Cyber-Physical Risks: When Data Attacks Meet Physical Safety Meeting Kit – French



QUELS SONT LES ENJEUX?

Autrefois, une cyberattaque se résumait au vol de mots de passe ou au blocage d'une boîte de courriel, mais cette époque est révolue. Aujourd'hui, les pirates peuvent s'introduire dans une usine et provoquer la panne d'un robot, contourner un dispositif de sécurité ou couper le système de chauffage et de climatisation du bâtiment. Lorsque les mondes numérique et physique s'interconnectent, chaque mot de passe faible devient un risque potentiel de blessure – et chaque travailleur se retrouve en première ligne.

QUELS SONT LES DANGERS?

Le Phishing s'Introduit dans l'Usine

La plupart des attaques cyber-physiques commencent par un simple clic sur un lien contenu dans un courriel ordinaire. À partir du réseau du bureau, les attaquants se déplacent latéralement vers les systèmes opérationnels. Un logiciel malveillant qui se propage à partir d'un ordinateur portable peut atteindre les contrôleurs des machines en quelques heures.

Capteurs et Alarmes Altérés

- Lectures falsifiées de gaz, de température ou de pression
- Alarmes désactivées qui auraient dû arrêter la chaîne de production
- Fausses alertes déclenchant des évacuations inutiles

Accès à Distance et robots non sécurisés

Les fournisseurs et les sous-traitants se connectent souvent aux systèmes de l'usine via des ordinateurs portables, des tablettes et des VPN laissés ouverts. Les chariots élévateurs, les véhicules à guidage automatique (AGV) et les robots collaboratifs reçoivent leurs commandes via le réseau et peuvent être redirigés au pire moment. Les travailleurs à proximité peuvent ne recevoir aucun avertissement avant qu'un véhicule ne change de trajectoire.

COMMENT SE PROTÉGER

La Cybersécurité dans l'Atelier est l'Affaire de Tous.

Soyez attentif aux comportements inhabituels des équipements

- Redémarrages ou réinitialisations inattendus et inexpliqués
- Modifications spontanées des points de consigne ou des minuteries
- Alarmes ne correspondant pas à la situation réelle

Considérez Chaque Connexion Comme un Verrou

Utilisez des mots de passe forts et uniques sur chaque système, et ne partagez jamais vos identifiants avec vos collègues — même si c'est plus rapide. Activez l'authentification multifactorielle partout où elle est disponible, y compris sur les tablettes de l'usine et les panneaux IHM. Une connexion fait la différence entre une machine contrôlée et une machine compromise.

Surveillez les Tentatives de Phishing sur les Appareils de l'Usine

Les tablettes IHM, les kiosques partagés et les terminaux de répartition sont des cibles de choix, car ils se situent à la jonction entre les bureaux et l'usine. Si un message semble suspect — expéditeur inattendu, ton urgent, lien étrange — ne cliquez pas dessus et ne l'ignorez pas. Signalez-le afin que le reste de l'équipe puisse être averti.

Sécurisez les Supports Amovibles

Les clés USB et les appareils personnels constituent l'une des voies d'attaque les plus courantes vers les réseaux d'usine. N'utilisez que des clés approuvées par l'entreprise sur les systèmes de l'usine, et ne branchez jamais un objet trouvé dans le stationnement ou reçu d'un fournisseur sans l'avoir inspecté. Traitez les supports inconnus de la même manière que vous traiteriez des produits chimiques inconnus.

Si cela se Produit : Agissez Rapidement

- Arrêtez la machine à l'aide de l'arrêt d'urgence physique
- Isolez-la du réseau si vous pouvez le faire en toute sécurité
- Signalez-le immédiatement au service informatique et à la supervision
- N'essayez pas de vous reconnecter ou de « réparer » le problème vous-même

MOT DE LA FIN

La frontière entre un clavier et un interrupteur d'urgence est plus ténue que jamais. Lorsque les attaques informatiques touchent le monde physique, ce sont les mêmes personnes qui assurent la sécurité des opérations qui remarquent quand quelque chose cloche. Restez vigilant en ligne, restez vigilant sur le terrain : ces deux aspects ne font plus qu'un aujourd'hui.