moet worden geanalyseerd. Het is bijgevolg niet verwonderlijk dat organisaties die de financiële of risico-impact van hun AI-projecten meten, vaker succesvol zijn. Iets meer dan de helft van de organisaties die AI inzetten in meerdere processen en business units, voeren bij elk project systematisch een financiële en/of risicoanalyse uit.

W. Andrews: "Als we geanalyseerd hebben hoe tevreden we zijn over een AI-project, moeten we dat vervolgens communiceren in de taal die het C-niveau gebruikt. Op die manier kunnen we bewijzen dat AI ook effectief waarde genereert. Als het potentieel duidelijk is, zal de goodwill voor volgende projecten ook groter worden. In dat kader helpt het natuurlijk ook dat je van meet af aan meerdere functies in het team hebt betrokken. Zo wordt het potentieel vlugger in de verschillende delen van de organisatie gespot. Iemand in het team kan het bijvoorbeeld interessant vinden om via AI's beelden te analyseren met het oog op een grotere veiligheid. Iemand anders wil via AI misschien de aanwezigheid van je merk op sociale media monitoren. Op die manier kun je ook de reacties van je klanten op het merk analyseren. Zo kun je AI stapsgewijs verder laten groeien in je organisatie."

"Maar voor alle duidelijkheid: je hoeft niet noodzakelijk bij elk project een positieve ROI te beloven. Veel bedrijven starten met AI in de wetenschap dat dat aanvankelijk zeker niet altijd het geval zal zijn. Het is vooral belangrijk in eerste instantie een goed beeld te krijgen van de mogelijke waarde voor het bedrijf, zodat je stapsgewijs kunt groeien op het vlak AI."

5. Pas zo weinig mogelijk proofs of concept toe

Geloof het of niet, maar Whit Andrews raadt aan zo weinig mogelijk proofs of concept (PoC) te gebruiken. "Toen AI opkwam, werden er veel PoC's toegepast om te zien wat werkt en wat niet. Maar tegenwoordig is er al heel wat ervaring opgebouwd en weten we vrij goed wanneer het zinvol is om AI te gebruiken en wanneer niet. Bedrijven die momenteel al verder staan met de uitrol van AI in hun organisatie, gebruiken trouwens twintig procent minder PoC's dan bedrijven die nog maar in de startblokken staan", legt hij uit.

Een vijfde goede gewoonte is dan ook om voor harmonie te zorgen. "Dat kun je doen door je projecten heel zorgvuldig uit te kiezen en het aantal proofs of concepts op die manier binnen de perken te houden. Probeer er ook voor te zorgen dat er interactie is tussen de verschillende proofs of concepts die je toepast", besluit Whit Andrews. "Samen met de andere goede gewoontes zal het beperken van je focus je helpen om een succesvolle AI-strategie te creëren en je digitale ambities op verschillende vlakken vorm te geven."

TC

Honderd proc

Hoe kwetsbaar is onze

Onderzoeksbureau Data Splunk verwacht dat de hoeveelheid cyberaanvallen op de supply chain dit jaar verder zal toenemen. Jelle Groenendaal, lector Risk Management & Cybersecurity aan de Haagse Hogeschool, schetst de mogelijke risico's. Hij legt uit hoe we aanvallen zoveel mogelijk kunnen voorkomen en geeft tips om de schade te beperken.

Volgens de Allianz Risk Barometer behoren cyberaanvallen jaarlijks tot de grootste bedrijfsrisico's. De dreiging van een digitale supply chain-aanval groeit jaar na jaar omdat bedrijven binnen hun keten steeds meer digitale informatie met elkaar delen. Aanvallen gebeuren op hun beurt steeds geraffineerder en zijn de afgelopen jaren in aantal toegenomen. Digitale kopzorgen zijn het deel van de CEO's, CIO's, logistieke en risicomanagers van bedrijven. "Cyber vormt vandaag voor alle sectoren een groot en relevant risico aangezien onze processen meer dan ooit gedigitaliseerd zijn", zegt Jelle Groenendaal, lector Risk Management & Cybersecurity aan de Haagse Hogeschool. "Je moet er als organisatie dus sowieso mee aan de slag."

Jelle Groenendaal noemt drie belangrijke risico's rond cybergevallen. "Hoewel er uiteraard een pak meer zijn en het deels afhankelijk is per sector", zegt hij. "Bij veel bedrijven staan DDos-aanvallen (Distributed Denial of Service) hoog op de agenda, zeker in coronatijden. Als je geen toegang tot de bedrijfsdata hebt of klanten kunnen je website

ent cyberveilig bestaat niet

supply chain?

niet bereiken, dan kost dat je als bedrijf heel veel geld. Een tweede gevaar is 'ransomware', die bestanden gijzelt en blokkeert. Ransomware kan ook via een derde partij waarmee je als bedrijf samenwerkt in je netwerk komen. Als derde is er 'phishing', wat heel vaak voorkomt en allerlei doelen kan hebben. Om data te stelen of iemand valse rekeningen te laten betalen, bijvoorbeeld. De mogelijke impact is per probleem verschillend, maar als je er als bedrijf intrapt, kunnen die bedreigingen een serieuze aderlating betekenen."

"Van zodra je anderen toestemming geeft om je data te verwerken, verlies je een deel van de controle."

Derde partijen

VC: De supply chain is een complex verhaal. Waar in de keten bevinden zich doorgaans de grootste gevaren?

Jelle Groenendaal: "Vroeger had je als organisatie vaak de volledige controle over je systemen en data. Tegenwoordig is dat anders. Zodra je andere bedrijven toestemming geeft om je data te verwerken, bijvoorbeeld bij het gebruik van cloudtoepassingen, verlies je een deel van de controle. Je bent dan deels afhankelijk van die derde partij. Dat is een kwetsbaarheid die je moet beheersen. Enerzijds vanwege de operationele impact wanneer die derde partij opeens uitvalt of ten prooi valt van hackers, anderzijds vanwege het reputatierisico. Als bedrijf riskeer je immers dat klanten jou als schuldige zullen aanzien wanneer gegevens zijn gestolen, terwijl het misschien wel de verantwoordelijkheid van een derde partij was."

"Een andere kwetsbaarheid is dat de supply chains almaar groeien. Een derde partij maakt op zijn beurt gebruik van nog een andere partij. Stel dat je als bedrijf een aantal IT-diensten afneemt van een dienstverlener, die op zijn beurt zijn lot verbindt aan een cloud provider. Wanneer bij die cloud provider iets misgaat, heeft de hele keten daar dan last van. Dan kun je als bedrijf nog zoveel moeite doen om bij je derde partijen de veiligheid te controleren, als ze verderop in de keten allemaal gebruik maken van dezelfde cloudleverancier, en die valt uit, dan heb je een probleem. Maar het werkt ook in de andere richting. Als die gemeenschappelijke cloud provider een hyperscaler is, zoals Amazon, Microsoft of Google, dan werk je met een grote en stabiele dienst. Kleine en zelfs grote bedrijven kunnen zelf nooit zo'n stabiele cloudoplossing maken als die grote spelers."

Jelle Groenendaal, lector Risk Management & Cybersecurity aan de Haagse Hogeschool: "Cyber security is voor alle sectoren een groot en relevant risico, aangezien zoveel processen gedigitaliseerd zijn. Of je nu bakker bent, verzekeraar of een chemisch bedrijf: je moet er als organisatie sowieso mee aan de slag."

Ethisch hacker

VC: Hoe kunnen we ervoor zorgen dat onze partners de spelregels rond de verwerking van data strikt naleven?

J. Groenendaal: "Als er persoonsgegevens in spel zijn, stel je altijd een verwerkingsovereen-

"Als je met derde partijen samenwerkt, verlies je sowieso een deel van de controle over de veiligheid van de uitgewisselde data. Een goed contract rond cyberveiligheid is dan ook cruciaal."

komst op. Die omvat onder meer afspraken over het omgaan met informatiebeveiliging. Afhankelijk van de risico's bepaal je hoe streng die eisen moeten zijn. Bij de selectie, onboarding en contractverlenging van een partner moet je ook altijd naar de cyberbeveiliging polsen. Welke standaarden gebruikt die partij bijvoorbeeld? En op welke manier zijn die geïmplementeerd? Worden incidenten tijdig gedetecteerd en afgehandeld?"

VC: Hoe verloopt dat in de praktijk?

J. Groenendaal: "Vaak gebeurt dat door een statement van een auditor, die gaat controleren of dat bedrijf aan enkele belangrijke criteria voldoet. Grote bedrijven hebben doorgaans centrale afdelingen voor third-party risk management die ook allerlei zaken rond cyber security en andere risico's bekijken tijdens het selectie- en onboardingproces van een partij, tijdens de samenwerking en bij de contractverlenging. Tools voor risicomanagement helpen om het risico- en compliance management van derde partijen te regelen. Een 'good practice' is daarnaast dat sommige organisaties een ethische hacker inhuren die bij de derde partij gaat kijken of alles in orde is. Als je dat wilt doen, moet je dat wel vooraf met die partij regelen en in het contract laten vastleggen. Daarnaast staat in de contracten ook vaak dat derde partijen eventuele incidenten rond cybercriminaliteit zo snel mogelijk bij jou moeten melden."

VC: U spreekt over de grote bedrijven, waar budgettair veel mogelijk is. Wat zijn de best practices op een kleinschaliger niveau?

J. Groenendaal: "Werk risicogericht. Bepaal welke derde partijen voor jouw organisatie cruciaal zijn en richt je aandacht daarop. Als je van derde partijen afhankelijk bent, zorg dan dat je betrouwbare partners uitkiest en neem cyber security en betrouwbaarheid mee als belangrijke selectiecriteria. Daarnaast is het belangrijk dat je als organisatie zelf nadenkt over jouw beschikbare alternatieven wanneer een derde partij onverhoopt haar diensten niet meer kan verlenen."

Draaiboek

VC: Moeten we ook een soort draaiboek opstellen met klanten en leveranciers, met daarin een 'worst case scenario'?

J. Groenendaal: "In mijn rol als adviseur en onderzoeker adviseer ik bedrijven altijd twee zaken. Enerzijds moet je ervoor zorgen dat de bedrijven waarmee je zakendoet alles netjes op orde hebben, met een goede beveiliging en tussentijdse updates op het vlak van beveiliging. Anderzijds moet je er altijd zelf voor zorgen dat je nog een alternatief hebt voor het bedrijf waarmee je zakendoet. Stel dat je erg afhankelijk bent van een bepaalde partij, dan moet je een draaiboek maken waarin staat wat

je zult doen als er bij die partij een cyberaanval is en die partij daardoor geen diensten meer aan jou kan leveren."

VC: U verwijst in dat verband vaak naar BCM. Wat is dat?

J. Groenendaal: "BCM staat voor Business Continuity Management. Het omvat verschillende onderdelen. Ten eerste een schets van de belangrijkste diensten of producten die je als organisatie levert en de processen die daaraan ten grondslag liggen. Ten tweede de bedreigingen voor die processen, zoals een aantal cyberdreigingen. Ten derde de maximale tijdsduur waarin je buiten dienst mag zijn als zo'n scenario zich voordoet. Stel dat het voor jouw bedrijf onacceptabel is om langer dan twee uur stil te liggen, dan ga je je BCM-plan zo uitstippelen dat je binnen de twee uur je supply weer op gang kunt trekken. Je gaat na wat je daarvoor nodig hebt. Je kunt bijvoorbeeld twee datacenters gebruiken. Of ervoor zorgen dat je netwerk goed gesegmenteerd is, zodat een geval van ransomware maar aan een deel van je netwerk raakt. BCM is risicogestuurd. Als je kijkt waar de grootste risico's zich bevinden, dan probeer je daar de meeste aandacht op te vestigen om ervoor te zorgen dat je zo snel mogelijk kunt reageren als er iets gebeurt."

Oefeningen en tests

VC: Bedrijven en supply chains veranderen sneller dan ooit. Hoe zorgen we ervoor dat wat we vorig jaar opstelden actueel blijft?

J. Groenendaal: "Dat is een terechte bedenking. Daarom ben ik ook kritisch over BCM in onze snel veranderende wereld. BCM werd in het verleden vooral op papier gezet. In de praktijk zag je dat wat je op papier zette, na een week alweer anders was, zeker in grote bedrijven. De IT-omgeving verandert continu. Ook bij je derde partijen veranderen zaken. Dan is een statisch plan niet heel zinvol. Je moet je papier dus zo dun mogelijk houden en enkel de belangrijkste dingen noteren. Wie bel je als er wat misgaat, wat zijn op hoofdlijnen, waar schuilen de tijdelijke oplossingen en wat zijn de zaken die je zeker niet moet vergeten? Belangrijker is om regelmatig oefeningen en tests te houden. Stel dat een derde partij uitvalt, hoe pak je dat aan? Welke opties heb je dan? Als bedrijf moet je naar een modus gaan van minder papier en meer tests en gesprekken met mensen."

"Zelfs sterk beveiligde organisaties blijven tot op zekere hoogte kwetsbaar."

VC: Als we het over beveiliging hebben, gaat het snel over software en de juiste tools. Als we daar een bekwame risicomanager in ons bedrijf aan toevoegen, is het plaatje dan compleet?

J. Groenendaal: "Zeker bij grotere bedrijven heb je een 'risk manager' nodig die de organisatie helpt met het besturen en managen van risico's. Maar uiteindelijk kun je risicomanagement niet uitbesteden aan risk managers. Risicomanagement is en blijft een fundamenteel onderdeel van ondernemen en hoort daarom thuis bij het lijnmanagement. Een risk manager kan wel helpen bij het inrichten van het risicomanagement. Een goede cyberbeveiliging bestaat uit een soort cyclisch model met verschillende fases. Je doorloopt daarbij vijf stappen. De eerste is identificatie. Hoe ziet mijn organisatie eruit en wat zijn de bedreigingen en risico's? De tweede stap is bescherming. Hoe bescherm ik me tegen de risico's? De derde fase is detectie. Je monitort of er een aanval of incident is. De vierde fase is beantwoording. Je gaat reageren en zorgen dat je iets tegen een aanval doet. De vijfde fase is herstel. Als er schade is: hoe ben je zo snel mogelijk 'back in business'? In die laatste fase zit BCM verwerkt."

Risico's horen erbij

VC: Verbaast het u dat er – ondanks alle geleverde inspanningen – toch nog zoveel misloopt, zelfs in hele grote bedrijven?

J. Groenendaal: "De meeste grote bedrijven leveren echt wel veel inspanningen. Toch blijven zelfs sterk beveiligde organisaties tot op zekere hoogte kwetsbaar. Veel heeft te maken met de kracht van de almaar toenemende en meer vernuftige aanvallen. En dat er ook in goed beveiligde bedrijven fouten worden gemaakt. Dat een bedrijf geraakt is, wijst dus niet noodzakelijk op een gebrekkige aanpak van de cyberrisico's."

VC: Mogen we concluderen dat honderd procent risico uitsluiten niet kan?

J. Groenendaal: "Inderdaad. Je moet die honderd procent ook niet per se willen nastreven. Er zijn maar een paar organisaties die dat echt willen, zoals geheime diensten of nucleaire installaties. Die zijn echt super beveiligd. Dat niveau kun je als normaal bedrijf niet eens proberen na te streven. Als je honderd procent veilig wilt zijn, kun je geen business meer doen. De supply chain houdt risico's in. Als je gebruik maakt van een aantal grote partijen die hun zaken goed op orde hebben, dan zorgt dat op zich ook voor veiligheid. Er kan altijd iets gebeuren en dat moet je accepteren."

VC: In een studie lichtte u het bekende cyberincident bij transportreus Maersk toe. Na de cyberaanval bij dat bedrijf kwam er onder meer heel wat improvisatie aan te pas, zo bleek. Is dat normaal?

J. Groenendaal: "In een crisissituatie heb je altijd improvisatie nodig. Ook al heb je vooraf nog zo'n goed plan opgesteld, de omgeving verandert zo snel dat plannen vaak achterhaald zijn wanneer je ze moet gebruiken. Dan blijkt soms dat de keten toch anders in elkaar zit. Improvisatie is in dat geval belangrijk en bepaalt of je goed uit een crisis komt of niet. Toch blijft een plan nuttig. Een plan kan je helpen bij bepaalde scenario's, om de juiste mensen in te schakelen en een helder beeld te krijgen op zaken waar je op voorhand al over hebt nagedacht."

KD/TR