Van hype naar aanpak

Publieke managementletter over cybersecurity

Mei 2016

NBA

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

De leden van de Koninklijke NBA vormen een brede, pluriforme beroepsgroep van ruim 20.000 professionals werkzaam in de openbare accountantspraktijk, bij de overheid, als intern accountant en in het management van organisaties. Integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag zijn essentiële waarden voor iedere accountant. De Koninklijke NBA helpt accountants hun cruciale rol in de maatschappij te vervullen, nu en in de toekomst.

Aan belanghebbenden en belangstellenden in het thema Cybersecurity

Postbus 7984
1008 AD Amsterdam
Antonio Vivaldistraat 2-8
1083 HP Amsterdam
T 020 301 03 01
nba@nba.nl
www.nba.nl

Datum
Mei 2016

Geachte mevrouw, heer,

De digitale snelweg biedt veel kansen, maar ook grote risico's. Steeds opnieuw worden cyber incidenten in de media gemeld. Voor elke online organisatie geldt niet zozeer de vraag of men wordt gehackt, maar wanneer en hoe vaak. En hoe snel daarop gereageerd kan worden.

Cybersecurity hoort daarom op elke bestuursagenda te staan. Het bestuur moet het goede voorbeeld geven en de juiste vragen stellen. Hierover is al veel geschreven. Deze publieke managementletter (PML) Van hype naar aanpak is dan ook niet bedoeld om nieuwe inzichten te geven, maar biedt een ander perspectief: het perspectief van de accountant die de jaarrekening controleert en de sterke en zwakke kanten van de organisatie kent.

De betrouwbaarheid van alle informatie in de jaarrekening is afhankelijk van de integriteit van de onderliggende data. Daarom dient databeveiliging voorop te staan. Maar ook hier ligt het primaat in de bestuurskamer. Bestuurders moeten cybersecurity inbedden in hun strategie en risicobeleid, verankeren in hun organisatie. Elke bestuurder moet zich realiseren dat cybercrime een van de grotere risico's is die een organisatie kunnen bedreigen. Net als fraude of brand. De accountant kan bijdragen aan de bewustwording, door de juiste vragen over cybersecurity te stellen aan bestuurders en toezichthouders. Uiteraard zal hij (of zij) cybersecurity een passende plaats in de controle geven.

Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

Alles beveiligen is onmogelijk. Daarom dient de focus op de kroonjuwelen gelegd te worden: de meest vitale data en processen. De mens is vaak de zwakste schakel, ook cultuur en gedrag verdienen de aandacht. Het gaat er in essentie om dat een organisatie over voldoende digitale weerbaarheid beschikt: incasseringsvermogen en slagkracht. Vanuit het perspectief van de accountant zijn vijf signalen geselecteerd. Met als focus de cyberbedreigingen van buiten af:

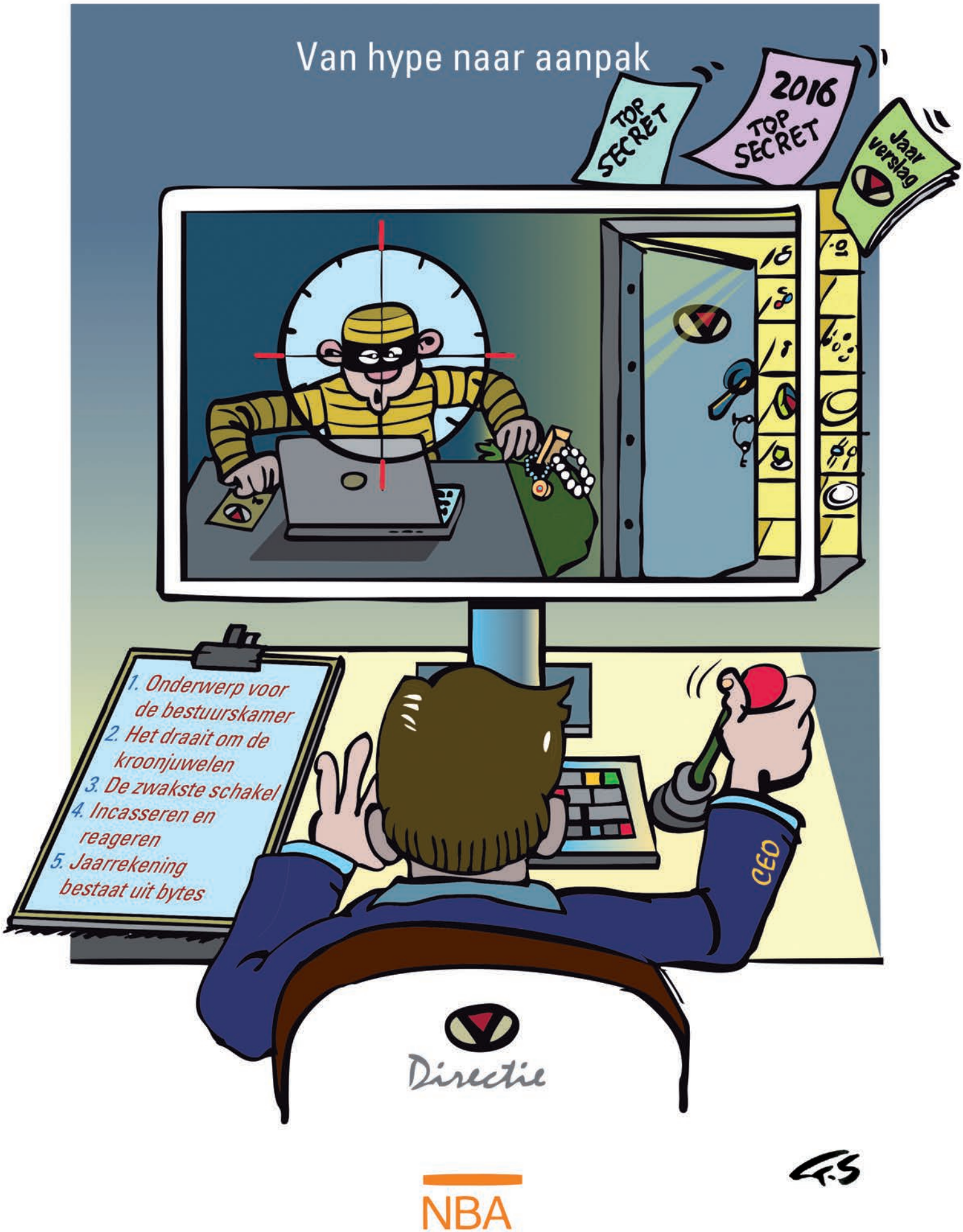
1. Onderwerp voor de bestuurskamer
2. Het draait om de kroonjuwelen
3. De zwakste schakel
4. Incasseren en reageren
5. De jaarrekening bestaat uit bytes

De signalen zijn gebaseerd op de kennis van onze leden en accountantsorganisaties die betrokken zijn bij het thema. Diverse belanghebbenden, onder wie NOREA en het Cybersecurity Raad (CSR) hebben hun commentaar aan ons kenbaar gemaakt. Wij zijn hen allen zeer erkentelijk voor hun bijdragen.

Hoogachtend,

Pieter Jongstra RA
Voorzitter NBA

Johan van Hall RA RE
Lid NBA Signaleringsraad


Van hype naar aanpak
TOP SECRET
2016 TOP SECRET
Jaar verslag
1. Onderwerp voor de bestuurskamer
2. Het draait om de kroonjuwelen
3. De zwakste schakel
4. Incasseren en reageren
5. Jaarrekening bestaat uit bytes
CEO
Directie
NBA

Inhoudsopgave

Van hype naar aanpak

Cybercrime, de tegenhanger van cybersecurity, is big business. Malafide organisaties verdienen veel geld door organisaties te hacken. Bedragen van tientallen miljoenen zijn geen uitzondering meer. De schade door de hack van de Amerikaanse warenhuisketen Target in 2013 bedroeg zelfs 236 miljoen dollar. In februari 2016 slaagden hackers er bijna in om 1 miljard dollar van de Federal Reserve Bank of New York over te maken. Vier eerdere verzoeken hadden al 81 miljoen dollar opgeleverd, de vijfde keer ging het alleen maar mis omdat één letter verkeerd was gespeld.

Langer bekend zijn de DDoS (Distributed Denial-of-Service) aanvallen, erop gericht om een netwerk plat te leggen door het te overbelasten. Banken zijn regelmatig het slachtoffer geweest, maar vorig jaar werd ook kabelbedrijf Ziggo getroffen. Een hack van persoonlijke foto's op iCloud in 2015 toonde aan dat ook beroemdheden doelwit voor cybercrime vormen. Volgens een recente studie vond in 2015 een toename van cybersecurity incidenten plaats van bijna 40 procent[1].

Het heersende idee dat alleen grote, internationale ondernemingen het slachtoffer worden klopt niet. Mkb-bedrijven, organisaties van maatschappelijk belang (zoals gemeenten, ziekenhuizen en energiebedrijven) en ook particulieren worden getroffen door cybercrime. Weliswaar is hun risicoprofiel anders, maar de dreiging is er net zo goed. Het is eigenlijk niet meer de vraag of je wordt gehackt, maar wanneer en hoe vaak. Absolute veiligheid bestaat niet.

De gevolgen van een cyberaanval kunnen verstrekkend zijn. Niet alleen door directe schade tijdens een hack, maar ook indirect. Diefstal van intellectueel eigendom, verlies van klanten en omzet, reputatieschade, claims van gedupeerden of boetes van externe toezichthouders. Aanvullend zijn er kosten voor (forensisch) onderzoek, juridisch advies en het herstel van de aangerichte schade.

Een zaak van nationale veiligheid

Ook de overheid is zich bewust van het belang van cybersecurity. Zo zijn enkele jaren geleden het Nationaal Cybersecurity Centrum (NCSC) en de Cybersecurity Raad (CSR) ingesteld.

Het NCSC bestaat uit een samenwerking van publieke en private organisaties die zich richt op de integrale aanpak van cybersecurity. Het is een informatieknooppunt en expertisecentrum, dat ook optreedt als Computer Emergency Response Team (CERT) voor de Rijksoverheid. Een belangrijk onderdeel van het NCSC is het Nationaal Cybersecurity Operations Center (NCSOC) dat dag en nacht bereikbaar is voor meldingen en ondersteuning. Het NCSC valt organisatorisch onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

De CSR is het onafhankelijke en strategische adviesorgaan van het overheid als het gaat om cybersecurity in Nederland. In april 2015 bracht de CSR de Handreiking Cybersecurity voor de bestuurder uit. Deze richtte zich op drie vragen: welke afwegingen maakt de bestuurder over cybersecurity, hoe belegt hij dit in zijn organisatie en hoe bouwt hij aan digitale veiligheid? Het werkprogramma van de CSR voor 2016 heeft de veelzeggende titel De toekomst is dichterbij dan je denkt. Een belangrijke constatering in dat programma is dat dat bewustwording (awareness) nog steeds een belangrijk wapen is in de strijd tegen cybercriminaliteit.

Het NCSC publiceert jaarlijks een cybersecurity beeld van Nederland (CSBN). Uit de meest recente uitgave[2] blijkt dat het grootste aantal incidenten betrekking heeft op

1 Turnaround and transformatio in cybersecurity. PwC , oktober 2015.
2 Cybersecuritybeeld Nederland (CSBN) 2015, september 2015

DDoS aanvallen, misbruik van gebruikersrechten, toegang tot gevoelige gegevens en het omzeilen van beveiligingsmaatregelen. Hierbij kijkt het NCSC naar de kans dat misbruik plaatsvindt en de schade die dat kan opleveren. De publicatie bevat ook een dreigingsmatrix met per doelwit (overheden, bedrijfsleven en burger) de mogelijke dreigingen. Als grootste dreigingen gelden nog steeds phishing (verzending van frauduleuze emails) en crypto-ware (frauduleuze versleuteling van bestanden). Het NCSC stelt vast dat de afhankelijkheid van ICT en internet steeds groter wordt. Gelukkig neemt het inzicht in cyber incidenten ook toe, zodat cybersecurity maatregelen meer gericht uitgevoerd kunnen worden.

Naar het juiste perspectief

Door alle aandacht voor cybersecurity, de vele publicatie op dat terrein en de vaak ongenuanceerde berichtgeving in de media zou een verkeerd beeld van cybersecurity kunnen ontstaan. Alsof talloze organisaties willoos slachtoffer zijn van cybercrime en geen enkel verweer mogelijk is. De waarheid is genuanceerder: met de juiste aanpak kan veel schade worden voorkomen. Zoals de SCR schreef, bewustwording is nog steeds een belangrijk wapen in de strijd. De oplossing ligt niet alleen in de techniek. Het gaat er veel meer om hoe cybersecurity in de hele organisatie is ingebed. Bestuurder, werknemer, toezichthouder, interne en openbare accountant spelen allemaal een rol. Er moet aandacht zijn voor de kroonjuwelen, cultuur en gedrag, bewustwording en opleiding. De digitale weerbaarheid moet omhoog, het vermogen om te incasseren en snel te reageren.

Een natuurlijke rol voor de accountant

Cybersecurity raakt de accountant vanuit verschillende routes. Vanuit zijn controleperspectief moet hij zich realiseren dat de basis voor de jaarrekening bestaat uit bytes. De betrouwbaarheid van de informatie is afhankelijk van de integriteit van de onderliggende data. De rol van de accountant gaat daarom verder dan het vaststellen dat de schade van een cyber incident getrouw in de jaarrekening is verwerkt of dat de continuïteit is gewaarborgd.

De belangrijkste rol voor de accountant ligt misschien wel in zijn natuurlijke adviesfunctie: het stellen van de juiste vragen over cybersecurity. Vaststellen dat er bij bestuur en toezichthouders voldoende awareness bestaat, toetsen of cybersecurity de juiste plaats heeft in de strategie en het risicobeleid.

Signaal 1 | Onderwerp voor de bestuurskamer

Vrijwel dagelijks bewijzen cyber incidenten dat de risico's in cyber space groot zijn. Zowel individuele hackers als professioneel georganiseerde cybercriminelen zijn actief. Het behoeft eigenlijk geen nadere toelichting dat cybersecurity de aandacht verdient van elke organisatie die online is.

De laatste tijd is het aantal cyberincidenten en de ernst ervan zozeer toegenomen, dat cybercrime voor elke organisatie een risico kan vormen. Het kan leiden tot reputatieschade en imagoverlies, inkomstenderving, boetes of zelfs het publiek worden van intellectueel eigendom. Door de toenemende digitalisering van de maatschappij is de beveiliging van waardevolle informatie van groot belang. Niet alleen de veiligheidsrisico's worden groter, ook het aantal incidenten stijgt.

De aandacht vanuit de klanten, media, toezichthouders en de wetgevers neemt toe. Klanten maken zich zorgen of hun informatie afdoende is beschermd. Toezichthouders vragen de aandacht van bestuurders en doen onderzoek naar getroffen maatregelen voor cybersecurity.

De wetgever zit ook niet stil. De laatste jaren is er meer en meer wetgeving in dit kader ingevoerd. Een voorbeeld hiervan is de per 2016 ingevoerde Meldplicht Datalekken[2]. Een bestuurder kan aansprakelijk worden gesteld als hij nalaat om adequate maatregelen voor cybersecurity te treffen, of als hij datalekken niet meldt. Boetes kunnen oplopen tot 10 procent van de wereldwijde omzet. Daarnaast zijn individuele claims van gedupeerden mogelijk.

Cybercrime dient op de agenda te staan van elke bestuurder, commissaris en toezichthouder. Dit geldt ook voor (semi)publiekrechtelijke organisaties of de directeur-eigenaar van een kleine mkb- onderneming.

Het thema is niet nieuw, maar cybercrime wordt steeds meer 'a fact of life'.

De media schetsen vaak een ongenuanceerd beeld van cybercrime, alsof veel organisaties een haast willoos slachtoffer zijn van cybercriminelen. Alles wordt over één kam geschoren, dat kan tot ongefundeerde angst leiden. De waarheid ligt genuanceerder. Een mkb-bedrijf heeft een ander risicoprofiel dan een multinational of een organisatie van maatschappelijk belang. Over veel van de in de media genoemde incidenten hoeft een mkb-bedrijf zich minder zorgen te maken. De risico's zijn beheersbaar, hoewel honderd procent veiligheid een illusie is. Het nastreven daarvan leidt niet alleen tot hoge kosten, maar ook tot schijnzekerheid.

Cybercrime is een risico dat dezelfde aandacht verdient als bijvoorbeeld het risico op brand of fraude. Het is een risico dat gestructureerd moet worden aangepakt door de bestuurders en de toezichthouders van de onderneming, vanuit overkoepelend risicomanagement. Ook de accountant moet hiervoor oog hebben bij de controle van de jaarrekening.

2 De NBA bereidt een aantal artikelen op dit terrein voor. In februari verscheen de publicatie Meldplicht Datalekken van De IT-jurist.

Negatief voorbeeld

Niet mijn verantwoordelijkheid, er is een afdeling voor

Tijdens een bestuursvergadering van grote organisatie A werd de vraag gesteld wat de organisatie doet op het gebied van cybersecurity. Het antwoord van de CEO was: daar hebben we een afdeling voor, dat is niet mijn verantwoordelijkheid. Kort daarna werd A getroffen door grootschalige cyberaanvallen en bleek A onvoldoende weerbaar op dit terrein. In de afgelopen jaren was onvoldoende geïnvesteerd in maatregelen op het gebied van cybersecurity. A leed hierdoor grote schade.

Positief voorbeeld

Positief voorbeeld: Cybersecurity als onderdeel van het risicomodel

In grote ICT multinational B is het cybersecurity risico opgenomen als één van de strategische risico's voor de organisatie. Het wordt op kwartaalbasis besproken in het bestuur, gebruikmakend van een dashboard dat de risico's van B weergeeft. De uitkomsten van deze discussies dragen bij aan de juiste prioriteitstelling bij investeringen en activiteiten op het terrein van cybersecurity. Dit ligt geheel in lijn met het geldende risicoprofiel en bijbehorende risicobereidheid van B.

AANBEVELING 1: Stel als bestuurder de juiste vragen

• Maak cybersecurity tot vast onderdeel van het risicomanagement.
• Stel als bestuurder de juiste vragen aan de organisatie:

1. **Wat is de risicobereidheid en -prioriteitstelling?**
   - Wat is de risicobereidheid voor downtime, verlies van gegevens en privacy incidenten?
   - Hoe is dit vast te stellen en hoe kan dit worden gemonitord (via een risico dashboard)?
   - Wat zijn de belangrijkste gegevens die de hoogste bescherming nodig hebben? Welke processen zijn cruciaal voor het voortbestaan van de organisatie?
2. **Wat is de interne organisatie op het gebied van cybersecurity?**
   - Hoe is de eerste- en tweedelijns defensie ingericht (op afdelingsniveau en qua interne controle)?
   - Hoe wordt over de cybersecurity risico's gerapporteerd?
   - Hoe vindt de coördinatie plaats tussen de verschillende bedrijfsfuncties?
3. **Wordt er voldoende geïnvesteerd, is er toegevoegde waarde?**
   - Wat zijn de geplande investeringen in cybersecurity voor de komende drie jaar?
   - Is dit toereikend om afdoende beschermd te zijn (in lijn met de risicobereidheid)?
   - Hoe verhouden de investeringen zich tot die van de concurrentie?
4. **Hoe veilig en weerbaar is de organisatie nu eigenlijk?**
   - Wat waren de meest relevante beveiligings- en privacy incidenten (en bij vergelijkbare organisaties) in de laatste 12 maanden?
   - Wat waren de leerpunten en wat doet de organisatie anders om nieuwe incidenten te voorkomen?
5. **Wordt de organisatie veiliger of onveiliger?**
   - Welke kritische kengetallen of KPI's staan op het cyberrisico dashboard?
   - Behaalt de organisatie de gestelde cyberrisico doelstellingen?
   - Hoe verhouden de cyberrisico KPI's zich ten opzichte van de concurrentie?
6. **Hoe wordt het risico van leveranciers en andere ketenpartners beheerst?**
   - Hoe wordt geborgd dat de externe leveranciers, hun leveranciers en andere ketenpartners de organisatie niet blootstellen aan onaanvaardbare cyberrisico's?
7. **Hoe is cybersecurity geborgd in de producten en diensten?**
   - Op welke wijze is cybersecurity geborgd in de huidige producten en diensten en in de ontwikkeling van nieuwe producten en diensten?

Signaal 2 |
Het draait om de kroonjuwelen

De kroonjuwelen van een onderneming zijn het meest gevoelig voor cyberaanvallen, omdat hiermee de grootste schade of de meeste winst valt te behalen. Investeringen in cybersecurity moeten zich daarom focussen op de kroonjuwelen. Dit vereist een omslag in risico denken.

Digitale kroonjuwelen vertegenwoordigen de hoogste waarde voor een organisatie vanuit strategisch, operationeel, financieel-juridisch en reputatie perspectief. Het zijn de meest vitale informatiebronnen, technologieën of processen van een organisatie. In het bijzonder:

- het goed functioneren van de webshop
- de beschikbaarheid van operationele en/of financiële data
- de persoonsgegevens van bijvoorbeeld klanten, patiënten, huurders of studenten
- de intellectueel eigendom en research investeringen in de high tech sector
- de operationele technologie in productie organisaties
- de continuïteit van dienstverlening door een ICT service/ Cloud dienstverlener

In de praktijk is het lastig om de verschillende informatiebronnen, technologieën en processen te rangschikken naar belang en waarde. Vaak worden alle bedrijfsmiddelen gelijk behandeld, zodat het zilvergoed op dezelfde wijze is beschermd als het campingbestek.

Georganiseerde misdaad, hacktivisten en terroristen, maar ook nationale overheden en zelfs eigen medewerkers zijn voorbeelden van kwaadwillenden. Ze zijn vastberaden en geduldig, hun aanpak is vaak verfijnd. Ze richten zich op individuen, organisaties of zelfs hele sectoren. Het hoofddoel van is meestal het behalen van economisch voordeel of het veroorzaken van schade. Het meest effectieve doelwit zijn de kroonjuwelen. Aanvallers ontwikkelen zich voortdurend om de kwetsbaarheden binnen digitale systemen te benutten. Uiteindelijk bepaalt de zwakste schakel de kwaliteit van het systeem. Na het uitlekken van intellectuele eigendom, klantgegevens of andere waardevolle informatie is de totale impact vaak veel later merkbaar. Het kan maanden of zelfs jaren duren voordat alle negatieve effecten ten volle bekend zijn.

In de praktijk investeren nog veel organisaties in beveiligingsproducten en -diensten gebaseerd op verouderde modellen, die onvoldoende zijn gericht op de echte kroonjuwelen. Dit resulteert in een aanpak die gelijk is voor alle digitale bedrijfsmiddelen, zonder onderscheid naar belang en waarde. Met meestal te weinig aandacht voor het tijdig identificeren en effectief afhandelen van security incidenten. Cybersecurity vraagt om een geheel andere benadering en denkwijze: start met het identificeren van de kroonjuwelen, bepaal daarna de waarde, de risico's en de bedreigingen. De security officer moet de stap maken van politieagent naar uitdager en regievoerder.

Gewapend met dit inzicht kan het management het risicoprofiel van de organisatie aanpassen. Het gaat om verkleining van de kans op schade door cyberaanvallen, niet om de volledige eliminatie van alle risico's. Door nieuwe bedreigingen continu in kaart te brengen, kunnen organisaties beter anticiperen op aanvallen en de negatieve effecten ervan beperken.

Negatief voorbeeld

Kroonjuwelen benaderbaar via de achterdeur

Innovatief bedrijf C had vastgesteld dat blauwdrukken en recepturen in ontwikkeling goed beschermd moesten worden. Hiermee wilde C voorkomen dat de concurrentie vroegtijdig met haar kennis aan de haal ging. De kritische gegevens werden in een apart netwerksegment met sterkere beveiliging opgeslagen, gescheiden van de segmenten met minder kritische gegevens. C was zich echter onvoldoende bewust van de koppelingen tussen de verschillende segmenten. Hierdoor konden hackers via een laag beveiligde netwerkomgeving alsnog toegang krijgen tot de waardevolle informatie van C.

Positief voorbeeld

Zolang de winkel open is en de klanten veilig zijn

Online retailer D worstelde met investeringskeuzes die zij moest maken op het vlak van beveiliging en continuïteit van de web omgeving. Uit een organisatiebrede risicoanalyse bleek dat de grootste impact lag bij het niet beschikbaar zijn van de webshop en het lekken van klantgegevens. Op basis hiervan besloot D om de structuur van de webshop dubbel uit te voeren en de omgeving met klantgegevens nog beter te beveiligen.

AANBEVELING 2: Breng de kroonjuwelen in kaart

- Neem als bestuur het initiatief bij het identificeren en classificeren van de kroonjuwelen.
- Stel vast waar ze zich bevinden, welke afhankelijkheden er bestaan en wie toegang heeft.
- Bekijk de kansen en bedreigingen niet alleen vanuit de organisatie, maar ook vanuit het perspectief van kwaadwillenden:
  - Wie heeft interesse in de kroonjuwelen en waarom?
  - Waar bevinden zich de kroonjuwelen en bestaat hier een afhankelijkheid van bijvoorbeeld externe leveranciers en partners?
  - Welke methodes en technieken zullen kwaadwillenden gebruiken om toegang tot de kroonjuwelen te krijgen of deze te verstoren?
- Prioriteer de maatregelen op basis van waarde en risico. Met dit inzicht kan een organisatie investeren in maatregelen die optimaal bijdragen aan de bescherming van kroonjuwelen en verlaging van het risicoprofiel.

Signaal 3 |
De zwakste schakel

Cybersecurity risico's ontstaan niet alleen vanuit de techniek. Vaak blijken medewerkers de zwakste schakel in de beveiligingsketen te zijn. Aanvallers maken gebruik van social engineering om medewerkers ertoe te brengen bedrijfskritische gegevens met hen te delen.

Social engineering is een opkomende trend bij aanvallen op organisaties. Via psychologische manipulatie wordt gebruik gemaakt van de goedgelovigheid en welwillendheid van medewerkers. Hackers passen het toe, omdat de slagingskans relatief groot is en het minder technische kennis vereist dan bij andere aanvallen. Enkele voorbeelden van social engineering zijn:

- *Baiting:* een aanvaller laat met kwaadaardige software (malware) besmette hardware achter op een plek waar deze zeker wordt gevonden. Vaak in de vorm van usb-sticks. De malware wordt geïnstalleerd zodra de hardware wordt aangesloten op het bedrijfsnetwerk.
- *Phishing:* het versturen van frauduleuze email, waarbij de afzender betrouwbaar overkomt.
- *Spear phishing:* gelijk aan phishing, waarbij er een maatwerk email gestuurd naar een specifiek bedrijf of zelfs een specifieke medewerker.
- *Quid pro quo:* Voor wat hoort wat, de aanvaller biedt iets aan (korting, waardebon) in ruil voor persoonlijke informatie zoals inloggegevens.
- *Spam:* met hagel geschoten junk email. Er zijn nog altijd mensen die hierin trappen.
- *Tailgating:* Een aanvaller loopt achter een medewerker aan in een beveiligde omgeving, vaak door de beveiligingspoort bij de ingang van een kantoor. Soms met de boodschap dat hij zijn toegangspas is vergeten of verloren.

Door gericht te werk te gaan met voor de medewerker vertrouwde templates, URL's, namen van collega's en bedrijfsjargon, wordt vertrouwen gewonnen. Vaak met gebruik van een fictieve autoriteit, tijdsdruk of hebzucht van de medewerker. Het resultaat van een geslaagde aanval is dat de hacker over bedrijfsgegevens beschikt waarmee hij schadelijke acties kan uitvoeren. Bijvoorbeeld het onttrekken van privacygevoelige informatie of het frauduleus overmaken van geld.

Door het toenemend gebruik van mobiele apparatuur, cloud opslag en flexibele werkplekken vervagen de grenzen van de traditionele kantooromgeving. Het onderscheid tussen een kantoorwerkplek, thuiswerkplek of werkplek in een internetcafé valt steeds moeilijker te maken. Deze andere manier van werken vraagt om een geheel nieuwe aanpak voor databeveiliging en een vergrote bewustwording voor social engineering.

De risicocultuur bepaalt hoe een organisatie met dergelijke risico's omgaat. De risico's van social engineering zijn toepasbaar op elke medewerker en dienen bij iedereen bekend te zijn. Om een organisatie nog verder bewust te maken van de risico's, is het goed om concreet aan de slag te gaan met de risicocultuur. Dit start met het onderkennen van de risico's die de organisatie loopt. Door gerichte training en simulatie van social engineering wordt de bewustwording vergroot. Er dient een duidelijke structuur te zijn voor het melden van incidenten. In de praktijk blijkt dat nog veel meldingen gedaan worden, zonder dat adequate opvolging plaatsvindt.

De rol van het bestuur is cruciaal. Naast het goede voorbeeld moeten bestuurders de juiste toon zetten. Zo wordt bewustwording bij de medewerkers vergroot en ontstaat een sfeer waarin zij elkaar aanspreken op risico's. Juist gedrag moet positief gestimuleerd worden. Het bestuur moet de cultuur en het gedrag in de organisatie op het gebied van cybersecurity voortdurend laten testen, meten, evalueren en verbeteren.

Negatief voorbeeld

Dan zal het wel goed zijn

Medewerker E krijgt een maand nadat hij in dienst is een email van personeelszaken waarin wordt gemeld dat er gegevens ontbreken. De email komt vanuit een emailadres met een vreemde extensie en vraagt om zijn naam, geboortedatum en kopie paspoort. Vreemd, denkt E. Hij had deze gegevens bij zijn indiensttreding toch doorgegeven? E doet navraag bij collega's om zich heen en het blijkt dat zij allen dezelfde email hebben gehad. Dan zal het wel goed zijn denkt E en hij verstuurt zijn gegevens. Een week later kan hij niet meer inloggen in zijn account. Zijn wachtwoord blijkt te zijn gestolen en een hacker heeft onder zijn naam toegang tot het bedrijfssysteem.

Positief voorbeeld

Stank voor dank voorkomen

Veel medewerkers van bedrijf F krijgen een email van een webwinkel met het bericht dat zij een eindejaarskado van 25 euro mogen uitzoeken van hun werkgever. Om gebruik te maken van de actie kan op de link in de email worden geklikt en een actiecode worden opgegeven. Enkele medewerkers vertrouwen de email niet: het afzendadres heeft vreemde letters, niet iedere medewerker blijkt de email te hebben ontvangen en de actie is niet vooraf kenbaar gemaakt. Argwanend informeren de medewerkers bij de security officer. Na onderzoek blijkt de email een poging tot social engineering te zijn. Door alert reageren en snelle actie is erger voorkomen.

AANBEVELING 3: Besteed ook aandacht aan cultuur en gedrag

- Realiseer dat cybersecurity meer is dan alleen ICT en techniek, de menselijke factor speelt een grote rol. Besteed daarom voldoende aandacht aan cultuur en gedrag in het risicomodel.
- Zet als bestuur de juiste toon op het gebied van cybersecurity. Beloon positief gedrag. Laat cultuur en gedrag ten aanzien van cybersecurity testen, meten, evalueren en verbeteren.
- Social engineering kan iedereen overkomen. Zorg ervoor dat alle medewerkers bekend zijn met dit fenomeen. Organiseer voorlichtingsbijeenkomsten, opleidingen of berichtgeving op het intranet. Hanteer concrete voorbeelden, zo worden situaties met social enginering door medewerkers sneller herkend. Zorg ook voor een duidelijk meldpunt in de organisatie.
- Neem elke melding over pogingen tot social engineering serieus. Een lakse houding of het nalaten van terugkoppelingen kan ertoe leiden dat incidenten niet meer worden gemeld.
- Vormen van social engineering veranderen continu. Social engineering moet daarom een vast onderdeel vormen in de risicoanalyse en risicocultuur van de organisatie. De effectiviteit van het risicomanagement op dit gebied dient voortdurend te worden getest en geëvalueerd.

Signaal 4 | Incasseren en reageren

Organisaties moeten digitaal weerbaar worden, om ze minder kwetsbaar te laten zijn voor cybercrime. Preventieve maatregelen alleen voldoen niet, detectie en response moeten meer aandacht krijgen. Ook bij de interne en openbare accountant.

De bescherming van kroonjuwelen vraagt om een juiste combinatie van beveiligingsmaatregelen. Bij verschillende grote hacks afgelopen jaren is gebleken dat organisaties nog teveel steunden op alleen preventie. De gedachte dat steeds hogere muren leiden tot een honderd procent veilig fort is achterhaald. Medewerkers zitten niet te wachten op nog meer lastige en complexe maatregelen. Organisaties moeten accepteren dat ze een keer worden gehackt of dat zelfs al zijn. Maatregelen gericht op detectie en response zijn daarom steeds belangrijker.

Opsporing is lastig wanneer men niet weet waarnaar gezocht wordt. Het identificeren van kroonjuwelen en mogelijke bedreigingen is een goed startpunt. Op grond hiervan kunnen scenario's gedefinieerd worden die potentiële aanvallers bewandelen. Het is belangrijk dat detectie niet alleen wordt ingericht op de buitengrenzen van de organisatie, maar ook op de toegangspaden tot de kroonjuwelen. Dit geeft de beste kans om mogelijke indringers vroegtijdig te signaleren.

Om succesvol indringers tegen te gaan, dienen detectie maatregelen ongewenst gedrag zo spoedig mogelijk te signaleren. De inrichting van een veiligheidscentrum (security operating center) is aan te bevelen, dat dagelijks meldingen verzamelt en vergelijkt met vooraf vastgelegde scenario's. Zodra een signaal wordt ontvangen komt het response team in actie. Dit team gaat in korte tijd na of het een incident betreft of een valse melding. Bij een incident wordt getracht zoveel mogelijk informatie te verzamelen, om een risico inschatting te maken en vervolgstappen te bepalen. Vastgestelde scenario's en actieplannen zorgen ervoor dat dit gestroomlijnd en efficiënt plaatsvindt. Naast deze scenario's, actieplannen en handboeken is ook de training in het afhandelen van incidenten belangrijk. Niet alleen de medewerkers van het security operating center moeten opgeleid worden, maar ook de leden van het organisatiebrede crisisteam en zelfs de top van de organisatie.

Een volledig bemand security operating center en goed getraind response team zijn niet goedkoop. Niet alle organisaties hebben de mensen en middelen om dit zelf in te richten. De markt biedt gelukkig uitkomst. Verschillende organisaties bieden detectie en response capaciteit aan via abonnementsystemen.

Een nieuwe trend is het jagen naar mogelijke incidenten. Het detecteren van incidenten gebeurt op basis van vooraf gedefinieerde scenario's en dreigingen. De jagers, zogenaamde hunting teams richten zich op het identificeren van onregelmatigheden en afwijkingen in de ontvangen security meldingen. Een afwijking die niet direct wordt geïdentificeerd kan een mogelijke inbraak zijn. Onregelmatigheden worden opgespoord en inbraakscenario's bijgesteld. Een ander voorbeeld van preventief onderzoek betreft red teaming oefeningen. Dit zijn testen uitgevoerd door externe cybersecurity specialisten om de werking van de aanwezige beveiliging te toetsen.

Het is van belang dat de accountant zich bewust is van de noodzaak van niet alleen preventieve, maar ook detectie en response maatregelen. De jaarlijkse accountantscontrole richt zich veelal op de effectiviteit van de preventieve maatregelen en bijbehorende processen. De meerwaarde van de controle wordt vergroot door ook de detectie en response capaciteit te toetsen. Als de accountant hiervoor niet voldoende is toegerust, moet hij samenwerken met specialisten.

Negatief voorbeeld

Zuinigheid bedriegt de wijsheid

Voor de verkoop van zijn producten beschikt ondernemer G over een webshop. G beheert de website zelf. Vanuit het content management systeem kan G gemakkelijk producten toevoegen en prijzen aanpassen. G heeft geen enkel idee wat op de achtergrond gebeurt, van techniek heeft hij geen verstand. Een fysieke scan van de bestanden van de webshop doet hij ook niet. Hierdoor heeft G niet in de gaten dat hackers wekenlang het betaalverkeer loggen. De creditkaart gegevens van alle klanten worden gehackt. Ze komen voor iedereen leesbaar op zijn website te staan.

Positief voorbeeld

Op tijd ontdekt

Mkb ondernemer H heeft zijn volledige administratie uitbesteed aan zijn accountant X. Voor het voeren van de administratie maakt X gebruik van de nieuwste digitale technieken. Mutaties van de bankrekening worden door de accountant geheel geautomatiseerd verwerkt. Ten overvloede controleert H ook zelf dagelijks de mutaties. Op een dag ontdekt H dat hij het slachtoffer is geworden van skimmen. Door de dagelijkse controle blijft de schade beperkt en stelt de bank hem schadeloos.

AANBEVELING 4: Vergroot de digitale weerbaarheid

- Accepteer dat cybercrime een inherent risico is, dat behoort bij de activiteiten en risico's van de organisatie. Het organisatie- en risicomanagement moeten hierop ingericht zijn.
- Stel de kroonjuwelen centraal bij de maatregelen tegen cybercrime. Geef naast preventie ook voldoende aandacht aan detectie en response capaciteit.
- Vergroot de digitale weerbaarheid in de gehele organisatie, van de werkvloer tot de directie. Zorg voor bewustwording en opleiding. Trek lering uit reeds gemelde incidenten.
- Zorg voor voldoende capaciteit om adequaat te kunnen reageren op beveiligingsincidenten. Eventueel kan dit via inhuur worden gerealiseerd. Werk vooraf noodscenario's uit, benoem een crisisteam en draai regelmatig proef om zwakke plekken beter in beeld te krijgen.

Signaal 5 | De jaarrekening bestaat uit bytes

De accountant beoordeelt bij de jaarrekeningcontrole de risico's voor de financiële verslaggeving en de continuïteit. Daaronder vallen ook cybercrime en cybersecurity. Dit betekent dat de accountant oog moet hebben voor de beheersmaatregelen op het gebied van data integriteit en beveiliging.

Een cyber aanval kan een organisatie direct of indirect raken. Van een directe impact is bijvoorbeeld sprake als een operationeel proces wordt aangevallen. Dit kan gebeuren via een DDoS aanval, het hacken van vertrouwelijke gegevens of frauduleuze transacties. De indirecte impact is vaak groter. Voorbeelden zijn diefstal van intellectueel eigendom, het verlies van klanten en omzet door reputatieschade, claims van gedupeerden of boetes van externe toezichthouders. Aanvullend zijn er kosten voor (forensisch) onderzoek, juridisch advies en het herstel van de schade.

Zowel direct als indirect kunnen cyberaanvallen gevolgen hebben voor de financiële verslaggeving en de continuiteit van de organisatie. Het is daarom noodzakelijk dat de accountant in zijn risicoanalyse expliciet aandacht besteedt aan cybersecurity. Vanzelfsprekend betreft dit risico's gerelateerd aan programma's en applicaties. Maar ook de gehele infrastructuur moet erbij worden betrokken . Deze wordt steeds complexer door virtuele werkplekken, cloud opslag, mobiele oplossingen en internetkoppelingen. De accountant moet zich afvragen of hij wel in staat is om zelfstandig een oordeel te geven over digitale risico's en maatregelen. Behoort dit tot zijn expertise of moet hij specialisten inschakelen?

Bij een verhoogd cyberrisico kan de accountant in de controleaanpak aanvullende werkzaamheden opnemen. Deze richten zich op gebieden waarvan de accountant inschat dat sprake is van verhoogd risico. Het is belangrijk dat deze werkzaamheden aansluiten bij de werkwijze van de hackers, om lekken zo goed mogelijk op te sporen. Ze zijn daarom sterk technisch georiënteerd. Voorbeelden zijn penetratietesten, de beoordeling van security log files en het uitvoeren van red teaming oefeningen.

Standaard moet de accountant in zijn controle aandacht besteden aan de ICT beveiliging. Het is echter niet voldoende om te steunen op alleen opzet en bestaan. De beveiliging moet continu op orde zijn en de data integriteit gewaarborgd. Er moet monitoring plaatsvinden om eventueel misbruik van zwakheden snel op te sporen (via de aanpak: prevent-detect-react). De belangrijkste conclusies op het gebied van cybersecurity in de organisatie moeten worden opgenomen in het accountantsverslag (management letter). Volgens artikel 2:393 lid 4 Burgerlijk Wetboek moet de accountant daarin ten minste melding maken van zijn bevindingen over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

De accountant zal zijn bevindingen ook bespreken met het bestuur en de toezichthouder (Raad van Commissarissen of Raad van Toezicht). Het ligt voor de hand dat hij jaarlijks nagaat, in hoeverre zijn bevindingen opvolging hebben gekregen. Door in de managementletter ook actuele risico's op het gebied van cybersecurity te vermelden, kan hij invulling geven aan zijn natuurlijke adviesfunctie.

3 De NBA ledengroep Intern en Overheidsaccountants publiceert mei 2016 het maturity model informatiebeveiliging. Dit model geeft inzicht in welke informatiebeveiligingsmaatregelen noodzakelijk zijn en welke maatregelen per niveau verwacht mogen worden.

Negatief voorbeeld

Kijk verder dan de jaarrekening

Accountant Y is verantwoordelijk voor de jaarrekeningcontrole van salarisverwerker I. Y heeft vooral de applicaties voor de salarisverwerking meegenomen bij de beoordeling van de financiële gegevens. Hij besteedt beperkt aandacht voor de onderliggende infrastructuur. Hackers weten deze te hacken en toegang te krijgen tot de databases. Data van de medewerkers van klanten worden grootschalig op internet gezet. Daardoor zegt een groot aantal klanten hun contract op bij I. Het is onduidelijk sinds wanneer de hackers actief waren. De media vragen zich af waarom Y niet meer aandacht heeft besteed aan cybersecurity.

Positief voorbeeld

Een onverwachte uitkomst

Accountant Z besluit als onderdeel van de jaarrekeningcontrole een hackerstest bij onderneming J te doen. Het bestuur van J stemt hiermee in. De cybersecurity specialisten van Z proberen de webomgeving van J binnen te komen zonder de medewerker van J te informeren. De hackerstest is succesvol en de specialisten kunnen grote financiële transacties doorvoeren in de systemen. Tijdens de test worden ook sporen gevonden van echte hackers. Direct wordt nader onderzoek uitgevoerd. Hackers blijken frauduleuze transacties te hebben uitgevoerd. Hierdoor zijn vele miljoenen euro's verdwenen. De systemen zijn gemanipuleerd om ontdekking te voorkomen. Op basis van het onderzoek van Z wordt de beveiliging verbeterd en zijn de financiële transacties gecorrigeerd.

AANBEVELING 5: Zorg voor voldoende cyber kennis bij de controle

- Deel cliënten in naar hun mogelijke cybersecurity risico (laag/midden/hoog). Pas op basis van deze classificatie de controleaanpak aan. Realiseer hierbij dat de indirecte impact van een beveiligingsincident veel groter kan zijn dan de directe impact. De totale schade dient een organisatie zo snel mogelijk te kunnen vaststellen.
- De controle aanpak moet zich niet alleen richten op de (administratieve) applicaties. Ook het toetsen of de juiste beveiligingsmaatregelen in de technische infrastructuur zijn aangebracht moet onderdeel zijn van de controle aanpak
- Stel gerichte cybersecurity vragen aan de cliënt, bijvoorbeeld:
  - Weet de organisatie wat de belangrijkste cyberrisico's zijn?
  - Weet de organisatie wat haar kroonjuwelen zijn?
  - Is het cybersecurity management ingericht om de belangrijkste risico's voor de organisatie te verkleinen en de kroonjuwelen te beschermen?
  - Heeft de organisatie de technologie, processen en mensen om aanvallen tijdig te detecteren en adequaat hierop te reageren? Is een security operating center ingericht?
  - Is incident management ingericht om snel te kunnen reageren op een incident (instellen multidisciplinair team, waaronder ICT, communicatie, operations, juridisch)?
  - Laat de organisatie de cybersecurity regelmatig en op alle onderdelen testen?
- Definieer aangepaste testwerkzaamheden voor die gebieden waar onvoldoende preventieve en/of reactieve beveiligingsmaatregelen zijn aangebracht. Voeg zonodig cyberspecialisten toe aan het controleteam of schakel expertise in.
- Neem de belangrijkste conclusies over cybersecurity op in de management letter. Evalueer elk jaar in hoeverre aan de conclusies van het voorgaande jaar opvolging is gegeven.


WORD
CRACKER
RE
CYBER
ENCRYPTION
TROJAN
IDENTITY
R
THEFT
PRIVACY
S
ITRUSION
DETECTION

Reacties van belanghebbenden

Onderstaande belanghebbenden hebben op verzoek gereageerd op de publieke managementletter.
Hun reacties zijn integraal opgenomen in dit hoofdstuk.

CSR Cyber Security Raad

Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5555
E contact@nctv.minvenj.nl

NBA
T.a.v. Drs. R.B.M. Mul MPA
Postbus 7984
1008 AD Amsterdam

Contactpersoon
mw. drs. E.C. van den Heuvel
Secretaris CSR
T 06-51095594
E e.c.van.den.heuvel@minvenj.nl

Den Haag, 6 april 2016

Betreft: Reactie publieke managementletter cybersecurity

Geachte heer Mul,

Hierbij ontvangt u de reactie van de Cyber Security Raad op de publieke managementletter cybersecurity van de NBA (beroepsorganisatie van accountants). De Cyber Security Raad dankt u voor de gelegenheid om te kunnen reageren en is verheugd dat uw beroepsgroep aandacht besteedt aan dit belangrijke onderwerp.

De CSR is het eens met de bevindingen in uw rapport dat cybersecurity een onderwerp voor de boardroom is. De CSR heeft eind 2014 de 'Handreiking cybersecurity voor bestuurders' gepubliceerd (bijlage 1). Ten aanzien van de inhoud van uw managementletter willen wij u een aantal aanvullende suggesties op het gebied van cybersecurity aan de hand doen.

Signaal 1: Onderwerp voor de bestuurskamer
Het is een juiste veronderstelling dat 100% digitale veiligheid niet haalbaar is. Organisaties moeten daarom vaststellen wat zij een aanvaardbaar cybersecurityniveau vinden. Als gevolg van het geheel of gedeeltelijk uitbesteden van IT-diensten of -beheer moet niet het beeld ontstaan dat daarmee ook de verantwoordelijkheid voor cybersecurity wordt uitbesteed. De organisatie blijft verantwoordelijk en daarom moeten de verantwoordelijkheden op alle niveaus en in de keten goed belegd en geregeld zijn. Het bestuur geeft hieraan strategisch sturing, bij voorkeur aan de hand van een (interne) lijnrapportage over relevante cybersecurity onderwerpen.

De focus van de bestuurskamer ligt echter niet alleen op het voorkomen van een cybersecurityincident, maar ook op het omgaan met een incident of calamiteit en het regelen van het herstel.
Toezien op een goede implementatie en naleving van de bestaande wet- en regelgeving, zoals de Meldplicht datalekken en de privacywetgeving, behoort ook tot de verantwoordelijkheden van de boardroom. Bedrijven en organisaties binnen de vitale infrastructuur hebben extra verantwoordelijkheden.

Een groot aantal bedrijven kampt met legacy problemen die niet of nauwelijks zijn op te lossen. Deze problematiek heeft onder andere betrekking op sterk verouderde softwareprogramma's die cruciale bedrijfsprocessen aansturen en waarvan vervanging complex en kostbaar is. Niet alleen het vervangen kan complex zijn ook het patchen (tegengaan van kwetsbaarheden) van dergelijke software kan van directe invloed zijn op de business continuïty. Bedrijven dienen zich bewust te zijn van hun legacy problematiek en daar een passend beleid op te ontwikkelen.

Signaal 2: Het draait om kroonjuwelen
Bedrijven moeten bij het bepalen van de kroonjuwelen het besef hebben welke informatie waardevol kan zijn voor kwaadwillenden. De cyber criminelen variëren van individuele hackers die het voor de roem doen tot statelijke actoren. Een bedrijf kan dus meer kroonjuwelen bezitten dan het zich in eerste instantie realiseert. Informatie kan al snel interessant zijn voor de cyber criminelen. Dit geldt ook voor statelijke actoren. Denk bijvoorbeeld aan Intellectual Property Rights (IPR).

Signaal 3: De zwakste schakel
Het management heeft een voorbeeldfunctie als het gaat om cybersecure handelen. De dreiging kan variëren van onwetende medewerkers die op phisingmails klikken of onbeveiligde USB sticks in computers stoppen tot gerichte acties van (ex) medewerkers Deze laatste categorie de zogenoemde 'Insider threat' is een serieuze bedreiging voor bedrijven. De onderneming moet een beleid hebben dat deze bedreiging tot een minimum terugbrengt. Wanneer medewerkers een andere functie binnen het bedrijf krijgen, moet er opnieuw naar hun autorisaties worden gekeken. Ook moeten paswoorden van systemen regelmatig worden vernieuwd. De menselijke factor blijkt in de praktijk telkens weer een zwakke schakel te zijn als het op cybersecurity aankomt.
Maar de mens is zeker niet de enige zwakke schakel. Bedrijven maken over het algemeen onderdeel uit van een keten. Ook in deze keten kunnen zwakke schakels zitten. Leveranciers die zich niet aan bepaalde basisnormen houden, kunnen een bedreiging voor de organisatie vormen. Cybersecurity in de keten verdient daarom voldoende aandacht. Bij veel bedrijven staat dit onderwerp echter nog niet op de agenda. Het stellen van (minimum) eisen aan leveranciers, het opnemen van cybersecurity-eisen in de inkoopvoorwaarden en het werken met bepaalde standaarden is aanbevelenswaardig.
Het regelmatig houden van cyber-incidentoefeningen en het daarbij betrekken van de belangrijkste stakeholders kan helpen om de bewustwording onder medewerkers te verhogen en de benodigde afspraken scherp op het netvlies te krijgen. Ook verbetert een oefening het crisismanagement en de crisiscommunicatie tijdens een incident.

Signaal 4: Incasseren en reageren

Organisaties worden weerbaarder door onderlinge samenwerking en informatie-uitwisseling op het terrein van cybersecurity. Binnen Nederland lopen al verschikkende initiatieven op dit gebied. Enkele voorbeelden zijn de alterteringsservice van het NCSC , het Nationaal Detectie Netwerk , en diverse overleggen binnen vitale sectoren.

Het mitigeren van cyberaanvallen zou ook tot het handelingsarsenaal van een organisatie moeten behoren. Evenals het tot op zekere hoogte afwenden van DDoS-aanvallen die de dienstverlening voor langere tijd kunnen stilleggen.
Het opsporen van hackers is geen eenvoudige zaak. Desondanks zou het doen van aangifte tot de standaardprocedure moeten behoren.

De CSR onderschrijft dat cybersecurity een belangrijk onderwerp is voor accountants om mee te nemen in een audit en mogelijk zelfs in de beroepsopleiding. Aangezien cybersecurity een dynamisch onderwerp is, adviseren wij enige standaardisatie aan te brengen in het cybersecurity-auditproces, zodat iedereen precies weet wat d eisen zijn en wat er verwacht wordt.

Wij onderschrijven de toegevoegde waarde een actieve rol van de accountant op het terrein van cybersecurity in de boardroom.

Hoogachtend,

Drs. E. Blok Dick Schoof

Co-voorzitters Cyber Security Raad

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Nederlandse Beroepsorganisatie van
Accountants, t.a.v. dhr. drs. R. Mul MPA,
Hoofd afd. Beroepsontwikkeling & Beleid,
Postbus 7984,
1008 AD AMSTERDAM

Datum : dinsdag 5 april 2016
Kenmerk : NOREA2016/AB-wo19
Betreft : Reactie publieke managementletter (PML) Cybersecurity NBA

Geachte heer Mul,

NOREA heeft grote waardering voor de poging van NBA om maatschappelijk relevante risico's te signaleren en daarmee het onderwerp cybersecurity nadrukkelijk op de agenda van bestuurders en managers te plaatsen.

De natuurlijke rol voor de accountant wordt in de publieke managementletter gemotiveerd vanuit zijn controleperspectief waarbij tevens is vermeld: 'de belangrijkste rol voor de accountant ligt misschien wel in zijn natuurlijke adviesfunctie'. Dit is ons inziens een ietwat (te) vrijblijvende rolopvatting. Immers, de accountant is verantwoordelijk voor het verwerven van inzicht in het informatiesysteem van de organisatie met inbegrip van de risico's voortkomend uit de ICT[1]. Ook moet hij eventuele bevindingen rapporteren in verband met de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking[2]. Ontoereikende informatiebeveiliging vormt daarvoor een belangrijk risico. De hoge automatiseringsgraad van ondernemingen en hyperconnectiviteit van onze samenleving ('Internet of Things') vergt specifieke expertise op het domein van cybersecurity.

Deze expertise reikt verder dan adviseren over informatiebeveiliging en cybersecurity en het rapporteren van risico's. Organisaties moeten voorbereid zijn op de gevolgen van en communicatie over cyberincidenten, zodat door adequate respons en eventueel herstel van vitale bedrijfsinformatie de continuïteit van de onderneming niet in gevaar komt.

[1] COS 315 (18 en 21)
[2] Artikel 2:393, lid 4 Burgerlijk Wetboek

POSTADRES
POSTBUS 7984
1008 AD AMSTERDAM

BEZOEKADRES
ANTONIO VIVALDISTRAAT 2-8
1083 HP AMSTERDAM

E-MAIL EN WEBSITE
NOREA@NOREA.NL
WWW.NOREA.NL

OVERIG
TEL: 00 31 (0)20 301 03 80
KVK-NR: 40537540
IBAN: NL02ABNA0475165403

Wil de accountant berekend zijn op deze taak dan zal hij zich deze expertise eigen moeten maken of waarborgen dat voldoende IT-audit expertise in zijn controleteam vertegenwoordigd is. Bij de meeste (middel)grote accountantskantoren en auditdiensten zijn IT-auditors aangesteld, die kunnen worden ingezet om adequaat te adviseren over vraagstukken inzake informatiebeveiliging en cybersecurity.

Onder Aanbeveling 1: 'Stel als bestuur de juiste vragen' wordt gevraagd naar de interne organisatie op het gebied van cybersecurity en de inrichting van de eerste en tweedelijns defensie. In dat verband bepleiten we ook nadrukkelijk aandacht voor de interne audit als 'derdelijns defensie', waarbij de externe auditor ook nog vanuit zijn perspectief kan oordelen of adviseren over de mate waarin de organisatie adequaat is voorbereid op risico's.

Bij het in kaart brengen van de 'Kroonjuwelen' (Signaal 2) is het inderdaad van belang om de waardevolle bronnen, technologieën en processen van de onderneming te onderkennen maar vooral belangrijk is het bepalen van de juiste scope en risicoanalyse als vertrekpunt voor het informatiebeveiligingsbeleid. Dat geldt te meer naarmate de automatiseringsgraad hoger is en bijvoorbeeld sprake is van industriële procesbesturing of systemen voor gebouwbeheersing.

Door de NOREA is een hulpmiddel (Cybersecurity Assessment) ontwikkeld, waarmee op hoofdlijnen de risico's rondom cybercrime in kaart gebracht kunnen worden. Daarnaast is door NOREA een website ingericht met informatie over de meldplicht datalekken (Allesoverdatalekken.nl), omdat voor ondernemingen ook als gevolg daarvan grote (d.w.z. materiële) risico's kunnen ontstaan.

Cybersecurity is een belangrijk thema en vergt een intensieve aanpak, in welk verband NOREA graag bereid is tot samenwerking met auditors van verschillende disciplines.

Met vriendelijke groet,

namens het bestuur,

drs. J. E. Biekart RE RA,
Voorzitter.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS


Phishing

Colofon

Kennis delen
In het NBA beleidsprogramma Kennis Delen wordt de kennis van accountants collectief ingezet om vroegtijdig risico's te signaleren in maatschappelijke sectoren of relevante thema's. Het accent ligt hierbij op risico's op het gebied van bestuur, bedrijfsvoering, verslaggeving en controle.

In deze publieke managementletter (PML) presenteert de NBA 5 aanbevelingen voor het thema Cybersecurity. Dit thema is het zestiende onderwerp dat door de Signaleringsraad van de NBA is geselecteerd. Een werkgroep van openbaar accountants en adviseurs betrokken bij het thema heeft geanonimiseerde bevindingen verzameld en bediscussieerd. Daarna is dit besproken in een bijeenkomst met belanghebbenden. De Signaleringsraad heeft de signalen vervolgens maatschappelijk geijkt. Belanghebbenden bij het thema zijn bereid gevonden om schriftelijk op de PML te reageren. De coördinatie en eindredactie waren in handen van het programmateam Kennis Delen.

Meer informatie
Een publieke managementletter is één van de publicatievormen van het beleidsprogramma Kennis Delen. Daarnaast verschijnen ook open brieven of discussierapporten. Inmiddels heeft de NBA de volgende publicaties uitgebracht:

- 2015: Curatieve zorg en Horeca
- 2014: Life Sciences en Banken
- 2013: MBO scholen, Risicomanagement en Transport en Logistiek
- 2012: Gemeenten, Toon aan de Top en Goede Doelen
- 2011: Commercieel Vastgoed, Pensioenen en Glastuinbouw
- 2010: Verzekeringen en Langdurige Zorg

Alle publicaties zijn openbaar en bedoeld voor een breed publiek.

Signaleringsraad
prof. dr. mr. Frans van der Wel RA (voorzitter)
Gineke Bossema RA
Johan van Hall RA RE
Mr. Charlotte Insinger MBA
Leon van den Nieuwenhuijzen RA
Carel Verdiesen AA

Expertgroep Cybersecurity
drs. Tony de Bos RA RE CEH (EY)
ing. John Hermans RE (KPMG)
ir. Bram van Tiel RE (PwC)
drs. Marko van Zwam RE (Deloitte)

Programmateam Kennis Delen
drs. Robert Mul MPA (programmaleider)
Michèl Admiraal RA (eindredacteur)
Jacques Urlus RE CISA (coördinator)
drs. Jenny Dankbaar (secretariaat)

De afgelopen vijf jaar bracht de NBA vijftien Publieke Managementletters (PMLs) uit, gericht op bepaalde sectoren of specifieke thema's.

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
F 020 301 03 02
E nba@nba.nl
I www.nba.nl