

Inquiétante explosion de cyberattaques dans les PME manufacturières

23 août 2021, 02:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

En ces temps de transformation numérique et d'Industrie 4.0, le risque de cybercriminalité n'a jamais été aussi réel pour les PME belges. Toute entreprise qui n'est pas suffisamment protégée peut en être victime. Pour se protéger des cyberattaques, les PME nécessitent une stratégie sur mesure et une feuille de route précise pour assurer leur résilience. Alors que cette démarche peut être malaisée à mettre en œuvre, Sirris peut vous aider !

Les cyberattaques ne sont plus l'apanage des grandes entreprises, mais touchent désormais de plus en plus souvent les PME. Chaque année, les menaces visant la production connectée atteignent un point critique. On dénombre aujourd'hui plus de 30 000 cyberattaques enregistrées, avec une croissance annuelle de 20% du nombre d'incidents. La cybercriminalité n'a jamais été aussi préoccupante pour les PME belges. La transformation numérique et l'Industrie 4.0 s'accompagnent de risques graves pour les entreprises lorsque d'anciennes machines à haut risque pour la sécurité sont connectées et que des données sont collectées et échangées entre plusieurs sites sans aucun contrôle. Toute entreprise qui n'est pas dotée d'un système de sécurité suffisant peut être victime de cybercriminalité et subir les conséquences d'une faille de sécurité - interruptions d'exploitation, perte de données et réputation ternie - qui peuvent anéantir l'activité ou nécessiter des mois voire des années avant d'être maîtrisées. Pour se protéger de telles attaques, les PME nécessitent une stratégie sur mesure et une feuille de route précise en matière de résilience.

Il existe aujourd'hui 2 obstacles majeurs empêchant les PME de définir ou mettre en œuvre leur stratégie de cybersécurité :

- Les entreprises belges de cybersécurité privilégient leurs propres profits et proposent des cyber-services trop coûteux et inatteignables pour la plupart des PME disposant des ressources limitées.
- Les standards et directives de cybersécurité existants sont soit trop généraux soit trop techniques pour permettre au personnel des PME manufacturières possédant une expérience et des connaissances limitées de les comprendre et de les appliquer pour réaliser leur stratégie de cybersécurité.

Nouvelle approche flexible

Ayant identifié ces 2 obstacles, Sirris a développé une nouvelle approche flexible de la cybersécurité pour aider les PME à réaliser leur stratégie de cybersécurité sans investir trop de temps et de ressources financières.

Etant donné qu'une relation de confiance est primordiale pour obtenir le niveau d'information dont nous avons besoin, nous commençons par une session d'introduction en ligne gratuite d'une 1 heure. L'objectif de notre approche accessible à tous est d'encourager les entreprises à se lancer le plus rapidement possible dans l'amélioration de leur niveau de cybersécurité. Cette session leur permet aussi de s'assurer que l'approche de Sirris en matière de cybersécurité est bien ce dont leur entreprise a besoin.

Cette première session se concentre brièvement sur 3 domaines :

- Infrastructure IT (de bureau)
- Infrastructure OT (de production) et intégration entre technologies IT et OT
- Aspects de sécurité des données (par ex. la propriété intellectuelle est-elle suffisamment protégée, etc.)



Illustrations graphiques, données et OT (3 domaines)

Au terme de cette session, nous remettons au client un rapport structuré présentant les problèmes que nous avons déjà détectés ainsi que quelques conseils sur la meilleure façon de les traiter. Pour chaque point soulevé, nous estimons également le niveau de maturité de l'entreprise pour qu'elle sache où elle en est et vers quel niveau elle devrait évoluer.

L'entreprise peut se baser sur les recommandations de ce rapport pour se lancer immédiatement dans l'amélioration de son niveau de cybersécurité général.

Scan de cybersécurité

Si l'entreprise souhaite aller plus loin et obtenir un scan de cybersécurité plus approfondi, nous allons sur place et examinons beaucoup plus en détail l'ensemble des sujets au moyen d'outils de scannage de sécurité et d'interviews.

Les résultats du scannage sont synthétisés dans un tableau structuré présentant les actifs, les vulnérabilités et les risques. Ce tableau aide l'entreprise à définir les priorités et la marche à suivre pour évoluer vers un niveau de cybersécurité plus résilient.

Domaine	Actif	Contrôles en place	Vulnérabilité	Risques
---------	-------	--------------------	---------------	---------

Sécurité OT	Capteurs IoT	Connectés avec pare-feu Ports réservés Temps d'accès limité	• Micrologiciel vulnérable • Audit insuffisant • Authentification inadéquate	Critiques : • Erreur dans le code du micrologiciel peut causer un dépassement de tampon • Un fraudeur peut facilement obtenir l'accès d'un dispositif en devinant un mot de passe vulnérable Moyens : • Un port inutilement ouvert peut permettre de réaliser une attaque par déni de service (DDoS) sur un dispositif Faibles : • Un suivi mal configuré entraîne un excès de faux positifs
Sécurité des données	Données personnelles des employés	Stockées sur un serveur protégé Accès limité	• Cryptographie vulnérable • Contrôle d'accès insuffisant • Absence de classification des données	Critiques : • Le fraudeur obtient et publie des données personnelles • Le fraudeur détourne des données personnelles pour accéder au compte d'un employé • Le fraudeur utilise les données personnelles pour se faire passer pour un cadre de l'entreprise et mener une attaque d'hameçonnage Moyens : • Le fraudeur chiffre ou supprime des données personnelles

Ce tableau structuré permet d'identifier d'éventuels problèmes et de les décrire directement afin de les traiter plus rapidement et efficacement.

Passer à l'action

Vous souhaitez en savoir plus sur notre approche ou participer à une session d'introduction gratuite d'une heure ? Alors, contactez security@sirris.be ou Tatiana.Galibus@sirris.be pour vous inscrire.

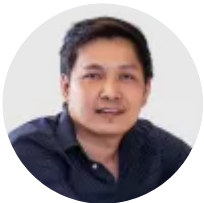
Vous souhaitez de plus amples informations sur les produits intelligents connectés ? Vous avez une question spécifique ? [Voir notre page web ou contactez-nous !](#)



(Source image banner: iStock)

]]>

Auteurs



Annanda Rath



Christophe Michiels



Tatiana Galibus