AUDIT MAGAZINE

ARTIKELEN | 1 SEPTEMBER 2022

KETENRISICOBEHEERSING MOET VOLWASSEN DISCIPLINE WORDEN

Auteur: Bram Ketting - Jelle Groenendaal
Beeld: Jackson - Simmer - Alexander Sinn - Mika Baumeister - Thomas Lefebvre
Leestijd: 6 min

Grote en kleine organisaties worden steeds meer afhankelijk van (ICT-)diensten van derden, maar zijn nog maar beperkt bezig met de beheersing van risico's die daardoor kunnen ontstaan. Auditors kunnen een belangrijke aanjagende rol vervullen bij het (verder) professionaliseren van deze risicodiscipline binnen organisaties.

In dit artikel vijf redenen waarom ketenrisicobeheersing volwassen(er) moet worden. We zullen deze redenen larderen met ICT-gerelateerde voorbeelden, al zien we in onze praktijk dat ze ook van toepassing zijn op proces- en productieketens. Tot slot geven we enkele tips hoe auditors concreet kunnen bijdragen aan een verdere professionalisering van de ketenrisicobeheersingsdiscipline.

Langere en complexere ketens

Steeds meer organisaties zijn voor hun functioneren in grote mate afhankelijk van derde partijen. Neem bijvoorbeeld verzekeraars. Volgens De Nederlandsche Bank (DNB) besteden verzekeraars ICT-oplossingen ondersteunend aan een

of meerdere kritieke bedrijfsprocessen steeds vaker uit. Daarnaast kiezen zij ervoor om (delen) van hun primaire bedrijfsproces volledig uit handen te geven, zoals de schadeafhandeling, het onderhouden van klantrelaties en de administratie.

Deze toegenomen afhankelijkheid van en verwevenheid met derde partijen maakt dat organisaties kwetsbaarder worden voor verstoringen of informatiebeveiligingsincidenten ergens in de keten. Ketenrisicobeheersing wordt daarmee belangrijker voor de continuïteit en kwaliteit van de dienstverlening.

Uitbestedingsketens van kritieke bedrijfsprocessen kunnen uit meerdere schakels bestaan. Deze schakels bevinden zich veelal in verschillende landen met andere wet- en regelgeving

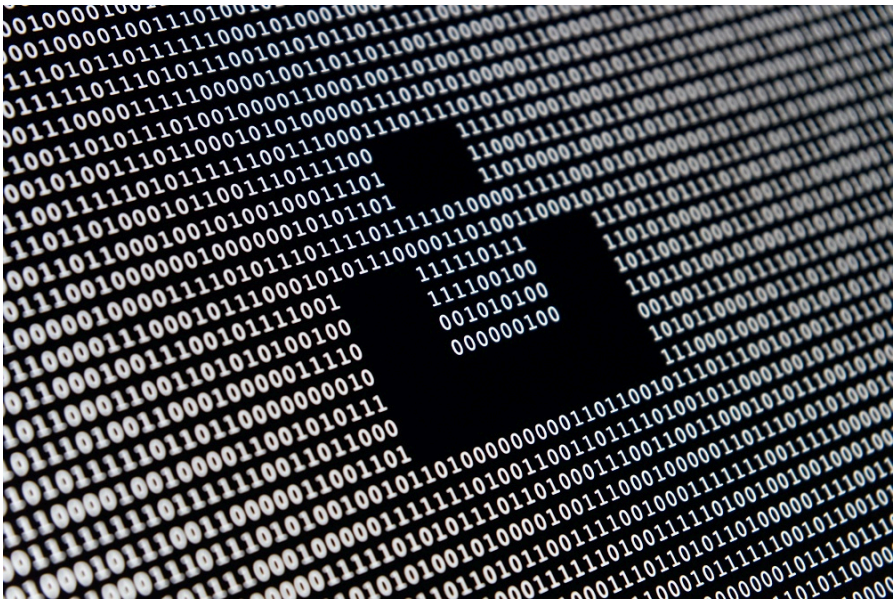
Bovendien worden de uitbestedingsketens steeds langer (en daardoor) complexer. Serviceproviders die diensten leveren aan organisaties besteden zelf vaak ook een deel van het werk uit aan derde partijen. Dit betekent dat uitbestedingsketens van kritieke bedrijfsprocessen uit meerdere schakels kunnen bestaan. Een complicerende factor is dat deze schakels zich veelal in verschillende landen begeven met andere wet- en regelgeving.

Inzicht in en beheersing van ketenrisico's wordt dus steeds ingewikkelder. Dit vraagt daarom om meer inspanning vanuit organisaties en de juiste ondersteunende technologie om dit voor elkaar te krijgen.

Toename van incidenten

Volgens het Europees Agentschap voor Cyber Security (ENISA) zijn ketenaanvallen of supply chain attacks een van de grootste cyberdreigingen van dit moment. SolarWinds is wellicht een van de meeste bekende ketenaanvallen van de afgelopen jaren. Aanvallers voegden een kwaadaardige code toe aan een software update van SolarWinds. Hierdoor kregen de aanvallers toegang tot alle klanten van SolarWinds die deze update hadden uitgevoerd. Onder de klanten van SolarWinds bevonden zich de Amerikaanse overheid, het Europese Parlement en vele grote internationale bedrijven.

Een ander en meer recentelijk voorbeeld is de Okta-aanval. Aanvallers wisten de systemen van Okta binnen te komen door middel van een gecompromitteerd systeem van een derde partij die de klantenservice verzorgde. Eenmaal binnen hadden de aanvallers weer toegang tot een deel van de systemen van twee klanten van Okta.



Beide voorbeelden laten zien dat organisaties zeer kwetsbaar kunnen zijn voor aanvallen die plaatsvinden via een derde partij en dat deze risico's actief beheerst moeten worden. Ook al heb je in dergelijke gevallen als organisatie geen directe invloed op het incident- en crisismanagement van de gecompromitteerde derde partij, wel kun je zelf risicobeperkende maatregelen nemen zoals het afsluiten van netwerkverbindingen met de derde partij en het proactief informeren van klanten en medewerkers.

Bestaande en aanstaande wet- en regelgeving

Organisaties die gebruik (willen) maken van buitenlandse ICT-dienstverleners moeten nu al anticiperen op bestaande wet- en regelgeving (denk aan de Amerikaanse Patriot Act) en de risico's hiervan beoordelen en mitigeren. Daarnaast worden er op Europees niveau verschillende nieuwe initiatieven ontplooid om organisaties te bewegen om meer aandacht te besteden aan ICT-ketenrisicobeheersing.

NIS-2

In de in 2022 door het Europese Parlement goedgekeurde Network and Information Security (NIS-2) directive wordt nadrukkelijk aandacht besteed aan ketenrisicobeheersing. Artikel 43 stelt bijvoorbeeld dat organisaties die essentiële maatschappelijke diensten leveren, moeten beoordelen of de cybersecurity van derde partijen en serviceproviders voldoende is. Artikel 45 eist van dezelfde organisaties dat zij de cybersecurity van derde partijen die data verwerken (bijvoorbeeld voor analyticsdoeleinden) grondig beoordelen en indien nodig passende maatregelen (laten) nemen. Onderdeel van de voorgestelde NIS-2 directive is om lidstaten de mogelijkheid te geven om boetes uit te delen aan organisaties die niet voldoen aan de vereisten. Medio 2024 wordt de NIS-2 directive doorgevoerd in Nederlandse wetgeving.

DORA

Specifiek voor financiële instellingen is de Digital Operational Resilience Act (DORA) aanstaande. Deze voorgestelde wet bevat maar liefst veertien artikelen waarin tot in detail wordt beschreven wat financiële instellingen moeten doen om ICT-risico's van derde aanbieders te beheersen. Hieronder valt onder andere een uitgebreid due diligence assessment bij aanvang van het contract en risicogestuurde monitoring om te beoordelen of derde partijen blijven voldoen aan de in het contract vastgelegde afspraken.

Organisaties die investeren in een volwassen ketenrisicobeheersingsorganisatie kunnen onder de streep voordeliger uit zijn dan organisaties die dit nalaten en maar blijven 'doormodderen'

Regelmatige audits

Voor auditors is het goed te weten dat beide wetgevingen voorschrijven dat ketenrisicobeheersing onderworpen moet worden aan regelmatige audits. Artikel 29 van NIS-2 spreekt bijvoorbeeld over regelmatige audits en gerichte beveiligingsaudits. Artikel 5.7 van DORA stelt dat auditors regelmatig (dat wil zeggen afhankelijk van de ICT-risico's van de financiële entiteit) moeten controleren of financiële instellingen effectief ICT-risico's beheersen, waaronder risico's geïntroduceerd door derde partijen.

Toenemende kosten

Nu de regeldruk rond derde-partijenrisico's vanuit verschillende kanten toeneemt, zullen organisaties moeten accepteren dat de kosten voor (keten)risicobeheersing zullen stijgen. Onze stelling is echter dat organisaties die investeren in een volwassen ketenrisicobeheersingsorganisatie onder de streep voordeliger uit kunnen zijn dan organisaties die dit nalaten en maar blijven 'doormodderen'.

Third party risk management

Uit onderzoeken van Deloitte en KPMG blijkt dat third party risk management bij veel organisaties nog in de kinderschoenen staat. Zo ontbreekt volgens deze onderzoeken in veel gevallen een goed geëquipeerde organisatie voor ketenrisicobeheersing, zijn rollen en verantwoordelijkheden binnen de organisatie onduidelijk belegd en wordt er onvoldoende gebruikgemaakt van technologie die inzicht geeft en delen van het (repetitieve) werk automatiseert.

Het gevolg is dat hoogopgeleide en schaarse professionals veel tijd kwijt zijn aan vrij simpel werk, zoals het opstellen en versturen van vragenlijsten, het vinden van de juiste verantwoordelijke collega's binnen de organisatie, het najagen van reacties en het bijhouden van spreadsheets. Werkzaamheden die in hoge mate geautomatiseerd kunnen worden zodat risk professionals zich kunnen richten op het daadwerkelijk mitigeren van onacceptabele risico's. Bij een hogere volwassenheid van ketenrisicobeheersing hoort ook een meer slimme samenwerking tussen organisaties. Zo zou op sectorniveau meer samengewerkt kunnen worden om kosten van individuele organisaties te drukken en de kwaliteit van bijvoorbeeld de assessmentvragenlijsten te verbeteren.

Krapte op de arbeidsmarkt

Het behoeft geen toelichting dat er momenteel sprake is van een enorme krapte op de arbeidsmarkt. Deze krapte maakt het noodzakelijk dat het beschikbare risicomanagementtalent in organisaties zo effectief en efficiënt mogelijk wordt ingezet. Dit geldt ook voor ketenrisicobeheersing. Heldere doelstellingen en strategie, duidelijk omschreven rollen en verantwoordelijkheden, en goede ondersteunende technologie maken ketenrisicobeheersing meer volwassen. Bovendien maken ze de discipline veel aantrekkelijker voor de toch al zo schaarse risicoprofessional.

Heldere doelstellingen en strategie, duidelijk omschreven rollen en verantwoordelijkheden, en goede ondersteunende technologie maken ketenrisicobeheersing meer volwassen

Tot slot: Wat kunnen auditors doen?

Auditors kunnen een belangrijke rol vervullen bij het verder professionaliseren van ketenrisicobeheersing binnen organisaties. Bijvoorbeeld door op het volgende te letten:

- *Actueel overzicht* – Ketenrisicobeheersing begint met een gedegen en actueel inzicht in de keten. Auditors moeten er dus op toezien dat de juiste randvoorwaarden gecreëerd zijn om tot dit complete en actuele overzicht te komen. Daarbij is het cruciaal dat bekend is welke derde partijen toegang hebben tot het bedrijfsnetwerk en wie de contactpersoon binnen de securityafdeling is.

- *Data triangulatie* – Enkel data verkregen uit self-assessmentvragenlijsten van derde partijen geeft onvoldoende zekerheid over eventuele risico's. Daarom is het belangrijk dat auditors aansturen op het gebruik van verschillende databronnen, bijvoorbeeld cybersecurityscores, nieuwsbronnen en fysieke inspecties. Bovendien zouden auditors kritisch moeten zijn op de frequentie van self assessments – namelijk gebaseerd op het risico van de derde partij en ook op basis van kritieke dreigingen zoals zero days

- *Risicogebaseerde opvolgingen* – Soms komen organisaties niet verder dan het identificeren van risico's uit due diligence assessments. Echter, een volwassen ketenrisicobeheersingsorganisatie zorgt ervoor dat er ook goede opvolging gegeven wordt. Hier zouden auditors op moeten sturen.

- *Frictieloze klantreis voor derde partijen* – Steeds meer organisaties voeren due-diligenceactiviteiten uit wanneer ze zaken willen doen met een derde partij. Het gevolg is dat de gemiddelde organisatie heel wat tijd spendeert aan het invullen van deze vragenlijsten. Hoe gemakkelijker en leuker je dit werk kunt maken, hoe hoger de betrouwbaarheid en kwaliteit van de antwoorden. Auditors zouden daarom kritisch moeten zijn op hoe de klantreis voor derde partijen is vormgegeven.

- *Aansturen op het gebruik van standaarden* – Hoe meer organisaties gebruik gaan maken van internationale standaarden (denk aan ISO 27001, NIST, CIS of SOC2), hoe gemakkelijker ingevulde vragenlijsten in de toekomst uitgewisseld kunnen worden. Dit zou een enorme winst betekenen voor het hele ecosysteem. Auditors zouden daarom kunnen aansturen op het volgen van internationale standaarden bij het opstellen van due-diligence-assessmentvragenlijsten.

Over
Bram Ketting is medeoprichter en CEO van 3rdRisk.

Jelle Groenendaal is chief product owner (CPO) bij 3rdRisk and senior associate onderzoeker bij Crisislab. Tevens is hij verbonden aan de IT Audit Compliance & Advisor- opleiding van de Vrije Universiteit Amsterdam.

Tags: Risicomanagement

Bron url: https://auditmagazine.nl/artikelen/ketenrisicobeheersing-moet-volwassen-discipline-worden/