AVIS DE SECURITE

Objet	Principales mesures d'atténuation visant à réduire les cybermenaces pesant sur les Technologie opérationnelle
Niveau de criticité	IMPORTANT
Référence	SNCSIRT-2025-ADS-138
TLP	WHITE

Résumé

L'Agence pour la cybersécurité et la sécurité des infrastructures (CISA), le Bureau fédéral des investigations (FBI), l'Agence de protection environnementale (EPA) et le Département en charge de l'énergie (DOE) des Etats-Unis d'Amérique dénommés "les organisations auteurs" ont été informés des cyber incidents qui affectent la technologie opérationnelle (OT) et les systèmes d'information.
Ainsi, ces organisations invitent les opérateurs d'infrastructures critiques à examiner et agir dès maintenant pour améliorer leur posture de cybersécurité contre les activités de cybermenaces ciblant spécifiquement et intentionnellement les OT et ICS connectés à l'internet.

Recommandations

- Supprimer les connexions OT à l'Internet public : accès à distance sécurisé aux réseaux OT, si l'accès à distance est essentiel, il convient de passer à une connexion de réseau IP privé afin de soustraire ces actifs OT à l'influence de l'Internet,
- Modifier immédiatement les mots de passe par défaut et utiliser des mots de passe forts et uniques
- Documenter et configurer les solutions d'accès à distance afin d'appliquer les principes du moindre privilège pour le bien spécifique et le rôle de l'utilisateur ou l'étendue du travail
- Désactiver les comptes dormants
- Segmenter les réseaux IT et OT. La segmentation des systèmes critiques et l'introduction d'une zone démilitarisée pour la transmission des données de contrôle à la logistique de l'entreprise réduisent le risque d'intrusion
- Pratiquer et maintenir la capacité d'utiliser manuellement les systèmes d'OT
- Communiquer régulièrement avec les fournisseurs de services gérés par des tiers, les intégrateurs de systèmes et les fabricants de systèmes, qui peuvent être en mesure d'assurer la sécurité des infrastructures critiques,
- La CISA recommande aux organisations d'infrastructures critiques d'examiner et de mettre en œuvre, si possible, les éléments suivants afin d'améliorer leur posture de sécurité.
    1- Pour une vue d'ensemble des outils permettant d'identifier les dispositifs publics sur Internet et des moyens de réduire votre surface d'attaque sur Internet : https://www.cisa.gov/resources-tools/resources/stuff-search .
    2- Pour plus d'informations sur l'utilisation de mots de passe forts : https://www.cisa.gov/secure-our-world/use-strong-passwords
    3- Pour plus d'informations sur l'Authentification multi factorielle (MFA) résistante au phishing : https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf .

4- Pour plus d'informations sur la segmentation du réseau : https://www.cisa.gov/sites/default/files/2023-01/layering-network-security-segmentation_infographic_508_0.pdf
5- Pour plus d'informations sur l'acquisition de composants OT Secure by Design : https://www.cisa.gov/sites/default/files/2025-01/joint-guide-secure-by-demand-priority-considerations-for-ot-owners-and-operators-508c_0.pdf
6- Pour plus d'informations sur les principales cyber actions visant à sécuriser les systèmes d'approvisionnement en eau et les ressources correspondantes : https://www.cisa.gov/sites/default/files/2024-03/fact-sheet-top-cyber-actions-for-securing-water-systems.pdf
7- Pour plus d'informations sur la segmentation des réseaux de distribution d'eau : https://www.epa.gov/system/files/documents/2024-07/segment-ot-and-it.pdf
8- Pour des contrôles de sécurité plus complets afin de lutter contre les acteurs de la menace avancée qui pivotent à travers réseaux d'entreprise pour atteindre la technologie de l'information : https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf