artikel 4 Risicoanalyse
1. In de risicoanalyse is met behulp van een onderbouwing vastgelegd welk risiconiveau acceptabel wordt geacht voor de levering van de essentiële dienst.
2. Bij de risicoanalyse worden de risico's binnen de keten van toeleveranciers en afnemers betrokken voor zover deze kunnen leiden tot een incident bij de levering van de essentiële dienst.
3. De risicoanalyse wordt op basis van een door de AED vastgelegde procedure periodiek geactualiseerd en telkens wanneer blijkt dat de dreigingen of kwetsbaarheden significant zijn toe- of afgenomen.

Artikel 5 Verbetercyclus
1. De AED hanteert een continue verbetercyclus, waarmee:
a. maatregelen worden toegepast ter beheersing van risico's;
b. de doeltreffendheid van deze maatregelen wordt beoordeeld; en
c. de maatregelen worden bijgesteld, wanneer de beoordeling daartoe aanleiding geeft.
2. De AED heeft inzicht in de mate waarin de maatregelen doeltreffend zijn en de risico's beheerst zijn.
3. De AED is, met behulp van het ISMS, in staat desgevraagd verantwoording af te leggen over de mate waarin de maatregelen doeltreffend zijn en de risico's worden beheerst.

Paragraaf 4 Organisatie van netwerk- en informatiebeveiliging

Artikel 6 Beschrijving taken, bevoegdheden en verantwoordelijkheden
De AED beschrijft bij wie of welke functionaris taken, bevoegdheden en verantwoordelijkheden, als bedoeld in de bijlage bij artikel 3a van het besluit, onderdeel 2, zijn belegd en actualiseert deze beschrijving als er wijzigingen zijn.

Artikel 7 Kwalificaties functionarissen
1. De AED waarborgt dat functionarissen over passende kwalificaties beschikken gelet op de bij hen belegde taken, bevoegdheden en verantwoordelijkheden.
2. De AED verzorgt voor de functionarissen die bij hem in dienst zijn periodieke bewustwordings- en trainingsactiviteiten en opleidingen, gericht op de voor netwerk- en informatiebeveiliging noodzakelijke kennis en kunde, het gewenste gedrag en daarop gerichte bewustzijn van betrokkenen.

Artikel 8 Gedrag van management en medewerkers
1. Het management van de AED bevordert bewustzijn en bewustwording van de noodzaak van informatiebeveiliging in de organisatie en neemt daarin het voortouw.
2. De AED legt beleid vast over screening, professionaliteit en integriteit van medewerkers, over geheimhouding door medewerkers en voor maatregelen in geval van schending van de geheimhouding of integriteit en past dat beleid toe.

Paragraaf 5 In kaart brengen

Artikel 9 Netwerk- en informatiesystemen
1. Het actuele overzicht, bedoeld in onderdeel 1 van de bijlage bij artikel 3a van het besluit, bevat actuele configuratie van de netwerk- en informatiesystemen en

de relevante kenmerken ervan. Onderdeel van het overzicht is een beschrijving van de zonering en koppelingen van netwerken.
2. Het overzicht classificeert de systemen en onderdelen ervan aan de hand van de business impact bij verstoringen en beschrijft het beveiligingsniveau.
3. De configuratie is vastgelegd in een configuratie management database. De beschrijving omvat de versies van hard- en software die in gebruik zijn bij onderdelen van netwerk- en informatiesystemen, die door de AED als kritiek zijn geclassificeerd.
4. De AED monitort de kwetsbaarheden voor de configuratie en legt deze vast.

Artikel 10 Asset- en lifecyclemanagement
1. Voor onderdelen van netwerk- en informatiesystemen die door de AED als kritiek worden geclassificeerd hanteert de AED asset- en lifecyclemanagement.
2. De AED stelt een proces vast voor het tijdig vernieuwen of afvoeren van systemen (end-of-support-management) en past dit toe.

Paragraaf 6 Beschermen en voorkomen

Artikel 11 Patchmanagement
Het patchmanagement, bedoeld in de bijlage bij artikel 3a van het besluit, onderdeel 3, is gebaseerd op een risicoanalyse over de kwetsbaarheid van de configuratie en een risicoanalyse over de uit te voeren patch.

Artikel 12 Leveranciersmanagement
1. De AED betrekt bij overeenkomsten met derden, waaronder leveranciers, relevante beveiligingseisen, -verantwoordelijkheden en -rollen, en maakt afspraken over de eisen aan beveiligingsprestaties van de leverancier, het melden van incidenten en de beëindiging van de overeenkomst. De AED houdt de gemaakte afspraken actueel.
2. Netwerk- en informatiebeveiliging maken onderdeel uit van de inkoopeisen van software, hardware en diensten.

Artikel 13 Security by design
1. De AED borgt netwerk- en informatiebeveiliging bij ontwerp, planning en realisatie van netwerk- en informatiesystemen.
2. De AED gebruikt segmentering om te verhinderen dat een kwetsbaarheid of ongeautoriseerde toegang tot een netwerk- of informatiesysteem gebruikt kan worden om andere netwerk- of informatiesystemen te compromitteren. De keuze voor het toepassen van segmentering wordt gemaakt op basis van een risicoanalyse.

Artikel 14 Fysiek beveiligingsbeleid
De AED heeft beleid vastgelegd over de fysieke beveiliging van netwerk- en informatiesysteemcomponenten en faciliteiten die de netwerken ondersteunen en past dit beleid toe.

Artikel 15 Logische toegangsbeveiligingsbeleid
1. De AED heeft beleid vastgelegd voor logische toegangsbeveiliging voor de toegang tot netwerk- en informatiesystemen en past dit beleid toe. Dit beleid ziet in ieder geval op beheer van identiteiten, authenticaties en autorisaties, waaronder uitgeven, monitoren van gebruik en intrekken ervan.
2. Autorisaties worden jaarlijks beoordeeld op juistheid en geactualiseerd.

Artikel 16 Software beveiliging
1. De AED past effectieve maatregelen toe tegen malware en monitort deze.
2. Indien gebruik gemaakt wordt van versleuteling, worden maatregelen toegepast om de betrouwbaarheid, integriteit en vertrouwelijkheid van de gebruikte sleutels te borgen.

Artikel 17 Gecontroleerd wijzigingenbeheer
1. De AED heeft beleid vastgelegd voor het beheerst doorvoeren van wijzigingen in en op een netwerk- en informatiesysteem en past dit beleid toe.
2. De AED heeft voorts de processen vastgelegd voor toepassen van een wijziging en past deze toe. Het proces omvat ook het testen van de wijziging.

Paragraaf 7 Detectie en respons

Artikel 18 Melden van incidenten, tekortkomingen en kwetsbaarheden
1. De AED heeft beleid vastgelegd voor het melden van incidenten door werknemers en ziet toe op de toepassing ervan.
2. De AED heeft beleid vastgelegd en processen beschreven voor het melden en identificeren van tekortkomingen en kwetsbaarheden en past deze toe.

Artikel 19 Loggen van beveiligingsgerelateerde handelingen
1. De AED heeft een proces vastgelegd voor het loggen van handelingen op een netwerk- en informatiesysteem en past dit toe. Als onderdeel van het proces zijn de parameters beschreven, waaronder handelingen die leiden tot een nadere analyse en onderzoek.
2. Het eerste lid is niet van toepassing op componenten van netwerk- en informatiesystemen waarvoor op technische gronden loggen van handelingen niet mogelijk is. De AED heeft vastgelegd voor welke componenten dit geldt.

Artikel 20 Monitoring van netwerk- en informatiesystemen
1. De AED heeft het proces vastgelegd over de methode van monitoring van een netwerk- en informatiesysteem.
2. De AED heeft detectieprocessen en -procedures vastgelegd om afwijkende gebeurtenissen tijdig op te merken, te classificeren en, waar noodzakelijk, op te volgen. De AED past deze processen en procedures toe en test deze.

Artikel 21 Respons op incident
1. De AED heeft procedures vastgelegd voor het classificeren, onderzoeken en verhelpen van incidenten, en het intern en extern communiceren en rapporteren over incidenten, en past deze procedures toe.
2. De AED borgt dat een incident naar de ernst ervan wordt beoordeeld. Bij de beoordeling van de ernst wordt de impact op ketenpartners betrokken.
3. Incidenten worden geanalyseerd en geëvalueerd. De uitkomsten van deze analyse en evaluatie worden gebruikt bij de verbetering van de beheersing van de risico's.

Paragraaf 8 Herstel

Artikel 22 Continuïteitsplannen

De crisis- of bedrijfscontinuïteitsplannen worden jaarlijks getest op doeltreffendheid en waar nodig aangepast. Testen kan plaatsvinden door middel van oefeningen.

Artikel 23 Herstel door backups
1. De AED heeft procedures vastgelegd voor het maken van backups (system, software en data), past deze procedures toe en past deze indien nodig aan.
2. Het eerste lid is niet van toepassing op componenten van netwerk- en informatiesystemen waarvoor op technische gronden het maken van backups niet mogelijk is. De AED heeft vastgelegd voor welke componenten dit geldt.
3. De AED test ten minste jaarlijks het terugzetten van backups waarvoor dat op technische gronden mogelijk is.

Paragraaf 9 Slotbepalingen

Artikel 24 Rechtsvermoeden
1. Een AED kan aantonen dat de paragrafen 3 tot en met 9 zijn toegepast, door aan te tonen dat een met deze regeling tenminste gelijkwaardige sectorspecifieke norm wordt toegepast.
2. De Beveiligingsnorm Procesautomatisering, zoals vastgesteld op [PM datum] door de drinkwaterbedrijven gezamenlijk en die geldt voor de sector drinkwater, wordt vermoed tenminste gelijkwaardig te zijn met deze regeling, behoudens [de paragrafen … en artikelen … PM].
3. EASA.rmt720, zodra deze is vastgesteld en geldt voor de sector vervoer, onderdeel luchtvaart, wordt vermoed tenminste gelijkwaardig te zijn met deze regeling.
4. Een wijziging in een sectorspecifieke norm wordt door de AED medegedeeld aan de Minister en aan de Inspecteur-Generaal van de Inspectie Leefomgeving en Transport.

Artikel 25 Inwerkingtreding
Deze regeling treedt in werking met ingang van [1 juli 2021.]

Artikel 26 Citeertitel
Deze regeling wordt aangehaald als: Regeling beveiliging netwerk- en informatiesystemen IenW.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

drs. C. van Nieuwenhuizen - Wijbenga

Toelichting

Algemeen

1. Inleiding
Deze ministeriele regeling beoogt het minimumniveau voor te schrijven van maatregelen die een aanbieder van een essentiële dienst (hierna: AED) moet nemen om te voldoen aan de artikelen 7 en 8 van de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni). Artikel 3a, eerste lid, van het Besluit beveiliging netwerk- en informatiesystemen (hierna Bbni) bepaalt dat ter uitvoering van de artikelen 7 en 8 van de Wbni de AED ten minste de maatregelen beschreven in de bijlage behorend bij artikel 3a van het Bbni neemt. In die bijlage zijn normen opgenomen, die de doelen beschrijven waartoe de maatregelen van de artikelen 7 en 8 van de Wbni toe moeten leiden. In deze regeling worden nadere regels gesteld over de door AED's in de sectoren op het terrein van het ministerie van infrastructuur en waterstaat (waaronder drinkwater en transport) te nemen maatregelen.

2. Hoofdlijnen van deze regeling
De regeling benoemt de aspecten waarover een AED beleid, processen en procedures moet ontwikkelen of ontwikkeld heeft. De regeling beoogt niet concreet voor te schrijven wat de inhoud van dit beleid, deze processen of deze procedures moet zijn. De concrete invulling, binnen de geschetste kaders, is vrij. Het noodzakelijke niveau van beveiliging is hoog. De verwachting is dat met deze regels de AED's de te nemen maatregelen makkelijker kunnen rechtvaardigen (intern en extern), en dat eventuele concurrentiele druk niet leidt tot onwenselijke (bezuinigings)keuzes waardoor zich risico's voor zouden kunnen doen in de levering van de essentiële dienst.

De nadere regels in deze regeling betreffen de onderdelen 1 tot en met 5 van de bijlage bij artikel 3a Bbni en zien op: het beschikken over een Information Security Management-System (hierna ISMS) (par. 3), de organisatorische aspecten van beveiliging (par. 4), inzicht in de toestand van de architectuur, hardware en software van de systemen (par. 5), het mitigeren van risico's (par. 6), het signaleren en opvolging geven aan signalen over kwetsbaarheden en compromittaties van de netwerk- en informatiesystemen (par. 7) en het herstel na een incident (par. 8). De belangrijkste elementen van deze regeling worden hieronder nader toegelicht.

ISMS
Een ISMS is een procesgerichte, stelselmatige, benadering voor informatiebeveiliging. Het is een managementsysteem waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd. Het is niet een specifiek instrument, tool of programma, maar een samenhangend geheel ervan. Er zijn wel programma's beschikbaar op de markt, die een ISMS faciliteren, maar deze regeling schrijft het gebruik ervan niet voor. Een ISMS kan gehanteerd worden met behulp van algemeen verkrijgbare database- of spreadsheet-programma's. Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Het helpt de betrokken partijen onder andere om risico's te beheersen,

passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid van de informatievoorziening en bedrijfscontinuïteit te waarborgen.

Risicoanalyse
Zoals bepaald in artikel 7 van de Wbni neemt de AED passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen.
De risicoanalyse stelt de AED in staat op basis van gekwantificeerde risico's (impact maal kans) beslissingen over deze mitigerende maatregelen te nemen en te onderbouwen. Bij die beslissingen is een belangrijke rol weggelegd voor het niveau van acceptatie van risico's (de risk-appetite). Deze regeling schrijft voor dat het niveau van acceptatie van risico's wordt onderbouwd en vastgelegd in de risicoanalyse.
Op grond van een risicoanalyse kunnen de volgende maatregelen worden genomen:
• Preventie: het voorkomen dat iets gebeurt of het verminderen/ verkleinen van de kans dat het gebeurt;
• Detectie: het detecteren van de (potentiële) schade wanneer een bedreiging optreedt;
• Repressie: het beperken van de schade wanneer een bedreiging optreedt;
• Correctie: het instellen van maatregelen die worden geactiveerd zodra iets is gebeurd om het effect hiervan (deels) terug te draaien
• Acceptatie: geen (additionele) maatregelen, men accepteert de kans en het mogelijke gevolg van een bedreiging.

Sectorspecifieke normen
Enkele sectoren, te weten drinkwater en luchtvaart, hebben sectorspecifieke normen, die, wanneer deze toegepast zijn, voorzien in een hoog niveau van beveiliging. Deze sectorspecifieke normen kunnen, nadat deze beoordeeld zijn, gelden als ten minste gelijkwaardig met deze regeling. Op aspecten waar deze gelijkwaardige sectorspecifieke normen maatregelen voor voorschrijven, biedt deze regeling geen toegevoegde waarde. In artikel 24 is opgenomen over welke aspecten de daarin genoemde sectorspecifieke normen als gelijkwaardig, worden beschouwd. Aanpassingen van sectorspecifieke normen of geheel nieuwe normen kunnen leiden tot wijziging van dat artikel.
Voor aspecten waar de sectorspecifieke normen niet op zien, en waar deze sectorspecifieke normen dus niet als gelijkwaardig kunnen gelden, heeft de regeling zelfstandig betekenis en moet de naleving van de regeling aangetoond worden, zonder daarvoor een beroep te kunnen doen op de naleving van de sectorspecifieke norm.

3. Verhouding tot Wbni en Bbni
Met ingang van 9 november 2018 geldt de Wbni. Deze wet vormt de omzetting van richtlijn 2016/1148/EU, houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L194) (hierna de NIB-richtlijn). Samen met de Wbni is op 9 november 2018 ook het Bbni in werking getreden. In het Bbni worden onder meer de vitale aanbieders aangewezen die onder de reikwijdte vallen van de verplichtingen van de Wbni.

Deze regeling biedt een kader voor de maatregelen die AED's reeds verplicht zijn om te nemen op grond van artikel 7 en 8 van de Wbni en de invulling die aan die artikelen is gegeven in artikel 3a van en de bijlage bij het Bbni. De grondslag van deze regeling biedt de mogelijkheid om nadere regels te stellen over de maatregelen die in het Bbni in de bijlage genoemd zijn. Vandaar dat de opbouw van de bijlage in de vijf onderdelen is te herkennen in de opbouw van deze regeling. Onderdeel 1. Risicogebaseerde aanpak, en onderdeel 2. Organisatie van netwerk- en informatiebeveiliging van de bijlage van het Bbni worden gespiegeld in de paragrafen 3 en 4 van deze regeling. Over de onderdelen 3, 4 en 5, zijn nadere regels opgenomen in de paragrafen 5, 6, 7 en 8. Bij de indeling in de paragrafen 5 tot en met 8 is aansluiting gezocht bij het de indeling van het National Institute for Security and Technology: *identify, protect, detect, respond* en *recover.*
Vanzelfsprekend wordt in deze regeling aangesloten bij het begrippenkader dat in de Wbni en de Bbni gebruikt wordt. Dat is met name relevant voor begrippen als "risico" en "netwerk- en informatiesystemen". Aan deze begrippen komt dezelfde betekenis toe als artikel 1 van de Wbni daaraan geeft, die daarvoor verwijst naar artikel 4 van de NIB-richtlijn.

4. Gevolgen
Het voorschrijven van een minimumniveau van beveiliging voor de AED's. Naar verwachting voldoen de AED's al uit eigen beweging en op grond van de Wbni aan het merendeel van de in deze regeling voorgeschreven aspecten. Dit is ook uit de informele consultatie gebleken.

5. Toezicht en Handhaving
De ILT is belast met het toezicht op de naleving van de Wbni. De Inspectie heeft op deze regeling een handhaafbaarheids-, uitvoerbaarheids- en fraudebestendigheidstoets (hierna: HUF-toets) op een concept van de regeling uitgevoerd. Als gevolg van deze toets [PM resultaten toets en beschrijving aanpassingen]

6. Consultaties
Bij de opstelling van onderhavige regeling zijn betrokken de vereniging van drinkwaterbedrijven Vewin, Rijkswaterstaat, het NCSC, de ILT en alle AED's die op het moment van schrijven als zodanig zijn aangeschreven. Zij hebben allen op conceptversies kunnen reageren. De suggesties die dit heeft opgeleverd zijn meegewogen in het opstellen van de definitieve teksten of de nota van toelichting. Na het opstellen van de conceptversie is nog een extra bijeenkomst geweest om toe te lichten welke wijzigingen zijn aangebracht in de conceptversie. [PM internetconsultatie]

7. Regeldruk
De regeling leidt tot een beperkte toename in de nalevingskosten voor de AED's. De meeste AED's hebben reeds eerder aangegeven dat de extra regeldruk als gevolg van de bijlage bij artikel 3a van het Bbni relatief beperkt zal zijn, ervan uitgaande dat de bijlage dusdanig kan worden geïnterpreteerd dat deze goed aansluit op de maatregelen die zij de afgelopen periode al hebben genomen om te voldoen aan de Wbni.
De maatregelen in deze regeling kunnen worden geïnterpreteerd als een aanscherping op de maatregelen die zij de afgelopen periode al hebben genomen

om te voldoen aan de Wbni en gaan nemen om te kunnen voldoen aan de bijlage bij artikel 3a van het Bbni.
Voor de meeste maatregelen in deze regeling geldt namelijk dat ze meer in detail uitgewerkt en in samenhang beschreven zijn ten opzichte van de bijlage bij artikel 3a van het Bbni. Een aantal maatregelen zijn aanvullend op deze bijlage omdat zij een grotere mate van detail kennen. Voor de meeste maatregelen betreft de verscherping een meer gestructureerde vastlegging van bijvoorbeeld processen, procedures, beleid en uitkomsten.
Er is een differentiatie aan te brengen in de gevolgen voor verschillende groepen AED's. Er zijn AED's die wel een sectoraal normenkader hebben waar ze aan moeten voldoen en AED's die dit nog niet hebben. Voor AED's die geen sectorspecifiek normenkader hebben en toepassen geldt dat de incidentele nalevingskosten samenhangen met het gestructureerd vastleggen van de maatregelen in een ISMS en het afstemmen erover met management. De groep betreft zes bedrijven in de sector vervoer, onderdeel luchtvervoer en een bedrijf in de sector vervoer, onderdeel vervoer over water. Incidenteel worden de lasten becijferd op € 3016 per AED (40 uur door een medewerker à € 60 p/u en 8 uur door management à € 77 p/u). Structureel komen daar op jaarbasis € 4800 bij (80 uur per jaar door een medewerker à € 60 p/u).

De structurele toename is becijferd op € 2400 jaarlijks voor AED's die reeds een sectoraal normenkader hebben en toepassen (40 uur per jaar door een medewerker à € 60 p/u). Dit betreft de 10 drinkwaterbedrijven.
De totale incidentele toename van de regeldruk is daarmee: € 21.112 en de jaarlijkse structurele toename € 57.600.

Artikelsgewijze toelichting

Artikel 2 Reikwijdte
De regeling is van toepassing op aanbieders van essentiële diensten in de sectoren transport, onderdelen luchtvervoer en vervoer over water, en drinkwater. Deze sectoren betreffen het domein van het Ministerie van Infrastructuur en Waterstaat. De regeling heeft alleen betrekking op de netwerk- en informatiesystemen die gebruikt worden voor het aanbieden van de essentiële dienst. Dat kunnen specifieke systemen zijn, of meer generieke systemen die ook, of zelfs in hoofdzaak, niet gebruikt worden voor de essentiële dienst, maar waarvan de essentiële dienst wel afhankelijk is. Voor die generieke systemen valt te denken aan het operating system, waarlangs inloggen moet plaatsvinden, voordat in een afgeschermde omgeving gekomen wordt. Een ander voorbeeld is een cloud-voorziening. Er zijn ook systemen (of componenten ervan) die niet gebruikt worden voor de essentiële dienst. Te denken valt aan de software voor loonadministratie.
Aan de hand van bijvoorbeeld een business-impact-analysis kan geïnventariseerd worden welke netwerk- en informatiesystemen gebruikt worden voor de essentiële dienst en hoe groot de impact is.

Paragraaf 3 ISMS en risicoanalyse
De regels in deze paragraaf zijn gesteld met het oog op de stelselmatige benadering van de beheersing van risico's en het verbeteren van deze beheersing. Een stelselmatige benadering vergt dat de sector- en organisatiespecifieke onderwerpen worden beschouwd in samenhang met de nationale strategie voor de beveiliging van netwerk- en informatiesystemen,

bedoeld in artikel 7, eerste lid, onder a, van de NIB-richtlijn en de opvolgers daarvan.

Artikel 3 ISMS
Een ISMS is een procesmatige geïntegreerde benadering van de beveiliging van informatie- en netwerksystemen. Voor deze regeling is relevant dat het niet zozeer gaat om het ISMS als specifiek instrument of tool, maar als management systeem.
Het eerste lid van artikel 3 schrijft voor dat de AED beschikt over een ISMS, en dat ISMS toepast. In het tweede lid is het doel of de doelen van het ISMS opgenomen. Wat het ISMS moet bevatten, is beschreven in het derde lid.

Artikel 4 Risicoanalyse
Dit artikel bevat aanvullende bepalingen voor de risicoanalyse. Het doel van deze bepaling is om te bewerkstelligen dat een risicoanalyse actueel genoeg is voor het treffen van de juiste maatregelen. Deze risicoanalyse is op grond van artikel 3a en onderdeel 1 van de bijlage bij het Bbni verplicht gesteld. De inhoud van de risicoanalyse is toegelicht bij het Besluit tot wijziging van het Besluit beveiliging netwerk- en informatiesystemen (aanwijzing vitale aanbieders en nadere regels over beveiliging aanbieders van een essentiële dienst). Deze risicoanalyse kan geschieden in iedere passende vorm. Dat kan dus een corporate risicoanalyse zijn. De regeling schrijft wel voor dat bij de risicoanalyse enkele elementen betrokken worden, zoals de risico's die zich in de keten van toeleveranciers en afnemers kunnen voordoen (tweede lid). De bijlage bij artikel 3a van het besluit schrijft voor dat de signalen die de AED ontvangt van leveranciers en relevante overheidsorganisaties worden gebruikt voor het beoordelen of de maatregelen nog passend zijn. Wijzigingen in dreigingen en kwetsbaarheden kunnen onder meer blijken uit door het NCSC ontvangen signalen, uit gewijzigde omstandigheden of uit wijzigingen in functionaliteiten van de systemen. Als gevolg van de gewijzigde omstandigheden kan het noodzakelijk zijn om na te gaan of de risicoanalyse nog actueel is.
In het derde lid is opgenomen dat de AED de risicoanalyse telkens actualiseert wanneer de dreigingen en kwetsbaarheden significant toe- of afnemen. Gangbaar is dat de AED de risicoanalyse tenminste eenmaal per jaar actualiseert. Deze actualisatie houdt ten minste in dat de AED nagaat of de informatie die gebruikt is voor de risicoanalyse nog actueel en juist is, en dan, waar nodig, de risicoanalyse opnieuw uitgevoerd wordt met de geactualiseerde informatie. De AED beschikt over een procedure die dit proces beschrijft. Indien wordt afgeweken van de jaarlijkse termijn wordt dit in die procedure onderbouwd.

Artikel 5 Verbetercyclus
Artikel 5 bevat nadere regels betreffende periodieke evaluatie en bijstelling van de maatregelen, bedoeld in de aanhef van de bijlage bij het Bbni. Artikel 6 schrijft voor dat de AED een verbetercyclus toepast, met het oog op het beoordelen van de doeltreffendheid van de maatregelen. Een andere naam voor zo'n cyclus is de plan-do-check-act-cycle of de Deming-cyclus. Het doel van die cyclus is een iteratief proces dat leidt tot verbetering van de beveiliging tegen en beheersing van risico's. Binnen de cyclus worden de maatregelen of hun doeltreffendheid beoordeeld en waar nodig bijgesteld. Bij de beoordeling van de doeltreffendheid kan onder meer gebruik gemaakt worden van audits, beschikbaarheidsrapportages, penetratietesten, evaluatie van beleid, meten van prestaties en managementreviews. De beoordeling en de bijstelling vinden plaats

tegen de achtergrond van de risicoanalyse en het acceptabele niveau van rest risico's. Zowel het ISMS als de onderbouwing van de risicoanalyse faciliteren het cyclische verbeterproces.

Het ISMS stelt de AED in staat inzicht te hebben in de mate waarin de maatregelen effectief zijn, dus de risico's beheerst zijn. Dat inzicht is in eerste instantie voor intern gebruik cruciaal, maar ook de toezichthouder (ILT) kan daarom vragen. In het derde lid is daarom opgenomen dat de AED desgevraagd in staat is om deze verantwoording af te leggen. De verplichting om de verantwoording af te leggen en antwoord te geven op de vragen van de toezichthouder vloeit niet voort uit deze regeling, maar uit de bevoegdheden die de toezichthouder kan inzetten op grond van o.a. hoofdstuk 5 van de Algemene wet bestuursrecht.

Paragraaf 4 Organisatie van netwerk- en informatiebeveiliging
De regels van deze paragraaf zijn gesteld met het oog op de voor netwerk- en informatiebeveiliging noodzakelijke kennis en kunde, het gewenste gedrag en daarop gerichte bewustzijn van betrokkenen.

Artikel 8 Gedrag van management en medewerkers
In het tweede lid wordt voorgeschreven dat de AED beleid vastlegt en toepast over de screening van medewerkers van de AED. Ten eerste geldt dit uitsluitend voor de medewerkers die betrokken zijn bij de netwerk- en informatiesystemen die gebruikt worden voor de essentiële dienst. Ten tweede wordt de inhoud van het screeningsbeleid niet voorgeschreven. De aard van de screening of aan de hand van welke gegevens die screening plaatsvindt is aan de AED. Het is denkbaar dat andere regelgeving van toepassing is op de screening van medewerkers, afhankelijk van de aard en inhoud van de screening. Te denken valt aan de Wet justitiële en strafvorderlijke gegevens, of de Wet op de veiligheidsdiensten en tevens de Algemene verordening gegevensbescherming (Verordening 2016/679/EU) en de Wet veiligheidsonderzoeken. Deze regeling laat de voorwaarden en verplichtingen onder die regelgeving onverlet.
Hoewel de inhoud van de screening niet wordt voorgeschreven is wel noodzakelijk dat een onderbouwing voor de inhoud van de screening gemaakt wordt op basis van een risicoafweging, met betrekking tot de noodzaak of afwezigheid van de noodzaak om tot screening te komen.

Paragraaf 5 In kaart brengen
De regels van deze paragraaf zijn gesteld met het oog op het inzicht in de infrastructuur en de toestand ervan.

Artikel 9 CMDB
In het derde lid is opgenomen dat de configuratie is vastgelegd in een configuratie management database. Het is mogelijk om gebruik te maken van meerdere configuratie management database. Het is daarbij van belang dat de configuratie van ieder onderdeel van het netwerk- of informatiesysteem in een configuratie management database wordt vastgelegd en geen onderdelen worden overgeslagen.

Artikel 10 Asset- en lifecyclemanagement
Onder het asset- en lifecyclemanagement wordt verstaan de reeks bedrijfsprocessen die zijn ontworpen om de levenscyclus en inventaris van assets

van een organisatie te beheren. Dit verschaft de AED inzicht in de voor de essentiële dienst gebruikte assets, die de AED zelf als kritiek beschouwd. Dat inzicht omvat ook een overzicht van de onderhoudscyclus en de end-of-support of end-of-service voor zover deze bekend zijn. Daarom is een aspect van het asset- en lifecyclemanagement dat er een zorgvuldig contractmanagement aan ten grondslag ligt en dat er aandacht is voor de toereikendheid van de licenties. Het asset- en lifecyclemanagement vindt zijn neerslag in het configuratie management database (in artikel 9).

Paragraaf 6 Beschermen en voorkomen
De regels van deze paragraaf zijn gesteld met het oog op het mitigeren van risico's.

Artikel 13 Security by design
In het tweede lid wordt de segmentering van netwerken voorgeschreven. Het doel van segmentering is het beperken van het aanvalsoppervlak, de verschillende manieren waarop een aanvaller een apparaat of netwerk kan binnendringen. Hierdoor kunnen bedreigingen en incidenten uit de ene zone moeilijker kunnen doorwerken in de andere zone. Het kan hierbij bijvoorbeeld gaan om het scheiden van netwerken voor kantoorautomatisering en procesautomatisering die een verschillend risicoprofiel hebben. Segmentering kan op meerdere aspecten worden ingericht, bijvoorbeeld via (logisch of fysiek) gesegmenteerde netwerken of gesegmenteerd access management. Hierbij kan specifiek gedacht worden aan het scheiden van netwerken die gebruikt worden voor de industriële automatisering en netwerken voor de kantoorautomatisering.

Paragraaf 7 Detectie en respons
De regels in deze paragraaf zijn gesteld met het oog op het signaleren van kwetsbaarheden en aantasting van de integriteit van systemen en geven van opvolging aan deze signalen. In deze paragraaf wordt nadere invulling gegeven aan de verplichtingen die samenhangen met onderdeel 4 van de bijlage bij het Bbni. In die bijlage worden aantasting van de integriteit van systemen 'compromittatie' genoemd. In deze regeling wordt dit begrip niet gebruikt, maar is wel hetzelfde beoogd. Het beleid bedoeld voor het melden van incidenten, tekortkomingen en kwetsbaarheden bedoeld in artikel 18, wordt ook wel beleid voor Coordinated Vulnerability Disclosure (CVD) genoemd.

Artikel 19 Loggen van beveiligingsgerelateerde handelingen
In onderdeel 4 van de bijlage bij artikel 3a van het Bbni wordt de AED verplicht relevante handelingen op netwerk- en informatiesystemen vast te leggen. Het tweede lid van artikel 19 expliciteert dat deze plicht niet geldt voor de componenten waarvoor dat op technische gronden niet mogelijk is. Deze beperking zal naar verwachting uitsluitend spelen bij OT-componenten. De AED is gehouden vast te leggen voor welke componenten op technische gronden de handelingen niet gelogd kunnen worden.

Artikel 20 Respons op incident
Het derde lid schrijft voor dat incidenten door de AED worden geanalyseerd en geëvalueerd. Deze analyse zou ook moeten zien op de oorzaak of oorzaken van het incident. De AED wordt bij die analyse naar de oorzaken geholpen door de gelogde handelingen (zie artikel 19).

Paragraaf 8 Herstel
De regels in deze paragraaf zijn gesteld met het oog op het beperken van de gevolgen in geval een incident zich voordoet en het bespoedigen van het herstel van de essentiële dienst.

Artikel 22 Continuïteitsplannen
In de bijlage bij het Bbni wordt voorgeschreven dat de AED gebruik maakt van crisis- of bedrijfscontinuïteitsplannen. Deze regeling voegt daaraan toe dat deze plannen regelmatig worden getest. Daarvoor is aansluiting gezocht bij internationale normenkaders (als het ISO 27002:2013, control 17.1.3) door voor te schrijven dat het testen ten minste jaarlijks plaatsvindt. Een test kan plaatsvinden door middel van een oefening, zoals een tabletop-exercise. Het is onwenselijk dat een test of oefening zou leiden tot het onderbreken van de dienst.

Artikel 23 Herstel door backups
Een backup is een reservekopie van bestanden, instellingen en programma's op een server of computer. Wanneer er iets mis gaat kan deze reservekopie geraadpleegd worden om bestanden, instellingen en programma's te herstellen naar een oude, of nieuwe locatie. Een backup kan gemaakt worden naar een fysieke gegevensdrager of bijvoorbeeld een cloudlocatie. In het tweede lid is een uitzondering gemaakt voor componenten van het systeem waarvoor het maken van een back-up hiervan op technische gronden niet mogelijk is. Voor welke componenten dat geldt wordt vastgelegd.
In de bijlage bij artikel 3a van het Bbni wordt voorgeschreven dat periodiek het crisismanagement wordt beoefend. Het derde lid regelt daarvoor nader dat een onderdeel daarvan betreft dat het terugzetten van backups betreft. Volgens internationale normenkaders, (onder meer ISO 27002:2013, control 12.3.1) is het gebruikelijk om minimaal jaarlijks het terugplaatsen van een backup te testen.

Paragraaf 9 Slotbepalingen

Artikel 24 Rechtsvermoeden
De AED's in de sectoren drinkwater en vervoer, onderdeel luchtvaart hebben te maken met sectorspecifieke normen ten aanzien van het beveiligingsbeleid. De drinkwaterbedrijven hebben zichzelf gebonden aan vaststelling en toepassing van de Beveiligingsnorm Procesautomatisering. Voor de sector vervoer, onderdeel luchtvaart, geldt dat het merendeel van de AED's daar verplicht zal zijn om de EASA.rmt720 toe te passen. Deze EASA-norm is in ontwikkeling, maar de verwachting is gerechtvaardigd dat deze in belangrijke mate overlappend zal zijn met deze regeling en nog specifiekere op de sector luchtvaart toegeschreven normen zal bevatten. Deze EASA-norm kan ook relevant zijn voor de AED's in de sector vervoer, onderdeel luchtvaart, die niet verplicht zullen zijn deze norm toe te passen.
Op de naleving en toepassing van de sectorspecifieke normen wordt ook toegezien en de toepassing ervan kan leiden tot certificering.
Met het oog op het voorkomen van dubbele lasten als gevolg van het in deze regeling bepaalde, is in artikel 24 opgenomen dat de AED de naleving van deze regeling kan aantonen aan de toezichthouder, door de naleving van de sectorspecifieke norm. In het tweede en derde lid is opgenomen in welke mate de sectorspecifieke normen gelden als gelijkwaardig.

De regeling blijft van toepassing op de AED's in de sectoren genoemd in artikel 2, zolang deze niet zijn uitgezonderd van toepassing van artikel 7 en 8 van de Wbni (bijvoorbeeld door opname in artikel 4 van de Bbni).
Als de sectorspecifieke norm wijzigt, kan dat ertoe leiden dat de gelijkwaardigheid wijzigt. Daarom is in het vierde lid een bepaling opgenomen dat wijzigingen worden gezonden aan de minister en de ILT. Eventueel kan de wijziging van de sectorspecifieke norm leiden tot aanpassing van de regeling.

DE MINISTER VAN INFRASTRUCTUUR EN WATERSTAAT,

drs. C. van Nieuwenhuizen - Wijbenga