Auteur: Lilian Knippenberg is senior information security officer en schrijft op persoonlijke titel. Ze is te bereiken via LinkedIn.

Ode aan de context

De context en omgeving van de organisatie waar je werkt zijn erg belangrijk. Niet alleen voor het type gegevens, maar ook omdat de mensen die er werken, de doelen die de organisatie nastreeft en de wensen van de directie allemaal specifiek voor die organisatie zijn. Hierbij een ode aan de context als startpunt, plus manieren om dit praktisch toepasbaar te maken.

Voordat ik een tweetal best practices bespreek, nodig ik je uit om even stil te staan bij wat jouw organisatie voor jou betekent. Waarom werk je waar je werkt? Wellicht heb je gekozen voor een bepaalde branche, zoals de gezondheidszorg of de overheid, of kies je voor IT-dienstverlening, een internationaal opererende organisatie of advocatenkantoor. Heb je specifiek gekozen voor deze werkgever? Waarom? Misschien sprak de filosofie of de culturele of religieuze achtergrond je aan. Misschien heb je zelf wel positieve ervaring bij de organisatie of was het zo simpel als nu eenmaal moeten werken voor je geld en maakt de context je niets uit. Ben je trots of blij met je werkgever? Zou je nog kunnen overstappen naar de directe concurrent of naastgelegen instelling? Die subtiele verschillen zijn belangrijk voor de cultuur van de organisatie en de mensen die er werken. En die verschillen maken de context! Sluit je met het informatiebeveiligingsprogramma daarbij aan, dan ben ik ervan overtuigd dat het programma meer succes heeft. Omdat jij voelt – en dus ook de medewerkers en andere stakeholders voelen – dat we informatieveiligheid samen nastreven voor hetzelfde doel.

De context in best practices: ISO en NIST

Goed, genoeg zachte overtuigingen, tijd voor de industry standards. Ik zoom in op ISO27001 en het NIST Cybersecurity Framework (CSF). Beide normen besteden aandacht aan de context van de organisatie. Ook deze normen kennen een context die interessant is om in het achterhoofd te houden. ISO is een onafhankelijke niet-overheidsinstantie waar 167 landen lid van zijn. Het instituut brengt de leden bij elkaar om middels consensus relevante standaarden voor de markt vast te stellen. De ISO-normeringen staan achter een betaalmuur. Vanuit Nederland is het NEN (Stichting Koninklijk Nederlands Normalisatie Instituut) lid van ISO. Het NIST CSF is gemaakt door het National Institute of Standards and Technology (NIST), dat onderdeel is van het U.S. Department of Commerce. De missie van het NIST is om Amerikaanse innovatie en industriële concurrentievermogen te stimuleren door het bevorderen van meetmethoden, standaarden en technologie op manieren die de economische zekerheid vergroten en onze kwaliteit van leven verbeteren. Het NIST CSF is verplicht gesteld in de Verenigde Staten voor alle federale overheidsinstellingen in het land en is gratis beschikbaar. Beide kaders hebben dus een andere insteek, die je terugziet in het concreet maken van de business context.

1. ISO 27001: Context of the organization

De ISO27001:2017 heeft de context beschreven in hoofdstuk 4. De context wordt als volgt concreet gemaakt:

- Understanding the organization and its context;
- Understanding the needs and expectations of interested parties;
- Determining the scope of the information security management system.

Hierin is ook direct de volgorde duidelijk: start met de organisatie zelf en haar omgeving, kijk daarna naar belanghebbenden en tot slot naar de omvang van het Information Management System (ISMS).

2. NIST Cybersecurity Framework: Business Environment

Naast de ISO 27001 wordt het CSF van het NIST steeds populairder om te gebruiken als standaard. Ook hier vind je de context terug: binnen de functie Identify (ID) staat de categorie Business Environment (BE) als tweede. Het doel van Identify.Business Environment (ID.BE) is: The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. En ook in het NIST CSF is dat verder uitgesplitst in subcategorieën:

- ID.BE-1: The organization's role in the supply chain is identified and communicated;
- ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated;
- ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated;
- ID.BE-4: Dependencies and critical functions for delivery of critical services are established;
- ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations).

Het NIST CSF geeft redelijk praktische invulling. Denk weer even terug aan de context van de norm: verplicht voor de Amerikaanse federale overheden. De vraag is natuurlijk hoe deze context passend te maken is voor ons in Nederland. Die vraag is aan eenieder om zelf voor jouw organisatie te beantwoorden. De invulling van ID.BE is in elk geval een stuk concreter en specifieker dan in de ISO27001. Het gaat hier om de keten, infrastructuur, missie, afhankelijkheden en weerbaarheid van de organisatie.

Overzicht geeft inzicht: geschreven en ongeschreven regels

Zowel de zachte als de hardere kanten van de context zijn van belang. De normen vragen vooral om overzicht over de meetbare en concrete punten, die ik de geschreven regels noem. Dat gaat onder meer over wetgeving, branchenormen, gedragscodes. De ongeschreven regels gaan over de belanghebbenden, de (onuitgesproken) verwachtingen, de concurrentie en ongrijpbare dingen als de historie en de toekomst. Als je op beide punten overzicht hebt, zorgt dat voor inzicht. Zorg er dus eerst voor dat je overzicht hebt door op te schrijven wat je weet. Maak een documentje aan en ga schrijven. Eerst voor de gehele organisatie, daarna per business unit, daarna per afdeling. Juist die specificering is belangrijk, want dan gaan mensen het voelen. Dat is dan weer basis voor risicomanagement en informatieveilig gedrag.

Hieronder mijn checklist, gebaseerd op ISO, CSF en eigen ervaring.

De geschreven regels

- Wat is de rol van de organisatie in Nederland? En in de wereld?
- Wat is de missie en visie (waarom bestaat deze organisatie/business unit/afdeling)?
- Wat levert de organisatie?
- In welke branche acteert de organisatie?
- Welke rol heeft de organisatie in de keten? Wat komt ervoor of erna vanuit het perspectief van de klant/cliënt? Met andere woorden: welke afhankelijkheden zijn er?
- Welke wetgeving, normen en gedragsregels zijn van toepassing?
- Welke eisen zijn er aan continuïteit?

De ongeschreven regels

- Welke stakeholders zijn er?
- Met awareness (de doelgroep) in het achterhoofd: welke functies hebben medewerkers?
- Zijn er leveranciers belangrijker dan andere?
- Wie zijn de vaste contactpersonen? Welke (formele) functie hebben zij?
- Welke reguliere overlegstructuren zijn er?
- Welke primaire processen zijn cruciaal?
- Welke vragen aan de ISO zijn als laatst gesteld? Of welke worden het meest gesteld?
- Welke vragen aan IT zijn als laatst gesteld? Of welke worden het meest gesteld?
- Wat waren de laatste incidenten en/of events?

Met overzicht over bovenstaande onderwerpen krijg je inzicht in de patronen en factoren die de context van jouw organisatie maken. Met deze context kun je vorm gaan geven aan je communicatie over informatieveiligheid en je invulling van het informatieveiligheidsprogramma/roadmap.

Communicatie met de stakeholders

Nu we de omgeving en de patronen van de organisatie in de basis helder hebben, kunnen we aan de slag met communicatie. Niet meteen een heel communicatieplan, dat komt bij de specifieke onderwerpen in het programma. Als onderdeel van de context ben ik op zoek naar verwachtingen, vragen en antwoorden. In de ongeschreven regels zit al een deel van de vragen die aan informatieveiligheid en IT gesteld worden. Hoe wordt daarop antwoord gegeven? Is de toon van communicatie zakelijk of juist persoonlijk? Door dit onderwerp specifiek te bekijken, kom je te weten hoe de organisatie impliciet functioneert. Ga dat ook na bij de afdeling communicatie (en marketing). Zij kunnen je helpen. Door de communicatie af te stemmen op de verschillende doelgroepen, sluit je goed aan bij de verwachtingen die zij hebben en word je een voorspelbare partner. Dat is natuurlijk een beetje kort door de bocht, maar de toon van de antwoorden én je vragen aanpassen aan de stakeholder helpt zeker. Ook een goede vraag die expliciet terugkomt in de ISO27001 is wat de stakeholders van jou nodig hebben. Ook daarop kun je aansluiten in de manier waarop je communiceert.

Tot slot: met de context geef je je programma vorm

Met inzicht in alle omgevingsfactoren kun je jouw informatiebeveiligingsprogramma vormgeven. Wat mij betreft geeft het NIST hier de duidelijkste richting aan door middel van Special publication 800-53. Hierin worden de Security and Privacy Controls for Information Systems and Organizations beschreven. In de familie Planning wordt invulling gegeven aan de controls die je nodig hebt om je informatieveiligheidsplan of programma vorm te geven. Dit zijn:

- Policy & procedures
- System security & privacy plans
- Rules of behavior
- Concept of operations
- Security and privacy architectures
- Central management
- Baseline selection
- Baseline tailoring

Door de context als eerste mee te wegen, ontstaan op deze cruciale onderwerpen de maatregelen en het plan dat bij jouw organisatie het best past. Neem de punten mee waar jouw organisatie iets aan heeft en vergeet de rest. Deze ode aan de context is dus met name een oproep om niet direct de maatregelen in te duiken, maar eerst aandacht te geven aan de omgeving. Zo maken we met het hele vakgebied de stap van beveiliging naar veiligheid en weerbaarheid!