INFORMATIEBEVEILIGING | *14 maart 2019*

'Informatiebeveiliging is geen feestje van IT alleen'

Leestijd van ongeveer 9 minuten 0 reacties

Ten overstaan van ruim 150 accountants, auditors en andere belangstellenden presenteerden NBA LIO en NOREA, de beroepsorganisatie van IT-auditors, begin dit jaar het vernieuwde volwassenheidsmodel informatiebeveiliging. Het onderwerp is hot. "Dit komt als een geschenk uit de hemel."

Ronald Bruins

NBA LIO kwam in 2016 al eens met een volwassenheidsmodel, maar dat kreeg nog maar weinig bekendheid. Ondertussen draaiden de raderen van informatiebeveiliging flink door. Cybersecurity kwam op. De kans om als organisatie gehackt te worden neemt hand over hand toe; het is niet de vraag of je wordt gehackt, maar wanneer.

Tijd voor een nieuw antwoord op zulke dreigingen. Want hoe kun je ervoor zorgen dat je organisatie klaar is om zijn informatie te beveiligen? Een antwoord daarop krijgen is welhaast de heilige graal. Dus zat de zaal begin februari bomvol, bij een rondetafelbijeenkomst van NBA LIO en NOREA waar het nieuwe volwassenheidsmodel werd gepresenteerd.

Registeraccountant en oud-president directeur van Schiphol Jos Nijhuis trapte af als dagvoorzitter. Nijhuis was tot voor kort ook co-voorzitter van de Cybersecurityraad, nationaal en onafhankelijk adviesorgaan van het kabinet. Daarvoor hield hij diverse boardroomgesprekken. "Ik merkte dat daarbij al snel de IT-directeur naar voren werd geschoven, maar ik ging er niet heen om met experts te praten, maar met ceo's. Hoe zit het daar met de *awareness*? Die ceo overlegt weer de details met de echte experts."

Nijhuis vindt dat accountants geëquipeerd moeten zijn om het gesprek, ook in het mkb, over cybersecurity aan te gaan. "Daarmee geef je invulling aan je maatschappelijke verantwoordelijkheid. Ik hoop dat het bij dit onderwerp niet zo vlak blijft als bij de opmerkingen over fraude in managementletters."

'Accountants moeten geëquipeerd zijn om het gesprek, ook in het mkb, over cybersecurity aan te gaan.'

Gereedschap

LAATSTE NIEUWS

NIEUWS | *Gisteren*
McKinsey: 'Waarde natuurlijk kapitaal kwantificeren essentieel voor bedrijven'

NIEUWS | *Gisteren*
Brussel in beroep tegen overwinning Apple en Ierland bij EU-hof

NIEUWS | *Gisteren*
ABN AMRO verwacht krimp bouwsector in 2021

NIEUWS | *Gisteren*
Omzet- en winststijging voor SRA-kantoren

NIEUWS | *Gisteren*
Controlekosten kleinere beursfondsen in vijf jaar ruim verdubbeld

Meer nieuws

Projectleider Jurgen Pertijs van de werkgroep Herziening Maturity Model Informatiebeveiliging gaf aan waarom het model tot stand kwam in 2016. "We gaven de auditor gereedschap in handen om het gesprek aan te gaan in de boardroom. Wat is de risicobereidheid van organisaties? Hoe weet ik dat mijn organisatie veilig genoeg is? Hoe is de governance geregeld? Op welke zaken kunnen we sturen, zodat het niet alleen een feestje is van de IT-directeur? Maar ook: hoe vergewis ik me ervan dat mijn leveranciers en ketenpartners hun beveiliging goed hebben geregeld?"

Ongeveer de helft van de aanwezigen kende de eerste versie van het model. Maar het gebruik van informatietechnologie is inmiddels zo vanzelfsprekend geworden en geïntegreerd in organisatie strategieën dat problemen met de beveiliging rechtstreeks van invloed zijn op de dagelijkse bedrijfsactiviteiten.. "Daarnaast wilden we de bekendheid vergroten van het model", aldus Pertijs. Zo onstond de link met NOREA. "Het zou namelijk eeuwig zonde zijn als slechts enkele mensen dit gereedschap in hun gereedschapskist hebben."

Volwassenheid op vijf niveaus

Het model schaalt de volwassenheid in informatiebeveiliging in op vijf niveaus. "Zat je in de eerste versie op niveau 4, dan kan dat anno 2019 niet meer het geval zijn als de informatiebeveiliging hetzelfde is gebleven. Je moet dus continu bijblijven", benadrukte Pertijs.

In de handreiking bij het volwassenheidsmodel staan diverse hulpmiddelen. Bijvoorbeeld om te benchmarken tussen onderdelen of met andere organisaties, om risicoanalyses uit te voeren of om de control objectives te bepalen. "Daarbij is het van belang welk beveiligingsniveau past bij de organisatie. De bakker om de hoek heeft een ander beveiligingsniveau nodig dan de bank." Ook zijn er in de handreiking *good practices* opgenomen. Wie werkt met de rapportages kan op vijftien deelgebieden in een oogopslag zien waar de organisatie staat. "Die rapportages zijn een 'praatplaat' richting de board. Ook om prioritering aan te brengen." Pertijs riep vervolgens de aanwezigen op met feedback in brede zin te komen, zodat het model periodiek herijkt kan worden.

Rijksbrede beoordeling

Tijdens de bijeenkomst kwamen ervaringen met het model aan bod, zoals van Edwin Hummel van de Auditdienst Rijk. Eén van de onderzoeken van die dienst wordt uitgevoerd in opdracht van het CIO-beraad en de Rijks-CIO en betreft een beoordeling van de informatiebeveiliging rijksbreed. Voordat het NBA-model werd gebruikt pakte de ADR vooral de Baseline Informatiebeveiliging Rijksoverheid (BIR) als uitgangspunt. Teams gingen aan de slag, kwamen centraal terug en vervolgens gingen de uitkomsten volgens Hummel "door een satéprikker". "Elk team keek op zijn eigen manier, waarbij je bij de combinatie van de resultaten ook tegen menselijke ruis aanliep. Deze methode van beoordelen hield ook geen rekening met specifieke aspecten van de departementen."

Nu werkt ADR met self assesments die de departementen invullen, waarna een klein team van zeven à acht leden bij de departementen langsgaat. "Een risicogerichte benadering. Het verzoek was ook vanuit het CIO-beraad om meer van elkaar te

leren. Het NBA-model was daarbij een geschenk uit de hemel", meende Hummel. "Dat model biedt de departementen eerst de kans om zelf hun evaluatie in te vullen. Per week konden we zo een departement oppakken. Aan het einde van die week lag er een mooie visuele plaat in Powerpoint. Die hielp ons om te kijken waar de leerpunten zitten van de departementen, ook in vergelijking met de buurman. Op een hoger abstractieniveau kun je kijken naar wat je nodig hebt en waar je wilt staan in informatiebeveiliging."

Als auditors of accountants het volwassenheidsmodel gebruiken moeten ze ook duidelijk maken dat een organisatie of een deel daarvan kan terugvallen. "Dat kan teleurstellend zijn. Vernieuwde inzichten kunnen namelijk tot een lagere score leiden. Er is dus een noodzaak om continu bij te blijven. Je ziet dat departementen de verbeterpunten oppakken om het volgend jaar nog beter te doen. Er zit een spelelement in."

'Je ziet dat departementen de verbeterpunten oppakken om het volgend jaar nog beter te doen.'

Een nadeel van het model is volgens Hummel dat niet elke activiteit leidt tot een hoger volwassenheidsniveau. "Je moet dus ook als auditor de context van de beoordeling schetsen." Eén van de aanwezigen wilde weten of het model ook te gebruiken is voor het in control-statement. "Formeel moet je bij het Rijk voldoen aan de BIR. Tegelijkertijd zie ik dat een aantal departementen de koppeling met dit model wel maakt."

DNB

Het beoordelingskader van De Nederlandsche Bank (DNB) voor de informatiebeveiliging van verzekeraars en pensioenfondsen omvat liefst 54 controls. Dat beoordelingskader, waar een minimumeis in zit, was één van de bronnen voor het volwassenheidsmodel van de NBA LIO en NOREA. "Ons kader is inmiddels breed geaccepteerd", stelde Derek Dijst van het expertisecentrum Operationele en IT-risico's van DNB. "Je ziet dat instellingen zelf elementen gebruiken om hun risk framework vorm te geven." Ervaring uit het toezicht leert dat instellingen nog te weinig rekening houden met uitbesteding. "Er is vaak wel een eerstelijns SLA-rapportage, maar dat is het dan. Instellingen moeten een beter beeld krijgen van wat is uitbesteed. Vooral om businesscontinuïteit te regelen en bijvoorbeeld samen testen uit te voeren op de systemen. Er is op dat gebied te weinig borging. Zorg dat de uitbesteding in de *grip* is."

DNB wil dat zijn beoordelingskader geen compliance-instrument wordt, maar "een taxonomie om richting te geven aan informatiebeveiliging. Let daarbij ook op cybersecurity, vaak een ondergeschoven kindje in de uitgewerkte risicoanalyses." Ook Dijst roemt het NBA-NOREA-model. "Je hebt hiermee een belangrijk en breed in te zeten instrument. Het laat het bestuur zien dat informatiebeveiliging geen feestje is van IT alleen, maar voor de hele organisatie."

Moeten we ons zorgen maken over financiële instellingen, wilde één van de aanwezigen weten. Dijst: "Er kan altijd een zwakte ontstaan in de keten. Dit onderwerp heeft blijvende aandacht nodig. Maar wees gerust: ook ik heb nog gewoon mijn geld op mijn rekening staan."

Betrek de werkvloer

Ton van Rhijn, director IT bij CZ Groep, pleitte als niet-auditor "in het hol van de leeuw" vooral voor belang van het betrekken van de werkvloer bij informatiebeveiliging. "Ik wilde op een sheet zetten dat het COBIT-model overbodig is, maar dat kwam niet door de keuring. Ik heb er dus maar van gemaakt dat COBIT een set winterbanden is." COBIT, de standaard voor controle over informatie en IT-gerelateerde risico's, helpt volgens Van Rhijn *an sich* niet om mensen in de organisatie uit te leggen wat er van ze verwacht wordt. "De teksten ervan zijn lastig, bijna juridisch." Een model is maar een model, meende hij, het gaat pas leven als gebruikers er daadwerkelijk wat mee doen.

'Een model is maar een model, het gaat pas leven als gebruikers er daadwerkelijk wat mee doen.'

Het belang van informatiebeveiliging bij CZ is levensgroot. Van Rhijn: "Als er persoonsgegevens op straat komen van verzekerden kan dat grote gevolgen hebben voor hun carrière." Volgens hem is er daarom binnen CZ "een diep bewustzijn" om voorzichtig te zijn met zulke data. "Of een datalek nooit kan gebeuren? Dat durf ik niet op die manier te zeggen, maar voor een zorgverzekeraar is een uitstekende reputatie onontbeerlijk. Ik vind het al met al dan ook het belangrijkste dat de boodschap van informatiebeveiliging landt. Ik kan het belang daarvan niet uitleggen aan de hand van 54 COBIT-controls. We hebben het model dan ook maar het model gelaten en zijn met de mens, met de werkvloer aan de slag gegaan." Om te zorgen dat het model gaat leven is CZ onder andere gaan werken met mystery guests en phishing mails.

Intrinsieke motivatie

Intrinsieke motivatie moet volgens Van Rhijn maken dat medewerkers als vanzelf voldoen aan COBIT, het DNB-beoordelingskader of het hernieuwde volwassenheidsmodel. "Niemand staat 's ochtends op met het idee 'ik ga lekker compliant zijn vandaag'. Het blijft een continue uitdaging informatiebeveiliging op het netvlies te houden bij medewerkers." CZ investeert daarnaast extra in security monitoring. "Zodat we sneller detecteren als een hacker aan onze spullen zit." Ook kijkt de verzekeraar kritisch naar uitbestedingen. "De grote uitbestedingen wat betreft IT hebben we wel in kaart, maar wat gebeurt er als een medewerker de company creditcard trekt? Die *shadow IT* wil ik ook op mijn lijstje hebben."

Jeroen Biekart, voorzitter van het NOREA-bestuur, Maureen Vermeij-de Vries, voorzitter van het bestuur van NBA LIO en dagvoorzitter Jos Nijhuis toonden zich blij met de uitkomsten van de bijeenkomst. "Als voormalige ceo spreekt het volwassenheidsmodel me aan", aldus Nijhuis. "Zeker omdat ik van benchmarking houd, maar ook van het neerzetten van je ambitie als organisatie. Waar moet je staan? Wellicht niveau vier of vijf? Wat kost dat dan? En wat kunnen we als raad van bestuur doen om op dat volwassenniveau te komen." Zijn advies aan de zaal: "Zorg dat de raad van bestuur met de ceo voorop het belang beseft, het ondersteunt en mede de kar gaat trekken."

- Ga naar het Volwassenheidsmodel Informatiebeveiliging

Reacties

Deel dit artikel

Ronald Bruins is journalist.

GERELATEERD

NIEUWS | *31 juli 2020*

NOREA-Handreiking Data Protection Impact Assessment (DPIA)

NOREA, de beroepsorganisatie van IT-Auditors, heeft een handreiking gepubliceerd voor het uitvoeren van een 'data protection impact assessment'. →

NIEUWS | *23 september 2019*

EY viert halve eeuw IT-audit in Nederland

EY meldt dat precies een halve eeuw geleden, op 23 september 1969, binnen het kantoor de Studiegroep Controle bij Automatische Informatieverwerking (SCAI) werd opgericht. →

NIEUWS | *18 september 2019*

NOREA publiceert nieuw privacy control framework

NOREA, de beroepsorganisatie van IT-auditors, heeft een nieuwe versie van het Privacy Control Framework (PCF) gepubliceerd. →

NIEUWS | *18 maart 2019*

VU start masterclass Digital Auditing

De Vrije Universiteit in Amsterdam heeft een nieuwe masterclass Digital Auditing ontwikkeld, gericht op ervaren accountants. →

NIEUWS | *12 maart 2019*

'Organisaties moeten meer oog hebben voor software asset management'

De meerderheid van de IT-auditors is van mening dat bedrijven niet genoeg aandacht schenken aan software asset management. Dat blijkt uit een recent onderzoek van... →

Aanmelden nieuwsbrief

Ontvang elke werkdag (maandag t/m vrijdag) de laatste nieuwsberichten, opinies en artikelen in uw mailbox.

Bent u NBA-lid? Dan kunt u zich ook aanmelden via uw ledenprofiel op MijnNBA.nl.

reCAPTCHA

Upgrade naar een ondersteunde browser om een reCAPTCHA-uitdaging te ontvangen.

Waarom gebeurt dit?

Privacy - Voorwaarden

Uw e-mail adres

Aanmelden

Accountant is een uitgave van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA).

NBA