Handleiding cyberincidenten: voorbereiding, respons en herstel

DEN

Juni 2026

Handleiding cyberincidenten: voorbereiding, respons en herstel

In 2023 liet DEN het onderzoek Cyber Security Scan uitvoeren. Daaruit bleek dat 3 op de 10 culturele organisaties tussen 2020-2023 te maken had met een cybercrime incident. De impact kan ingrijpend zijn: denk aan diefstal van bezoekersgegevens, het platleggen van ticketing-systemen, of zelfs sabotage van klimaatsystemen waardoor kwetsbare collecties in gevaar komen. Zulke incidenten hebben niet alleen financiële consequenties, maar kunnen leiden tot reputatieschade van de organisatie en het afnemen van het vertrouwen van publiek, subsidieverstrekkers en partners. Naast cybersecurity is digitale weerbaarheid – het vermogen om niet alleen aanvallen te voorkomen, maar ook snel te reageren en te herstellen – daarom essentieel.

Om deze digitale weerbaarheid in de praktijk te brengen, helpt een incident- en herstelplan je organisatie om voorbereid te zijn op een cyberincident. Het combineert afspraken over de aanpak van een incident (Incident Response Plan) met afspraken over het herstel van systemen, data en processen (Disaster Recovery Plan). Door vooraf vast te leggen wie wat doet en welke stappen moeten worden gezet, kun je sneller handelen, de impact beperken en de organisatie sneller terugbrengen naar de normale situatie.

Voor wie is deze handleiding bedoeld?

Middelgrote en kleinere culturele instellingen hebben vaak beperkte middelen en geen eigen IT-afdeling. Toch is digitale weerbaarheid geen luxe, maar een noodzaak. Met een heldere en praktische handleiding kan iedere organisatie, ook met vrijwilligers en beperkte expertise, zich voorbereiden op een cyberincident en de schade beperken.

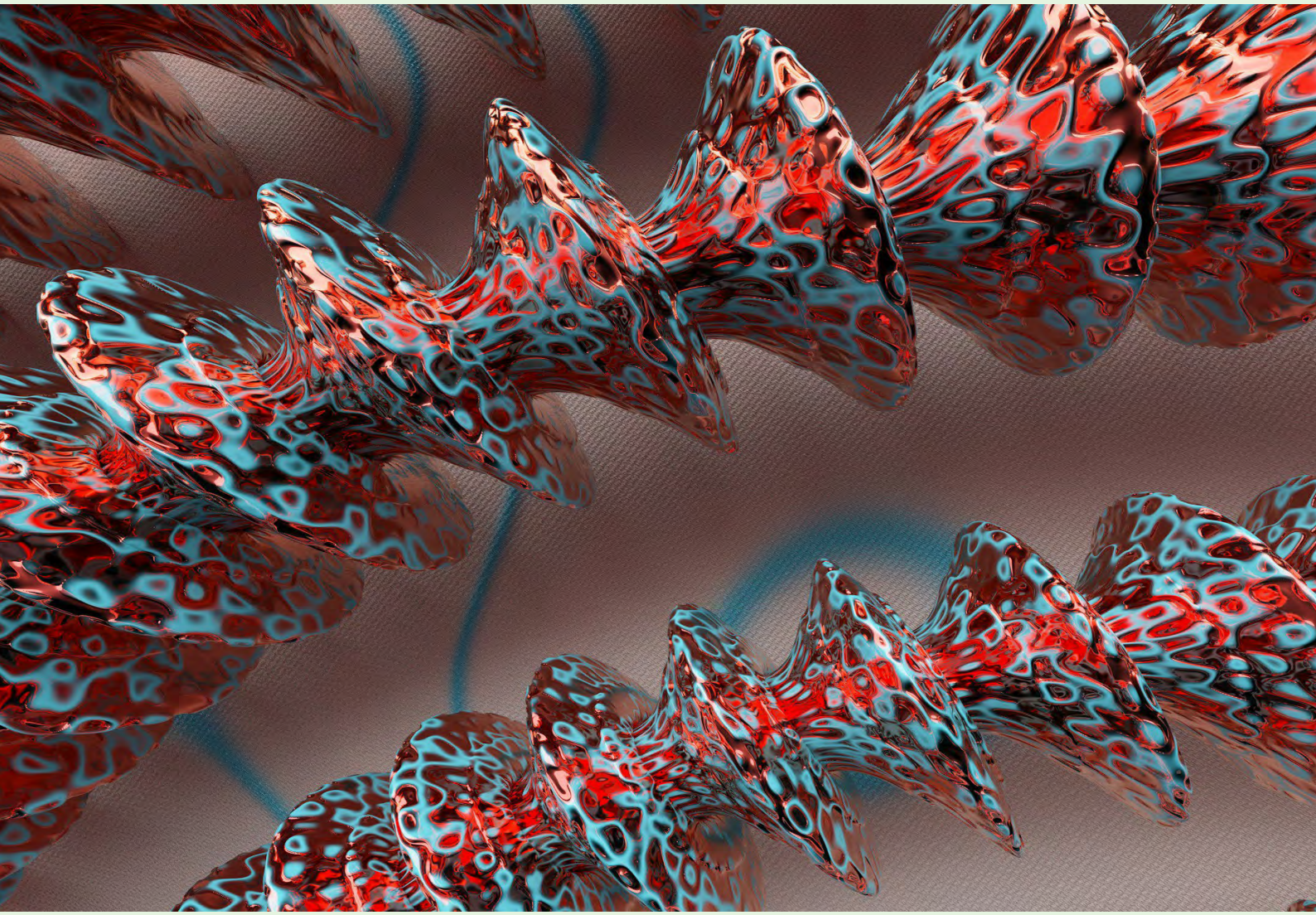
Wat biedt deze handleiding?

Dit document ondersteunt je bij het uitwerken van een beknopt incident- en herstelplan, zodat je direct en effectief kunt reageren zodra zich een probleem voordoet. Geen ingewikkelde theorie, maar concrete stappen en tips, gebaseerd op bestaande kaders van Nationaal Cyber Security Centrum (NCSC) en Kennisinstituut cultuur & digitale transformatie (DEN), aangevuld met sectorspecifieke aandachtspunten. Zo ben je voorbereid op wat écht telt: het beschermen van je organisatie, je publiek en je unieke collectie.

De handleiding neemt je stap voor stap mee naar het opstellen van een compleet incident- en herstelplan. Het proces bestaat uit drie delen:

1. **Continuïteit: voorbereid zijn op verstoring;**
2. **Respons: handelen tijdens een incident;**
3. **Herstel: terug naar normaal.**

Deze handleiding biedt een praktische eerste stap voor het versterken van de digitale weerbaarheid van culturele organisaties. De handleiding bevat voorbeeldtabellen, formats en handreikingen die helpen bij het opstellen van een eigen incident- en herstelplan. De inhoud is ondersteunend van aard en vraagt altijd om maatwerk en eigen afwegingen.



Inhoudsopgave

1 Continuïteit: voorbereid zijn op verstoring (Prevent)

Doel = zorgen dat de organisatie kan blijven functioneren of snel kan overschakelen bij een incident.

1.1. Basis op orde: voorbereidende werk

Voordat je een incident- en herstelplan opstelt, is het van belang dat de fundamenten van digitale veiligheid in je organisatie op orde zijn. Door eerst dit voorwerk te doen, leg je een sterke basis en verzamel je essentiële input voor het plan.

Stappen voorafgaand aan opstellen van incident- en herstelplan:

- Stap 1 > **Doe de** CyberVeilig Check: Een goed startpunt is de online CyberVeilig Check voor cultuur. Deze korte scan (ontwikkeld door het NCSC (voormalig DTC) i.s.m. DEN) geeft inzicht in hoe goed jouw organisatie op dit moment beschermd is en genereert een actieplan met basismaatregelen. Het doorlopen van deze check (ca. 10 minuten) zorgt ervoor dat je meteen eventuele grote gaten in je cyberbeveiliging ziet en kunt aanpakken, vaak simpele dingen die je vandaag nog kunt doen. Denk aan het inschakelen van multifactor authenticatie, het maken van backups, etc. Het resultaat van de check vormt een lijst met aanbevelingen die je idealiter oppakt terwijl je parallel aan je incident- en herstelplan werkt.

- Stap 2 > **Gebruik de** Checklist Digitale Veiligheid: DEN heeft een praktische 8-punten checklist gepubliceerd (februari 2024) om organisaties direct minder kwetsbaar te maken. Loop deze checklist na binnen je organisatie, het zijn veelal “quick wins” die je parallel aan of vóór het uitwerken van het plan kunt realiseren.

- Stap 3 > **doorloop het** Stappenplan Cyberveiligheid: De kern daarvan bestaat uit vier aandachtspunten:

  - Identificeer je “kroonjuwelen”.
  - Bepaal je risicoacceptatie.
  - Implementeer beheersmaatregelen.
  - Voorzie in monitoring, training en evaluatie.

  Deze vier punten vormen samen de basis van een volwassen cyberweerbaarheid. Door dit stappenplan te doorlopen krijg je al een hoop input voor je eigen incident- en herstelplan: je weet wat je belangrijkste assets zijn, welke specifieke risico’s jullie lopen, en welke voorzieningen er al zijn of nog getroffen moeten worden.

1.2. Kaders en standaarden voor de voorbereiding

Hanteer bestaande standaarden: Naast praktische checks en quick wins is het raadzaam om je te baseren op bestaande, breed geaccepteerde standaarden voor informatiebeveiliging en continuïteit. Deze standaarden helpen structuur aan te brengen, lacunes inzichtelijk te maken en maatregelen systematisch te borgen. Tenzij contractueel voorgeschreven zijn de standaarden in principe niet verplicht om te hanteren.

- **ISO/IEC 27001 (Informatiebeveiliging)** [1]
  Toegevoegde waarde: biedt een integraal raamwerk voor het beheersen van informatiebeveiligingsrisico's (technisch, organisatorisch en menselijk).
  Toepassing: gebruik de norm als referentiekader om beleid, rollen, maatregelen en risicoafwegingen te toetsen. Een volledige certificering is niet noodzakelijk.

- **SO 22301 (Business Continuity Management)** [2]
  Toegevoegde waarde: richt zich specifiek op bedrijfscontinuïteit en het vermogen om essentiële processen te blijven uitvoeren of snel te herstellen.
  Toepassing: de uitgangspunten (zoals kritieke processen, hersteltijden en scenario's) kunnen rechtstreeks input leveren voor het incident- en herstelplan.

- **CIS Controls** [3]
  Toegevoegde waarde: een praktische en technisch concrete set basismaatregelen ('what works') die helpt bij prioriteren naast vaak abstractere normen.
  Toepassing: toepasbaar als checklist of nulmeting om te bepalen waar directe verbeteringen mogelijk zijn, vooral op IT- en operationeel niveau.

Voor meer informatie zie:

[1] ISO/IEC 27001:2022 – Information security management systems
[2] ISO 22301:2019 – Business continuity management systems
[3] CIS Critical Security Controls & CIS Critical Security Controls Version 8.1

In de volgende stappen ga je het incident- en herstelplan voor jouw organisatie vormen, op basis van de input die je al verzameld hebt. Het eindresultaat is een compact document dat jouw crisisteam kan gebruiken tijdens een cyberincident.

1.3. Kroonjuwelen en risico's

Noteer als eerst de belangrijkste processen/systemen en hun belang, potentiële incidenten/risico's, de kans/impact inschatting en de beheersmaatregelen. Orden deze op herstelprioriteit. Gebruik de identificatie van je kroonjuwelen en risicoacceptatie uit het Stappenplan Cyberveiligheid als basis.

Onderstaande Tabel 1 maakt inzichtelijk waar de grootste risico's liggen en vormt de basis voor de volgende stappen.

Pas de kolommen aan indien nodig (bijv. toevoeging "Huidige kwetsbaarheden") en orden de processen op volgorde van prioriteit (van hoog naar laag) voor herstel.

Tabel 1: Kroonjuwelen & risicoacceptatie met fictieve voorbeelden

Proces/ systeem	Belang	Mogelijke incidenten/ risico's	Impact/ gevolg [4]	Kans [5]	Beheersmaatregel
Ticketing en reservingssysteem	*Essentieel voor kaartverkoop*	*Ransomware, DDoS-aanval*	*G*	*M*	*MFA, back-ups*
CRM-/donateurs-database	*Bevat persoonsgegevens van donateurs, bezoekers en leden*	*Datalek, phishing, ongeautoriseerde toegang*	*G*	*H*	*Autorisatiebeheer*
Digitaal collectiebeheersysteem	*Kernregistratie van collectie*	*Ransomware*	*G*	*L*	*Back-ups*

[4] Impact/gevolg: de invloed van het incident/risico wanneer het optreedt. G= Groot: direct maatregelen treffen. M= Middel: vraagt aandacht, enige maatregelen zijn raadzaam. K= Klein: goed om te weten, geen directe maatregelen nodig.
[5] Kans: waarschijnlijkheid dat het betreffende risico optreedt: H = Hoog (>50% kans dat het gebeurt). M = Middel (10-50% kans dat het gebeurt). L = Laag (<10% kans dat het gebeurt).

1.4. Business Impact Analyse (BIA)

Voer een BIA uit op de kroonjuwelen. Voor elk kroonjuweel bepaal je: Hoe snel moet dit weer werken na een incident? En hoeveel data of vooruitgang mogen we maximaal verliezen? In cybersecurity jargon: stel per essentieel proces de Recovery Time Objective (RTO) en Recovery Point Objective (RPO) vast.

Bijvoorbeeld: "Bij uitval van het ticketsysteem tijdens openingstijden: binnen 4 uur moeten we weer tickets kunnen verkopen (RTO = 4 uur), en we accepteren maximaal 1 dag aan ticketdata verlies (RPO = 24 uur)."

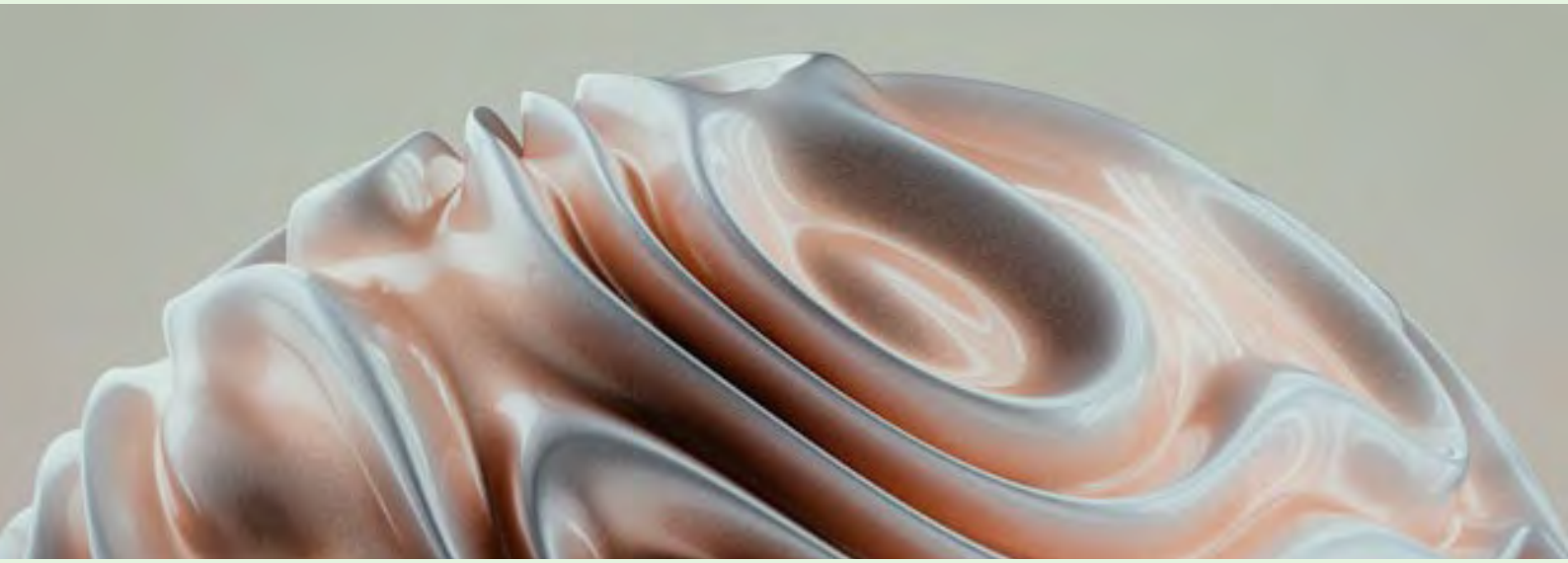
Deze RTO/RPO-waarden dwingen tot een realistische planning en om na te denken over noodmaatregelen: als je zulke doelen stelt, moet je er voorzieningen voor hebben (denk aan backups, offlineticketmethodes, etc.). De BIA geeft ook een prioriteitsvolgorde: misschien komt uit de analyse dat eerst het klimaatsysteem hersteld moet worden (binnen 2 uur), daarna de ticketing (binnen 4 uur) en daarna pas andere zaken. Leg deze volgorde en doelen vast – dit vormt het hart van je herstelstrategie.

Tip: betrek bij het opstellen van RTO/RPO ook externe verwachtingen, bijv. subsidie-eisen of verzekeringspolissen die bepaalde maxima stellen aan downtime of data recovery.

Tabel 2 wordt ingevuld in de volgorde van prioriteit van herstel.

Tabel 2: Business Impact Analyse met fictieve voorbeelden

Proces/ systeem	Max. uitvaltijd (RTO)	Max. data/ werkverlies (RPO)	Herstelmaatregel	Noodmaatregel
Ticketingsysteem	*4 uur*	*24 uur*	*Herstel vanuit back-up of uitwijkomgeving, ondersteuning leverancier inschakelen*	*Handmatige gastenlijsten, kaartverkoop aan balie, reserveringen via telefoon/e-mail*
Website	*8 uur*	*48 uur*	*Website herstellen vanuit back-up*	*Communicatie via sociale media en/of nieuwsbrief*
Financiële administratie	*24 uur*	*24 uur*	*Herstel boekhoudsysteem en financiële data vanuit back-up*	*Handmatige registratie van facturen en betalingen*



1.5. Organisatorische paraatheid: rollen, verantwoordelijkheden en bereikbaarheid

Stel vast wie het crisisteam vormt bij een ernstig incident. Zorg dat duidelijk is wie wat moet en mag doen in geval van een calamiteit en werk dit uit in een overzichtelijke tabel. Print deze lijst en voeg hem toe aan het plan. Zo kan het crisisteam snel gealarmeerd worden zodra nodig:

✔ Benoem rollen en verantwoordelijkheden per teamlid (bij kleine organisaties zullen mensen meerdere petten ophebben). Typische rollen zijn: een crisisleider (bv. de directeur), een IT-verantwoordelijke (bv. externe IT-partner of tech-vrijwilliger), iemand voor communicatie/pr (voor woordvoering naar publiek) en iemand die notuleert/het overzicht houdt. Leg voor elke rol vast wat de verantwoordelijkheid is.

✔ Noteer de contactgegevens van de verschillende leden van het crisisteam.

✔ Schrijf ook de beperkingen van hun autoriteit in geval van een incident op.

✔ Bepaal de uitgavelimieten (bijvoorbeeld als er materialen moeten worden aangekocht).

✔ Maak ook een bellijst met namen en 24/7 bereikbaarheid van de teamleden, én van belangrijke externe contacten (IT-leverancier, CERT Meldpunt, politie, eventueel sectorloket).

De rol van crisisleider kan over twee personen verdeeld worden: besluitvormer en procesvoorzitter/procescoördinator. De besluitvormer is degene die formeel opschaalt en mandaat heeft om beslissingen te nemen. De procesvoorzitter is degene die de vergadering voorzit aan de hand van de BOB-methodiek. Deze methodiek is effectief voor crisisbesluitvorming en staat voor:

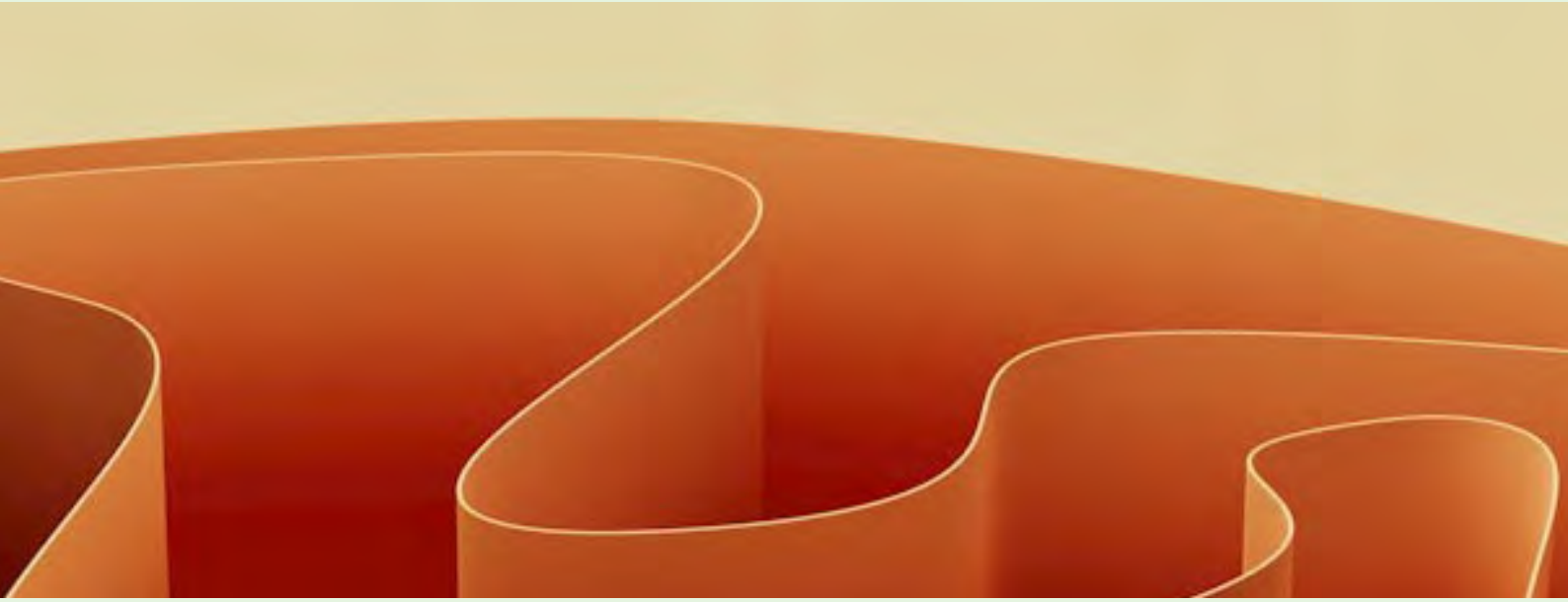
- **Beeldvorming: Wat zijn de feiten?**
  - Wat weten we al?
  - Welke informatie mist er nog?
  - Zitten de juiste mensen aan tafel?
- **Oordeelsvorming: Wat proberen we te bereiken?**
  - Wat is het doel van het crisisteam?
  - Wat verwachten we op basis van de bekende informatie?
  - Aan welke voorwaarden moeten besluiten voldoen?
  - Wat zijn de knelpunten en risico's? Wat kan eraan gedaan worden?
- **Besluitvorming: Wat gaan we doen?**
  - Wat wordt er besloten?
  - Wie is verantwoordelijk?
  - Wanneer is het volgende overleg en welke acties zijn dan afgerond?

Indien het incident- en herstelplan wordt geactiveerd, dient het crisisteam ingeschakeld te worden zoals vastgelegd in tabel 3.

Tabel 3: Rollen en verantwoordelijkheden kerngroep met fictieve voorbeelden

Rol	Verantwoordelijkheden	Beperkingen van autoriteit in geval van incident	Uitgavelimieten
Crisisleider	*Leidt incidentrespons, besluitvorming en escalatie*	*Geen betaling van losgeld zonder bestuursbesluit*	*Tot €10.000 noodmaatregelen*
IT-verantwoordelijke	*Technische analyse, isoleren systemen, herstel coördineren*	*Geen externe communicatie namens organisatie*	*Tot €5.000 technische ondersteuning*
Communicatie / PR	*Interne en externe communicatie, persvragen*	*Geen uitspraken over oorzaak zonder bevestiging crisisteam*	*Tot €2.500 communicatievoorzieningen*
Notulist/planner	*Logboek, actielijst, planning en besluiten vastleggen*	*Geen operationele beslissingen*	*Geen zelfstandig budget*

Rol	Naam	Telefoon	E-mail
Crisisleider	...	...	...
...	...	...	...



Naast de vaste kerngroep van het crisisteam, kunnen er op basis van het type incident rollen uit de flexibele schil toegevoegd worden.

Tabel 4: Rollen en verantwoordelijkheden flexibele schil met fictieve voorbeelden

Rol	Verantwoordelijkheden	Beperkingen van autoriteit in geval van incident	Uitgave-limieten
Applicatiebe-heerder	*Beheer ticketing-, CRM- en collec-tiesystemen*	*Geen wijzigingen zonder afstemming IT-verantwoordelijke*	*Tot €2.500*
Functioneel beheerder	*Ondersteunt gebruikers en kri-tische processen*	*Geen technische beveiligingsmaatregel-en zelfstandig doorvoeren*	*Tot €1.500*
HR / Vrijwilliger Coördinator	*Coördinatie medewerkers, vrijwil-ligers en bereikbaarheid*	*Geen externe communicatie*	*Tot €1.000*
Bedrijfsvoering / Financiën	*Financiële impact, contracten en verzekeringen*	*Geen strategische besluiten zonder crisisleider*	*Tot €5.000*
Juridische me-dewerker	*AVG, datalekmeldingen, leveranci-erscontracten*	*Geen publieke communicatie*	*Tot €2.500*
Externe onders-teuning	*Incident response*	*Alleen op opdracht crisisteam*	*Volgens over-eenkomst*
Bestuurlijk aanspreekpunt	*Contact met Raad van Toezicht of bestuur*	*Geen operationele aansturing*	*Niet van toe-passing*

Rol	Naam	Telefoon	E-mail
Applicatiebeheerder	...	...	...
...	...	...	...

Maak met de kerngroep en de flexibele schil ook afspraken omtrent bereikbaarheid en beschikbaarheid:

- Op welke manier wordt het crisisteam ingeschakeld buiten werktijden?
- Is er een piketstructuur?
- Worden vakanties met elkaar afgestemd?
- Wie zijn de plaatsvervangers in geval van verlof of verzuim?

2 Respons: handelen tijdens een incident (Respond)

Doel = snel orde scheppen, schade beperken en regie houden in de eerste fase van het incident.

2.1. Wanneer treedt het plan in werking?

Definieer helder waar het incident- en herstelplan betrekking op heeft: de **scopebepaling**. Gebruik de eerder in kaart gebrachte kroonjuwelen en risicoacceptatie als basis: welke systemen/processen zijn cruciaal voor de bedrijfscontinuïteit en worden dus in het plan behandeld?

Bijvoorbeeld: je besluit dat het incident- en herstelplan zich richt op de continuïteit van ticketing, klimaatbeheer en financiële administratie na een cyberincident, omdat uit je analyse bleek dat dit de kern is van jullie organisatie.

Leg ook eventuele randvoorwaarden vast: geldt het plan alleen voor cyberaanvallen, of ook voor IT-storingen door bijvoorbeeld brand of stroomuitval? Kortom, bepaal en documenteer waarop dit plan van toepassing is en wat er niet in meegenomen wordt. Dit voorkomt onduidelijkheid tijdens crises en helpt focussen op wat het belangrijkst is.

Beschrijf in het **activatieplan** expliciet wanneer het incident- en herstelplan in werking treedt en hoe de opschaling verloopt.

Bijvoorbeeld: "Als systemen langer dan 30 minuten platliggen door onbekende oorzaak, of bij vermoeden van hacker/datalek, activeer het crisisteam."

Noteer dat de crisisleider (of diens vervanger) het besluit neemt tot activeren. Schrijf stap voor stap op:

- Wie moet gebeld worden (volg de bellijst);
- Waar het team samenkomt (fysiek of via een alternatief kanaal, bijvoorbeeld als Teams uit de lucht is);
- Welke beslissingen eerst genomen moeten worden (bijv. systemen tijdelijk uitzetten om verdere schade te voorkomen?).

Deze informatie zorgt dat er geen discussie is op een crisismoment over "vallen we hier al onder het plan of niet": de drempel is gedefinieerd.

2.2. Het eerste uur: incidentrespons

Deze sectie beschrijft het stappenplan direct na ontdekking van een cyberincident. Het is feitelijk het “eerste uur”-plan om de chaos te structureren: signaleren → alarmeren → schade beperken → informeren.

1. **Signalen erkennen & verzamelen:** Medewerkers merken op dat er iets mis is. Noteer objectief welke signalen op een incident wijzen. Deze signalen worden gerapporteerd aan de crisisleider. *Bijvoorbeeld: onverklaarbare computerstoringen, ransomware melding op scherm, vreemde e-mails of inlogpogingen.*

2. **Escaleren naar IT-experts:** De crisisleider neemt contact op met de externe IT-partner of een cybercrisisteam. Bespreek samen de aard en ernst van het incident en besluit wat er wel en vooral niet moet gebeuren. *Bijvoorbeeld: systemen offline halen om verdere schade te stoppen.*

3. **Schade beperken en alternatieven zoeken:** De noodmaatregelen worden ingeschakeld om de continuïteit te waarborgen.

4. **Meldingen bij toezichthouders:**
   (a) AP: een ernstig datalek moet binnen 72 uur gemeld worden
   (b) NCSC: als je onder de Cyberbeveiligingswet (Cbw) valt, ben je verplicht om significantie incidenten te **melden bij het NCSC via deze link**. Alle organisaties kunnen vrijwillig melden.

5. **Houdt een incidentlogboek** bij, zie Tabel 6: Incidentlogboek als voorbeeld.

Tabel 5: Bellijst IT-experts

IT-expert/Organisatie	Telefoonnummer
...	...
...	...

Tabel 6: Incidentlogboek met fictieve voorbeelden

Tijdstip	Actie	Uitgevoerd door
09:05	*Melding ontvangen dat ticketingsysteem niet bereikbaar is*	*Frontoffice medewerker*
09:15	*Server geïsoleerd van netwerk*	*IT-verantwoordelijke*
10:00	*Crisisteam bijeengeroepen en eerste impactanalyse uitgevoerd*	*Crisisleider*

2.3. Communicatie tijdens het incident

Informeer de juiste interne en externe stakeholders. Gebruik conceptboodschappen om externe stakeholders te informeren. In tabel 7 staan richtlijnen voor de kernboodschap van de communicatieberichten. Verwijs in het incident- en herstelplan naar de locatie van de conceptboodschappen.

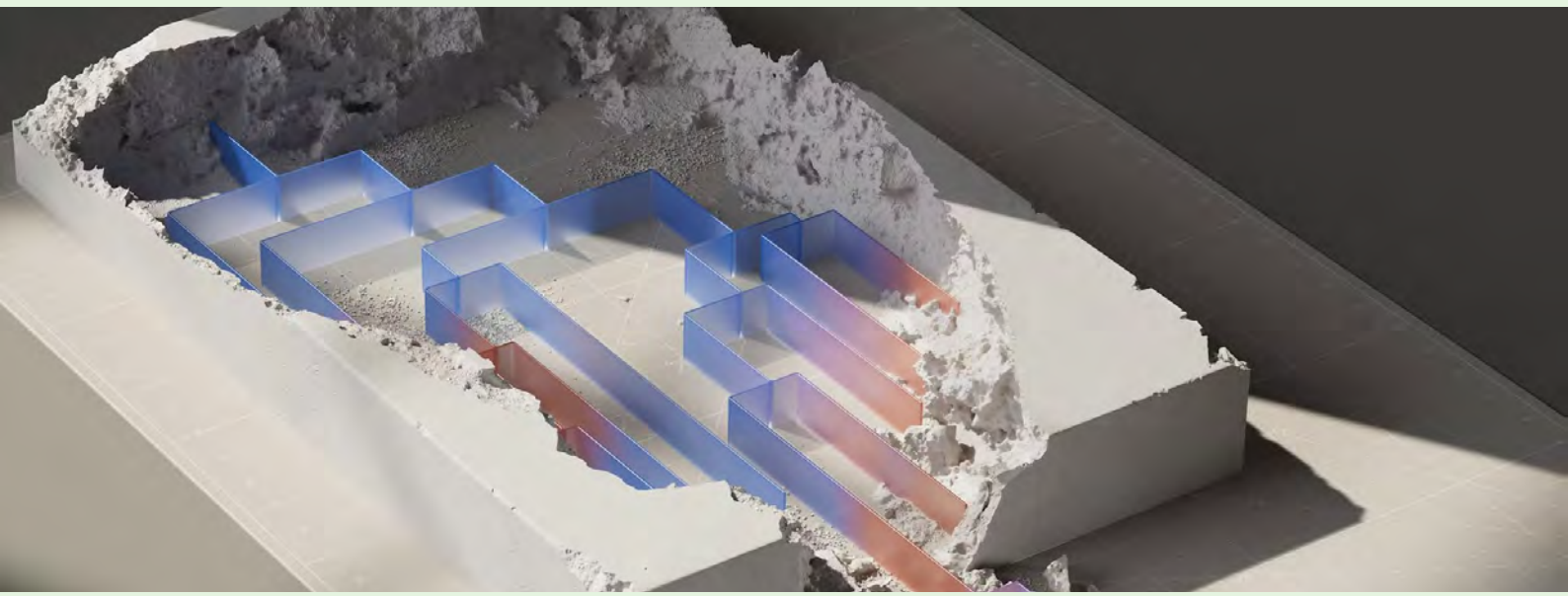
Tabel 7: Kernboodschap communicatie

Onderdelen kernboodschap
Beschrijf kort de situatie
Toon empathie
Beschrijf wat het betekent voor de lezer en wat de lezer wel/niet kan doen
Beschrijf kort de acties vanuit de organisatie
Geef aan waar vragen kunnen worden gesteld
Geef aan wanneer, waar en hoe men een volgende update kan verwachten

2.4. Wettelijke meldingen en verantwoording

Vergeet niet de wettelijke kant mee te nemen in het incident- en herstelplan. Bij een ernstig datalek moet bijvoorbeeld binnen 72 uur de Autoriteit Persoonsgegevens gewaarschuwd worden. Sommige organisaties vallen onder incidentmeldplicht[6] . Noteer in het plan wie verantwoordelijk is voor het doen van welke meldingen en binnen welke termijn.

[6] De meldplicht geldt voor alle organisaties die volgens de Cbw een belangrijke of essentiële entiteit is. Doe de Zelfevaluatie om erachter te komen of jouw organisatie onder de richtlijn valt, of doorloop **deze flowchart**. Vrijwillige meldingen kunnen worden gedaan door elke organisatie.



2.5. Kaders en standaarden voor incidentrespons

Voor de inrichting van de incidentrespons tijdens een digitaal incident kan aansluiting worden gezocht bij bestaande internationale kaders. Deze standaarden bieden houvast voor rolverdeling, eerste acties, besluitvorming en vastlegging, maar zijn niet wettelijk verplicht en vereisen geen formele certificering

- **ISO/IEC 27001 – Beheer van informatiebeveiligingsincidenten**[7]
  Toegevoegde waarde: beschrijft hoe beveiligingsincidenten gestructureerd worden herkend, opgevolgd, geëscaleerd en geregistreerd. De norm benadrukt besluitvorming onder tijdsdruk en het leren van incidenten.

- **NIST SP 800-34 – Contingency Planning Guide**[8]
  Toegevoegde waarde: biedt een concreet en praktisch kader voor het omgaan met verstoringen van informatiesystemen, inclusief noodmaatregelen, tijdelijke work-arounds en besluitvorming in de eerste fase van een incident.

- **CIS Critical Security Controls – Incident Response & Management**[9]
  Toegevoegde waarde: vertaalt incidentrespons naar concrete, uitvoerbare stappen zoals escalatie, rollen, contactlijsten en herstelacties.

Voor meer informatie zie:

[7] ISO/IEC 27001:2022 - Information security management systems
[8] SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems | CSRC
[9] CIS Critical Security Controls

3 Herstel: terug naar normaal (Recover)

Doel = gecontroleerd herstellen, leren van het incident en weerbaar verdergaan.

3.1. Herstelprocedures en draaiboeken

Werk per kritisch systeem of scenario uit hoe te herstellen. Dit is het meest operationele deel van het plan en resulteert in handleidingen voor noodgevallen. Idealiter maak je voor de top-3 risico-scenario's een beknopt draaiboek.

Bijvoorbeeld: bij het scenario ransomware aanval staan er stappen in zoals "loskoppelen netwerk, externe expert bellen, back-up van nacht X terugzetten zodra virus verwijderd is". Bij het scenario uitval website/tickets staan er stappen in zoals "IT bellen, overschakelen op offline verkoop (Excel-lijst bij entree), communicatie op sociale media 'wij ondervinden technische problemen'".

Hierbij is het belangrijk de bestaande backup- en uitwijkmogelijkheden te benoemen: waar staan de backups en hoe worden deze teruggezet, is er een reserve-laptop beschikbaar, kun je tijdelijk op pen en papier verder, et cetera. Ook alle relevante documentatie moet paraat zijn: voeg in bijlage een up-to-date inventaris van accounts, systemen, leverancierscontracten, locaties van backups, licentiecodes, enz. toe.

Kortom, je schrijft een degelijk maar beknopt herstelplan-draaiboek uit, dat precies past op jullie organisatie. Dit plan bevat wie er in actie komen, wat ze moeten doen, en in welke volgorde, om de organisatie zo snel mogelijk weer operationeel te krijgen na een incident.

Let op: Vanwege de gevoelige informatie in het incident- en herstelplan, is het van belang dat het adequaat beveiligd wordt, bijvoorbeeld door een wachtwoord in te stellen op een digitaal document. Update wijzigingen direct in alle kopieën. Bewaar een papieren kopie in een kluis voor noodgevallen.

3.2. Documentatie en bijlagen

Hieronder zijn voorbeeldtabellen om voor de top-3 risico-scenario's concrete herstelprocedures uit te werken. Deze stappen moeten door het crisisteam gevolgd worden indien het risico-scenario zich voordoet.

Tabel 8: Top-3 risico-scenario's met fictieve voorbeelden [10]

Scenario 1: ransomware in ticketing- en kassaomgeving

Stappen	Uitvoeren door	Benodigde middelen / back-ups	Communicatie tijdens herstel [11]
1 Ticketingsysteem isoleren	*IT-verantwoordelijke*	*Netwerktoegang, noodprocedure*	*Intern melding medewerkers*
2 Impact bepalen en herstel voorbereiden	*IT-verantwoordelijke & leverancier*	*Back-ups*	*Intern update crisisteam*
3 Herstel vanuit back-up	*Leverancier*	*Back-up en herstelplan*	*Extern update bezoekers over dienstverlening*
4 ...	*...*	*...*	*...*

Scenario 2: datalek van bezoekers- en donateursgegevens

Stappen	Uitvoeren door	Benodigde middelen / back-ups	Communicatie tijdens herstel
1 Verdachte toegang blokkeren	*IT-verantwoordelijke*	*Toegangsbeheer*	*Interne update directie*
2 Omvang datalek vaststellen inclusief risicobeoordeling	*IT-verantwoordelijke + juridische medewerker*	*Logbestanden, overzicht betrokken systemen, AVG-richtlijnen*	*Interne melding medewerkers*
3 Betrokkenen informeren	*Communicatie*	*Standaard communicatie boodschap*	*Externe communicatie (bezoekers, donateurs, AP)*
4 ...	*...*	*...*	*...*

Scenario 3: Uitval digitaal collectiebeheersysteem

Stappen	Uitvoeren door	Benodigde middelen / back-ups	Communicatie tijdens herstel
1 Vaststellen oorzaak en omvang uitval	*Applicatiebeheerder*	*Monitoring en logbestanden*	*Interne update*
2 Omschakelen naar noodprocedures	*Functioneel beheerder*	*Werkinstructies*	*Interne update*
3 Systeem herstellen vanuit back-up	*IT-verantwoordelijke & leverancier*	*Back-ups*	*Externe update richting gebruikers*
4 ...	*...*	*...*	*...*

[10] De voorbeelden zijn fictief en dienen uitsluitend ter illustratie. De beschreven scenario's en maatregelen zijn niet volledig of uitputtend.
[11] Moet er intern of extern gecommuniceerd worden over het voorvallen van het incident en eventuele updates?

Documenten als bijlagen:
- Contactgegevens van leveranciers
- Systemen- en applicatie inventarisatie inclusief locaties
- Licenties
- Netwerkbeschrijvingen en – schema's
- Leverancierscontracten en Service Level Agreements

3.3. Evaluatie, testen en actualisatie

Het is belangrijk je incident- en herstelplan regelmatig te testen, te evalueren en indien nodig aan te passen. Dit kan bijvoorbeeld het geval zijn wanneer je vaststelt dat de gedefinieerde procedures niet de gewenste resultaten opleveren of de afgesproken RTO en RPO overschrijden.

Naast testen is het jaarlijks updaten van je incident- en herstelplan ook belangrijk. Een incident- en herstelplan met verouderde contact- en contractinformatie is schadelijk omdat er kostbare tijd verloren zal gaan op cruciale momenten. Updaten is ook van belang wanneer je nieuwe activiteiten of diensten aan je organisatie toevoegt. Het loont dan om af te wegen welke impact deze nieuwe activiteiten en of diensten op je incident- en herstelplan hebben en in welke mate het plan aangepast moet worden. Belangrijk is om een medewerker met een bepaalde functie eigenaar te maken van het incident- en herstelplan zodat dit proces goed geborgd wordt.

Voeg aan de voorkant van het incident- en herstelplan een overzicht met de informatie uit tabel 9 toe.

Tabel 9: Versiebeheer met fictieve voorbeelden

Versie	Datum	Gewijzigd door	Omschrijving van de wijzigingen
0.1	*14-07-2026*	*Projectteam*	*Eerste concept incident- en herstelplan*
0.2	*21-07-2026*	*ICT-coördinator*	*Risicoscenario's toegevoegd*
1.0	*01-09-2026*	*Directeur-bestuurder*	*Definitieve vaststelling*

Beschrijf de datum vanaf wanneer deze versie van het incident- en herstelplan geldt en waar het document bewaard wordt.

Bijvoorbeeld:
- In papieren vorm in de kluis op de volgende locaties: [**locaties**].
- In digitale vorm op volgende locaties: [**locatie op computer**].

Beschrijf tevens wie eigenaar is van het document. Het is de verantwoordelijkheid van deze medewerker om minstens eenmaal per jaar te controleren of het DRP aangepast dient te worden. Daarnaast moet het DRP na elk incident geëvalueerd worden.

3.4. Kaders en standaarden voor herstel en continuïteit

Voor het gecontroleerd herstellen na een incident en het structureel verbeteren van de weerbaarheid kan gebruik worden gemaakt van bestaande internationale standaarden. Deze standaarden kunnen helpen om herstel gecontroleerd en herhaalbaar uit te voeren, en zorgen ervoor dat het incident- en herstelplan een levend document blijft dat aansluit bij de daadwerkelijke inrichting van de organisatie. Deze kaders bieden houvast voor herstelprocedures, uitwijk, prioritering en evaluatie, zonder dat toepassing wettelijk verplicht is of formele certificering vereist.

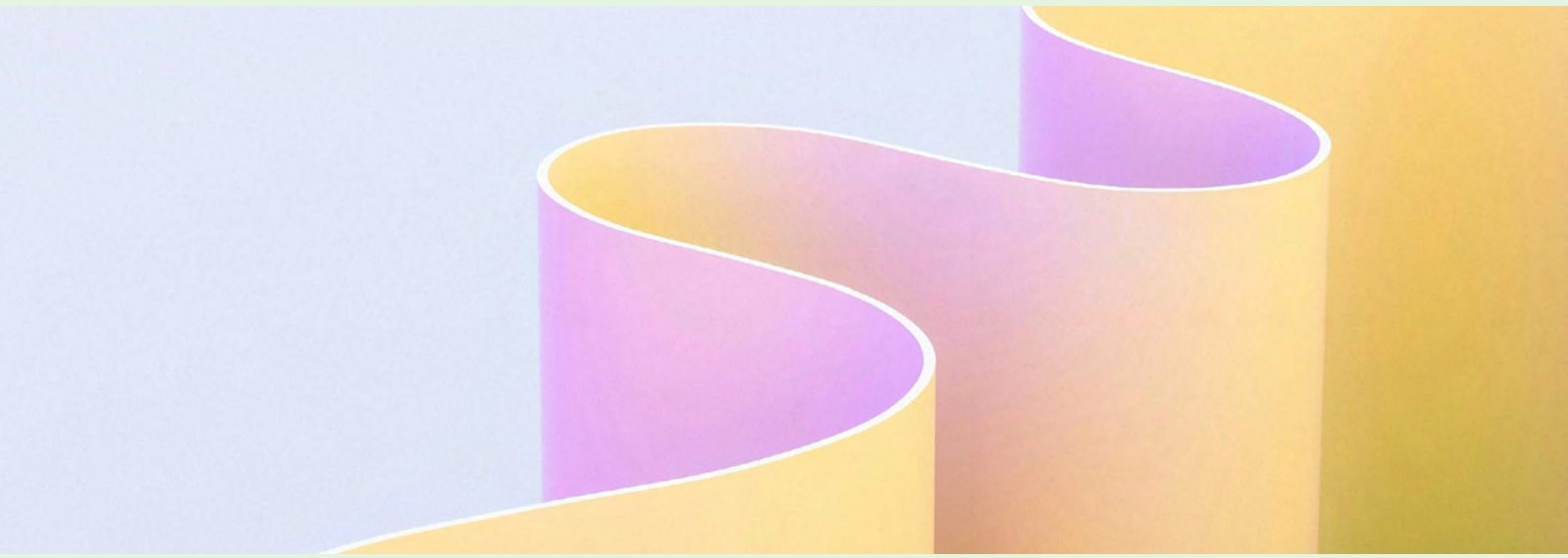
- **ISO/IEC 27031 – ICT Readiness for Business Continuity** [12]
  Toegevoegde waarde: richt zich op het borgen van de beschikbaarheid en het herstel van ICT-voorzieningen ter ondersteuning van businesscontinuïteit. De standaard vertaalt continuïteitsdoelstellingen naar concrete ICT-maatregelen, zoals back-ups, uitwijkvoorzieningen, herstelvolgorde en RTO/RPO, en verbindt deze expliciet aan kritieke bedrijfsprocessen.

- **ISO 22301 – Business Continuity Management**[13]
  Toegevoegde waarde: biedt een integraal kader voor het herstellen van kritische processen en het borgen van continuïteit na een incident. De norm legt nadruk op testen, evalueren en continu verbeteren.

- **NIST SP 800-34 – Contingency Planning Guide**[14]
  Toegevoegde waarde: biedt een praktisch stappenplan voor herstel na uitval van informatiesystemen, inclusief tijdelijke work-arounds en terugkeer naar normaal bedrijf.

Voor meer informatie zie:

[7] ISO/IEC 27031:2025 - Cybersecurity — Information and communication technology readiness for business continuity
[8] ISO/IEC 27001:2022 - Information security management systems
[9] NIST 800-34 Contingency Planning: A Practical Guide to Resilience - Codific & CIS Critical Security Controls



4 Van handleiding naar praktijk

4.1. Routekaart implementatie

Het opstellen van een incident- en herstelplan hoeft geen langdurig proces te zijn. Onderstaand tijdpad laat zien hoe je in ongeveer 10 weken deze handleiding kunt doorlopen en een werkend plan op poten zet. Uiteraard kun je het tempo aanpassen aan je eigen agenda, maar dit schema geeft een idee van de opeenvolging:

- **Week 1: Start en bewustwording:** Stel een kernteam samen. Communiceer intern dat jullie aan de slag gaan met cyberveiligheid en licht het waarom toe.
- **Week 2: Quick scans & basis op orde:** Voer de CyberVeilig Check en de Checklist Digitale Veiligheid uit en bespreek de resultaten. Pak direct 1-2 quick wins op (bijv. updates uitvoeren, een bellijst opstellen).
- **Week 3-4: risicoanalyse sessie:** Organiseer een korte sessie (1-2 uur) met het kernteam en eventueel andere sleutelpersonen. Breng tijdens deze sessie de kroonjuwelen in kaart en brainstorm over 'wat kan er misgaan'. Gebruik het DEN stappenplan vragen. Bepaal de top-5 risico's en bespreek jullie huidige maatregelen en hiaten.
- **Week 5: BIA invullen:** Op basis van de risicoanalyse bepaal per kritisch proces de RTO/RPO. Zorg dat directie akkoord is met deze hersteldoelstellingen, want ze impliceren mogelijke investeringen.
- **Week 6-7: opstellen concept DRP:** Stel het incident- en herstelplan stap voor stap op.
- **Week 8: review en definitief maken:** Laat relevante collega's het concept nalezen. Verwerk de feedback. Leg het incident- en herstelplan hierna ter goedkeuring voor aan het management/bestuur.
- **Week 9: oefenen:** Plan een eerste oefening of doorloop. Bijvoorbeeld een table-top simulatie: "Stel, onze website is gehackt en we lopen ons plan door." Kijk wat er goed gaat en noteer verbeterpunten. Pas het plan aan op basis van deze ervaring.
- **Week 10: afronden en communiceren:** Verspreid het definitieve incident- en herstelplan binnen de organisatie. Zorg dat iedereen die een rol heeft het plan (digitaal en liefst geprint) ontvangt. Communiceer de kernboodschap nogmaals aan alle medewerkers: waarom dit belangrijk is en dat er crisisteams zijn in geval van incidenten.

Bovenstaande routekaart benadrukt dat beginnen is belangrijker dan perfectie. Splits het werk in stukjes, werk iteratief aan verbeteringen, en houd de vaart erin. Liever een "80% goed" plan binnen enkele weken, dan maanden uitstel voor een theoretisch 100% plan. Cyberveiligheid is immers urgent: elke week uitstel is een risico. Deze handleiding en planning helpen je om gestructureerd en pragmatisch te werk te gaan.

Meer weten over cybersecurity?
Op de website van DEN vind je aanvullende kennis, hulpmiddelen en praktische handreikingen voor het versterken van de digitale weerbaarheid van culturele organisaties: den.nl

DEN