De riskante wereld van de IT

Marcel Spruit
Lector Informatiebeveiliging

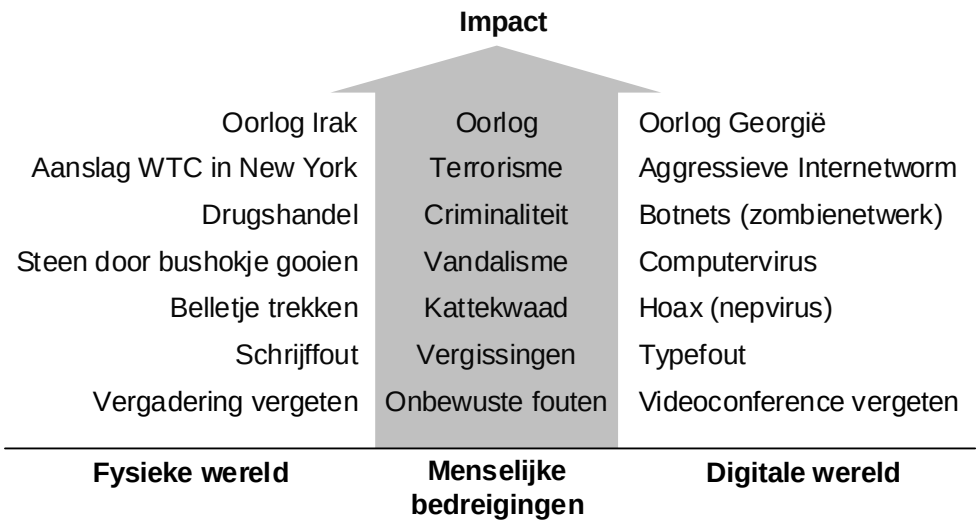
Informatietechnologie

Informatietechnologie, ofwel IT,[1] komen we allemaal iedere dag tegen. IT zit niet alleen in computers, maar ook in (mobiele) telefoons, audiovisuele apparatuur, auto's, wasmachines, koelkasten, klokken, pinpassen, et cetera. We zijn zo langzamerhand gewend geraakt aan al die IT. Het valt de meesten van ons niet eens meer op dat er IT in bijvoorbeeld een wasmachine zit. En we kijken er ook niet meer van op als een wasmachinemonteur aan komt zetten met een draagbare computer om een storing op te sporen. Al die IT is gemeengoed geworden. We bellen mobiel, we sparen met een airmiles-kaart in plaats van zegeltjes te plakken, we betalen met een pinpas in plaats van geld, we sturen een e-mail in plaats van een brief, we doen onze bankzaken via het Internet, et cetera.

De digitalisering rukt nog steeds verder op. Informatie en informatiestromen die niet digitaal waren, worden gedigitaliseerd. Zo wordt tegenwoordig digitaal geschreven, gebeld, gemaild, gefotografeerd, muziek geluisterd, et cetera. Ook bedrijven en instellingen zijn aan het digitaliseren.[2] Papieren informatiestromen worden gedigitaliseerd. Veel organisaties scannen alle papieren post bij het binnenkomen en sturen deze vervolgens als e-mails verder de organisatie in. Ook worden documenten, boeken en tekeningen door scannen gedigitaliseerd. De voordelen hiervan zijn dat de opslag van digitale informatie veel minder ruimte kost, en dat digitale informatie veel sneller op te halen en te verspreiden is.

Mensen en organisaties accepteren de toegenomen mogelijkheden en comfort die met IT gerealiseerd worden als een vanzelfsprekendheid. Deze vanzelfsprekendheid heeft ook een keerzijde, namelijk dat we ons nauwelijks bewust zijn van de gevaren die aan het gebruik van IT kleven.[3,4,5] Toch ontstaan nieuwe bedreigingen juist bij de introductie van nieuwe technologieën. Zo leidde de komst van de videorecorder tot illegale videohandel, de komst van de computer tot computervirussen, en pinpassen tot pinpasfraude. Ook bij de introductie van nieuwe toepassingen van bestaande technologieën ontstaan veelal nieuwe bedreigingen. Toen computers gemeengoed waren, leidde grootschalige koppeling ervan tot nieuwe bedreigingen, waaronder hacking; de mobiele telefoon leidde tot extra verkeersongelukken doordat er gebeld werd tijdens het rijden, e-mail leidde tot spam, et cetera.

De IT zit zo vervlochten in onze maatschappij, dat het voor niemand meer te ontwijken is. De digitale wereld biedt veel mogelijkheden, maar ook veel gevaren. Veel bedreigingen die we kennen uit de fysieke wereld krijgen een equivalent in de digitale wereld. In figuur 1 zijn een paar voorbeelden van door mensen veroorzaakte bedreigingen gegeven.



Figuur 1: Voorbeelden van menselijke bedreigingen in de fysieke en de digitale wereld.

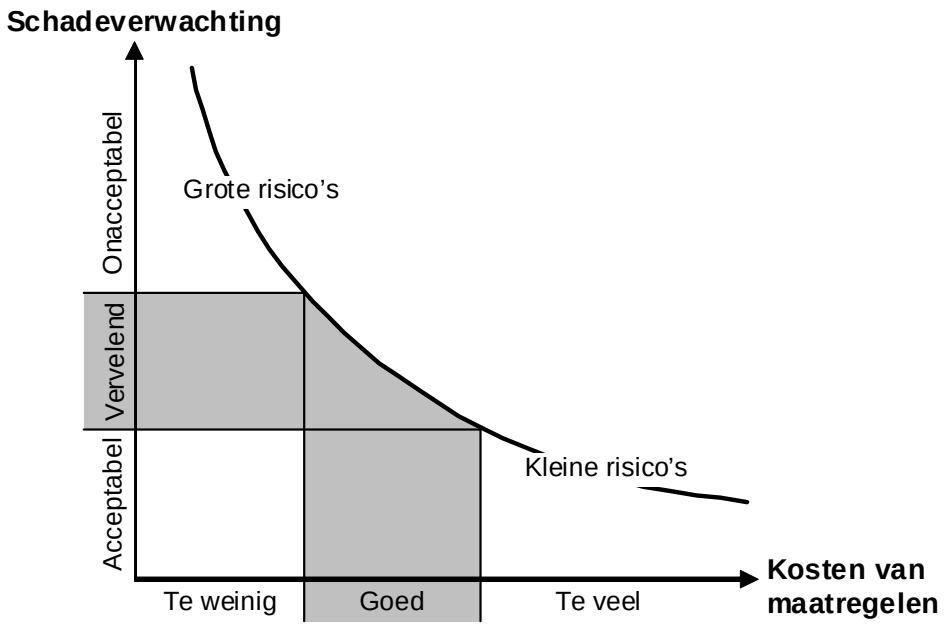
Veel organisaties zijn inmiddels zo afhankelijk van hun digitale informatie geworden dat ze geen moment zonder kunnen. De juiste informatie moet op de juiste tijd op de juiste plaats zijn, anders lopen er processen spaak. Bovendien is een deel van de informatie niet alleen belangrijk voor de processen, maar ook interessant voor derden. Hierbij valt te denken aan bijvoorbeeld financiële informatie en marktinformatie. Deze informatie mag niet in verkeerde handen vallen. Dit geldt ook voor informatie over personen, zowel klanten als eigen medewerkers. Iedere organisatie is wettelijk verplicht om daar zorgvuldig mee om te gaan.[6]

De digitale informatie in organisaties moet adequaat beschermd worden. Maar wanneer is de bescherming adequaat? En wat is daarvoor nodig? Dit zijn vragen waar binnen het lectoraat Informatiebeveiliging onderzoek naar gedaan wordt. Dit artikel gaat daar op in.

Risico's en risicomanagement

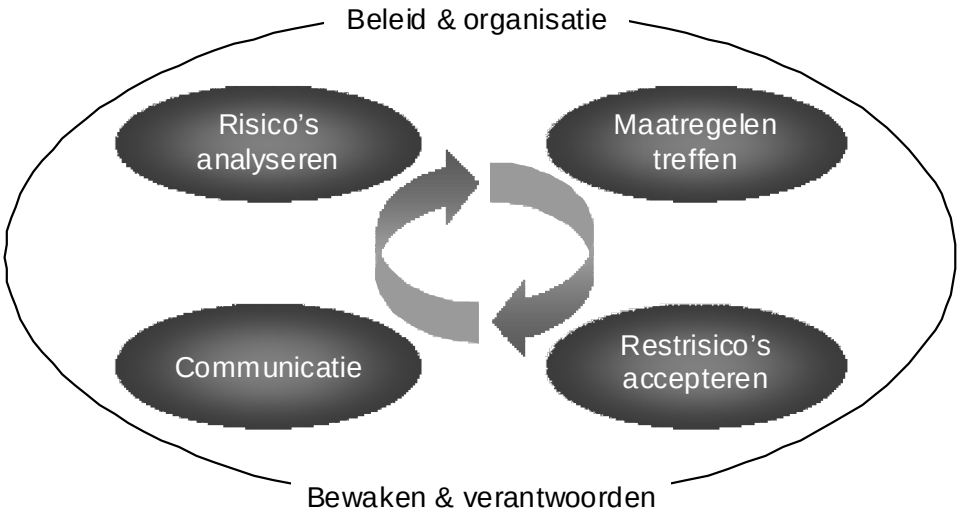
Hoe belangrijker de IT voor een organisatie is, des te groter de schade bij een incident kan zijn. Daarom moet de IT tegen allerlei verschillende bedreigingen beschermd worden. Hieronder vallen bedreigingen, zoals onopzettelijke fouten, vandalisme, criminaliteit, terrorisme, brand, bliksem, storm, elektriciteitsuitval, software-bugs, apparatuurstoring, et cetera.[7] Niet alle bedreigingen zijn in elke situatie even ernstig. Bovendien is de kans van optreden voor de verschillende bedreigingen heel verschillend. Daarom is het rücksichtslos treffen van beveiligingsmaatregelen geen goed idee. Naast het nemen van te weinig maatregelen is het namelijk ook mogelijk te veel maatregelen te treffen. Om dit inzichtelijk te maken is in figuur 2 het verband tussen de risico-omvang, ofwel de te verwachten schade door bedreigingen, en de kosten van de getroffen maatregelen geschetst. In de onderste zone van de figuur bevinden zich de overbodige maatregelen, waar euro's uitgegeven

worden om dubbeltjes te beveiligen. De kunst is om voldoende maatregelen te treffen, niet te weinig maar ook niet te veel.[8]



Figuur 2: Schadeverwachting versus kosten van maatregelen

Het proces risicomanagement richt zich achtereenvolgens op het bepalen welke set maatregelen nodig is, het treffen van de betreffende set maatregelen, het accepteren van de overblijvende risico's en het communiceren over de genomen beslissingen. Daarnaast moeten zowel het proces als de daarbinnen getroffen maatregelen bewaakt worden en moet verantwoording afgelegd worden over de geboekte resultaten en de ontstane problemen. Het proces risicomanagement is in figuur 3 schematisch weergegeven.



Figuur 3: Het proces risicomanagement

Vanuit het lectoraat Informatiebeveiliging wordt door de lector deelgenomen aan het onderzoek van de werkgroep "Risk Assessment and Risk Management" van het Europese agentschap ENISA (European Network and Information Security Agency). De werkgroep heeft het proces risicomanagement verder gedetailleerd naar een aantal subprocessen, te weten:[9]

- Beleid en organisatie:
    1. Inventariseren van de externe omgeving.
    2. Inventariseren van de interne organisatie.
    3. Inventariseren van de risicomanagementcontext.
    4. Formuleren van het risicoacceptatieniveaus.

- Risico's analyseren:
    5. Inventariseren van de risico's.
    6. Analyseren van de relevante risico's.
    7. Evalueren van de risico's.

- Maatregelen treffen:
    8. Inventariseren van de mogelijke opties.
    9. Opstellen van een plan van aanpak.
    10. Goedkeuren van het plan van aanpak.
    11. Implementeren van het plan van aanpak.
    12. Identificeren van de overblijvende risico's.

- Restrisico's accepteren:
    13. Accepteren van de overblijvende risico's.

- Bewaken en verantwoorden:
    14. Risicomanagement bewaken en verantwoorden.

- Communicatie:
    15. Communiceren over risico's en verbeteren van draagvlak.

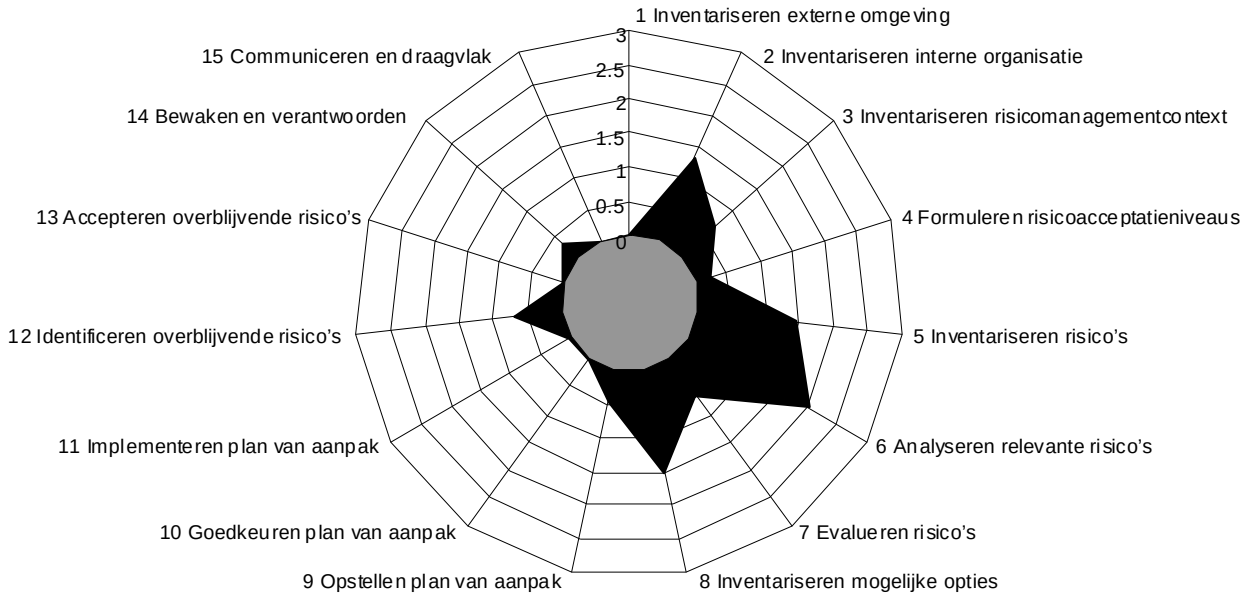
Methoden voor risicomanagement

Om een eenduidige invulling van de verschillende subprocessen van risicomanagement te krijgen, is methodische ondersteuning wenselijk. Temeer daar verschillende subprocessen in de praktijk tamelijk lastig blijken te zijn.

De behoefte aan methodische ondersteuning is zo duidelijk dat in verschillende landen initiatieven hiertoe ontplooid zijn. Dit heeft geleid tot een scala aan methoden die ieder beogen het proces risicomanagement in meerdere of mindere mate te ondersteunen. Een greep uit de methoden, met het land van oorsprong:

- A&K-analyse (Afhankelijkheids- en Kwetsbaarheidsanalyse), Nederland.
- CRAMM (CCTA Risk Analyses and Management Methodology), Groot Brittanië.
- IT Grundschutz, Duitsland.
- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), Frankrijk.
- OCTAVE, Verenigde Staten.
- SARA (Simple to Apply Risk Management), internationale industrie.
- Etc.

De ontstaansgeschiedenis van de verschillende methoden verschilt aanzienlijk. Op basis van de hierboven gedefinieerde subprocessen van risicomanagement, is het mogelijk om van iedere methode te bepalen in hoeverre de betreffende methode de verschillende subprocessen ondersteunt.



Figuur 4: De mate waarin de A&K-analyse de subprocessen van risicomanagement ondersteunt

Voor de A&K-analyse,[10] die binnen de Nederlandse overheid veel toegepast wordt, is de mate van ondersteuning weergegeven in figuur 4. In de radardiagram staat ieder van de assen voor één van de subprocessen. De mate van ondersteuning per subproces kan lopen van in het geheel niet (waarde=0) tot zeer volledige en gedetailleerde ondersteuning (waarde=3).

Onderwerpen die in de methode A&K-analyse weinig of niet ondersteund worden, zijn:

- Ondersteuning voor beleid en organisatie.
- Risicotolerantielimieten.
- Risicoacceptatiecriteria.
- Standaard bedreigingen.
- Standaard maatregelen.
- Invulschema's.
- Ondersteuning voor bewaken en verantwoorden.
- Ondersteuning voor communicatie en draagvlak.

Bovendien bevat het beheer van de methode een paar zwakke plekken:

- De handleiding is onvolledig en verouderd.
- De methode heeft geen formele eigenaar die de methode onderhoudt.
- Er is geen digitale documentatie en ondersteuning beschikbaar.
- Er zijn geen standaard hulpmiddelen op de markt.

Uit bovenstaande kanttekeningen zou men de conclusie kunnen trekken dat de A&K-analyse geen goede methode is. Dat blijkt erg mee te vallen. Ten eerste is er geen ideale methode beschikbaar, dus elke methode heeft wel een paar nadelen. Ten tweede hangt de benodigde methodische ondersteuning sterk af van de situatie. In sommige situaties is alleen globale ondersteuning op hoofdlijnen nodig. In dergelijke gevallen is een zeer volledige en gedetailleerde methode overkill. De gedetailleerde acties en lijsten die vanuit de methode aangereikt worden, kunnen zelfs het draagvlak voor risicomanagement aantasten. In andere gevallen, zoals in sterk geformaliseerde organisaties met een complexe IT-infrastructuur kan het juist wel nodig zijn om zeer formele en gedetailleerde methodische ondersteuning te hebben.

In het algemeen bepalen de volgende factoren in welke mate de methodische ondersteuning formeel en gedetailleerd moet zijn en welke methode of methoden daarvoor in aanmerking komen:

- Het belang van de informatievoorziening.
- De complexiteit van de informatievoorziening.
- De organisatiecultuur.
- De ervaring met risicomanagement.
- De compatibiliteit met eerder gebruikte methoden en hulpmiddelen.
- De compatibiliteit met risicomanagement in ander (keten)organisaties.
- Eisen die vanuit wet- en regelgeving aan risicomanagement gesteld worden.
- Eisen die externe stakeholders aan risicomanagement stellen.

Verantwoordelijkheid voor risicomanagement

Risicomanagement kan pas werken, als er eerst beleid voor bepaald is en het een plek in de organisatie gekregen heeft. Dat betekent dat iemand de organisatie van risicomanagement moet regelen. In de praktijk wordt dit nogal eens als een hete aardappel heen en weer geschoven tussen enerzijds de managers en anderzijds de risico- en beveiligingsspecialisten. Vaak vinden beide partijen dat de andere partij daar het meest geschikt voor is.

De theorie is heel duidelijk over het beleggen van de verantwoordelijkheid voor risicomanagement:[7] risicomanagement over alle onderdelen binnen de organisatie, dus ook risicomanagement met betrekking tot de informatievoorziening, maakt deel uit van integraal management en is dus een natuurlijk onderdeel van lijn-, proces- en projectmanagement. In het bedrijfsleven wordt vaak, terecht, het motto “ondernemen is risico’s nemen” gebruikt. Het managen van risico’s is een onderwerp voor het management van de organisatie.

De praktijk blijkt echter weerbarstig te zijn. Risicomanagement krijgt structureel te weinig aandacht van het management. Eerst moet er een incident gebeuren; dan volgt actie. Veelal beperkt de actie zich tot het voorkomen van hetzelfde incident in de toekomst. Het volgende

incident dat door een andere bedreiging veroorzaakt is, leidt weer tot een beperkte actie, et cetera. In het algemeen stoelt risicomanagement, voor zover het al expliciet aandacht van het management krijgt, te weinig op preventie.

Het tekort aan aandacht voor preventie is wel verklaarbaar. Veelal schatten managers de risico-omvang binnen hun organisatie veel te laag in. Voor een groot deel wordt dit veroorzaakt doordat de risico- en beveiligingsspecialisten hun management te weinig informeren over de risico-omvang. Daardoor hebben managers veelal het onterechte idee dat er binnen hun organisatie weinig relevante risico's zijn. In praktijk komen regelmatig incidenten voor, maar ze worden niet aan het management gerapporteerd. Behalve de grote incidenten. Maar de vele kleine incidenten zorgen bij elkaar voor een aanzienlijke schadepost, waarvan het management veelal volstrekt onwetend is.

Managers die te weinig informatie over risico's en incidenten krijgen, zijn zich hier in het algemeen niet van bewust. Daarom zullen ze niet achter deze informatie aan gaan. Bovendien onderschatten ze het belang van risicomanagement en zullen dus niet inzetten op het aannemen van betere risico- en beveiligingsspecialisten, die hun wellicht wel goed zouden informeren. Betere opleiding van risico- en beveiligingsspecialisten is nodig om deze vicieuze cirkel te kunnen doorbreken. De opleiding Information Security Management die in 2008 aan de Haagse Hogeschool gestart is, kan een zinvolle bijdrage leveren aan het invullen van deze behoefte. Daarnaast wordt binnen het lectoraat Informatiebeveiliging onderzoek gedaan naar wat er nodig is om de perceptie van managers met betrekking tot risico's en incidenten te verbeteren. Met de resultaten uit dat onderzoek wordt het wellicht duidelijker welke informatie managers nodig hebben en hoe die informatie aangeleverd kan worden.

Tot slot

Elke organisaties is in meer of mindere mate afhankelijk van digitale informatie. In de toekomst zal deze afhankelijkheid toenemen. Adequate bescherming van de informatie en de IT is nu al broodnodig, maar zal in de toekomst nog belangrijker worden. Er zijn verscheidene methoden beschikbaar om het inrichten van de bescherming te ondersteunen. Hoewel de ideale methode waarschijnlijk nooit gevonden zal worden, is verder onderzoek nodig om de bestaande methoden voor de toekomst te verbeteren. In aanvulling daarop is meer aandacht nodig voor het verbeteren van de perceptie van managers met betrekking tot risico's en incidenten en het beter opleiden van risico- en beveiligingsspecialisten.

Referenties

[1] W. Stallings, *Data and computer communications*, Prentice-Hall, Upper Saddle River, 2003.

[2] P. Mettau, *Mijnoverheid.nl*, Het Expertise Centrum, Den Haag, 2005.

[3] P. Neumann, *Illustrative risks to the public in the use of computer systems and related technology*, http://www.csl.sri.com/users/neumann/illustrative.html

[4] CSI, *CSI Computer Crime & Security Survey 2008*, Computer Security Institute, New York, 2008.

[5] Govcert, *Trendrapport 2009; Inzicht in cybercrime: trends & cijfers*, Govcert.nl, Den Haag, 2009.

[6] *Wet Bescherming Persoonsgegevens*, 6 juli 2000, zie www.wetten.overheid.nl en www.cbpweb.nl

[7] P. Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*, Pearson, Amsterdam, 2005.

[8] M. Spruit, *Waardevol maakt kwetsbaar: het belang van informatiebeveiliging*, Haagse Hogeschool, Den Haag, 2004.

[9] ENISA, *Risk Management*, http://www.enisa.europa.eu/act/rm

[10] ACIB (1996) Handleiding Afhankelijkheids- en Kwetsbaarheidsanalyse, Den Haag: Ministerie van BZK.