Waterschap Rivierenland

Crisisbestrijdingsplan van Waterschap Rivierenland

Digitale verstoring

Opgesteld:	J.M.H.E. van den Tillaart
Vastgesteld door:	Directieraad Waterschap Rivierenland
Vastgesteld op:	30 januari 2023
Status:	Definitief

Inhoudsopgave

Inleiding

Achtergrond

De fysieke wereld en digitale wereld is zich al jaren steeds meer aan het verweven met elkaar. Beide werelden zijn daarom ook steeds meer afhankelijk van elkaar. Een verstoring in het digitale landschap kan daarom grote gevolgen hebben. Dit omdat deze op veel gebieden randvoorwaardelijk zijn. Een grote verstoring kan al snel ontwrichtend zijn. Dit kan impact hebben op de voortgang van primaire processen en de voortgang van de operatie. Hierdoor kan er schade ontstaan aan mens en milieu en ontstaat er financiële- en imagoschade.

Voorheen werden risico's rondom digitale verstoring opgenomen in het crisisbestrijdingsplan niet water gerelateerd. De dreigingen voor digitale verstoring zijn elk jaar groter geworden en verdienen daarom een eigen crisisbestrijdingsplan.

Kader en uitgangspunten

De algemene aanpak van crisisbeheersing staat in het Crisisplan van Waterschap Rivierenland. Het Crisisplan beschrijft de wijze waarop het waterschap optreedt bij gebeurtenissen die het normale functioneren van het waterschap als overheidsorganisatie ernstig verstoort en tot maatregelen dwingt die niet binnen de dagelijkse routine vallen.

Dit crisisbestrijdingsplan beschrijft de risico's en opschalingscriteria met betrekking tot digitale verstoring. Dit plan biedt geen kant en klare oplossing maar beschrijft wel een aanpak die voor verschillende digitale verstoringen is uitgewerkt. Deze digitale verstoringen zijn uitgewerkt in verschillende hoofdstukken met als basis een algemeen hoofdstuk. In dit plan is per crisis het volgende vastgelegd:

- Het risico voor het waterschap;
- Een afwegingskader om te bepalen of en tot hoever de crisisorganisatie opschaalt;
- De afwijkingen in de opbouw van de crisisorganisatie ten opzichte van hetgeen het crisisplan is vastgelegd;
- Maatregelen die het waterschap neemt om de betreffende crisis te bestrijden;
- Partners die betrokken zijn bij de bestrijding van de crisis;
- Gerelateerde documenten die van toepassing zijn op de betreffende crisis.

Doel en doelgroep

Dit plan heeft als doel om:

- met de beschikbare middelen en menskracht zorg te dragen dat crises op een zo effectief en efficiënt mogelijke wijze worden aangepakt;
- met de beschikbare middelen en menskracht zorg te dragen dat zo min mogelijk schade aan mens, milieu, financiën en het vertrouwen in het waterschap wordt toegebracht en daarmee de bedrijfsvoering te borgen.

Dit bestrijdingsplan is opgesteld voor de volgende doelgroepen:

- De eigen crisisorganisatie. Zij maakt gebruik van het crisisbestrijdingsplan inclusief bijlagen en data.
- De netwerkpartners. Zij kunnen kennisnemen van het bestrijdingsplan om inzicht te krijgen in de organisatie, de risico's, de scenario's en de maatregelen;

1. Risicoanalyse

De bedrijfscontinuïteit van het waterschap is in hoge mate afhankelijk van het goed functioneren van het digitale landschap. Als er verstoringen in dat landschap optreden, heeft dat vrijwel direct gevolgen voor de continuïteit. Die gevolgen van verstoringen kunnen betrekking hebben op elke kerntaak van het waterschap.

De werkelijke oorzaak van een digitale verstoring is vaak pas in een later stadium van de crisis of zelfs pas na de crisis te constateren. Risico's zijn daarom vanuit verschijningsvorm omschreven, niet vanuit de oorzaak. Binnen het digitale landschap zijn de risico's terug te brengen naar twee hoofdrisico's waaronder verschillende verschijningsvormen vallen: uitval van dienstverlening én ongeautoriseerde digitale toegang. Eén verschijningsvorm heeft een daadwerkelijk andere crisisaanpak en kan ook los als risico worden gezien. Om die reden is het onderwerp datalek in een apart hoofdstuk opgenomen.

1.1. Uitval dienstverlening

Uitval van dienstverlening die toegang tot data en systemen aantast, tast ook de bedrijfsvoering van ons waterschap aan. Uitval met een kleine omvang wordt opgepakt vanuit de lijn. Wanneer uitval de gehele organisatie treft of een vitaal proces verstoort, is het gevolg hiervan een groot risico voor de bedrijfscontinuïteit. Het waterschap kan hierdoor haar taken niet of onvolledig uitvoeren en eventuele afspraken, wettelijke en andere verplichtingen niet nakomen. Wanneer uitval optreedt, is dit hoofdzakelijk zonder opzettelijk handelen opgetreden.

Enkele oorzaken van uitval van dienstverlening zijn:

- Problemen met software of hardware;
- Menselijke fouten;
- Cybercrime – zie hoofdstuk *Ongeautoriseerde toegang.*

Bijbehorende verschijningsvormen kunnen zijn:

- Meldingen van het niet functioneren van systemen;
- Geen toegang tot data;
- Automatische signalering vanuit software of hardware;
- Visuele signalering.

1.2. Ongeautoriseerde digitale toegang

Ongeautoriseerde digitale toegang wordt ook wel cybercrime genoemd. Dit is een vorm van criminaliteit waarbij een ICT-systeem of de informatie die daardoor wordt verwerkt, het doelwit is. Cybercrime is een vorm van menselijk handelen, waarbij opzettelijke manipulatie van een ICT-systeem of digitale informatie plaatsvindt. De veroorzaker kan zowel een losse actor, een samenwerkingsverband of ook een statelijke actor zijn. De gevolgen van cybercrime kunnen variëren van het permanent verdwenen documenten, naar het trekken van onjuiste conclusies door gemanipuleerde kerngegevens tot aan het hinderen, verstoren of stilvallen van reguliere werkzaamheden.

Enkele oorzaken van cybercrime zijn:

- Hacken; op afstand inbreken in computers of computernetwerken via internet. De doelen variëren van vandalisme tot georganiseerde misdaad;
- Ramsomware; met gijzelingssoftware blokkeren van een computer of de bestanden op een computer om die tegen betaling van losgeld weer vrij te geven;

- (Spear)phishing; via e-mail, sms of nep-websites vissen naar beveiligingscodes om daarmee misbruik te maken van een beveiligd ICT-systeem;
- Malware; kwaadwillende software die gebruikt wordt om een ICT-systeem te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot een ICT-systeem.
- Zeroday aanval; een beveiligingslek waarin je letterlijk nul dagen hebt om de fout op te lossen. Bij een aanval misbruikt een hacker deze kwetsbaarheid.

Bijbehorende verschijningsvormen kunnen zijn:

- Meldingen van het niet functioneren van systemen;
- Meldingen van externe autoriteiten;
- Aantasting informatie:
    - Data is gelekt;
    - Data is gegijzeld;
    - Data is verloren;
- Visuele signalering.

1.3. Datalek

Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens. Of het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. Hierdoor kunnen betrokken personen schade leiden. Een datalek kan een risico veroorzaken voor de bescherming van de persoonlijke levenssfeer van betrokkenen. Een betrokkene kan bijvoorbeeld slachtoffer worden van fraude, afpersing of kan benadeeld worden door diefstal of andere schadelijke gedragingen.

Het afdoende beveiligen van de verwerking van persoonsgegevens is een wettelijke verplichting op grond van de Algemene Verordening Gegevensbescherming (AVG). Het niet voldoen aan de wettelijke verplichting tot beveiligen kan leiden tot sancties in de vorm van boetes opgelegd door de Autoriteit Persoonsgegevens (AP). Ook aan het niet tijdig melden van een datalek bij de AP, kunnen sancties verbonden zijn.

Ook loopt het waterschap het risico op imago-, reputatie- en relatieschade, als blijkt dat het onzorgvuldig omgaat met persoonsgegevens.

Enkele oorzaken van een datalek zijn:

- Menselijke fout; door kwijtgeraakte gegevens, onvoldoende beveiligingsmaatregelen of verkeerd verzonden gegevens;
- Moedwillig handelen; fysieke en digitale diefstal;
- Brand, overstroming of andere natuurramp in een datacentrum.

2. Algemeen

In dit hoofdstuk wordt in zijn algemeenheid gekeken naar opschaling, crisisorganisatie, maatregelen, netwerk en documenten. In de verdere hoofdstukken wordt per beschreven risico benoemd welke aanpak en bijzonderheden specifiek voor deze risico's gelden. Dit hoofdstuk kan ook worden benut wanneer het betreffende risico niet is benoemd in een van de verdere hoofdstukken.

De beschrijving van de standaard crisisorganisatie staat in het *Crisisplan* van Waterschap Rivierenland. Kenmerkend voor een digitale verstoring crisis is:

- De grote snelheid waarmee de crisis zich manifesteert;
- De crisis treft zelden alleen het digitale domein;
- De impact op de continuïteit is vaak groot;
- De bron/oorzaak kan lastig te achterhalen zijn;
- De zeer korte besluitvormingstijd;
- Het mogelijke intensieve en langdurige herstel.

Dit maakt een flexibele organisatie en werkwijze noodzakelijk.

2.1 Opschaling

2.1.1 Melding en alarmering

Iedere crisis begint bij een melding, storing of waarschuwing. Deze kunnen via de onderstaande kanalen binnen komen:

- Melding van een collega die Servicedesk benaderd, al dan niet vanuit een escalatie;
- Melding vanuit detectiesystemen;
- Melding vanuit leveranciers;
- Melding vanuit CERT-WM;
- Melding vanuit externen, zoals burgers, pers enzovoort.

Al deze meldingen worden verwerkt in TOPDESK. De opschalingslijn loopt als volgt: meldingen in TOPDESK met een prioriteit 1 worden met de teamleider besproken. Eventueel escaleert dit verder wanneer dat nodig is. De teamleider schat de omvang, impact en duur van de storing in en informeert de 3Ce en het afdelingshoofd IDT daarover. De 3Ce adviseert vervolgens de secretaris-directeur om op te schalen.

Er kan ook gekozen worden voor een gecoördineerde aanpak, zonder opschaling. Dit kan bij een ernstig incident of een dreigende situatie waarbij coördinatie nodig is, maar die nog niet ernstig genoeg is om op te schalen. Zo is er wel een gestructureerde aanpak en wordt de eerste informatie in het crisismanagementsysteem LCMS gedeeld voor het geval de situatie verder escaleert. Dit wordt besloten door een adviseur van de 3Ce in samenspraak met de betrokkenen. Hierna wordt een kernteam geformeerd. Let hierbij wel op dat het geen opschaling is en het bijbehorende beleid dus ook niet van toepassing is.

2.1.2 Opschalingscriteria

Bij een opschaling door een digitale verstoring gaat het altijd om een stapeling van impact, urgentie en oplossingssnelheid. Onder impact wordt verstaan, anders dan bij de Service Level Agreement (SLA's), een aantasting van:

- Vertrouwelijkheid (privacy en datalekken);
- Beschikbaarheid (data en systemen);
- Integriteit (kwaliteitstandaarden en wettelijke eisen).

Daarnaast wordt een digitale verstoring pas een probleem wanneer de urgentie om een probleem op te lossen en de oplossingssnelheid niet overeenkomt met elkaar. Wanneer hier een te groot verschil tussen zit en de impact is hoog, dan dient er opgeschaald te worden.

Algemene criteria voor opschalen zijn:

- Coördinatiefase 1, indien sprake is van een situatie waarvan de impact zich beperkt tot het waterschap, de maatregelen hoofdzakelijk bestaan uit het monitoren van en informeren over de situatie en/of de afhandeling binnen de bevoegdheden van een afdelingshoofd liggen;
- Coördinatiefase 2, indien sprake is van een situatie waarvan de impact zich uitstrekt tot buiten het waterschap, de maatregelen ingrijpen op het reguliere functioneren van het waterschap en/of de afhandeling binnen de bevoegdheden van een directeur liggen;
- Coördinatiefase 3, indien sprake is van een situatie waarbij bestuurlijke coördinatie met andere overheden aan de orde is, de situatie zich richting de buitenwereld keert, de maatregelen afwijken van het reguliere beleid van het waterschap en/of inzet van bestuurlijke bevoegdheden noodzakelijk is voor de afhandeling.

2.2 Crisisorganisatie

De opbouw en het functioneren van de crisisorganisatie staat in het *Crisisplan*. De afwijkingen op het crisisplan voor een digitale verstoringscrisis staan in deze paragraaf beschreven.

2.2.1. ***Duo vorming Hoofd ACW – Teamleider***

Nog sterker dan bij water gerelateerde crises is kennis van ICT noodzakelijk om goede besluiten te kunnen nemen tijdens een crisis digitale verstoring. Om deze reden is het hoofd ACW, ook het afdelingshoofd IDT. Is dit niet mogelijk, dan worden er duo's gevormd. Een duo bestaat uit een ander hoofd ACW samen met een teamleider IDT (of afgevaardigde), waarvan de taken van het team niet het leidend onderwerp zijn van de crisis. Het hoofd ACW stuurt het proces en heeft het mandaat om besluiten te nemen en de betreffende teamleider is verantwoordelijk voor het informeren en verduidelijken van de ICT gerelateerde onderwerpen richting het hoofd ACW. Samen zorgen zij voor de leiding en coördinatie van de crisis.

2.2.2. ***Samenstelling crisisteam algemeen***

De basis van het ACW is als volgt:

- Hoofd ACW;
- Informatiecoördinatoren (ICO's);
- Strategisch adviseur communicatie;
- Adviseur crisisbeheersing.

Deze basis vult het hoofd aan met:

- Leidinggevenden van de direct betrokken afdelingen;
- Medewerkers met kennis op het gebied van de betreffende crisis.

Het hoofd ACW kan ervoor kiezen andere medewerkers aan het team toe te voegen. Bijvoorbeeld: als juridische aspecten een rol spelen, is het gewenst om een jurist toe te voegen.

Het kan gebeuren, dat een digitale verstoring crisis leidt tot een water gerelateerde crisis, bijvoorbeeld een grote verstoring bij een gemaal. In het *Crisisplan* is vastgelegd dat bij twee verschillende type crises die gerelateerd zijn aan elkaar twee ACW-teams die gelijktijdig naast elkaar actief zijn. Onderlinge afstemming vindt dan plaats in het Waterschap Operationeel Team (WOT). De operationeel leider kan kiezen om hier één team van te maken.

2.2.3. ***Veldteams***

Bij een digitale verstoring zijn net als bij een water gerelateerde crisis veldteams bezig. Deze staan onder leiding van de betreffende teamleider als zogenoemd hoofd veld. De hoofden veld van de betreffende veldteams zijn onderdeel van het ACW. Aan een veldteam wordt ook een ICO-veld toegevoegd.

2.2.4. ***Omgang outsourcingpartner***

Het digitale landschap van Waterschap Rivierenland is grotendeels ondergebracht bij een outsourcingpartner. Verstoringen bij beide partijen hebben vrijwel altijd effect op elkaar. Bij een verstoring binnen Waterschap Rivierenland fungeren de medewerkers van de outsourcingpartner als een veldteam. Dit veldteam valt onder het hoofd veld van het team ICA, mits hierin bewust een andere keuze wordt gemaakt. De outsourcingpartner kan aanwezig zijn bij overleggen van het ACW, WOT, WBT, maar alleen als dit niet leidt tot belangenverstrengeling.

Uitgewerkte samenwerkingsafspraken zijn beschreven in bijlage 3.

2.3 Maatregelen

De maatregelen zijn afhankelijk van de crisis en vooraf niet vast te leggen. Wel zijn er algemene stappen te benoemen met betrekking tot de aanpak van de crisis en digitale verstoring crisis.

De volgende stappen zijn te onderscheiden voor een algemene crisisaanpak:

1. Beeldvorming. Breng feiten, genomen maatregelen en betrokken partners in beeld;
2. Oordeelsvorming. Bepaal welke scenario's (mogelijke ontwikkelingen van de crisis) zich kunnen voordoen, welke knelpunten er zijn voor het waterschap, welke mogelijke oplossingen er zijn en wat voorkeursoplossing is;
3. Besluitvorming. Besluit tot het nemen van bestrijdingsmaatregelen die voortvloeien uit de voorkeursoplossing. De maatregelen hebben achtereenvolgens betrekking op het beheersbaar maken van de crisis (stabiliseren), het bestrijden van oorzaken en gevolgen en tot slot het herstellen van de normale situatie;
4. Informeren. De betrokken netwerkpartners informeren over de stappen 1, 2 en 3 voor het afstemmen van de maatregelen en het samenwerken bij het nemen van de maatregelen;
5. Communiceren over de crisis extern naar burgers en media, intern naar medewerkers en bestuurders.

De volgende maatregelen zijn te nemen bij een digitale verstoring:

1. Zet apparatuur niet uit die aanstaat (afhankelijk van de situatie);
2. Verbreek de netwerk/internetverbinding (afhankelijk van de situatie);
3. Stel back-ups veilig of blokkeer toegang tot back-up; (afhankelijk van situatie)
4. Zet de automatische back-up uit; (afhankelijk van situatie)
5. Stel logfiles veilig; (afhankelijk van situatie)
6. Informeer interne organisatie;

7. Documenteer genomen stappen (logboek);
8. Eventueel een externe specialist inschakelen (afhankelijk van de situatie).

2.4 Netwerkpartners

De betrokken netwerkpartners zijn geheel afhankelijk van de betreffende crisis. Specifiek voor digitale veiligheid zijn de volgende netwerkpartners van belang.

2.4.1. *Nationaal Cyber Security Centrum (NCSC)*

Het NCSC is permanent bezig met het voorkomen van en reageren op cyberaanvallen. Het NCSC functioneert als nationaal Computer Emergency Response Team (CERT) en werkt samen met andere CERT's in binnen en buitenland. Dus ook met het CERT-WM dat er specifiek voor waterschappen is.

Het NCSC biedt 24 uur per dag, 7 dagen per week een meldpunt voor cyberincidenten. Meldingen lopen voor het waterschap via het CERT-WM. Dit meldpunt is voor de rijksoverheid en voor aanbieders van vitale infrastructuren. Het NCSC adviseert, ondersteund en levert zo nodig assistentie op locatie voor beheerders van vitale infrastructuur, waartoe de waterschappen ook behoren.

2.4.2. *CERT-WM*

Het CERT-WM is een samenwerking tussen 21 waterschappen en Rijkswaterstaat om de operationele informatiebeveiliging binnen de waterketen te versterken. Zij zijn de contactpartij vanuit waterschappen richting het NCSC. In samenwerking worden (inter)nationale adviezen over kwetsbaarheden in ICT-systemen geleverd aan waterschappen. Ook ondersteunen zij waterschappen tijdens crisis met adviezen op afstand.

2.4.3. *Autoriteit Persoonsgegevens*

De Autoriteit Persoonsgegevens is opgericht en aangewezen als toezichthouder op de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet AVG (UAVG). De Autoriteit Persoonsgegevens is een zelfstandig bestuursorgaan met een eigen rechtspersoonlijkheid. Een organisatie is verplicht datalekken direct te melden bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. Het melden van een datalek verloopt via de Functionaris Gegevensbescherming van ons waterschap.

2.4.4. *Politie*

Indien Waterschap Rivierenland slachtoffer is geworden van cybercrime, dienen wij aangifte of melding te doen bij de politie in de regio. Dat kan via 0900-8844 of op een politiebureau. Belangrijk is dat er geen digitale sporen verloren gaan. Een aantal vormen van cybercriminaliteit kan ook online gemeld worden.

2.4.5. *Outsourcingpartner*

De outsourcingpartner van Waterschap heeft het grootste deel van het digitale landschap van Waterschap Rivierenland in zijn beheer. Verstoringen bij beide partijen heeft vrijwel altijd effect op elkaar. De outsourcingpartner is ook verantwoordelijk voor onderliggende partijen voor dataverbindingen en firewalls. Ook hebben zij een Security Operation Centre van waaruit ondersteuning geboden kan worden.

Uitgewerkte samenwerkingsafspraken zijn beschreven in bijlage 3. Waaronder uitgewerkte afspraken rondom prioritering bij storingen outsourcingpartner.

2.4.6. ***Applicatieleverancier***

2.5 Documenten

In de documentenbank *J:\Calamiteitenzorg Bestrijding\2. Documentenbank* staan de onderstaande documenten die gerelateerd zijn aan dit plan.

- In het *Crisisplan van Waterschap Rivierenland* staat beschreven hoe het waterschap zich organiseert voor het bestrijden van crises.
- In de standaardprocedure *Melding en alarmering* is vastgelegd hoe dat proces verloopt, inclusief een processchema.
- In de standaardprocedure *Op- en afschaling* staat hoe dat is geregeld, met een uitgebreid processchema.
- De standaardprocedure voor *Informatiemanagement* bevat een gedetailleerde beschrijving en uitgewerkt schema van de wijze waarop relevante informatie tot stand komt, wordt vastgelegd en wordt gedeeld.
- In de standaardprocedure *Leiding en coördinatie* is vastgelegd hoe besluiten tot stand komen. Dit is ook in een schema weergegeven.
- De *Telefoonkaart* bevat de namen voor de rollen in de crisisorganisatie, inclusief de plaatsvervangers en de contactgegevens.
- De *Bestuurlijke netwerkkaarten crisisbeheersing.* Er zijn voor diverse crisissituaties bestuurlijke netwerkkaarten opgesteld met daarin bevoegdheden, maatregelen en aandachtspunten van en voor betrokken overheden. Deze kaarten zijn in beheer bij het Nederlands Instituut Publieke Veiligheid en ontsloten via de website van dat instituut: www.nipv.nl.

3. Uitval dienstverlening

Onder uitval dienstverlening verstaan wij een aantasting van toegang tot data en systemen die hoofdzakelijk zonder opzettelijk handelen is opgetreden.

3.1 Opschalingscriteria

3.1.1 Melding en alarmering

Een medewerker die een ICT-storing signaleert, meldt die storing binnen kantoortijd bij de ICT-Servicedesk en buiten kantoortijd (uitsluitend voor peilbeheer, zuiveringsbeheer en crisisbeheersing) bij de wachtdienst van de ICT.

Indien de ICT-Servicedesk of wachtdienst ICT de desbetreffende ICT-storing niet kan verhelpen, dan melden ze dat bij de teamleider ICA (ICT en Applicatiebeheer). De teamleider schat de omvang, impact en duur van de storing in en informeert de 3Ce en het afdelingshoofd IDT daarover. De 3Ce adviseert vervolgens de secretaris-directeur om op te schalen.

3.1.2 Opschaling

- Coördinatiefase 1, dienstverlening valt organisatiebreed uit, maar de vitale processen kunnen blijven draaien.
- Coördinatiefase 2, dienstverlening valt (organisatiebreed) uit en dreigt vitale processen te raken.
- Coördinatiefase 3, dienstverlening valt (organisatiebreed) uit en heeft een dusdanige impact dat vitale belangen in het geding zijn en bestuurlijke afstemming noodzakelijk is.

3.2 Crisisorganisatie

De opbouw van het crisisteam staat omschreven in hoofdstuk 2.2 van dit plan. Bij uitval van dienstverlening moet er gedacht worden aan de volgende deskundigen in het ACW en WOT:

ACW:

- Service- en contractmanager
- Service Delivery Manager
- Information Security Officer (ISO) en/of Operational Security Officer (OSO KA of PA)

WOT:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)

3.3 Maatregelen

De maatregelen zijn sterk afhankelijk van de aard en omvang van de uitval. Hieronder staat een algemene aanpak beschreven:

- Analyseer de getroffen partijen (netwerk, leveranciers, getroffen interne medewerkers)
- Bepaal de effecten van de uitval voor de getroffen partijen en wettelijke verplichtingen
- Neem contact op met de getroffen partijen
- Los de problemen op

3.4 Netwerk

- Outsourcingpartner; uitgewerkte samenwerkingsafspraken zijn beschreven in bijlage 3;
- Leveranciers van hard/software
- Getroffen partijen.

3.5 Documenten

De *Telefoonkaart* bevat de namen voor de rollen in de crisisorganisatie, inclusief de plaatsvervangers en de contactgegevens.

4. Ongeautoriseerde digitale toegang

Onder ongeautoriseerde digitale toegang verstaan wij een vorm van menselijk handelen, waarbij opzettelijke manipulatie van een ICT-systeem of digitale informatie plaatsvindt.

4.1 Opschalingscriteria

4.1.1 Melding en alarmering

Een melding van ongeautoriseerde digitale toegang kan op meerdere manieren binnen komen:

- Via ICT Servicedesk;
- Via Operational Security Officers (OSO)
- Via CERT-WM, het signaal wordt doorgegeven aan de Operational Security Officers (OSO), de Information Security Officer (ISO), de teamleider ICA en de ICT Servicedesk.
- Via monitoringsysteem
- Via leverancier
- Via applicatiebeheerder
- Via outsoursingpartner

Een melding van ongeautoriseerde digitale toegang wordt voorgelegd aan de teamleider ICA en de ISO. Zij beoordelen de melding en schatten de impact in en informeren het afdelingshoofd IDT, de Chief Information Security Officer (CISO), de Chief Information Officer (CIO) en de 3Ce. Voor deze beoordeling raadplegen zij zonnodig leveranciers van beveiligingssoftware. De 3Ce adviseert vervolgens de secretaris-directeur om op te schalen.

Buiten kantoortijd belt een medewerker de Meldkamer van Waterschap Rivierenland, die de situatie voorlegt aan de wachtdienst van de outsoursingpartner. Wanneer blijkt dat er het waterschap een direct risico loop belt de Meldkamer de wachtdienst 3Ce. Die daarna op zijn beurt de secretaris directeur adviseert om op te schalen.

4.1.2 Opschaling

Criteria voor opschaling zijn:

- Coördinatiefase 1, er is alleen een dreiging maar nog geen merkbare gevolgen of delen van systeem zijn niet te gebruiken, het betreft applicaties met een beperkte impact op functioneren van de organisatie;
- Coördinatiefase 2, het gehele systeem is niet te gebruiken wat ook impact heeft op kerntaken van het waterschap zoals peilbeheer en zuiveringsbeheer;
- Coördinatiefase 3, door aantasting van het gehele systeem kan het waterschap niet voldoen aan wettelijke verplichtingen. Hierbij zijn het imago, de wettelijke aansprakelijkheid en de bereikbaarheid voor derden in het geding. De gevolgen van de cybercrime zijn zichtbaar voor derden en het waterschap dient daarover verantwoording af te leggen.

4.2 Crisisorganisatie

De opbouw van het crisisteam staat omschreven in hoofdstuk 2.2 van dit plan. Bij ongeautoriseerde digitale toegang moet er gedacht worden aan de volgende deskundigen in het ACW en WOT:

ACW:

- Information Security Officer (ISO)
- Jurist
- Service- en contractmanager
- Service Delivery Manager
- Operational Security Officer(s) (OSO KA/PA)
- Functionaris Gegevensbescherming (FG) bij inbreuk op privacy

WOT:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)

4.3 Maatregelen

Bij cybercrime die niet door het CERT-WM of het NCSC is gemeld, informeert de ISO direct de contactpersoon van het CERT-WM.

Bij cybercrime die niet door het CERT-WM is gemeld, doet het hoofd ACW direct aangifte bij de politie.

Het bestrijden van de gevolgen van cybercrime omvat op hoofdlijnen de volgende maatregelen. Deze maatregelen zijn contextafhankelijk.

Stel de volgende vragen bij de prioritering en het uitvoeren van maatregelen:

- Waar is toegang toe geweest?
- Wanneer is dit geweest?
- Is er een digitaal spoor?

Maatregelen:

1 Een snelle analyse op basis van de melding om te bepalen wat er aan de hand is.
2 Het ICT-systeem geheel of gedeeltelijk afsluiten. Dit kan bijvoorbeeld zijn door de internetverbinding los te koppelen en onderdelen uit te schakelen. Het kan ook nodig zijn om alle toegang in een keer dicht te zetten (met uitzondering van admin) of alle wachtwoorden ongeldig te laten zijn waardoor deze gewijzigd moeten worden. De teamleider ICA of PAR is bevoegd om hiertoe te beslissen;
3 Stel back-ups veilig en zet de automatische back-up uit;
4 Stel logfiles veilig en documenteer genomen stappen in een logboek;
5 Alle medewerkers informeren die getroffen zijn door de cybercrime of die daar hinder van kunnen ondervinden;
6 Een impactanalyse uitvoeren om de gevolgen en effecten van de cybercrime in beeld te brengen;
7 De oorzaak van de cybercrime onderzoeken. Het hiaat in de beveiliging opsporen en dichten. Kwaadwillende software opsporen en verwijderen;
8 Een herstelplan opstellen om het ICT-systeem en de digitale informatie weer in oorspronkelijke staat terug te brengen;
9 Het herstelplan uitvoeren door onderdelen van het ICT-systeem gefaseerd terug te brengen, te testen en vrij te geven voor gebruik;
10 De medewerkers informeren dat de ICT-systeem en digitale informatie weer te gebruiken is.

4.4 Netwerk

De volgende partners zijn mogelijk betrokken bij ongeautoriseerde digitale toegang:

- Outsourcing partner; uitgewerkte samenwerkingsafspraken zijn beschreven in bijlage 3;
- Leveranciers die niet onder outsourcing partner vallen;
- Leveranciers met eigen hard- en software of SAAS-toepassingen;
- CERT-WM (Computer Emergency Response Team voor Water Management, alarmeren het waterschap bij een cybercrime, worden door het waterschap geïnformeerd bij cybercrime, geven advies aan het waterschap bij cybercrime);
- NCSC (Nationaal Cyber Security Centrum, alarmeren via CERT-WM);
- Politie voor aangifte

4.5 Documenten

De *Telefoonkaart* bevat de namen voor de rollen in de crisisorganisatie, inclusief de plaatsvervangers en de contactgegevens.

De *Bestuurlijke netwerkkaarten crisisbeheersing, kaart 21b - cybersecurity*. Hierin staan de bestuurlijke bevoegdheden en bijbehorende maatregelen inzake cybersecurity

5. Datalek

Onder datalek verstaan wij toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie.

5.1 Opschalingscriteria

5.1.1 Melding en alarmering

Meldingen van een (veronderstelde) datalek kunnen van derden komen of van medewerkers van Waterschap Rivierenland. Meldingen komen in kantoortijd binnen via STROOM (Melding datalek) of via het e-mailadres privacy@wsrl.nl. De melding komt altijd binnen bij de Privacy Officers en de Functionaris Gegevensbescherming (privacy team). Een van de leden van het privacy team neemt

Een melding van een datalek bij de ICT-Servicedesk wordt ter beoordeling doorgegeven naar de teamleider ICA. De teamleider ICA beoordeelt de melding, schat de impact in en informeert de FG. Als de FG niet beschikbaar is, is de Privacy Officer de vervanger.

De FG beoordeeld de melding:

- Grote waarschijnlijkheid dat er geen sprake van verlies of onrechtmatige verwerking
  - Geen opschaling;
  - FG registreert het incident in Privacy log.
- Datalek kan worden afgedaan met enkel een melding aan de Autoriteit Persoonsgegevens (AP):
  - Geen opschaling;
  - Melding bij AP.
- Verlies of onrechtmatige verwerking:
  - FG consulteert het hoofd IDT en de 3Ce. De 3Ce adviseert vervolgens de secretaris-directeur om op te schalen.

Buiten kantoortijd belt een medewerker de Meldkamer van Waterschap Rivierenland, die de situatie meld via STROOM of het e-mailadres privacy@wsrl.nl. Wanneer blijkt dat het waterschap een direct risico loopt, belt de Meldkamer de wachtdienst 3Ce. De wachtdienst van de 3Ce consulteert de FG. De wachtdienst 3Ce belt daarna de secretaris directeur en adviseert om op te schalen.

5.1.2 Opschalingscriteria

Het dreigingsniveau dat van een datalek uitgaat, bepaalt de FG op basis van onderstaande scoretabel. De tabel geeft een richtlijn. Er kan door specifieke omstandigheden worden afgeweken.

Impact > **V Factor**	**Beperkt** **score 1**	**Gemiddeld** **score 3**	**Groot** **score 5**	**Zeer groot** **score 10**
Het aantal betrokkenen waarvan persoonsgegevens gelekt is	1 tot 10 betrokkenen	10 tot 100 betrokkenen	100 tot 1.000 betrokkenen	Meer dan 1.000 betrokkenen
De hoeveelheid gegevens die gelekt is	Eén of enkele niet-gevoelige persoonsgegevens	Meerdere niet-gevoelige persoonsgegevens	Een uitgebreide set niet-gevoelige persoonsgegevens	Volledige set persoonsgegevens per betrokkene

	per betrokkene	per betrokkene	per betrokkene	
De aard en gevoeligheid van de gelekte gegevens	Geen bijzondere of gevoelige persoonsgegevens			Gevoelige en/of bijzondere persoonsgegevens
De mate van toegankelijkheid van de gelekte informatie	Toegankelijk voor één of enkele onbevoegde personen	Toegankelijk voor een beperkte groep (< 100) onbevoegde personen	Toegankelijk voor een grote groep (> 100) onbevoegde personen	Publiek toegankelijk
De waarschijnlijkheid dat betrokkenen benadeeld worden door misbruik van de gegevens	Zeer onwaarschijnlijk	Onwaarschijnlijk maar niet uit te sluiten	Waarschijnlijk	Zeer waarschijnlijk
De actuele situatie van de crisis	De kwetsbaarheid is niet meer aan de orde		De kwetsbaarheid duurt (waarschijnlijk) nog voort	De kwetsbaarheid duurt nog voort

De FG adviseert het hoofd ACW en de secretaris-directeur over het opschalen aan de hand van de volgende criteria, waarbij de score de optelsom van de scores op de zes factoren is. Dit geeft een indicatie om op te schalen.

- Geen opschaling, score lager dan of gelijk aan 20;
- Coördinatiefase 1, score 21 tot en met 40, en/of het datalek beperkt zich tot eigen organisatie;
- Coördinatiefase 2, score 41 tot en met 50, en/of het datalek rijkt tot buiten de eigen organisatie;
- Coördinatiefase 3, score hoger dan 50, en/of het datalek heeft media-aandacht en/of bestuurlijke betrokkenheid.

Aan de hand van dit adviseert de FG het hoofd IDT en de 3Ce. De 3Ce adviseert vervolgens de secretaris-directeur om op te schalen.

5.2 Crisisorganisatie

De opbouw van het crisisteam staat omschreven in hoofdstuk 2.2 van dit plan. Bij een datalek moet er gedacht worden aan de volgende deskundigen in het ACW en WOT:

ACW:

- Functionaris Gegevensbescherming (FG)
- Privacy Officer (jurist)
- Information Security Officer (ISO)

WOT:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)

5.3 Maatregelen

De maatregelen zijn afhankelijk van de aard en ernst van het datalek, maar omvatten in iedere geval het volgende:

- Het opsporen en dichten van het datalek;
- Onderzoek naar de exacte aard, omvang en ernst van het datalek;
- Het documenteren van het datalek:
    - Het invullen van het registratieformulier “inventarisatie en melding datalek”;
    - Het registreren van het datalek in het incident- en dataregister.
- (Indien nodig) Het melden van het datalek bij de Autoriteit Persoonsgegevens binnen 72 uur na ontdekking van het lek;
- (Indien nodig of gewenst) Het melden van het datalek aan betrokkenen:
    - Verwerkers van persoonsgegevens;
    - Getroffen personen;
- Het nemen van schade beperkende of herstellende maatregelen;
- Het doen van aangifte indien van toepassing;
- Het bepalen van de communicatiestrategie;
- De gevolgen voor de bedrijfscontinuïteit bepalen;
- Het nemen van preventieve maatregelen ter voorkoming van herhaling.

5.4 Netwerk

De volgende partners zijn mogelijk betrokken bij datalekken:

- De Autoriteit Persoonsgegevens;
- Verwerkers van persoonsgegevens (zoals salarisadministratie, Arbodienst);
- Politie (bij aangifte);
- Leveranciers van (beveiliging)software;
- Het Cyber Emergency Response Team Waterschappen (CERT-WM)
- Nationaal Cyber Security Centrum (NCSC).

5.5 Documenten

De *Telefoonkaart* bevat de namen voor de rollen in de crisisorganisatie, inclusief de plaatsvervangers en de contactgegevens.

De *Algemene Verordening Gegevensbescherming (AVG)* vormt de wettelijke grondslag voor het omgaan met persoonsgebonden gegevens.

De meldplicht voor datalekken is vastgelegd in de AVG, artikel 33 en 34. De Artikel 39 Werkgroep (samenwerkende toezichthouders) heeft de “Richtsnoer voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679” uitgegeven.

Actuele informatie over de meldplicht datalekken is te vinden op de website van de Autoriteit Persoonsgegeven:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

Bijlagen

1. Cybersecurity woordenboek
2. Het landschap van crisisbeheersing
3. Afspraken outsourcingpartner (volgt later)

Vanwege de verschillende type en grootte bestanden is ervoor gekozen de bijlagen niet op te nemen in dit document. De bijlagen zijn opgeslagen in de map: J:\Calamiteitenzorg Bestrijding\2. Documentenbank\2.02 Calamiteitenbestrijdingsplannen.