Vijf vragen aan

Joep Janssen

25 juli 2018

1. Wie is Joep Janssen en welke expertise heb je?

Ik ben 62 jaar en woon samen met Loes op een mooi klein boerderijtje in het fraaie Land van Cuijk, pal aan de Maas en de Duitse grens.
Mijn favoriete hobby is skiën; 's winters in de sneeuw en de rest van het jaar op de kunstskibaan. Ik werk nu dertien jaar bij Verdonck, Klooster & Associates. VKA is actief op het grensvlak van organisatieontwikkeling en ICT. Mijn interesse ligt op het gebied van digitale dienstverlening aan burgers en bedrijven, met name door overheidsorganisaties, maar ook door particuliere organisaties. Naast IT-audits doe ik ook strategische ICT-opdrachten, zoals de inrichting en herinrichting van ketensamenwerking en ICT-regieorganisaties.

2. Waarom ben je actief geworden als voorzitter van de DigiD-Werkgroep?

Bij DigiD-assessments komen twee van mijn interessegebieden samen: overheidsdienstverlening aan burgers en bedrijven en digitale ketensamenwerking. De essentie van de DigiD-assessments is de beoordeling van de beveiliging van webapplicaties, die gebruik maken van de DigiD-authenticatie. Ik ben vanaf het begin lid van de werkgroep en ben door de eerste voorzitter Peter Verstege gevraagd het stokje over te nemen. Als voorzitter heb je de taak de afstemming tussen Norea en de voor DigiD verantwoordelijke overheidsorganisatie Logius in goede banen te leiden. Het helpt daarbij dat ik twintig jaar rijksambtenaar ben geweest en de Haagse mores zo'n beetje ken. Heel inspirerend is het om samen te werken met collega's uit het vakgebied. Het valt daarbij op dat je ons vak vanuit verschillende invalshoeken kan benaderen. De kunst is deze invalshoeken bij elkaar te brengen tot één werkbaar geheel, waarmee de IT-auditor in de praktijk uit de voeten kan.

3. Wat hoop je te bereiken met deze werkgroep?

Mijn centrale motto is: hoe maken we digitaal Nederland weer een beetje veiliger? Uitdagend vat ik ons vak wel eens samen met twee simpele opgaven:

1. Geen ongeautoriseerde toegang tot gegevens.
2. Geen ongeautoriseerde toegang tot programma's.

Vooral de samenhang tussen de steeds hogere eisen aan identificatie- en authenticatiediensten, zoals DigiD en eHerkenning, en het groeiende aantal diensten dat de overheid digitaal aanbiedt aan burgers en bedrijven, biedt iedere dag weer nieuwe opgaven.

Als werkgroep willen we graag een werkbare set aan normen aanreiken waarmee organisaties, die gebruik maken van DigiD, aantoonbaar hun beveiligingsmaatregelen op orde kunnen brengen. Steeds meer gaat het er daarbij om dat de organisaties zelf de nodige maatregelen treffen, deze monitoren en daar verslag over doen. De auditor komt langs en ziet dat alles op orde is. In de praktijk blijkt hier nog een weg te gaan. Vanzelfsprekend willen we niet alleen zien dat er mooie procedures zijn geschreven (opzet) en toegepast (bestaan), maar ook dat dit gedurende het gehele jaar heeft plaatsgevonden (de werking). Hier gaan we nu concrete voorstellen voor doen.

4. Wat moeten IT-auditors weten over beveiliging van webapplicaties om ook in de toekomst als RE relevant te blijven?

De webapplicatie is geen geïsoleerd onderzoeksobject, maar vervult een rol binnen de digitale dienstverlening van de organisatie. De webapplicatie is slechts één van de systemen die een organisatie in productie heeft. En steeds meer is een groot deel van de webapplicaties uitbesteed aan een serviceprovider.

Dit zijn de onderwerpen waar de RE zich op moet richten: kennis van de ontwikkelingen op het gebied van digitale dienstverlening en de procesketens die daarbij ingericht dienen te worden, van identificatie- en authenticatietechnieken, beveiligde koppelvlakken, firewalls, webapplicaties en *reversed proxies*, tot *Intrusion Detection and Prevention Systems* en de achterliggende servicebussen en zaaksystemen. Maar ook de wijze waarop afspraken gemaakt worden met serviceproviders over de dienstverlening en de wijze waarop daar controle op gehouden wordt, vraagt kennis van de RE.

5. Is de beveiliging van webapplicaties een specialisme of is het een van de aandachtspunten van een IT-auditor?

De specifieke kennis van de kwetsbaarheden en de beveiliging van webapplicaties wordt steeds meer een specialisme. De bedreigingen en aanvallen vanaf internet worden steeds geavanceerder. Alleen door geavanceerde analyse- en detectietechnieken zijn deze nog enigszins te herkennen en te beheersen. Dit kan de RE niet overlaten aan de penetratietester. Ook de RE zal kennis moeten hebben van technische beveiligingsonderzoeken. Dit is niet eenvoudig in één persoon te verenigen, dus moet de RE ook de vaardigheid hebben in teamverband met andere experts samen te werken en daar leiding aan te geven.

Drs. Joep Janssen RE MIM | Lead IT Auditor en Management Consultant bij *Verdonck, Klooster & Associates*

Joep Janssen is samenwonend in het Land van Cuijk