Stay Ahead. Stay Secure.

La sécurité chez STOBER.

De quoi s'agit-il ?

Le nombre croissant de cybermenaces et la numérisation grandissante des installations de production ont déjà fait de la sécurité un sujet d'une importance majeure dans la technique d'entraînement par le passé. Ce sujet est également une préoccupation dans l'Union européenne – dans un avenir proche, les directives ci-après s'appliqueront pour le domaine de la construction de machines et d'installations, en adéquation avec sa cyberstratégie.

Directive UE NIS 2.

La directive NIS (sécurité des réseaux et des systèmes d'information) avait été adoptée dès 2016 en vue d'un renforcement général de la cybersécurité. Son successeur, la NIS 2, est en vigueur depuis début 2023. La directive NIS 2 qui, à l'origine, ne concernait pas le secteur de la technique d'entraînement, enjoint désormais également aux entreprises de construction de machines et d'installations de prouver qu'elles prennent des mesures de protection contre les incidents de sécurité. Cela implique en premier lieu une analyse des risques des systèmes existants, y compris dans les environnements de production.

Nouveau règlement (UE) 2023/1230 sur les machines.

Avec le nouveau règlement (UE) 2023/1230 sur les machines, le thème de la « sécurité » devient une obligation incombant aux fabricants. Il remplace l'ancienne directive Machines et est entré en vigueur le 19 juillet 2023. Les fabricants de machines ont certes 42 mois pour se mettre en conformité, mais les nouvelles exigences en matière de sécurité doivent être entièrement satisfaites d'ici 2024. Cela signifie qu'à l'avenir, les fabricants devront s'assurer que les fonctions de sécurité d'une machine ne sont en aucun cas compromises, que ce soit par inadvertance ou intentionnellement.

Loi sur la cyber-résilience.

En septembre 2022, la Commission européenne a présenté un projet de loi sur la cyber-résilience (CRA). L'objectif est d'améliorer considérablement la cybersécurité des produits qui peuvent être connectés entre eux ou à Internet.

Principaux objectifs de ce règlement :

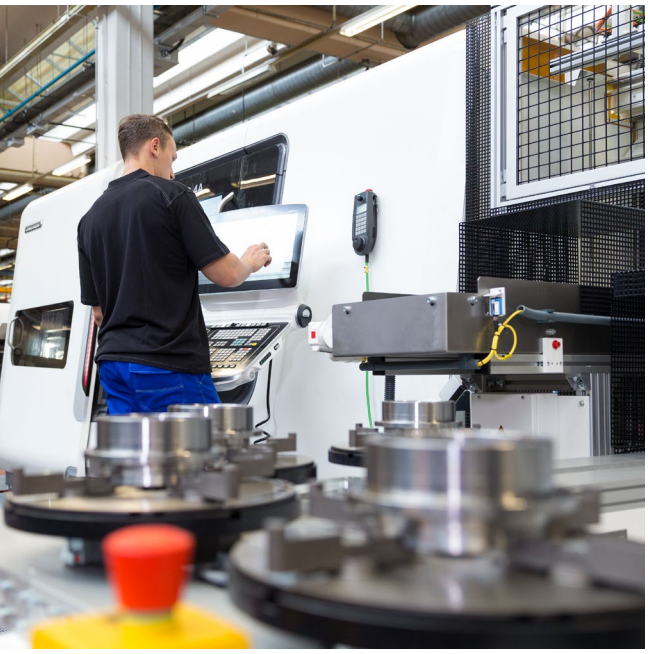
- Les produits contenant des composants numériques commercialisés dans l'Union européenne devraient présenter moins de vulnérabilités.
- Les fabricants sont responsables de la cybersécurité de leurs produits pendant une période définie et …
- … ils s'engagent à combler les failles de sécurité tout au long du cycle de vie du produit.
- Plus de transparence sur la sécurité des produits matériels et logiciels.
- Une sécurité renforcée pour les utilisateurs.

Les fabricants et les développeurs sont désormais appelés à mettre en œuvre les exigences élevées de la CRA. En effet, les produits qui ne sont pas conformes aux prescriptions ne pourront plus être mis sur le marché à partir de 2025.
Et c'est précisément ce qui fait de la sécurité un élément essentiel pour leur vente dans l'Union européenne.

Pourquoi est-ce si important ?

Plus la fabrication est numérique, plus le risque de cyberattaques est élevé. Celles-ci peuvent conduire à l'espionnage ainsi qu'au sabotage. Il suffit d'une seule faille dans le système. Et plus la paralysie de la production est longue, plus les déficits économiques sont dramatiques : d'une part financièrement en raison du manque à gagner, d'autre part cela sape la confiance des clients et la réputation de l'entreprise.

D'autres conséquences très graves des cyberattaques peuvent être les dommages corporels. En particulier lorsque la sécurité, à savoir la sécurité fonctionnelle, qui est responsable de la prévention des dommages aux personnes et aux biens, est manipulée.



La sécurité au niveau opérationnel.

Tandis que les mesures continues en faveur de la cybersécurité au niveau des technologies de l'information (IT) vont de soi, le niveau de la technologie opérationnelle (OT) est généralement négligé. Pourtant, les installations ne sont pas des unités fermées et, avec la numérisation croissante, elles s'ouvrent aux flux de données et aux accès à distance – et donc aussi aux pirates.

Notre stratégie de sécurité repose sur la norme internationale CEI 62443, la norme de sécurité pour les systèmes d'automatisation industrielle.

Elle englobe :

- Des directives et meilleures pratiques pour la sécurité de vos systèmes d'information et de contrôle dans les environnements industriels.
- Des mesures concrètes pour le contrôle des accès et la protection des réseaux.

La conception des processus axée sur la sécurité, empêchant par exemple qu'une personne non autorisée puisse manipuler les produits entre leur expédition et leur réception par le client.

Sous réserve de modifications techniques | 443462_fr.00 | 10/24

STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Straße 12
75177 Pforzheim, Allemagne
Tel. +49 7231 582-0
mail@stoeber.de
www.stober.com

STOBER S.a.r.l.
131 Chemin du Bac à Traille
69300 Caluire-et-Cuire – France
+33 478 98 91 80
contact@stoeber.fr
www.stober.fr