Risico’s beheersen: de waarde van informatie als uitgangspunt.

Over eigenaarschap en verantwoordelijkheden.

Factsheet FS-2020-04 | versie 1.2 | februari 2022

Incidenten met belangrijke en/of gevoelige informatie kunnen een serieuze impact hebben op de organisatiedoelen. De directie is om die reden eindverantwoordelijke voor een goede omgang met de risico's rondom informatie.

Lijnmanagers zijn verantwoordelijk voor de tactische en operationele risico's rondom de informatie die binnen hun afdeling verwerkt wordt. Om risico's te kunnen beheersen, is het noodzakelijk dat ze op een zorgvuldige manier inzichtelijk worden gemaakt en beoordeeld.

Zicht en grip op de risico's rondom informatie vereisen zicht en grip op de informatie zelf. Zorg daarom dat ook het eigenaarschap van de informatie zelf en de bijbehorende verantwoordelijkheden goed zijn ingericht.

Achtergrond

In deze informatiegestuurde samenleving verwerken we een hoop informatie. Hoewel we in veel gevallen afhankelijk zijn van deze informatie, kan het voor uw organisatie of voor anderen ook de nodige risico's opleveren.

Sommige risico's bieden kansen, andere risico's kunnen leiden tot vervelende incidenten. Dit laatste soort risico's moet beheerst worden. Hoe belangrijker of gevoeliger de informatie of hoe groter de gevolgen van een incident, des te groter de noodzaak om dit soort risico's rond informatie te beheersen.

Doelgroep

Deze factsheet richt zich op de directie, het bestuur, het management en de CISO van organisaties die zicht en grip willen krijgen op de risico's die horen bij het werken met informatie.

Aan deze factsheet hebben bijgedragen

Brabantse waterschappen, CISO Masterclass BV, Digital Trust Center (EZK), Hoogheemraadschap van Rijnland, NBV van de AIVD en Octopus-IB.

Wat is er aan de hand?

Organisaties zijn afhankelijk van informatie voor het uitvoeren van hun kernactiviteiten. Ze zijn zich alleen niet altijd voldoende bewust van wat die informatie waard is voor henzelf, maar ook zeker voor kwaadwillende. Gebrek aan dit inzicht zorgt ervoor dat organisaties te weinig aandacht hebben voor het kennen en beheersen van de risico's die ontstaan bij het werken met hun informatie.

Managers hebben een verantwoordelijkheid voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in hun processen. Ze zullen, hoe dan ook, de gevolgen ondervinden van incidenten met hun informatie. Echter, ze geven niet altijd de juiste invulling aan deze verantwoordelijkheid.

In deze factsheet wordt gesproken over 'directie'. Daarmee wordt het hoogste bestuursorgaan in een organisatie mee bedoeld. Dit kan voor uw organisatie anders heten. Voor het leesgemak wordt de term 'directie' aangehouden.

Hoe risicomanagement het beste ingericht kan worden, is voor iedere organisatie anders. Neem de boodschap mee over het inrichten van het eigenaarschap van informatie en de bijbehorende risico's en het vaststellen van de verantwoordelijkheden daarbij, maar vul de details vooral anders in daar waar wenselijk of noodzakelijk.

Wat is het probleem?

De afgelopen decennia is de hoeveelheid informatie die we verwerken enorm toegenomen. Door de mogelijkheden die ICT-middelen bieden, zijn we ook meer informatie aan elkaar gaan koppelen. Hierdoor is de informatieverwerking ook complexer geworden. Deze twee ontwikkelingen zorgen voor extra uitdagingen bij het beheer van informatie. Echter, onze aandacht voor het beheer van informatie is achtergebleven bij de groei in omvang, complexiteit en het belang van die informatie.

Het gebruik van ICT-middelen maakt het krijgen van zicht op informatie lastig. Van een hangmappenkast of archiefruimte is door iedereen te bepalen hoeveel informatie daarin opgeslagen ligt en wat waar ligt. Om datzelfde te kunnen bepalen van informatie in ICT-systemen is inzicht in de digitale verwerking van informatie binnen de infrastructuur nodig. Dit is veelal erg omvangrijk en technisch complex. Bevinden deze ICT-systemen zich (deels) in de cloud, dan wordt het achterhalen van wat waar ligt nog complexer.

Informatie en ICT zijn tegenwoordig onlosmakelijk verbonden. Vroeger waren de middelen om informatie vast te leggen (typemachine, drukker, papier, binding, et cetera) eenvoudiger en stelden we daar niet bijzonder veel eisen aan. Vandaag de dag is dat anders. ICT-middelen moeten sneller, gebruiksvriendelijker, mooier en draagbaarder zijn. Ze moeten ook meer functionaliteiten bevatten en zijn continue aanwezig. Onze aandacht gaat dus veel meer dan vroeger uit naar het middel. Informatie is hierdoor geen zelfstandig ding meer, maar is onderdeel geworden van het middel.

Het beperkte zicht op informatie en een grote aandacht voor het middel zien we ook terug in de informatiebeveiliging. We richten ons op technische beveiligingsmiddelen en de technische kant van digitale aanvallen, maar richten ons soms te weinig op de waarde en het belang van onze informatie.

Eerst zal worden ingegaan op het verkrijgen van zicht en grip op informatie, gevolgd door het verkrijgen van zicht en grip op de risico's rondom die informatie.

Hoe krijgt u zicht en grip op informatie?

Om zicht en grip te krijgen op de risico's rondom informatie, moet u eerst zicht en grip krijgen op de informatie zelf. Inzien dat informatie, net als bijvoorbeeld personeel, de voorraad en de financiën, een bedrijfsmiddel is dat actief beheer nodig heeft, helpt daarbij. Omdat informatie door de gehele organisatie wordt gebruikt, moet de gehele organisatie worden meegenomen in de aanpak. In de aanpak zijn de volgende stappen te onderkennen.

Rol van de directie

Voor een werkende en blijvende aanpak, is betrokkenheid van de directie randvoorwaardelijk. Een organisatie is net zo afhankelijk van informatie als van arbeid, kapitaal en natuur. De directie dient informatie als volwaardige productiefactor te besturen en dit uit te dragen naar de gehele organisatie.

Eigenaarschap van informatie

Om informatie goed te kunnen beheren, moet alle informatie een eigenaar hebben. Bij voorkeur is dat een expliciete eigenaar en niet een via het proceseigenaarschap afgeleide eigenaar. Informatie kan namelijk in meerdere processen gebruikt worden, gekopieerd worden, gekoppeld worden, et cetera. Dit kan onduidelijkheid gegeven over wie de daadwerkelijke eigenaar is. Zeker in het geval van een incident is het goed om daar direct duidelijkheid over te hebben.

Lijnmanagers zijn de aangewezen personen om informatieeigenaar te zijn. Zij geven dagelijkse leiding aan de organisatie, op de plekken waar het direct impact heeft als informatie niet betrouwbaar of beschikbaar is. Om goed beheer van informatie af te dwingen, rekent de directie informatie-eigenaren af op de invulling van hun verantwoordelijkheid.

Iemand eigenaar maken van informatie, betekent niet automatisch dat diegene de juiste kennis heeft om die verantwoordelijkheid te kunnen dragen. Eigenaren behoren daarom, waar nodig, de juiste ondersteuning te krijgen vanuit de afdeling informatiemanagement.

Informatiemanagement

Goed beheer van informatie is een vak apart. De organisatie moet daarom beschikken over de juiste kennis van informatiemanagement. Vanuit informatiemanagement[1] wordt toegezien en ondersteuning geboden op goed beheer van informatie. De afdeling informatiemanagement heeft dus geen directe zeggenschap over de informatie. Die verantwoordelijkheid ligt bij de informatie-eigenaren.

Voor een goede afstemming van hoe binnen de organisatie met informatie omgegaan moet worden en wat van informatie-eigenaren precies verwacht wordt, heeft informatiemanagement directe toegang tot de directie en is er een met de directie afgestemd informatiebeleid. Ondanks dat informatie veelal met ICT verwerkt wordt, is informatie geen onderdeel van ICT. Informatiemanagement binnen de ICT-afdeling plaatsen is daarom geen verstandige aanpak. Informatie is een zelfstandig bedrijfsmiddel en informatiemanagement verdient daarom als een zelfstandige afdeling een onafhankelijke plek binnen de organisatie.

> De CFO onder de ICT-manager?
>
> Informatiebeheer bij de ICT-afdeling onderbrengen met als argument dat informatie uitsluitend via de computer

[1] Afhankelijk van de grootte van de organisatie, wordt dit ingevuld door een persoon of door een afdeling. Voor het leesgemak spreken we in deze factsheet over een afdeling.

verwerkt wordt, is geen goede aanpak. Met datzelfde argument kunt u ook de afdeling financiën onder de ICT-afdeling plaatsen. Immers, geldzaken doen we tegenwoordig ook bijna volledig met behulp van de computer.

Zicht op de informatie

Goed zicht hebben op informatie is noodzakelijk om deze te kunnen beheren. Voor het maken van een overzicht van de relevante informatie binnen een organisatie, zijn de primaire en andere belangrijke bedrijfsprocessen een goed uitgangspunt. De afdeling informatiemanagement is de aangewezen partij om het verkrijgen van inzicht in het informatielandschap te coördineren.

Het inzichtelijk maken van informatie moet zich niet beperken tot informatie binnen de organisatie. Informatie waar de organisatie verantwoordelijk voor is, kan opgeslagen liggen bij externe partijen. Ook kan de organisatie in zekere mate afhankelijk zijn van informatie uit externe bronnen. Neem dit soort informatie mee in het overzicht.

De Algemene Verordening Gegevensbescherming eist in artikel 30 dat de verwerkingsverantwoordelijke een register van verwerkingsactiviteiten bijhoudt. In plaats van een register voor enkel en alleen de verwerking van persoonsgegevens, is het goed om te kijken naar een algemeen register voor alle relevante informatie en de bijbehorende verwerkingen, waarbij 'persoonsgegeven' slechts een eigenschap is van hetgeen daarin is vastgelegd.

Zorg ervoor dat na het verkrijgen van zicht op de informatie-huishouding, dit zicht ook behouden blijft. Maak het behouden van dit zicht onderdeel van change managementprocessen in de organisatie.

Risicobewust gedrag

Iedere medewerker moet zich bewust zijn van zijn of haar aandeel en medeverantwoordelijkheid in een zorgvuldige omgang met informatie. Dit geldt met name voor ICT-beheerders. Het werken met informatie gaat gepaard met duidelijke werkinstructies over wat wel en wat niet is toegestaan. Bij de verwerking van belangrijke of gevoelige informatie moet ook nagedacht worden over trainingen en of periodieke campagnes om risicobewust gedrag te bevorderen.

Hoe krijgt u zicht en grip op risico's?

Nadat zicht en grip op informatie is verkregen, kan gewerkt worden aan het krijgen van zicht en grip op de beveiliging daarvan. Ook daarin zijn meerdere stappen te onderkennen.

Rol van de directie

De directie is eindverantwoordelijke voor wat er in de organisatie gebeurt. In het geval van een serieus incident met informatie waarbij de gevolgen tot buiten de organisatie reiken, zal zij namelijk degene zijn die door toezichthouders, de media, betrokkenen en/of andere belanghebbenden wordt aangesproken.

Eigenaarschap van risico's

Omdat incidenten met belangrijke of gevoelige informatie de hele organisatie kunnen raken, is het zorgen voor een veilige en zorgvuldige omgang met informatie een directie-verantwoordelijkheid. De verantwoordelijkheid voor de uitvoering van de dagelijkse zorg hiervoor, kan de directie delegeren naar de informatie-eigenaren. Om een goed beheer van risico's zeker te stellen, laat de directie zich door de informatie-eigenaren informeren over de invulling van hun verantwoordelijkheid en stuurt zij bij wanneer dat nodig is.

Chief Information Security Officer

Het beheersen van risico's, en zeker rondom digitale informatie, is een vak apart. De informatie-eigenaren hebben daarom ondersteuning nodig van een expert, om op

een goede manier invulling te kunnen geven aan hun verantwoordelijkheden hierin. Een Chief Information Security Officer (CISO) kan daarbij helpen. Een CISO heeft de volgende drie hoofdtaken:

- Adviseren: Antwoord geven op vragen over informatiebeveiliging binnen de organisatie;
- Coördineren: Verantwoordelijkheid over specifieke acties op het gebied van informatiebeveiliging, zoals bijvoorbeeld het beheren van het ISMS, het begeleiden van risicoanalyses, penetratietesten of awareness-campanges en het bijhouden van een register voor beveiligingsincidenten;
- Controleren: Nagaan of de organisatie zich houdt aan haar eigen regels over informatiebeveiliging en de directie hierover informeren.

Hoewel in de praktijk de CISO regelmatig binnen de ICT-afdeling wordt gepositioneerd, is dit niet de ideale plaats, omdat dit dan leidt tot belangenverstrengeling met de ICT-manager. De CISO heeft, net als informatiemanagement, een zelfstandige en onafhankelijke positie binnen de organisatie nodig, die directe toegang biedt tot de directie en het lijnmanagement. De CISO moet vrij kunnen rapporteren, zonder dat degene die verantwoordelijk is voor hetgeen waarover gerapporteerd wordt, daar tussen zit.

Een ICT-afdeling die behoefte heeft aan een medewerker die zich specifiek op IT-beveiliging richt, kan gebruik maken van een IT security officer, die nauw samenwerkt met de CISO.

Risico's vinden en beheersen

Hoe je risicomanagement inricht en uitvoert, is aangegeven in de ISO 31000 norm en specifiek voor informatiebeveiliging, in de ISO 27005-norm[2]. In beide normen worden, naast een aantal algemene en randvoorwaardelijke zaken, de volgende stappen beschreven waarmee waarmee risico's geïdentificeerd, geanalyseerd, geëvalueerd en beheerst kunnen worden.

De Risicoklassenindeling voor Digitale Veiligheid is een risicoclassificatiemodel voor het mkb. Aan de hand van 11 vragen wordt een inschatting gemaakt hoe groot het risico op een cyberincident is. Deze inschatting bepaalt in welke risicoklasse (1 t/m 4) de onderneming valt en welke maatregelen er genomen kunnen worden om op een passend niveau van weerbaarheid te komen.

Risicoklassenindeling voor Digitale Veiligheid is te vinden op de website van het Digital Trust Center.[3]

1: Risicoanalyse

Risico's kunnen worden geïdentificeerd en geanalyseerd door middel van een risicoanalyse. Voor de uitvoering daarvan zijn verschillende aanpakken mogelijk. Van een pragmatische workshop tot aan gedetailleerd beschreven methodieken. Geen van deze aanpakken is goed of fout. De beste aanpak is er een die goed aansluit bij de behoeften van de organisatie en waar de organisatie zich prettig bij voelt. Het is wel verstandig om uiteindelijk voor een vaste aanpak voor de gehele organisatie te kiezen, zodat resultaten van verschillende risicoanalyses met elkaar vergeleken kunnen worden en progressie door de tijd heen gemeten kan worden.

[2] Er zijn meer publicaties die een beschrijving geven van risico-management. Echter, het bieden van een compleet overzicht vormt geen doel van deze factsheet.

[3] www.digitaltrustcenter.nl/risicoklasse

De verantwoordelijkheid voor het identificeren van de strategische risico's ligt bij de directie en voor de tactische en operationele risico's bij de informatie-eigenaren. De CISO kan deze processen faciliteren en ondersteunen, maar kan nooit de proceseigenaar zijn of dit proces zonder de directie of de informatie-eigenaar uitvoeren. Een CISO die zelfstandig risicoanalyses initiëert, zal moeite ondervinden bij het neerleggen van de geïdentificeerde risico's bij de betreffende informatie of proceseigenaar.

Een risicoanalyse moet goed worden voorbereid. De facilitator van zo'n analyse moet goed thuis zijn in de gekozen aanpak en de aanwezigen moeten goed op de hoogte zijn van wat er gaat gebeuren en wat van hen verwacht wordt. Bij een risicoanalyse moet minimaal de informatie-eigenaar aanwezig zijn, aangevuld met de benodigde domein experts.

Risico acceptatie.

Tijdens een risicoanalyse kan van een risico vastgesteld worden dat deze acceptabel is en dus geaccepteerd kan worden. Zorg voor duidelijke risico-acceptatiecriteria en proces.

Het is noodzakelijk om ook grip te hebben op de risico's voor informatie van de organisatie die in handen is van externe partijen. Neem dit daarom mee in uw eigen risicoanalyse. Maak ook iemand binnen de eigen organisatie verantwoordelijk voor die externe verwerking. Bepaal de vereiste zekerheid over de beveiliging van de informatie bij die externe partij op basis van de gevoeligheid van de informatie. Voor laag-gevoelige gegevens kan vertrouwen in de externe partij voldoende zijn. Bij de hoger-gevoelige gegevens kan een directieverklaring wenselijk zijn. Bij nog gevoeligere gegevens kan gedacht worden aan een certificering, zoals bijvoorbeeld ISO 27001 of een ISAE3402/3000 verklaring.

2: Maatregelselectie

Voor de geïdentificeerde risico's die niet (volledig) geaccepteerd worden, worden maatregelen gekozen. De CISO kan hierbij adviseren of ondersteunen. Sommige hulpmiddelen voor risicoanalyse bieden een geautomatiseerde maatregelselectie aan op basis van voorgedefiniëerde risico's. Een kritische kijk op deze selectie en het overwegen van andere maatregelen dan die in het hulpmiddel zitten, is daarbij verstandig.

Risico's waarderen we met kans × impact. De kans wordt bepaald door alles wat bijdraagt aan het optreden van een incident en de impact bestaat uit alle gevolgen van een incident. Maatregelen kunnen kans-verlagend, impact-verlagend of beide zijn. Let daarom goed op of het effect van de maatregelen aansluit bij de gewenste aanpak van een risico.

Met het nemen van maatregelen zijn veelal kosten gemoeid. Ook kunnen maatregelen een negatief effect hebben op de bruikbaarheid van ICT-systemen.

Zorg daarom voor een goede afstemming van de maatregelen met de daardoor geraakte gebruikersgroep(en) om de kans op shadow-IT te verlagen.

Ga over veiligheidsmaatregelen die op enige wijze of in enige mate conflicterend kunnen zijn met de overige bedrijfsdoelen in gesprek met mensen die het juiste mandaat hebben om daar een beslissing over te kunnen nemen.

3: Implementatie van de maatregelen. Eigenaarschap en kosten.

Een deel van de maatregelen om risico's te verminderen, zal door andere afdelingen geïmplementeerd moeten worden, waaronder vaak de ICT-afdeling. Een maatregel kan dus een andere eigenaar hebben dan het proces waarin het risico gelopen wordt. Dit vraagt om het maken van goede afspraken over de implementatie en het beheer van de maatregelen door die andere afdeling.

Indien een organisatie niet werkt met een interne doorberekening, dan zijn de kosten voor de beveiligingsmaatregelen voor rekening van de afdeling die ze uitvoert. Een informatie-eigenaar is hierdoor mogelijk minder kritisch bij de selectie van een maatregel, wat mogelijk leidt tot meer maatregelen dan nodig is en daardoor tot onnodig hogere kosten. Een minder kritische informatie-eigenaar is mogelijk ook minder betrokken bij de implementatie van een maatregel, wat negatieve gevolgen kan hebben voor de effectiviteit van die maatregel.

4: Voortgangbewaking en terugkoppeling

Van maatregelen wordt gecontroleerd dat ze goed geïmplementeerd worden en dat het beoogde effect, voor zolang het nodig is, blijvend is. Het is niet de taak van de CISO om daarop toe te zien. Dit is een verantwoordelijkheid die belegd is bij de informatie-eigenaar. De voortgang van de implementatie van maatregelen die bij anderen zijn belegd, wordt daarom rechtstreeks bij de informatie-eigenaar gemeld.

De CISO rapporteert onafhankelijk aan de directie over de voortgang van de implementatie. Deze rapportages worden zo veel mogelijk meegenomen in bestaande (risico)rapportages, zodat informatiebeveiliging niet als iets aparts gezien wordt.

Information Security Management System

Om voldoende zekerheid te hebben dat het hele proces van risico's identificeren tot aan rapporteren richting directie, zoals beschreven in de voorgaande paragrafen, goed geborgd is in de organisatie, kan gebruik gemaakt worden van een Information Security Management System (ISMS), zoals beschreven in de ISO 27001 norm voor informatiebeveiliging.

Samenwerking

Zorgen voor een goede omgang met informatie en de bijbehorende risico's, vraagt om een goede samenwerking tussen iedereen die daarmee te maken heeft. Dit zijn naast de informatie-eigenaar, informatiemanager, CISO en ICT-manager, ook de functionaris gegevens-bescherming en/of privacyofficer. Vragen en hulpverzoeken vanuit informatie-eigenaren worden, zoveel als nodig is, gezamenlijk door belanghebbenden opgepakt, wat moet gaan leiden tot een eensgezinde en breed gedragen omgang met informatie. Dit is iets waar een directie op moet sturen.

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

Februari 2023