



POLAR RISK

Voorbeeld cyberrisico- scenario's

Per sector

Inleiding

Een goede risicoanalyse valt of staat met duidelijke risicoscenario's. De Polar Risk [Scenariobouwer](#) helpt je met het formuleren van risicoscenario's.

De European Union Agency for Cybersecurity (ENISA) publiceert jaarlijks een dreigingsrapport. Dit dreigingsrapport beschrijft (sectorale) trends in dreigingen en aanvalsmethoden. Hiermee is het een nuttige bron voor organisaties.

Polar Risk heeft de inzichten uit het [dreigingsrapport van 2025](#) ter illustratie en inspiratie vertaald naar risicoscenario's.

De risicoscenario's zijn samengesteld op basis van de methode uit de [FAIR™ Cyber Risk Taxonomy](#) van het [FAIR Institute](#).

Blauwdruk risicoscenario

Elk scenario bestaat uit een aantal vaste elementen:

- Een **dreiging**
Wie of wat bedreigt het functioneren van een systeem of data?
- Een **asset**
Welk systeem of data wordt bedreigd?
- Een **methode**
Op welke manier wordt het systeem of data bedreigd?
- -Optioneel- een **aanvalspad**
Wat, waar of waarmee start de aanval?
- Een **effect**
Op welke manier ondervindt de organisatie hinder of schade?

Daarmee ontstaat de volgende structuur:

<Dreiging> valt <asset> aan met <methode> via <aanvalspad>, met als gevolg <effect>.

Algemeen

Cyberrisico's zijn bedrijfsrisico's. Organisaties hebben met behulp van ICT hun bedrijfsvoering gedigitaliseerd. Betrouwbare ICT en data is daarmee een randvoorwaarde voor de bedrijfsvoering geworden.

Dreigingen

Cybercriminelen hebben een financieel oogmerk met de aanvallen die ze uitvoeren; er moet geld mee verdiend worden. Datadiefstal en ransomware zijn bekende voorbeelden hiervan.

Organisaties afhankelijk van ICT zijn daarmee een interessant doelwit. Ongeacht de sector.

Voorbeeldscenario's

Een aantal cyberrisico's zijn relevant voor praktisch alle organisaties.

- Cybercriminelen vallen de ICT-infrastructuur aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.
- Cybercriminelen vallen de ICT-infrastructuur aan met ransomware via kwetsbaarheden (CVE), met als gevolg bedrijfsonderbreking.
- Cybercriminelen vallen het klanten- of personeelsbestand aan met data-exfiltratie via phishing, met als gevolg inbreuk op de privacy van informatie.
- Cybercriminelen vallen het cloud- of hostingplatform aan met cryptomining via kwetsbaarheden (CVE), met als gevolg financieel verlies.
- Hacktivisten vallen de website aan met een DDoS via een botnet, met als gevolg bedrijfsonderbreking.

Deze scenario's zijn algemeen van aard. Maak ze specifiek voor jouw organisatie door de asset verder te specificeren.

Bijvoorbeeld door de asset "het personeelsbestand" te vervangen door de naam van het HR softwarepakket in gebruik in jouw organisatie.

Transport

De transportsector is de afgelopen jaren in rap tempo gedigitaliseerd. Belangrijke processen zoals het bijhouden van goederen of passagiers en het plannen van routes zijn vrijwel volledig gedigitaliseerd.

Dreigingen

Door deze afhankelijkheid van technologie is de transportsector een interessant doelwit voor cybercriminelen. Daarnaast is de sector door zijn globale karakter ook een interessant doelwit voor hacktivisten en staats-gelieerde aanvallers vanuit een geopolitiek oogpunt.

Denk bijvoorbeeld aan steun voor Oekraïne of het spelen van een rol in internationale sancties.

Voorbeeldscenario's

- Cybercriminelen vallen de planning-, passagier- of goederensystemen aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.
- Cybercriminelen vallen planning-, passagier- of goederensystemen aan met ransomware via kwetsbaarheden (CVE), met als gevolg bedrijfsonderbreking.
- Hacktivisten vallen de website aan met DDoS via een botnet, met als gevolg bedrijfsonderbreking.
- Staats-gelieerde aanvallers vallen planning-, route- en sanctiedata aan met data-exfiltratie via phishing met als gevolg inbreuk op de vertrouwelijkheid van informatie.
- Staats-gelieerde aanvallers vallen planning-, route- en sanctiedata aan met data-exfiltratie via kwetsbaarheden (CVE) met als gevolg inbreuk op de vertrouwelijkheid van informatie.

Maakindustrie

De maakindustrie bestaat uit een divers palet aan organisaties. Van fabrikanten van consumentengoederen, tot automotive tot aan defensie.

Dreigingen

Voor cybercriminelen is de sector een interessant doelwit. Een verstoring in de IT of OT heeft direct impact op de productie.

Vanuit een geopolitiek oogpunt is de sector een gewild doelwit voor cyberspionage (intellectueel eigendom) of hacktivisme vanuit ideologisch oogpunt.

Voorbeeldscenario's

- Hacktivisten vallen Operational Technology aan met DDoS via een botnet, met als gevolg bedrijfsonderbreking.
- Cybercriminelen vallen Operational Technology aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.
- Cybercriminelen vallen de webshop aan met een DDoS via een botnet, met als gevolg bedrijfsonderbreking.
- Staats-gelieerde aanvallers vallen intellectueel eigendom aan met data-exfiltratie via kwetsbaarheden (CVE), met als gevolg inbreuk op de vertrouwelijkheid van informatie.
- Staats-gelieerde aanvallers vallen intellectueel eigendom aan met data-exfiltratie via supply chain compromitatie, met als gevolg inbreuk op de vertrouwelijkheid van informatie.

Digitale Infrastructuur & Dienstverlening

De sector digitale infrastructuur en dienstverlening omvat onder andere hosting- en telecomproviders, software-ontwikkelaars en leveranciers van digitale consumentenproducten en -diensten.

Dreiging

Voor zowel cybercriminelen en staats-gelieerde aanvallers is de sector een interessant doelwit vanwege de hoeveelheid gevoelige data die zij beheren. Van persoonsgegevens van klanten tot aan bedrijfsgeheimen die opgeslagen of verwerkt worden in opdracht van een groot aantal klanten.

Voorbeeldscenario's

- Hacktivisten vallen de website aan met DDoS via een botnet, met als gevolg bedrijfsonderbreking
- Cybercriminelen vallen klantdata aan met data-exfiltratie via phishing, met als gevolg inbreuk op de vertrouwelijkheid van informatie.
- Cybercriminelen vallen de ICT-infrastructuur aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.

Gezondheid

In de gezondheidszorg staat het welzijn van patiënten voorop. De sector wijkt af van andere sectoren in de zin dat cyberrisico's niet alleen een maatschappelijk of economisch effect hebben, maar in het ergste geval ook lichamelijk of mentaal. Het niet kunnen leveren van acute zorg of het uitstellen van planbare zorg kan leiden tot letsel.

Dreigingen

Voor cybercriminelen is de sector een interessant doelwit, omdat bedrijfsonderbreking als gevolg van bijvoorbeeld een ransomware-aanval direct het welzijn van patiënten onder druk zet.

- Cybercriminelen vallen patiëntendossiers aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.
- Cybercriminelen vallen zorgsystemen aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.

Overheid

Op verschillende niveaus vervult de overheid een maatschappelijke functie. In tegenstelling tot de for-profit sectoren, is de overheid minder gevoelig voor financiële prikkels in de context van cyberrisico's

Dreigingen

Voor hacktivisten is de overheid een gewild doelwit met DDoS-aanvallen. Beleidskeuzes op centraal of regionaal niveau, verkiezingen of andere gebeurtenissen met een hoge mate van nationale aandacht zijn aanleiding voor deze aanvallen.

Op lokaal niveau is de dreiging van ransomware door cybercriminelen meer aanwezig.

Staats-gelieerde aanvallers richten zich met name op overheidsorganisaties met diplomatieke, wetgevende of uitvoerende taken. Enerzijds uit interesse voor de identiteit van werknemers en anderzijds voor de inhoudelijke besluitvorming.

Voorbeeldscenario's

- Staats-gelieerde aanvallers vallen medewerkersgegevens aan met data-exfiltratie via kwetsbaarheden (CVE), met als gevolg een inbreuk op de privacy van informatie.
- Cybercriminelen vallen de ICT-infrastructuur aan met ransomware via phishing, met als gevolg bedrijfsonderbreking.

En nu verder?

Een goed risicoscenario stelt je in staat om concreet te maken wat mis kan gaan en daarmee de kans en impact te onderbouwen.

Kans

De kans dat het risicoscenario zich voordoet is gebaseerd op twee elementen:

- De dreiging
Hoe vaak probeert de dreiging het risicoscenario te laten gebeuren?
- Getroffen maatregelen
Hoe succesvol zijn de getroffen preventieve maatregelen in het voorkomen van het risicoscenario?

Impact

De impact draait om de verliezen die kunnen optreden voor de organisatie op het moment dat het risicoscenario zich voordoet. Deze verliezen zijn afhankelijk van het soort effect uit het risicoscenario.

Grofweg zijn er twee soorten verliezen die optreden:

- **Primaire** verliezen die optreden als direct gevolg van het risicoscenario
Bijvoorbeeld een verlies van omzet door de bedrijfsonderbreking, IT-forensisch onderzoek en herstelkosten.
- **Secundaire** verliezen die optreden als indirect gevolg van het risicoscenario
Bijvoorbeeld boetes opgelegd door een toezichthouder, aansprakelijkstelling door een klant of boeteclausules uit contracten.

Wil je op de hoogte blijven van soortgelijke handreikingen? Meld je dan gratis aan voor de Polar Risk mailinglist.

Klik hier om je aan te melden



POLAR RISK

De scenario's in dit document zijn illustratief en bedoeld als inspiratie en vormen geen beveiligingsadvies. Vertaal de scenario's altijd naar de specifieke context van jouw organisatie. Polar Risk geeft geen garantie op volledigheid, actualiteit of toepasbaarheid voor een specifieke situatie; het gebruik van dit document blijft de verantwoordelijkheid van de gebruiker.