Dyami Service Highlight

Spionage en jouw onderneming

- Waarom spionagerisico door ondernemers vaak wordt onderschat
- Nederlandse bedrijven zijn een gewild doelwit voor spionage uit het buitenland
- Cybersecurity alleen is niet voldoende bescherming tegen spionage

Wat is spionage eigenlijk?

Spionage draait om vertrouwelijke informatie, oftewel inlichtingen — *intelligence* in het Engels. Spionage is het proberen te bemachtigen van die inlichtingen.

Er zijn verschillende soorten informatie die voor een spionerende partij interessant kunnen zijn. Voor ondernemingen zijn dit:

1. **Intellectueel eigendom (IP)**
   Met name van toepassing voor innovatieve ondernemingen, over het algemeen door eigen ideeën en research & development ontwikkeld
2. **Gevoelige data**
   Personeelsdata, klantendata, research, bedrijfsgevoelige informatie, veiligheidsgevoelige informatie
3. **Details van contracten en kosten**
   Alle informatie die concurrenten kan helpen om een aanbesteding te winnen of een contract (verlenging) weg te kapen
4. **Geheime plannen**
   Toekomstige plannen, nieuwe producten of diensten die voor concurrenten interessant kunnen zijn

Concurrenten zijn dus een mogelijke partij die een spionagedreiging vormt. Maar we zien vaker dat buitenlandse regimes en inlichtingendiensten dit voor eigen strategisch of commercieel gewin doen.

Welk risico loop ik?

Aan de hand van het lijstje links kun je zelf bedenken of je informatie hebt die interessant zou kunnen zijn voor anderen. Hoe waardevoller, hoe groter je risico.

De AIVD — de Algemene Inlichtingen- en Veiligheidsdienst en de MIVD, de militaire evenknie, waarschuwen al jaren dat spionage in Nederland veel voorkomt. We hebben een relatief hoog kennisniveau en veel innovatieve bedrijven in ons land. Met name andere landen als bijvoorbeeld China en Rusland hebben verregaande ervaring, methodieken en budget voor. Hun focus is met name op IP en data, vooral als ze door sancties afgeschermd worden tegen bepaalde technologieën en innovatie.

Vaak wordt het risico onderschat

Diefstal van belangrijke informatie kan in bepaalde gevallen zo schadelijk zijn voor een onderneming dat de onderneming die klap niet overleeft.

Toch zien we dat veel ondernemingen het risico zodanig onderschatten dat ze niet of weinig actie ondernemen om zicht tegen spionage te wapenen.

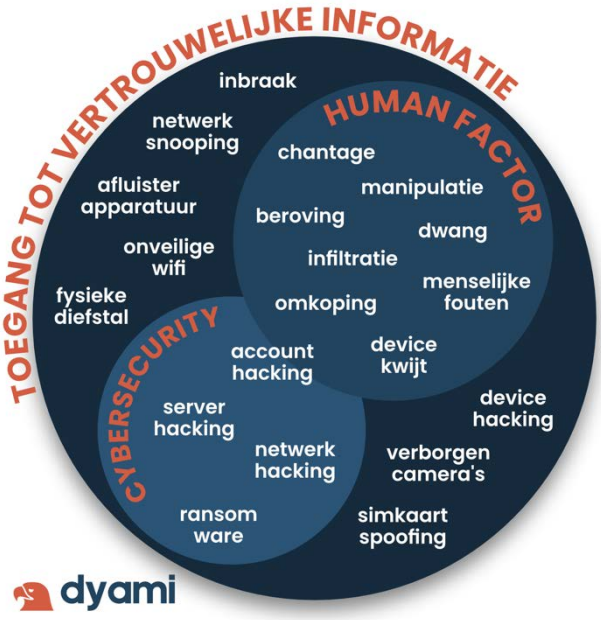
Dat komt meestal door één van deze redenen:

- Algehele onderschatting: het gebeurt mij niet
- De veronderstelling dat het juridisch borgen van IP en data door contracten en octrooien voldoende is
- De veronderstelling dat cybersecurity voldoende is
- Eigenlijk nooit echt ter sprake gekomen

Dyami B.V. | **info@dyami.services** | **www.dyami.services**
Parijsboulevard 209 | 3541 CS Utrecht | The Netherlands | +31 30 207 2120
CoC: 76991377 | IBAN: NL93 BUNQ 2041 4574 81 | VAT: NL860865228B01

Hoe spionage plaatsvindt

Als je je wilt wapenen tegen spionage is het belangrijk om te weten op welke manieren het kan plaatsvinden. Zoals hierboven al benoemd kan informatie ook op andere wijzen dan via het cyber-domein worden bemachtigd:



In december 2020 heeft de AIVD bekendgemaakt dat Russische spionnen actief waren in Nederland en ze op grote schaal technologische informatie hebben bemachtigd. Dat ging geheel buiten het cyber-domein om, namelijk door mensen van organisaties te manipuleren en om te kopen en zo toegang te krijgen tot informatie. De AIVD zegt zelfs dat mogelijk hierdoor de nationale veiligheid is aangetast, bijvoorbeeld doordat verkregen kan worden voor militaire doeleinden en cyber-warfare.

Belangrijk is dus dat met alleen cybersecurity bescherming, je nog lang niet veilig bent tegen spionage.

Het begint met awareness

Je kunt je uiteraard niet wapenen tegen een dreiging als je je niet bewust bent van die dreiging. Het lezen van dit document is een eerste stap!

Een volgende, noodzakelijke stap is het uitbreiden van die awareness. Niet alleen dat de dreiging bestaat en dat die dreiging ook voor jou een risico is maar ook waar je op moet letten om dat risico zoveel mogelijk te reduceren. En welk gedrag daarbij hoort. Dat geldt voor iedereen in je onderneming.

De zwakste schakel: mensen

Mensen zijn tegelijkertijd één van de belangrijkste assets en één van de grootste risico's van een onderneming. Daar maken spionnen gebruik van.

Niet alleen kunnen bestaande medewerkers worden bedreigd, gemanipuleerd of omgekocht, ook kunnen spionnen in je organisatie infiltreren door er simpelweg te solliciteren of stage te doen. Of een innige relatie beginnen als partner, leverancier of klant. Dat noemen we de *insider threat*. Mensen maken ook soms fouten of denken ergens niet aan, zeker onder stress.

Maar een onderneming waar een cultuur van wantrouwen heerst is ook niet wenselijk. Gelukkig zijn er allerlei maatregelen beschikbaar die ervoor zorgen dat je goede relaties met je mensen en partners houdt en het risico van spionage tot een minimum houdt.

Op zakenreis zijn er uiteraard extra uitdagingen. Een andere omgeving, cultuur en dreigingen. Ook veilig internationaal op zakenreis is een specialiteit van ons.

Veilig tegen spionage met Dyami

Dyami wapent je onderneming tegen spionage. Daarvoor bieden we de volgende diensten:

- Cybersecurity
- Ontwerp en implementatie van securitybeleid en procedures
- Noodplan (Emergency Response Plan)
- Risico- en dreigingsanalyses
- Training voor medewerkers: awareness en weerbaarheid
- Internationaal veilig reisbeleid
- Due diligence van nieuwe en bestaande partners, klanten, leveranciers en medewerkers
- Sweeping: Kantoren, auto's, woningen vrijmaken van afluisterapparatuur (audio/video/netwerk)
- Fysieke beveiliging van mensen, assets, reizen en transport

Je eigen securityafdeling

Met Dyami haal je een heel securityteam in huis. We hebben een uitgebreide achtergrond in inlichtingen, overheid, politie, Defensie, cybersecurity, luchtvaart en de reisindustrie. Met ons in-house team van analisten maken wij wereldwijde analyses op maat.

Dat doen we allemaal voor zeer kosteneffectieve prijzen. Neem voor meer info contact met ons op!

www.dyami.services

Dyami B.V. | **info@dyami.services** | **www.dyami.services**
Parijsboulevard 209 | 3541 CS Utrecht | The Netherlands | +31 30 207 2120
CoC: 76991377 | IBAN: NL93 BUNQ 2041 4574 81 | VAT: NL860865228B01