Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe bepaal ik de meest relevante risico's voor mijn organisatie?

Next steps voor het beoordelen van risico's

Factsheet FS 2024 | Versie 1.0 | Oktober 2024

Het beheersen van digitale risico's blijkt in de praktijk een uitdagende opgave. Het dreigingslandschap verandert snel en nieuwe aanvalstechnieken wisselen elkaar in hoog tempo af. De risico's die hieruit voortkomen kunnen ernstige gevolgen voor het functioneren van organisaties hebben. Organisaties moeten daarom zicht en grip op deze risico's krijgen. Maar hoe breng je deze risico's in kaart en hoe beoordeel je met welke risico's je als eerst aan de slag moet? Deze publicatie biedt praktische handvatten die je kunt gebruiken om de meest relevante risico's voor jouw organisatie te bepalen.

Deze publicatie is onderdeel van de kennisproducten reeks '*NIS2: Bereid je voor op de Cyberbeveiligingswet*'.[1]

Het handelingsperpectief in dit kennisproduct vormt een verdieping op de eerdere publicaties in deze reeks die ingaan op het identificeren van risico's.

De handvatten in dit document zijn geschreven om je te helpen bij de volgende stap: het beoordelen van de meest relevante risico's voor jouw organisatie.[2]

Lees hieronder verder en zet de volgende stap in een risicobeheersingsproces.

Let op! Voor deze publicatie geldt dat risico's niet alleen betrekking kunnen hebben op netwerk- en informatiesystemen, maar ook op de medewerkers die met deze systemen werken.

Doelgroep

Deze publicatie richt zich op organisaties die onder de NIS2-richtlijn komen te vallen en is geschreven voor personen die een rol hebben bij het beheersen van risico's en op zoek zijn naar handvatten voor het in kaart brengen van de meest relevante risico's voor hun organisatie

Deze publicatie is tot stand gekomen met bijdrage van

Het Ministerie van Volksgezondheid, Welzijn en Sport en de Belastingdienst

NIS2

De zorgplicht van de NIS2-richtlijn verplicht essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen te nemen, afgestemd op de risico's die zich voordoen.[3]

[1] NIS2: Bereid je voor op de Cyberbeveiligingswet | Over het NCSC | Nationaal Cyber Security Centrum

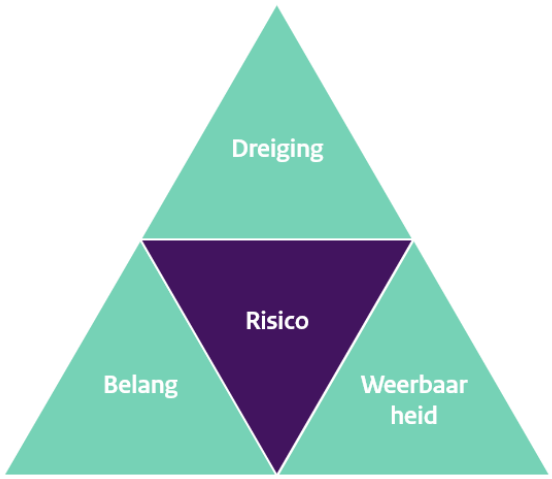
[2] Routekaart risicomanagement | Wat kun je zelf doen? | NCSC

[3] NIS2 Verplichtingen: NCSC Zorgplicht Infosheet

Voordat je aan de slag gaat: Wat heb je nodig?

Een goed begin is het halve werk. Overweeg voordat je aan de slag gaat de volgende stappen:

1. Ga na of er binnen jouw organisatie al een overzicht van geïdentificeerde risico's aanwezig is.
2. Breng risico's in kaart wanneer er geen overzicht aanwezig is. Om risico's te kunnen beoordelen, moet je eerst risico's in kaart hebben gebracht.[4] Kort samengevat kun je dit doen door:
   a) De Te Beschermen Belangen (TBB's) in kaart te brengen. Dit zijn belangen die essentieel zijn voor het functioneren en zelfs het voortbestaan van jouw organisatie. Stem de uitkomsten van de analyse af met het bestuur.
   b) De dreigingen in kaart te brengen die deze TBB's kunnen raken.
   c) De huidige beveiligingsmaatregelen in kaart te brengen en deze af te zetten tegen het gewenste en/of vereiste weerbaarheidsniveau voor jouw organisatie. Deze onderdelen bepalen samen het risico.
3. Verwerk de resultaten van de onderdelen 'dreiging', 'te beschermen belangen' en 'weerbaarheid 'op een gestructureerde manier. Om resultaten te verwerken, documenteren en periodiek bij te houden, moet er binnen jouw organisatie een risicomanagementproces aanwezig zijn.[5]
4. Wijs een risico-eigenaar aan. Onderzoek of de geïdentificeerde risico's een risico-eigenaar toegewezen hebben gekregen en welke mandaatafspraken er in overleg met het bestuur zijn gemaakt.



Een visueel overzicht voor het identificeren van risico's

Tot slot: Wat is een risico?

Een risico wordt omschreven als de kans op schade of verlies gecombineerd met de impact die deze schade op de organisatie heeft.[6] Denk hierbij aan de verstoring van kritieke bedrijfsprocessen, het verlies van gevoelige data of reputatieschade.

Met de 'meest relevante' risico's bedoelen we in dit kennisproduct de risico's die een hoge impact op de organisatie zouden hebben wanneer de kans van een potentiële dreiging tot een daadwerkelijk incident leidt. Maar hoe pak je dit aan? Hoe bepaal je wat voor jouw organisatie de meest relevante risico's zijn?

Je kunt dit inzichtelijk maken met behulp van een risicomatrix. Een risicomatrix is een hulpmiddel dat structuur en houvast biedt om binnen jouw organisatie het gesprek over de meest relevante risico's aan te gaan.

Hieronder lichten we de stappen voor het invullen van een risicomatrix verder toe.

[4] Wanneer jouw organisatie aan het begin staat om risico's in kaart te brengen, adviseren we je om voor meer informatie de publicaties 'Hoe breng ik mijn dreigingen in kaart', 'Hoe breng ik mijn te beschermen belangen in kaart en 'Hoe krijg ik grip op mijn security controls' te lezen: Hoe breng ik mijn dreigingen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum (ncsc.nl), Hoe breng ik mijn te beschermen belangen in kaart? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum (ncsc.nl) en Hoe krijg ik grip op mijn security controls? | Wat kun je zelf doen? | Nationaal Cyber Security Centrum (ncsc.nl)

[5] Er bestaan verschillende methoden om een risicomanagementproces in te richten. Belangrijk is dat deze methode aansluit bij de werkwijze van jouw organisatie en rekening houdt met de bestaande wet- en regelgeving die op jouw organisatie van toepassing is

[6] Woordenboek - Cyberveilig Nederland

We maken per stap ook gebruik van een fictief voorbeeld om een vertaalslag naar praktische handvatten te maken.[7]

Stap 1: Het identificeren van relevante risico's

Bij het beoordelen van de meest relevante risico's komen een aantal onderdelen samen. Zo speelt niet alleen de dreiging een rol, maar ook de kans dat deze dreiging tot een daadwerkelijk incident leidt.

Maar hoe erg is het als een dergelijk incident plaatsvindt? Heeft jouw organisatie zicht op welke belangen geraakt zouden worden? En loopt daarmee de continuïteit van kritieke diensten en producten gevaar? Of zijn er beveiligingsmaatregelen getroffen die de kans op een dergelijk incident kunnen verlagen en eventuele schade kunnen beperken?

De mate van de impact van een bepaald risico op de belangrijkste TBB's van de organisatie vormt dus ook een belangrijk houvast om te bepalen wat voor jouw organisatie de meest relevante risico's zijn.

Een risicomatrix wordt doorgaans dan ook opgebouwd uit de assen 'kans' en 'impact'. Ons advies is om stapsgewijs aan de slag te gaan bij het invullen van een risicomatrix. Zo behoud je het overzicht en kom je tot een bruikbaar resultaat.

Het identificeren van relevante risico's vormt hierbij de eerste stap. Om te bepalen wat in het geval van jouw organisatie relevante risico's zijn, is het belangrijk dat het bestuur heeft ingestemd met de resultaten van een risicoanalyse en hierbij heeft aangegeven wat voor de organisatie de belangrijkste te beschermen belangen te zijn.

Misschien staat jouw organisatie aan het begin om risico's in kaart te brengen.[8] Bespreek in dit geval de resultaten van een analyse met je bestuur, onderzoek wat de bijbehorende risicobereidheid is en leg dit vast. Wijs ook per risico een risico-eigenaar aan en beschrijf welk mandaat deze heeft. Zo kun je identificeren en afstemmen wat relevante risico's voor jouw organisatie zijn.

Het kan ook zijn dat het bestaande overzicht als gevolg van een veranderend dreigingslandschap of een nieuw TBB opnieuw onderzocht moet worden. In dit geval beschikt jouw organisatie al over een bestaand overzicht dat als basis gebruikt kan worden. Ga hierbij ook na of ieder risico een risico-eigenaar heeft, welk mandaat deze heeft en welke afspraken er in overleg met het bestuur over risicobereidheid zijn gemaakt. Onderzoek of het bestaande overzicht aangepast moet worden en opnieuw afgestemd moet worden.

Een fictief voorbeeld

Een organisatie staat aan het begin om risico's in kaart te brengen. De organisatie heeft eerst onderzoek naar de belangrijkste TBB's gedaan en is hierbij op het volgende overzicht uitgekomen:

- Het intellectueel eigendom met betrekking tot het vervaardigen van product X.
- De operationele techniek (OT) die wordt ingezet om product X te kunnen maken.
- Onderzoek & Ontwikkeling (O&O) voor het innoveren van product X, maar ook het ontwikkelen van nieuwe producten.
- De opslag van product X in verschillende opslaglocaties.
- De systemen die bedrijfsprocessen ondersteunen zoals voorraadbeheer, betalingen en retourzendingen.

Vervolgens heeft de organisatie voorstelbare dreigingen in kaart gebracht die deze belangen kunnen raken:

- Het versturen van (gerichte) spearphishing e-mails door cybercriminelen.
- Insider threat. Activiteiten uitgevoerd door een kwaadwillende via een leverancier of een eigen medewerker.

[7] Het fictieve voorbeeld is een versimpelde weergave van de werkelijkheid. De handvatten in dit kennisproducten zijn bedoeld om een vertaalslag naar jouw eigen organisatie te kunnen maken

[8] Zie pagina 3 'voordat je aan de slag gaat: wat heb je nodig?' punt 2 voor meer informatie

- Het uitvoeren van een kwaadaardige update die a) bewust is aangebracht b) onbewust een fout bevat.
- Misbruik van 'vergeten systemen' die verouderd zijn.
- Misbruik van edge devices zoals firewalls, routers en VPN-servers.
- Kwetsbaarheden in de supply-chain.

Tot slot is er ook inzichtelijk gemaakt welke huidige beveiligingsmaatregelen er zijn getroffen. De organisatie heeft hierbij specifiek gekeken naar de te beschermen belangen en dreigingen die eerder in kaart zijn gebracht. Op basis van deze onderdelen heeft de organisatie bepaald welke kwetsbaarheden er momenteel bestaan:

Beveiligingsmaatregelen

- Er wordt gebruik gemaakt van multifactorauthenticatie.
- Er worden jaarlijkse phishing- en awareness trainingen aangeboden.
- Er wordt jaarlijks een pentest uitgevoerd.
- Er is passieve monitoring aanwezig.

Kwetsbaarheden

- De organisatie beschikt nog niet over Business Continuity Management (BCM) of Incident Response (IR) plannen.
- Een grote groep medewerkers heeft momenteel toegang tot het intellectueel eigendom in verband met de O&O activiteiten.
- De organisatie werkt primair in de Cloud, maar beschikt ook nog over on-premises koppelingen. Deze koppelingen worden niet actief gemonitord.

Voorbeeld: De resultaten van stap 1

De organisatie is op basis van een risicoanalyse tot de volgende risico's gekomen:

- Het intellectueel eigendom is beperkt afgeschermd.
- Er vindt geen actieve monitoring op kritieke systemen plaats.
- Er wordt niet structureel getest om mogelijke kwetsbaarheden te onderkennen.
- IRP en BCM plannen zijn nog niet ontwikkeld.

De bovenstaande risico's worden voorgelegd aan het bestuur. Het bestuur merkt hierbij de continuïteit van het operationele proces en het intellectueel eigendom als meest kritiek aan.

Er worden tot slot risico-eigenaren aan deze risico's toegewezen.

Stap 2: Het beoordelen van relevante risico's

In de vorige stap heb je relevante risico's in kaart gebracht. De volgende stap is om deze risico's te beoordelen. Om dit te kunnen doen, zul je de impact van deze risico's concreter inzichtelijk moeten maken.

Denk hierbij bijvoorbeeld aan:

- In welke mate heeft een succesvolle digitale aanval impact op de operationele bedrijfsactiviteiten? Zijn er uitwijkmogelijkheden om door te werken of komen kritieke processen stil te liggen?
- Is het financiële verlies van kritieke risico's inzichtelijk gemaakt? Is dit uitgedrukt in cijfers?
- In hoeverre schaadt een succesvolle aanval de reputatie van de organisatie en het vertrouwen van klanten?
- Wat zijn de juridische gevolgen van een succesvolle aanval?

Om deze vragen te kunnen beantwoorden zullen de personen die een rol hebben bij het in kaart brengen van relevante risico's in gesprek moeten gaan met de risico-eigenaren. De risico-eigenaar is verantwoordelijk voor het bewaken en het beheersen van het risico en weet in het geval van ontbrekende informatie waar deze opgevraagd kan worden.

Het plotten van de risico's

Een risicomatrix biedt een overzicht van verschillende risico's op basis van twee assen:

- **De kans**: Hoe waarschijnlijk is het dat een voorstelbare digitale dreiging zich voordoet? Dit wordt doorgaans beoordeeld van laag tot hoog.
- **De impact**: Als de dreiging leidt tot een daadwerkelijk incident, hoe ernstig zijn de gevolgen voor de organisatie? Dit wordt ook beoordeeld van laag tot hoog.

Een risico wordt ingedeeld op het raster waar deze twee assen elkaar kruisen. Bijvoorbeeld, een risico met een hoge waarschijnlijkheid en een hoge impact wordt in de rechterbovenhoek van de matrix ingedeeld.

Dit overzicht helpt organisaties om in één oogopslag te zien welke risico's als 'hoog' worden aangemerkt. Het doel hiervan is om een prioritering aan te brengen en te bepalen wat de 'meest relevante risico's' voor jouw organisatie zijn.

Het opstellen van een risicomatrix: een fictief voorbeeld

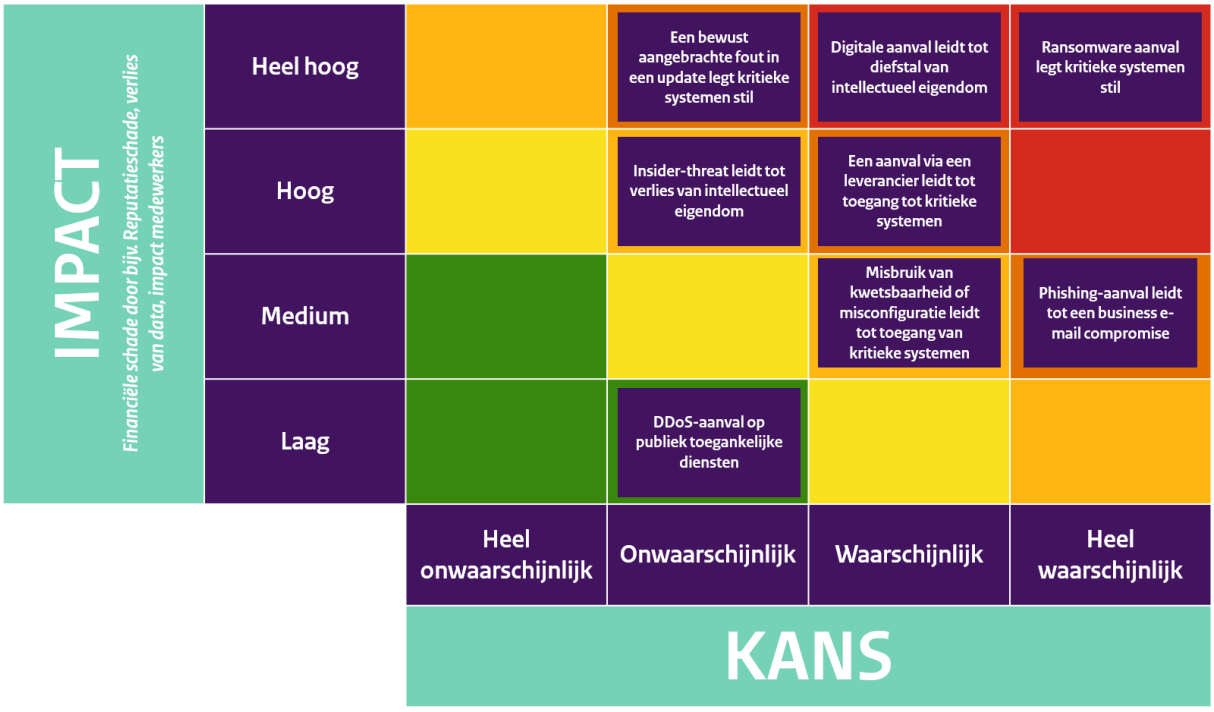
De security professional die in de eerste stap de relevante risico's in kaart heeft gebracht, gaat vervolgens in gesprek met de risico-eigenaren van de bijbehorende risico's.

Er ontbreekt momenteel nog belangrijke informatie om een gerichte inschatting te kunnen maken van zowel de kans als de impact van het betreffende risico.

Zo is het bijvoorbeeld nog onduidelijk hoeveel een succesvolle ransomware aanval de organisatie financieel zou kunnen kosten, maar is het daarnaast onduidelijk in hoeverre de schade beperkt kan worden door de huidige beveiligingsmaatregelen en hoe dit zich verhoudt tot het financieel verlies. Ook kunnen de huidige beveiligingsmaatregelen de kans dat een dreiging tot een daadwerkelijk incident leidt beïnvloeden.

Door met de risico-eigenaar het gesprek aan gaan, kan er per risico gerichter in kaart worden gebracht wat de kans en impact is.

Op basis van deze gesprekken is de onderstaande risicomatrix tot stand gekomen:



Stap 3: Bespreek de risicomatrix en leg de uitkomsten vast

Als laatste stap adviseren we om de resultaten van de risicomatrix aan de bijbehorende risico-eigenaren voor te leggen.

Er zijn meerdere redenen waarom dit een belangrijke laatste stap vormt.

Deze worden hieronder verder toegelicht:

Afstemmen

De mate van risicobereidheid kan per organisatie verschillen. Wat een onacceptabel risico is voor de ene organisatie, past voor de andere organisatie binnen de doelstellingen. Stem per risico af wat de risicobereidheid is en leg de uitkomsten hiervan vast. Als de gevolgen van een bepaalde risicobereidheid boven het mandaat van de risico-eigenaar gaan, dan moet er verder afgestemd worden met de juiste risico-eigenaar. Zie hiervoor ook ‘eigenaarschap’.

Prioriteren

Bespreek met welke risico’s jouw organisatie als eerst aan de slag gaat. Prioriteer de meest relevante risico’s om als eerst mee aan de slag te gaan op basis van de resultaten van de risicomatrix. Leg dit besluit ook vast.

Eigenaarschap

Een risico-eigenaar moet over voldoende middelen beschikken om het risico te kunnen beheersen. Denk hierbij bijvoorbeeld aan beslissingsbevoegdheid, maar ook financiële middelen voor het treffen van aanvullende beveiligingsmaatregelen. Als dit onvoldoende blijkt in relatie tot de mogelijke impact van een risico op de organisatie, dan moet dit aan het bestuur voorgelegd worden.

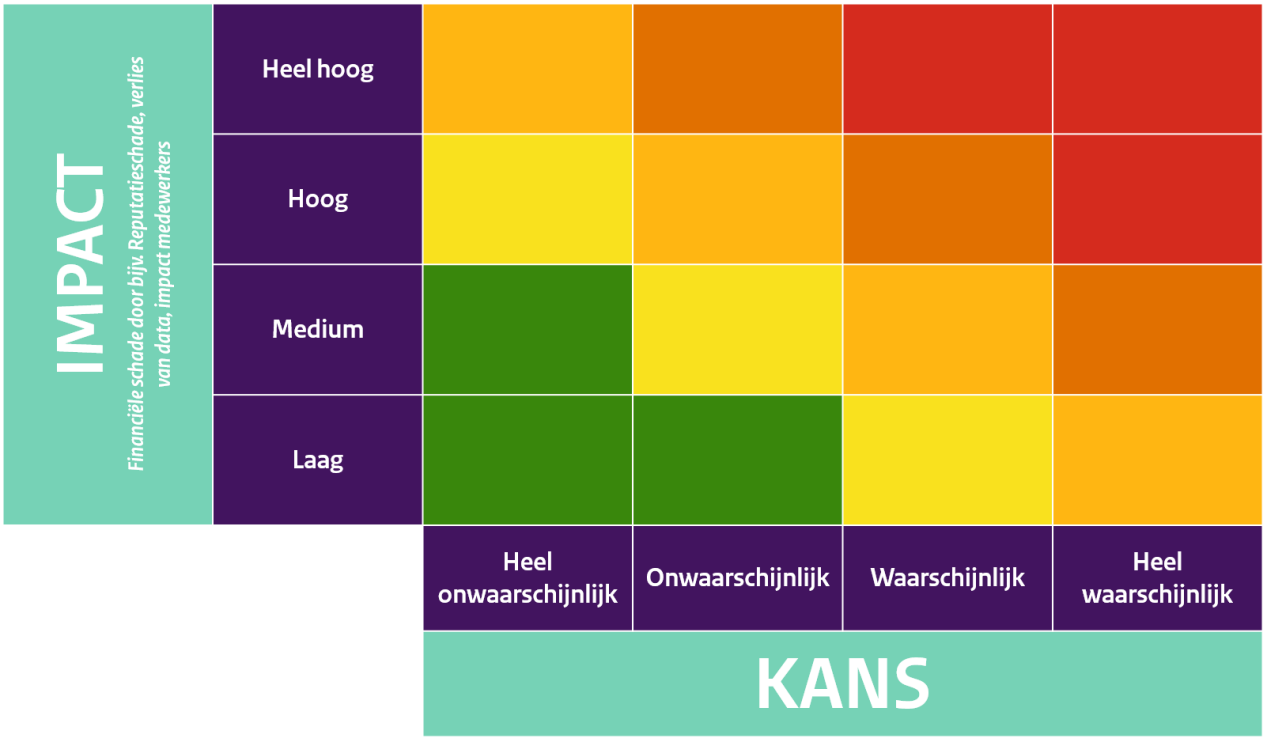
Kennis

Beschikt de risico-eigenaar over de juiste kennis met betrekking tot beveiligingsmaatregelen? Of moet er bijvoorbeeld bij een externe leverancier of interne specialist aanvullende informatie opgehaald worden om een vollediger beeld te vormen? Dit geldt ook voor het inzichtelijk maken van de impact van een risico op de organisatie.

Tot slot

Het beoordelen van risico’s is doorgaans geen eenmalige actie, maar moet periodiek uitgevoerd worden om de risicomatrix actueel te houden.

Bijlage Risicomatrix Template



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

Oktober 2024