Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

Handreiking

Risicomanagement voor digitale weerbaarheid

Werken aan de basis. Van Nederland en ons Koninkrijk.

Uitgave

CIO Rijk, afdeling IB&P
Turfmarkt 147, 2511 DP Den Haag
cisorijk@minbzk.nl

September 2025

Rechten

Inhoudsopgave

1 Inleiding

Voor een goede dienstverlening aan burgers en ondernemers is de overheid in grote mate afhankelijk van betrouwbare informatie. Die betrouwbaarheid staat voortdurend onder druk als gevolg van dreigingen op het digitale vlak, die vanwege de aantallen, complexiteit en professionaliteit om een goede beheersing vragen. Goed bestuur vereist een goede beveiliging van die informatie, waarbij nieuwe wetgeving verplicht om bij die beveiliging te kiezen voor een risicogebaseerde aanpak. Dit vraagt om een rijksbreed geaccepteerde en toegepaste aanpak voor gestructureerd risicomanagement voor digitale weerbaarheid. Deze handreiking geeft verdiepingen en aanvullende overwegingen op deze rijksbrede aanpak.

Doelgroepen

Deze handreiking vormt samen met de beleidsrichtlijn en de implementatierichtlijn één geheel. Deze documenten bieden een gestructureerde aanpak voor risicomanagement voor digitale weerbaarheid. Deze documenten zijn opgesteld voor verschillende doelgroepen.

- De beleidsrichtlijn is geschreven voor en vanuit het strategische perspectief van de bestuurders en lijnmanagers. Hierin wordt vooral uitgelegd wat er wordt verwacht op het gebied van risicomanagement voor digitale weerbaarheid.
- De implementatierichtlijn is technischer van aard en meer geschreven voor en vanuit het perspectief van de specialisten die de bestuurders en de lijnmanagers ondersteunen bij het uitvoeren van risicomanagement. Hierin wordt meer uitgelegd hoe invulling moet worden gegeven aan risicomanagement.
- Deze handreiking bevat verschillende verdiepingen en aanvullende overwegingen voor de uitvoering van risicomanagement en is vooral gericht aan de inhoudelijk specialisten.

Leeswijzer

De hierboven genoemde documenten behandelen risicomanagement voor digitale weerbaarheid. Om de leesbaarheid te vergroten is dit op sommige plekken in deze handreiking ingekort tot alleen de term risicomanagement.

Deze handreiking bevat verschillende onderwerpen ter inspiratie en ondersteuning voor de uitvoering van risicomanagement. Ieder hoofdstuk behandelt een apart onderwerp. Er zit geen inhoudelijke volgordelijkheid in de hoofdstukken.

Binnen informatiebeveiliging wordt vaak gesproken over applicaties en IT-systemen. Omdat applicaties en IT-systemen slechts een middel zijn om informatie te verwerken en voor de leesbaarheid van dit document, worden deze niet expliciet benoemd in deze handreiking. Echter, met het beveiligen van informatie wordt dus ook het beveiligen van applicaties en IT-systemen bedoeld.

2 Gebruikte definities

De begrippen risico, dreiging, incident, risicogebeurtenis en kwetsbaarheid worden veelvuldig gebruikt, soms zelfs als synoniemen. Voor effectief risicomanagement is het belangrijk om zorgvuldig onderscheid te maken tussen deze begrippen en om de onderlinge samenhang ervan te begrijpen. Het doel van de onderstaande lijst is niet om een nieuwe invulling van definities te introduceren, maar slechts om aan te geven welke invulling is gehanteerd bij het gebruik van deze begrippen in de beleidsrichtlijn, de implementatierichtlijn en deze handreiking. In andere hoofdstukken van deze handreiking wordt dieper ingegaan op sommige van deze begrippen.

Beschikbaarheid

De mate waarin informatie toegankelijk is, zoals bedoeld op zekere momenten en vanaf zekere locaties.

Integriteit

De mate waarin informatie juist, volledig en actueel is.

Vertrouwelijkheid

De mate waarin informatie exclusief toegankelijk is voor de daartoe geautoriseerde personen.

Dreiging

Een dreiging is een wijze waarop het behalen van doelstellingen negatief beïnvloed kan worden. Een dreiging is beschreven in de vorm van een gebeurtenis. In het geval van digitale weerbaarheid vindt de negatieve beïnvloeding van het behalen van doelstellingen plaats door aantasting van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Kwetsbaarheid

Een kwetsbaarheid is het ontbreken of niet goed werken van een maatregel ter bescherming van de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie. Hierdoor kan een dreiging zich manifesteren tot een incident of wordt de kans daarop vergroot. Kwetsbaarheden kunnen van technische of organisatorische aard zijn, maar bestaan ook in de vorm van menselijk handelen.

Actor

Een persoon of een groepering die door moedwillig of onbewust handelen zorgt voor een inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie. Die inbreuk kan het doel zijn, maar kan ook optreden als bijeffect.

Een actor wordt in de praktijk vaak als iemand met kwade intenties gezien. Het is echter goed om te realiseren dat ook mensen met goede bedoelingen voor beveiligingsincidenten kunnen zorgen. Neem deze groep mensen daarom mee in bij de uitvoering van een risicoanalyse.

Risico

Een risico is een dreiging, voorzien van een of meerdere oorzaken, een of meerdere gevolgen, een ingeschatte hoogte van de kans en een ingeschatte hoogte van de impact, welke allemaal betrekking hebben op de organisatie. Het dreigingsdeel in een risicobeschrijving wordt ook wel de risicogebeurtenis genoemd.

Het bruto risico is het risico waarbij voor de bepaling van de hoogte (kans x impact) geen rekening is gehouden met mitigerende maatregelen. Het netto risico (restrisico) is het risico waarbij voor de bepaling van de hoogte wel rekening is gehouden met mitigerende maatregelen.

Soms wordt het verschil tussen bruto en netto ook bekeken vanuit een risicoanalyse. Het bruto risico is dan het risico voorafgaand aan de risicoanalyse, dus inclusief de dan aanwezige maatregelen. Het netto risico is het risico dat overblijft na de implementatie van de maatregelen die tijdens de risicoanalyse zijn bepaald.

Incident

Een incident is een manifestatie van een risico. Een incident kan het gevolg zijn van het handelen van een actor, maar ook van een toevallige samenloop van omstandigheden.

3 Informatiemanagement

Om informatie goed te kunnen beveiligen, is het noodzakelijk om goed zicht te hebben op die informatie. Hierdoor kunnen maatregelen effectiever en efficiënter worden doorgevoerd. We kunnen stellen dat informatiemanagement een zeer belangrijke basis is voor informatiebeveiliging.

Zicht op informatie

Zicht op informatie is vooral belangrijk bij de uitvoering van een risicoanalyse. Weten om welke informatie het gaat, wat de waarde is van deze informatie (in termen van beschikbaarheid, integriteit en vertrouwelijkheid), in welke systemen deze informatie opgeslagen ligt en wie er wat mee doet helpt bij het vinden van risico's en het vaststellen van de hoogte van deze risico's.

Bij voorkeur zijn dit soort overzichten opvraagbaar bij de informatiebeheerafdeling. Als zo'n afdeling niet binnen de organisatie aanwezig is of als deze afdeling niet over zo'n overzicht beschikt, dan is het verstandig om zo'n overzicht ter voorbereiding op de analysesessie zelf te maken.

Mogelijk kunnen ICT-architecten helpen bij het opstellen van een overzicht van het informatielandschap. Let daarbij goed op dat het resultaat leesbaar is voor mensen die geen achtergrond hebben in ICT-architectuur.

Eigenaarschap van informatie

Goed informatiemanagement valt of staat bij het juist inrichten van het eigenaarschap van informatie. Eigenaarschap voor informatie behoort te liggen bij mensen met het juiste mandaat om beslissingen te kunnen nemen over informatie. Lijnmanagers komen om die reden het meeste in aanmerking hiervoor. De hoogste bestuurder van de organisatie is verantwoordelijk voor het aanwijzen van informatie-eigenaren, het toekennen van de bijbehorende verantwoordelijkheden
en het aanspreken van de informatie-eigenaren op de invulling van hun eigenaarschap.

Typische verantwoordelijkheden die horen bij informatie-eigenaarschap zijn het bepalen van de toegangsrechten, het vaststellen van de classificatie (beschikbaarheid, integriteit en vertrouwelijkheid), het maken van afspraken met de ICT-beheerorganisatie over de wijze waarop de informatie beschikbaar wordt gesteld (SLA, applicatiebeheer, et cetera), het maken van afspraken met andere instanties over de omgang met informatie bij de uitwisseling van die informatie, beheer van de kosten voor de gehele informatieverwerking en het beheersen van de risico's ten aanzien van de informatie.

4 Actoren

Incidenten kunnen het gevolg zijn van de acties van actoren. Hoe bedreigend zo'n actor is, is afhankelijk van de kennis die een actor bezit, de middelen waarover een actor beschikt en de motivatie van een actor om een gerichte aanval uit te voeren. Actoren kunnen kwaadwillende mensen of groeperingen zijn, zoals statelijke actoren, criminelen, hacktivisten en script kiddies, maar ook mensen met goede bedoelingen die door onoplettendheid of gebrek aan kennis voor een incident zorgen, zoals medewerkers. Er zijn externe actoren (actoren buiten de organisatie) of interne actoren (mensen die werkzaam zijn binnen de organisatie).

Stel een lijst op van actoren en geef op basis van bovengenoemde eigenschappen een score van 1 t/m 5 aan de dreiging dit uitgaat van een actor. De betekenis van deze waarden is als volgt:

1. Verwaarloosbaar
2. Gering
3. Gemiddeld
4. Bedreigend
5. Zeer bedreigend

De scoringswaarde heeft naast het aangeven van hoe bedreigend een actor is, ook nog een andere toepassing, welke uitgelegd staat in hoofdstuk 8, genaamd 'Kans'.

Deze actorenlijst is nuttig bij de uitvoering van een risicoanalyse, maar hoeft niet voor iedere risicoanalyse bijgewerkt te worden. Doe dit jaarlijks of wanneer daar aanleiding toe is.

Voor advies over het in kaart brengen van actoren of de dreigingen die van hen uitgaan, raadpleeg de website van het NCSC, de AIVD of de NCTV of neem in het geval van concrete vragen of urgente dreigingen contact met hen op.

5 Dreigingen

Tijdens een risicoanalyse worden dreigingen besproken. Het is verstandig om een lijst van mogelijke dreigingen beschikbaar te hebben tijdens een risicoanalyse. Dit geeft de deelnemers van de analysesessie houvast en een denkrichting.

Op het internet zijn dreigingslijsten te vinden, die als uitgangspunt gebruikt kunnen worden.

- ENISA: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox
- ATT&CK: https://attack.mitre.org/
- NIST 800-30: https://www.nist.gov/privacy-framework/nist-sp-800-30
- RAVIB: https://www.ravib.nl/koppelingen
- VNG: https://www.informatiebeveiligingsdienst.nl/product/diepgaande-risicoanalyse-methode-excel/

Bij voorkeur wordt zo'n lijst van mogelijke dreigingen aangevuld met nieuwe dreigingen die tijdens een risicoanalyse zijn vastgesteld. Op deze manier wordt de lijst meer organisatie-specifiek.

Bij het opstellen van een eigen dreigingenlijst is het goed om per dreiging scherp te hebben of deze een bedreiging vormt voor de beschikbaarheid, de integriteit of de vertrouwelijkheid van de informatie. Dat helpt bij het bepalen van de impact van een mogelijk bijbehorend incident en het vinden van passende tegenmaatregelen.

6 Risicomatrix

De risicomatrix is een hulpmiddel bij het uitvoeren van een risicoanalyse. Stel een risicomatrix op voor de organisatie. Hanteer onderstaande risicomatrix als voorbeeld.

impact \ kans	zeer klein	klein	gemiddeld	groot	zeer groot
desastreus	hoog	hoog	kritiek	kritiek	kritiek
groot	midden	hoog	hoog	kritiek	kritiek
gemiddeld	laag	midden	hoog	hoog	hoog
klein	laag	laag	midden	midden	midden
minimaal	laag	laag	laag	laag	midden

Het zal opvallen dat bovenstaande matrix niet symmetrisch is over de diagonale as van linksonder naar rechtsboven. Hiervoor zijn de volgende twee redenen.

Weging kans en impact

Als eerste, bij een volledig symmetrische risicomatrix weegt een risico met een zeer kleine kans en desastreuse impact voor de organisatiedoelen even zwaar als een risico met een zeer grote kans en minimale impact voor de organisatiedoelen. Dat zou een onjuiste conclusie zijn. Zolang een risico minimaal tot geen effect heeft op de organisatiedoelen, kan de organisatie besluiten om geen risicobeperkende maatregelen te treffen. Daarentegen zal de organisatie in het algemeen risico's met mogelijk desastreuse gevolgen voor de realisatie van de organisatiedoelen niet accepteren, al is de kans daarop minimaal. In dergelijke gevallen mag verwacht worden dat maatregelen worden getroffen om de gevolgen van dergelijke risico's tot op een voor de organisatie acceptabel niveau te beperken. Het is verstandig om daarmee in de risicomatrix rekening te houden.

Vluchtigheid van het aspect kans

De tweede reden is de vluchtigheid van het aspect kans. De kans van een risico kan sneller veranderen dan de impact. Om de impact te veranderen is vaak een verandering nodig in wat een organisatie doet. Dat is niet van het ene op het andere moment doorgevoerd. De kans kan wel van het ene op het andere moment veranderen. De motivatie van een kwaadwillende actor kan veranderen door bijvoorbeeld een beslissing of uitspraak op politiek niveau. De benodigde kennis om een aanval uit te voeren kan veranderen door het bekend worden van een kwetsbaarheid. Helemaal als daar een kant en klare exploit voor wordt uitgegeven. Om die reden gaan de verticale lijnen bij de kansen 'zeer klein' en 'klein' naar een hoog risico, terwijl de horizontale lijnen bij impact 'minimaal' en 'klein' tot een midden risico gaan.

Aantal risiconiveaus

Naast de keuze voor de grootte van de matrix (in bovenstaand voorbeeld is dat dus 5 bij 5), is er ook de keuze voor het aantal risiconiveaus in de matrix. In bovenstaande matrix zijn dat vier niveaus: laag, midden hoog en kritiek. Voor het aantal niveaus kan men gebruik maken van het aantal managementlagen met tekenbevoegdheid voor de acceptatie van een risico. Zoals in het hoofdstuk 'Risicobereidheid' van de implementatierichtlijn wordt beschreven, moet om een risico te accepteren dat boven de acceptatiegrens valt, een akkoord van een manager worden verkregen. Omdat je niet voor ieder risico naar de hoogste bestuurder wil stappen, kunnen dat managers op meerdere niveaus zijn. Stel, je hebt als organisatie te maken met drie goedkeuringsniveaus. Dan is het zinvol om voor je matrix vier risiconiveaus te kiezen. Namelijk, een niveau dat de risicobereidheid aangeeft (het groene niveau in de matrix) en drie niveaus voor de acceptatie van risico's die buiten de acceptatiegrens liggen (de niveaus geel, oranje en rood in de matrix).

Het gebruik van een en dezelfde matrix bij risicoanalyses zorgt ervoor dat analyses op een consistente manier worden uitgevoerd, waardoor deze met elkaar vergelijkbaar zijn. Hierdoor is het mogelijk om te zien of situaties door de tijd heen verbeteren of verslechteren en hoe verschillende organisatieonderdelen ten opzichte van elkaar presteren.

Wees zeer terughoudend in het aanbrengen van wijzigingen in de matrix nadat deze is toegepast in een risicoanalyse, omdat dat mogelijk gevolgen heeft voor de resultaten van eerder uitgevoerde risicoanalyses.

7 Risico

Het doel van een risicoanalyse is het in kaart brengen van de oorzaken en gevolgen van de risico's en het beoordelen en rangschikken van de risico's. Een goed begrip van wat een risico precies is, is dan ook belangrijk. Risico is meer dan alleen de combinatie van kans en impact. In dit hoofdstuk wordt daar verder op ingegaan.

Verschil tussen risico's en feiten

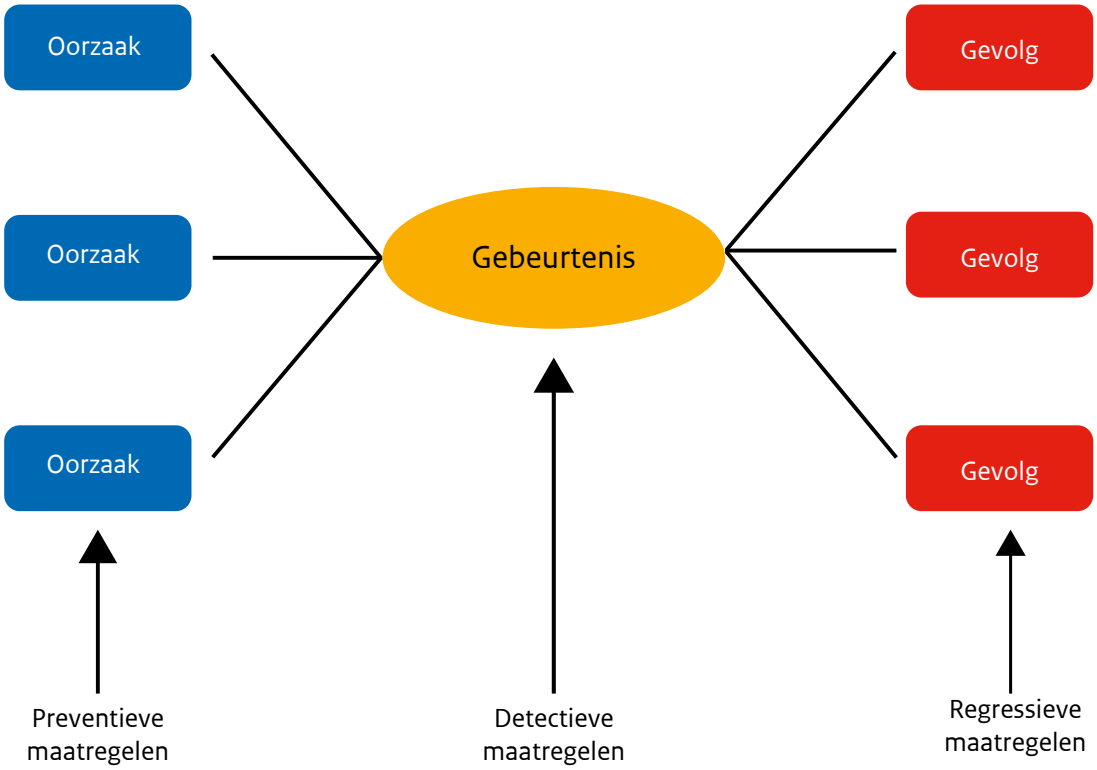
In de context van digitale weerbaarheid van informatie is een risico een gebeurtenis dat met een zekere kans een impact kan hebben op de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie. Bedreigingen waarbij er geen sprake is van een kans, zijn geen risico's en moeten dus ook niet tijdens een risicoanalyse behandeld worden. Zo is een ransomware aanval, mits die zich niet op dat moment voordoet, een risico. Er is sprake van een kans op een ransomware-aanval en zo'n aanval heeft een zekere impact. Zo is bijvoorbeeld het hebben van legacy-systemen geen risico. Als je ze hebt, dan is het een feit. Er is geen sprake van een kans.

Het hebben van legacy-systemen zelf is dus niet iets wat je tijdens een risicoanalyse als risico behandelt. Echter, het hebben van legacy-systemen is wel een interessant gegeven voor een risicoanalyse, want het vergroot mogelijk de kans op bijvoorbeeld een ransomware-aanval. Het hebben van legacy-systemen vormt dus een kwetsbaarheid. Het is daarmee een mogelijke oorzaak van een risicogebeurtenis.

Oorzaak, gebeurtenis en gevolg

Een incident gebeurt niet zomaar. Het heeft altijd een of meerdere oorzaken. En hoe onwenselijk een incident is, is vooral afhankelijk van de gevolgen ervan. Om een risico goed te begrijpen, is het zinvol om deze kenmerken goed in kaart te brengen. Een bowtie-diagram, zoals hieronder weergegeven, helpt bij het visualiseren en begrijpen van de oorzaken, de gebeurtenis en de gevolgen van een risico. Een bowtie-diagram is bedoeld voor een enkel risico. Daarin staat de risicogebeurtenis centraal. Links van de gebeurtenis staan de oorzaken en rechts van de gebeurtenis staan de gevolgen. Een bepaalde oorzaak kan weer een andere oorzaak hebben en een bepaald gevolg van weer leiden tot een ander gevolg. Een bowtie-diagram kan daarmee zeer uitgebreid ingevuld worden, maar het is verstandig om daar niet in door te schieten. Het doel is om inzicht te krijgen in een risico.

Naast het goed definiëren van het risico zelf, helpt het maken van een bowtie-diagram ook bij het selecteren van de juiste maatregelen. Oorzaken pak je aan met preventieve maatregelen en de gevolgen pak je aan met repressieve maatregelen. De kans dat een onwenselijke gebeurtenis onopgemerkt gebeurt, verlaag je door middel van detectieve maatregelen.



Lijn

Bij het inschatten van de kans en de impact van een risico, worden beide vaak vertaald naar een waarde. Een risico wordt daarbij gezien als een stip op de matrix. Echter, in de praktijk is een risico meestal een lijn over de matrix. Zo hebben we generieke malware dat dagelijks als hagelschot over het internet wordt afgeschoten en dat door de meeste anti-malware-oplossingen direct wordt onderschept. Daarnaast hebben we malware met een zero-day exploit die doelgericht worden ingezet. De eerste heeft een grote kans en een kleine impact. De laatste heeft een kleine kans (omdat het niet vaak voorkomt) en een grote impact. Tussen deze twee uiterste hebben we vele varianten, die uitgezet in de risicomatrix, een lijn vormen.

De risicolijn in de matrix gaat door vele kans/impact-combinaties heen. Al deze combinaties behandelen levert onnodig veel werk op. Kies daarom tijdens een risicoanalyse de kans/impact-combinatie die het hoogste risico oplevert. Hierdoor krijgen de mitigerende maatregelen de hoogst mogelijke prioriteit.

8 Kans

Het goed inschatten van de kans van een risico is voor velen een lastige opgave. Een verkeerd ingeschatte kans kan leiden tot een onterechte acceptatie van een risico of tot een onjuiste prioritering van mitigerende maatregelen, met risicoblootstelling als gevolg. Een vrij te bepalen kans geeft ook de mogelijkheid om een kans bewust lager in te vullen dan wat deze is, om het werk van maatregelen of het goedkeuringsproces voor acceptatie te ontlopen. Dit is uiteraard onwenselijk.

Sommige dreigingen hebben handelingen van een actor nodig om tot een incident te leiden. Hoe bedreigender een actor, des te groter de kans op een incident vanuit die actor. Dit kan gebruikt worden bij de inschatting van de kans.

Bepaal voor het inschatten van de kans, als eerst welke actoren achter een dreiging kunnen zitten. Ga vervolgens uit van de meest bedreigende actor, op basis van kennis, middelen en motivatie. Hanteer als initiële waarde voor de kans, de waarde van de dreiging die uitgaat van die actor. Heeft de organisatie enige maatregelen genomen tegen die dreiging, ga dan een stap in waarde omlaag. Heeft de organisatie goede, gerichte maatregelen genomen, ga dan twee stappen in de kans omlaag.

Bekijk de dreigingswaarden die vermeld staan in hoofdstuk 4 en de kans-as van de matrix in hoofdstuk 6. Stel, je hebt te maken met een dreiging vanuit een bedreigende actor (dreigingswaarde = 4). Daarbij hoort dus initieel een grote kans (kanswaarde = 4). Heb je geen maatregelen genomen tegen deze dreiging vanuit deze actor, dan behoud je de kans op deze waarde. Heb je enkele maatregelen genomen, dan mag je voor de kans een stap lager (naar ‘gemiddeld’ in dit geval). Heb je gerichte maatregelen genomen tegen deze dreiging vanuit deze actor en zijn die maatregelen bewezen effectief, dan mag je twee stappen lager (naar ‘klein’).

Deze aanpak zorgt voor een meer consistente en minder subjectieve benadering van het begrip kans. Het voorkomt ook dat de kans op een incident vanuit een bedreigende actor als laag wordt ingeschat, omdat het bijvoorbeeld nog niet eerder is voorgekomen.

Kwaadwillende actoren zijn niet altijd externen. Ook eigen medewerkers kunnen, bijvoorbeeld na een arbeidsconflict, acties uithalen die leiden tot schade voor de organisatie. Actoren zijn daarnaast niet altijd kwaadwillend. Ook medewerkers of externen kunnen onbedoeld voor een inbreuk op de beveiliging zorgen. Onwetendheid, stress of even niet goed opletten zijn daarbij medebepalend.

Naast actoren als achterliggende reden, gebeuren incidenten ook wel eens ‘spontaan’. Hardware gaat wel eens stuk en natuurrampen gebeuren onverwachts. In zo’n geval kan naar de incidentgeschiedenis of zaken vanuit de fysieke beveiliging gekeken worden voor het bepalen van de kans.

9 Impact

Een incident kan op verschillende manieren schade veroorzaken. Aan de gehele organisatie, aan een afzonderlijke afdeling, maar ook aan derden. Neem uit appendix B van de implementatierichtlijn de impactcategorieën over die relevant zijn voor de organisatie, een afdeling of relevante derden en vul deze aan met eigen relevante impactcategorieën.

Hanteer per impact-categorie een aantal niveaus van schade dat overeenkomst met de grootte van de risicomatrix. Indien gekozen is voor een 5×5 matrix, hanteer dan ook vijf impact-niveaus per categorie.

Geef per niveau een heldere omschrijving van de impact op dat niveau. De uitdaging is om via deze omschrijvingen voldoende houvast te bieden voor het vaststellen van het juiste impactniveau tijdens de uitvoering van een risicoanalyse. Het kiezen van de impact moet namelijk niet iets zijn dat op onderbuikgevoel gaat of dat bewust lager gedaan wordt dan het feitelijk is om het werk van maatregelen of het proces van acceptatie te ontlopen. Het resultaat van omschrijvingen per niveaus van een impactcategorie heet een referentietabel.

In appendix A is een voorbeeld-referentietabel opgenomen.

Bij het opstellen van de referentietabel zal je waarschijnlijk ontdekken dat de ene categorie zich qua ernst lastig een-op-een laat vergelijken met een andere categorie. Zo is een grote impact op reputatie van een andere orde dan een grote impact op personele veiligheid of milieu. Het enige juiste antwoord op de vraag hoe hiermee om te gaan, bestaat niet. Het belangrijkste hierbij is te beseffen en intern te bespreken waar de referentietabel toe dient. Dat is het vaststellen van de impact om, gecombineerd met de kans, de hoogte van het risico te kunnen bepalen. Het uiteindelijke doel is om, op basis daarvan, de mitigerende maatregelen te kunnen prioriteren.

10 Scenario's

Een optionele stap in de risicoanalyse is het combineren van meerdere kleine incidenten tot een groot incident, een scenario. De grote incidenten bestaan namelijk vaak uit een serie van meerdere dingen die misgingen en kwetsbaarheden die zijn misbruikt. Dit zijn vaak de kleine-kans/grote-impact incidenten die het nieuws halen en een organisatie in grote problemen brengen.

Bij grootschalige digitale aanvallen is de aanvaller vaak een tijd bezig met de voorbereiding op een aanval en ook de aanval zelf. De aanvaller gaat daarbij vaak niet direct voor het einddoel, maar dringt eerst via een onbelangrijk en dus minder goed beveiligd systeem binnen en zet de aanval van daaruit verder voort. Als zo'n eerste stap al in een risicoanalyse is behandeld, dan is deze mogelijk als laag ingeschat, omdat de directe impact van alleen die stap klein is. Het maken van scenario's kan helpen om het grotere plaatje te zien en om risico's die onterecht als klein zijn ingeschat beter te kunnen beoordelen.

11 Risicoregister

Voor het registeren van risico's zijn tal van oplossingen beschikbaar. Zelfgemaakte Excelsheets, kleine open-source programma's en zelfs grote commerciële GRC oplossingen. Kies uiteraard een oplossing die aansluit bij de behoeften vanuit de organisatie. Hieronder staan enkele overwegingen voor bij het selecteren van de juiste oplossing.

- Het risicoregister kan de risico's vastleggen op een manier die aansluit bij de werkwijze van de organisatie. Denk daarbij aan de attributen die je per risico wil kunnen vastleggen, maar vooral ook aan het bowtie-diagram.
- In een goed risicoregister zijn niet alleen risico's te registreren, maar ook de bijbehorende maatregelen. Indien voor de bow-tie-aanpak is gekozen, dan maakt het register onderscheid tussen preventieve, detectieve en repressieve maatregelen.
- Het register kan automatisch notificaties versturen bij bijvoorbeeld het toekennen van een risico aan een eigenaar, het verlopen van de geldigheidsduur van een risico of het verlopen van de implementatie-deadline van een maatregel.
- Het accepteren van een risico boven de acceptatiegrens is een bijzondere maar belangrijke behandeling van een risico. Een goed register biedt daar ondersteuning voor.
- Staar je niet blind op de mogelijkheden van een register voor het maken van grafieken en rapportages. Goed risicomanagement gaat om het bespreekbaar maken van risico's op het juiste niveau en om het toetsen van de werking van het management-proces. Grafieken kunnen daarbij handig zijn, maar zijn niet het hoofddoel en ook zeker niet per se noodzakelijk daarvoor. En rapportages over de werking van het managementproces is niet iets dat een risicoregister kan genereren. Dat is toch echt handwerk.

Indien de organisatie overgaat tot het in gebruik nemen van een risicoregister, is het verstandig om deze te vullen met de actuele stand van zaken rondom risico's en maatregelen. Stel vast welke beveiligingsmaatregelen momenteel geïmplementeerd zijn en bedenk welke risico's deze maatregelen mitigeren. Leg deze vast in het risicoregister.

12 Maatregelen

Er bestaat een grote diversiteit aan maatregelen die door een organisatie ingezet kunnen worden om de risicoblootstelling tot op een acceptabel niveau te beperken. Zo bestaan er maatregelen die erop gericht zijn om incidenten te voorkomen of om de kans daarop te beperken. Maatregelen ter vaststelling of identificatie van incidenten en maatregelen ter beperking van de gevolgen van incidenten. Deze maatregelen kunnen organisatorisch, technisch of mensgericht van aard zijn.

Idealiter passen organisaties een mix van verschillende soorten maatregelen toe. Zij wegen daarbij de kosten en baten van de maatregelen zorgvuldig tegen elkaar af. Het is belangrijk om ervoor te zorgen dat de maatregelen aansluiten op de tijdens de risicoanalyse vastgestelde oorzaken en gevolgen van incidenten.

Er bestaan verschillende bronnen waarin overzichten zijn opgenomen van algemeen toegepaste maatregelen. Organisaties kunnen deze bronnen raadplegen om inspiratie op te doen voor het selecteren van de noodzakelijk gewenste maatregelen. Hieronder een selectie van enkele veel gebruikte bronnen.

- BIO – https://www.bio-overheid.nl/
- NEN-ISO/IEC 27002 – https://www.nen.nl/
- NIST SP 800-53 rev.5 – https://csrc.nist.gov/
- Critical Security Controls – https://www.cisecurity.org/

13 Monitoring

Na de identificatie en analyse van risico's worden maatregelen getroffen om manifestatie van die risico's, ofwel incidenten, te voorkomen, vroegtijdig te ontdekken en om de gevolgen van incidenten tot op een acceptabel niveau terug te beperken. Of de kans op incidenten daadwerkelijk wordt verlaagd en of incidenten daadwerkelijk worden opgemerkt en de gevolgen daarvan worden beperkt, hangt af van de effectiviteit van de getroffen maatregelen.

Met de effectiviteit van de maatregelen wordt bedoeld dat deze het beoogde effect hebben en dat de maatregelen worden uitgevoerd zoals bedoeld. De effectiviteit van de maatregelen wordt op een gestructureerde manier getoetst. De planning beschrijft wanneer de effectiviteit van de maatregelen wordt getoetst en wanneer dat gereed moet zijn. In deze aanpak wordt beschreven wie de effectiviteit van de maatregelen toetst en op welke manier. Ook wordt vooraf vastgesteld aan wie de resultaten van die toetsing worden gerapporteerd en door wie deze worden besproken en met welk doel.

Hoe de toetsing moet worden uitgevoerd en of bijvoorbeeld ook onderliggend bewijs moet worden verzameld, wordt vastgelegd in een toets-instructie. Dat kan een generieke instructie zijn, maar ook een gespecificeerde instructie per maatregel.
De risico-eigenaar en de maatregeleigenaar bepalen samen de diepgang van de toetsing.

De feitelijke toetsing wordt afgerond met een oordeel over de effectiviteit van de maatregel. Bijvoorbeeld 'de maatregel wordt uitgevoerd conform instructie en ressorteert het gewenste effect', of 'de maatregel wordt niet uitgevoerd zoals bedoeld'. In dat laatste geval is het belangrijk om te achterhalen wat de oorzaak is van het niet, of niet correct uitvoeren van de maatregel. Dat kunnen organisatorische, technische of mens-gerelateerde oorzaken zijn, of een combinatie daarvan.

De resultaten van de uitgevoerde toetsingen worden op een door de risico-eigenaar en maatregeleigenaar overeengekomen manier gerapporteerd. De rapportages worden besproken door bestuurders en betrokken experts en ondersteuners. Dit wordt de risicodialoog genoemd. Op basis van deze dialoog besluiten bestuurders welke interventies door of namens hen uitgevoerd moeten worden. En vervolgens zien zij toe op de correcte uitvoering van deze interventies.

14 Operationele Technologie

Naast informatie, applicaties en IT-systemen zijn systemen binnen de operationele technologie (OT) ook een belangrijk onderwerp binnen de digitale weerbaarheid. Het beheersen van risico's voor OT-systemen kent grote vergelijkingen met het beheersen van risico's voor informatie, applicaties en IT-systemen als het gaat om de organisatorische zaken. Er zijn ook verschillen tussen deze twee domeinen en die worden vooral duidelijk tijdens het inventariseren en beoordelen van concrete risico's. Zo wordt bij informatie gekeken naar de beschikbaarheid, de integriteit en de vertrouwelijkheid. Bij OT gaat het onder anderen om safety (veiligheid van mensen), beschikbaarheid (doorgaan van processen) en onderhoudbaarheid.
Waar IT-systemen doorgaans enkele jaren meegaan, worden OT-systemen doorgaans voor gebruik van enkele tientallen jaren aangeschaft.

Ondanks dat het beheersen van risico's voor OT-systemen onderdeel is van digitale weerbaarheid, is dit onderwerp niet in de beleidsrichtlijn en de implementatierichtlijn opgenomen. De verschillen zouden de leesbaarheid ervan niet ten goede komen. Daarnaast bestaat er al een goede handreiking die zich volledig op dat onderwerp richt. Voor het beheersen van risico's binnen het OT-domein is er namelijk de "Handreiking risicobeheer in OT" vanuit het Ministerie van Infrastructuur en Waterstaat.
Deze is te vinden op de website Versterken cyberweerbaarheid[1].

1 https://www.versterkenweerbaarheid.nl/thema/ketens-en-risicomanagement/risicobeheer-in-ot.

Appendix A: Voorbeeld referentietabel

Onderstaande tabel is puur illustratief. Neem de inhoud dus niet over, maar vul deze zelf in met voor de organisatie zinvolle waarden.

	Organisatiedoel	Financieel	Imago / reputatie	Juridisch
Desastreus	De realisatie van het organisatiedoel is blijvend verstoord. Het voortbestaan van de organisatie wordt bedreigd.	Financiële consequenties vallen buiten de begroting van de aangesloten partijen.	Het incident bereikt het nieuws wereldwijd.	Punitief - strafrechtelijke vervolging van de organisatie en/of bestuurders door het Openbaar Ministerie
Groot	De realisatie van het organisatiedoel is ernstig verstoord. Het vertrouwen in de organisatie is beschadigd.	Financiële consequenties vallen buiten de begroting van de organisatie.	Het incident bereikt de landelijke pers.	Repressief - het opleggen van een bestuurlijke sanctie door een toezichthouder (last onder dwangsom, bestuursdwang en bestuurlijke boete)
Gemiddeld	De realisatie van het organisatiedoel is tijdelijk verstoord. Er worden vragen gesteld over de betrouwbaarheid van de organisatie.	Financiële consequenties vallen buiten de post onvoorzien, maar binnen de begroting van de organisatie.	Het incident bereikt het regionale nieuws.	Correctief - een (mogelijke publieke) waarschuwing door een toezichthouder en/ of een bindende aanwijzing van een toezichthouder om aanbevelingen of verbetertraject uit te voeren
Klein	De realisatie van het organisatiedoel is lichtelijk verstoord, zonder serieuze gevolgen.	Financiële consequenties vallen binnen de post onvoorzien van begroting van de organisatie.	Het incident bereikt het lokale nieuws.	Coöperatief - aanbevelingen door een toezichthouder en/ of het maken van afspraken met een toezichthouder over verbetertrajecte
Minimaal	De realisatie van het organisatiedoel is zeer tijdelijk en/of gedeeltelijk, lichtelijk verstoord, zonder gevolgen.	Geringe financiële consequenties.	Het incident krijgt niet of nauwelijks media-aandacht.	Informatief - gesprek met en/of voorlichting door een toezichthouder

	Maatschappelijk	Milieu	Politiek	Veiligheid mensen
Desastreus	Meerdere steden of meer dan een miljoen mensen worden geraakt.	Grote en blijvende schade aan het milieu.	Het kabinet / de verantwoordelijke bewindspersoon treedt af.	Ongeval met een of meerdere doden.
Groot	Meerdere honderdduizenden mensen worden geraakt.	Grote schade aan het milieu met een hersteltijd van meerdere jaren.	Een incident leidt tot een plenair debat of een onderzoek vanuit de Algemene Rekenkamer.	Ongeval met een of meerdere personen met blijvend zwaar letsel.
Gemiddeld	Vele tienduizenden mensen worden geraakt.	Schade aan het milieu met een hersteltijd van meerdere maanden tot maximaal 2 jaar.	Een incident leidt tot meerdere Kamerbrieven en schriftelijke vragen en Kamerdebatten.	Ongeval met een of meerdere personen met herstelbaar zwaar letsel.
Klein	Vele duizenden mensen worden geraakt.	Beperkte schade aan het milieu met een hersteltijd van enkele weken.	Een incident leidt tot schriftelijke vragen in de Tweede Kamer.	Ongeval met een of meerdere personen met licht letsel.
Minimaal	Minder dan duizend mensen worden geraakt.	Minimale schade aan het milieu. Geen noemenswaardige hertsteltijd.	Aandacht is beperkt tot mondelinge vragen tijdens vragenuurtje in Tweede Kamer.	Ongeval met een of meerdere personen met verwaarloosbaar letsel.

Deze brochure is een uitgave van:
CIO Rijk, afdeling IB&P

Turfmarkt 147, 2511 DP Den Haag
cisorijk@minbzk.nl

September 2025