Cyberrisico's in de Supply-Chain

De onzichtbare vijand

De afgelopen tijd nam het aantal cyberincidenten wereldwijd aanzienlijk toe. Deze incidenten variëren van datalekken tot ransomware-aanvallen en hebben verstrekkende gevolgen voor zowel bedrijven als individuen. De belangrijkste oorzaken? Menselijke fouten door het klikken op phishing links en het gebruik van zwakke wachtwoorden. Verouderde software en systemen die organisaties kwetsbaar maken voor aanvallen. En, in sommige gevallen, nog steeds onvoldoende geïmplementeerde beveiligingsmaatregelen, zoals het ontbreken van tweefactorauthenticatie en monitorings-instrumenten.

Bestuurders en commissarissen/toezichthouders moeten meer kennis van de beheersing van IT hebben. DORA en NIS2 helpen daarbij.
Marc Welters analyseert de risico's en legt uit wat organisaties kunnen doen om die te mitigeren.

Marc Welters is partner IT Audit bij EY en houdt zich bezig met het robuust maken en houden van de beheersing van IT in complexe IT-omgevingen. Daarnaast is hij voorzitter van NOREA (de beroepsgroep van alle in Nederland geregistreerde IT-auditors) en (gast)docent IT audit en IT governance aan VU, Nyenrode, UMIO en ESAA.

Menselijke fouten, verouderde software en systemen en onvoldoende beveiligingsmaatregelen zijn de belangrijkste oorzaken voor cyberincidenten. Eerst een paar voorbeelden waar het fout gegaan is.

De retailer en de distributeur
Een cyberaanval in 2021 had aanzienlijke gevolgen voor Albert Heijn: computers werden gehackt bij hun kaasleverancier, waardoor de helft van de vrachtwagens van deze leverancier niet op pad kon. Het gevolg voor de retailer waren drie weken lege schappen waar kaas had moeten liggen, veel media-aandacht, en vervolgens veel onderzoek en aanvullende beveiliging.
Doordat bij de leverancier ransomware was geïnstalleerd, vielen de computersystemen die de kaasleveranties regelen bij de winkels uit. Een voorbeeld van bedrijven die samenwerken in een netwerk of keten, waar een zwakke (beveiligings)schakel in de keten schade kan veroorzaken. Dit voorbeeld laat zien dat naast een goede operationele veerkracht van de eigen organisatie, de maatregelen bij de partners in het business netwerk of keten minstens zo relevant is. Samen doe je business, maar dan moet wel iedereen meedoen. Commissarissen zullen zeggen: 'Albert Heijn had de IT-beheersing wel op orde.' Dat is nog maar de vraag. Als Albert Heijn een bank was geweest en de outsourceprovider die de IT van de bank beheert zou zijn gehackt, dan had die bank niet meer bestaan. Het had tot een bankrun geleid omdat spaarders niet meer bij hun geld konden.

In deze casus zijn de gevolgen op de gebieden van privacy (gevoelige gegevens), de eventuele juridische gevolgen van het niet kunnen naleven van contracten en de daaruitvolgende boetes en rechtszaken, evenals het verlies van concurrentievoordeel (bedrijfsgeheimen/intellectueel eigendom) niet meegewogen. Het betrof 'slechts' kaas.
In november 2024 was Albert Heijn zelf het doelwit van een cyberaanval in de USA. Systemen voor e-commerce werden offline gehaald, creditcardbetalingen in de winkels konden niet plaatsvinden, online bestellingen moesten tijdelijk worden stopgezet.

Meer recente voorbeelden zijn:
- TU Delft (januari 2025)
  Een cyberaanval op het netwerk, de impact was niet heel groot.
- TU Eindhoven (januari 2025)
  Een cyberaanval op het netwerk, sommige onderwijsactiviteiten zijn tijdelijk stopgezet.
- Centric (januari 2025)
  In december 2024 wisten cybercriminelen in te breken bij Centric via een kwetsbaarheid in de software van een Amerikaanse leverancier van bestandsoverdrachtsoftware. De aanval werd pas in januari 2025 bekend.

- Gemeenteraad Almere (januari 2025)
  De website van de gemeenteraad van Almere werd gehackt, waardoor mogelijk persoonlijke gegevens zijn gestolen. De aanval werd ontdekt toen de website onbereikbaar werd.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (maart 2025)
  Op 13 maart waren DigiD en aanverwante diensten zoals DigiD Machtigen, BSNk, Digipoort en MijnOverheid tijdelijk beperkt beschikbaar door een cyberaanval.

Het belang van operationele veerkracht in de gehele keten

Operationele veerkracht is het vermogen van een organisatie om effectief te reageren op verstoringen en zich aan te passen aan veranderende omstandigheden, terwijl de kernactiviteiten en dienstverlening worden voortgezet. Daar moet een aantal zaken voor geregeld worden. Zoals een proactieve planning, robuuste infrastructuren en flexibele processen die de continuïteit van de bedrijfsvoering waarborgen, ongeacht de aard van de verstoring, zoals cyberincidenten, natuurrampen of economische schommelingen. De dienstverlening aan de keten(s) (of netwerken van organisaties) waarvan deel wordt uitgemaakt moet doorgang vinden, ook in geval van een verstoring of incident. De bestuurders moeten de governance daarop inrichten. Bestuurders moeten in dit geval weten wat er is uitbesteed, aan wie maar vooral ook aan welke onderaannemer achter de eigen outsourceprovider, en welke risico's worden gelopen bij deze uitbesteding. En vooral: hoe houden we grip op die risico's?

'Wanneer een IT-systeem van een ketenpartner faalt, kan dit domino-effecten veroorzaken die de hele supply chain ontwrichten'

Waar gaat het fout in de IT-keten?

De verknoopte IT-systemen maken de supply chain kwetsbaar voor cyberaanvallen. Hackers kunnen toegang krijgen tot gevoelige bedrijfsinformatie en deze informatie misbruiken, wat kan leiden tot financiële verliezen en reputatieschade. Wanneer een IT-systeem van een ketenpartner faalt, kan dit domino-effecten veroorzaken die de hele supply chain ontwrichten. Het gevolg kan zijn dat orders vertragen, de productie stilvalt en klanten niet tijdig bediend worden. De integriteit van data is cruciaal. Fouten of corruptie in gedeelde gegevens kunnen leiden tot verkeerde beslissingen, inefficiënties en zelfs juridische problemen. Het waarborgen van accurate en betrouwbare data-uitwisseling is daarom essentieel. Met de toenemende regelgeving rondom data privacy en bescherming moeten bedrijven zorgen dat hun IT-systemen voldoen aan de wetgeving. Schendingen kunnen leiden tot zware boetes en juridische complicaties. De afhankelijkheid van externe IT-leveranciers betekent dat problemen bij deze leveranciers directe gevolgen kunnen hebben voor de eigen bedrijfsvoering. Het is belangrijk dat bestuurders een goede governance regelen die waarborgt dat de organisatie robuuste overeenkomsten en noodplannen ontwikkelt om deze risico's te mitigeren. Door zich

bewust te zijn van de risico's en proactieve maatregelen te nemen, kunnen bedrijven de voordelen van IT-integratie in hun supply chain maximaliseren, terwijl ze de potentiële nadelen minimaliseren.

Wat kun je eraan doen?

De governance moet van reactief (brandjes blussen) naar proactief, en de bestuurders zijn verantwoordelijk voor deze ommezwaai. Een proactieve aanpak stelt bedrijven in staat om de bedrijfsvoering aan te passen aan de omstandigheden, en kansen te benutten die voortvloeien uit veranderende omstandigheden, in plaats van alleen te reageren op crises, lees: brandjes blussen. Zo moeten de Business Impact Analyses (BIA's) op orde zijn waardoor duidelijk is hoelang IT uit de lucht mag zijn voordat de business pijn voelt. Veel organisaties weten niet hoelang dit mag. Door Digital Operational Resilience Act (DORA) en Network and Information Security Directive (NIS2) na te leven moeten organisaties die wel bepalen en vastleggen.

Het belang van operationele veerkracht zit in het beschermen van de reputatie. Snel kunnen herstellen na een incident geeft klanten vertrouwen, versterkt de geloofwaardigheid van het bedrijf in de markt. En niet in het minste belang: het zorgt voor de continuïteit van de organisatie.

Bestuurders die regelen dat operationele veerkracht een speerpunt wordt van de governance, kunnen hun intellectueel eigendom en bedrijfsgeheimen beter beschermen tegen diefstal. Dit helpt bij het behouden van concurrentievoordeel omdat het voorkomt dat gevoelige informatie in handen van concurrenten valt. Een bedrijf dat veerkrachtig is en snel kan reageren op incidenten, kan een hogere klanttevredenheid en -loyaliteit bereiken. Klanten waarderen de betrouwbaarheid en het vermogen van het bedrijf om ononderbroken diensten te leveren. Dit bevordert klantretentie en daarmee het zakelijk succes.

De geopolitiek maakt het niet makkelijker

Geopolitieke verschuivingen spelen een rol in de operationele veerkracht van bedrijven. Politieke instabiliteit en economische sancties die leiden tot internationale handelsconflicten zijn recente geopolitieke verschuivingen. Bedrijven die actief zijn in gebieden met politieke instabiliteit moeten voorbereid zijn op mogelijke verstoringen in hun supply chain en operationele processen. Proactieve planning en diversificatie van leveranciers kunnen helpen bij het mitigeren van deze risico's.

Economische sancties, opgelegd door regeringen, kunnen de toegang tot markten en grondstoffen beperken. Handelsconflicten beperken het vermogen om goederen en diensten te exporteren of importeren. Handelsconflicten kunnen leiden tot tariefverhogingen, invoerbeperkingen en andere handelsbarrières. Deze conflicten verhogen de kosten van grondstoffen en producten, verlagen de winstgevendheid en verstoren de supply chain. Bedrijven moeten flexibel zijn en bereid zijn om hun strategieën aan te passen aan veranderende handelsregels en voorwaarden. Geopolitieke spanningen kunnen ook leiden tot verhoogde cybersecuritybedreigingen, zoals door een staat gesponsorde cyberaanvallen en spionage. Bedrijven moeten robuuste cybersecuritymaatregelen implementeren om hun systemen en gegevens te beschermen tegen cyberaanvallen.

Samenvattend, de bestuurders moeten de veranderende geopolitieke factoren betrekken bij het herijken van de governance, omdat geopolitiek een aanzienlijke impact op de operationele veerkracht van bedrijven heeft. Door zich bewust te zijn van de mogelijke risico's en proactief maatregelen te nemen, kunnen organisaties hun continuïteit en succes waarborgen. Tevens laat het zien dat goederen en diensten voortkomen uit een keten of netwerk, daarmee is het van belang om de onderlinge afhankelijkheid in het samenwerkingsverband in kaart te brengen. De IT maakt hiervan een belangrijk onderdeel uit. Vanwege de hoge mate van data-uitwisseling is de IT-infrastructuur onderling verregaand aan elkaar gekoppeld, de IT is min of meer verknoopt. En dan is het maar de vraag of iedere deelnemer zijn verantwoordelijkheden voor de IT-beveiliging voldoende heeft ingevuld, zodat het geheel goed beveiligd is tegen cyberaanvallen, of andere incidenten. Het goed in kaart brengen van de IT-keten is een eerste en zeer belangrijke stap. Het verhogen van de weerbaarheid van organisaties hangt af van deze eerste inventariserende stap.

De digitale operationele veerkracht

De toezichthouders De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM) geven ieder op hun eigen wijze invulling aan toezicht. Beide organisaties doen onderzoek en geven bevindingen en aanbevelingen op het gebied van verbetering van operationele veerkracht voor met name organisaties in de financiële sector. Hierna volgen recente uitingen van de DNB en AFM waar bestuurders kennis van kunnen nemen voor het verder regelen van de governance.
DNB[1] benadrukt het belang van het in kaart

'De governance moet van reactief (brandjes blussen) naar proactief, en de bestuurders zijn verantwoordelijk voor deze ommezwaai'

brengen van de IT-keten, vooral in het kader van de nieuwe Europese verordening, DORA. Volgens DORA moeten financiële ondernemingen in kaart brengen welke IT-leveranciers zij gebruiken en hoe weerbaar deze partijen zijn. Dit helpt bij het identificeren van zwakke plekken in de keten en het verbeteren van de cyberweerbaarheid. Daarnaast is het belangrijk dat financiële instellingen goed zicht hebben op de beheersing van risico's in de gehele uitbestedingsketen, omdat een cyberaanval zich vaak richt op de zwakste schakel.

De AFM heeft de afgelopen jaren onderzoeken uitgevoerd bij beleggingsondernemingen, beheerders van beleggingsinstellingen en beheerders van ICBE's (Instelling voor Collectieve Belegging in Effecten) naar uitbesteding in de asset managementsector in brede zin. De AFM heeft hiermee een beeld gekregen van de materiële werkzaamheden die worden uitgevoerd door derde partijen en de beheersmaatregelen die ondernemingen daarbij treffen ('Keten In Beeld').
De AFM rapporteert op basis van hun onderzoek het volgende als belangrijkste bevindingen (bron AFM[2]):

- Ondernemingen hebben niet altijd een goed onderbouwde aanpak ten aanzien van het bepalen van wat gezien moet worden als uitbesteding en welke uitbesteding kwalificeert als materieel.

- Bij de inrichting van uitbestedingen denken ondernemingen vaak nog te beperkt na over maatregelen en afspraken die voorsorteren op een passende monitoring.
- Ondernemingen gaan zeer verschillend om met de monitoring van uitbestedingen; een meer consistente en uitlegbare aanpak op grond van risico's is noodzakelijk.
- Voor intra-groep uitbestedingen wordt vaak (te) veel geleund op informele maatregelen en afspraken.
- Ondernemingen zijn zich niet altijd bewust van ICT-componenten in uitbestedingen en de bijbehorende ICT-risico's.

Gebaseerd op dit onderzoek formuleert de AFM twintig aanbevelingen voor verbetering van de situatie. Deze zijn opgenomen in hun rapport.

Het vaststellen van de digitale operationele veerkracht

De bestuurders moeten het initiatief nemen voor het in kaart brengen en versterken van de (digitale) operationele veerkracht. Het vaststellen van de digitale operationele veerkracht van een bedrijf begint met een grondige evaluatie van de huidige IT-infrastructuur en processen. Dit omvat het identificeren van alle IT-leveranciers en het beoordelen van hun individuele weerbaarheid. Vervolgens moeten de risico's binnen de gehele uitbestedingsketen in kaart worden gebracht en beheersmaatregelen worden geïmplementeerd om de cyberweerbaarheid te verhogen.

Opvolgend aan de implementatiefase is het van belang om een gedegen monitoringaanpak te ontwikkelen, waarbij zowel formele als informele maatregelen worden afgestemd op de specifieke ICT-componenten en risico's. Hierover dient instemming en afstemming plaats te vinden met de IT-leveranciers omdat het de risico's betreft binnen de gehele uitbestedingsketen. Een effectieve aanpak omvat het aanbrengen van structuur. Dit kan bijvoorbeeld door middel van kwaliteitsframeworks en risicobeheersystemen die een gestructureerde benaderingen bieden voor risicobeheer, compliance en continue verbetering.

Kwaliteitsframeworks en Risicobeheer

Om risico's aan te pakken kan gebruik worden gemaakt van verschillende kwaliteitsframeworks die ieder een eigen werkingsgebied hebben, zoals ISO-standaarden. ISO 31000[3] helpt organisaties bij het identificeren, beoordelen en beheren van risico's op een systematische manier. Met ISO 22301[4] kunnen organisaties robuuste plannen ontwikkelen om verstoringen, zoals die veroorzaakt door handelsconflicten en economische sancties, effectief aan te pakken en hun kritieke bedrijfsprocessen te waarborgen. ISO 27001[5] biedt een raamwerk voor het implementeren van een Information Security Management System (ISMS). Dit helpt bedrijven bij het beschermen van hun informatie en systemen tegen cyberaanvallen en het handhaven van de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens.

Interne audits

Interne audits helpen organisaties bij het monitoren van hun compliance met interne policies en externe regelgeving. Deze audits identificeren verbeterpunten en zorgen ervoor dat managementsystemen effectief functioneren.

Assurance Rapporten[6] – bijvoorbeeld ISAE3402[7] en SOC2[8] rapporten
Assurance rapporten zijn essentieel om de effectiviteit van de bovengenoemde kwaliteitsframeworks en risicobeheerprocessen te evalueren en te verbeteren. De assurance rapporten bieden onafhankelijke beoordelingen van de naleving van normen, de prestaties van managementsystemen, en de robuustheid van risicobeheerstrategieën.

Door deze kwaliteitsframeworks te integreren in hun bedrijfsvoering, en door assurance rapporten te gebruiken voor continue evaluatie en verbetering, kunnen organisaties proactieve maatregelen nemen om de impact van geopolitieke risico's te minimaliseren en hun operationele veerkracht te versterken.

Het is belangrijk te benadrukken dat assurance rapporten gebaseerd zijn op gegevens en analyses uit het verleden, en derhalve geen garanties bieden voor toekomstige prestaties of compliance. Deze rapporten geven een mate van zekerheid van de effectiviteit van kwaliteitsframeworks en risicobeheerprocessen over een periode in het verleden.
Desondanks bieden assurance rapporten aanzienlijke voordelen:

- Inzicht en transparantie: assurance rapporten leveren waardevolle inzichten in de naleving van normen en de prestaties van managementsystemen, waardoor organisaties een duidelijk beeld krijgen van hun huidige situatie.
- Verbetering van processen: door zwakke punten en gebieden die verbetering behoeven te identificeren, stellen assurance rapporten organisaties in staat om gerichte maatregelen te nemen om hun systemen en processen te versterken.
- Vertrouwen en geloofwaardigheid: onafhankelijke externe audits en assurance rapporten helpen bedrijven hun geloofwaardigheid te vergroten en het vertrouwen van stakeholders te winnen door te laten zien dat ze voldoen aan erkende normen en 'good practices'.
- Risicobeheer: deze rapporten ondersteunen organisaties bij het identificeren en beheersen van potentiële risico's, waardoor ze proactief maatregelen kunnen nemen om de impact van de risico's te minimaliseren.
- Certificering: externe assurance rapporten zijn vaak een voorwaarde voor het verkrijgen van officiële certificeringen, wat kan bijdragen aan het verbeteren van de marktpositie en het voldoen aan klantverwachtingen.

Conclusie

Een effectieve governance over de IT-keten is essentieel, het draagt bij aan de langetermijnbestendigheid van de keten, en is de optimale wijze om risico's in de keten te managen. Ieder bedrijf in de keten dient te worden betrokken en actief te participeren, omdat de hele keten daarvan profiteert.

Noten

1 https://www.dnb.nl/voor-de-sector/open-boek-toezicht/wet-regelgeving/dora/
2 https://www.afm.nl/~/profmedia/files/rapporten/2024/rapport-uitbestedingen.pdf
3 https://www.iso.org/standard/65694.html
4 https://www.iso.org/standard/75106.html
5 https://www.iso.org/standard/27001
6 https://www.nba.nl/wet--en-regelgeving/hra/1619/7285/8331/8376
7 https://www.iaasb.org/publications/staff-overview-international-standard-assurance-engagements-isae-3402-assurance-reports-controls
8 https://www.norea.nl/uploads/bfile/87b07304-10b1-4b36-9976-fd34165c3513