In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

De invloed van de wereld op onze leveranciers

In eerdere edities van iB-Magazine hebben we de risico's binnen de toeleveringsketen besproken, waarbij we recent focusten op de Europese Digital Decade-wetgeving. Deze regelgeving biedt kansen, maar roept ook vragen op over ethiek en verantwoordelijkheden binnen de informatiebeveiliging. Ondertussen spelen geopolitieke ontwikkelingen, zoals de handelsoorlog tussen China en de VS, een steeds grotere rol. Wat betekenen deze veranderingen voor onze aanpak in Nederland, en hoe houden we rekening met internationale leveranciers?

In de vorige editie van Achter Het Nieuws onderzochten we de juridische implicaties binnen de toeleveringsketen, met nadruk op Europese wetgeving en de kansen die deze voor informatiebeveiligers kan bieden. Naast deze interne ontwikkelingen vraagt ook het internationale speelveld om onze aandacht: denk aan de aanhoudende spanningen tussen de VS en China, met directe gevolgen voor bedrijven als ASML. Hoe beïnvloeden deze wereldwijde krachten ons werk, en wat betekent dit voor de samenwerking met leveranciers wereldwijd?

Fook Hwa Tan – Ketenrisico's omzetten in kansen

Geopolitieke uitdagingen dwingen Nederlandse bedrijven om zich aan te passen en veerkrachtig te zijn. Handelsoorlogen en strikte regelgeving veranderen het speelveld, maar in plaats van te focussen op risico's, kunnen we juist kansen benutten. De Nederlandse handelsgeest en openheid voor samenwerking met diverse partijen helpen ons om nieuwe kansen te grijpen en onze toeleveringsketen te versterken. Door overzicht en inzicht in de keten te creëren, kunnen we verbeterpunten identificeren en processen optimaliseren, wat leidt tot meer efficiëntie en een toekomstbestendig model waarin risico's vroegtijdig worden aangepakt.


Fook Hwa Tan


Leo van Koppen

Een cruciale uitdaging is het vinden van een balans tussen veiligheid, objectiviteit en inclusiviteit. Leveranciers uit complexe regio's kunnen risicovol lijken, maar een rigide benadering leidt tot uitsluiting. We moeten risico's beheersen zonder vooroordelen, door transparant en objectief te evalueren. Zo doen we recht aan zowel veiligheid als eerlijke kansen voor alle leveranciers, ongeacht hun herkomst. Culturele verschillen spelen hierbij een rol: intensief screenen kan in sommige Aziatische culturen als wantrouwen worden gezien, terwijl dit in westerse landen vaak als professionaliteit wordt opgevat. Begrip en respect voor culturele verschillen helpen ons effectiever te communiceren en duurzamere relaties met leveranciers op te bouwen.

Veerkracht vraagt vertrouwen en samenwerking. Laten we samen streven naar Digital Trust door transparantie en samenwerking. Alleen samen realiseren we een veilige, veerkrachtige en vertrouwde digitale toekomst.

Leo van Koppen – Polarisatie als risicofactor

Het antwoord op de gestelde vraag is natuurlijk een no-brainer, natuurlijk heeft het impact! Helaas moet ik constateren dat polarisatie op alle plaatsen in de wereld toeneemt. Ik ben daar niet van, het past niet bij mijn karakter, ben altijd op zoek naar harmonie, maar dat terzijde. Polarisatie wordt zichtbaar wanneer mensen uitgesproken meningen aan de uiterste kanten van een onderwerp innemen. Die discussie wordt in dit tijdperk met name via digitale middelen gevoerd en daarmee is de link gelegd naar het domein cybersecurity. Om je macht te kunnen tonen, je economie te versterken, je business te beschermen, je territorium uit te breiden, lijken alle middelen en methoden toegestaan. Nation state actors zijn daarbij de belangrijkste actoren.

De vraag heeft een nogal brede scope die ik omwille van de lengte van deze bijdrage maar wat kleiner kies. Ik beperk me dan ook tot deze threat actor en het nieuwe fenomeen van AI, dat zowel als maatregel of als bedreiging kan worden gezien. Voordat ik daar op in ga, eerst maar even de invloed van AI op de bedrijfsvoering beschouwen. Als die verwachtingen worden waargemaakt dan betekent dat de bedrijfsvoering, nog sterker dan het nu al het geval is, afhankelijk zal worden van informatievoorziening. Het gaat dan met name om de integriteit van de onderliggende data waarop AI is gebaseerd. We kennen deze relatie: toename in afhankelijkheden betekent in cybersecurity grotere risico's.

Artificiële Intelligentie heeft geen twee maar vier invalshoeken, althans zo stelt de AIVD in het onlangs verschenen document (3). Omdat ik het zelf niet beter kan verwoorden hierbij een ingekorte versie:

Aanvallen (dreiging)

1. Op generatieve AI, gericht op het verstoren of misleiden van AI-systemen, inclusief pogingen om de trainingsdata te beïnvloeden of de AI op ongepaste wijze te manipuleren
2. Met behulp van generatieve A, waarbij GenAI wordt ingezet als middel voor het uitvoeren van cyberaanvallen

Verdediging (maatregelen)

1. Van generatieve AI. Verdedigingsmaatregelen zijn gericht op het beschermen van AI-systemen tegen externe aanvallen en interne misbruiken. Dit omvat het veiligstellen van trainingsdata en het model, evenals het ontwikkelen van robuuste systemen die zichzelf kunnen verdedigen tegen aanvallen.
2. Met behulp van generatieve AI. AI wordt ook gebruikt als een hulpmiddel om te verdedigen tegen cyberaanvallen, door middel van realtime dreigingsdetectie en respons, of het combineren van en handelen op dreigingsinformatie uit verschillende bronnen.

Mijn conclusie bij het bovenstaande is dat er sowieso werk aan de winkel is, immers: de aanvallers beschikken door AI over meer geavanceerde tools. Hiervan kunnen we nog nauwelijks overzien welke impact het zal hebben, daarbij is ook het aanvalsoppervlak (data) verder uitgebreid. Natuurlijk komen er ook nieuwe tools beschikbaar waarmee we onze verdediging kunnen versterken, maar het beschermen van die complex AI-systemen en de bijbehorende data vraagt nieuwe expertise en veel tijd.

Drie effecten bij deze beperkte scope samengevat:

- State actors zullen een agressievere houding gaan vertonen om macht te behouden of uit te breiden
- Een sterkere afhankelijkheid van informatie en bijbehorende systemen ten gevolge van de toepassing van AI in bedrijfsvoering en economische bedrijvigheid
- En een sterk veranderend (complexer) speelveld door de komst van AI. Kortom de gevolgen van toenemende polarisatie op het wereldtoneel zijn enorm. Ik hoop, tegen beter weten in dat 'de wereld' gaat inzien dat polarisatie niets oplost. Een meer constructieve attitude zou ons veel verder brengen.

Referenties

(1) https://www.businessinsider.nl/topman-asml-kritisch-op-steeds-verder-gaande-exportbeperkingen-voor-china/

(2) https://nos.nl/artikel/2540868-asml-hard-onderuit-op-de-beurs-na-te-vroeg-verschenen-kwartaalcijfers

(3) https://www.aivd.nl/documenten/publicaties/2024/10/17/generatieve-ai.-een-transformatieve-impact-op-cybersecurity