ISF World Congress 2007

Het Information Security Forum (ISF) is een internationale, onafhankelijke organisatie die samen met haar leden verschillende onderwerpen op het gebied van informatiebeveiliging onderzoekt. Het ISF telt meer dan driehonderd leden; dit zijn organisaties en bedrijven verspreid over de hele wereld en uit tal van sectoren zoals de financiële dienstverlening, telecommunicatie, energie en overheid.

Juriaan Rijnbeek

Drs. J.W. (Juriaan) Rijnbeek RE is als senior ICT auditor werkzaam bij Fortis Audit Services.

Een organisatie die lid is van het ISF heeft toegang tot artikelen, tools en best practices over informatiebeveiliging. Daarnaast zijn er op lokaal niveau diverse chapters waarin kennis en ervaring kan worden uitgewisseld, en kunnen leden deelnemen aan werk- en studiegroepen die zich richten op het samenstellen van nieuwe tools en best practices. Een andere manier voor de deelnemende organisaties om kennis en ervaring uit te wisselen is het jaarlijkse 'World Congress'. Afgelopen jaar vond van 9 tot 11 december het achttiende 'World Congress' van het ISF plaats in Kaapstad, Zuid Afrika. Het zou te ver gaan om hier een volledig overzicht te geven van drie dagen congres; in plaats daarvan volgt een korte impressie van deze bijeenkomst, waarop 500 deelnemers uit de internationale informatiebeveiligingsgemeenschap met elkaar van gedachten wisselden. Het congres was onderverdeeld in zeven plenaire 'mainroom' sessies en een totaal van bijna vijftig 'break-out' sessies. Twee thema's waren in deze sessies nadrukkelijk aanwezig: IT Governance en Cyber Security.

IT Governance

Na een spetterende muzikale opening, waarbij de aanwezige security professionals op Afrikaanse trommels konden meeslaan met de lokale drumband, mocht professor Mervyn King (o.a. voorzitter van het King Committee over corporate governance in Zuid-Afrika) als eerste spreker aantreden. Zijn presentatie betrof corporate en IT governance. Gezien het toegenomen belang van IT en de informatie die opgeslagen is in systemen, is het essentieel deze door middel van IT governance goed te beheersen. King betoogde, dat Informatiebeveiliging moet worden gezien als een belangrijk en integraal onderdeel van IT Governance. Volgens King is 'verdere wetgeving niet het middel om te komen tot goede IT governance. De markt moet worden gezien als de ultieme compliance officer.'
Stuart McIrvine (Director Corporate Security Strategy bij IBM) toonde drie invalshoeken om naar IT governance te kijken en deze te verbeteren. De eerste invalshoek is die van IT performance management, waarbij het Val IT framework kan helpen om IT performance management te verbeteren. De tweede invalshoek is die van security risk management, waarbij het ERM framework als raamwerk van pas kan komen. De laatste invalshoek is IT compliance management. Volgens McIrvine is volwassenheid van IT processen hiervoor essentieel. ITIL is een middel dat hierbij kan worden ingezet.

Cyber security

Een ander thema dat opviel in de diverse sessies was cyber security. Een van de sprekers die ingingen op dit onderwerp was Ira Winkler (Internet Security Advisors Group). De kern van zijn betoog was dat veel mensen weliswaar claimen voldoende kennis te hebben van informatiebeveiliging, maar dat uit de praktijk blijkt dat het tegendeel het geval is. Volgens Winkler 'weten veel mensen niet wat ze niet weten over informatiebeveiliging'. Hierdoor worden risico's niet altijd juist ingeschat. Belangrijk is om de juiste experts in te schakelen en een goede afweging te maken tussen risico's en kosten van maatregelen. Hierbij moet worden uitgegaan van de waarde van de informatie.
Mikko Hyppönen (Chief Research Officer F-Secure) toonde in zijn presentatie de toename van computercriminaliteit. Vroeger werden virussen geschreven door hobbyisten; tegenwoordig worden virussen, wormen, trojans, etc. geschreven door professionals en steeds meer gebruikt voor criminele activiteiten. Volgens Hyppö-

nen zullen virussen en dergelijke in de toekomst ook voor spionagedoeleinden worden gebruikt. Hij liet in zijn presentatie enkele sprekende voorbeelden zien, zoals het afpersen van mensen door te dreigen met een *denial of service attack* en de succesvolle zoektocht naar de schrijver van een worm. Ook liet hij zien hoe eenvoudig het is om aan credit card gegevens te komen en op welke wijze crimineel geld kan worden weggesluisd.

Break-out sessies

De bijna vijftig break-out sessies werden voor een belangrijk deel tegelijkertijd gehouden, waardoor er slechts zeven gevolgd konden worden. De keuze was hierdoor niet altijd eenvoudig. Twee sprekers vielen op. Bruce Schneier (BT Counterpane) is een bekend spreker en publicist van diverse boeken over beveiliging en cryptografie zoals bijvoorbeeld het welhaast monumentale standaardwerk 'Applied Cryptography'. Waar sommigen een technische presentatie verwachtten, ging zijn betoog juist over de psychologie van beveiliging. Met verschillende voorbeelden liet Schneier zien dat beslissingen die we nemen lang niet altijd rationeel zijn. Als het gaat om het inschatten van risico's, kansen en kosten blijken we soms meer te reageren op basis van ons 'instinct' en angst dan op feitelijkheden.
Na afloop van de presentatie ontving iedereen Schneier's boek 'Beyond fear – thinking sensibly about security in an uncertain world'. Dit boek gaat verder in op het thema van zijn presentatie en is zeker het lezen waard.
Geert Huyck (Fortis Audit Services) hield een presentatie getiteld 'Internet Banking – new threat landscape and protection measures'. In deze presentatie liet hij zien dat de Internetbedreigingen voor de bancaire wereld aan het veranderen zijn. Net zoals de main room speakers toonde hij aan dat er sprake is van een criminalisering van het Internet. Hij behandelde methoden die door criminelen kunnen worden gebruikt om Internetbankieren aan te vallen. Hierbij ging hij dieper in op 'phishing' en man-in-the-middle attacks. Daarnaast liet hij ook zien welke maatregelen getroffen kunnen worden om deze nieuwe bedreigingen het hoofd te bieden.

Tot slot

Al met al was het een geslaagd congres, waar naast de reguliere sessies een belangrijke plaats was weggelegd voor networking tussen security professionals. Het spreekt vanzelf dat de ambiance waarin het congres plaatsvond – in de schitterende omgeving van de Kaap in het zomerseizoen – de combinatie van het nuttige en het aangename heel goed mogelijk maakte. ■

Erasmus School of Accounting & Assurance

First Global Academic Conference on 'Internal Audit and Corporate Governance'

Deze conferentie wordt op 21 en 22 april georganiseerd op de Erasmus Universiteit te Rotterdam.
Via www.auditing.nl kunt u zich inschrijven. U vindt daar ook meer informatie over het programma. Op 22 april zal tevens aandacht worden besteed aan het 15-jarig bestaan van de opleiding I/OA.

ESAA: erkende onderwijsinstelling voor PE-punten

Inmiddels is ESAA ook door het NIVRA erkend als onderwijsinstelling en kunnen RA's (RO's, RE's en RC's) bij de opleidingen van ESAA officieel PE-punten halen in het kader van hun permanente educatie.

Uitwisseling Université Paris-Dauphine

In juni komen IT-Auditing studenten van de Université Paris-Dauphine naar Rotterdam voor een uitwisseling en training. Met de studenten IT-Auditing van de Erasmus Universiteit zal een dag worden besteed aan het gezamenlijk uitwerken van een audit case.

Buluitreiking

Met ingang van dit collegejaar vindt twee maal per jaar een buluitreiking plaats. Op donderdag 3 april staat de eerstvolgende buluitreiking op de agenda, gezamenlijk met de I/OA studenten.