Verslag CISO-17 Esmeralda-lezing

Cybersecurity op de bestuurlijke agenda

In de Esmeralda-lezing die dit jaar plaatsvond op 7 juni in het Koetshuis van Kasteel de Haar keek Aart Jochem terug op zijn ervaringen als CISO bij Capgemini, GovCert en PGGM.

Bart van Staveren opent de bijeenkomst in de fraaie ambiance met een kort toelichting op de naam Esmeralda-lezing. Die is afgeleid van het sprookje van Jaap Fischer waarin Hans eist dat zijn vrouw een meisje moet zijn met prachtige kleren en goudblonde lokken, met ogen als meren die niet kunnen jokken, een mond als van honing en dan weer scherp als een mes, en hopelijk is haar vader koning en zij dan prinses. ***Maar*** Ze moet Liesje heten! En toen keek de prinses hem aan en zei: Ik heet Esmeralda, maar zeg maar Liesje. Deze versie van identiteit-toe-eigening was aanleiding tot de naamgeving van de Esmeralda-lezingen, waarin bijzondere buitenstaanders hun visie op ons werkveld geven.

Deze keer heeft de organisatie het idee aangepast en iemand uit eigen gelederen gevonden op zijn ervaring en visie met ons te delen: Aart Jochem behandelde de trendrapportage en factsheets van GovCert en stond uitgebreid stil bij de case Diginotar, medio 2011, die voor alle aanwezigen nog een bekend fenomeen was. Aart kon een mooi insite beeld schetsen van de ontwikkelingen die in de eerste dagen van de Diginotar-crisis plaatsvonden en welke acties er waren ondernomen. Aart benadrukte dat het succes van de afhandeling lag en ligt in herkenbaarheid en bereikbaarheid. Door het goed opgebouwde netwerk kon er snel geschakeld worden en door het snel inrichten van een centraal centrum is in de bereikbaarheid voor alle relevante actiehouders voorzien.

Aart vindt het teleurstellend dat bij de overgang van GovCert (Computer Emergency Response Team voor de Rijksoverheid) tot Nationaal Cyber Security Centrum (NCSC) in 2012, geen Nationaal Centrum is ingericht, maar nog NCSC nog steeds beperkt blijft tot de Rijksoverheid en Vitale functies.

Aart besprak dat cases als de aanval op KPN en de DDos aanvallen op de banken in 2013 alsmede de actie van Benno de Winter om een tijd lang iedere dag een lek te bespreken ertoe hebben bijgedragen dat een aantal bedrijven nu over CERT/CISO-teams beschikken.

Vanuit zijn ervaring ziet hij belangrijke ontwikkelingen:

Samenwerking

Aart benadrukte vooral de rol van samenwerking. Er zijn nu veel CERT's. Het gebruik van dezelfde tools stelt organisaties in staat snel met elkaar te schakelen en gezamenlijke acties op te pakken.
Bij PGGM heeft Aart een CERT ingericht en daarmee verbinding gelegd met de ketenpartners. Bij PGGM zitten de CERT en kwaliteitsmanagement met succes bij elkaar, dit levert een goede kruisbestuiving.
Het treft hem dat bij veel besturen/organisaties er slechts een paar personen zijn, die beseffen dat een kleine fout op beveiligingsgebied kritiek kan uitpakken voor de organisatie.

Professionalisering

Criminele worden steeds professioneler. Dat brengt de noodzaak mee dat ook van onze kant continue aan de professionaliteit gewerkt moet worden.
Een van die aspecten is dat criminelen meer tijd nemen om rustig kennis van de business op te doen om daarna heel gericht toe te slaan. De tijd van Hit en Run is voorbij.
Dat brengt de noodzaak mee om vroegtijdig aanvallen te detecteren. Continue monitoring/logging en opmerken van abnormaal gedrag.
Van belang is het inrichten van eigen CERT die niet alleen moet focussen op eigen organisatie maar breed moet kijken naar ontwikkelingen en ook de omgeving moet betrekken, met name de ketenpartners.
Tot slot is het belangrijk te kijken naar de nieuwe instroom van problemen, die de noodzaak meebrengt medewerkers met een frisse kijk, kennis en ervaring aan te trekken: nerds en hackers

Veilige producten

Volgens Aart is er een grote urgentie om te kijken naar en het ontwikkelen van veilige producten. Hij besprak o.a. IP-scans, MongoDb en Agile werken. Je hebt geen tijd meer om in alle rust ene watervaltraject te doorlopen. Het wordt ook steeds moeilijker alle in en outs te kennen. De inrichting van zgn devil teams is dan ook een goede richting.

Raad van Bestuur

Aart komt tot de conclusie dat van de RvB een andere kijk, een ander geluid vereist wordt.
De rol van een bestuurder zal in Belbin termen van vormer/voorzitter naar zorgdrager moeten verschuiven.
Besturen hebben ook zelf geleerd: door zelfassessments, incidenten en wetgeving
De samenleving verwacht tegenwoordig veel van bedrijven. Daardoor komt het besef dat de data het kapitaal van de organisatie vormt en continue innovatie in ICT essentieel is.

Vanwege de samenhang wordt de rol van ketens het steeds belangrijker, maar ook moeilijker. De RvB moet dus weten wie de strategische partners zijn en die beoordelen op hun interne beheersing, met name de leveranciers zowel nieuwe als de bestaande.

Daarbij is de CISO adviserend, onafhankelijk, en dient een directe lijn naar RvB te hebben.

Afsluitend ziet Aart de noodzaak dat bestuurders hetzelfde traject doorlopen als PvIB afgelopen 10 jaar hebben doorgemaakt. En bestuurders moeten beseffen dat een substantieel deel van de innovaties, bv 10% maar dat is geen hard getal, aan IT-security nodig is en vanaf het begin meegenomen moet worden. Security by Design begint bij het bestuur. Het wordt essentieel dat besturen een intuïtie ontwikkelen voor (de risico's van) nieuwe ontwikkelingen.

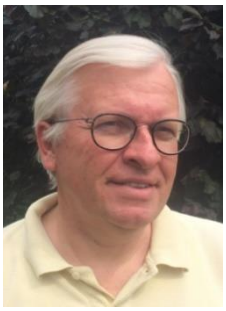
Vragen

De laatste vraag van Bart was wat Aart afgelopen 10 jaar aan NOREA heeft gehad. Aart gaf aan dat hij veel gehad heeft aan (de regelmatige ontmoetingen met) collega's en ook van de vertegenwoordiging door NOREA/PvIB van het vakgebied in de media.

Tot slot adviseerde Aart om zelf (alsnog) een programmeertaal te leren, bv C, Java, Jason of iets over APi's om beter te begrijpen hoe bedreigingen kunnen ontstaan.

Aart Jochem is Corporate Information Security Officer bij PGGM, de pensioenuitvoerder voor onder meer het pensioenfonds voor Zorg en Welzijn. Hij heeft een achtergrond in elektrotechniek en computerarchitectuur en heeft voor zowel publieke als private organisaties gewerkt voordat hij in december 2016 de overstap maakte naar PGGM. Als een van de grondleggers van het Nationaal Cyber Security Centrum in Nederland en daar verantwoordelijk voor monitoring en respons heeft hij bijgedragen aan de ontwikkeling van cyber security in Nederland en Europa en van dichtbij ervaren hoe incidenten impact hebben op organisaties. Aart is sinds 2006 actief lid van het GvIB/PvIB.

Het verslag is geschreven door Geert Martens



Geert Martens was sr ICT/OA auditor en sr proces en financieel controller bij UWV. Sedert februari 2017 is hij met pensioen, maar nog geïnteresseerd in issues tav Governance, (risico)beheersing en kwaliteitszorg. Hij is bereikbaar via gjm.martens@hccnet.nl en linkedin.