Auteur: Renco Schoemaker is senior adviseur informatiebeveiliging & privacy en mede-eigenaar bij IB&P. Hij is werkzaam bij een G4 gemeente als senior information security officer en waar hij de ENSIA verantwoording coördineert. Eerder was hij adviseur en CISO (a.i.) bij diverse gemeenten. Renco is bereikbaar via r.schoemaker@ib-p.nl.

Het NIST CyberSecurity Framework als kans?

Het CyberSecurity Framework (CSF) is ontwikkeld door het NIST, ofwel het National Institute of Standards and Technology. Onder Obama werd in 2013 aan het NIST de opdracht gegeven een cybersecurity framework te ontwikkelen. En onlangs door Biden opnieuw. Maar wat kan je er als Nederlandse, overheidsorganisatie mee en hoe verhoudt het zich tot de BIO en de ISO27000 reeks?

Allereerst het verschil tussen een framework en een standaard. Een framework is een conceptuele structuur die inzicht geeft in hoe de onderlinge componenten zich tot elkaar verhouden. Vaak krijg je dit inzicht doordat een framework een visuele weergave bevat. Je kunt de vergelijking met de fysieke wereld maken: in de bouw houdt een framework het gebouw overeind doordat individuele componenten zich tot elkaar verhouden. Maar aan de hand van een framework kun je nog weinig zeggen over het eindresultaat. Frameworks vertellen je iets over de grote lijnen, de context en vooral: samenhang. Enkele voorbeelden van security gerelateerde frameworks: NIST CSF, COBIT en COSO.

Standaarden dienen een geheel ander doel, namelijk standaardisatie van best practices. In standaarden vind je dus concreet beheersmaatregelen waaraan je kunt of wilt voldoen. Vanzelfsprekend zijn deze logisch geordend in hoofdstukken, maar verder bevatten ze weinig context. Standaarden vertellen je iets over het wát, alhoewel het 'wat' nog uit te splitsen valt. Enerzijds gaat het over de feitelijk te nemen beveiligingsmaatregelen en anderzijds over het managementsysteem waarbinnen je deze beveiligingsmaatregelen neemt. Enkele voorbeelden van security standaarden voor beveiligingsmaatregelen: ISO270002/BIO, CIS Controls en NIST SP 800-53. Enkele voorbeelden van standaarden voor een managementsysteem: ISO27001 (ISMS), ISO27701 (PIMS) en meer voorbeelden zijn te vinden op de website van het ISO.

Standaarden zijn dus veel voorschrijvender dan frameworks en dat is tevens de reden dat je je wél kunt laten certificeren tegen enkele standaarden, maar niet tegen een framework. Bij overheidsorganisaties gaat het hoofdzakelijk over de BIO - ofwel ISO27002 - maar in toenemende mate ook over het ISMS (ISO27001). Wel is het ISMS lastig 'te pakken' voor velen. Maar je hoort bijna niemand over frameworks, waarom niet?

Kans of afleidingsmaneuver?

De cynicus (in mij) kan stellen dat een framework vooral de aandacht afleidt. Het is informatiebeveiliging in een ander verpakking die afleidt van achterblijvende implementatie van beveiligingsmaatregelen en/of een gebrekkig functionerend ISMS-proces. Van een framework wordt een organisatie niet veiliger, maar beveiligingsmaatregelen wél. Alhoewel in het slechtste geval niet onwaar, valt er meer over te zeggen. Informatiebeveiliging aanvliegen vanuit primair, of zelfs uitsluitend compliance is een 'dead end' wat mij betreft. Je schuift de BIO of ISO27002 nu eenmaal niet via de achterdeur naar binnen. Informatiebeveiliging aanvliegen vanuit primair, of zelfs uitsluitend risicomanagement wordt vooral een heel láng verhaal. En deels onzinnig ook: je hebt al een best practice qua maatregelen, maar gaat die toch steeds identificeren via tijdrovende risicoanalyses. Maar hoe dan wél?

Allereerst door de risicoanalyses zo gestructureerd en afgebakend te houden als mogelijk en qua maatregelen uitsluitend te putten uit wat er al is. Wat dat betreft is de Informatiebeveiligingsdienst (IBD) als CERT van de lokale overheden in Nederland je beste vriend; zij voorstaan mijns inziens deze werkwijze. Maar ook degene die deze werkwijze al jaren volgt heeft het niet makkelijk. Immers, hoe krijg je dat verrekte management en bestuur écht aangehaakt? Talloze beveiligingsincidenten en datalekken ten spijt, lukt het vaak niet. En dat moeten we vooral onszelf aanrekenen, meen ik.

En precies dáár biedt een framework een kans. Ik bezie het als het pragmatische midden tussen de lange, tijdrovende route van het managementsysteem en de kille, weinig tot de verbeelding sprekende route van compliance. Een framework biedt je de kans om op een geheel andere wijze het verhaal en belang van informatiebeveiliging over te brengen. Maar eerst iets meer over het NIST Cyber Security Framework.

CSF: core, tiers & profiles

Het CSF bestaat uit drie componenten: de core, tiers en profiles. Laten we starten bij het belangrijkste: de kern (core) van het framework. Die bestaat uit functies en (sub)categorieën. Er zijn vijf functies: Identify, Protect, Detect, Respons en Recover. Die termen moet je als lezer toch aardig kunnen plaatsen in de wereld van informatiebeveiliging. En niet onaardig: in de nieuwe, komende ISO27002 norm zal er ook een referentie terug zijn naar deze vijf CSF functies.

Afbeelding 1 – De vijf functies van het CSF.

Alle functies zijn onder te verdelen in categorieën: zo valt Identify uiteen in Asset Management, Business Evironment, Governance, Risk Assessment, Risk Management Strategy en Supply Chain Risk Management. Elk van deze categorieën bevat subcategorieën en daar wordt het redelijk concreet. Zo heeft de functie Identify (ID) de categorie Asset Management (AM) een subcategorie ID.AM-1 die als volgt luidt (vrij vertaald): Fysieke apparaten en systemen binnen de organisatie worden geïnventariseerd. Iedere subcategorie heeft referenties naar o.a. ISO27001, Bijlage A en via deze bijlage dus naar ISO27002/BIO. Het CSF bevat naast de 'core' ook nog 'implementation tiers'. Alhoewel er steeds wordt gesteld dat dit géén volwassenheidsniveaus zijn, bezie ik ze toch als zodanig. Om dit artikel 'on topic' te houden ga ik hier nu verder niet op in, evenmin op de profiles – wat toepassingen van het CSF zijn in specifieke sectoren.

Reframe het frame

Wat mij betreft kan het NIST CSF je helpen het 'grote verhaal' over informatiebeveiliging richting het (hoger) management en het bestuur opnieuw en beter te framen. Blijf weg uit de compliancehoek en mijd het lastige, ongrijpbare managementsysteem. Het CSF vervangt geenszins je managementsysteem of de BIO – deze standaarden zijn er niet voor niets – maar het framework helpt je dit alles beter uit te leggen. De vijf CSF functies vragen nauwelijks voorkennis en de eenvoud van volwassenheidsniveaus spreekt doorgaans aan. Dus het NIST CSF is wat mij betreft zeker een kans. Maar je zal je wel goed moeten inlezen om alle ingrediënten van het verhaal overtuigend te kunnen brengen. Ik hoop dat dit artikel daar positief aan heeft bijgedragen. IB&P heeft ruime ervaring met het implementeren van standaarden, managementsystemen en frameworks op het gebied van informatiebeveiliging en privacy, specifiek bij overheidsorganisaties.