

Leven met risico's

Risicomanagement. Ongemerkt doet iedereen er aan, heeft iedereen er ervaring mee en kan iedereen er over meepraten. Het verschilt enorm hoe we met risico's omgaan, zowel in de privé-situatie als op het werk. Hoe komt een bepaald risico tot stand? Wat kun je er aan doen om als organisatie meer op één lijn te zitten? Hierover meer in dit artikel. [REIN DE VRIES*](#)

De theorie zegt dat risico gelijk is aan kans x schade. In plaats van schade gebruiken we ook wel de termen 'impact' of 'negatieve gevolgen'. Immers, niet iedere schade laat zich gemakkelijk uitdrukken in geld. Denk bijvoorbeeld aan letselschade, schade aan het milieu, emotionele schade en – voor organisaties een belangrijke – imago- of reputatieschade.

Risicoperceptie

Om de omvang van een risico te ramen, moet je twee zaken inschatten: kans én schade. Van deze twee is de factor schade vaak het gemakkelijkst in te schatten. Echter, feit blijft dat twee

factoren moeten worden ingeschat en dus kunnen zich tussen personen die onafhankelijk van elkaar een schatting doen grote verschillen voordoen. Verschil in risicoperceptie resulteert er in

zeer verschillend met het vraagstuk omgaan.

De vraag is welke organisatie(onderdeel) het juiste doet. Is er sprake van risicobewusteloosheid of van angst-

Een zeker restrisico is niet te vermijden en moet worden geaccepteerd

dat de ene organisatie maatregelen treft om het risico tegen te gaan, terwijl de andere organisatie niets doet. Zelfs binnen organisaties kunnen afdelingen

hazerij? De waarheid valt hierbij moeilijk te achterhalen, het onderwerp is hiervoor te subjectief. Op enig moment blijkt de waarheid en kunnen we precies vertellen waar het fout is gegaan en wat we eigenlijk hadden moeten doen. Zolang het goed gaat, blijft de vraag open. Noch de ene situatie, noch de andere is wenselijk. Als je serieus risico loopt, dan wil je dat weten zodat je een gepast antwoord kunt formuleren. Waarbij bewust 'nee' (risicoacceptatie) ook een antwoord kan zijn. Het te hoog inschatten van risico's leidt tot te veel maatregelen en is evenmin wenselijk. Wat valt er te doen tegen verschillen in risicoperceptie? Zorg allereerst dat je risicoanalyses met een team van inhoudelijk betrokkenen uitvoert, met bij voorkeur drie of meer personen. Laat ieder teamlid zijn visie en ervaring inbrengen. Discussieer over de kans en de mogelijke schade. Neem de tijd voor analyse en het achterhalen van informatie, bijvoorbeeld historische gegevens. Bij complexe doelobjecten kunnen bepaalde mogelijkheden over het hoofd zien. Inschattingfouten zijn mogelijk door een gebrek aan inzicht in de situatie. De mate van dekking, compleetheid en juistheid hangt voor een

Link met informatiebeveiliging

Als we een en ander betrekking laten hebben op de voorziening en verwerking van informatie in de organisatie, kunnen zich bij het manifest worden van gebeurtenissen drie typen gevolgen voordoen die direct of indirect een verdere impact hebben.

Gevolgen voor de beschikbaarheid

Een gebeurtenis kan er voor zorgen dat informatie of functionaliteit niet beschikbaar is op het moment dat deze beschikbaar zou moeten zijn. Het gevolg kan zijn dat de uitvoering van een activiteit als onderdeel van een bedrijfsproces, bijvoorbeeld de uitbetaling van salarissen of het verwerken van bestellingen, niet langer mogelijk is. Verder gevolg kan zijn achterstallig werk, misgelopen omzet, enzovoorts.

Gevolgen voor de exclusiviteit

Een gebeurtenis kan er voor zorgen dat onbevoegden kennis kunnen nemen van informatie die slechts voor bepaalde ogen is bestemd. In het algemeen wordt dit als onacceptabel tot zeer onacceptabel beschouwd (bijvoorbeeld als het om persoonsgegevens gaat) en leidt het voorval wanneer dit in de publiciteit komt zeker tot imago- of reputatieschade.

Gevolgen voor de integriteit

Een gebeurtenis kan er voor zorgen dat de integriteit van informatie wordt aangetast. Foutieve informatie of incomplete informatie is het gevolg. Dit kan verder leiden tot verkeerde beslissingen, extra werk (om integriteit te herstellen), verkeerde communicatie, enzovoorts.



Foto: www.drenthebeweegt.nl

Fietsen: gevaarlijk of niet?

belangrijk deel af van degenen die de risicoanalyse uitvoeren. Dit pleit voor een groter team.

Om risico's systematisch, uniform en objectief te beoordelen is het raadzaam om een methodiek met een waarderings-schema vast te stellen (zie kader). Ga bedachtzaam te werk. Niet iedere gebeurtenis vormt een risico dat moet worden verzacht. Een usb-geheugenstick met bedrijfsinformatie verliezen is bijvoorbeeld vervelend, maar vormt geen bedreiging zolang de kans dat unieke gegevens verloren gaan nihil is en/of de kans op onbevoegde toegang tot de gegevens nihil is. Zo vormt onbevoegde fysieke toegang ook geen risico zolang de kans op verdere negatieve gevolgen nihil is. Anders gezegd: mogelijke gebeurtenissen moeten zorgvuldig worden gewogen om te beoordelen of er werkelijk sprake is van een bedreiging en daarmee van een risico.

Uitval

Verschillende bedreigingen kunnen wanneer ze manifest worden, ieder op zichzelf leiden tot een specifieke situatie (voorval, incident) die niet gewenst is. Een voorbeeld hiervan is uitval van een informatiesysteem. Uitval, met als

gevolg productieverlies, kan verschillende oorzaken hebben, bijvoorbeeld stroomuitval, hardwarestoring, een bedieningsfout, een DoS-aanval (Denial of Service), enzovoorts. In plaats van het onder de loep nemen van een groot aantal losse bedreigingen kunnen in een risicoanalyse ook ongewenste situaties als vertrekpunt worden genomen. In dat geval wordt eerst een beperkt aantal ongewenste situaties geïdentificeerd. Situaties waarvan kan worden voorzien dat ze geen aanmerkelijke schade met zich meebrengen kunnen buiten beschouwing blijven. Een voorbeeld van een ongewenste situatie in het kader van een risicoanalyse 'werken buiten de locatie' is 'onbevoegde leestoeegang tot (gevoelige) informatie van de organisatie'.

Vervolgens wordt voor elke ongewenste situatie een boomstructuur (*fault tree*) opgebouwd, waarbij, binnen de grenzen van het waarschijnlijke en van toepassing op het doelobject, wordt geïnventariseerd welke gebeurtenissen leiden tot de bedoelde ongewenste situatie. Maatregelen zijn nodig als de kans op optreden van de ongewenste situatie ten gevolge van kansrijke gebeurtenis-

sen te hoog is in combinatie met de omvang van de schade volgens het vastgestelde waarderingschema.

Risico-inperking

Als een risico als te groot is beoordeeld, zijn risico-inperkende maatregelen nodig. De vraag is welke maatregelen en wat deze mogen kosten? Ook dit is een lastig te beantwoorden vraag. Risico's vallen veelal op meerdere manieren te bedwingen. Welke maatregelen kies je en wanneer is het goed genoeg? Theoretisch gezien wil je een risico precies terugbrengen tot het niveau dat acceptabel is. Meer doen dan nodig brengt extra kosten met zich mee. Van veel maatregelen valt echter niet te zeggen boven welke drempel ze moeten worden ingevoerd of met hoeveel het risico wordt gereduceerd.

Neem *two-factor authentication*. Deze vorm van logische toegangsbeveiliging voer je in om een grotere mate van zekerheid te hebben dat alleen bevoegde personen kunnen inloggen. Maar wanneer voer je deze maatregel in? En in welke vorm? De kosten van oplossingen kunnen aanzienlijk verschillen. Ook het vaststellen van een maatregel- »

Waarderingschema


Om risico's systematisch, uniform en objectief te beoordelen is het nodig om een waarderingschema vast te stellen. Het kan geen kwaad om binnen de organisatie voor risicobeheersing een norm af te spreken, zowel wat betreft methodiek als het in getallen uitdrukken van risico's. Bijvoorbeeld met gebruik van een risicomatrix met de geijkte assen 'kans' en 'impact'. De dimensies kans en impact worden in een beperkt aantal waarden opgedeeld, bijvoorbeeld laag, midden en hoog. In de praktijk wordt veelal gewerkt met een schaal met vier of vijf waarden. Drie waarden blijken vaak te beperkt, terwijl bij meer dan vijf waarden het onderscheid tussen de waarden vervaagt en te klein wordt om er zinvol mee te kunnen werken. Per kans-impactcombinatie spreek je af of maatregelen nodig zijn. Zo zijn voor een potentieel schadelijke gebeurtenis met een kans 1 en impact 4 geen tegenmaatregelen nodig, maar voor een gebeurtenis met kans 2 en impact 5 wel. Je ontkomt veelal niet aan een grijs gebied – twijfelgevallen – waarbij verdere analyse nodig is om te achterhalen of tegenmaatregelen nodig zijn of niet.

Kans	Omschrijving
1 Onvoorstelbaar	Met de huidige kennis en ervaring is het bijna niet voor te stellen dat de bedoelde gebeurtenis zich zal voordoen.
2 Onwaarschijnlijk	Met de huidige kennis en ervaring lijkt het onwaarschijnlijk, maar wel voorstelbaar, dat de bedoelde gebeurtenis zich zal voordoen. De kans dat de gebeurtenis zich niet voordoet is (veel) groter dan de kans dat de gebeurtenis zich wel voordoet.
3 Waarschijnlijk	Met de huidige kennis en ervaring lijkt het waarschijnlijk dat de bedoelde gebeurtenis zich zal voordoen. De kans dat de gebeurtenis zich voordoet is groter dan de kans dat de gebeurtenis zich niet voordoet.
4 Vrijwel zeker	Met de huidige kennis en ervaring is het vrijwel zeker dat de bedoelde gebeurtenis zich zal voordoen. De kans dat de gebeurtenis zich voordoet, of zelfs meerdere malen, is vele malen groter dan de kans dat de gebeurtenis niet voordoet.
5 Regelmatig	Met de huidige kennis en ervaring is het vrijwel zeker dat de bedoelde gebeurtenis met regelmaat zal voordoen.

Impact	Omschrijving
1 Verwaarloosbaar	Nauwelijks impact op organisatie, alleen impact op eigen omgeving (bijvoorbeeld medewerkers kunnen niet werken) en / of tijdig herstel / inhalen achterstallig werk mogelijk zonder, of met zeer beperkte, extra middelen. Kosten < € 10.000 per dag. Geen media aandacht).
2 Middelgroot	Van invloed op het behalen van afdelingsdoelstellingen, alleen impact op eigen omgeving (bijvoorbeeld medewerkers kunnen niet werken) en / of tijdig herstel / inhalen achterstallig werk vergt inzet extra middelen. Kosten < € 100.000 per dag. Geen media aandacht.
3 Groot	Zekere gevolgen voor behalen van afdelingsdoelstellingen, bedrijfsmatige consequenties voor de afnemer zijn beperkt in duur en omvang. Leidt tot grote klantontevredenheid. Kosten < € 500.000 per dag. Krijgt aandacht van de media. Leidt tot reputatie- of imagoschade.
4 Zeer groot	Zekere gevolgen voor de omvang van de organisatie, bedrijfsmatige consequenties (ook voor eventuele leveranciers en/of afnemers) zijn substantieel in duur en /of omvang. Er kan sprake zijn van contractbreuk, boetevorderingen / schadeclaims. Grote kans op verlies van klanten. Kosten < € 1.000.000 per dag. Kan leiden tot instellen van onderzoek door stakeholders. Krijgt grote media aandacht. Verlies van vertrouwen van stakeholders (medewerkers, klanten, leveranciers, investeerders, et cetera).
5 Catastrofaal/desastreus	Brengt het voortbestaan van de organisatie serieus in gevaar, bedrijfsmatige consequenties (ook voor eventuele leveranciers en/of afnemers) zijn groot tot zeer groot. Aanzienlijke boetevorderingen / schadeclaims. Kosten > € 1.000.000 per dag. Kan leiden tot al dan niet gedwongen aftreden van bestuurders. Grootschalig reputatie- of imagooverlies.

lenset maakt deel uit van de risicoanalyse en kan het beste door een team ter hand worden genomen. Om te komen tot die maatregelen die echt nodig zijn. Waak daarbij voor de manager die gaat

voor 'goud' omdat dat zo mooi is terwijl 'zilver' goed genoeg is. En pas op voor de accountant die je vertelt dat je wachtwoord per se uit minimaal acht karakters moet bestaan in plaats van zes. Laat

hem eerst maar eens calculeren hoeveel risicoreductie dat oplevert! 

* Rein de Vries is senior consultant en partner bij LBVD (www.lbvd.nl)