



In deze blogreeks neem ik je mee op reis om de wereld rondom informatiebeveiliging te bekijken vanuit mijn ogen. Naast audit zijn deze ogen ook getraind te kijken vanuit persoonlijke ontwikkeling en communicatie.

BLOGREEKS DEEL 1

Anders kijken... naar informatiebeveiliging

Nationale veiligheidsdiensten lijken in hun werk bij het maken van dreigingsanalyses op security-afdelingen. Uit hun praktijkervaring kunnen securityprofessionals daarom nuttige zaken leren.

Het begint namelijk niet bij de techniek maar bij de bovenkant van de organisatie: de directie, Raad van Bestuur (RvB) of board. Zij staan bovenaan en voeren de leiding over de betreffende organisatie. Deze 'tone at the top' of 'demonstrate leadership' is ontzettend belangrijk. Maar hoe kan leiderschap getoond worden voor informatiebeveiliging? Heel simpel: als informatiebeveiliging door hen niet belangrijk gevonden wordt, krijgt het ook geen aandacht en gaat het niet gebeuren! Informatiebeveiliging begint met het maken van keu-

zes. Deze keuzes zullen vervolgens verankerd moeten worden in een strategisch beleid en er zullen rollen en (eind)verantwoordelijkheden moeten worden toegekend. De board moet dat regelen, of ervoor zorgen dat er mensen zijn die dat voor hen gaan regelen. Bij kleinere organisaties zal de directie zelf een actievere betrokkenheid hebben. En wanneer de organisatie groter wordt, moeten zij zorgen voor de juiste governance, het besturen. Daarbij moet een framework voor de beheersing juist ingericht worden, zodat zij de juiste signalen krijgen op de juiste momenten.

Zij moeten in staat gesteld worden om de juiste keuze te maken, door ervoor te zorgen dat op het juiste moment de benodigde informatie aanwezig is. Dit kan weer leiden tot de juiste opvolging.

Leef je in

Wat vragen we dan concreet van de directie? Uitdragen van datgeen wat belangrijk gevonden wordt. Hoeveel focus op dikke omzet draaien en hoeveel focus op degelijke kwalitatieve bedrijfsvoering? Deze twee hoeven elkaar niet uit te sluiten, maar helaas is mijn ervaring dat dit vaak wel zo wordt gezien. Vervolgens is het van belang dat juist op dit strategische niveau een koppeling gelegd wordt naar de missie en visie van het bedrijf.

De why (1) moet vertaald worden naar het belang van het wel of niet hebben van bepaalde kwaliteitsstandaarden. En dit bedoel ik niet primair vanuit de wetten en regels, maar vanuit de intrinsieke motivatie. Waarbij het gaat om 'het goed doen', ook zonder dat daar een stok of een wortel tegenover staat. Daarna is het een kwestie van uitdagen 'hoe' dit dan gedaan kan worden. Wat is de exacte vraag aan de individuele medewerker? Door het zo toegepast mogelijk, op concrete werksituaties, te blijven communiceren zal na verloop van tijd een nieuwe manier van werken ontstaan. En sta open voor het commentaar en de opmerkingen die medewerkers geven. Het feit dat ze reageren betekent dat er een wens is tot betrokkenheid! Kijk wat er eventueel extra nodig is of geef, wanneer dat niet mogelijk is duidelijk uitleg over duidelijk uitleg over. "Probeer hen eerst te begrijpen voordat het jouw recht wordt om begrepen te worden. Leef je in de werksituatie van deze medewerkers in." Het bewust inrichten van een cultuur en vervolgens daarop blijven sturen, is één van de lastigste elementen die een organisatie kan proberen te beheersen. Dat is namelijk niet zomaar in een middag gedaan. Afhankelijk van de omvang van de organisatie, is dit een proces van één of enkele jaren. Uiteindelijk zal dit over de loop van maanden of jaren, afhankelijk van de grootte van de organisatie, leiden tot een cultuuromslag. Daarmee hebben we de nieuwe manier van werken gecreëerd. Ook het alloceren van voldoende mensen en middelen om gedaan te krijgen wat er moet gebeuren is belangrijk. We kunnen wel zeer goede informatiebeveiliging willen, maar als er maar

Voorbeeld van transparantie: Universiteit Maastricht

Een goed voorbeeld van deze transparantie is de Universiteit van Maastricht (3). Er is online een 47 pagina's tellende rapportage beschikbaar over de werkwijze en afhandeling van de ransomware die zij ruim een jaar geleden over hun organisatie heen kregen. Hierin staat ook beschreven hoe door het College van Bestuur de (risico)afweging gemaakt is over de keuze om wel of niet het losgeld te betalen. Aanvullend gaat het ook over de tekortkomingen en de daaropvolgende acties. Deze manier van handelen draagt enorm bij aan de algehele digitale weerbaarheid van Nederland.

anderhalve man en een paardenkop voor verantwoordelijk is, zal dit niet gaan werken.

Transparantie van gedrag

Tot slot wil ik het nog hebben over de transparantie van gedrag. Een aspect dat ook naar voren komt bij de acht basissoftcontrols (2). Hoe beter organisaties hun eigen handelen kunnen waarnemen, introspectie, inclusief het effect ervan, hoe beter ze in staat zijn om het eigen gedrag aan te passen aan de verwachtingen van anderen. Op bestuursniveau kan dit ook betekenen dat daar waar te kort geschoten wordt bijvoorbeeld in de informatiebeveiliging, dat ook hierover gesproken en/of gerapporteerd wordt. Er is openheid over geslaagde en niet-

geslaagde hackpogingen. Net als openheid over datalekken en risicoanalyses. Beseffen en communiceren dat het niet is zoals je wilt en daar actie op ondernemen. Door deze transparantie ontstaat ook een welwillendheid tot verbetering en tot groei.

Geen compromissen

De informatiebeveiliging mag nooit de beslisser zijn, maar zit in een controlerende en vervolgens adviserende rol. Wanneer de directie het advies onvoldoende opvolgt, kunnen we niets anders dan wijzen op de risico's en – voor ons het belangrijkste – CYA, Cover Your Ass. Mocht het zo uit de hand lopen en hard indruisen tegen je morele en ethische kompas, dan zal er verdere escalatie nodig zijn. In het ergste geval kan dit in de vorm van een officiële klokkenluidersrol. Maar laten wij het zover komen? Ik vind dat wij als informatiebeveiligers sneller moeten besluiten en eieren voor ons geld moeten kiezen wanneer een organisatie het niet al te nauw neemt met het volgen van de regels. Voor goede mensen is altijd plek. Ga staan voor wat jij belangrijk vindt. Geen compromissen. En ook dát is leiderschap... persoonlijk leiderschap.

Delen van dit artikel zijn overgenomen uit mijn boek.

Referenties

(1) Simon Sinek – Start with Why

(2) Muel Kaptein – Acht basis softcontrols

(3) <https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-lessons-learned>