EY Focus op Fraude

Cybercrime en -security
Key take-aways 15 mei 2023

Building a better working world

Op 15 mei vond de tweede editie van EY Focus op Fraude plaats. Deze sessie maakt deel uit van een serie rondetafelgesprekken waarin we deze keer met onze gasten in gesprek gingen over cybercrime en -security.

Tijdens het vorige webinar werd duidelijk dat er meer aandacht voor cybercriminaliteit nodig is. Digitalisering biedt kansen, maar brengt ook risico's met zich mee. Als EY vinden we het belangrijk om hierover in debat te gaan en kennis te delen om dit belangrijke, maatschappelijke probleem aan te pakken. Moderator Joep Stassen en EY assurance bestuurder Auke de Bos trapten het webinar af en toonden de eerste uitkomsten van een korte survey onder de deelnemers. Ook daaruit bleek dat het onderwerp niet voor niets op de agenda staat: 25% van de respondenten of de bedrijven waar zij werken, zijn wel eens slachtoffer van cybercrime geworden.

Cybercriminaliteit groeit explosief

Dr. Sander Zeijlemaker en Jatin Sehgal gaven vervolgens een introductie waarin ze het huidige cyberlandschap schetsten:

- Doordat de wereld steeds meer digitaal verbonden is, bevindt cybercriminaliteit zich op een hoogtepunt. Naar verwachting zal cybercriminaliteit de maatschappij wereldwijd dit jaar 8 biljoen dollar kosten en in 2025 zelfs uitgroeien tot 10,5 biljoen dollar.
- Uit onderzoek blijkt dat hackers gebruik maken van een breed scala van aanvalsmethoden, met in de top 4 Denial of Service-aanvallen, malware, ransomware en phishing. Dagelijks worden zelfs bijna 3 miljard phishing-e-mails verstuurd.
- Hackers beginnen vaak met het identificeren en verkrijgen van details over een doelwit, bepaalde patronen, werktijden, sociale media-activiteiten, locatiegegevens en andere (persoonlijke) informatie, waarmee zij vervolgens heel gericht te werk kunnen gaan.
- De ‘threat actors’ komen overigens niet altijd van buiten de organisatie; maar liefst 20% van de bedreigingen komt van binnenuit of met hulp van personen die bekend zijn met de organisatie en fysieke of logische toegang hebben.
- De ‘human factor’ moet sowieso niet onderschat worden – bijvoorbeeld qua awareness voor het niet klikken op kwaadaardige links, maar ook als het gaat om keuzes die worden gemaakt in het ontwerp van applicaties en systemen, beschikbaar stellen van budget en al dan niet treffen van beheersingsmaatregelen.

Bescherming tegen cybercriminaliteit

De constatering is dat dit onderwerp zeker op bestuursniveau besproken moet worden. Het World Economic Forum identificeert cybercriminaliteit als een van de top 10 wereldwijde risico's, op korte en lange termijn. Ook verschijnt op verschillende niveaus wet- en regelgeving die betrouwbare en veilige technologie afdwingt.

Jatin en Sander gaven de bestuursleden onder de kijkers gelijk een stappenplan mee:

- Stap 1: Breng het specifieke dreigingslandschap van de organisatie in kaart, inclusief de risico’s met betrekking tot derden, leveranciers en klanten;
- Stap 2: Beoordeel de maatregelen die deze risico’s moeten beheersen en of deze voldoen;
- Stap 3: Zorg dat er een detectiemechanisme om cyberaanvallen tijdig te ontdekken aanwezig is. Het kost organisaties gemiddeld meer dan 275 dagen om een inbreuk te ontdekken en dat is simpelweg veel te lang.

- Stap 4: overtuig je ervan dat er naast ‘identify’, ‘protect’ en ‘detect’ mechanismes een goede ‘response & recovery’ aanwezig is (en oefen dit).

Te meer omdat de kosten van een datalek gemiddeld ongeveer 4,35 miljoen dollar bedragen en voor beursgenoteerde bedrijven nog hoger liggen. Daarom is ook de juiste mindset aan de top en eronder belangrijk. Beveiliging moet integraal onderdeel zijn van de bedrijfsvoering. Proactiviteit is daarbij het kernwoord, aangezien het technologische en geopolitieke landschap continu verandert.

En dat geldt niet alleen voor grote bedrijven. Ook kleine organisaties moeten waakzaam zijn, want cybercriminelen maken hierin geen onderscheid en houden van makkelijke doelwitten.

Datadiefstal

Sjoerd Bakker heeft persoonlijk de gevolgen van een cyberaanval bij zijn bedrijf Ticketcounter ervaren. Daar werden klantgegevens gestolen en Sjoerd werd als directeur tijdens deze stressvolle periode afgeperst om bitcoins te betalen. Hij besloot dat echter niet te doen, deed aangifte en informeerde snel zijn partners en hun klanten, om op die manier de wapenen uit handen van de criminelen weg te nemen. Ook stelde Ticketcounter ‘frequently asked questions’ op en bouwde het een tool waarmee klanten konden zien of hun gegevens ook gestolen waren. Ondanks nog verdere bedreigingen door de hackers richting Sjoerd, pakte het uiteindelijk goed uit. Klanten reageerden geschrokken, maar waardeerden de openheid en de geboden ondersteuning. Transparant is hij nu ook over zijn ervaringen, zodat andere organisaties daarvan kunnen leren. Sjoerd noemt het incident overigens geen datalek meer maar datadiefstal, net zoals de politie dat doet, want onderaan de streep is gewoon sprake van een criminele activiteit. Hij heeft zijn les geleerd en is er bewuster mee bezig. Hij heeft maatregelen getroffen en bijvoorbeeld voor extra bewustwording in zijn organisatie een ISO-certificering gehaald. Zijn verhaal kan worden gezien als een good practice waar een ieder van kan leren.

Altijd op de agenda

In het rondetafelgesprek dat volgde, gingen Arjen Dorland, Commissaris bij o.a. ABN Amro en Essent, Peter Kornelisse, Partner Technology Risk EY Nederland en vanuit zijn rol betrokken bij ‘cyber in the audit’, Rudrani Djwalapersad, Partner Cybersecurity EY Nederland en vooral actief in het adviseren en ondersteunen van organisaties, en wederom Sjoerd Bakker in op de rollen die verschillende partijen hebben en hun belangrijkste aandachtspunten op het gebied van cybersecurity.

In de eerder genoemde survey geeft 51% van de respondenten aan dat bedrijven cybercrime en cybersecurity volgens hen onvoldoende serieus nemen. Dat is schokkend. Het strookt gelukkig niet met de ervaringen van Arjen als commissaris, die merkt dat het onderwerp vaak op de agenda staat. Commissarissen moeten proactief zijn en niet wachten tot een incident plaatsvindt. Zij kunnen informatie op verschillende plekken verkrijgen, naast van bestuurders bijvoorbeeld ook van de accountant en internal audit of de ondernemingsraad.

Accountants hebben ook een rol bij cybercrime en -security. Als onderdeel van de controle kijkt de accountant naar de cyberrisico en de wijze waarop deze worden beheerst door onder meer naar de ‘logical access’ procedures te kijken in het kader van de jaarrekeningcontrole.

Het is echter niet zo dat accountants een specifieke opdracht hebben om beveiliging van een onderneming te testen door bijvoorbeeld penetratietesten uit te voeren. Er zijn wel initiatieven voor meer transparantie en mogelijke assurance hierbij. Een initiatief vanuit NOREA, de beroepsorganisatie van IT-auditors wil komen tot een IT-beheersverslag en IT-verklaring. Hierbij is het management primair aan zet.

Nogmaals werd bevestigd dat cybersecurity onderdeel moet zijn van de business en verankerd moet zijn in de organisatie, gedreven vanuit inherente motivatie en vanuit een *security by design* gedachte. Ook al is de *return on investment* niet direct zichtbaar, de impact en schade bij een incident kunnen enorm zijn en de afgelopen jaren is meermaals gebleken dat 'black swan events' zich daadwerkelijk voor kunnen doen. Het denken in scenario's kan bedrijven daarbij helpen. Op basis van de kenmerken van het bedrijf, de producten, et cetera de kroonjuwelen identificeren en bepalen welke scenario's *most likely* zijn, om vervolgens keuzes te kunnen maken en te focussen op wat het belangrijkst is. De respons is vervolgens een combinatie van maatregelen, van awarenesstraining voor phishing tot inspelen op bekende (technische) kwetsbaarheden en toetsing door bijvoorbeeld penetration testing. Dat alles in de wetenschap dat 100% beveiligen niet mogelijk is en weerbaarheid, zoals genoemd, dus essentieel is.
Organisaties die het uiteindelijk het beste doen zijn organisaties met een 'beveiligingscultuur', die zich kwetsbaar durven opstellen en een governance hebben die hen in staat stelt goed geïnformeerd te zijn en goed aan te kunnen sturen.

Tijdens de discussie kwamen ook diverse concrete tips aan de orde, waaronder:

- Betrek medewerkers uit de business bij cybersecurity.
- Heb oog voor voldoende detectiemaatregelen, omdat (en specifiek waar) de preventie niet waterdicht is, bijvoorbeeld rond de logische toegangsbeveiliging.
- Maak rapportages aan bestuurders en commissarissen niet te technisch, voor commissarissen gaat het om inzicht in zaken als de grootste risico's, waar het bedrijf staat en of genoeg gedaan en geïnvesteerd wordt.
- Goede managementinformatie is 'integraal' en omvat de volgende elementen:
    - Inzicht in bestaande restrisico's
    - Inzicht in ontwikkelende dreigingen en wat daaraan wordt gedaan
    - De effectiviteit van getroffen maatregelen
    - Incidenten (ook die goed zijn afgevangen, want dat geeft informatie over de weerbaarheid van de organisatie)
    - Verbeterprogramma's (en of die de essentie voor de komende 3 tot 12 maanden wel omvatten)
- Vertrouw niet op aannames, maar krijg daadwerkelijk inzicht in de implementatie en effectiviteit van de cybersecurity, ook als gebruik wordt gemaakt van externe diensten, zoals 'de cloud'.
- Ga na of jouw organisatie een onwijzigbare back-up heeft, die criminelen dus niet ook kunnen aanpassen of vernietigen (iets dat noodzakelijk is voor de weerbaarheid, maar lang niet bij alle organisaties bekend)
- Zorg voor de juiste expertise en voldoende challenge, binnenshuis, maar bijvoorbeeld ook door experts van buiten te betrekken – zij overzien vaak het gehele speelveld

- Sta open voor risico's van binnenuit en ga er vanuit dat ethiek even niet bestaat – denk aan het screenen van medewerkers voor zij toegang krijgen tot gevoelige informatie, maar ook het voorkomen van het gebruik van gedeelde accounts.

Ter afsluiting, het mag duidelijk zijn dat cybersecurity hoog op de agenda dient te staan van bestuurders en commissarissen. Dat het niet alleen een technisch onderwerp is waar IT-specialisten een belangrijke rol hebben, maar ook dat het een bepaalde cultuur binnen organisaties vereist. Wees niet naïef dat het je niet zal overkomen. Want het lijkt niet de vraag of je met cybercrime te maken krijgt, maar veel meer wanneer en dat vraagt om voldoende aandacht voor dit onderwerp.

Voor de gehele discussie, meer tips en meer achtergrond is de volledige replay van het webinar beschikbaar.

Het volgende Focus op Fraude webinar staat gepland op 9 oktober en gaat over Greenwashing. We hopen u dan weer te mogen verwelkomen.

Gasten:
Arjen Dorland
Voorzitter RvC Bovemij, Vice-voorzitter RvC ABN Amro en Essent

Dr. Sander Zeijlemaker
Directeur Disem Institute, Research affiliate cybersecurity MIT Sloan, agenda contributor World Economic Forum

Sjoerd Bakker
Algemeen directeur en co-owner Ticketcounter

Rudrani Djwalapersad
Partner Cybersecurity EY Nederland

Peter Kornelisse
Partner Technology Risk EY Nederland

Jatin Sehgal
Partner Cybersecurity EY Nederland