

*Selecteren van beveiligingsmaatregelen vaart wel bij pragmatische aanpak*

## Wanneer is het veilig genoeg?

Van tijd tot tijd duikt de vraag op welke (informatie)beveiligingsmaatregelen genomen moeten worden om 'voldoende' beveiligd te zijn. Veelal gaat de vraag vergezeld van enige hoopvolle non-verbale communicatie die duidelijk maakt dat een 'kant-en-klare' oplossing erg gewenst zou zijn. Helaas luidt dan het enigszins onbevredigende antwoord: "Dat hangt ervan af ...".

Jeroen van Dongen gaat in op het selecteren van beveiligingsmaatregelen en legt daarbij de relatie tussen maatregelen, afgedekt risico en haalbaarheid.

**Jeroen van Dongen**

Wat voldoende beveiliging is voor de een, is ontoereikend voor de ander, en te veel voor een derde. Een 'one-size fits all'-t-shirt past bij nader inzien eigenlijk zelden. Situaties verschillen, de te nemen maatregelen dus ook. Daarom moet voor de selectie van beveiligingsmaatregelen gekeken worden naar de aanwezige risico's. Op dit punt valt dan vaak de term *risicoanalyse*. En twee tellen later haakt een deel van het publiek af. Immers: risicoanalyse is voor velen synoniem aan moeilijk en kostbaar. Als alternatief wordt dan al vaak gegrepen naar termen als *best practices* en *baselines*.

Maar hoe komt zo'n baseline tot stand? Wat moet daarin staan? En voor wie zijn die best practices nu eigenlijk het best? Neem bijvoorbeeld iets als de Code voor Informatiebeveiliging. Erg nuttig, zo'n verzameling best practices en richtlijnen, maar niet alle richtlijnen zijn voor iedere organisatie in even grote mate van toepassing. En ook de wijze van implementatie kan een enorm verschil uitmaken in het uiteindelijke resultaat. Zelfs als in een bepaalde branche normen zijn voorgeschreven, blijft het toch vaak nodig keuzes te maken.

### **Maatregelen, risico's en kosten**

Maatregelen zijn uiteindelijk bedoeld om risico te verminderen. Risico wordt doorgaans beschreven als de kans dat een ongewenste gebeurtenis zich voordoet, vermenigvuldigd met de impact die de onwenselijke gebeurtenis heeft op het te beschermen object. Kortweg:  $\text{risico} = \text{kans} \times \text{effect}$ . Dat klinkt simpel, maar als je wat dieper nadenkt, zie je de

### **Standaarden en baselines**

- *Code voor Informatiebeveiliging* (verkrijgbaar via [www.nen.nl](http://www.nen.nl))
- ISO 27001, ISO 17799 (verkrijgbaar via [www.nen.nl](http://www.nen.nl))
- *Threats catalogue* en *Safeguard catalogue* van het Duitse BSI (<http://www.bsi.de/english/gshb/manual/download/safeguard-catalogue.pdf>, <http://www.bsi.de/english/gshb/manual/download/threat-catalogue.pdf>)
- *Standard of Good Practice* van het Information Security Forum ([http://www.isfsecuritystandard.com/index\\_ns.htm](http://www.isfsecuritystandard.com/index_ns.htm))

## Beveiliging inbedden

Beveiligingsmaatregelen zijn slechts een middel om het gestelde doel te bereiken. Dat doel is het voorkomen van schade aan de bedrijfsvoering en het waarborgen van de bedrijfscontinuïteit, met andere woorden: het verkleinen van risico's voor die bedrijfsvoering. Hiervoor is meer nodig dan alleen een set maatregelen; de beveiliging moet ingebed zijn in de organisatie. Een startpunt hiervoor is een beleid waarin bijvoorbeeld de visie van de organisatie ten aanzien van beveiliging, de globale aanpak en de diverse verantwoordelijkheden zijn vastgelegd. Beveiliging moet ook op de agenda van het management staan en met regelmaat onder de aandacht van de medewerkers worden gebracht. En zo is nog een aantal randvoorwaarden voor een solide (informatie)beveiligings-situatie te benoemen. Dit artikel gaat alleen in op het bepalen van de juiste mate van beveiliging.

problemen zó opdoemen. Hoe bepaal je bijvoorbeeld de kans dat iemand je systemen hackt? En moet je wellicht onderscheid maken naar verschillende aanvalsmethoden? En hoe druk je dat effect dan uit? Vragen te over. Voor je het weet, verdrink je in een zwembad vol details en verdwijnt de hoofdlijn uit het zicht. Wellicht hoeven we ook niet alle vragen te beantwoorden. Door op gestructureerde wijze hierover na te denken kan de hoeveelheid tijd en middelen die hiermee gemoeid is worden beperkt.

In dit artikel zal worden ingegaan op de selectie van beveiligingsmaatregelen. Daarbij staan twee doelen centraal: de kosten gemoeid met de maatregelen en de kosten verbonden aan de analyse moeten in verhouding staan tot het afgedekte risico.

### Selectie in drie stappen

Bij de methode voor maatregelenselectie in dit artikel wordt een maatregelset in drie stappen opgebouwd. De diepgang van de analyse die ten grondslag ligt aan de selectie wordt aangepast aan de aard

van de maatregelen en de noodzaak tot onderbouwing. Aan het begin van het traject wordt vooral geredeneerd vanuit de maatregelen; naarmate het traject vordert wordt steeds meer in termen van risico's geredeneerd. Er is voor deze opbouw gekozen omdat veel mensen eerder geneigd zijn aandacht te hebben voor de maatregelen (tegen dingen waar ze *nu* last van hebben) dan voor de risico's (die wellicht ooit manifest worden). Beginnen vanuit de maatregelen maakt de problematiek concreter en zorgt daardoor voor meer betrokkenheid. Naarmate het selectieproces vordert, ontkomt men er echter niet aan om te gaan kijken naar risico's.

### Stap 1: basismaatregelen

Allereerst wordt een set van algemeen geldende basismaatregelen opgesteld

– de *baseline*. In deze set zitten alleen maatregelen waarover binnen de organisatie en/of de beveiligingswereld een belangrijke mate van overeenstemming bestaat en die redelijkerwijs uitvoerbaar worden geacht. Deze set is van toepassing op alle informatiesystemen en de omgang met informatie in het algemeen. Er wordt nog niet echt gezocht naar een relatie tot de bedrijfsvoering (noodzaak); de maatregelen worden vooral geselecteerd op basis van hun technische relevantie en toepasbaarheid (nut) alsmede de acceptatiegraad. Deze baseline moet redelijk eenvoudig te implementeren zijn en een bepaald minimaal niveau van bescherming bieden.

De gedachte hierachter is dat het beter is om een beperkte set maatregelen deugdelijk geïmplementeerd (= effectief) te krijgen dan een zeer uitgebreide en zorgvuldig samengestelde set te implementeren, wat praktisch ondoenlijk is en waarbij men voortdurend vertraging blijft oplopen. Onder de bescherming van deze minimale dekmantel kunnen vervolgens ambitieuzere beveiligingsactiviteiten worden ontplooid.

Een goede manier om deze basisset vast te stellen is door in heel klein comité (een à twee personen) een bronlijst op te stellen met alle maatregelen die mogelijk in deze categorie zouden kunnen vallen. Hierbij kan onder andere geput worden uit de verschillende standaarden en baselines die in het gelijknamige kader worden opgesomd. Ten minste de volgende onderwerpen zouden onderdeel moeten zijn van de bronlijst:

- back-up van gegevens (ook op een andere locatie!) en het testen van restores;



# dossier security management

- basisnetwerkbeveiliging (patchen van systemen, afscherming van systemen, wachtwoordpolicy, antivirus- en antispammaatregelen, het regelmatig testen van deze zaken);
- omgaan met bezoekers;
- richtlijn voor het omgaan met informatie door medewerkers (inclusief een clausule die nader onderzoek toestaat bij een vermoeden van onregelmatigheden);
- regelmatige auditing, opvolging van de resultaten en rapporteren over deze zaken.

## Consensus bereiken

Uit deze lijst kan vervolgens in een of meerdere plenaire sessies met relevante personen (onder anderen vertegenwoordigers van IT, HR, OR, facilitaire zaken en de belangrijkste operationele bedrijfstakken) een baseline worden gedestilleerd. Ga alle maatregelen af, leg de maatregel uit, beschrijf het risico dat deze maatregel afdekt, geef aan wat de gevolgen van implementatie bij benadering zullen zijn en laat een korte discussie toe waarin nut, noodzaak en haalbaarheid aan de orde komt. Het kan ook zeer interessant zijn om te bespreken hoe het onderhavige punt momenteel geregeld is. Het is van groot belang dat de leider van de sessie goed thuis is in de materie – niet alleen in de techniek, maar ook de bedrijfseconomische kant van de zaak. Hij moet in staat zijn om het realiteitsgehalte van de sessie op peil te houden.

Als vervolgens in grote lijnen consensus is bereikt over nut en noodzaak van een maatregel, neem de maatregel dan op in de baseline. Alle maatregelen die op (grote) weerstand stuiten maar die door een deel van de groep wel als relevant worden ervaren, worden geparkeerd op een lijst voor nadere beoordeling. Tevens wordt genoteerd in welk gezelschap de knoop dan wel doorgemaakt kan worden. Maatregelen die door vrijwel de gehele groep als niet-relevant, te complex of te duur worden ervaren, worden inclusief motivatie opgenomen in een aparte lijst.

Deze worden niet geïmplementeerd, tenzij een formele risicoanalyse (als verderop besproken) de noodzaak hiertoe aantoont. Deze lijst kan later worden gebruikt voor naslag.

## *Ver kies na vaststelling van de baseline en de 'gezondverstand- maatregelen' implementatie boven analyse*

Na deze plenaire sessie(s) wordt de lijst met nader te beoordelen maatregelen in een aantal vervolggesprekken besproken. Het (wisselende) gezelschap waarin deze gesprekken plaatsvinden, kan in meer diepgang ingaan op de maatregelen, de afgedekte risico's en de kostenbatenanalyse. Sommige maatregelen komen wellicht alsnog in aanmerking om opgenomen te worden in de baseline. Andere zullen worden aangemerkt als specifiek van toepassing op een bepaald systeem, een bepaalde afdeling of een bepaald proces – een soort 'gezondverstandmaatregelen' - en weer andere zullen alsnog op de lijst van afgewezen maatregelen belanden.

## **Stap 2: implementeren**

Op dat moment beschikt de organisatie over een gedefinieerde set van zowel globale als specifieke maatregelen die, wanneer geïmplementeerd, een basisbeveiligingsniveau biedt. Nu ontstaat een tweesporetraject. In de eerste plaats moet begonnen (of verdergegaan) worden met het implementeren van de algemene maatregelen uit de baseline en de specifieke gezondverstandmaatregelen.

In de tweede plaats kan men starten met de risicoanalyse (deel 3).

## **Stap 3: formele analyse**

Nu kan een traject worden opgestart om door middel van een meer formele analyse te beoordelen of voor bepaalde organisatieonderdelen, processen of informatiesystemen nog aanvullende beveiligingsmaatregelen nodig zijn. Als er prioriteiten gesteld moeten worden, verkies dan - zeker in het eerste jaar na de vaststelling van de baseline en de gezondverstandmaatregelen - implementatie boven verdere analyse.

Het hoe en wat van een formele risicoanalyse zou onderwerp kunnen zijn van een apart artikel. De kern is echter:

- 1 het in kaart brengen van de te analyseren objecten (processen, systemen, afdelingen);
- 2 het ordenen van deze objecten naar relatief belang voor elkaar en voor de organisatie als geheel;
- 3 het in kaart brengen van de dreigingen waaraan deze objecten blootstaan en deze ordenen naar kans op voorkomen en mogelijke impact.

Door de resultaten van stap 2 en stap 3 te combineren ontstaat inzicht in de dreigingen die de meeste impact op de organisatie zullen hebben en die de grootste kans hebben om voor te komen. Op basis hiervan kan besloten worden om bepaalde extra maatregelen te nemen, of bewust niet te nemen en dus het risico te nemen.

Een laatste advies: vermijd te grote diepgang. Is het echt wel vast te stellen of iets eens in de tien jaar plaatsvindt of eens in de twintig jaar? En als dat al mogelijk is, maakt het wat uit, als die ene keer toevallig volgende maand is? Theorie kan ondersteuning bieden aan de praktijk, maar is niet zaligmakend. Kies het haalbare als doel, en werk van daaruit verder.

*Jeroen van Dongen (jeroen.van.dongen@lbvd.nl) is partner bij LBVD Informatiebeveiligers.*