BEWAAR DIT GOED

ITDS | EMBRACING CHANGE

Bereid je voor op digitale ontwrichting

Wat je vandaag organiseert, bepaalt of je morgen blijft draaien

De inhoud van dit boekje is ontwikkeld door **ITDS Risk & Compliance.** Het is opgesteld door onze consultants op basis van actuele IT-risk-, cyber- en continuïteitsinzichten.

Jelmer van Heest
Associate Consultant

Ilana van Berkum
Senior Manager

Sander Kerens
Management Consultant

Ronald van Wanrooij
Senior Manager

Meer informatie over ITDS en onze diensten vind je op **www.itds.nl/diensten/wet-en-regelgeving**/. Hier lees je hoe wij organisaties helpen om digitaal weerbaar te worden en continuïteit te waarborgen bij IT-incidenten.

Scan Me

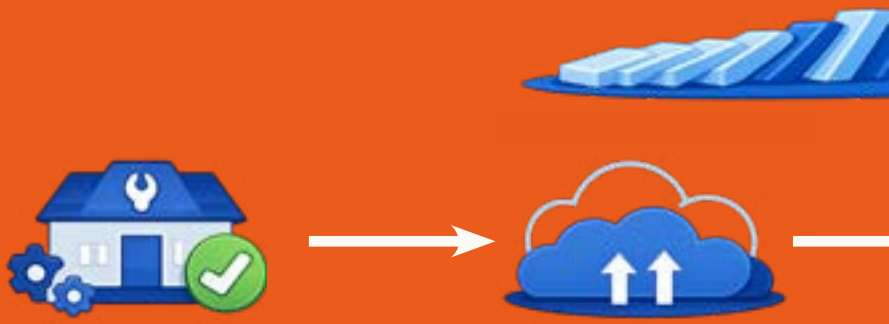
Wij denken graag met je mee over een passende aanpak voor jouw organisatie.

Inhoudsopgave

1 Waarom krijg jij dit boekje nu?

Digitale incidenten raken

Domino effect

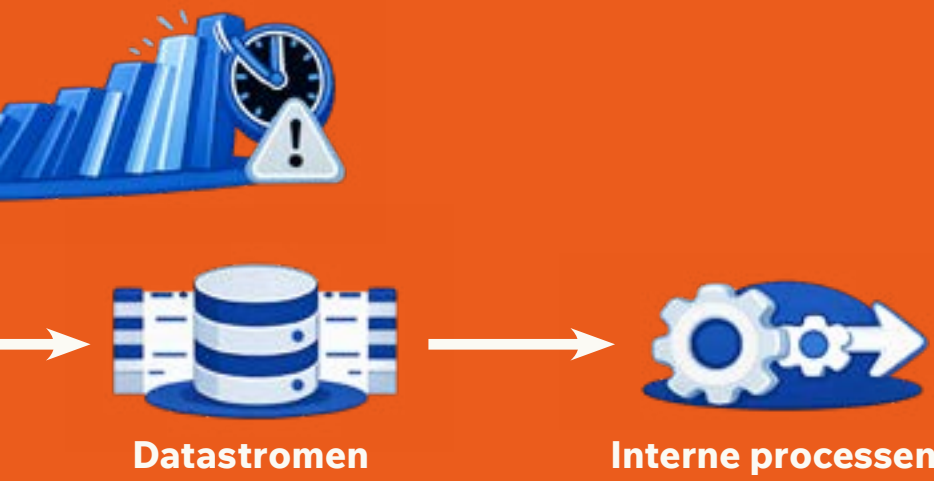


Digitale verstoringen zijn geen uitzondering meer, ze zijn dagelijkse realiteit. Wanneer IT-systemen uitvallen, raakt dat de hele organisatie: dienstverlening stopt, klantvragen blijven liggen en besluitvorming vertraagt.

De vraag is niet of het gebeurt, maar wanneer...

zelden alleen de IT-afdeling

in de keten



Met dit boekje krijg je praktische handvatten om jouw organisatie beter voor te bereiden op digitale verstoringen.

Met als **doel:** in de cruciale 24–72 uur na een incident blijven leveren wat belangrijk is. Zonder chaos, zonder verrassingen.

2 Waarom verstoringen vaker voorkomen

Digitale verstoringen nemen toe omdat organisaties steeds sterker met elkaar verbonden zijn. Processen draaien op digitale ketens, clouddiensten en externe leveranciers. Deze verbondenheid maakt organisaties sneller en efficiënter, maar ook kwetsbaarder.

Een probleem op één plek blijft zelden lokaal. Door onderlinge afhankelijkheden kan een kleine verstoring zich razendsnel verspreiden door systemen, afdelingen en zelfs hele ketens.
Daarnaast ontstaan incidenten niet alleen door cybercriminelen. In de praktijk zijn fouten in configuraties, mislukte software-updates, datacorruptie of verstoringen bij leveranciers minstens zo vaak de oorzaak.

In de praktijk vallen ze vrijwel altijd binnen vier herkenbare clusters:

Technisch falen
Complexe en gekoppelde systemen kunnen onverwacht uitvallen of elkaar verstoren. Bijvoorbeeld:
- Uitval van een cloud- of SaaS-dienst
- Mislukte software-update

Menselijk handelen
Onbedoelde fouten kunnen direct grote digitale impact veroorzaken. Bijvoorbeeld:
- Verkeerde configuratie
- Klikken op een phishing-link

Ketenafhankelijkheid
Een verstoring bij een leverancier werkt direct door in de eigen organisatie. Bijvoorbeeld:
- Storing bij een IT-partner
- Afhankelijkheid van buitenlandse infrastructuur of platformen

Externe dreiging
Gerichte aanvallen of externe ontwikkelingen kunnen systemen ontregelen. Bijvoorbeeld:
- DDoS-aanvallen
- Datadiefstal of sabotage

3

Weerbaarheid & veerkracht: meer dan preventie

Wat betekent dit voor jouw organisatie?
Digitale risico's volledig voorkomen is in de praktijk niet altijd mogelijk. Organisaties investeren terecht in beveiliging, monitoring en preventieve maatregelen. Toch blijft er altijd een kans bestaan dat een incident zich voordoet. Juist daarom is het belangrijk om verder te kijken dan alleen het voorkomen van verstoringen.
Traditionele risicoanalyse richt zich op kans en impact. Bij digitale continuïteit draait het echter om een andere vraag:

"Stel dat het gebeurt. Wat doen we dan?"

Weerbaarheid en veerkracht gaan over het vermogen van een organisatie om zich aan te passen wanneer systemen uitvallen, data tijdelijk niet beschikbaar is of externe diensten wegvallen. Het gaat niet alleen om het voorkomen van schade, maar vooral om het beperken van gevolgen en het versnellen van herstel.

Net zoals organisaties zich voorbereiden op brand, stroomuitval of evacuaties, vraagt ook digitale ontwrichting om voorbereiding. Niet omdat incidenten dagelijks plaatsvinden, maar omdat de impact groot kan zijn wanneer ze zich voordoen.

Weerbaarheid betekent concreet weten wat absoluut moet blijven draaien en hoe. Het vraagt een gestructureerde aanpak waarin processen, mensen en informatie systematisch worden voorbereid. Veerkracht betekent getest hebben dat herstel ook echt werkt onder druk.

4 Voorbeeldscenario: Cyberaanval

AVG / NIS2 / ISO 27001

Mogelijke phishing. Bewustzijn van risico's en alert handelen zijn belangrijk, maar organisaties zijn ook wettelijk verplicht passende beveiligingsmaatregelen te nemen (AVG/NIS2).

Verdachte e-mail ontvangen

Een medewerker ontvangt een e-mail die lijkt te komen van een leverancier of interne afdeling. De boodschap oogt geloofwaardig en bevat een bijlage of link.

Tip: Meld verdachte e-mails direct via het interne meldpunt of IT-servicedesk.

T=0 uur | +2 uur | +6 uur

NIS2 / ISO 27001

Mogelijk beveiligingsincident: volgens ISO 27001 moeten effectieve beheersmaatregelen tegen malware zijn geïmplementeerd.

Bijlage gedownload / gegevens achtergelaten

Een medewerker opent en download de bijlage of klikt op de link en laat gegevens achter op een valse website. Onbewust wordt kwaadaardige software geïnstalleerd of ongeautoriseerde toegang verkregen.

Tip: Meld direct bij IT zodat impact beoordeeld kan worden.

NIS2 / DORA / ISO 27001

Onvoldoende detectie kan leiden tot aansprakelijkheid bij datalekken of uitval.

Onopgemerkte verspreiding malware binnen het netwerk

De malware (kwaadaardige software) nestelt zich en probeert toegang te krijgen tot andere systemen of accounts.

Tip: Zorg voor logging, EDR/monitoring en een effectief incidentproces.

Houdt rekening met wettelijke kaders en normen

Tips ter overweging vanuit ITDS

AVG / NIS2 / DORA

Mogelijk datalek of ernstig incident. Wettelijke meldtermijnen kunnen lopen (24-72 uur).

ISO 27001 / ISO 22301 / NIS2

Na incident is evaluatie verplicht voor toekomstige preventie.

Eerste verstoringen merkbaar

Bestanden openen trager, applicaties reageren vreemd of medewerkers verliezen toegang tot gedeelde mappen. Ook kan afwijkend netwerkverkeer optreden dat afwijkt van het normale gebruikspatroon.

Herstel of blijvende schade

Nadat het incident is geïdentificeerd, worden systemen geïsoleerd om verdere verspreiding te voorkomen. Geïnfecteerde systemen worden opgeschoond of opnieuw ingericht, waarna herstel kan starten. Back-ups worden gecontroleerd op integriteit en beschikbaarheid voordat systemen gefaseerd weer online komen. In deze fase blijkt of herstel volledig mogelijk is, of dat langdurige verstoring of blijvende schade optreedt.

Tip: Start formeel incidentproces en beoordeel meldplicht bij toezichthouder.

Tip: Voer een post-incident evaluatie uit en verbeter beheersmaatregelen, herstelprocedures en back-upstrategie waar nodig.

+12 uur | +24 uur | +48 uur | +72 uur

NIS2 / DORA / ISO 22301

Kritiek incident. Organisaties moeten aantoonbaar beschikken over herstel- en continuïteitsplannen.

AVG / NIS2 / Contractueel

Externe impact kan contractuele verplichtingen raken.

Systemen en data versleuteld

Bestanden worden onbruikbaar en er verschijnt een melding: data is versleuteld. Productie- en kantoorsystemen vallen uit.

Operationele impact en externe druk

Klanten ervaren hinder, leveranciers wachten op reacties en mogelijk melden toezichthouders of media zich. Interne druk neemt toe.
Contractuele afspraken of SLA's kunnen onder druk komen te staan, met mogelijke financiële of reputatieschade als gevolg.

Tip: Incident escaleren naar crisisteam en activeren crisismanagement en herstelplan.

Tip: Zorg voor duidelijke en consistente communicatie richting stakeholders en leg besluiten en acties zorgvuldig vast.

5

Digitale weerbaarheid in drie stappen

Digitale weerbaarheid ontstaat niet door één maatregel, maar door een combinatie van voorbereiding, duidelijke afspraken en oefening. De volgende drie stappen helpen organisaties om niet alleen risico's te verkleinen, maar ook goed te kunnen reageren wanneer een incident zich voordoet.

Stap 1 – Stel je IT-noodpakket samen

Wanneer systemen uitvallen, heb je direct toegang nodig tot essentiële informatie en middelen. Een IT-noodpakket bevat alles wat nodig is voor medewerkers om niet te hoeven improviseren bij noodsituaties. Denk aan:

- Offline back-ups van kritieke data
- Documentatie van kernsystemen en toegang
- Contactgegevens van IT-leveranciers
- Noodaccounts en alternatieve inlogmogelijkheden
- Voorbereide communicatie-templates (intern/extern)
- Alternatieve werkmogelijkheden (noodlaptops, thuiswerken, papieren procedures)

Stap 2 – Maak een digitaal continuïteitsplan

Een continuïteitsplan beschrijft wie wat doet wanneer een incident plaatsvindt. Niet alleen IT, maar de hele organisatie. Belangrijke onderdelen:

- Crisisorganisatie en verantwoordelijkheden
- Besluitvormings- en escalatielijnen
- Interne en externe communicatieafspraken
- Prioritering van kritieke processen en systemen
- Afstemming met leveranciers en ketenpartners
- Scenario's per type incident (ransomware, uitval leverancier, dataverlies)

Stap 3 – Oefen crisissituaties

Plannen die nooit geoefend zijn, falen onder druk. Het oefenen van crisissituaties onthult hiaten die op papier onzichtbaar blijven. Blijf na elke oefening evalueren, verbeteren en opnieuw testen. Voorbeelden van oefeningen:

- Table-top simulaties met management en IT
- Technische hersteltests van back-ups en systemen
- Communicatie-oefeningen (pers, klanten, medewerkers)
- Leveranciers- en ketenoefeningen
- Evaluaties en verbeteracties na elke oefening

Pak je digitale weerbaarheid aan!

Digitale weerbaarheid vraagt om maatwerk. Iedere organisatie heeft een eigen risicoprofiel, afhankelijkheden en prioriteiten. De checklist op de rechterpagina helpt om inzicht te krijgen in waar behoefte ligt - van governance en risicomanagement tot continuïteit en compliance.

Niet elke organisatie start op hetzelfde niveau. Soms gaat het om het opzetten van fundamenten, soms om het verdiepen of aantoonbaar maken van bestaande maatregelen. Door scherp te krijgen waar versterking nodig is, ontstaat richting voor gerichte actie.

Staat jouw specifieke behoefte niet tussen de genoemde punten? Ook dan denken wij graag mee over een passende aanpak.

Checklist

Loop de checklist langs en ontdek waar jouw organisatie behoefte aan heeft. Staan er vakjes open? We helpen je bepalen waar je begint.

1. Strategie & Governance

- [ ] Cybersecuritybehoeften in kaart gebracht
- [ ] Verantwoordelijkheden belegd
- [ ] Governance-structuur opgezet
- [ ] Managementsysteem (ISMS) opgezet
- [ ] Beleid vastgesteld én gecommuniceerd
- [ ] Jaarlijkse managementreview uitgevoerd

2. Risicomanagement

- [ ] Kritieke bedrijfsprocessen geïdentificeerd
- [ ] Risicoanalyse uitgevoerd
- [ ] Risicomanagement opgesteld
- [ ] Actuele Risicoregisters
- [ ] 0-meting uitgevoerd bij aanvang van nieuwe projecten
- [ ] Kritieke data & processen geïnventariseerd

3. Informatiebeveiliging & Controls

- [ ] Classificatie van IT-data uitgevoerd
- [ ] Autorisatiebeheer ingericht
- [ ] Effectieve controls & bewijslast op orde
- [ ] Mitigerende maatregelen gedefinieerd per risico

4. Continuïteit & Herstel

- [ ] Bedrijfscontinuïteitsplannen (BCP) opgesteld
- [ ] Herstelplannen inclusief hersteltijd (RTO) en dataverlies-tolerantie (RPO) per kritiek systeem gedocumenteerd
- [ ] Backup-strategie getest en gedocumenteerd
- [ ] Crisisprotocol en communicatieplan beschikbaar
- [ ] BCP minimaal jaarlijks geoefend of gesimuleerd

5. Keten & Compliance

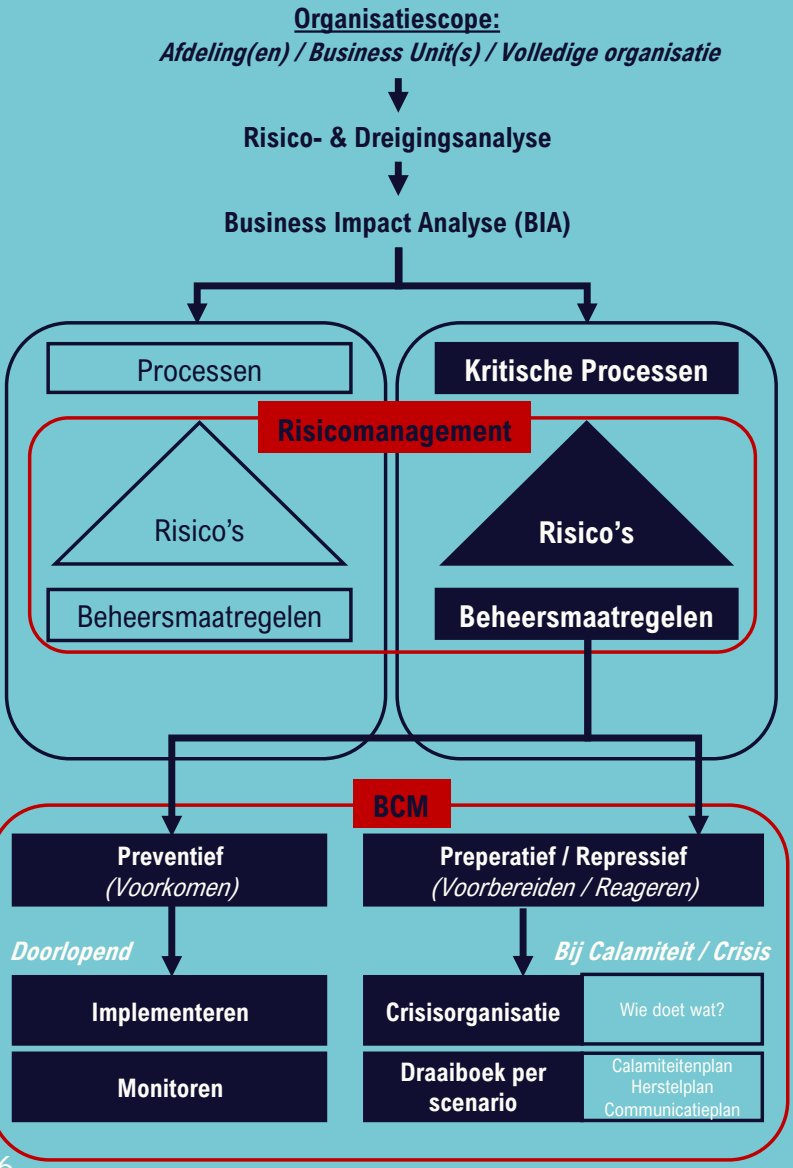
- [ ] Leveranciersafhankelijkheden in kaart gebracht
- [ ] Contractuele beveiligingseisen aan leveranciers gesteld
- [ ] Ketenbeheer (leveranciersmanagement) ingericht
- [ ] Compliancy/ GAP-analyse uitgevoerd t.o.v. wetgeving

6. Awareness & Educatie

- [ ] Basistraining cyberveiligheid voor alle medewerkers
- [ ] Phishing-simulaties uitgevoerd
- [ ] Awareness-programma opgesteld en ingericht
- [ ] Workshop Informatiebeveiliging/ NIS2/DORA gevolgd door relevante stakeholders

Wat je vandaag organiseert, bepaalt of je morgen blijft draaien

6 Bedrijfscontinuïteits-management (BCM)



Een continuïteitsplan is meer dan een document. Het bepaalt hoe een organisatie blijft functioneren wanneer systemen, processen of leveranciers uitvallen. Met de juiste structuur, begeleiding en aansluiting op erkende normen zoals ISO 22301 wordt een plan daadwerkelijk toepasbaar in de praktijk. Wij ondersteunen organisaties hier graag bij.

BCM begint bij inzicht. Welke onderdelen van de organisatie zijn kritisch? Welke processen kunnen tijdelijk stilvallen en welke absoluut niet? Door risico's en dreigingen in kaart te brengen, ontstaat een duidelijk beeld van waar de grootste kwetsbaarheden liggen.

Een belangrijk onderdeel hierbij is de Business Impact Analyse (BIA). Deze analyse maakt zichtbaar welke processen, systemen en afhankelijkheden essentieel zijn voor het functioneren van de organisatie. Niet alles heeft dezelfde prioriteit - het onderscheid tussen reguliere en kritische processen bepaalt waar maatregelen en herstelcapaciteit als eerste op gericht moeten zijn.

Vanuit dit inzicht kunnen gerichte beheersmaatregelen worden ingericht. Deze maatregelen richten zich op het verkleinen van risico's, het voorbereid zijn op verstoringen en het effectief reageren wanneer een incident zich voordoet. Continuïteit gaat immers niet alleen over het voorkomen van verstoringen, maar vooral over het vermogen om te blijven functioneren wanneer een incident zich voordoet.

BCM verbindt daarmee twee werelden:

- Preventief - risico's verkleinen door maatregelen te implementeren en continu monitoren
- Preparatief en repressief - voorbereid zijn op een calamiteit, met een duidelijke crisisorganisatie, draaiboeken per scenario en heldere communicatieafspraken

Waar een continuïteitsplan vaak een document is, is BCM een doorlopend proces. Het vraagt om periodieke evaluatie, actualisatie en oefening, maar ook om heldere afspraken, duidelijke verantwoordelijkheden en effectieve communicatie. Zo blijft de organisatie niet alleen beschermd tegen bekende risico's, maar ook wendbaar bij onverwachte gebeurtenissen.

7

Wat wij voor je kunnen betekenen

Digitale verstoringen gaan niet alleen over systemen, maar over de vraag of je als organisatie kunt blijven draaien wanneer het misgaat.

Dat vraagt om inzicht, duidelijke keuzes en een aanpak die werkt in de praktijk. Wij helpen organisaties om die weerbaarheid stap voor stap op te bouwen - van analyse tot concrete plannen en toetsing.

- Wij vertalen jouw context naar maatregelen die echt passen bij jouw organisatie.
- Wij vertalen wet- en regelgeving naar concrete acties voor jouw organisatie en processen.
- Wij brengen risico's scherp in beeld en vertalen bevindingen naar gedragen prioriteiten.
- Wij bewegen met je mee en passen ons continu aan op nieuwe technologie, dreigingen en wetgeving.
- Wij zorgen dat plannen echt landen in processen en dagelijks worden toegepast.

Digitale weerbaarheid ontstaat niet vanzelf. Het vraagt om inzicht, structuur en doorlopende aandacht. Veel organisaties weten wat er nodig is maar zoeken ondersteuning bij het vertalen van plannen naar pragmatische inrichting en uitvoering.
Wij helpen organisaties bij het versterken van hun digitale weerbaarheid en continuïteit.

Dit doen wij door risico's inzichtelijk te maken, beheersmaatregelen in te richten en organisaties te begeleiden bij implementatie, monitoring en toetsing. Niet als eenmalige actie, maar als een doorlopend proces dat meebeweegt met veranderingen in technologie, wet- en regelgeving en organisatieontwikkeling.

IT-noodpakket samenstellen
Wat wij kunnen betekenen:
- Inventariseren welke systemen en data kritiek zijn voor jouw
- bedrijfsvoering
- Opstellen van actuele documentatie van kernsystemen, toegangen en leverancierscontacten
- Uitvoeren van risicoanalyses
- Voorbereiden van communicatie-templates voor verschillende scenario's (klanten, personeel, pers)

Digitaal continuïteitsplan ontwikkelen
Wat wij kunnen betekenen:
- Bepalen van crisisrollen en verantwoordelijkheden binnen jouw organisatie
- Uitwerken van heldere besluitvormings- en escalatielijnen
- Opstellen van interne en externe communicatieprotocollen
- Prioriteren van kritieke processen en systemen op basis van impact
- Afstemmen met leveranciers en ketenpartners over wederzijdse verwachtingen
- Uitwerken van herstelscenario's per type incident (ransomware, uitval leverancier, dataverlies)

Crisissituaties oefenen
Wat wij kunnen betekenen:
- Voorbereiden van table-top simulaties met management en IT om besluitvorming te testen
- Organiseren van leveranciers- en ketenoefeningen om externe afhankelijkheden te toetsen
- Evalueren van elke oefening en vertalen naar concrete verbeteracties
- Plannen van vervolgtoetsen om continu bij te blijven

Notities

Notities

Colofon

Samenstelling Jelmer van Heest, Ilana van Berkum, Sander Kerens
Ronald van Wanrooij
Eindredactie Ilana van Berkum en Florence van Hoof-Brugmans
Vormgeving Florence van Hoof-Brugmans
Fotografie David Stegenga
Druk Drukkerij Walden

Wil je direct in gesprek over de digitale weerbaarheid van jouw organisatie? Neem contact op met:

Ilana van Berkum
Senior Manager Risk & Compliance
+31 6 4249 3974

Daan Roozendaal
Senior Account Manager
+31 6 4993 9720

Wij denken graag met je mee over een passende aanpak voor jouw organisatie.

ITDS | EMBRACING CHANGE

ITDS | EMBRACING CHANGE