Cybersecurity 4.0 : conclusions de l'enquête sur les besoins des entreprises manufacturières en matière de cybersécurité

30 mars 2023, 15:53

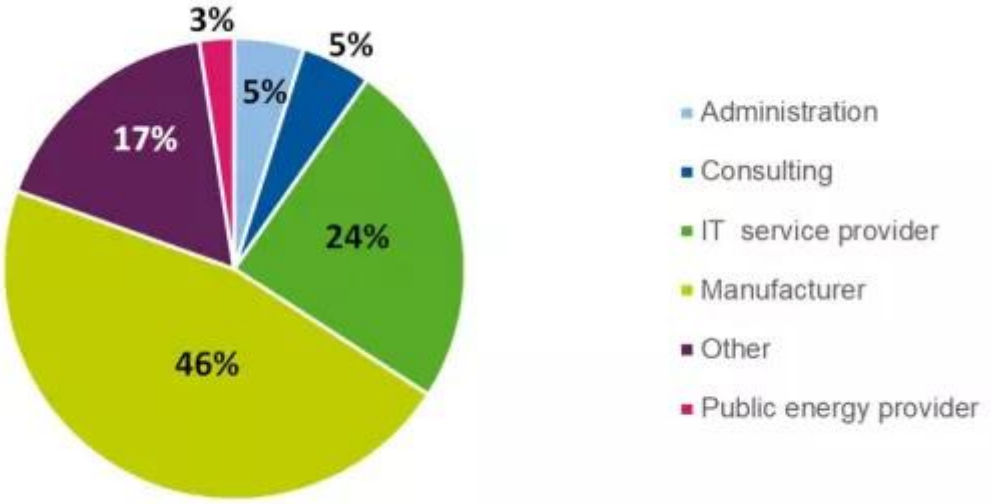
Tatiana Galibus
Annanda Rath

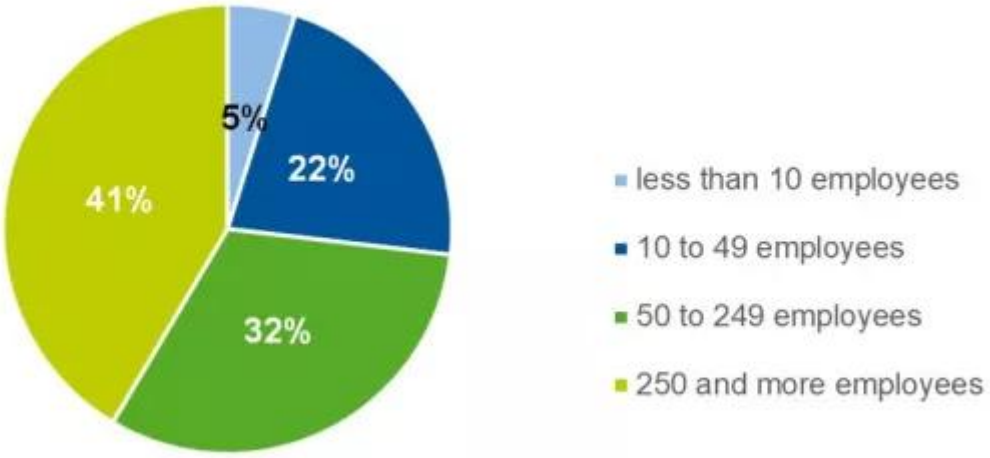
De mars à octobre 2022, dans le cadre du projet de recherche Cybersecurity 4.0., nous avons mené une enquête auprès d'entreprises manufacturières de Belgique et d'Allemagne. Ce billet de blog fait le point sur les conclusions de cette enquête et sur les tendances intéressantes circonscrites à cette occasion.

Cybersecurity 4.0 est un projet de recherche dont l'ambition est de proposer aux PME un cadre de cybersécurité et d'apprentissage viable, qui accorde la priorité à la connectivité ainsi qu'à la sécurité des données et de la chaîne logistique.

Analyse des cas et des besoins des utilisateurs

41 entreprises ont été interrogées ou sondées.





Nous avons analysé les conclusions de l'enquête au moyen d'une méthodologie statistique de classification, de notation et d'évaluation. L'enquête a circonscrit **trois grands profils d'entreprises** : les entreprises manufacturières, les PME et les prestataires de services. Nous avons identifié 11 grands axes en matière de sécurité, à prendre en compte par les entreprises soucieuses de leur cybersécurité. Épinglons la sécurité des réseaux et des données, la sécurité de la chaîne logistique, le contrôle d'accès et la sécurité OT/IOT.

Risques en matière de sécurité dans les entreprises manufacturières

Nous avons identifié les **risques les plus élevés en matière de sécurité** pour le secteur manufacturier. Force est de constater que des lacunes en matière de sécurité y subsistent encore dans de nombreux domaines essentiels, principalement la surveillance du contrôle d'accès, la classification des données, la formation à la cybersécurité et l'évaluation des risques de sécurité des maillons de la chaîne logistique. Parmi les 20 (soit 46 %) entreprises interrogées et ayant répondu à l'enquête en ligne, 13 ne classifient pas leurs données, 11 ne contrôlent pas l'accès à leur système et à leur réseau et 8 ne chiffrent pas leurs sauvegardes. Plus de 50 % des entreprises (12) n'évaluent pas les risques de sécurité de leurs partenaires logistiques et 10 ne disposent pas de programmes de formation à la cybersécurité, pourtant considérée comme un élément essentiel des bonnes pratiques en matière de cybersécurité.

Deficit	Frequencies	Comments
No back up encryption	8	+ 1 "Not specified" + 1 "Don't know"
No access control	5	-
No audit of access control	11	+ 1 "Don't know" + 1 "Not specified"
No data classification	13	+ 1 "Not specified"
No network segmentation	5	+ 2 "Don't know"
No network monitor	6	+ 1 "Don't know"
No cyber security training	6	-
No implementation standards for cyber security training	10	+ 2 "Don't know" + 7 "Not specified"
No risk assessment for supply chain partners	12	+ 2 "Don't know"

Tableau 1. Liste des lacunes en matière de sécurité dans les entreprises manufacturières interrogées

Security risks for service provider companies

Chez les fournisseurs de services, nous constatons une relative amélioration en matière de sécurité. Toutefois, des failles subsistent dans des domaines essentiels, comme le contrôle d'accès, la classification des données et l'évaluation des risques de sécurité des maillons de la chaîne logistique. 5 entreprises sur 10 (soit 24 %) ne disposent toujours pas d'un système de contrôle d'accès adéquat ou de bonnes pratiques en la matière. 7 sur 10 ne procèdent pas à l'évaluation des risques de sécurité chez leurs partenaires logistiques. 4 entreprises ne disposent pas d'un programme de formation à la cybersécurité, pourtant considérée comme un élément

Deficit	Frequencies	Comments
No backup encryption	1	+ 4 "Not specified"
No access control	5	+ 1 "Not specified"
No audit of access control	5	+ 1 "Not specified"
No data classification	5	+ 1 "Don't know" + 1 "Not specified"
No network segmentation	2	+ 1 "Not specified"
No network monitor	3	+ 2 "Not specified" + 1 "Don't know"
No cyber security training	4	
No implementation standards for cyber security training	4	+ 4 "Not specified" + 1 "Don't know"
No mitigation plan	4	+ 2 "Not specified"
No risk assessment for supply chain partners	7	-

Tableau 2. Liste des lacunes en matière de sécurité chez les prestataires de services

Risques en matière de sécurité dans les PME

59 % des 41 entreprises sondées et interrogées sont des PME (c'est-à-dire des entreprises de moins de 250 salariés). Nous observons des similitudes s'agissant des lacunes en matière de sécurité, allant du contrôle d'accès à la classification des données, en passant par la surveillance du réseau, la formation à la cybersécurité ou le plan d'atténuation et d'évaluation des risques de sécurité chez les partenaires logistiques.

Deficit	Frequencies	Comments
No backup encryption	-	+ 1 "not specified" + 1 "don't know"
No access control	3	+ 1 "don't know"
No audit of access control	4	+ 1 "don't know"
No data classification	4	+ 1 "don't know"
No network segmentation	4	-
No network monitor	2	+ 1 "don't know"
No cyber security training	3	-
No implementation standards for cyber security training	3	+ 2 "not specified" + 2 "don't know"
No mitigation plan	2	+ 2 "don't know"
No risk assessment for supply chain partners	4	+ 1 "don't know"

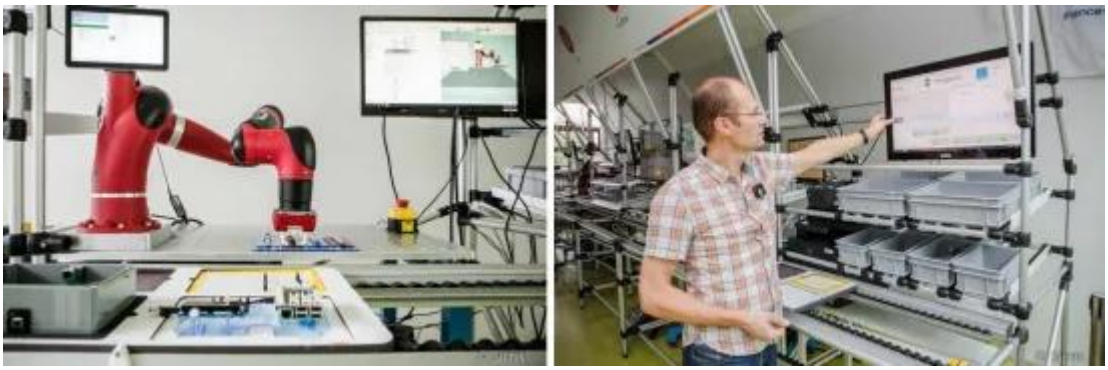
Tableau 3. Liste des lacunes en matière de sécurité dans les PME

Formulation d'un modèle de maturité, analyse de la vulnérabilité et des risques

Nous sommes occupés à définir des critères de maturité en matière de cybersécurité en fonction du profil de l'entreprise et du risque. Dès que nous aurons établi un modèle efficace et pertinent, e 1 à 4.

En avril, Sirris et FIR Aachen publieront le questionnaire d'enquête pour permettre à toute entreprise d'y répondre en ligne.

Dans une prochaine phase, nous établirons **un cadre, un outil web et des lignes directrices** sous la forme d'une plate-forme web d'appui à la cybersécurité. Un **démonstrateur** sera mis en œuvre. Il se présentera comme une chaîne de production connectée **simulant des scénarios de cyberattaque classiques et des mesures d'atténuation** pour différents niveaux de protection, dont des mesures et des configurations de sécurisation.



configuration actuelle du démonstrateur

Ensemble vers la cybersécurité 4.0

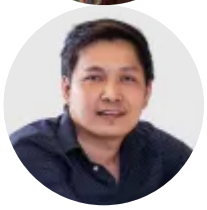
L'objectif du projet Cybersecurity 4.0 est de mettre au point des outils de sensibilisation et de diffusion. Vous vous intéressez à un aspect particulier de la cybersécurité ? Vous souhaitez examiner les résultats en détail ou organiser une visioconférence avec nous ou avec d'autres entreprises belges ? Contactez-nous!

Fin avril, nous organiserons une visioconférence du consortium belge, un webinaire destiné au groupe d'utilisateurs ou des séances de questions/réponses.
Le **27 avril**, Sirris lancera un programme de formation de deux mois, axé sur la pratique, pour assister les entreprises manufacturières dans leurs démarches en matière de cybersécurité. Inscrivez-vous!

Nous proposons aussi des séances de coaching individuel et des masterclasses dans vos locaux, afin de vous aider à concevoir votre propre stratégie de cybersécurité et à éliminer les risques spécifiques. Découvrez nos offres collectives ou individuelles !

Auteurs

Tatiana Galibus



Annanda Rath