Cyberveiligheid in de industriële sector

De Nederlandse industriële sector hoort bij de wereldtop en levert een belangrijk aandeel in de export en het scheppen van hoogwaardige werkgelegenheid. Om die positie te behouden en door te groeien, is innoveren en het omarmen van (nieuwe) digitale technologieën cruciaal. Als industrieel bedrijf bevat uw productieproces diverse digitale technologieën; het gebruik van internet, op afstand bestuurbare robots en digitale dataopslag worden als vanzelfsprekend gezien. Maar tegenover de vele voordelen van digitalisering staat de toename van veiligheidsrisico's. Binnen uw eigen organisatie, maar ook in de (leveranciers)keten.

Voor de omgang met deze risico's bestaat lang niet altijd al beleid, laat staan dat er maatregelen genomen zijn om ze te verkleinen. In hoeverre bent u zich bewust van de risico's en hoe cyberveilig is uw organisatie?

Van hack tot menselijke fout

Cybervraagstukken zijn er in allerlei soorten en maten. Het kan gaan om bekende zaken als hacks, infecties door malware of een onbeveiligde laptop vol bedrijfsgegevens die wordt verloren. Er zijn echter nog veel meer risico's door het gebruik van digitale technologie, waar soms niet aan gedacht wordt of waartegen de beveiliging afdoende lijkt, maar dat eigenlijk niet is. Een leverancier die bijvoorbeeld is geïnfiltreerd door cybercriminelen en u (onbewust) gemanipuleerde informatie toestuurt. Of een medewerker die thuis werkt via een onveilige wifi-verbinding.

Voor fabrikanten verdelen wij de cyberrisico's in drie deelgebieden, te weten:

- ketenintegratie
- bedrijfscontinuïteit
- de medewerkers van een onderneming

We vatten bij elk deelgebied de cyberrisico's samen.

Ketenintegratie: grotere efficiency, meer kans op dreigingen

De industriële sector is bij uitstek een branche waar goede ketenintegratie het verschil maakt. Snelle en duidelijke lijnen met verschillende leveranciers en klanten zorgen dat u sneller, beter én goedkoper kunt produceren. De toenemende mate van ketenintegratie zorgt echter ook voor een vergroot risico op cyberaanvallen. Hoe groter of complexer de supply chain wordt, hoe meer potentiële zwakke plekken er ontstaan. Twee ontwikkelingen zijn in 2019 van belang:

- Door de explosieve toename in koppeling van apparaten via het internet krijgen cybercriminelen steeds meer opties om binnen te dringen. Dit kan binnen uw eigen bedrijf zijn, maar ook via een van de toeleveranciers.
- 'Just in time'-leveringen groeien in belang. Om de supply chain optimaal in te zetten, worden datastromen aangeboden door toeleveranciers of service providers.

AON
Empower Results®

Bij ketenintegratie spelen niet alleen risico's als hacks of malware een rol, maar ook de betrouwbaarheid van uw informatie. Hoe zeker kunt u zijn dat de gegevens die u via leveranciers binnenkrijgt volledig juist zijn? Het manipuleren van bijvoorbeeld betalingsverkeer of productspecificaties komt in de praktijk al voor en verdient uw aandacht, want de verwachting is dat dit sterk gaat toenemen.

Bedrijfscontinuïteit: cyberrisico's hebben grote impact

Cyberveiligheid raakt ook de continuïteit van uw bedrijf. Een te grote afhankelijkheid van digitale technologieën kan ervoor zorgen dat de productie of dienstverlening stopgezet moet worden. In een sector als de industrie kan dit niet alleen tot stilstand leiden, maar zelfs tot grote schade aan installaties of levensbedreigende situaties voor medewerkers en klanten. De imagoschade die kan ontstaan wanneer een grote crisis ontstaat door een cyberincident, kan daarnaast leiden tot het einde van uw bedrijf.

Het in kaart brengen van de risico's is daarom van groot belang. Zorg niet alleen voor een goede beveiliging van systemen en apparaten. Weet wat er kan gebeuren en hoe u daarmee om moet gaan.

Medewerkers: de zwakste schakel?

Uw medewerkers vormen een ander essentieel onderdeel van uw cyberveiligheid. Sterker nog, zij vormen op dit gebied zelfs de zwakste schakel binnen uw bedrijf. In 2018 bleek uit onderzoek onder cyberprofessionals dat 53% van de ondervraagden zogenaamde insider-aanvallen had meegemaakt. Dat was lang niet altijd een bewuste poging van medewerkers om schade aan te richten: onwetendheid kan hier net zo goed voor zorgen.

Wanneer u medewerkers toegang geeft tot belangrijke informatie, schept u enerzijds vertrouwen, maar vergroot u ook de kans op misbruik van die informatie. Omgekeerd, wanneer uw personeel merkt dat zij weinig rechten hebben op ICT-gebied, bestaat de kans dat zij op eigen houtje andere oplossingen gaan gebruiken (denk aan cloud-omgevingen, privé-mail of eigen mobiele apparaten), met hierbij ook weer een verhoogd risico. Het delen van verantwoordelijkheden is op dit gebied dan ook verstandig. Door uw medewerkers bewust te maken van het thema cyberveiligheid en gedragscodes vast te leggen, weten zij wat er van hen verwacht wordt en waar grenzen liggen.

Bent u zich bewust van alle risico's op het gebied van cyberveiligheid in de industriële sector? Zijn uw bedrijfsgegevens voldoende beveiligd? Heeft u inzicht in de dreigingen die kunnen optreden via zwakke plekken in uw supply chain of door (onbewuste) handelingen van uw eigen personeel? Aon kan u helpen met het in kaart brengen van al deze risico's en hoe u hiermee omgaat.

Wij helpen u graag succesvol te ondernemen

Neem contact op voor meer informatie of een vrijblijvende afspraak over cyberveiligheid.

Jean-Pierre Palmen
Aon Industry Senior Manufacturing
m jean.pierre.palmen@aon.nl
t +31 (0)88 343 4624

Maarten de Jonge
Sr. consultant cyber solutions
cybersolutionsgroup@aon.nl
m +31 (0)10 4487765

aon.nl

19.0024-01-cyber-industr-V2

Empower Results®