Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Digitale continuïteit en weerbaarheid op de bestuurstafel

Handreiking voor lijnmanager en CISO

Inleiding

Wat biedt deze handreiking?

De beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit van informatie- en communicatiesystemen en gegevens (data) zijn *chefsache*. Valt een primair proces stil door verstoring of uitval van telecom of IT (vanaf nu ICT) of gegijzelde bedrijfsdata? De directie is eindverantwoordelijk voor omzetverlies, reputatieschade en de maatschappelijke impact als direct gevolg hiervan. Maar wat als de directie het belang van digitale continuïteit en weerbaarheid niet voldoende inziet? Hoe stel je de directie in staat geïnformeerde besluiten te nemen over risico's en investeringen in digitale continuïteit en weerbaarheid? De aandachtspunten in dit document helpen om effectief het gesprek met de directie aan te gaan zodat zij dit belang inziet en in staat gesteld wordt om deze geïnformeerde besluiten te nemen.

Voor wie is deze handreiking?

De aandachtspunten in dit document richten zich op de lijnmanagers die verantwoordelijk zijn voor het voorkomen van ICT-incidenten en het beheersen van de impact op organisatieprocessen wanneer er een ICT-incident optreedt. Daarnaast richten de aandachtspunten zich op de ondersteuners van het lijnmanagement, zoals een Chief Information Security Officer (CISO) of een vergelijkbare functie, die het lijnmanagement en de directie van de juiste informatie dienen te voorzien.

Bijdrage aan deze handreiking
Deze handreiking is voortgekomen uit bijeenkomsten van Agentschap Telecom met en voor ICT-professionals en de inbreng van dr. Marcel Spruit, lector aan De Haagse Hogeschool en Lennert l'Amie, CISO van de Royal Schiphol Group. Het Digital Trust Center, ECP Platform voor de InformatieSamenleving en het Nationaal Cyber Security Centrum hebben bijgedragen aan de totstandkoming van deze handreiking.

Hoe is het advies opgebouwd?

Het deel *Kom in gesprek* bestaat uit drie uitgangspunten die helpen de ideale situatie te bereiken om effectief het gesprek met de directie aan te gaan. Het doel is de directie in staat te stellen geïnformeerde besluiten te nemen over risico's en investeringen in digitale continuïteit en weerbaarheid. Per uitgangspunt worden drempels beschreven die het belemmeren om de ideale situatie te bereiken met daarbij aandachtspunten om deze drempels weg te halen. Deze aandachtspunten helpen te komen tot de ideale situatie. Zijn de drempels weg? In het deel *Blijf in gesprek* worden een aantal aandachtspunten beschreven die helpen om ervoor te zorgen dat digitale continuïteit en weerbaarheid in de organisatie een *doorlopend* en *adaptief* proces is en een terugkerend onderwerp op de bestuurstafel blijft.

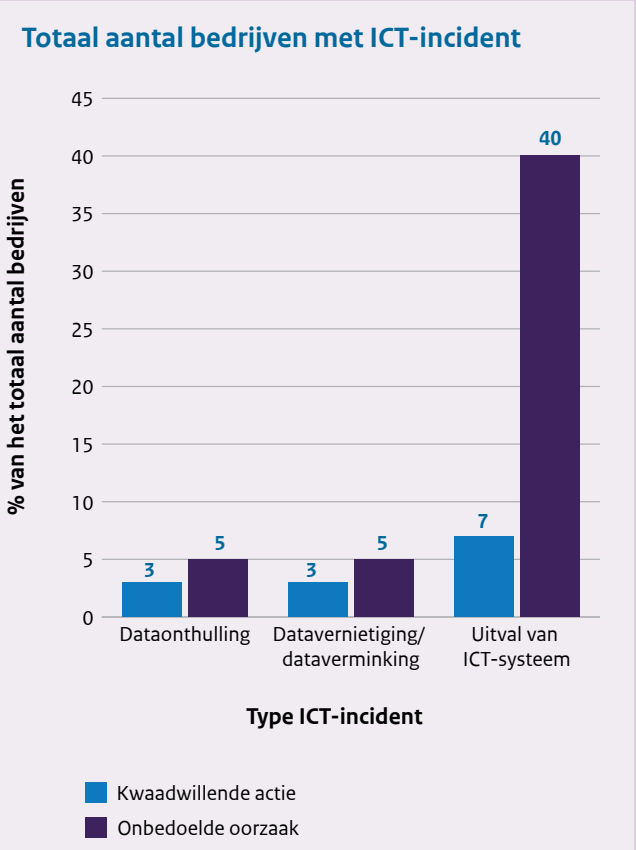
"Hoe stel je de directie in staat geïnformeerde besluiten te nemen over digitale continuïteit en weerbaarheid?"

Wat zijn ICT-incidenten?

Digitale continuïteit en weerbaarheid in dit document richt zich op voorkomen van en voorbereid zijn op verstoring of uitval van ICT en misbruik van ICT, oftewel ICT-incidenten, in de organisatie. ICT-incidenten kunnen gebeuren als gevolg van een kwaadwillende actie van binnenuit of buitenaf (cyberaanval) maar kunnen ook het gevolg zijn van een onbedoelde oorzaak (natuurlijke of niet-intentionele oorzaak). Denk aan software en hardware fouten, menselijke fouten, een overstroming, brand of stroomuitval. Denk hierbij ook aan uitval van ICT door een verstoring bij een dienstverlener aan wie een telecom- of IT-dienst is uitbesteed.

Hoe vaak komen ICT-incidenten voor?

Het Centraal Bureau voor de Statistiek (CBS) geeft jaarlijks in de Cybersecuritymonitor een beeld van hoeveel bedrijven te maken hebben gehad met een ICT-incident. Onderstaande grafiek geeft de cijfers voor 2020 per type ICT-incident weer:



Wat voor typen ICT-incidenten zijn er?

In de grafiek wordt onderscheid gemaakt tussen 2 soorten incidenten: ICT-incidenten als gevolg van een kwaadwillende actie (in blauw) en ICT-incidenten door een onbedoelde oorzaak (in paars). Voor beide groepen zijn drie type ICT-incidenten te onderscheiden: dataonthulling, datavernietiging/dataverminking en uitval van een ICT-systeem. Dit resulteert in totaal in 6 typen ICT-incidenten. Hieronder een omschrijving van elk type incident, inclusief een voorbeeld:

Voorbeelden van ICT-incidenten met een onbedoelde oorzaak

1. *Dataonthulling* door onopzettelijk toedoen van eigen personeel:
   - De camera's van een benzinestation zijn door een configuratiefout via internet voor iedereen toegankelijk.
2. *Datavernietiging of dataverminking* als gevolg van bijvoorbeeld een hardware- of softwarestoring:
   - Het bedrijfssysteem van een administratiekantoor heeft een hardware probleem en de backup blijkt onleesbaar.
3. *Uitval van ICT-systeem* als gevolg van een natuurlijke of niet-intentionele oorzaak bijvoorbeeld een hardware- of softwarestoring, brand of een stroomstoring:
   - Een ziekenhuis kan door een storing bij de clouddienstverlener niet bij het Elektronisch Patiënten Dossier.

Voorbeelden van ICT-incidenten door een kwaadwillende actie

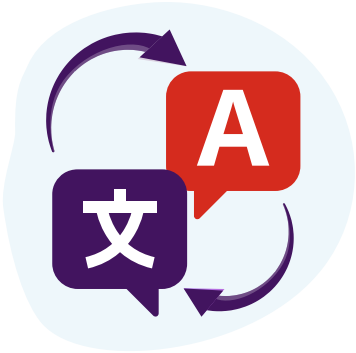
1. *Dataonthulling* door cyberinbraak, phishing of pharming:
   - Een medewerker van een tomatenkwekerij stuurt de inloggegevens van de bank naar aanleiding van een 'urgente mail van de directeur'.
2. *Datavernietiging of dataverminking* als gevolg van een infectie met kwaadaardige software of door ongeoorloofde elektronische toegang:
   - Een scholier verandert onvoldoendes in voldoendes in het administratiesysteem van haar school.
3. *Uitval ICT-systeem* als gevolg van een aanval van buitenaf, bijvoorbeeld door een DDoS (Denial of Service) of ransomware-aanval waarbij ICT-systemen niet meer gebruikt kunnen worden:
   - Een kartonfabriek moet door een ransomware-aanval het productieproces stilleggen.

Benieuwd naar de cijfers per bedrijfstak of bedrijfsgrootte? Zie voor meer informatie de Cybersecuritymonitor van het CBS.

Kom in gesprek

Dit deel bestaat uit drie uitgangspunten die helpen de ideale situatie te bereiken om effectief het gesprek met de directie aan te gaan.
Per uitgangspunt worden een aantal drempels omschreven die het lastig maken om de ideale situatie te bereiken. Daaraan gekoppeld zijn aandachtspunten om deze drempels weg te nemen. De volgende drie uitgangspunten komen aan bod:

A. Creëer wederzijds begrip en inzicht



B. Kies de juiste taal en boodschap

C. Beleg verantwoordelijkheden en maak procesafspraken

“Hoe zorg je voor de juiste vorm en inhoud in het gesprek met de directie over digitale continuïteit en weerbaarheid? ”

A. Creëer wederzijds begrip en inzicht

Er is wederzijds begrip nodig over het onderwerp tussen directie en het lijnmanagement en de CISO. De lijnmanager en CISO moeten inzicht hebben in wat de directie nodig heeft om geïnformeerde keuzes te kunnen maken over risico's en investeringen in digitale continuïteit en weerbaarheid. Andersom moet de directie (in hoofdlijnen) inzicht hebben in wat de lijnmanager en de CISO nodig hebben om ervoor te zorgen dat digitale continuïteit en weerbaarheid in de organisatie geborgd is. Welke drempels moeten weggenomen worden om wederzijds begrip en inzicht te creëren tussen de directie en het lijnmanagement en de CISO?

Drempels in de organisatie	Aandachtspunten
Digitale continuïteit en weerbaarheid heeft geen prioriteit Digitale continuïteit en weerbaarheid is slechts één van de prioriteiten waar geld, tijd en middelen voor beschikbaar moet zijn. De directie weegt meerdere belangen af, niet alleen die van digitale continuïteit en weerbaarheid.	**Neem zelf het initiatief** Wacht niet op de opdracht vanuit de directie om digitale continuïteit en weerbaarheid te borgen. Ga zelf met het verhaal naar de directie. Als expert heb je een beter beeld en kun je de directie voorzien van de benodigde informatie. Dit helpt de directie om de juiste inschatting te maken en de urgentie te zien zodat geïnformeerde keuzes gemaakt kunnen worden. De directie is nodig om mandaat te geven. Leg uit dat onduidelijkheid over verantwoordelijkheden ten koste gaat van preventie en tijdig ingrijpen.
Bagatelliseren van de risico's Het bagatelliseren van de risico's door de directie kan een terugkerend thema zijn. De directie is vaak eerder tevreden met het niveau van beveiliging dan de lijnmanager of CISO.	**Creëer een goed beeld van de risico's** De perceptie van risico's door de directie is meestal lager dan bij de lijnmanager of CISO. Zorg ervoor dat de directie een goed beeld krijgt van de risico's van verstoring van de organisatieprocessen en de gevolgen hiervan voor het behalen van de organisatiedoelen. Maak deze risico's inzichtelijk en begrijpelijk. Focus in het gesprek minder op de kans van een incident maar meer op de impact van een incident op de bedrijfscontinuïteit en het behalen van de organisatiedoelen. Gebruik voorbeelden uit een incidentenmonitoring (zie onderaan deze pagina) om de impact van een incident op organisatieprocessen te tonen. **Werk met scenario's** Maak kort en bondig helder wat de issues zijn. Laat de keuze aan de directie: leg een aantal realistische scenario's voor van deze issues en de oplossingen inclusief voor- en nadelen. Bijvoorbeeld een scenario van een ransomware aanval, uitval van een IT-leverancier of een hardware storing.
Verkeerd imago: digitale continuïteit en weerbaarheid als kostenpost Digitale continuïteit en weerbaarheid wordt buiten de expert primair als kostenpost of als last ervaren en niet als mogelijke *enabler* van continuïteit en groei.	**Vertaal in waarde** Toon de waarde die maatregelen voor digitale continuïteit en weerbaarheid toevoegen, bijvoorbeeld in een business case. Vertaal de expertkennis naar bedragen: wat zijn de kosten van mitigatie en wat bespaar je met het uitvoeren van de maatregel. Een organisatie die de risico's beheerst kan ervoor zorgen dat bij ICT-incidenten de impact wordt geminimaliseerd. Daardoor kunnen organisaties net een stapje extra zetten vergeleken met de concurrent als het gaat om betrouwbaarheid.
Waan van de dag De directie verschuilt zich achter korte termijndoelen en andere belangen gaan voor. Er is een natuurlijke neiging tot 'niet willen weten'.	**Haal de directie uit eigen 'bubble'** Benoem in het gesprek dat aandacht voor digitale continuïteit en weerbaarheid een gevoel van onzekerheid of extra druk kan opleveren over verantwoording, maar dat het voor de langere termijn onmisbaar is voor de organisatie. Probeer de directie mee te krijgen door hen zelf mee te laten denken. Als overtuigen op de inhoud niet lukt, overtuig op bestuurlijk afbreukrisico. Relevante voorbeelden van (bijna) incidenten binnen dezelfde sector kunnen ook helpen om de directie uit hun eigen 'bubble' te halen.

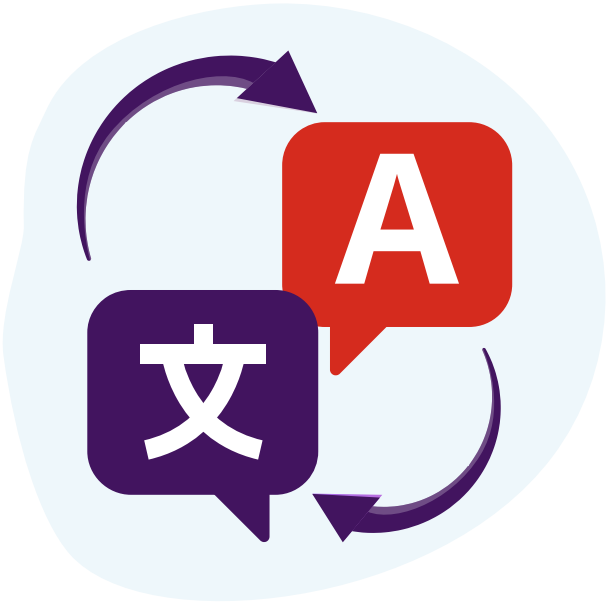
Het belang van incidentenmonitoring en incidentenanalyses

Registreer de grote én kleine (of bijna) ICT incidenten in de organisatie. Deze voorbeelden helpen in het gesprek met de directie. Besteed in de monitoring aandacht aan de oorzaak van de verstoring én de (potentiële) gevolgen van een verstoring op de organisatieprocessen. De gevolgen van een verstoring laten zien *hoe* de organisatie geraakt wordt. Geef ook aan op welke wijze de organisatie gehandeld heeft en wat (eventueel) verbeterd kan worden. Het helpt om ook bijna-incidenten mee te nemen om de effectiviteit van genomen maatregelen aan te tonen. Analyseer incidenten met grote impact, en bijna-incidenten met een potentiële grote impact, die aansprekend zijn voor de organisatie. Al deze voorbeelden van (bijna) incidenten helpen in het gesprek met de directie om de urgentie van het borgen van digitale continuïteit en weerbaarheid aan te tonen.

Op zoek naar voorbeelden van ICT incidenten?
Zijn er nog geen voorbeelden van (bijna) incidenten binnen de eigen organisatie? Ga in gesprek met andere (vergelijkbare) organisaties, bijvoorbeeld via een brancheorganisatie. Leer van elkaar. Is dit niet mogelijk? Op de website van het Digital Trust Center zijn verschillende voorbeelden te vinden van cyberincidenten bij ondernemers. Of bekijk in het rapport van de Onderzoeksraad voor Veiligheid voorbeelden van ICT uitval in ziekenhuizen. Voorbeelden uit de media kunnen ook naar de eigen organisatie vertaald worden. Bijvoorbeeld de 'lessons learned' van de cyberaanval op Universiteit Maastricht, gemeente Lochem of Maersk.

B. Kies de juiste taal en boodschap

Om wederzijds begrip en inzicht te creëren is de juiste taal en boodschap nodig. De juiste boodschap gaat over het verhaal dat de lijnmanager en CISO overbrengen aan de directie. De lijnmanager en de CISO spreken de juiste taal en appelleren aan de belevingswereld van de directie. Maar wat is de juiste taal en boodschap en welke drempels maken het moeilijk om als expert de juiste boodschap te kiezen?



Drempels in de organisatie	Aandachtspunten
Verschil in urgentie Urgentie voor securitymensen is niet altijd hetzelfde als business urgentie. En zonder incidenten ontbreekt vaak 'de sense of urgency' voor de directie om geld/tijd/middelen te besteden aan digitale continuïteit.	**Om het gesprek te openen kunnen uitkomsten besproken worden van:** 1. Incidentenanalyses: neem de directie mee in (potentiële) zwakheden in de digitale en fysieke omgeving en toon de impact van een ICT incident op de organisatieprocessen en de organisatiedoelen. 2. Pentesten: uitkomsten uit een pentest kunnen als bijna-incident gebruikt worden. 3. IT-Audits: uitkomsten van een IT-audit kan zwakheden in de digitale en fysieke omgeving aantonen. 4. Inspecties of onderzoeken van (interne) toezichthouders: uitkomsten van een inspectie of een onderzoek van de toezichthouder helpen om de urgentie aan te tonen om als organisatie compliant te worden.
Digitale continuïteit als doel op zich Experts kunnen vanuit een "ivoren beveiligingstoren" redeneren en digitale continuïteit *an sich* belangrijk maken zonder uitleg over de impact op de organisatieprocessen als digitale continuïteit niet gewaarborgd is.	**Werk vanuit eigen organisatieprocessen** Doorgrond en werk vanuit de eigen processen. Ga na welke kritieke organisatieprocessen afhankelijk zijn van ICT. Vergelijk bijvoorbeeld ook hoe de processen van een aantal jaar geleden en nu veranderd zijn en wat dit voor de organisatie betekent. Zijn er ICT-diensten die een aantal jaar geleden nog niet essentieel waren maar inmiddels onmisbaar zijn voor de kritieke organisatieprocessen? Zijn er kritieke ICT-processen en diensten uitbesteed aan derden? Vermijd valkuilen zoals: de *apocalypse now* valkuil: 'Nu niet ingrijpen betekent dat alles stilvalt'. Dat kan één keer en nooit weer. de *SMAC (social media analytics cloud)* valkuil: 'Onze voorstellen zijn nodig want alles is online en digitaal'. de *digital transformation* valkuil: 'Onze voorstellen zijn nodig want iedereen digitaliseert'.
Half oog op organisatiedoelen Als expert teveel focus leggen op het eigen proces en te weinig in relatie tot organisatiedoelen.	**Redeneer vanuit organisatiedoelen** Directiebetrokkenheid bereik je door de juiste vragen: welke kant wil de organisatie op? Wat hebben we hiervoor nodig? Wijs op technologische innovaties die zorgen voor nieuwe risico's. Geef aan wat de lijn daarbij nodig heeft. Bied altijd een oplossing voor het probleem dat je aandraagt. Het helpt om hierbij aan te geven hoe een investering in digitale continuïteit en weerbaarheid bijdraagt aan de doelen, missie en visie van de organisatie.
Andere taal Experts spreken niet dezelfde taal als de directie: de taal van financiële risico's en kosten van mitigatie.	**Pas je taal aan op de directie** Wees in het gesprek mild voor de directie en gebruik geen jargon. Bewustzijn beïnvloeden vraagt andere vaardigheden dan technische expertise op het gebied van digitale continuïteit en weerbaarheid. Pas je taalgebruik hierop aan. Focus minder op de digitale dreiging voor de organisatie maar meer op de business impact. Toon de impact van een ICT-incident op de bedrijfscontinuïteit en geef aan hoe hierdoor het behalen van de organisatiedoelen mogelijk bedreigd worden.
Verkeerde spreker Het inhoudelijke verhaal wordt niet verteld door een deskundige, maar bijvoorbeeld door een programmamanager.	**Ga als deskundige zelf het gesprek aan** Ga als lijnmanager of CISO zelf in gesprek met de directie. Test van tevoren of het verhaal overkomt bij een collega die geen technische expert is.

C. Beleg verantwoordelijkheden en maak procesafspraken

Om het gesprek met de directie effectief te voeren is het van belang dat organisatorisch de basis goed is ingericht. Wanneer de rollen en verantwoordelijkheden effectief zijn belegd kunnen er procesafspraken gemaakt worden binnen de organisatie om digitale continuïteit en weerbaarheid blijvende aandacht te schenken. Deze procesafspraken zijn vastgelegd, ook over samenwerking met ketenpartners. Welke drempels belemmeren het om verantwoordelijkheden te beleggen en procesafspraken te maken?

Drempels in de organisatie	Aandachtspunten
Geen stabiele basis voor digitale continuïteit en weerbaarheid Er mist een stabiele basis doordat communicatie over risico's van uitval en misbruik van ICT via verschillende lagen naar de directie komt en/of alleen wanneer er een incident heeft plaatsgevonden.	**Beleg digitale continuïteit en weerbaarheid onder Business Continuity Management (BCM)** Een incident heeft nut om digitale continuïteit en weerbaarheid op de agenda te krijgen, maar een incidentgedreven aanpak is geen stabiele basis voor BCM. Maak digitale continuïteit en weerbaarheid onderdeel van het BCM-plan in de organisatie (zie ook ISO norm 22301/22313) en zorg voor een integrale aanpak waarbij risico-, crisis- en continuïteitsmanagement samenkomen. Weet wat er in de organisatie moet gebeuren als, ondanks alle maatregelen, uitval of misbruik van ICT alsnog voorkomt. Immers, uitval of misbruik van ICT is nooit 100% te voorkomen. Maar door voorbereid te zijn wordt de impact ervan op de bedrijfscontinuïteit beperkter. Maak duidelijk onderscheid tussen maatregelen om risico's en/of impact te verkleinen en noodzakelijke acties tijdens een incident. Zorg ook voor één aanspreekpunt.
Gebrek aan structuur Risicomanagement vindt ad hoc plaats en is niet gewaarborgd in de organisatie.	**Hanteer de '3 lines of defense'** Het '3 lines of defense' model is een methode om risicomanagement in de organisatie te borgen. De kern: Maak dagelijkse werkafspraken, zorg voor security management en vervolgens interne audits. Dit model is gekoppeld aan de norm voor risicomanagement zoals ISO31000 en het Coso Enterprise Risk Management framework.
Geen terugkerend item Digitale continuïteit en weerbaarheid heeft niet blijvend de aandacht binnen de organisatie.	**Digitale continuïteit en weerbaarheid als KPI** Maak van digitale continuïteit en weerbaarheid een Kritieke Prestatie-Indicator (KPI) zodat het terugkomt in managementrapportages. Op deze manier blijft het onderwerp onder de aandacht binnen de organisatie. Bijvoorbeeld door onbeschikbaarheid in gebruikersminuten (aantal getroffen gebruikers maal duur van het incident) aan te geven.
Uitval bij ketenpartners Niet elke ketenpartner heeft aandacht voor digitale continuïteit en weerbaarheid.	**Ken je ketenpartner** Stel digitale veiligheidseisen bij inkoopprocessen. Voorkom dat je alleen over functionaliteiten spreekt, maar neem digitale veiligheid mee in de contracten en periodieke afstemming met ketenpartners. Bijvoorbeeld door contractuele eisen te stellen aan security management en BCM. Zorg voor inzicht in de risico's die deze afhankelijkheid met zich mee brengt. Bespreek welke extra maatregelen in jouw organisatie en bij de ketenpartner genomen kunnen worden om deze risico's te beperken. Naarmate de afhankelijkheid van een externe partij groter is, zullen er zwaardere eisen worden gesteld. Besteed extra aandacht aan je IT dienstverlener(s). Dit is een belangrijke ketenpartner als het gaat om het borgen van digitale continuïteit en weerbaarheid. Realiseer je daarnaast dat ketenpartners ook afhankelijk van jou kunnen zijn. Werk ook binnen ketens risico-gestuurd: vanuit het eigen primaire proces. Stel prioriteiten waar je je op richt en accepteer waar nodig risico's waarvan de kosten om deze te mitigeren niet opwegen tegen de baten.
Geen betrokkenheid vanuit primair proces De werkvloer wordt niet gevraagd serieus mee te denken.	**Bewustzijn begint op de werkvloer** Maak medewerkers medeverantwoordelijk voor BCM en digitale continuïteit van hun proces. Bewustzijn begint met de mensen op de werkvloer. Zij weten als geen ander de impact van uitval of misbruik van ICT op het primaire proces. Haal de input bijvoorbeeld uit workshops in de organisatie. Het kan hierbij helpen om 'ambassadeurs' in de organisatie te hebben (op verschillende lagen) die het belang van digitale continuïteit en weerbaarheid uitdragen.

In het algemeen is het volgende nodig om organisatorisch de basis in te richten:

De directie

De directie (ook wel het Managementteam, bestuur of hoogste bestuursorgaan genoemd) is eindverantwoordelijk voor digitale continuïteit en weerbaarheid en zorgt ervoor dat duidelijk is wie waarvoor verantwoordelijk is. Zij beleggen eigenaarschap en sturen op de invulling ervan. De directie neemt het besluit over risico's en investeringen op het gebied van digitale continuïteit en weerbaarheid.

Het lijnmanagement

Het lijnmanagement (ook wel middenmanagement of de tactische laag genoemd) is verantwoordelijk voor de verschillende onderdelen van digitale continuïteit en weerbaarheid. Zij organiseren dat er expertise op dit gebied is en beleggen de verantwoordelijkheden binnen de afdelingen.

De CISO

De CISO (of een vergelijkbare functie) is de persoon met een adviserende, controlerende en coördinerende rol in dit geheel. De CISO is niet verantwoordelijk voor het waarborgen van digitale continuïteit en weerbaarheid, maar ondersteunt het lijnmanagement bij hun verantwoordelijkheid (zie ook de handreiking cybersecuritymaatregelen van het NCSC)

Vanuit hun rol zorgen in de ideale situatie het lijnmanagement en de ondersteuners, zoals de CISO, ervoor dat de experts binnen de organisatie de risico's op het gebied van digitale continuïteit en weerbaarheid in kaart brengen. Het lijnmanagement beoordeelt deze risico's, mede op basis van het advies van de CISO en de experts binnen de afdelingen. De directie is meestal geen expert, maar wordt door het lijnmanagement en de CISO in staat gesteld om geïnformeerde besluiten te nemen over risico's en investeringen in digitale continuïteit en weerbaarheid. In de praktijk kan dit in de organisatie anders zijn ingericht. Het belangrijkste is dat rollen en verantwoordelijkheden effectief zijn belegd.

Meer weten over rollen en verantwoordelijkheden?
De handreiking cybersecuritymaatregelen van het NCSC geeft een goed overzicht over de rollen en verantwoordelijkheden die nodig zijn om digitale continuïteit en weerbaarheid te borgen. De rol van de CISO en de inrichting van risicomanagement wordt nader beschreven in de factsheet Risicobeheersing van het NCSC. Daarnaast geeft het whitepaper 'Een robuustere cybersecurity' van The Hague Security Delta ook een goed beeld van de rol van de CISO.

"Welke rollen en verantwoordelijkheden moeten belegd worden om digitale continuïteit en weerbaarheid te borgen?"

Waar op te letten bij uitbesteding van ICT dienstverlening?

Veel organisaties hebben in meer of mindere mate hun ICT dienstverlening uitbesteed. Dit wordt ook wel “IT-outsourcing” genoemd. De externe serviceproviders leveren dan voor verschillende processen de software, hardware en bijbehorende diensten zoals beheer en onderhoud. Denk bijvoorbeeld aan het gebruik van clouddiensten. Maar wat als er een ICT-incident optreedt bij één van deze ketenpartners en jouw organisatie hierdoor geraakt wordt?

Hieronder een aantal tips waar op te letten bij uitbesteding van ICT dienstverlening:

- Zorg ervoor dat inzichtelijk is welke IT-dienstverleners (en ICT-leveranciers) essentieel zijn voor de organisatie en welke (primaire) organisatieprocessen afhankelijk zijn van hun dienstverlening. Weet wat de impact is van een potentiële verstoring bij deze ketenpartner op de bedrijfscontinuïteit.

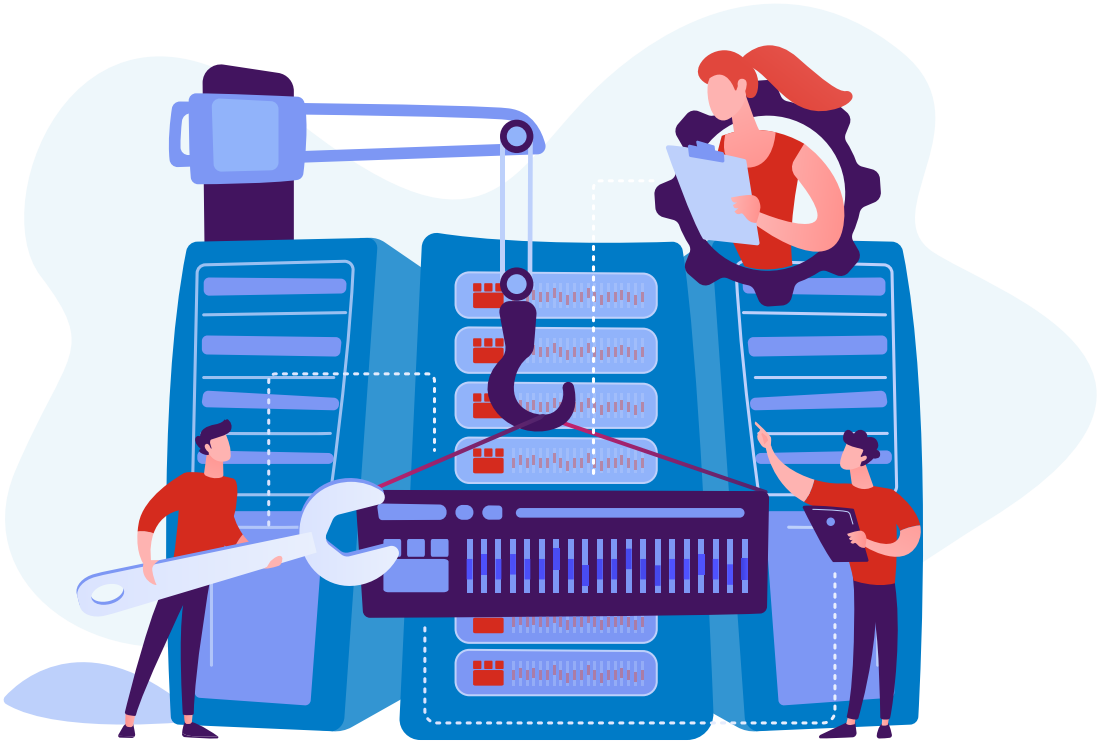
- Bespreek met de essentiële IT-dienstverleners wat de risico’s zijn van de uitbesteding en hoe deze risico’s ingeperkt kunnen worden. Werk hierbij nauw samen met de productowners in de organisatie die het contact met deze ketenpartners beheren. Zorg ervoor dat in het gesprek met hen niet alleen contractuele verplichtingen aan de orde komen, maar dat ook de risico’s besproken worden om te zorgen dat de kans en impact van een verstoring beperkt worden. Welke processen kunnen worden ingericht om risico’s te monitoren en hoe te reageren als er iets fout gaat?

- Sluit aan op bestaande audits in de eigen organisatie. Ga bijvoorbeeld het gesprek aan met de externe accountant die bij de jaarrekeningcontrole steeds vaker ook analyseert waar de bedrijfscontinuïteit afhankelijk is van externe ICT dienstverlening en of de organisatie de risico’s die hierbij komen kijken goed kent en beheerst.

- Sluit aan bij de onderzoeken die de externe IT-auditor uitvoert in de context van de financiële processen. Overleg met de directie om de scope van die onderzoeken gaandeweg te verbreden van alleen financiële aspecten naar de gehele ICT-omgeving (interne en geoutsourcete ICT-omgeving). Uit de onderzoeken van zowel een interne als externe IT-auditor komt als extra check naar voren wat de risico’s zijn van de uitbesteding en welke maatregelen bij de leverancier en binnen de eigen organisatie nodig zijn om de risico’s voldoende te beheersen.

- Vraag de IC-dienstverlener naar bestaande IT-audit rapportages en assurance rapportage zoals de ISAE 3402 of SOC2 verklaringen en certificeringen zoals ISO27001. Steeds vaker hebben dienstverleners deze rapportages beschikbaar om inzage geven in de risico’s (hun internationale en beursgenoteerde klanten vragen daar al om maar ook andere klanten kunnen dat vragen).

Meer weten over dit onderwerp?
Zie bijvoorbeeld het Good practices document over uitbesteding van De Nederlandsche Bank en de informatie van Norea over de IT-Auditverklaring.



Blijf in gesprek

Voer het gesprek met je directie: stem je boodschap af op de directie en spreek vanuit de doelen van de organisatie. De directie heeft als taak de doelen van de organisatie en de strategie te bepalen. Laat de directie meedenken over hoe deze organisatie-doelen mogelijk worden gemaakt door het borgen van digitale continuïteit en weerbaarheid in de organisatie. Geef in het gesprek met de directie aan hoe het behalen van deze organisatiedoelen mogelijk bedreigd wordt door risico's op het gebied van digitale continuïteit en weerbaarheid. Laat zien wat de impact is en de kosten zijn wanneer als gevolg van deze risico's de doelen niet behaald worden. Kom altijd met (potentiële) oplossingen hoe deze risico's voldoende beheerst kunnen worden.
Door de directie te voorzien van de juiste informatie worden zij in staat gesteld om geïnformeerde besluiten te nemen over risico's en investeringen op het gebied van digitale continuïteit. Dankzij de aanpak die is vastgelegd in procesafspraken kun je regelmatig de voortgang laten zien. Maar kom niet alleen in gesprek, blijf ook in gesprek. Hieronder volgen een aantal aandachtspunten die helpen om ervoor te zorgen dat digitale continuïteit en weerbaarheid een *doorlopend* en *adaptief* proces is en een terugkerend onderwerp op de bestuurstafel blijft:

"Hoe zorg je ervoor dat digitale continuïteit en weerbaarheid een terugkerend onderwerp op de bestuurstafel blijft?"

Blijf weerbaar

Het borgen van digitale continuïteit en weerbaarheid is een dynamisch proces: verouderde diensten en technieken worden uitgefaseerd; nieuwe risico's ontstaan bij het implementeren van innovaties; cyberdreigingen verschillen en een menselijke fout is niemand vreemd. Door digitale continuïteit en weerbaarheid onder BCM te beleggen blijf je weerbaar.
Test jaarlijks met uitval van ICT op de werkvloer, doe social engineering testen en voer bewustwordingscampagnes voor bijvoorbeeld informatiebeveiliging uit. Betrek de werkvloer bij de opzet en evalueer gezamenlijk het proces en de uitkomsten. Zorg voor blijvende aandacht voor digitale continuïteit en weerbaarheid in de gehele organisatie.

Blijvende aandacht bij directie

Zorg ervoor dat de directie het belang van digitale continuïteit en weerbaarheid blijft inzien. Praat hen jaarlijks bij aan de hand van de KPI's die zijn vastgelegd. Vertaal actuele voorbeelden van ICT-incidenten uit de landelijke media die goed passen naar de eigen organisatie. Laat bijvoorbeeld zien hoe uitgevoerde maatregelen succes hebben gehad en de organisatie beschermd hebben tegen een soortgelijk incident.

Wees toekomstgericht

De verwachting is dat business en digitale continuïteit en weerbaarheid, net als business en IT, steeds meer geïntegreerd raken. Waar gaat jouw organisatie naar toe, wat is nodig over vijf jaar? Breng veiligheid en business (innovatie) daarom bij elkaar. Leg potentiële conflicten tussen veiligheid en innovatie in de bestuurskamer op tafel. Kom daarbij niet alleen met problemen maar ook met oplossingen. Zorg ook voor een strategie voor digitale continuïteit en weerbaarheid op de lange termijn voor de organisatie.

Tools van Agentschap Telecom

Wil je weten wat je als ICT-professional kunt doen om jouw organisatie voor te bereiden op uitval van telecom of IT? Agentschap Telecom biedt tools om organisaties bewust te maken van hun afhankelijkheid van telecom en IT en helpt hen zich beter voor te bereiden op uitval.

Wil je weten hoe je digitale risico's voor jouw organisatie in kaart brengt?
Neem het Vijfstappenplan digitale continuïteit & weerbaarheid door
Het Vijfstappenplan bevat een aantal praktische instrumenten om jouw organisatie bewust te maken van de afhankelijkheid van ICT, digitale kwetsbaarheden te onderzoeken en digitale continuïteit en weerbaarheid in jouw organisatie te borgen. Deze handreiking is onderdeel van het Vijfstappenplan. Zie voor meer informatie: Vijfstappenplan

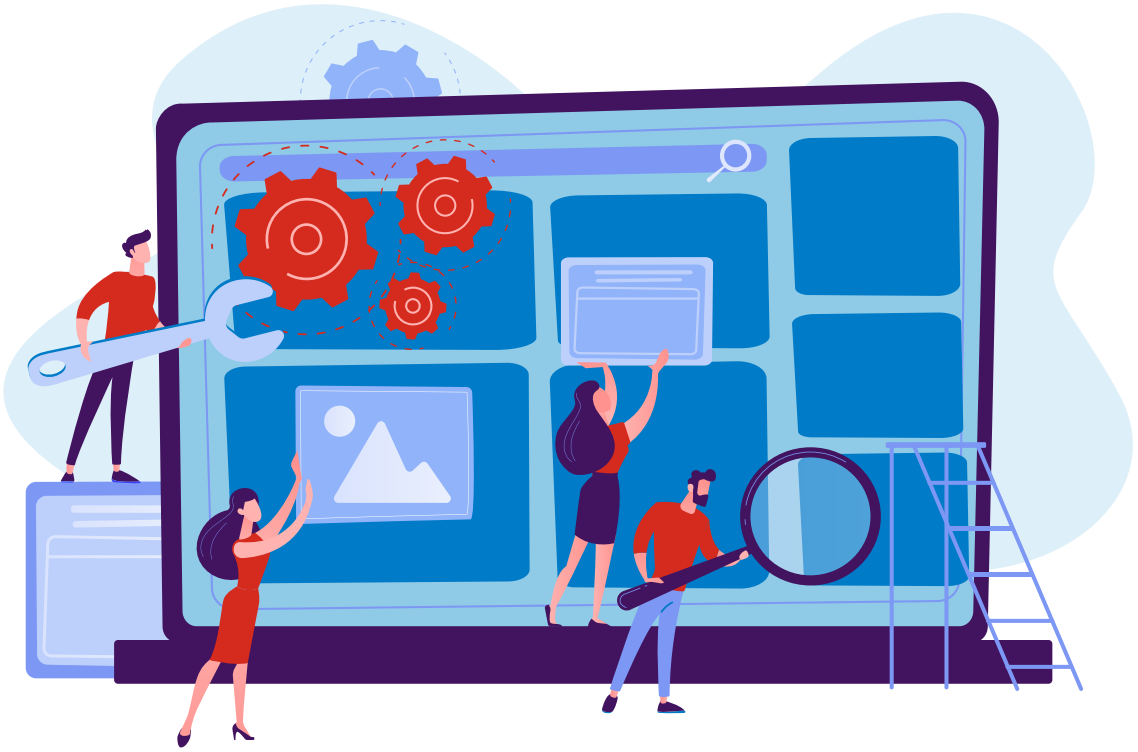
Wil je weten hoe goed jouw organisatie is voorbereid als telecom of IT uitvalt?
Doe de quickscan uitval telecom
De quickscan geeft een indruk hoe goed jouw organisatie is voorbereid op de gevolgen van uitval van telecom of IT. Na het invullen van de vragenlijst ontvang je een advies op basis van de door jou gegeven antwoorden. Dit advies kan je gebruiken als leidraad voor het gesprek met de directie. Zie voor meer informatie: Quickscan uitval telecom

Tools van het Digital Trust Center

Wil je meer weten over hoe je als ICT-professional aan de slag kunt met cyberweerbaarheid? Digital Trust Center (DTC) helpt jouw organisatie met advies en tools om je weerbaarheid te vergroten.

Wil je kennis en ervaring uitwisselen met andere cyber security professionals en dreigingsinformatie ontvangen?
Meld je aan bij de DTC Community
In de DTC Community blijf je in een besloten online omgeving op de hoogte van actuele dreigingsinformatie. Kom in contact met IT-, ICT- en cybersecurity verantwoordelijken van andere organisaties en deel kennis. Zie voor meer informatie: DTC Community

Wil je weten hoe groot de kans is op een cyberincident in jouw organisatie?
Vul de risicoklasse tool in
Aan de hand van 11 vragen wordt een schatting gemaakt hoe groot het risico is op een cyberincident. Deze inschatting bepaalt in welke risicoklasse (1 t/m 4) je onderneming valt en welke maatregelen je moet nemen om je digitale veiligheid op orde te hebben. De uitkomsten kan je gebruiken als leidraad voor het gesprek met bijvoorbeeld de directie. Zie voor meer informatie: Risicoklasse tool



Dit is een uitgave van:

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat
Postbus 450 | 9700 AL | Groningen
agentschaptelecom.nl

Oktober 2022 | Publicatie-nr. 22406229