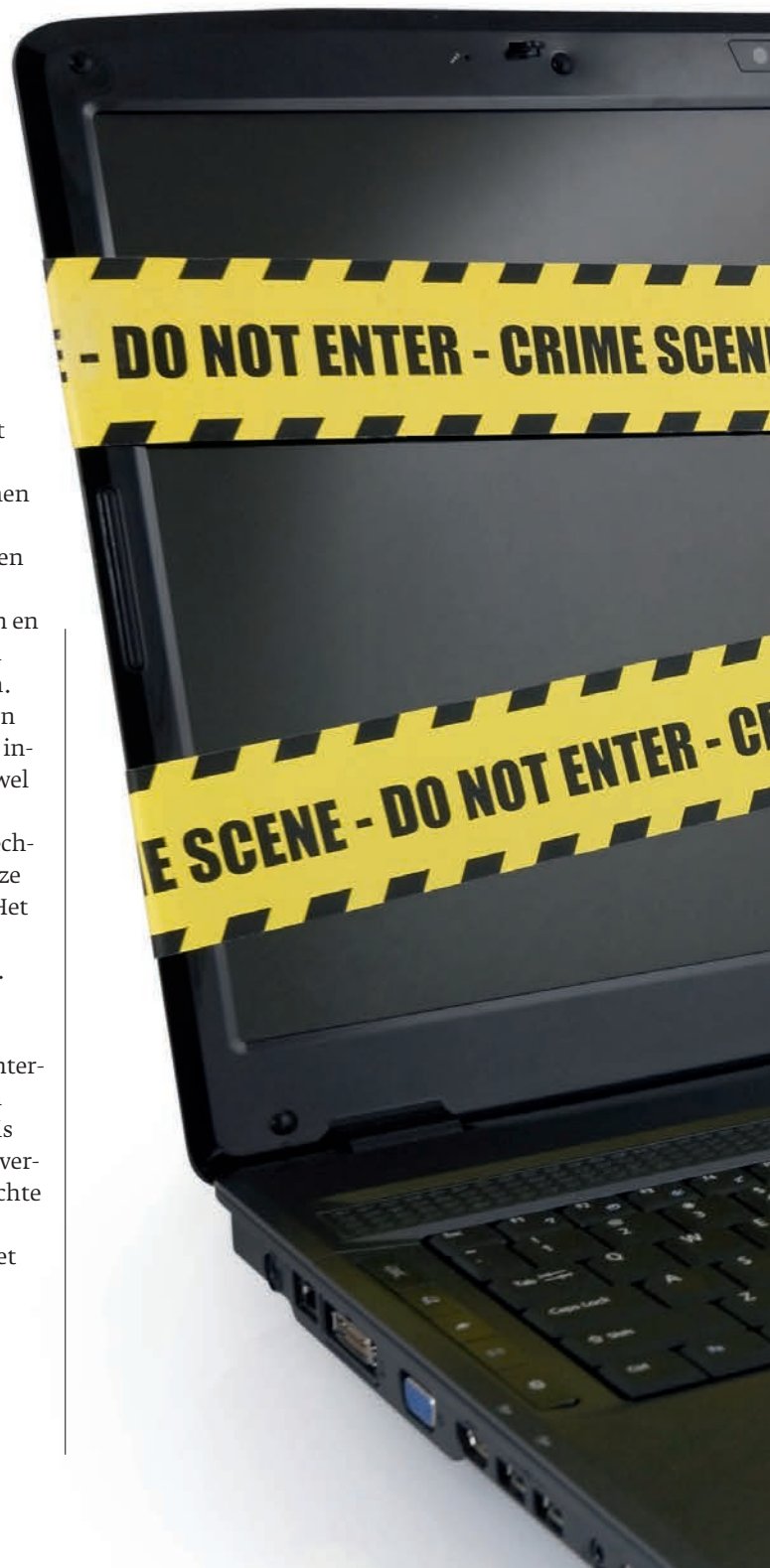
Cybercrime en -se je kan er niet omh

De cyberwereld staat in brand vanwege de vele incidenten. Zelfs de Nederlandse overheid onderkent de cyberrisico's en treft nu doortastend maatregelen. Binnen de accountancy blijft het echter verrassend stil over dit onderwerp. Zorgwekkend, want cybercrime en cyberrisico's zijn zeer relevant voor de accountantscontrole.

TEKST: **JAN MATTO*** | BEELD: **DREAMSTIME**



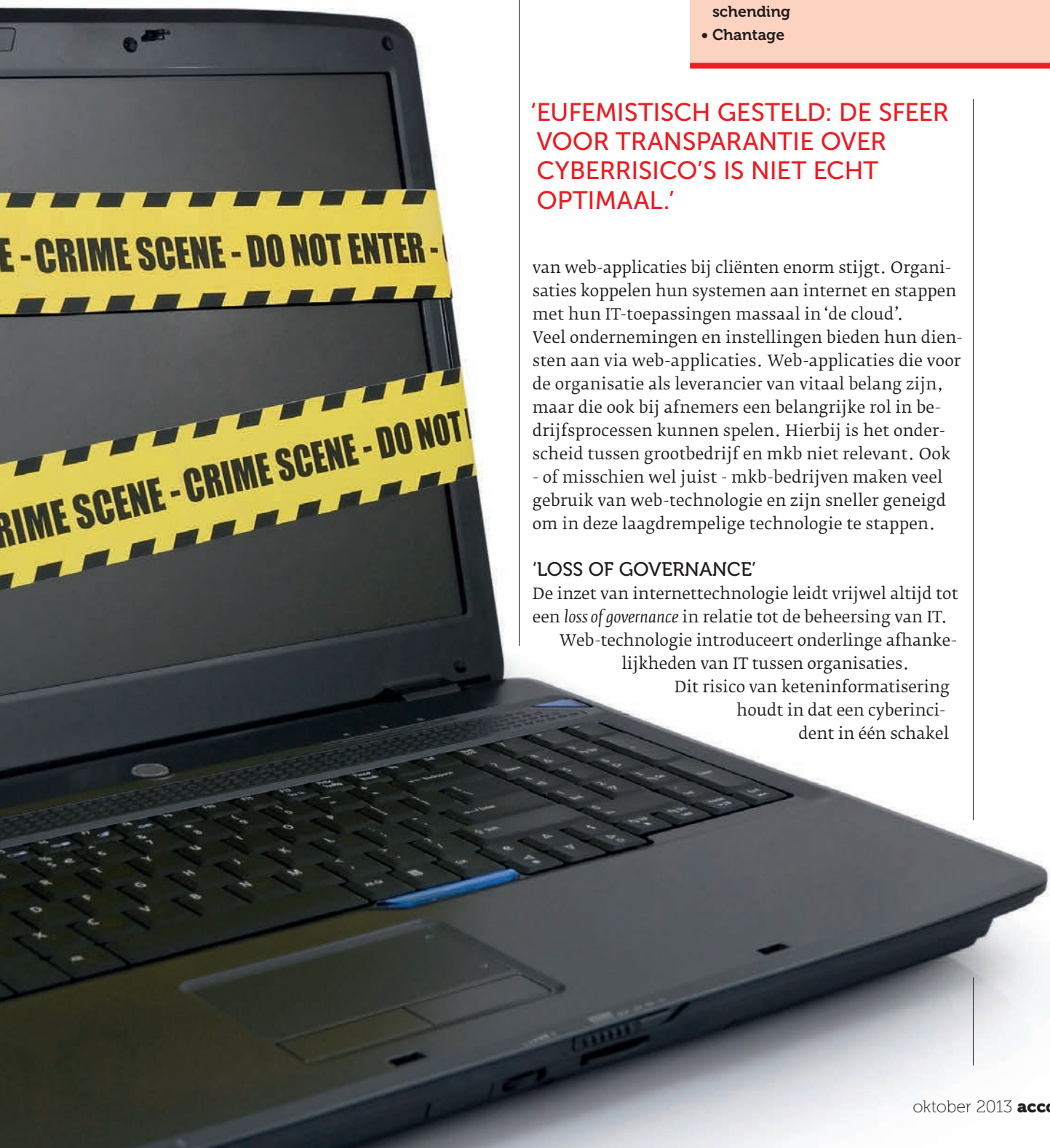
Bij de jaarrekeningcontrole maakt een accountant meestal gebruik van gegevens uit geautomatiseerde systemen. Hierbij is het van belang om vast te stellen dat IT-systemen betrouwbaar functioneren en dat de integriteit van gegevens is gewaarborgd. Cybersecurity is hierbij een randvoorwaarde.
Cyberincidenten kunnen de integriteit van systemen en data ondermijnen. Een onveilige web-applicatie kan impact hebben op alle daaraan gekoppelde systemen. Dus een onveilige web-applicatie die functioneel geen rol speelt binnen financiële processen kan een risico introduceren voor achterliggende systeemdelen waar wel financiële data wordt verwerkt.
Systeemgrenzen vervagen bij de inzet van internettechnologie en uitbesteding van ICT-diensten waarbij deze technologie per definitie een dominante rol speelt. Het wegredeneren of 'uitscopen' van cyberrisico's bij de controleaanpak is een moeilijk houdbaar standpunt.

CLIËNTEN IN 'DE CLOUD'

Cybercrime en -security zijn direct gekoppeld aan internetgebruik en web-services. Het internetgebruik in Nederland stijgt explosief. De publicatie 'ICT, kennis en economie' (CBS, juli 2013) meldt dat het internetverkeer in 2012 met vijftig procent is gestegen ten opzichte van 2011. In Europa is een zelfde groei te zien.
Maar ook in de praktijk is goed zichtbaar dat de inzet

'WEGREDENEREN OF 'UITSCOPEN' VAN CYBERRISICO'S BIJ DE CONTROLEAANPAK IS EEN MOEILIJK HOUDBAAR STANDPUNT.'

curity: een!



GEVOLGEN CYBERINCIDENTEN:

- **Imagoschade**
- **Diefstal van (vertrouwelijke) informatie en intellectueel eigendom**
- **Schade bij stakeholders en cliënten (denk ook aan gestolen creditcardgegevens, wachtwoorden, identiteitsfraude et cetera)**
- **Discontinuïteit van processen en diensten, verlies aan kwaliteit**
- **Directe financiële schade als gevolg van fraude**
- **Privacy-schendingen, juridische risico's, compliance schending**
- **Chantage**

'EUFEMISTISCH GESTELD: DE SFEER VOOR TRANSPARANTIE OVER CYBERRISICO'S IS NIET ECHT OPTIMAAL.'

van web-applicaties bij cliënten enorm stijgt. Organisaties koppelen hun systemen aan internet en stappen met hun IT-toepassingen massaal in 'de cloud'. Veel ondernemingen en instellingen bieden hun diensten aan via web-applicaties. Web-applicaties die voor de organisatie als leverancier van vitaal belang zijn, maar die ook bij afnemers een belangrijke rol in bedrijfsprocessen kunnen spelen. Hierbij is het onderscheid tussen grootbedrijf en mkb niet relevant. Ook - of misschien wel juist - mkb-bedrijven maken veel gebruik van web-technologie en zijn sneller geneigd om in deze laagdrempelige technologie te stappen.

'LOSS OF GOVERNANCE'

De inzet van internettechnologie leidt vrijwel altijd tot een *loss of governance* in relatie tot de beheersing van IT. Web-technologie introduceert onderlinge afhankelijkheden van IT tussen organisaties. Dit risico van keteninformatisering houdt in dat een cyberincident in één schakel

IDENTITEITSFRAUDE

Op van 2 april 2013 stuurde minister Plasterk een brief en bijbehorende rapportage over de Voortgang Toekomstbestendigheid Identiteitsinfrastructuur naar de Kamer. Hieruit bleek het volgende:

- **Circa 5,6 procdent van de burgers in de periode 2007-2011 (vier jaar) is slachtoffer van identiteitsfraude.**
- **In de jaren 2007-2012 (zes jaar) is dit circa 13,3 procent.**
- **Van deze slachtoffers heeft een deel financiële schade geleden: naar schatting 9,5 procent van de gehele bevolking.**
- **Over 2012 is berekend dat tussen de 672.787 en 869.816 burgers slachtoffer zijn geweest, die gezamenlijk tussen de 393 en 508 miljoen euro schade hebben geleden.**

‘AUDITORS HEBBEN TE VEEL GESTEUND OP NORMENKADERS DIE GROTE BEPERKINGEN KENNEN ALS HET OM WEB-GERELATEERDE IT-RISICO’S GAAT.’

in de keten ook gevolgen heeft voor andere deelnemers in deze keten. Een lek in het ene systeem kan de kwaadwillende hacker vaak informatie opleveren om andere systemen binnen te dringen en frauduleuze acties te ondernemen.
Bijvoorbeeld door inloggegevens, creditcardgegevens of andere cliëntgegevens buit te maken. De uitval van een web-service in een keten kan alle deelnemers in die keten raken.
Steeds meer organisaties vragen terecht aan hun leveranciers: ‘Hoe veilig is mijn data bij jullie?’ en ‘Hoe is de continuïteit van de web-service geborgd?’ Transparantie over veiligheid en continuïteit van web-services en achterliggende systemen wordt steeds belangrijker. Er ontstaat een nieuwe markt voor cyber-assurance diensten die niet direct gekoppeld is aan de jaarrekening controle.

IJSBERG

Dagelijks zijn cyberincidenten in het nieuws over datalekken, DDoS-aanvallen *(zie kader)* en gehackte systemen. Dit zijn uiteraard alleen incidenten die de media halen. Bedrijven en ICT-dienstverleners staan namelijk niet te trappelen om de vuile was buiten te hangen of risico’s scherp te duiden.
Een hacker die onveilige situaties aan de kaak stelt en in de openbaarheid brengt, wordt door Justitie vervolgd, zoals Kamerlid Henk Krol recentelijk nog heeft ondervonden. Eufemistisch gesteld: de sfeer voor transparantie over cyberrisico’s is niet echt optimaal. Slechts een klein topje van de ijsberg is zichtbaar. Vrijwel ieder cyberincident heeft naast directe schade veel grotere indirecte schade. De wereldwijde schade door cybercrime wordt geschat op tussen de driehonderd miljard en één biljoen dollar (bron: 23 juli 2013, Amerikaanse denktank ‘Center for Strategic and International Studies’ en beveiligingsfirma McAfee).
Recente door de rijksoverheid gepubliceerde onderzoeksrapporten over cybercrime en -incidenten in Nederland geven aan dat cybercrime en -incidenten schering en inslag zijn. De cijfers zijn ronduit schokkend.

DIGITALE IDENTITEITSFRAUDE

Dat meer aandacht voor cybercrime en -security nodig is, blijkt onder meer uit de feitenopsomming in de recente Kamerbrief van minister Plasterk *(zie kader)*.
Identiteitsfraude in de virtuele wereld is van een maatschappelijke omvang en brengt ook nog een ander fenomeen met zich mee. Namelijk dat het in de cyber-

Zie ook Accountant.nl/ Vaktechniek

wereld niet meer zeker is wie nu wie is. Dat betekent dat er geen garantie is dat er onder de naam van een argeloze gebruiker geen 'fout internetgedrag' plaatsvindt of frauduleuze transacties worden uitgevoerd. Het gevolg: een gebruiker staat mogelijk zonder dat hij het weet in de verdachtenhoek en in de registers van de NSA, AIVD of andere inlichtingen- en opsporingsdiensten. Iets waar klokkenluiders als Snowden en anderen voor waarschuwen. Overigens ook interessante materie voor slimme advocaten die te maken hebben met rechtszaken waar zogenaamd digitaal bewijs wordt aangeleverd.
Voor de overheid is de actuele situatie rond digitale identiteiten reden om een nieuw stelsel te ontwikkelen. Het nieuwe elektronisch identiteitenstelsel (eID) moet in 2017 afgerond zijn en is bruikbaar binnen zowel het publieke als het private domein.

POBELKA BOTNET

Internetcriminelen proberen computers te infecteren met malafide software. Met deze software wordt informatie van een computer verzameld of wordt de computer gebruikt om andere criminele activiteiten te ontplooien. Een verzameling geïnfecteerde en door criminelen beheerde computers die met elkaar verbonden zijn via internet, wordt een botnet genoemd.
Op 28 maart 2013 heeft het Nationaal Cyber Security Centrum (NCSC), in samenwerking met onder meer de AIVD, de politie en het OM, een onderzoeksrapport gepubliceerd over het spectaculaire Pobelka Botnet. Dit rapport geeft cijfers over infecties van computers in Nederland. In de periode januari 2009 tot juni 2010 zijn er 1,1 miljoen IP-adressen geïdentificeerd met een mogelijke infectie. Van deze adressen waren er ongeveer negenhonderdduizend in het netwerk van de grote Nederlandse Internet Service Providers. Een conservatieve interpretatie hiervan zou duiden op ongeveer 450.000 tot 900.000 geïnfecteerde computers. Dit komt erop neer dat zo'n vijf tot tien procent van alle Nederlandse breedband internetabonnees een geïnfecteerde computer heeft. Uit de onderzoeksgegevens blijkt ook dat het aantal geïnfecteerde computers stijgt. De kans dat de computer van de accountant of die van hun clienten is gecompromitteerd, is dus redelijk groot.
Een andere conclusie van het rapport is dat dit botnet er vooral op is gericht om inloggegevens te verzamelen en het manipuleren van financiële transacties. Het risico achter dergelijke cybercrime is dat inloggegevens kunnen worden onderschept en dat daarmee autorisatiesmechanismen en daarvan afhankelijke functiescheidingen kunnen worden doorbroken.

DIGINOTAR

Voor vertrouwelijk verkeer op internet - bijvoorbeeld bij internetbankieren - moet een website beschikken over een veiligheidscertificaten. DigiNotar was een vooraanstaande leverancier van veiligheidscertificaten voor onder andere overheidsdiensten, maar ook voor private ondernemingen. In 2011 is DigiNotar gehackt waardoor vele websites onveilig waren geworden en de authenticiteit van digitale berichten via deze sites niet meer was te waarborgen. Een gevolg was onder meer dat systemen van de Belastingdienst niet meer te bereiken of te vertrouwen waren. Hetzelfde gold voor vele private web-toepassingen, waaronder die van een aantal accountantskantoren.
DigiNotar is aan deze hack snel ten ondergegaan. Interessant aan de DigiNotar-case is de rol van de auditors en vooral de onderzoeken die daarnaar zijn verricht. De onderzoeken geven onder meer aan dat de auditors te veel gesteund hebben op normenkaders die grote beperkingen kennen als het om web-gerelateerde IT-risico's gaat. En ook dat auditors te veel (alleen!) focussen op beheerstelsels en procedures en geen aandacht hebben geschonken aan wat wordt aangeduid als de 'ICT-werkelijkheid'.
Een andere constatering uit de onderzoeken is dat ten onrechte assurance werd ontleend aan de uitspraken van deze auditors. Een nogal stevige constatering die verrassend weinig aandacht kreeg en nog steeds krijgt.

CYBERCRIME, CYBERSECURITY EN ACCOUNTANT

Cybersecurity anno 2013 is onderdeel van interne beheersing en verdient bij elke controleopdracht aandacht waar sprake is van web-applicaties en internetgebruik. Het toetsen van security van een ICT-systeem aan de hand van een checklist met procedures is niet meer toereikend om een opinie te kunnen vormen over de veiligheid van dat systeem. ICT-systemen en daaraan gerelateerde security-risico's zijn veel te dynamisch. De 'ICT-werkelijkheid' zelf moet aan onderzoek worden onderworpen.

DDOS-AANVALLEN

Het zal niemand ontgaan zijn: begin april 2013 is een groot aantal banken in Nederland dagenlang aangevallen met zogenaamde Distributed Denial of Service attacks (DDoS). Deze aanvallen hebben er toe geleid dat financiële diensten, waaronder het uitvoeren van elektronische betalingen niet meer mogelijk waren. De aanvallen waren zeer intensief en zorgden voor overbelasting van systemen met als gevolg het niet bereikbaar zijn van websites met betaaldiensten. Ook betaaldiensten als iDEAL zijn in die periode als gevolg van de DDoS-aanvallen regelmatig uitgevallen.
DDoS-aanvallen zijn relatief makkelijk op te zetten en door kwaadwillenden bedoeld om de beschikbaarheid van IT-services aan te tasten. De aanvallen zijn niet direct bedoeld om in te breken in systemen. De meeste DDoS-aanvallen gebruiken een netwerk van geïnfiltreerde computers (botnet) om een grote hoeveelheid berichten op een computer of computernetwerk af te sturen en deze daarmee te overbelasten. De software voor het opzetten van een DDoS-aanval is vrij als *open source* beschikbaar.

'HET LIGT VOOR DE HAND DAT DE ACCOUNTANT ZIJN KLANTEN WIJST OP DE RISICO'S VAN WEB-APPLICATIES EN CLOUD-DIENSTEN.'

'ER ONTSTAAT EEN NIEUWE MARKT VOOR CYBER-ASSURANCE-DIENSTEN DIE NIET DIRECT IS GEKOPPELD AAN DE JAARREKENINGCONTROLE.'

Enkele voorbeelden van normen uit de richtlijnen van het NCSC (Nationaal Cyber Security Centrum) die focussen op de veiligheid van web-applicaties zijn:

- *Hardening*
  Cybersecurity wordt voor een belangrijk deel bepaald door de robuustheid van de software van webapplicaties. Overbodige functionaliteit in web-applicaties brengen risico's met zich mee. Het elimineren van overbodige functionaliteit heet hardening.

- *Actualiteit van software patches*
  Het is belangrijk dat de laatste software updates zijn geïnstalleerd en daarmee de laatst bekende veiligheidslekken worden gedicht. Patchmanagement ziet erop toe dat de actuele software is geïnstalleerd

- *Uitvoering van periodieke vulnerability scans*
  Dit zijn geautomatiseerde scans die aan de hand van een database met bekende veiligheidsrisico's websites kunnen screenen op het afdekken van deze risico's . Vulnerability scans kunnen toetsen conform bekende standaarden van bijvoorbeeld OWASP (Open Web Application Security Program), PCI -DSS (Payment Card Industry - Data Security Standard) of ETSI (Europees Telecommunicatie en Standaardisatie Instituut).

- *Uitvoering van periodieke penetratietesten*
  Een penetratietest is een handmatige test door een specialist waarbij met hacking-vaardigheden wordt geprobeerd zwakheden in web-applicaties te vinden. Een goed uitgevoerde penetratietest kan veel bewijs opleveren over de status van de veiligheid van een systeem.

- *Intrusion detection en analyse van incidenten*
  Een eerste vereiste is dat security-incidenten kunnen worden onderkend. Vervolgens is logging en evaluatie essentieel zodat maatregelen kunnen worden genomen. Intrusion detection is nodig om cyber-incidenten en bijvoorbeeld datalekken in een vroeg stadium te kunnen detecteren.

- *Code reviews*
  Veel beveiligingsrisico's komen voort uit slecht geconstrueerde software. Een code review richt zich op het vaststellen van de robuustheid van de software hetgeen relevant is voor de beveiliging.

De inzet van tools bij deze onderzoeken is onvermijdelijk om inzicht te verkrijgen in de toestand binnen de 'ICT-werkelijkheid'.

Adviesrol

In de adviesrol van de accountant ligt het voor de hand dat hij zijn klanten wijst op de risico's die kleven aan het gebruik van web-applicaties en cloud-diensten. Een handig en actueel overzicht van de top 10 van cybersecurity-risico's wordt gepubliceerd door OWASP. Open Web Application Security Program is een internationaal initiatief om een veilig gebruik van internet te bevorderen. Het overzicht van de OWASP top 10 over 2013 is recent gepubliceerd en beschikbaar via www.owasp.org . De meeste OWASP-risico's gaan over het misbruik (hacken) van web-applicaties waarlangs achterliggende systemen kunnen worden gemanipuleerd.

Certificeringen

In geval van uitbestede internetservices verdient het aanbeveling om te vragen naar certificeringen van deze services in relatie tot cybersecurity. Er dient wel opgelet te worden dat gebruik is gemaakt van een zinvol certificeringsschema met aandacht voor de 'ICT-werkelijkheid'. De richtlijn beveiliging web-applicaties van het NCSC biedt hier aanknopingspunten toe.

Deskundigen

Het is verstandig dat de accountant allereerst zelf voldoende kennis vergaard over cyberrisico's en cybersecurity om deze risico's en maatregelen goed te kunnen inschatten. Maar het verdient, gezien de aard en de gespecialiseerde materie, zeker ook aanbeveling om tijdig een deskundige IT-auditor in te schakelen. □

Op de Accountantsdag van 27 november 2013 wordt een deelsessie aan cybercrime gewijd.

Noot

** Jan Matto is partner bij Mazars en verantwoordelijk voor de IT-audit- en adviesactiviteiten.*

LEKTOBER

Oktober 2011 heeft de bekende internetjournalist Brenno de Winter elke dag en met succes een gemeentelijke website laten hacken. Een actie die hij van te voren heeft aangekondigd. Omdat veel van de gemeentelijke websites aansluitingen hebben met DigiD was dit aanleiding voor de Nederlandse regering om tot actie over te gaan. Het risico van identiteitsfraude bleek zeer hoog. Het Nationaal Cyber Security Centrum (NCSC) heeft in samenwerking met een aantal IT-auditorganisaties de Richtlijn Beveiliging Webapplicaties opgesteld (begin 2012 gepubliceerd). Lektober was de aanleiding voor de Nederlandse overheid om 1.600 organisaties te verplichten om voor eind 2013 een verplicht 'DigiD-assessment' uit te voeren op basis van een subset van de richtlijnen van het Nationaal Cyber Security Centrum. Teleurstellend in dit proces is overigens dat een aantal belangrijke normen uit de NCSC-standaarden zijn geschrapt voor de DigiD-assessments die juist de ICT-werkelijkheid raken. Een stap die misschien nog wel eens rare gevolgen kan gaan krijgen.