# VEILIGER MET VOORKENNIS

## Deel 1

"Bij uitval van het navigatiesysteem bestaat er geen recht op vervangend vervoer. Er is namelijk geen sprake van uitval van het voertuig. We adviseren reizigers naast het navigatiesysteem ook wegenkaarten mee te nemen." – SOS International

In het huidige informatietijdperk raakt IT alle aspecten van ons leven. Voor organisaties is het belangrijker dan ooit om te weten wat ze aan de zich steeds sneller ontwikkelende technologie hebben en hoe kansen veilig kunnen worden benut. De technologische ontwikkeling heeft ook invloed op de beveiliging van informatie zelf. Welke kennis is dan nodig om informatie veilig te houden? Die vraag beantwoord ik in twee delen.

In het eerste deel start ik met het besturingsparadigma als context voor informatiebeveiliging. Vervolgens geef ik aan wat de rol is van een systematische analyse om risico's goed in te schatten. In de conclusie van dit deel vat ik samen welke kennis organisaties meestal missen bij de invulling van risicomanagement.

In het tweede en laatste deel analyseer ik de kansen en risico's van ontwikkelingen zoals de toenemende complexiteit en het voortdurend opschalen van organisaties en systemen. Ik schets tevens de invloed die kwantumcomputers kunnen hebben op de encryptie van data. Ik sluit af met een samenvatting welke kennis voor informatiebeveiliging nuttig is.

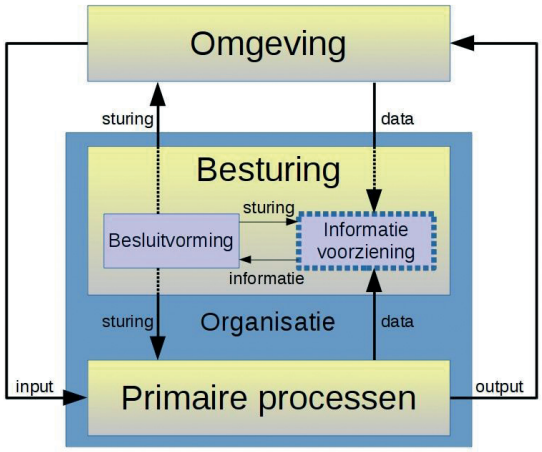
*"One of the functions of an organization, of any organism, is to anticipate the future, so that those relationships can persist over time" – Kevin Kelly*

## Sturen van organisaties

Personen en organisaties die open staan voor de mogelijkheden van nieuwe technologie kunnen grote stappen vooruit maken. Organisaties willen daarom relevante technologische verbeteringen tijdig opmerken, het effect van deze technologie kunnen voorspellen binnen de eigen context, op het juiste moment de juiste beslissing nemen en het effect van veranderingen optimaliseren.

Het besturingsparadigma plaatst de sturing van organisaties in context, zie afbeelding 1. In dit eenvoudige model stuurt het management op basis van informatie het primaire proces en de omgeving, de ondersteunende processen blijven buiten beschouwing. De informatievoorziening produceert deze sturingsinformatie uit in- en externe data. Informatiebeveiliging is voornamelijk geconcentreerd rond de informatievoorziening, inclusief de sturing daarop en rapportage daarover naar het management.

De informatievoorziening is meer gedetailleerd weergegeven in afbeelding 2. De data vanuit het primaire proces als input voor de informatievoorziening bestaat onder andere uit feed forward data (gegevens over de input) en feed back data (bijv. gegevens over eindproducten). Met feed back data kan je later, maar effectiever




**Afbeelding 1 - het Besturingsparadigma als context voor besluitvorming**

bijsturen, omdat dan bijvoorbeeld precies bekend is in hoeverre het eindproduct voldoet aan de kwaliteitsnormen. Sturen op de kwaliteit van het eindproduct met feed forward data is sneller en onnauwkeuriger, omdat de fouten in de input en de verwerking niet kunnen worden gecorrigeerd.

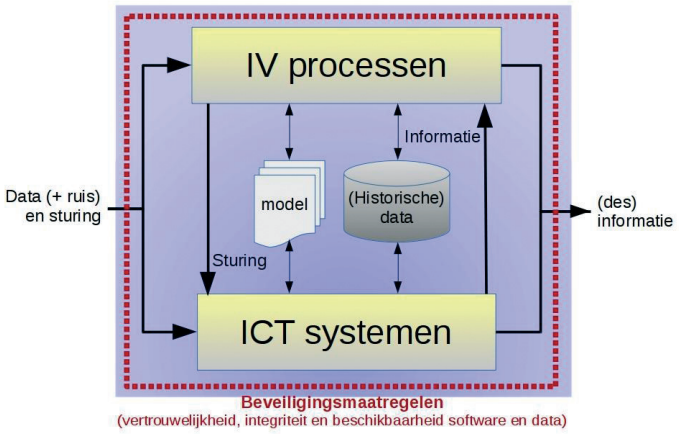
Beiden soorten data zijn complementair aan elkaar en ook allebei nodig, omdat data een onbekende hoeveelheid ruis kan bevatten en foutloze informatiesystemen niet bestaan. Feed forward besturing is gevoelig voor Garbage In, Garbage Out: als de input niet deugt, zal het resultaat ook niet goed zijn. Effectief sturen op basis van feed forward data is daarnaast alleen mogelijk met een model dat betrouwbaar kan voorspellen hoe afwijkingen in de input doorwerken in de kwaliteit van het eindproduct. Feed back data is dus tevens nodig om voorspellende modellen te toetsen en te verbeteren. Ik kom later nog terug op de kwaliteit van modellen.

***"Everything should be as simple as possible, but not simpler" – Albert Einstein***

## Waarom een systematische analyse

De ontwikkelingen in de ICT gaan steeds sneller, zoals blijkt uit het voortduren van de wet van Moore en de steeds korter durende Hype Cycle van Gartner voor nieuwe producten. In het begin van het ICT tijdperk lag de nadruk op het nuttig maken van computers, bijvoorbeeld door met een geschikte programmeertaal processen te automatiseren die informatie uit databases kunnen halen. Het oplossen van steeds

*Henk-Jan van der Molen is freelance docent bij de Security Academy.*
*De auteur wil iedereen bedanken die een positieve inbreng heeft geleverd aan dit artikel, in het bijzonder Jurgen van der Vlugt en Charlotte Rugers.*




**Afbeelding 2 - Informatievoorziening (IV) binnen het besturingsparadigma**

complexere problemen vormt de uitdagingen voor de nabije toekomst, zoals het real time volgen van significante veranderingen in netwerken, het halen van informatie uit grote meerdimensionale en ongestructureerde datasets, het verwerken van grote datastromen, kortom: de extractie van relevante informatie uit de beschikbare verzameling data inclusief ruis. En er is behoorlijk wat data beschikbaar als "ruis". Van alle data die nu beschikbaar is, is negentig procent in de afgelopen twee jaar gegenereerd [1].

Overigens verandert de wetenschap zelf ook door de voortdurende ontwikkelingen op ICT gebied. Vroeger moest je bijvoorbeeld wiskundige problemen handmatig kunnen oplossen, tegenwoordig kan de computer dat proces steeds beter ondersteunen. Daardoor verschuift de aandacht naar het stellen van de juiste vragen, het wiskundig goed kunnen formuleren van praktijkproblemen en het valideren van de berekende oplossing [2].

***"The purpose of abstraction is not to be vague, but to create a new semantic level in which one can be absolutely precise"***
***- Edsger Dijkstra***

Abstracties kunnen niet-relevante ruis verwijderen, zodat het onderzoek zich kan richten op het modelleren van het specifieke gedrag van het systeem. Invloed op de input vertaalt zich dan in de beheersing van het systeem. Een goede abstractie vereenvoudigt het beantwoorden van de vraag "hoe kan ik de werking van een systeem optimaliseren?". Een slechte abstractie maakt de vraag onoplosbaar, of (erger) produceert een fout antwoord dat juist lijkt. Een vaak toegepaste manier van onderzoek is per experiment slechts één variabele te veranderen en te kijken hoe die variabele het gedrag van het systeem beïnvloedt.

Daarnaast helpt een abstractie kennis meer generiek toepasbaar te maken, zodat meer soortgelijke problemen kunnen worden opgelost. Toepassing van een abstract model buiten de context is pas verantwoord als die situatie voldoet aan de uitgangspunten en randvoorwaarden (zeg maar: de bijsluiter) van dat model. De afwijkingen van de nieuwe situatie moeten worden vertaald naar wijzigingen in de scope, parameters en input van het abstracte model. Daarna moeten de conclusies en aanbevelingen uit de analyse van het abstracte model worden terugvertaald naar de praktijksituatie.

Het abstract modelleren van systemen lijkt veel op de zogenaamde "empirische cyclus" in de wetenschap:

1. het beschrijven van relevante waarnemingen uit de praktijk;
2. het opmerken van patronen in de werking van het systeem;
3. het construeren van een logisch model dat de waarnemingen kan verklaren;
4. het voorspellen van nieuw, nog niet waargenomen gedrag van het systeem met dat model;
5. het toetsen van het model door deze voorspellingen te verifiëren in de praktijk.

Een model kan de werking van het systeem correct voorspellen als van alle relevante variabelen de gezamenlijke effecten op het systeem bekend zijn. In de praktijk zullen nooit alle variabelen en hun onderlinge relaties bekend zijn en resteert er in elk systeem een bepaald ruisniveau. Zelfs een correct model kan daarom in de praktijk nooit helemaal nauwkeurig zijn en dat hoeft ook niet. Als de gebruikte modellen met de brondata maar een betrouwbare voorspelling kunnen maken. In het verleden zijn echter regelmatig modellen gebruikt die later onbetrouwbaar bleken. Bijvoorbeeld omdat het model gebaseerd was op verkeerde waarnemingen en pseudo-informatie uit ruis produceerde of het gemodelleerde systeem te chaotisch was om het gedrag betrouwbaar te voorspellen.

***"Errors using inadequate data are much less than those using no data at all" – Charles Babbage***

Waarom dan toch modellen gebruiken, als die beslissers op het verkeerde been kunnen zetten? Dat komt omdat sturen met een redelijk model meestal beter is dan sturen zonder model. Een logisch model helpt ons de wereld om ons heen te begrijpen en te beheersen. Als een model een bepaalde uitkomst niet kan voorspellen omdat die uitkomst afhangt van een samenloop van omstandigheden, kan het model of de bijsluiter worden verbeterd [3].

Toetsing van modellen en systemen blijft altijd nodig, om het nut ervan in de praktijk te bepalen en onnauwkeurige modellen te verbeteren of af te schaffen. Als een structureel onbetrouwbaar model in gebruik blijft, voert de organisatie deze toetsing niet goed uit. Of er is onvoldoende rekening gehouden met de bijsluiter van het model, bijvoorbeeld door het weer van volgende maand te voorspellen of één weersverwachting te maken voor een groot gebied. De betrouwbaarheid van sommige modellen kan verbeteren door de scope in tijd en ruimte te verkleinen.

Voor het bedenken, toetsen, aanpassen aan de context en verbeteren van modellen en systemen zijn analytische vaardigheden nodig en logisch redeneren. Modellen die zonder deze vaardigheden worden gebruikt zullen minder nauwkeurig voorspellen.

***" There is no security on this earth; there is only opportunity"***
***– Douglas MacArthur***

## Beveiliging in de praktijk

Ten opzichte van veel andere landen zijn de loonkosten in Nederland (veel) hoger. Om op kostprijs te kunnen blijven concurreren in "the global village" is een steeds grotere inzet van ICT in bedrijfsprocessen nodig. Zonder de juiste ICT ondersteuning zijn concepten zoals "Just in Time", "Zero Inventory" en "On Demand" niet te integreren in bedrijfsprocessen. Concurreren op basis van innovatie is effectief als de organisatie erin slaagt (concurrentie)gevoelige informatie geheim te houden en de primaire processen ongestoord kunnen doordraaien. De keerzijde van de continue innovatie is dat organisaties steeds afhankelijker worden van ICT systemen.

De voortdurende technologische vernieuwing introduceert naast voordelen ook steeds nieuwe beveiligingsrisico's en dat maakt informatiebeveiliging een dynamisch vakgebied. De volgende vragen en dilemma's vergroten die dynamiek verder:

- Een adequate beveiliging of de afwezigheid van kwetsbaarheden zijn onmogelijk objectief aan te tonen.
- Wegen de verwachte voordelen van veranderingen op tegen de (on)bekende nadelen?
- Hoe complexer een systeem, hoe meer kans dat er beveiligingsgaten aanwezig zijn.
- Een aanvaller heeft aan een kwetsbaarheid genoeg, terwijl een verdediger alle gaten moet dichten.
- Welke risico's loop ik en met welke maatregelen verminder ik die risico's tot een acceptabel niveau?
- Hoe kan ik incidenten het beste signaleren en afhandelen, zodat de impact op mijn bedrijfsprocessen minimaal is?
- Waar kan ik verantwoord bezuinigen op de kosten van mijn beveiliging?

Een beveiligingsincident vermindert de performance van de ICT resources van bedrijfsprocessen en kan gevoelige klantinformatie lekken. Ook het niet tijdig kunnen leveren van de juiste producten of als de kwaliteit lager is dan afgesproken, schaadt de reputatie van het bedrijf en verslechtert de concurrentiepositie. Om de impact van beveiligingsincidenten efficiënt te verminderen, moet de organisatie risicogericht maatregelen nemen. Daarom vullen veel organisaties hun beveiliging in met acties die de volledige PDCA-cyclus afdekken, zie tabel 1.

Cybercriminelen profiteren ook van de technologische ontwikkelingen, waarbij malafide software, tools en diensten op de zwarte markt worden verhandeld. Daardoor kan een steeds breder publiek geavanceerde cyberaanvallen uitvoeren. Dat is onder andere merkbaar bij de detectie van malware, die afhankelijk is van feed back informatie die gedeeld moet worden over meerdere organisaties. Daardoor heeft malware detectie in de afgelopen jaren zoveel achterstand opgelopen, dat up-to-date Antivirus pakketten nog maar ca. 50% van de nieuwste malware detecteren [4]. Die trend lijkt stabiel – wist in 2012 nog 37% van de slachtoffers zelf vast te stellen dat hun systemen waren besmet, in 2013 daalde dat naar 33% [5]. Verontrustend is dat investeringen in cybersecurity vooralsnog de vatbaarheid voor aanvallen nauwelijks vermindert [6]. We zijn nog niet in staat om het rendement van investering in beveiligingsmaatregelen goed te voorspellen. Hierdoor worden individuele systemen steeds kwetsbaarder, waardoor de frequentie van incidenten toeneemt. Gecombineerd met de toenemende afhankelijkheid, groeit de impact en daarmee het risico van cyber incidenten.

***"It is not certain that everything is uncertain"***
***– Blaise Pascal***

| | |
|---|---|
| **Plan** | Opstellen van **beveiligingsbeleid en plannen** om te voldoen aan wet- en regelgeving met o.a.:<br>• doelstellingen, uitgangspunten, taken, inventarisatie en toleranties van risico's;<br>• een strategie en plannen om de beveiliging op het gewenste niveau te krijgen en<br>• regels en standaarden om de beveiliging op het gewenste niveau te houden. |
| **Do** | Het **uitvoeren** van plannen om de beveiliging op het gewenste niveau te krijgen met o.a.<br>• Verwerving, inzet, optimalisatie en uitfasering van resources;<br>• Opleiding, training en oefening personeel;<br>• Het ontwikkelen en toepassen van **standaarden**, zoals best practice beveiligingsnormen, architecturen en procedures, zoals voor:<br>  • het uitvoeren van risico-analyses;<br>  • de preventie van incidenten (o.a. vermijden single-points-of-failure);<br>  • het realtime signaleren en oplossen van kwetsbaarheden, incidenten en aanvallen, en<br>  • het beheerst doorvoeren van veranderingen in de informatievoorziening. |
| **Check Act** | Het **monitoren** van de implementatie van het beleid, de plannen, de performance van sturing, (human) resources en standaarden, het uitvoeren van periodieke audits en het evalueren van (bijna) incidenten.<br>Het treffen van preventieve en correctieve **maatregelen** op basis van de analyse van monitoring, audits en andere evaluaties. |

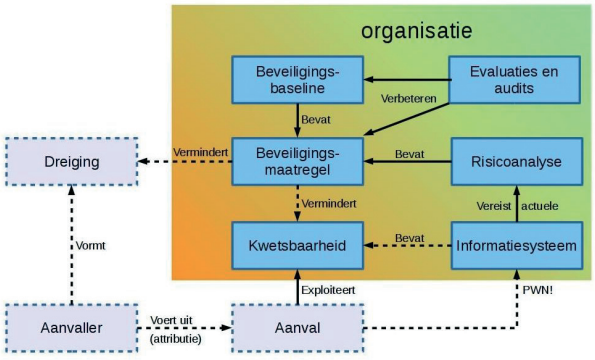
**Tabel 1 - Voorbeelden van beveiligingsacties als onderdeel van de PDCA-cyclus**

In onzekere tijden wil het management van een organisatie gevraagd en ongevraagd advies over risicotrends, zeker als overschrijding van risicotoleranties dreigt. Dat vergt een periodieke en systematische analyse om relevante trends voor informatiebeveiliging te signaleren. Op basis van gezond verstand is informatie alleen goed te beveiligen met de volgende randvoorwaarden:

- beschreven processen – alleen zo is herhaling, controle en continue verbetering mogelijk,
- specifieke en tijdige informatie over eigen kwetsbaarheden en (elders) uitgevoerde aanvallen,
- de mogelijkheid om effectieve en veilige standaarden in te zetten,
- modellen om te voorspellen welk effect veranderingen op de beveiliging hebben en
- regelmatige objectieve evaluaties van (doorgevoerde veranderingen op) beveiligingsmaatregelen.

Voldoen aan het bovenstaande lijstje met eisen voor het oplossen van de vragen en dilemma's heeft echter nogal wat voeten in de aarde. Afbeelding 3 vat de vragen en dilemma's met een eenvoudige aanvalsvector samen, waarbij de gestippelde lijnen en informatiebronnen aangeven dat een organisatie daar slecht zicht op heeft. Een organisatie kent bijvoorbeeld meestal niet alle kwetsbaarheden van een informatiesysteem en hoeveel de operationele beveiligingsmaatregelen deze kwetsbaarheden verminderen. Het signaleren dat een informatiesysteem is gecompromitteerd wordt ook steeds lastiger. Cybercriminelen willen zo lang mogelijk profiteren van gehackte systemen en verifiëren vaak vooraf dat reguliere beveiligingsmaatregelen zoals Antivirus en firewalls hun aanvallen niet opmerken [7]. Het gemiddeld aantal dagen dat aanvallers in 2013 gebruik konden maken van een besmet netwerk voordat ze werden ontdekt is 229 dagen [8].

Er zijn twee gangbare methoden om de schade van incidenten te bepalen [9]. De schade van uitval van een systeem kan bijvoorbeeld worden berekend met de factoren MTBF, MTTD en MTTR (Mean Time Between Failure, Mean Time to Detect, Mean Time to Repair). De MTTR's van de essentiële productiesystemen bepalen of de Recovery Time Objective van de organisatie kan worden gehaald.




**Afbeelding 3 - samenhang vragen en dilemma's van informatiebeveiliging**

Anderzijds kan met een schatting van de SLE (Single Loss Expectancy) vermenigvuldigd met de jaarlijkse frequentie van incidenten de ALE (Annual Loss Expectancy) worden bepaald. De businesscase van een beveiligingsmaatregel wordt dan als volgt ingevuld: schat de ALE met en zonder de maatregel en verminder dit verschil met de eenmalige en jaarlijkse kosten van de maatregel. De impliciete aanname voor dergelijke berekeningen is echter dat de kansverdelingen van de MTTR, MTTD en SLE normaal zijn verdeeld. Deze aanname is echter niet altijd correct, zie het tweede deel van dit artikel.

In dit eerste deel van dit artikel heb ik het besturingsparadigma geïntroduceerd als context voor informatiebeveiliging. Ik heb aangegeven waarom een systematische analyse nuttig is om de effecten van veranderingen te bepalen en welke kennis organisaties meestal missen bij de invulling van risicomanagement. In het volgende deel analyseer ik de risico's en kansen van enkele nieuwe ontwikkelingen, zoals de toenemende complexiteit en het voortdurend opschalen van organisaties en systemen. Ik schets tevens de invloed die kwantumcomputers kunnen hebben op de encryptie van data. In de conclusie vat ik samen welke kennis voor informatiebeveiliging nuttig is en waarom dat zo is.

## Referenties

[1] "Big Data – for better or worse", SINTEF, 2013

[2] Zie bijvoorbeeld wolframalpha.com, sagemath.org en "Homotopy Type Theory – Univalent Foundations of Mathematics" – Univalent Foundations Program, 2013

[3] Als de factoren onafhankelijk zijn, dan is de kans dat ze zich allebei gelijktijdig manifesteren het product van hun individuele kansen. Daarom is volgens Occam's Scheermes de eenvoudigste oorzaak meestal de juiste en kan een eenvoudig model dus goed genoeg zijn. Aangeven wanneer de uitkomst van een model betwijfeld moet worden, verbetert de bijsluiter van het model. En als er tussen afhankelijke factoren een causaal verband bestaat, dan kan het model met die relatie worden uitgebreid.

[4] 'Do Anti virus Products Detect Bots?', Staniford, S., 20 november 2008, http://blog.fireeye.com. Zie ook Retrospective/Proactive Test, AV-Comparatives.org, May 2011, www.av-comparatives.org .

[5] Mandiant 2014 Threat report "Beyond the Breach"

[6] Zie Cyber Security Perspectives 2013.

[7] "Before We Knew It - An Empirical Study of Zero-Day Attacks In The Real World" L. Bilge e.a., 2012

[8] Mandiant 2014 Threat Report "Beyond the Breach"

[9] CISSP Exam Guide, Sixth Edition, Shon Harris