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 rapport willen wij u bij een aantal signalen suggesties aan de hand doen.

Signaal 1: Onderwerp voor de bestuurskamer
Het is een juiste veronderstelling dat 100% digitale veiligheid niet haalbaar is. Bestuurders moeten daarom vaststellen wat zij een aanvaardbaar cybersecurityniveau vinden. Door 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 verantwoordelijkheden moeten op alle niveaus en in de keten goed belegd en geregeld zijn. Het bestuur geeft hieraan strategisch sturing, bijvoorbeeld aan de hand van een (interne) lijnrapportage over onderwerpen die te maken hebben met cybersecurity. Denk bijvoorbeeld aan patchbeleid. Hoe is dat geregeld om kwetsbaarheden in software te verhelpen? Wie neemt de beslissing als er conflicterende belangen zijn?

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.

Een groot aantal bedrijven kampt met legacyproblemen die niet of nauwelijks zijn op te lossen. Deze problematiek heeft onder andere betrekking op sterk verouderde softwareprogramma's die cruciale bedrijfsprocessen aansturen en niet zo maar kunnen worden vervangen. Het patchen van dergelijke software kan zeer ingewikkeld zijn en van directe invloed zijn op de business continuïty. Bedrijven dienen zich bewust te zijn van hun legacyproblematiek 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. Een bedrijf kan dus *meer* kroonjuwelen bezitten dan in eerste instantie wordt gedacht. Informatie is al snel interessant voor criminelen, zeker als zij de informatie kunnen combineren met informatie die zij uit andere (digitale) bronnen weten te verkrijgen.

Signaal 3: De zwakste schakel
Het management heeft een voorbeeldfunctie als het gaat om cybersecure handelen. 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
De accountant is geen cybersecurityspecialist. Daarom is het betrekken van deskundigen bij de audit iets wat de CSR toejuicht. Het gebruikmaken van bestaande initiatieven kan helpen om de organisatie weerbaarder te maken tegen cybercrime. Ik denk dan bijvoorbeeld aan de Information Sharing and Analysing Centers (ISAC's) die per sector cybercrime gerelateerde informatie delen, alerteringen van het Nationaal Cyber Security Centrum en het Nationaal Detectie Netwerk om anoniem informatie over cyberaanvallen te delen.
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 wensen u succes met de publicatie van de managementletter en bij het auditen op cybersecurity.

Hoogachtend,

Drs. E. Blok
Co-voorzitter Cyber Security Raad