INVENTARISATIE EN CLASSIFICATIE VAN STANDAARDEN VOOR CYBERSECURITY

Leesvervangende samenvatting bij het eindrapport

Auteurs:
Dr. B. Hulsebosch, CISSP
A. van Velzen, M.Sc.

20 mei 2015

In opdracht van:
Het Wetenschappelijk Onderzoek- en Documentatiecentrum van het Ministerie van Veiligheid en Justitie
Project nummer 2552

HET BELANG VAN STANDAARDEN VOOR CYBERSECURITY

De Nederlandse samenleving is voor haar functioneren afhankelijk geworden van ICT-systemen. Dit is het cyberdomein: de informationele infrastructuur van computersystemen en telecommunicatie-netwerken. Dit maakt kwetsbaar, dus is met de digitalisering ook cybersecurity in belang toegenomen. Cybersecurity is het voorkomen van schade door verstoring, uitval of misbruik van ICT, en indien er toch schade is ontstaan, het herstellen ervan.

Voor het treffen van cybersecurity-maatregelen bestaan vaak uitgeschreven normen, zodat iedereen deze op een optimale wijze kan invullen en niet opnieuw het wiel tracht uit te vinden. Dit zijn standaarden: generieke verzamelingen van voorschriften die een ideale uitvoering van bepaalde maatregelen weergeven. Dit kan de vorm hebben van best practices, richtlijnen, aanpakken, referentie-raamwerken, etc.

Het inzetten van cybersecurity-maatregelen volgens gestandaardiseerde normen is verstandig. Standaarden creëren efficiëntie van de beveiliging, faciliteren integratie en interoperabiliteit, maken het mogelijk om maatregelen onderling zinvol te vergelijken, reduceren complexiteit en bieden structuur voor het toepassen van nieuwe ontwikkelingen. Standaardisatie zorgt ervoor dat er veilig en betrouwbaar samengewerkt kan worden in het cyberdomein op basis van goed gedefinieerde kaders en afspraken.

Wereldwijd zijn er echter meer dan duizend van zulke standaarden voor cybersecurity, hoe door de bomen het bos te zien? Onderliggend onderzoek brengt overzicht in cybersecurity standaarden. De vraag die we ons hierbij stellen is; *Welke standaarden op het gebied van cybersecurity zijn er nationaal en internationaal beschikbaar en hoe kunnen deze standaarden ten opzichte van elkaar gepositioneerd worden?* De gehanteerde aanpak behelst een aantal fasen. Allereerst zijn beschikbare cybersecurity standaarden geïnventariseerd uit 25 bestaande overzichtsstudies. Vervolgens is een classificatieraamwerk ontwikkeld volgens welke de standaarden te vergelijken. Daarna is het raamwerk uitgebreid getoetst middels interviews en expertsessies. Het classificatieraamwerk is ook geoperationaliseerd tot een stappenplan voor het selecteren van standaarden voor implementatie. Ten slotte zijn de onderzoeksvragen beantwoord en de resultaten gefinaliseerd.

INVENTARISATIE

Om een goed beeld te krijgen van de meest voorkomende nationale en internationale standaarden voor cybersecurity is een inventarisatie gemaakt op basis van overzichtsstudies (25 stuks). Hieruit is een lijst van meer dan 180 standaarden opgesteld. De tien meest voorkomende standaarden zijn weergegeven in de tabel hieronder.

Titel	Bron	Herkomst	Taal	Aard	Vitale sector
ISO/IEC 27002	ISO/IEC	Internationaal	Engels	Standaard	Algemeen
ISO/IEC 27001	ISO/IEC	Internationaal	Engels	Standaard	Algemeen
NERC CIP 002 - 009	NERC	USA	Engels	Standaard	Energie
NIST SP-800 series	NIST	USA	Engels	Richtlijn	Algemeen
ISA/IEC 62443	ISA	USA	Engels	Framework	Industrie
AGA No. 12	AGA	USA	Engels	Best practices	Telecom
COBIT5	ISACA	Internationaal	Verschillend	Methode	Algemeen
ISO/IEC 15408	ISO/IEC	Internationaal	Engels	Standaard	Algemeen
API 1164	API	USA	Engels	Standaard	Energie
PCI-DSS	PCI	Internationaal	Verschillend	Standard	Finance

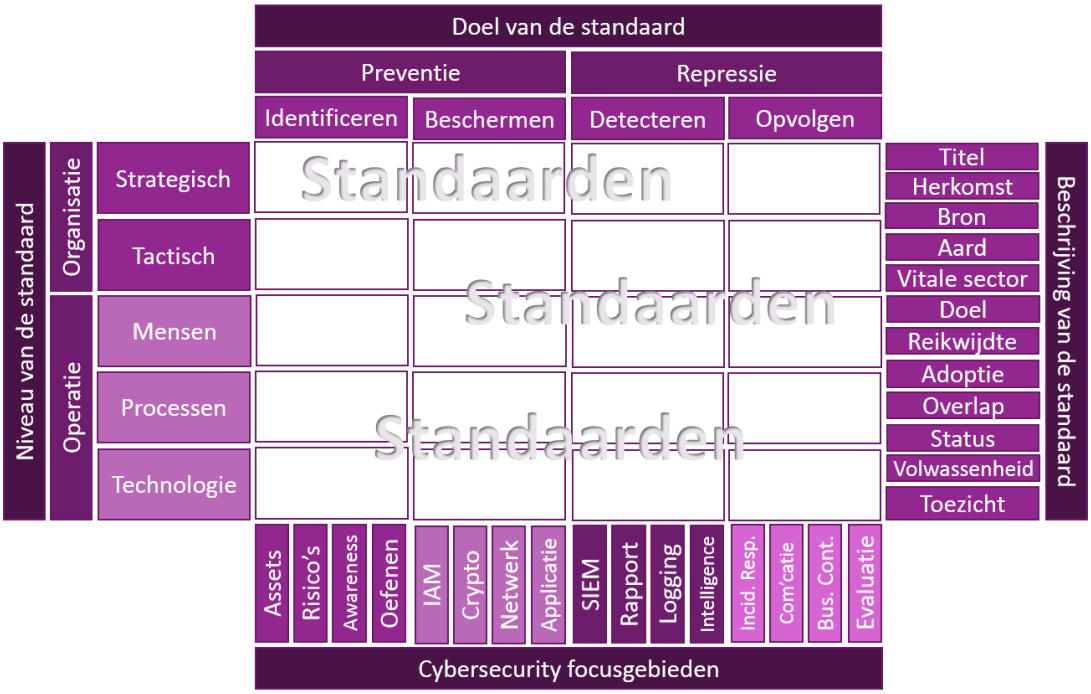
DOOR DE BOMEN HET BOS ZIEN: HET CLASSIFICATIERAAMWERK

Uit het grote aantal geïnventariseerde standaarden is af te leiden dat het cybersecurity domein complex en divers is. Dit maakt het bijvoorbeeld lastig om standaarden te kiezen of om te bepalen waar standaardisatie tekortschiet. Een classificatieraamwerk biedt ondersteuning om overzicht te krijgen en om standaarden ten opzichte van elkaar te kunnen positioneren.

Omdat een dergelijk classificatieraamwerk tot op heden niet bestond, is dit ontwikkeld als onderdeel van deze onderzoeksopdracht. Hiertoe is een aantal relevante classificerende dimensies geïdentificeerd. De eerste dimensie betreft verschillende variabelen die de standaard op een eenduidige manier beschrijven. Denk hierbij aan variabelen als herkomst, aard, adoptie, sector en beschikbaarheid van de standaard.

De tweede dimensie betreft de breedte van de standaard in termen van de beoogde doelen waarvoor een standaard maatregelen voorschrijft. Deze doelen zijn het voorkomen van incidenten, het treffen van maatregelen, het detecteren van ongewenste activiteiten en het beantwoorden van incidenten. Er zijn algemene standaarden die de hele breedte afdekken, zoals ISO 27001 en COBIT. Hiermee kan een baseline voor cybersecurity ingericht worden. Daarnaast zijn per doel verschillende specifieke focusgebieden te benoemen. Dit zijn gebieden waar specifieke cybersecurity-maatregelen benodigd zijn. Denk hierbij aan standaarden voor risico-assessment, identity en access management of business continuity. Er is geen standaardindeling van de focusgebieden; meestal worden ze bepaald door de gebruikte algemene standaard voor het inrichten van de cybersecurity baseline. De relevantie van de verschillende focusgebieden hangt af van het risicoprofiel van de organisatie en kan per vitaal domein verschillen.

De derde dimensie komt voort uit de organisatorische en operationele inbedding van standaarden in de organisatie en representeert de diepte (of specificiteit) van de standaard. Hiervoor zijn verschillende lagen te identificeren: besturing (strategisch), management (tactisch), mensen, processen en technologie (operationeel). Dit resulteert in het volgende classificatieraamwerk:



Figuur 1: Classificatiemodel voor cybersecurity standaarden.

CLASSIFICEREN VAN STANDAARDEN

Aan de hand van het classficatieraamwerk zijn alle geïnventariseerde standaarden voor cybersecurity te classificeren. De geïnventariseerde standaarden zijn dus grotendeels volledig geclassificeerd, voor zover de beschikbare informatie dit toeliet. Deze kunnen nu in het classificatieraamwerk op een gestructureerde manier worden gepositioneerd en vergeleken.

CONTEXT ALS KEUZEFACTOR

Het classificatieraamwerk staat niet op zichzelf en valt te plaatsen in een bepaalde context. Naast de reeds genoemde eigenschappen en inhoud van cybersecurity standaarden is deze context mede van invloed op de keuze voor een bepaalde standaard. De context bestaat uit invloeden van buitenaf (externe factoren) en vanuit de organisatie (interne factoren). Deze factoren zijn:

- Extern
  - Wet- en regelgeving;
  - Technologische ontwikkelingen en trends;
  - De netwerken en ketens waarin organisaties in toenemende mate opereren;
  - Maatschappelijke en individuele belangen;
  - IT-leveranciers en software ontwikkelaars;
  - Veranderende werkwijzen van cybercriminelen.
- Intern
  - Business drivers;
  - De menselijke factor;
  - De volwassenheid van de organisatie en de vitale sector op het gebied van cybersecurity;
  - De impact die de implementatie van een bepaalde standaard voor een organisatie kan hebben;
  - Onderlinge relaties tussen standaarden.

INZICHTEN: STATISTIEKEN EN VIEWPOINTS

Met het classificeren van de standaarden aan de hand van de dimensies van het classificatieraamwerk kunnen inzichten verkregen worden. Statistische informatie over cybersecurity-standaarden op basis van de variabelen uit het classificatieraamwerk geeft inzicht in bijvoorbeeld de beschikbaarheid of eigenschappen van standaarden. Door deze variabelen vervolgens te combineren, ontstaan meer gedetailleerde “viewpoints”. Het classificatieraamwerk geeft bijvoorbeeld een beeld van de gebruikte standaarden in een bepaald vitaal domein. Op basis hiervan kan worden bepaald voor welke doel- of focusgebieden standaardisatie van cybersecurity al dan niet voldoende geadopteerd of gerealiseerd is. Niet alleen voor professionals die voor hun organisatie op zoek zijn naar standaarden is dit relevant, maar bijvoorbeeld ook voor brancheorganisaties of toezichthouders. Naast dit domeinspecifieke viewpoint van het raamwerk zijn verschillende andere viewpoints uitgewerkt.

BESLISMODEL VOOR HET SELECTEREN VAN STANDAARDEN

Het classificatieraamwerk kan daarnaast worden ingezet als hulpmiddel voor het verkrijgen van beslissingsondersteunende informatie teneinde standaarden te selecteren voor te treffen maatregelen om geïdentificeerde risico’s te mitigeren. Hiervoor is een beslismodel ontwikkeld aan de hand waarvan een professional volgens een aantal stappen op een onderbouwde manier tot een keuze voor een standaard kan komen. Het startpunt is een risico- en dreigingsanalyse met behulp waarvan de professional stap voor stap wordt geleid naar één of meerdere posities in het classificatieraamwerk. Iedere positie levert een aantal standaarden en geclassificeerde informatie op. Op basis van deze informatie en de contextuele situatie kan de professional een standaard selecteren.

AANBEVELINGEN VOOR TOEKOMSTIG ONDERZOEK

Uit het onderzoek volgt een aantal aanbevelingen om de inventarisatie van de standaarden en het bijbehorende classificatieraamwerk verder te optimaliseren:

1. Het vergroten van de bruikbaarheid van het classificatieraamwerk door:
    - Het definiëren van een vaste set van focusgebieden voor cybersecurity op basis waarvan standaarden kunnen worden geclassificeerd.
    - De inventarisatie verder uit te breiden met standaarden voor de focusgebieden en hun classificering conform het raamwerk.
2. Het verkrijgen van inzicht in het daadwerkelijk gebruik van standaarden in vitale sectoren door het classificatieraamwerk per vitale sector in te vullen. Dit kan door middel van expertsessies of een enquête. Het stappenplan kan hierbij van nut zijn.
3. Het borgen van het onderhoud van het classificatieraamwerk en de onderliggende verzameling standaarden:
    - Door na te denken over de presentatie van het model; bijvoorbeeld als online tool.
    - Door na te denken over het beheer en onderhoud van de geclassificeerde standaarden.
4. Nader te onderzoeken wat precies de invloed is van de contextfactoren bij het selectieproces van standaarden:
    - Hoe beïnvloedt het volwassenheidsniveau van de organisatie of de sector de selectie van standaarden?
    - Hoe wordt de kwaliteit van standaarden bepaald? Wat zijn hiervoor de criteria?
5. Het vergaren van kennis over het daadwerkelijke gebruik van standaarden voor cybersecurity:
    - Wanneer is de implementatie van standaarden succesvol? Wat zijn hiervoor de criteria en kunnen die gemeten worden?

SLOTOPMERKING

Er kan nog veel vooruitgang worden geboekt als het aankomt op cybersecurity. Dit is onder andere de inzet van de Nationale Cybersecurity Strategie 2[1] en de cybersecurity agenda van de Europese Commissie[2]. Beveiliging tegen cyberrisico's zou in Nederland kunnen worden versterkt door optimaal gebruik te maken van beschikbare standaarden. De onderliggende inventarisatie van cybersecurity-standaarden en de classificatie ervan aan de hand van het opgestelde classificatieraamwerk kan daarbij van grote waarde zijn.

[1] Rijksoverheid (2013). Nationale Cybersecurity Strategie 2: van bewust naar bekwaam. Zie https://www.nctv.nl/Images/ncss-2-webversie-def_tcm126-519975.pdf.

[2] Europese Commissie (2015). European Union Digital Agenda: Cybersecurity. Zie https://ec.europa.eu/digital-agenda/en/cybersecurity.