20.05.2025

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Allemagne
https://www.pilz.com

Communiqué de presse

La cybersécurité industrielle, une affaire de dirigeants : comment les entreprises se lancent-elles ?

Ostfildern, Allemagne, 20.05.2025 - **Simon Nutz, Consultant en cybersécurité industrielle**

« La cybersécurité ? Cela ne nous concerne pas ! » – Lorsqu'il est question de cybersécurité, c'est encore une réponse courante de la part des fabricants et des exploitants de machines. « La cybersécurité est du ressort de notre service informatique », ajoutent-ils en s'excusant quelque peu. Mais dans la pratique, l'informatique manque de connaissances spécifiques, surtout en ce qui concerne les réseaux d'automatisation. D'autre part, les concepteurs ou les chargés de la sécurité (Health and Safety Manager, HSE) ne sont pas suffisamment à l'aise avec la cybersécurité. Alors comment se préparer à la cybersécurité industrielle ?

À partir de janvier 2027, le règlement machines doit être appliqué de manière obligatoire dans l'Union européenne. Il concerne toutes les entreprises qui souhaitent importer ou exploiter des machines dans l'Union européenne. Le règlement prévoit une cybersécurité industrielle sous la forme de mesures de protection contre la corruption. La cybersécurité industrielle devient ainsi une priorité commerciale et une responsabilité de gestion. Le personnel de direction doit veiller à ce que la cybersécurité industrielle soit ancrée dans l'entreprise.

Réunir tout le monde autour d’une table

Dans cette optique, la première étape consiste à réunir toutes les parties prenantes autour d’une table. Chez les constructeurs de machines, cela comprend les services Informatique et de Développement / Conception et – le cas échéant – les Responsables de la cybersécurité (par exemple, le RSSI). Chez les utilisateurs, il s’agit, en plus du service Informatique, des services Technique de production et Direction de la production, HSE et le RSSI. Il convient tout d’abord d’acquérir des connaissances et de développer une compréhension commune de la cybersécurité industrielle : Quelles sont les obligations légales qui incombent à l’industrie des machines et des installations ? Quel est le lien entre la sécurité et la cybersécurité ? Au niveau de quelles interfaces les technologies de l’information et de l’exploitation se rencontrent-elles ?

La deuxième étape consiste pour ces équipes interdisciplinaires à élaborer une stratégie adaptée à l’entreprise, y compris un concept de mise en œuvre. Cela implique de se repérer et de se structurer au sein de l’entreprise : Où se situeront les responsabilités à l’avenir ? Quelle est la topologie du réseau de ses propres machines ? Comment cela répond-il aux nouvelles obligations réglementaires ?

L’appréciation du risque marque le début de la mise en œuvre

Ensuite seulement, l’entreprise sera en mesure de mettre en œuvre le thème de la cybersécurité industrielle. Cela commence par l’évaluation et la quantification des événements dommageables possibles et l’élaboration d’une analyse des besoins de protection. Au cours de cette démarche, on identifie par ailleurs les vulnérabilités éventuelles ainsi que les potentiels d’attaque et de fraude liés à la mise en réseau, à la numérisation et à l’IA. Il est important de noter que les objectifs de protection de la cybersécurité industrielle comprennent, outre les objectifs de protection informatique classiques tels que la confidentialité, l’intégrité et la disponibilité, également la sécurité, c’est-à-dire la sécurité fonctionnelle de la machine.

Une appréciation du risque de cybersécurité est toujours le point de départ. Il s’agit de considérer les dangers et les risques générés par les failles de cybersécurité. Cela nécessite une surveillance et une adaptation permanentes des mesures de sécurité. Pour cela, il faut souvent tenir compte des infrastructures informatiques et des réseaux complexes, ce qui nécessite une expertise technique et des ressources supplémentaires.

Expert en cybersécurité et sécurité recherché !
Celui qui cherche un accompagnement externe pour se lancer dans la cybersécurité industrielle dans le domaine de l’automatisation doit être conscient que le savoir-faire en matière de cybersécurité informatique n’apporte qu’une aide limitée. En effet, les processus visant à réduire les risques d’attaques sur les machines (cybersécurité industrielle) ressemblent beaucoup aux processus visant à réduire les risques pouvant provenir des machines (sécurité). Pour mettre en œuvre la cybersécurité industrielle, il faut être expert en sécurité des machines et connaître les directives et les normes qui s’y rapportent, à commencer par le règlement machines.

La mise en œuvre concrète de la législation est actuellement en pleine évolution. Sur certains points, les normes harmonisées sont seulement en cours d’élaboration. En tant qu’expert en sécurité des machines, Pilz est impliqué de près et participe activement à l’élaboration des normes pertinentes. Pilz transmet ce savoir-faire à ses clients sous forme de prestations de services et de formations. La formation « Principes fondamentaux de la cybersécurité industrielle » s’adresse aux débutants. Les participants se familiarisent avec la terminologie et les exigences et étudient la cybersécurité dans le contexte de la sécurité des machines et des réseaux. Les meilleures pratiques contribuent à la compréhension des risques de cybersécurité dans leur propre production.
La formation « Certified Expert for Security in Automation (CESA) » fournit les outils nécessaires pour prendre des mesures organisationnelles et techniques efficaces dans les réseaux d’automatisation industrielle.

Au-delà de son offre de formations, Pilz propose avec sa gamme « Identification and Access Management » (I.A.M.) des produits et des solutions personnalisées pour une multitude de tâches concernant la sécurité des collaborateurs, la responsabilité civile, l'optimisation de la productivité ainsi que la protection des données. Parmi les applications, on trouve par exemple l'authentification des utilisateurs, la sélection du mode de fonctionnement en toute sécurité, la sécurité des données et des réseaux tout comme la gestion des accès. De cette manière, la sécurité et la cybersécurité peuvent être couvertes par un seul et même système.

Pour être prêts à temps à relever les défis de la cybersécurité industrielle, les fabricants et les exploitants de machines du monde entier devraient se pencher dès maintenant sur le sujet. Il faut acquérir des connaissances, définir les responsabilités et les interfaces et élaborer leur propre stratégie. Idéalement, c'est le personnel de direction qui doit initier ce processus.

Légende:

Vous trouverez des textes et des images à télécharger ci-dessous :
https://www.pilz.com/fr-INT/company/press/messages/articles/245666

Pilz – The Spirit of Safety

Pilz est un fournisseur mondial de produits, de systèmes et de prestations de services pour les techniques d’automatismes. En tant que pionnier des automatismes de sécurité, Pilz fournit la sécurité pour les personnes, les machines et l’environnement. Fondée en 1948, l’entreprise familiale dont le siège social se trouve à Ostfildern est aujourd’hui représentée dans le monde entier et compte 2 500 collaboratrices et collaborateurs répartis dans 42 filiales et succursales.
Le leader technologique propose des solutions complètes pour les automatismes concernant la sécurité et la cybersécurité industrielle des machines. Celles-ci comprennent les capteurs ainsi que les systèmes de contrôle-commande et le Motion Control – y compris les systèmes pour la communication industrielle, le diagnostic et la visualisation. Une offre internationale de prestations de services, comprenant les conseils, l’ingénierie et les formations, complète la gamme. Au-delà de la construction de machines et d’installations, les solutions de Pilz sont utilisées dans de nombreux secteurs d’activités, comme par exemple l’intralogistique, l’emballage et le ferroviaire ou dans le domaine de la robotique.

Pilz sur les réseaux sociaux

Sur nos réseaux sociaux, vous trouverez des informations concernant la vie de l'entreprise et les dernières nouveautés de nos systèmes d'automatismes.

https://www.facebook.com/pilzINT

https://www.youtube.com/user/PilzINT

https://www.linkedin.com/company/pilz

Interlocuteur

Martin Kurth
Presse d’entreprise et presse spécialisée
+49 711 3409 - 0
publicrelations@pilz.com

Sabine Skaletz-Karrer
Presse spécialisée
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de