Comment sécuriser vos données dans un environnement de production ?

24 février 2022, 01:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

Sirris a récemment lancé son service de cybersécurité pour l'industrie manufacturière. Alors que nous commençons à entrer en contact avec les entreprises par le biais d'une introduction gratuite ou d'un coaching individuel, nous recevons de plus en plus de questions sur la manière de protéger les données dans les environnements de fabrication, où machines et activités sont de plus en plus connectées. La protection totale des données contre les cyberattaques est une tâche complexe. Plusieurs bonnes pratiques de sécurité peuvent toutefois contribuer à résoudre une grande partie du problème.

Il n'existe pas de solution universelle. Le choix des solutions de protection des données dépend largement de l'architecture du système, des capacités de la machine et des protocoles utilisés. Cependant, il existe des règles de sécurité générales qui, si elles sont mises en œuvre, peuvent contribuer à réduire le risque de violation des données.

- La première stratégie importante à envisager consiste à **mettre en place un contrôle d'accès aux données**. Appliquez le principe du « moindre privilège » : accordez le niveau minimal de droits qui permet à l'utilisateur d'effectuer son travail. Les données qui ne sont pas destinées aux utilisateurs ne doivent pas leur être accessibles. Vous pouvez ainsi contribuer à empêcher l'accès et l'utilisation inutiles des données. Un protocole de contrôle d'accès standard doit être utilisé autant que possible. Au cas où d'anciennes machines sont en service (et où seule la traditionnelle combinaison de nom d'utilisateur et de mot de passe est possible) et qu'une technologie avancée de contrôle d'accès, comme l'authentification multifactorielle, n'est pas disponible, une bonne pratique de gestion des mots de passe est nécessaire (p. ex. une politique de mot de passe et son renouvellement, etc.). Évitez l'emploi d'un seul mot de passe pour tous (p. ex. un même mot de passe pour plusieurs machines). Les mots de passe doivent en outre être conservés en lieu sûr. Utilisez un gestionnaire de mots de passe si vous devez gérer plusieurs mots de passe pour différents comptes ou différentes machines. Il existe de nombreux logiciels de gestion des mots de passe, qu'ils soient open source ou propriétaires (p. ex. KeePass, Bitwarden, etc.).
  Les données doivent également être classées en fonction de leur niveau de confidentialité. Les données hautement confidentielles exigent une protection renforcée. Lors de la définition de la politique de contrôle d'accès à ces données, le rôle de l'utilisateur dans une organisation (entreprise) est utilisé comme condition pour accorder l'accès. Par exemple, les données doivent être séparées en différentes catégories : données financières, données relatives aux salariés, données opérationnelles (provenant des machines et des

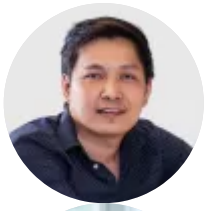
communications sur site) et données relatives à la propriété intellectuelle (PI).

- Une deuxième stratégie consiste à examiner la **protection des données en mode inactif**. En règle générale, dans un environnement de fabrication, les machines produisent une grande quantité de données qui sont stockées dans un historique des données. Ces données doivent être sécurisées à tout moment et doivent également être accessibles à des fins d'analyse. Il existe différentes solutions pour protéger l'historique des données ; tout dépend si elles sont stockées sur site ou dans le cloud. Toutefois, la règle générale est que les données importantes ou hautement classifiées doivent être protégées par voie cryptographique avant d'être stockées. Cela ajoute une couche de protection supplémentaire au contrôle d'accès mentionné ci-dessus. Les données à stocker doivent également être analysées avant le stockage, afin de s'assurer qu'elles sont exemptes de virus ou de logiciels malveillants. Des copies multiples des données doivent être conservées en sécurité à différents endroits afin de réduire les risques en cas de corruption ou de piratage des données (p. ex. attaque de ransomware). Pour la sauvegarde des données, une stratégie 3-2-1 doit être utilisée (3 copies des données (données de production et 2 copies de sauvegarde) sur deux supports différents (disque et bande), avec une copie conservée hors site à des fins de reprise après sinistre.

- Une troisième stratégie consiste à examiner la **sécurité des données en transit**. Ceci comprend l'échange et le partage sécurisés de données sur site ou entre sites via un réseau public (p. ex. internet) ou avec un système tiers (p. ex. la chaîne logistique ou un sous-traitant). Les données échangées sur site doivent également être protégées par l'emploi d'un canal de communication sécurisé/chiffré (p. ex. TLS ou DTLS, etc.) pour les déplacer d'un endroit à un autre (p. ex. entre réseaux) sur site. Si des données doivent être envoyées via un réseau public, il est recommandé d'utiliser un VPN ou une technologie zero-trust, de façon à établir un tunnel sécurisé pour envoyer ou échanger des données.

- En employant des outils avancés et sophistiqués, les pirates peuvent toujours trouver un moyen de s'introduire dans le réseau ou le système, quelle que soit la force de la sécurité mise en place. Le pirate peut accéder aux données à notre insu. Il est donc vital de disposer d'un **outil de surveillance de l'accès aux données**. Cet outil permet de surveiller les activités d'accès aux données des utilisateurs et fournit une alerte en temps utile si une anomalie est détectée. Des outils commerciaux tels que Microsoft 365 et OneDrive proposent un journal d'audit qui peut être utilisé pour vérifier/suivre les activités d'accès et de partage des données sur la plate-forme.

Auteurs



Annanda Rath



Christophe Michiels



Tatiana Galibus