Deel 1
Informatie-beveiliging

Digitalisering en IT

Top 3 onderwerpen voor toezichthouders

De meeste commissarissen hebben weinig kennis van en ervaring met digitalisering en IT, blijkt uit recent onderzoek van NR Governance. In de update van de Code Corporate Governance wordt hier echter expliciet aandacht voor gevraagd.

Arnoud Klerkx schreef *Digitalisering en IT voor commissarissen en toezichthouders* en legt hierin helder uit wat 'digitaal' en 'IT' inhouden. Zijn 'Digi&IT cockpit' geeft aan op welke onderwerpen commissarissen toezicht dienen te houden en welke vragen zij daarover kunnen stellen.

Tijdens Klerkx' colleges bij commissarissen-opleidingen hebben commissarissen steevast over drie items veel vragen: informatiebeveiliging, grote IT-projecten en digitale disruptie. Voor *Goed Bestuur & Toezicht* gaat hij hier in drie artikelen op in. In dit eerste deel: informatiebeveiliging.

Arnoud Klerkx is lid RvB bij de Kramp Groep als Chief Digital Officer. Hij heeft ervaring in managementadviesrollen (Accenture en Gartner), directieposities (Robeco, Ziggo en Sanoma Learning) en als commissaris (Habion, Kruitbosch/Cortina). Hij is auteur van diverse (wetenschappelijke) artikelen over Toezicht op IT en docent bij de commissarissenopleiding van de Erasmus Universiteit en de Governance University. In 2015 werd hij verkozen tot CIO van het jaar.

Informatiebeveiliging staat bij menig commissaris met stip op 1 als belangrijkste onderwerp voor het toezicht op digitalisering en IT. Elke week staan er bedrijven in de krant die gehackt dan wel gegijzeld zijn. Het is niet meer de vraag óf je gehackt wordt als bedrijf, maar wanneer. Inmiddels kunnen de meeste bedrijven simpelweg niet meer functioneren zonder IT-systemen en raakt een hack dus de continuïteit van de onderneming. En laat dat nu de belangrijkste taak van een commissaris zijn: toezicht houden op de bedrijfscontinuïteit. Veel commissarissen vinden informatiebeveiliging echter een moeilijk en lastig onderwerp[1]. En dat is het ook.

Waar bestaat Informatiebeveiliging uit?

Informatiebeveiliging bestaat uit drie lagen.

- De eerste laag is cybersecurity. *Cybersecurity* gaat over de bescherming tegen 'alle ellende op internet'. Die wil je te allen tijde buiten de deur houden. Cybersecurity is al jaren – ook op wereldniveau – oorlog. Rusland, China en de VS vechten in de cyberwereld daadwerkelijk een oorlog uit. Maar ook op bedrijfsniveau is er sprake van grote dreiging. Denk bijvoorbeeld aan een ddos-aanval, waarbij een website door een paar miljoen computers tegelijkertijd wordt bestookt, waardoor deze 'omvalt'. Een ander fenomeen zijn de pfishing e-mails. Deze beogen toegang te krijgen tot je computer of je wachtwoord te ontfutselen. Dit zijn die nep e-mails van bijvoorbeeld banken. Die zien er nu nog vrij beroerd uit, maar over een paar jaar kun je de echte niet meer onderscheiden van nep. En dan heb je nog *deep fake*. Een bekend voorbeeld is dat filmpje van Obama dat echt lijkt, maar het zeker niet is.
- De volgende laag is de *informatiebeveiliging* binnen het bedrijf zelf. Dat gaat bijvoorbeeld over beveiliging tegen spionage, interne fraude en *malware*. Veel mensen denken bij spionage aan films, maar bedrijfsspionage is aan de orde van de dag. Zeker bij bedrijven die veel aan onderzoek doen of belangrijke data hebben, zoals ASML en ziekenhuizen. Ook interne fraude bestaat al heel lang en is met de komst van verschillende IT-systemen alleen maar een grotere bedreiging geworden. En dan is er malware, ofwel dat mailtje met een attachment waar je *niet* op moet klikken. Als je dat wel doet, wordt er een virus geactiveerd. Het bekendste voorbeeld van malware is *ransomware*. Dit virus pakt al je systemen in waardoor je er niet meer mee kunt werken. Vervolgens word je afgeperst (ransom) om ze weer uitpakt te krijgen.
- De derde laag gaat over *business continuity management*, *recovery* of *uitwijk*. Dit zijn de maatregelen die getroffen worden voor het geval er iets misgaat. Wat gebeurt er als er als alle IT-systemen niet meer werken door een

‘De allereerste vraag die een commissaris kan stellen is eenvoudig: wat is het informatiebeveiligingsbeleid en kan dit worden toegelicht?’

overstroming of een ransomware aanval? Hoe zien de komende 24 uur eruit? Heeft het bedrijf van al zijn systemen en data een kopie gemaakt (back-up). Hoe oud is die kopie? En hoe snel kan die werkzaam zijn, zodat iedereen weer aan het werk kan?

Drie vragen die de commissaris moet stellen

Goed toezicht houden op informatiebeveiliging doe je door het stellen van de juiste vragen. De belangrijkste drie vragen die elke commissaris kan stellen over dit onderwerp zijn:

1. Wat is het informatiebeveiligingsbeleid?
2. Wat zijn de grootste risico’s?
3. Wat is de top 10 van security-incidenten van het afgelopen jaar?

Het informatiebeveiligingsbeleid

Stel, je bent eigenaar van een hotel, dat je goed wilt beveiligen tegen dieven en indringers. Daarvoor kun je een aantal *maatregelen* treffen, zoals sloten, camera’s, sensoren of een alarminstallatie.
Bij informatiebeveiliging werkt het net zo. Je begint met het opstellen van een informatiebeveiligingsbeleid. Hierin staan alle maatregelen en controles die een bedrijf inzet om zich te beschermen tegen de uitdagingen uit de eerdergenoemde drie lagen. En daarmee is de allereerste vraag die een commissaris kan stellen eenvoudig: wat is het informatiebeveiligingsbeleid en kan dit worden toegelicht? Hiermee krijgt een commissaris een beeld van de beschermende maatregelen en controles die het bedrijf wil gebruiken. En vervolgens – nog belangrijker – komt de aanvullende vraag: in hoeverre is dat beleid ook daadwerkelijk geïmplementeerd?
Er zijn verschillende maatregelen en controles die een bedrijf kan implementeren. Hiervan is een handig overzicht beschikbaar. Dit is het CSC-18 framework[2]. Dit framework laat de achttien belangrijkste controles en maatregelen zien die een bedrijf zou moeten gebruiken om zichzelf goed te beveiligen. In tabel 1 worden de belangrijkste kort en bondig uitgelegd.

Het is van belang dat de commissarissen weten welke maatregelen een bedrijf wil nemen en in hoeverre deze ook daadwerkelijk zijn geïmplementeerd.
De zwakste schakel van informatiebeveiliging zijn echter niet de systemen, maar de medewerkers. In meer dan 40 procent van alle security-incidenten gaat het mis door de medewerkers zelf. Dat komt omdat zij degenen zijn die op die verkeerde attachments klikken of zich een wachtwoord laten ontfutselen. De belangrijkste maatregel is het opzetten van reguliere zogenoemde *security awareness* campagnes. Hierin worden medewerkers met gefingeerde phishingmails verleid om bijvoorbeeld hun wachtwoord op te geven. De hieruit voortvloeiende leerervaring zorgt ervoor dat ze vervolgens weer scherper blijven opletten. Ook is het aan te bevelen om medewerkers middels permanente educatie op de hoogte te houden van alle ontwikkelingen. Hierdoor blijven ze alert op hun eigen gedrag en leren ze continu waar ze wel of niet op moeten klikken.

Maatregel	Uitleg
Overzicht van hardware en software	Informatiebeveiliging begint met het goed in kaart hebben van alle hardware (computers, laptops, tablets, smartphones et cetera) en alle software die een bedrijf heeft, zodat bekend is wat beveiligd moet worden.
Patching en upgrading	IT-systemen werken hun software regelmatig bij. Dat heet een patch, een soort kleine softwarewijziging. Het is belangrijk om alle patches en upgrades van systemen op tijd en gestructureerd uit te voeren.
Monitoring, detecting en intrusion	Dit zijn systemen die de IT-omgeving in de gaten houden en inbraken signaleren na bijvoorbeeld een software hack.
Account monitoring and logging	Dit zijn systemen die de activiteit in verschillende IT-systemen in de gaten houden en registreren. Bij vreemde activiteit (bijvoorbeeld activiteit op een ongebruikelijk tijdstip) wordt dit gesignaleerd. Onjuist gebruik kan vastgesteld worden door de log files te bekijken waarin staat wie wat in het systeem gedaan heeft.
Toegang (Role Based Access)	Elke medewerker heeft een bepaalde rol in een bedrijf waar toegang tot bepaalde systemen bij hoort. Er is software die deze toegang gestructureerd kan beheren en bijhouden.
Master user accounts	Ook IT heeft vaak een loper die op alle kamers past. Deze worden vaak master of superuser accounts genoemd. De uitgifte en het bezit daarvan moet goed beheerd worden.
Malware protection	Dit soort systemen zijn op de hoogte van de laatste ontwikkelingen en filteren de slechte attachments, e-mails en links al uit de mailbox voordat ze bij de medewerker komen. Ook kunnen ze onbekende links en attachments in een veilige omgeving testen en checken voordat ze beschikbaar komen.
Data en application recovery	Dit zijn systemen die zorgen dat er recente kopieën van de data en systemen zijn, inclusief een uitwijkplan waarin staat beschreven hoe de back-up wordt geactiveerd. Vraag als commissaris niet of dat plan er is, maar vraag of het plan al getest is.
Firewalls	Dit zijn systemen die het bedrijf beschermen bij hackpogingen van buitenaf.
Network compartmentalization	Net als een duikboot kun je een IT-netwerk in meerdere compartimenten indelen zodat onderdelen apart afgegrendeld kunnen worden om in geval van een lek verdere schade te voorkomen.
Penetratie testing	Er zijn ook 'goede hackers'. Hen kan gevraagd worden om te proberen het bedrijf – in opdracht uiteraard – te hacken. Hierdoor kan de kwaliteit van de informatiebeveiliging worden getest.

Tabel 1: De belangrijkste maatregelen uit het CSC-18 framework.

De grootste risico's

Elk bedrijf kent zijn eigen dynamiek en context. Als commissaris wil je weten waar de grootste risico's zitten en in hoeverre het informatiebeveiligingsbeleid hierin afdoende beschermt. Misschien goed om te beseffen dat volledige veiligheid niet bestaat. Het is altijd een afweging tussen risico's, kosten en haalbaarheid. Een bedrijf zou idealiter een complete back-up van al

zijn systemen en data moeten hebben van maximaal vijf minuten oud. Als er dan wat misgaat, ben je alleen maar de data kwijt van de afgelopen vijf minuten. Echter, zo'n hele recente back-up is erg kostbaar. En weegt dat op tegen een back-up van bijvoorbeeld 24 uur oude data die vele malen goedkoper is? Dit vraagt dus om een goede afweging vanuit de directie.
Ook is het van belang om goed te beseffen waar de grootste risico's zitten. Wat zijn de zogenaamde kroonjuwelen die je als bedrijf graag wilt beschermen? Bij een ziekenhuis zijn dit ongetwijfeld de patiëntgegevens. Bij een hightechbedrijf zijn dit mogelijk de onderzoek-, ontwerp- en patentgegevens. Bij een e-commercebedrijf zijn dat de betaalgegevens van zijn klanten. Een luchthaven heeft juist een issue als de IT-systemen die de bagage-afhandeling verzorgen gehackt zouden worden.

Top 10 security incidenten

Ten slotte is er nog een zeer eenvoudige vraag die je als commissaris kunt stellen om toezicht te houden op de informatiebeveiliging. Vraag aan de directie een overzicht van de top 10 van security incidenten van de afgelopen twaalf maanden. Dat zou geen goed gevulde lijst moeten zijn. En al helemaal niet eentje met grote ernstige incidenten. Belangrijk is ook om te vragen in hoeverre er maatregelen genomen zijn die voorkomen dat een bepaald incident zich opnieuw kan voordoen.

Tot slot: de rol van de accountant

Ook de accountant beweegt zich op het terrein van informatiebeveiliging. Het is een onderwerp in de jaarrekeningcontrole, het krijgt aandacht in de management letter en ook in geval van een IT-audit zal de accountant hier uitgebreid naar kijken. Het is wel van belang om je goed te realiseren dat de accountant niet het totale gebied van informatiebeveiliging afdekt. De rol van de accountant is om te kijken naar de financiële verslaglegging en financiële bedrijfscontinuïteit. Hij kijkt daarbij naar alle IT-systemen die daarmee te maken hebben, maar bijvoorbeeld minder (of niet) naar systemen die gebruikt worden door de klantenservice, de webshop of meer operationele systemen.

De enige manier om als commissaris goed toezicht te houden op de informatiebeveiliging, is door het gesprek aan te gaan over het informatiebeveiligingsbeleid en de status van de implementatie ervan. En zoals ook met veel andere onderwerpen, de RvC kan altijd een externe partij het beleid laten reviewen, zodat een beter beeld ontstaat in hoeverre de informatiebeveiliging op orde is en waar de risico's precies liggen.

Bronnen

1-meting digitale transformatie in boardrooms in Nederland, 2022, Nationaal Register.
De Nederlandse Corporate Governance Code 2022, Monitoring Commissie Corporate Governance Code.
Digitalisering en IT voor commissarissen en toezichthouders, Arnoud Klerkx, Boom uitgeverij, 2022 (ISBN97890244528 97).
Toezicht op IT begint met het stellen van de juiste vragen, *Goed Bestuur & Toezicht*, 3 2021 pag. 16, Arnoud Klerkx.

Eindnoten

1 Gebaseerd op meer dan 2500 commissarissen die de module 'Goed toezicht op digitalisering en IT' hebben gevolgd bij onder andere het non-executive program van de Erasmus Universiteit, de commissarissenopleiding bij de Governance University en het board programma van NR Governance.
2 ps://www.cisecurity.org/controls/cis-controls-list.