Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Herstel van een cyberincident

Voor als het dan tóch misgaat

Basisboek | 1.0 | 13 mei 2024

Mailen lukt niet meer. Belangrijke data zijn niet meer toegankelijk. Tot overmaat van ramp zijn ook de back-ups versleuteld. Zo maar een scenario dat jou kan overkomen. In zulke gevallen wil je snel terugkeren naar 'business as usual'. Het vermogen te herstellen van cyberincidenten is een voorwaarde om digitaal weerbaar te zijn. Maar herstel omvat meer dan back-ups. Weten wat je moet beschermen, welke middelen je daarvoor nodig hebt en hoe je je herstel uitvoert en oefent is noodzakelijk.

In dit basisboek licht het NCSC toe wat het belang van herstel is, hoe je dat inricht en welke maatregelen je kunt nemen om effectief te herstellen van cyberincidenten.

Achtergrond

Ongeveer 1 op de 5 bedrijven krijgt jaarlijks te maken met een cyberincident met schade of uitval als gevolg.[1] Kwetsbaarheden in software, menselijke fouten, maar ook rampen, pandemieën of stroomuitval; ze kunnen leiden tot onverwachte gebeurtenissen en zelfs uitmonden in disruptieve incidenten en leiden tot een crisis. Herstellen van een cyberincident kan ingewikkeld en tijdrovend zijn: zo kan het herstel van gijzelsoftware dagen zo niet weken in beslag nemen. Hersteloperaties verlopen bovendien lang niet altijd vlekkeloos. Vaak blijkt dat het herstellen onvoldoende is geoefend of dat back-ups niet goed kunnen worden teruggezet.[2] Hoe langer de hersteltijd en ingewikkelder de hersteloperatie, hoe groter de impact op de bedrijfsvoering. Dat kan geld kosten, je reputatie schaden of in een ernstig geval zelfs leiden tot faillissement. Bij een cyberincident komt het aan op een effectief en efficiënt herstelvermogen van je organisatie zodat de dienstverlening gecontinueerd kan worden.[3]

Wat herstellen betekent en hoe je dat inricht, dat lees je in dit basisboek. We gaan in op wat herstel precies is, hoe je het organisatorisch inricht en welke maatregelen je kunt treffen om effectief te herstellen van cyberincidenten.

Doelgroep

Chief Information Officers, Chief Information Security Officers, Business Continuity Managers, Risk- en Crisis Managers.

Samenwerkingspartners

ASML, De Volksbank, Nederlandse Vereniging van Banken, Rabobank, Triodos Bank en de AIVD.

[1] CBS Cybersecuritymonitor 2022. In 2021 had circa 14% van de bedrijven te maken met een cyberincident met een interne oorzaak en 7% met een aanval van buitenaf.

[2] Gartner Global Security and Risk Management Governance Survey 2021.

[3] Zie ook het TNO-rapport: Herstelvermogen binnen IT-infrastructuren.

Cyberincidenten met impact

Cyberincidenten verstoren de beschikbaarheid, integriteit of vertrouwelijkheid van informatiesystemen en data. In het geval dat het impact heeft op kritieke producten en/of diensten met de daarbij behorende bedrijfsprocessen, wil je terug kunnen vallen op een herstelplan om zo snel als mogelijk terug te kunnen keren naar de normaalsituatie.

Herstel waarvan?

In dit basisboek verstaan we onder cyberincidenten: incidenten die de IT verstoren waardoor kritieke producten, diensten en processen niet meer kunnen worden geleverd. In dergelijke gevallen kan het betekenen dat de organisatiedoelstellingen niet meer verwezenlijkt kunnen worden, met schade als gevolg. Het is dan van belang dat je terug kunt vallen op plannen, procedures en afspraken zodat de hersteloperatie zo goed als mogelijk kan worden opgestart en uitgevoerd.

Inrichten van herstel

Voordat een cyberincident met ontwrichtende effecten op je bedrijfsvoering je organisatie treft, is het van belang om herstel in je organisatie in te richten. Maar hoe doe je dat? Hieronder benoemen we de instrumenten die nodig zijn om te bouwen aan je herstelvermogen.

Stap 1: Weet wat je moet beschermen

Je organisatie volledig beschermen tegen elke vorm van uitval of cyberdreiging is een utopie. Het is daarom verstandig potentiële dreigingen en de effecten daarvan op je producten en diensten vroegtijdig te identificeren en deze te prioriteren. Dat kan met een Business Impact Analyse (BIA). De BIA is een voorwaarde voor effectief bedrijfscontinuïteitsbeheer (BCM).[4] De BIA helpt je zicht te krijgen op je te beschermen belangen.[5] Met een BIA breng je, samen met de verantwoordelijken en eigenaren de kritieke producten, diensten en processen in kaart. Daar horen ook de daaraan gerelateerde assets (software, hardware, mensen, leveranciers en data) bij die deze ondersteunen. Hierdoor weet je welke producten, diensten en processen kritiek zijn voor je bedrijfsvoering en wat ervoor nodig is om deze draaiende te houden. De volgende 4 stappen helpen bij het opstellen van de BIA:

1. **Breng je belangen in kaart.** Een BIA begint met het onderscheiden van kritische en ondersteunende producten, diensten en bedrijfsprocessen en de assets die benodigd zijn deze draaiende te houden. Denk hierbij ook aan toeleveranciers, IT-dienstverleners en afhankelijkheden hiertussen.[6] Het gaat hier om de gehele keten van leveranciers waar je dataverantwoordelijke bent. Per dienst of product geef je aan wat de impact is van een mogelijke verstoring van assets op de continuïteit van de dienst of het product en daarmee de organisatie. Denk hierbij aan financiële impact, operationele verstoring, juridische en wetgevende sancties, reputatieschade of gezondheid en

[4] Het Digital Trust Center heeft voor ondernemers een stappenplan risicoanalyse gemaakt. Dit is nuttig voor als een BIA minder passend is. De achterliggende principes zijn echter dezelfde.

[5] De Business Impact Analyse omvat naast cyberincidenten ook andere mogelijke verstoringen die impact hebben op de continuïteit en gaat dus niet alleen over IT.

[6] Zie voor meer info de NCSC publicatie 'Omgaan met risico's in de toeleveringsketen' en maak gebruik van de 'Cybercheck'.

veiligheid (of andere bedrijfsdoelstellingen).

2. **Voer een dreigingsanalyse uit**
   Nu de kritische producten, diensten en processen inzichtelijk zijn, is het nodig te bedenken welke dreigingen relevant zijn voor jouw organisatie. Het kan hier gaan om aanvallen van cybercriminelen, maar ook dreigingen als uitval van internet, stroom of schade door een overstroming. In een dreigingsanalyse stel je per dreiging vast hoe groot de kans is dat deze zich manifesteert, welke processen dat kan raken en welke impact dat heeft.[7]
3. **Stel de maximale uitvalduurvast**
   Voor elk van de producten, diensten en onderliggende processen stelt de business vast wat de maximaal tolereerbare uitvalsduur is (Maximum Tolerable Period of Disruption, MTPD). Na hoeveel tijd (uren, dagen, weken) zorgt uitval van het leveren van een product of dienst ervoor dat het echt kritiek wordt? Daarbij is het noodzakelijk om te weten hoe lang het duurt om na een incident te herstellen naar een acceptabel niveau waarbij de continuïteit van het product of de dienst geborgd wordt. Dit kan worden gekwantificeerd met de '*Recovery Time Objective*' (RTO). Als blijkt dat (gedeeltelijk) herstel van een cyberincident langer duurt dan de RTO voorschrijft, dan kan dat betekenen dat je de MTPD overschrijdt en mogelijk ernstige schade oploopt. Het is nodig om in deze fase het gesprek tussen de business en IT (en leveranciers) te facilliteren om belemmeringen hier vast in kaart te brengen en te adresseren. Daarnaast is het in sommige gevallen nodig na te gaan hoeveel dataverlies je maximaal kunt accepteren. Dit wordt met de '*Recovery Point Objective*' (RPO) gekwantificeerd. Op het moment dat er onvoldoende frequent een back-up wordt gemaakt van data, dan kan in een geval van een cyberincident dataverlies optreden. Als dit dataverlies te groot wordt, dan kan dat eveneens leiden tot schade aan je organisatie. Met de MTPD, RTO en de RPO krijg je zicht op de eisen die gesteld moeten worden aan je herstelvermogen. Ook in deze stap is het van belang je toeleveranciers en IT-dienstverleners te betrekken. Zij beschikken over essentiële informatie die helpen je MTPD, RTO en RPO te bepalen.
4. **Prioriteer je kritische producten en diensten**
   Op basis van de risico's, de impact van mogelijke verstoringen en de maximale uitvalsduur kun je vervolgens prioriteren. Maak onderscheid tussen kritische en niet-kritische producten, diensten en processen. Bepaal wat de kroonjuwelen zijn en welke IT-assets daaraan gerelateerd zijn. Rangschik de processen naar de mate van impact op je bedrijfsvoering (waarbij de RTO en RPO leidend zijn).

[7] Zie voor meer info de NCSC factsheet 'Risico's: de waarde van informatie als uitgangspunt'. En over digitale dreigingen de NCSC weblog: Digitale aanvalstechnieken, leer je tegenstander kennen!

Stap 2: Ontwikkel een herstelplan

Met de inzichten uit de BIA heb je de tools in handen om te bouwen aan het herstelplan (ook wel (IT) Disaster Recovery Plan genoemd). Een herstelplan is een document – of een onderdeel van het bedrijfscontinuïteitsplan - waar richtlijnen en benaderingen in zijn opgenomen die beschrijven hoe je na een cyberincident snel weer de werkzaamheden kunt hervatten. Het herstelplan is als het ware het draaiboek dat tijdens een cyberincident gebruikt wordt om effectief en snel te kunnen herstellen.

Maatwerk

Het herstelplan is maatwerk. Kleinere organisaties kunnen voldoende hebben aan bellijst met hun IT-leveranciers en een overzicht van afspraken die zij met hen hebben gemaakt over het herstellen van een cyberincident.[8] Voor organisaties met een complexe IT-omgeving is het nodig een uitgebreider plan op te stellen.

Zorg er daarom voor dat het herstelplan altijd paraat en up-to-date is. Een herstelplan of een scenariokaart (zie hieronder) bevat mogelijk gevoelige gegevens. Bedenk hoe je je plannen beschermt en beschikbaar houdt. Een oplossing is de plannen op versleutelde laptops op te slaan, of goed beveiligde externe locaties te gebruiken die losstaan van het eigen netwerk. In een herstelplan is in elk geval beschreven:

- **Activatie, uitvoering en beëindiging**
  Beschrijf wie het plan in werking mag stellen en definieer in welke gevallen het herstelplan geactiveerd moet worden (activatie), wie dat dient uit te voeren en op welk moment de hersteloperatie moet worden beëindigd. Beschrijf welke besluiten genomen mogen worden binnen welke rol (bijv. 'stekkermandaat'). Doorgaans ligt de beslissingsbevoegdheid voor activatie, uitvoering en beëindiging van het herstelplan bij het hoger management. Zij kunnen een *herstel managementteam* vormen waar de strategische besluiten worden genomen.
- **Rollen en verantwoordelijkheden**. In het herstelplan is beschreven wie er in het *herstelteam* zit, welke rollen zij hebben (netwerkteam, applicatieteam, serverteam, communicatieteam) en – niet onbelangrijk – wat hun contactgegevens zijn. Een notificatielijst of belboom is daarin onmisbaar. Denk hier ook na over toeleveranciers en IT-dienstverleners en hun contactgegevens. Beschrijf welke rol zij hebben in het herstelproces en welke afspraken (SLA's) en contracten relevant zijn. Bespreek welke eisen je stelt aan continuïteit en welke inspanningen jij verwacht van de leveranciers om je hersteltijd af te stemmen op je eisen uit de BIA. Denk vooraf na over wie welke verantwoordelijkheden heeft binnen het herstelproces en beschrijf deze in het herstelplan.
- **Scenariokaarten**
  Een goed herstelplan is actiegericht en in staat een handreiking te zijn voor het herstelteam op het moment dat een cyberincident plaatsvindt. Dat kan door het herstelplan aan te vullen met scenariokaarten ('playbooks'). Gebasseerd op de dreigingsanalyse uit de BIA, beschrijf je hier bondig scenario's en hoe je daar stap-voor-stap van kunt herstellen. Denk bijvoorbeeld aan scenario's als

[8] Zie voor meer informatie de pagina van het Digital Trust Center Afspraken maken met een IT-leverancier.

ransomware[9], DDoS-aanval[10], uitval door een stroomstoring[11], brand,lekkage enzovoorts. Bedenk wel dat cyberincidenten in de praktijk vrijwel nooit precies passen op een scenariokaart.

- **Communicatieplan en uitwijklocatie**
  Beschrijf hoe je in geval van een cyberincident communiceert richting diverse stakeholders. Zie hiervoor het kopje 'maak melding van een incident' onder Communicatie en coördinatie. Zorg voor alternatieve communicatiekanalen en uitwijklocaties (indien mogelijk), bijvoorbeeld voor het geval het internet of mobiele telefonie niet functioneert ('out of band communications').
- **Inventaris van systemen en applicaties**
  Voeg een overzicht van alle systemen en applicaties toe en de onderlinge afhankelijkheden, leveranciers e.d. Rankschik ze naar de impact op je bedrijfsvoering.
- **Netwerkbeschrijvingen en schema's**
  Voeg netwerkbeschrijvingen en schema's toe zodat je inzicht hebt in je netwerk en de onderlinge afhankelijkheden daartussen. De uitdaging hier is deze regelmatig up to date te houden. Dit moet in een proces geborgd worden.
- **Back-up strategie**
  Een back-up strategie is nodig in het geval een cyberincident de beschikbaarheid, integriteit of toegankelijkheid van data treft. Het is aan te raden de back-up strategie in te richten aan de hand van de dreigingsanalyse uit de BIA. Een door water ondergelopen serverruimte vraagt immers om een ander type back-up dan een aanval met gijzelsoftware. Een goede back-up strategie houdt daarom rekening met diverse dreigingen en de onderliggende RTO's en RPO's van de getroffen processen. Overwegingen rondom back-up media (snapshots, harddisks, cloud), locaties (onsite, offsite, offline), type back-ups (volledig, incrementeel, differentieel) en bewaartermijnen zijn uiteindelijk allen afhankelijk van de risico's, kosten, wet- en regelgeving en voorkeuren.[12] Denk daarnaast ook aan het kunnen vervangen van hardware (switches, servers e.d.) en het back-uppen van systeem- en netwerkconfiguraties (virtuele machines, config-bestanden). Tot slot is het raadzaam ook na te gaan welke afspraken (SLA's) je met IT-leveranciers hebt gemaakt over systemen en applicaties die niet in eigen beheer zijn.

Stap 3: Oefen, test en train het herstel

Het papier is geduldig, maar op zichzelf onvoldoende. Hersteloperaties blijken in de praktijk weerbarstig en een belangrijke oorzaak daarvan is dat plannen onvoldoende zijn geoefend, getest en getraind. Het beoefenen van het herstelplan en onderliggende scenario's maakt duidelijk of het herstelvermogen in lijn is met de vereisten om bedrijfsprocessen weer op tijd te herstellen. Oefenen zorgt ervoor dat de mensen die het herstel uitvoeren ook leren hoe zij als team

[9] Zie voor meer informatie de pagina van het Digital Trust Center

cier" Afspraken maken met een IT-leverancier.

NK
"https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten"
Continuïteit van online diensten.

[11] Zie de scenariokaart uitval door stroomstoring ontwikkeld door de Informatiebeveiligingsdienst (IBD).

[12] Een goed voorbeeld van een back-up strategie is de 3-2-1 strategie. Zie voor meer informatie de pagina van het DTC: Een back-up strategie opstellen

effectief kunnen optreden. Oefenen kan in diverse vormen. Denk aan een *tabletop* oefening, oefening met live herstel enzovoorts.[13]

Daarnaast is het regelmatig testen en het terugzetten van back-ups cruciaal. Hieruit blijkt of de back-ups in staat zijn de data terug te zetten naar het gewenste moment (RPO), resultaat (data-integriteit), de kwaliteit en hoe lang dat duurt (RTO). Beoordeel op basis van de tests of de back-up strategie moet worden aanscherpt.

Tot slot is het periodiek opleiden en trainen van personeel een punt van aandacht. Zij moeten vertrouwd raken met de taken die zij hebben in het herstelteam, processen internaliseren, de herstelprocedures kennen en vlieguren maken in de uitvoering van herstelwerkzaamheden.

Communicatie en coördinatie

Tijdens een cyberincident kun je niet zonder effectieve communicatie en coördinatie. Een cyberincident kan de gemoederen binnen de organisatie flink bezighouden. Ook kan het zorgen voor onrust bij klanten, leveranciers en andere stakeholders, met reputatieschade als gevolg.[14] Een communicatieplan, zoals eerder beschreven bij het herstelplan, is nodig omdat je veel overwegingen al van tevoren kunt uitdenken. De volgende overwegingen zijn hierin nuttig:

- **Werk aan je cultuur**
  Herstellen van een cyberincident is mensenwerk. Mensen moeten het gevoel hebben dat zij veilig melding kunnen maken van een incident en het vertrouwen krijgen bij te kunnen dragen aan het herstel daarvan. Ruimte om fouten te maken is daar een belangrijke voorwaarde voor.
- **Communiceer intern**
  Als een deel van de bedrijfsvoering stilligt, dan heeft dat niet alleen impact op de bedrijfsvoering zelf. Medewerkers zullen vragen hebben over hoe het werk verder moet, of bepaalde verwachtingen hebben ten aanzien van de duur van de verstoring. Ook zullen daartoe aangewezen medewerkers in actie moeten komen om bij te dragen aan herstel of het continueren van de bedrijfsvoering. Het is aan te raden zo open en vooral zo feitelijk als mogelijk te communiceren zodat de juiste verwachtingen worden geschept en eventuele ruis wegneemt. Besef tegelijkertijd dat interne communicatie óók externe communicatie is. Stem daarom goed af wat er wordt gedeeld, door wie en wat de boodschap is. Communiceer wat je weet, maar ook wat je (nog) niet weet.
- **Communiceer extern**
  Klanten, leveranciers en andere stakeholders kunnen als gevolg van een cyberincident ook schade of hinder ondervinden. Ze kunnen afhankelijk zijn van jouw product- of dienstverlening of direct te maken krijgen met een vergelijkbaar cyberincident. Het is daarom voor het behouden van de relatie van belang snel, transparant en feitelijk te informeren over het incident. Vergeet daarbij niet een concreet handelingsperspectief te bieden. Een belangrijke voorwaarde voor open communicatie is dat vooraf wordt nagedacht over de doelgroepen die moeten worden benaderd, waarbij wettelijke verplichtingen, belangen, informatiebehoeftes en reputatierisico's centraal staan. Wees ook bedacht op

[13] Het NCSC organiseert tweejaarlijks de ISIDOOR-oefening, waar het Landelijk Crisisplan Digitaal wordt beoefend zie de pagina: Isidoor NCSC voor meer info.

[14] Zie ook de NCSC publicatie Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten.

mogelijke juridsche gevolgen van de communicatie. Dit vraagt om een zorgvuldige afweging.

- **Coördineer het herstel**
  Coördinatie van de hersteloperatie is nodig om ervoor te zorgen dat het herstel goed getimed wordt. Te vroeg of te laat herstellen kan ineffectief zijn of het verhelpen van een cyberincident in de weg zitten. Denk daarbij aan forensische sporen en de 'chain-of-custody'.
  Coördinatie tussen interne en externe stakeholders zoals managed service providers (MSP's), systeemeigenaren, ontwikkelaars of autoriteiten is belangrijk om het herstel vlekkeloos te laten verlopen. En een praktisch punt: organiseer facilitaire ondersteuning (ruimtes, schrijfmateriaal, secretariële ondersteuning e.d.).
- **Maak melding van het incident**
  In sommige gevallen is het nodig om melding te maken van het cyberincident. Vitale aanbieders en aanbieders van essentiële diensten hebben een meldplicht voor ernstige cyberincidenten bij het NCSC.[15] In het geval van strafbare feiten kan aangifte worden gedaan bij de politie[16] en bij een datalek bij de Autoriteit Persoonsgegevens.[17] Bij vermoedens van betrokenheid van een statelijke actor, kan contact worden opgenomen met de AIVD.[18]

Continu leren en verbeteren

Cyberincidenten zijn leerzaam. Als het puin is geruimd, het incident verholpen is en de bedrijfsprocessen weer door kunnen, is het tijd om na te gaan welke lessen daaruit getrokken kunnen worden.

- **Verslaglegging**
  Het mag een open deur lijken, maar in de chaos van een cyberincident kan het weleens worden vergeten: de verslaglegging. Om lessen te trekken uit een cyberincident is het nodig om verslag te leggen van de hersteloperatie. Zorg ervoor dat besluiten en werkzaamheden uit het herstelteam, managementteam, responsteam, correspondentie met externen (IT-leveranciers) nauwkeurig en op een eenduidige wijze worden vastgelegd. De BOB-methodiek (beeldvorming, oordeelsvorming en besluitvorming) kan hierin een nuttig hulpmiddel zijn om de verslaglegging te ordenen. Denk ook aan de duur van de werkzaamheden, zodat een tijdslijn kan worden opgesteld. Het geniet de voorkeur om per betrokken team een persoon aan te wijzen die verantwoordelijk is voor de vastlegging.
- **Evalueer**
  Kort na het cyberincident kan een evaluatie helpen om de eerste lessen vast in kaart te brengen. Zeker als het over (menselijke) fouten gaat, kan dit pijnlijk zijn. Heb daarom ook oog voor wat er juist wel goed ging. Dit bevordert de bereidheid tot leren. Na een eerste evaluatie wordt vaak meer duidelijk over de toedracht en schade van het cyberincident en welke activiteiten de respons- en herstelwerkzaamheden bevorderden of juist verslechterden. Zorg dat verbeterpunten uit de evaluatie duidelijk belegd worden en monitor de voortgang hiervan.

[15] Melden kan via de website van het NCSC: Wbni-melding

[16] Zie de website van de politie: aangifte of melding doen.

[17] Zie de website van APB: datalek melden.

[18] Zie de website van de AIVD: contact.

- **Herstelinformatie**
  De verslaglegging en evaluatie(s) helpen om inzicht te krijgen in de duur en kwaliteit van de herstelwerkzaamheden. Deze informatie kunnen worden omgezet in herstelinformatie.[19] Herstelinformatie kan nuttig zijn om de kwaliteit van het herstel te bevorderen. Denk aan de tijdsduur van het herstellen van een met malware geïnfecteerde server, of de tijd die het duurt om back-ups terug te zetten. Andere informatie zoals de kosten van een cyberincident (juridisch, hardware, software, arbeidskosten e.d.) of de frequentie van bepaalde cyberincidenten per jaar kunnen eveneens nuttig zijn om het herstel van je organisatie beter in te richten.
- **Verbeteren**
  Zet de geleerde lessen om in actie door ze naast de in de BIA geïdentificeerde belangen, dreigingen, RTO's, RPO's en prioritering te leggen. Kloppen deze nog of moeten ze worden bijgeschaafd? Hebben we de juiste middelen of moet er aanvullend geïnvesteerd worden? De geleerde lessen zijn cruciaal om deze vragen te beantwoorden. Wanneer de geleerde lessen worden geïntegreerd, beoefend en getest ontstaat een verbetercyclus.

Tot slot

Cyberincidenten zijn lang niet altijd te voorkomen. Als het dan toch gebeurt, wil je daar snel en effectief van herstellen. Om herstel in te richten is het nodig te weten wat je moet beschermen, herstelplannen op te stellen en deze regelmatig te beoefenen. Tijdens een cyberincident is communicatie en coördinatie een belangrijke voorwaarde voor succes. Door zowel intern als extern de betrokkenen op de hoogte te stellen en hen te voorzien van een handelingsperspectief, beperk je schade en onjuiste verwachtingen. Herstellen na een cyberincident betekent tot slot dat je leert van wat er goed ging en wat er fout ging. Deze geleerde lessen helpen je om nóg weerbaarder te worden.

[19] Voorbeelden zijn te vinden in het MITRE rapport: Cyber Resiliency Metrics

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Mei 2024