



# Koos Ziere

**Ing. Koos Ziere RE CISA** is senior IT-auditor bij Berk IT Audit & Risk Management. Berk heeft een mantelovereenkomst met de EC voor het uitvoeren van financial- en informatiebeveiligingsaudits. De beschreven feiten geven een sfeerimpressie weer en betreffen een combinatie van ervaringen uit meerdere, vergelijkbare audits.

**‘Onze “taxi” blijkt één van de dienstauto’s van de ministers te zijn en over de bijbehorende privileges te beschikken’**

## **Zondagmiddag 12.00 uur**

Ik pak de laatste spullen in mijn koffer en doe nog even een check of ik wel voor alle dagen de juiste combinatie van kostuum, overhemd en stropdas bij me heb. Even later stop ik de koffer en mijn laptoptas achter in de auto en brengt mijn vrouw mij naar Schiphol voor mijn vlucht naar een van de lidstaten van de Europese Unie.

In het vliegtuig zie ik kans om het programma van de komende week door te nemen. In opdracht van de Europese Commissie moeten we de informatiebeveiliging van een betaalkantoor voor het Europees Landbouw Garantie Fonds en het Europees Landbouwfonds voor Plattelandsontwikkeling beoordelen. De betaalkantoren zijn volgens de Europese reglementen verplicht hun informatiebeveiliging in te richten op basis van CoBIT, ISO 27000 of de Duitse BSI-standaard en de EC heeft het recht om audits uit te voeren.

Rond acht uur land ik en neem een taxi naar het station voor het laatste deel van de reis. Even voor twaalfen check ik in het hotel in en vraag meteen bij de receptie na of mijn lokale collega van ons Baker Tilly International netwerk al is aangekomen. We hebben afgesproken dat we elkaar maandag om half acht bij het ontbijt zullen treffen, dus dat gaat wel goed komen.

## **Maandag 09.30 uur**

We beginnen de audit met een kick-off bijeenkomst. Deze beveiligingsaudit valt samen met een financial audit van de EC en we zijn dus met een omvangrijk gezelschap. Tijdens de bijeenkomst maken we kennis met de directeur en de belangrijkste medewerkers van het betaalkantoor. Bij deze audit maak ik voor de eerste keer de inzet van tolken mee. Het betekent dat ik mijn introductie in het Engels kan houden en de tolken zorgen voor een letterlijke vertaling. Bij andere audits was het

altijd de lokale collega, die de aftrap verzorgde in de landstaal.

Na de plenaire sessie scheiden de wegen van de IT-auditors en de financial auditors zich. Het betaalkantoor heeft voor ons de interviews met de diverse verantwoordelijken voor de informatiebeveiliging al ingepland en dus kunnen we snel van start. In de middag hebben we al een goede indruk van de werkwijze en weten we hoe het kantoor de Europese wetgeving uitvoert. Want, hoewel alle landen met dezelfde regelgeving te maken hebben, de werkwijze is iedere keer weer anders. Aan het einde van de middag evalueren mijn lokale collega en ik deze eerste dag. Voor de avond wacht ons het door nemen van de ter beschikking gestelde documentatie om het beveiligingsbeleid inhoudelijk te toetsen. Aangezien het betaalkantoor ervoor gekozen heeft om ISO 27000 te hanteren, nemen we ons ISO normenkader en beginnen alvast de bevindingen daarin vast te leggen.

## **Dinsdag 08.30 uur**

De tweede dag beginnen we weer met een interview. Nu is internal audit aan de beurt. Zij hebben een uitgebreid auditprogramma, waarin informatiebeveiliging periodiek aan een audit wordt onderworpen. Ook compliance is onderdeel van het auditprogramma en heeft dus expliciet de aandacht.

‘s Middags interviewen wij de beheerders van de applicaties voor de subsidieaanvragen. Zij leggen ons uit op welke manier het betaalkantoor aanvragen vastlegt, berekent en uitbetaalt met hun systemen. Wij stellen vast dat de diverse stappen in het proces telkens door een andere afdeling worden uitgevoerd en dat de functiescheiding daardoor in opzet al aanwezig is. Verder wordt er een fysiek dossier bijgehouden, waarin bij de overdracht van de ene naar de andere afdeling formeel voor overdracht en overname wordt gete-



kend. We vragen naar een actuele lijst met autorisaties en medewerkers en hun rollen. We letten vooral op de beveiliging rond het einde van het proces, de daadwerkelijke betalingen. Gezien de omvang van de bedragen is een adequate beveiliging hier een must.

Voor 's avonds worden we samen met de financial auditors uitgenodigd om met de medewerkers van het betaalkantoor te gaan eten in een lokaal specialiteiten restaurant. Even overweeg ik of hiermee de onafhankelijkheid niet in het gedrang komt, maar in overleg met de collega's komen we tot de conclusie dat we deze kleine geste als gastvrijheid moeten beschouwen en een weigering eerder als onbeleefd zal worden ervaren. Geen documentatie dus vanavond.

#### **Woensdag 08.30 uur**

Woensdag zijn we al bijna halverwege de audit. Vandaag staat de fysieke beveiliging op de agenda. Het is prachtig weer en dus wandelen we naar het gebouw

waarin zich de serverruimte bevindt. We stellen vast dat het met de toegangscontrole wel goed zit. Er wordt gebruik gemaakt van verschillende 'schillen' en toegang tot de serverruimte krijg je alleen met een persoonlijke pas en de bijbehorende pincode. In de serverruimte zien we dat deze op de begane grond een aantal ramen heeft met afmetingen van winkelruiten. De servers staan bijna letterlijk in de etalage! Het aggregaat voor de noodstroom staat fysiek onbeveiligd op het parkeerterrein achter het gebouw. Ook een punt voor verbetering dus, wat zeker terug zal komen in onze afsluitende presentatie op vrijdag.

#### **Donderdag 08.30 uur**

Donderdag krijgen we de bestanden met de actuele autorisaties en doen we daarop een analyse. In Excel zetten we de autorisaties in een draaitabel en beoordelen we of de rollen en de autorisaties de gewenste functiescheiding waarborgen. Het lijkt allemaal te kloppen, totdat we bij het betaalsysteem aankomen. In eerste instan-

tie ziet het er goed uit: naast een gebruikersnaam en wachtwoord heb je ook een smartcard met PIN-code nodig om betalingen te kunnen uitvoeren. De beheerder van de autorisaties heeft geen smartcard en kan dus niet betalen. Als we wat verder kijken, blijkt de directeur echter over alle autorisaties te beschikken. Wij vragen de directeur hiernaar en hij vertelt ons dat dit is om in vakantietijd betalingen te kunnen uitvoeren. Wij geven hem aan dat wij deze autorisaties ongewenst vinden en dat er best andere mogelijkheden zijn om in de vakantieperiode betalingen te kunnen verrichten.

De avond besteden we aan de eindpresentatie voor de vrijdagmorgen. Deze is in de landstaal, omdat de EG-lidstaten recht hebben om in hun eigen taal te worden aangesproken.

#### **Vrijdag 07.30 uur**

Vrijdagochtend vroeg krijg ik een telefoontje van mijn echtgenote met de mededeling dat het openbaar vervoer waar ik ben, staakt en het dus moeilijk kan worden om op tijd op het vliegveld te zijn. Om 11.00 uur is onze eindpresentatie van de informatiebeveiligingsaudit met alle auditors en belanghebbenden van het betaalkantoor. Ook nu weer met tolken, die onze presentatie van de eindbevindingen in het Engels vertalen. Ik merk dat de letterlijke vertaling van de tolk niet helemaal aansluit bij de terminologie in IT-land. Snel maak ik hier een opmerking over om onze bevindingen in het juiste perspectief te plaatsen.

De directeur van het betaalkantoor vertelt dat hij voor ons vervoer naar het vliegveld heeft geregeld. Als wij om twaalf uur buiten komen, staat daar een grote, glimmend gepoetste, BMW. Onze 'taxi' blijkt één van de dienstauto's van de ministers te zijn en over de bijbehorende privileges te beschikken. Achterin gezeten, zoeven wij dan ook met bovenwettelijke snelheid naar het vliegveld. Ik ben ruim op tijd en moet vaststellen dat het vliegtuig meer dan twee uur vertraging heeft. Moe, maar voldaan, word ik die avond van Schiphol opgehaald door mijn echtgenote. Voor maandag wacht mij het rapport van deze audit. ■