Veiligheid in een veranderende wereld

(Digitale) spionage

Risico's voor het bedrijfsleven en wat kun je er aan doen

Spionage is geen ver-van-ons-bed-show. Het vormt een reële en groeiende dreiging voor Nederland en zijn economie. Buitenlandse inlichtingendiensten zijn actief in ons land – digitaal én via menselijke netwerken – op zoek naar gevoelige informatie, technologische kennis en economische voorsprong. Deze whitepaper met informatie afkomstig van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), biedt inzicht in de aard van de dreiging, de werkwijze van spionnen, de risico's voor bedrijven én wat jij als organisatie kunt doen om je te beschermen.

Wat is spionage?

Spionage is het heimelijk verzamelen van gevoelige informatie of objecten. Het gaat om staatsgeheimen, technologie, persoonsgegevens of vertrouwelijke bedrijfsinformatie. Dit gebeurt digitaal via hackaanvallen, maar ook door persoonlijk contact met medewerkers die toegang hebben tot waardevolle informatie.

Nederland is een aantrekkelijk doelwit vanwege:

- Lidmaatschap van NAVO en EU
- Aanwezigheid van internationale organisaties (zoals OPCW en ICC)
- Hoogontwikkelde kenniseconomie met veel technologische innovatie

Wie spioneren – en waarom?

Meerdere landen spioneren in Nederland om:

- Politieke besluitvorming te beïnvloeden
- Economische kennis te stelen
- Regimekritische landgenoten te volgen
- Internationale machtspositie te versterken

De landen die dit doen beschikken vaak over professionele inlichtingendiensten. De exacte dreiging verschuift met geopolitieke ontwikkelingen.

Hoe wordt er gespioneerd?

Digitale spionage:

- Hacken van bedrijfsnetwerken en overheidsinstellingen
- Gebruik van phishing, malware en spyware

Klassieke spionage:

- Benaderen van personen met toegang tot informatie
- Opbouwen van vertrouwen via schijnbaar onschuldige relaties
- Langdurige beïnvloeding, soms met betaling voor informatie

Waarom is spionage schadelijk voor bedrijven?

- Economisch verlies: gestolen innovaties, daling in concurrentievermogen
- Risico op reputatieschade: verlies van vertrouwen bij partners
- Financiële impact: schadeclaims, verlies van subsidies of marktaandeel
- Nationale veiligheid: door lekken in gevoelige sectoren zoals energie of defensie

Hoe herken jij spionagepogingen?

Let op signalen zoals:

- Onverwachte toenadering van onbekenden (bijv. via LinkedIn)
- Grote interesse in je werk of netwerk
- Vragen om ogenschijnlijk onschuldige informatie
- Cadeaus of uitnodigingen buiten werktijd

Vaak gaat het om subtiele beïnvloeding over een langere periode.

Wat kan jij doen?

- Bewustwording creëren binnen je organisatie
- Train medewerkers in herkenning van spionage-signalen
- Houd vertrouwelijke informatie beperkt toegankelijk
- Gebruik goede beveiligingssoftware en update regelmatig
- Deel online geen informatie over gevoelige projecten
- Meld verdachte situaties bij de interne veiligheidsafdeling of de AIVD

Conclusie

Spionage is een reëel risico voor het Nederlandse bedrijfsleven. Wees alert, deel bewust en neem maatregelen. Alleen door proactieve beveiliging kunnen we economische en nationale schade voorkomen.

Meer weten?

Bezoek de website www.aivd.nl/spionage of neem contact op met Arjan Linschooten, regiomanager VNO-NCW Midden: linschooten@vno-ncwmidden.nl / (06) 12 92 27 89.

Cyberaanvallen door statelijke actoren

De AIVD en MIVD waarschuwen voor de toenemende digitale dreiging door statelijke actoren die zich richten op Nederlandse overheden én bedrijven. Deze actoren, organisaties of personen die namens een regering of staat opereren, proberen bedrijfsgevoelige informatie te stelen of systemen te saboteren. Hoe gaan de actoren te werk en hoe kun je als ondernemer je organisatie hiertegen beschermen.

Cyber Kill Chain: 7 fasen van een aanval

De Cyber Kill Chain is een internationaal erkend model dat de verschillende fasen van een cyberaanval beschrijft. Door elke fase te begrijpen, kunnen ondernemers gerichter investeren in preventie en detectie.

1. Reconnaissance – Verkenning
Aanvallers verzamelen informatie over zwakke plekken (mensen, systemen, partners).
ACTIE: *Verminder het aanvalsoppervlak door poorten te sluiten, systemen te patchen, en informatie op sociale media te beperken.*

2. Weaponization – Wapenen
Gevonden kwetsbaarheden worden omgezet in aanvallen via malware of exploits.
ACTIE: *Begrijp welke actoren je als doelwit kunnen zien, en stem je maatregelen hierop af (gebruik bijvoorbeeld MITRE ATT&CK).*

3. Delivery – Bezorging
De malware wordt afgeleverd, vaak via (spear)phishing of geïnfecteerde websites.
ACTIE: *Scan e-mails en bijlagen actief, gebruik sandboxes en blokkeer ongewenste bestandstypen en onbekende afzenders.*

4. Exploitation – Uitbuiten
De malware wordt geactiveerd, bijvoorbeeld wanneer een medewerker op een link klikt.
ACTIE: *Application whitelisting, medewerkers trainen in phishingherkenning en gebruik maken van EDR-oplossingen.*

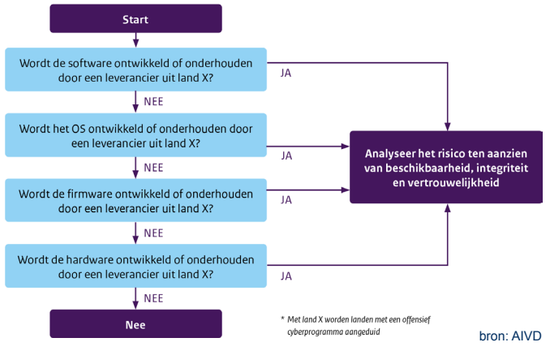
5. Installation – Installeren
De aanvaller installeert backdoors en verkrijgt beheerrechten om zich blijvend te nestelen.
ACTIE: *Netwerken segmenteren, rechten beperken, MFA instellen en beheeraccounts afschermen.*

6. Command and Control – Besturing op afstand
De aanvaller communiceert met de malware om controle te houden en nieuwe opdrachten te geven.
ACTIE: *Monitor netwerkverkeer, gebruik DNS-sinkholing, proxies en NGFW's om C2-verkeer te detecteren en blokkeren.*

7. Actions on Objectives – Doel uitvoeren
De aanvaller steelt informatie, saboteert systemen of verkoopt toegang.
ACTIE: *Implementeer DLP (Data Loss Prevention), zorg voor back-ups en een goed incident responseplan. Laat forensisch onderzoek uitvoeren na een aanval.*

Conclusie
Door kennis te nemen van deze zeven fasen en per fase passende beveiligingsmaatregelen te treffen, verhoog je de digitale weerbaarheid van je organisatie en verklein je het risico op geslaagde cyberaanvallen door statelijke actoren.

Cybercheck



bron: AIVD

De wereldwijde toeleveringsketens van digitale producten en diensten brengen steeds vaker risico's met zich mee, vooral als deze afkomstig zijn uit landen met een offensief cyberprogramma. Deze landen kunnen via wetgeving bedrijven en burgers dwingen om mee te werken aan digitale spionage of sabotage.

De Cybercheck is een praktische handreiking voor organisaties met vitale belangen (zoals intellectueel eigendom, infrastructuur of gevoelige data) om inzicht te krijgen in deze risico's. Door systematisch te onderzoeken wie verantwoordelijk is voor de ontwikkeling, het onderhoud en de levering van software, hardware, besturingssystemen en firmware, kunnen potentiële kwetsbaarheden worden geïdentificeerd.

De aanpak bestaat uit vier stappen:

1. Selecteer kritieke producten of diensten.
2. Bepaal de scope van deze onderdelen.
3. Beantwoord de Cybercheck-vragen.
4. Voer bij risicosignalen een aanvullende risicoanalyse uit.

Deze risicoanalyse maakt gebruik van scenario's gebaseerd op bekende aanvalstechnieken (zoals backdoors, kwaadaardige updates of sabotage) en onderzoekt de weerbaarheid van de organisatie op drie niveaus: toegang verkrijgen ('in'), verspreiden binnen het netwerk ('through') en schade aanrichten ('out').

Belangrijk voor ondernemers: het nemen van preventieve maatregelen tegen supply chain risico's is geen kwestie van paranoia, maar van strategisch risicomanagement. De Cybercheck biedt een gestructureerde aanpak om deze dreiging praktisch en organisatiebreed te benaderen.

Cyberaanvallen

Wees altijd alert

De meeste cyberaanvallen beginnen niet met een geniale hacker die een systeem kraakt. Ze beginnen met een mens: iemand klikt op een link, opent een bijlage of geeft een wachtwoord af. Of met een vergeten systeem dat nog openstaat op internet.

Bij Odido kwamen criminelen binnen door phishingmails te sturen naar klantenservicemedewerkers. Nadat ze een wachtwoord hadden bemachtigd, belden ze de medewerkers op en deden zich voor als de ICT-afdeling. Zo wisten ze de medewerkers te verleiden hun frauduleuze inlogpoging goed te keuren – en zo de tweestapsverificatie te omzeilen.

Hoe criminelen binnenkomen en wat je direct kunt doen

- **De meeste bedrijven worden niet gehackt, ze worden 'ingelogd' met gestolen of geraden wachtwoorden.**
- **Tweestapsverificatie (MFA) is geen luxe. Het blokkeert het overgrote deel van eenvoudige aanvallen. Zelfs als criminelen je wachtwoord hebben, komen ze er vaak niet in.**
- **Een open remote-toegang (RDP) op internet is als je voordeur openzet met een briefje: 'Kom binnen'.**
- **Een back-up die permanent aan het netwerk hangt, wordt bij ransomware vaak mee versleuteld. Een offline of niet-aanpasbare back-up is cruciaal.**
- **Criminelen scannen automatisch. 'Wij zijn te klein' is geen bescherming.**
- **Oude accounts van ex-medewerkers of leveranciers zijn populaire achterdeurtjes.**

Een voorbeeld uit de praktijk

Bij een Brabantse plantenkwekerij begon het met een trage computer. Al snel bleken alle bestanden versleuteld. De back-up? Die stond op een harde schijf die aan de server hing – en was dus ook besmet. Het bedrijf had geen werkende back-up meer want een back-up die permanent aan het netwerk hangt, is geen back-up. Die wordt bij ransomware gewoon meegegijzeld.

Wat als eerste doen?

- **Zet overal tweestapsverificatie aan – zeker op e-mail, VPN, cloud en beheeraccounts.**
- **Installeer updates direct, vooral op systemen die vanaf internet bereikbaar zijn.**
- **Zet remote-toegang nooit zomaar open; gebruik een beveiligde verbinding.**
- **Maak back-ups die niet continu aan het netwerk hangen en test of je echt kunt terugzetten.**
- **Leer medewerkers phishing herkennen en melden.**

Bij Bun, de grootste Albert Heijn-franchisenemer, werden paspoorten, salarisgegevens en ziekteverzuim gestolen. De hackers gebruikten gijzelsoftware. Een deel van de buit verscheen op het darkweb, met dreiging tot meer als er niet betaald werd. Criminelen kijken niet naar je branche. Ze kijken naar kansen. Een plantenkwekerij, een afvalverwerker, een hotelketen – iedereen met data is een doelwit

Doe deze checks met regelmaat

- **Maandelijks: MFA-dekking, open poorten, patchstatus.**
- **Elk kwartaal: toegangsrechten opschonen, back-up restore testen, phishing-simulatie.**
- **Halfjaarlijks: een ransomware-scenario oefenen.**
- **Jaarlijks: leveranciers en wachtwoordbeleid tegen het licht houden.**

Kort gezegd: criminelen komen via mensen, gestolen wachtwoorden en vergeten systemen. MFA, updates, back-ups en bewustwording verhogen de drempel enorm. Je hoeft niet onkwetsbaar te zijn; je moet vooral geen makkelijk doelwit zijn.

Hoe goed is jouw organisatie beschermd?

Een hack kan vertrouwelijke informatie blootleggen, systemen stilleggen en medewerkers belemmeren in hun werk. Naast herstelkosten en omzetverlies kan reputatieschade ontstaan. Met een pentest onderzoek je waar jouw organisatie kwetsbaar is en welke maatregelen prioriteit hebben.

Waarom een pentest?

Een pentest toetst hoe je beveiliging in de praktijk werkt. Ethische hackers proberen binnen afgesproken grenzen toegang te krijgen tot systemen. Kunnen zij klantgegevens, contracten of technische ontwerpen inzien? Kunnen zij verder komen in het netwerk? En welke bedrijfsprocessen kunnen daardoor geraakt worden?

De uitkomsten helpen je om gericht te investeren in beveiliging en onderbouwde keuzes te maken over risico's.

Weet waar je staat

- Welke informatie en systemen zijn essentieel voor onze bedrijfsvoering?
- Wanneer zijn deze voor het laatst met een pentest onderzocht?
- Zijn gevonden kwetsbaarheden verholpen en is dat gecontroleerd?

Systemen en toegangsrechten veranderen. Bepaal daarom wanneer opnieuw onderzoek nodig is, bijvoorbeeld na een belangrijke wijziging.

Mensen en herstel

Leer medewerkers verdachte situaties herkennen en melden. Oefen hoe je handelt bij een incident. Test ook je back-ups: die helpen bij herstel, maar buitgemaakte informatie kan nog steeds worden verspreid of misbruikt.

Van inzicht naar verbetering

Cybernext voert onafhankelijke pentests uit en vertaalt technische bevindingen naar begrijpelijke risico's en concrete verbeterstappen voor management en technische teams. Met bewustwording en praktische training helpen we ook medewerkers om veilig te handelen.

Securitytips

Praktisch veiliger online werken

Een initiatief van Cybernext

info@cybernext.nl | 085-0604084

Wil je weten wat een pentest voor jouw organisatie kan opleveren? Spreek ons aan tijdens de bijeenkomst op 29 oktober of neem contact op:

Voorbereiden op onverwachte situaties

De samenleving moet voorbereid zijn op onverwachte situaties. Communicatie speelt daarbij een sleutelrol: overheid, veiligheidsregio's, maatschappelijke organisaties én bedrijven dragen samen verantwoordelijkheid. Ook ondernemers moeten nadenken over wat er gebeurt als processen of voorzieningen uitvallen en hoe zij continuïteit kunnen waarborgen.

VeiligheidsregioFlevoland

Weerbaarheid betekent vooruitdenken: wat kan er misgaan, wat is de impact en welke maatregelen zijn nodig? Het gesprek hierover binnen organisaties is essentieel. De NCTV biedt hiervoor een gesprekstool met instructies en gesprekskaarten. Deze helpen bedrijven scenario's te verkennen en hun weerbaarheid te versterken. Je vindt ze op de website van de NCTV: **www.nctv.nl**

Lees op www.aivd.nl meer over veilig digitaal werken.