INFORMATIEBEVEILIGING | *16 januari 2019*

NBA LIO en NOREA presenteren model informatiebeveiliging

Wat is in tijden van hackers, cloud computing, het internet of things en cyber security een volwassen informatiebeveiliging? Die hamvraag beantwoorden de Ledengroep Intern en Overheidsaccountants (LIO) van de NBA en NOREA, de beroepsorganisatie van IT-Auditors, samen met een handig model.

Ronald Bruins

Officieel heet dat model het 'Volwassenheidsmodel Informatiebeveiliging'. Er lag in mei 2016 al een eerste versie van. "We hadden het idee dat het door verschillende oorzaken in de la was beland", aldus Maureen Vermeij-De Vries. "Zonde, want een dergelijk volwassenheidsmodel is belangrijker dan ooit." Daar heeft de voorzitter van LIO een goed punt. Hackpogingen, DoS-aanvallen en andere verstoringen zijn aan de orde van de dag.

Onlangs nog kreeg het onderzoeksbureau GSR de gegevens van 87 miljoen Facebookgebruikers in handen. Recenter is het datalek bij hotelketen Marriott International. Daar belandden de gegevens van een half miljard hotelbezoekers op straat. NOREA-voorzitter Jeroen Biekart vat het zo samen: "Het is niet de vraag of je wordt gehackt, maar wanneer en wat je respons dan is."

IT geïntegreerd in strategie

Informatietechnologie is zodanig in bedrijfsstrategieën geïntegreerd dat bestuurders er niet meer omheen kunnen. "Problemen met de informatiebeveiliging zijn rechtstreeks van invloed op de dagelijkse bedrijfsactiviteiten", stelt Biekart. "Daarbij komt dat er meer en meer regelgeving en toezicht komt op informatiebeveiliging en de bescherming van persoonsgegevens. Denk aan de Algemene verordening persoonsgegevens."

> **'Het is niet de vraag of je wordt gehackt, maar wanneer en wat je respons dan is.'**

Alle reden dus om te komen met versie 2.0 van het volwassenheidsmodel dat LIO eerder in zijn eentje uitbracht. "De eerste versie was al grotendeels door internal auditors met een RE-achtergrond gemaakt. We hebben nu bewust de samenwerking gezocht met NOREA. Niet alleen om hun expertise op dit vlak, maar zeker ook om het volwassenheidsmodel breder te laten landen", aldus Vermeij-De Vries. "LIO bepaalde samen met de Kennisgroep Cybersecurity van NOREA de samenhang tussen het volwassenheidsmodel voor informatiebeveiliging en de Inherente Cyber Risicoanalyse (ICR) en Cyber Security Assessment (CSA) van NOREA. Auditors en bestuurders hebben zo met het nieuwe model de handvatten om samen het gesprek aan te gaan: hoe zetten we een volwassen informatiebeveiliging neer?"

Uitdaging daarbij is voor bestuurders hoe ze het probleem tackelen, zegt Vermeij-De Vries. "Hoe begin ik? Aan welke thema's en beheersmaatregelen moet ik denken?" Voor auditors geldt dat het soms lastig is om het gesprek met bestuurders hierover aan te gaan, beschouwt Biekart. "Met deze publicatie brengen we de twee partijen samen. Maar niet alleen hen. Je zou dit boek ook voor een bespreking met de raad van commissarissen, raad van toezicht of andere toezichthouders kunnen gebruiken." Het is de bedoeling dat organisaties op basis van de elementen van het model nagaan hoe ze ervoor staan en waar er verbeteringen mogelijk zijn.

Meer dan techniek alleen

Welke elementen maken de informatiebeveiliging volwassen? Wanneer is veilig veilig genoeg? Jurgen Pertijs, Manager Internal Audit bij verzekeraar CZ, projectcoördinator van de werkgroep en lid van NOREA: "Het volwassenheidsmodel beschrijft vele aandachtsgebieden. Van onder meer het bestuur, de organisatie en het risicobeheer tot aan het personeelsbeheer en het configuratiebeheer tot aan fysieke beveiliging, de computeroperatie, het bedrijfscontinuïteitbeheer en het beheer van de keten." Per aandachtsgebied volgt een beschrijving van het risico, het gewenste volwassenniveau en de beschrijving van de beheersmaatregel.

> **'Informatiebeveiliging moet doordringen en verankeren in processen en dagelijkse werkzaamheden.'**

Informatiebeveiliging gaat allang niet meer over de techniek alleen, stelt Biekart. "Daar moeten bestuurders zich van bewust zijn. Het gaat over informatie. Data verzamelen, verwerken en vastleggen. Dat doet iedere medewerker van een

organisatie elke dag. Techniek helpt om een basisniveau aan veiligheid af te dwingen, maar vervolgens moet informatiebeveiliging doordringen en verankeren in processen en dagelijkse werkzaamheden. Je moet het meenemen in je planning- en controlcyclus."

Voortschrijdend technologisch inzicht

Wat is er nieuw in het 2019-model, versus het model van 2016? "We hebben ons model, dat breder bruikbaar is dan alleen in de financiële sector, meer laten aansluiten op het raamwerk dat DNB voor financiële instellingen hanteert, waarin zij ook meer de nadruk legt op cyber security", zegt Pertijs van CZ. "Logisch, want we zijn tegenwoordig allemaal verbonden aan het internet. De risico's dat derden van buiten naar binnen komen, zijn daarmee veel groter geworden. Daarnaast hebben we aansluiting gezocht op de richtlijnen en normen van The National Institute of Standards and Technology en die van de Overheid. Al met al is het een flinke update geworden, waarmee ook de lat hoger komt te liggen. Als je als organisatie in 2016 maatregelen hebt getroffen waarmee je op niveau vier kwam, dan is een aantal van die maatregelen tegenwoordig slechts goed voor niveau drie. Dat komt door technologisch voortschrijdend inzicht. Alleen een username en wachtwoord zijn bijvoorbeeld allang niet meer genoeg."

Kroonjuwelen

Het model kijkt ook naar de inherente risico's die er zijn. Pertijs: "Een verzekeraar en een bank hebben een ander basisniveau nodig dan - bij wijze van spreken - een bouwonderneming of een winkelketen. Het risicoprofiel is per organisatie anders. In het model kun je precies zien waar voor jouw organisatie de lat zou moeten liggen." Volgens Biekart helpt het model om te bepalen wat de 'kroonjuwelen' aan informatie zijn en hoe ver organisaties moeten willen gaan om die te beveiligen. "Bij kroonjuwelen gaat het niet alleen om persoonsgegevens van je klanten, maar ook om receptuur of het ontwerp van een chipmachine."

Bijeenkomst over informatiebeveiliging

NOREA en NBA LIO organiseren samen op 4 februari 2019 een rondetafel bijeenkomst over informatiebeveiliging.

Doelgroep zijn bestuurders, auditors, accountants, maar ook commissarissen en toezichthouders.

De bijeenkomst wordt georganiseerd in samenwerking met DNB, CZ en de Auditdienst Rijk.

Tijdens de bijeenkomst wordt ook het Volwassenheidsmodel Informatiebeveiliging officieel gepresenteerd.

Inschrijven kan via de NBA-website.

Het model wordt vervolgens ook beschikbaar gesteld via de websites van de NBA en NOREA: www.nba.nl en www.norea.nl.

Tot slot: Als de werkgroep over een jaar bij elkaar komt, wat hoopt deze dan bereikt te hebben met het model? Vermeij-De Vries: "Dat het gebruikt wordt door toezichthouders, bestuurders, IT-auditors en accountants. Dat het ervaren wordt als een praktisch model en de uitkomsten inspireren tot het goede gesprek. Waarbij betrokkenen streven naar verbetering en bewuster met informatiebeveiliging omgaan." Biekart: "En dat we zo gezamenlijk Nederland een veiliger land hebben gemaakt."

Deel dit artikel

Ronald Bruins is journalist.

GERELATEERD

NIEUWS | *11 april 2022*

Weinig animo voor cybersecurity-audit bij rvc- en rvb-leden thuis

Commissarissen zijn het erover een dat digitalisering een belangrijk onderdeel moet zijn van de strategie van de organisatie. Een cybersecurity-audit bij commissarissen... →

NIEUWS | *18 maart 2022*

Schade door cyberaanval bij Crowe Foederer 'beperkt'

De cyberaanval op Crowe Foederer, waardoor het accountantskantoor dagenlang werd platgelegd, heeft maximaal één dag verlies aan data gekost. Sinds enkele dagen is... →

NIEUWS | *15 maart 2022*

Crowe Foederer getroffen door cyberaanval

Cybercriminelen leggen accountantskantoor Crowe Foederer sinds enkele dagen lam. Gijzelsoftware heeft de bestanden en computerprogramma's van het kantoor geblokkeerd.... →

NIEUWS | *16 februari 2022*

Agentschap Telecom versterkt toezicht op cyberveiligheid

Omdat er steeds meer dreiging van cyberaanvallen uitgaat, moeten aanbieders van netwerken alles in het werk stellen om hun netwerken veilig en betrouwbaar te houden. →

NIEUWS | *09 februari 2022*

PwC: Nederlandse bedrijven nog steeds kwetsbaar voor cyberaanvallen

Het Nederlandse bedrijfsleven is nog onvoldoende gewapend tegen cyberdreigingen, ondanks de explosieve toename van het aantal cyberaanvallen. →
