Sécuriser l’accès aux appareils?OT dans un monde hyperconnecté

24 juin 2026, 16:00

Annanda Rath

Gestion des identités et des accès dans les environnements industriels connectés

L’Industrie?4.0 remodèle le secteur manufacturier et améliore l’efficacité, les performances et la compétitivité. À mesure que de plus en plus de machines et de systèmes sont connectés, les risques liés à la cybersécurité augmentent. Souvent, en raison de contraintes techniques, les appareils?OT hérités ne sont pas compatibles avec les solutions de sécurité modernes. L’identification sécurisée et le contrôle d’accès constituent dès lors un niveau de protection essentiel. De nouvelles réglementations telles que NIS2 et le Cyber Resilience Act (CRA) intensifient encore l’urgence de cet enjeu.

Éléments clés de la gestion de l’accès sécurisé aux appareils?OT

La gestion de l’accès sécurisé aux appareils?OT associe plusieurs mesures complémentaires?:

1. **Répertoire de données d’identité centralisé?:** un répertoire unifié met en correspondance les identités des personnes et des machines. Il est ainsi possible d’éviter que des appareils non gérés et non autorisés, ainsi que des ressources inconnues, n’entrent sur le site de production.
2. **Accès à distance sécurisé?:** sécurisation des hôtes de bastion et des zones démilitarisées (DMZ) industrielles afin d’isoler les réseaux?OT de l’Internet public. Les ingénieurs à distance peuvent alors exécuter des activités de maintenance sans exposer directement le réseau.
3. **Authentification avancée?:** authentification multifacteur (MFA) résistante aux attaques, pour les connexions locales et externes, en particulier pour les comptes habilités à émettre des commandes de contrôle critiques. L’authentification par certificat peut offrir une protection supplémentaire tout en garantissant la continuité des opérations.
4. **Gestion des accès privilégiés et principe du moindre privilège?:** les données d’identification doivent être gérées de manière sécurisée. Les sessions distantes peuvent être surveillées ou enregistrées si nécessaire. Les utilisateurs ne doivent disposer que des autorisations nécessaires à l’exécution de leurs tâches spécifiques.
5. **Surveillance continue et audit?:** la surveillance en continu suit l’activité des utilisateurs et enregistre les modifications de configuration. Les audits réguliers contribuent à identifier les comptes inactifs et les privilèges excessifs avant qu’ils ne constituent un risque de sécurité.
6. **Architecture Zero Trust?:** une approche Zero Trust repose sur le principe «?never trust, always verify?» (ne jamais faire confiance, toujours vérifier). Chaque session, qu’elle soit lancée par une personne ou par une machine, doit faire l’objet d’une authentification et d’une autorisation avant que l’accès ne soit accordé.

Fonctionnalités clés du démonstrateur

Le système de contrôle d'accès que nous avons développé combine ces technologies afin d'offrir des fonctionnalités de sécurité avancées?:

- **Identification sécurisée des utilisateurs et contrôle d'accès?:** la SSI permet une gestion décentralisée des identités, un contrôle des données par les utilisateurs et une authentification respectueuse de la vie privée grâce à des mécanismes de divulgation sélective.
- **Journalisation fiable des accès?:** la technologie blockchain permet une journalisation inviolable des événements d'accès et garantit une traçabilité transparente.
- **Soutien fiable des audits et de la conformité?:** les enregistrements vérifiables et inaltérables offrent un soutien lors des audits et aident les organisations à se conformer aux réglementations en constante évolution en matière de cybersécurité.
- **Fonctionnalité d'authentification hors ligne?:** la solution prend en charge l'authentification sécurisée même lorsque les appareils sont temporairement déconnectés du réseau IT ou OT.

SecuWeb?: relever les défis liés à la sécurité?OT

Dans le cadre du projet SecuWeb, Sirris et ses partenaires relèvent ces défis par le biais de la recherche pratique et de l'innovation. Ce projet explore les méthodes, technologies et procédures permettant l'identification sécurisée et le contrôle d'accès des utilisateurs et des opérateurs dans les environnements?OT. En associant des technologies émergentes telles que l'identité auto-souveraine (SSI), Solid et la blockchain, l'équipe du projet a développé un démonstrateur de pointe dédié à la gestion des identités et au contrôle d'accès.

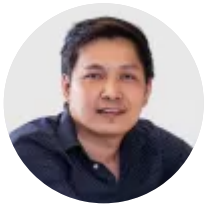
Découvrez le projet SecuWeb.

Rejoignez le projet SecuWeb en tant que partenaire industriel

Souhaitez-vous explorer des solutions innovantes de cybersécurité dans un environnement industriel ? Dans le cadre du projet SecuWeb, nous recherchons des partenaires industriels pour collaborer sur des cas d'usage concrets et valider de nouvelles approches en matière de gestion des identités et des accès dans les environnements OT. Discutons ensemble de vos défis et découvrons comment ces technologies peuvent soutenir votre organisation.

Contactez-nous

Auteurs



Annanda Rath