Hoe beheers je alle risico's in de supply chain?

De supply chain is de nieuwe frontlinie in cybersecurity. Terwijl organisaties hun eigen systemen steeds beter beveiligen, blijven leveranciers, partners en schaduwleveranciers vaak onzichtbare risico's vormen. De Cyberbeveiligingswet, de Nederlandse implementatie van de Europese NIS2-richtlijn, maakt organisaties expliciet verantwoordelijk voor deze ketenafhankelijkheden. Hoe creëer je overzicht en beheersing in een steeds complexer wordend netwerk, waar een aanval op de zwakste schakel de hele keten kan ontwrichten?

Marcel Knippen,
Oprichter en CEO, RiskStudio

Risico's stoppen niet bij de grenzen van je eigen organisatie, stelt Marcel Knippen, oprichter en CEO van RiskStudio. Volgens hem kijken bedrijven traditioneel vooral naar hun eigen beveiliging, terwijl aanvallen steeds vaker via leveranciers verlopen. "Het aantal supply chain-aanvallen is de afgelopen jaren explosief gegroeid. Bij bijna een derde van de incidenten ligt de oorzaak inmiddels ergens in de keten."

Knippen is een bekende naam binnen de Nederlandse cybersecuritywereld. Hij stond eerder aan de basis van beveiligingsbedrijf QSight – later overgenomen door KPN – en was betrokken bij de oprichting van brancheorganisatie Cyberveilig Nederland. Met RiskStudio richt hij zich volledig op supply chain security: inzicht krijgen in leveranciers, onderliggende afhankelijkheden en de digitale risico's die daaruit voortkomen.

Digitale afhankelijkheden

Knippen stelt dat veel organisaties onderschatten hoe groot hun digitale ecosysteem werkelijk is. "Je denkt misschien dat je zakendoet met één leverancier, maar daarachter zitten vaak weer tientallen andere partijen. Denk hierbij aan mailproviders, cloudleveranciers en betalingsdienstverleners; alles is met elkaar verbonden."

> *Het aantal supply chain-aanvallen is explosief gegroeid*

Dat netwerk van afhankelijkheden brengt RiskStudio visueel in kaart. Het platform bouwt als het ware een digitale kopie van een organisatie en haar ketenpartners. Leveranciers worden gekoppeld aan afdelingen, processen en zogenoemde kroonjuwelen, de bedrijfskritische onderdelen van een organisatie. "Wij noemen het een digital twin", zegt Knippen. "Sommige partijen blijken digitaal veel kritischer dan je op basis van omzet of contractwaarde zou denken." Op een platform dat hij toont, blijkt Microsoft de meest kritieke leverancier binnen de supply chain van een organisatie, terwijl deze organisatie zelf geen Microsoft gebruikt. "Juist dat soort verborgen afhankelijkheden wil je zichtbaar maken."

Outside-in-benadering

De aanpak van RiskStudio verschilt van traditionele complianceprocessen. Waar organisaties vaak werken met vragenlijsten, audits en jaarlijkse beoordelingen, gebruikt het platform een zogenoemde outside-in-benadering. Daarbij worden organisaties continu extern gemonitord op signalen rondom kwetsbaarheden, datalekken, configuratiefouten en gelekte gegevens. "Bij klassieke compliance ga je ervan uit dat alles veilig is als de administratie klopt", zegt Knippen. "Maar uiteindelijk draait het om de praktijk: zijn systemen goed ingesteld, staan partijen op blacklists, zijn er signalen van incidenten?"

Via geautomatiseerde analyses verzamelt het platform informatie uit publieke bronnen, dreigingsinformatie, nieuwsberichten en technische scans. "Dagelijks controleren we leveranciers op cyberhygiëne en veranderingen in hun risicoprofiel. In cybersecurity is een jaarlijkse audit eigenlijk een eeuwigheid."

Wet maakt het concreet

De spoedige bekrachtiging van de Nederlandse Cyberbeveiligingswet versnelt de aandacht voor supply chain security. Organisaties worden verplicht om ook risico's bij leveranciers actief te beheersen en daarover verantwoording af te leggen. Knippen vertelt dat het onderwerp inmiddels nadrukkelijk leeft in bestuurskamers. "Het voelt voor veel organisaties nog als een verplichting, maar geopolitieke ontwikkelingen maken het ineens heel concreet."

RiskStudio ziet vooral groeiende interesse vanuit overheden, zorginstellingen, financiële organisaties en gemeenten. Daarbij wordt naast cyberdreigingen ook de digitale soevereiniteit een steeds belangrijker item. "Bestuurders willen weten in welke landen hun dataopslag staat, onder welke wetgeving ze vallen en welke afhankelijkheden ze hebben." Dat thema speelde ook binnen de eigen organisatie van RiskStudio – inmiddels heeft het bedrijf de infrastructuur bewust verhuisd naar Nederlandse datacenters. Knippen: "Ik wil weten hoe er met onze data wordt omgegaan. Als dit onder buitenlandse wetgeving valt, heb je daar weinig controle meer over."

> *In cybersecurity is een jaarlijkse audit een eeuwigheid*

Praktisch beginnen

Een belangrijk uitgangspunt van RiskStudio is dat organisaties klein moeten kunnen beginnen. Knippen noemt cyberbeveiliging in de supply chain "de olifant in de kamer": veel bedrijven zien de omvang van het probleem, maar weten niet waar ze moeten starten. Daarom ontwikkelden ze een methode waarbij organisaties in korte tijd hun belangrijkste leveranciers in kaart kunnen brengen. "Ook als je niet weet met wie je allemaal te maken hebt, kun je binnen een uur een eerste overzicht opbouwen. Daarna stroomt de informatie live binnen."

Dat inzicht helpt organisaties om prioriteiten te stellen. Niet iedere leverancier vormt immers hetzelfde risico. "Je kijkt naar signalen en ziet meteen hoe kritisch deze partij is voor je bedrijfsproces. Pas dan kun je gericht handelen." Volgens hem vormt dat uiteindelijk de kern van moderne ketenbeveiliging. "De financiële kredietwaardigheid van leveranciers controleren we al jaren. Waarom zouden we hun cyberwaardigheid dan niet controleren?"