

Alarmerende realiteit van cyberaanvallen in kmo's in de industrie

23 augustus 2021, 02:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

In tijden van digitale transformatie en Industrie 4.0 is cybercriminaliteit nog nooit zo reëel geweest voor Belgische kmo's. Elk bedrijf dat niet over voldoende beveiligingsveerkracht beschikt is een potentieel slachtoffer. Kmo's hebben een strategie op maat en een duidelijk stappenplan voor veerkracht nodig om zichzelf te beschermen tegen dergelijke aanvallen, maar er zijn nog hindernissen te overwinnen. Sirris kan hierbij helpen!

Grote bedrijven zijn niet langer het enige doelwit van cybercriminelen. Ook in kmo's zijn cyberaanvallen een veelvoorkomend probleem. Elk jaar bereiken dreigingen voor verbonden productiebedrijven een kritiek punt. Momenteel zijn er meer dan 30.000 cyberaanvallen geregistreerd met een jaarlijkse stijging van 20 procent van het aantal incidenten. Cybercriminaliteit is nog nooit zo reëel geweest voor Belgische kmo's. De digitale transformatie en Industrie 4.0 vormen een groot risico voor ondernemingen omdat verouderde machines met een hoog beveiligingsrisico verbonden zijn en data verzameld en uitgewisseld worden tussen websites zonder enige controle. Elk bedrijf dat niet beschikt over voldoende beveiligingsveerkracht kan slachtoffer worden van cybercriminaliteit en de gevolgen van beveiligingsinbreuken (onderbreking van activiteiten, gegevensverlies en een reputatiebeschadiging) kunnen een bedrijf onderuithalen. Indien dit al niet het geval is kan het maanden of zelfs jaren duren om ervan te herstellen. Om zich tegen dergelijke aanvallen te beschermen hebben kmo's een strategie op maat en een duidelijk stappenplan voor terugveerkracht nodig.

Momenteel zien we twee grote hindernissen die ervoor zorgen dat kmo's hun cyberbeveiligingsstrategie niet kunnen realiseren of implementeren:

- Cyberdiensten aangeboden door commercieel georiënteerde professionele bedrijven in België zijn veel te duur en onbereikbaar voor de meeste kmo's die over beperkte middelen beschikken.
- De bestaande normen en richtlijnen met betrekking tot cyberbeveiliging zijn ofwel te algemeen ofwel te technisch, waardoor het voor de mensen in industriële kmo's met een beperkte kennis en achtergrond moeilijk is om ze te begrijpen en te gebruiken voor de realisatie van hun cyberbeveiligingsstrategie.

Nieuwe flexibele aanpak

Sirris begrijpt deze pijnpunten en heeft een nieuwe flexibele aanpak van cyberbeveiliging ontwikkeld om kmo's te helpen bij het realiseren van hun cyberbeveiligingsstrategie zonder al te veel moeite en financiële middelen te investeren.

We begrijpen dat vertrouwen essentieel is om te komen tot het informatieniveau dat hierbij nodig is en daarom starten we met een gratis online intakesessie van 1 uur. Het opzet van deze laagdrempelige benadering is om ervoor te zorgen dat bedrijven zo snel mogelijk hun cyberbeveiligingsniveau verhogen. Ook kunnen ze in deze sessie nagaan of de aanpak van Sirris omtrent cyberbeveiliging datgene is wat het bedrijf nodig heeft.

In deze eerste sessie richten we ons kort op drie domeinen:

- IT (kantoor)-infrastructuur
- OT (productie)-infrastructuur maar ook de integratie tussen IT en OT
- Gegevensbeveiligingsaspecten (bv. is de intellectuele eigendom genoeg beschermd? enz.)



Visuals, gegevens en OT (drie domeinen)

Na deze sessie zorgen we voor een gestructureerd rapport met de reeds gedetecteerde problemen en geven we daarbij ons advies over hoe deze problemen aan te pakken. We maken ook een schatting van het maturiteitsniveau van elk onderdeel. Op die manier weten bedrijven waar ze staan en naar welk niveau ze zouden moeten evolueren.

Het bedrijf kan op basis van de aanbeveling(en) in dit document onmiddellijk beginnen met het verbeteren van de algemene cyberbeveiliging.

Cyberbeveiligingsscan

Indien het bedrijf nog een stap verder wil gaan en een diepgaandere cyberbeveiligingsscan wenst te krijgen, komen we ter plaatse en gaan we veel dieper in op alle afzonderlijke punten op basis van de resultaten van beveiligingsscan's en interviews.

Het resultaat van de scan levert een gestructureerde tabel op van bedrijfsmiddelen, kwetsbaarheden en risico's. Het bedrijf kan op die manier gemakkelijker een beslissing nemen over de volgende te nemen stappen en prioriteiten voor een veerkrachtigere cyberbeveiliging.

Domein	Bedrijfsmiddel	Bestaande controles	Kwetsbaarheid	Risico's

OT-beveiliging	IoT-sensor-apparaten	Verbonden via firewall Begrensde poorten Beperkte toegangstijd	• Kwetsbaarheid in de firmware • Onvoldoende controle • Ontoereikende authenticatie	Kritisch: • Fout in de firmwarecode kan een buffer- overflow veroorzaken • Criminelen krijgen gemakkelijk toegang tot het toestel door het wachtwoord te raden via 'brutal force' aanvallen. Medium: • Onnodig geopende poort maakt DDoS-aanval op een apparaat mogelijk Laag: • Onjuist geconfigureerde bewaking leidt tot heel wat valse positieven
Data-beveiliging	Persoonlijke gegevens werknemer	Opgeslagen op een beveiligde server Beperkte toegang	• Zwakke cryptografie • Ontoereikende toegangscontrole • Geen gegevens-classificatie	Kritisch: • Criminelen hebben toegang tot privégegevens en publiceren deze • Criminelen misbruiken de PII- gegevens om in te breken in het account van de werknemer • Criminelen gebruiken PII-gegevens om zich voor te doen als bedrijfsmanagers voor 'spear phishing' Medium: • Criminelen versleutelen of verwijderen de PPI-gegevens

Deze gestructureerde tabel maakt het mogelijk om te verwijzen naar mogelijke problemen en deze onmiddellijk te beschrijven. Op die manier kan men deze problemen sneller en efficiënter oplossen.

Tijd voor actie

Wilt u meer weten over onze aanpak of deelnemen aan een gratis 1 uur durende intake? Neem contact op met security@sirris.be of met Tatiana.Galibus@sirris.be om u in te schrijven.

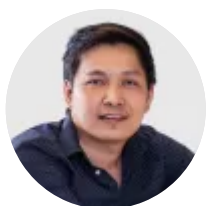
Wilt u meer info over cybersecurity in manufacturing of hebt u een specifieke vraag? [Klik dan hier!](#)



(Bron beeld banner: iStock)

]]>

Auteurs



Annanda Rath



Christophe Michiels



Tatiana Galibus