Accès à distance aux appareils OT: problèmes de sécurité et solutions possibles

La pandémie du Covid-19 a entraîné des changements importants dans le monde entier, notamment dans les habitudes de travail. Les entreprises ont été contraintes d'adapter leurs processus opérationnels pour répondre aux exigences du lockdown. Pour celles qui utilisent la technologie opérationnelle (OT), l'accès à distance aux appareils OT a été une mesure cruciale pour assurer la continuité de leurs activités. Bien que l'accès à distance présente des avantages indéniables, il comporte également des risques importants. Cet article se penche sur les problèmes de sécurité liés à l'accès à distance aux appareils OT et présente des solutions telles que les privileged access management (PAM), virtual private network (VPN) et zero trust network access (ZTNA) afin de garantir un accès à distance sécurisé.

La sécurité OT est une obligation

La sécurité des systèmes OT est d'une importance capitale, car ils soutiennent souvent des infrastructures sensibles telles que l'approvisionnement en énergie, les installations de transport et de fabrication. Cependant, l'accès à distance aux équipements OT ouvre de nombreux points d'attaque potentiels pour les cyber-attaques, qui peuvent avoir de graves conséquences.

Parmi les trois principaux vecteurs d'attaque, on trouve notamment une authentification faible. Des mécanismes d'authentification insuffisants ou peu sûrs permettent aux pirates de se connecter aux appareils OT. Cela peut conduire à des manipulations non autorisées des appareils, voire au sabotage des systèmes concernés. Des mots de passe faibles ou l'absence d'une authentification multifactorielle ouvrent la porte aux pirates. D'autre part, il est souvent impossible d'implémenter des méthodes modernes d'authentification sur des installations parfois vieilles de plusieurs décennies. Une authentification adéquate se fait alors généralement par l'accès au réseau lui-même.

Le verrouillage de l'ensemble du réseau permet également de lutter contre la deuxième porte d'entrée la plus importante: la communication non cryptée – et souvent de structure simple – dans l'environnement OT. Dans les réseaux ouverts, il est possible de procéder à des tentatives d'écoute et de manipulation des données. Ainsi, les pirates ont la possibilité de voler des informations confidentielles ou d'introduire des codes malveillants. Le contrôle d'accès est donc d'une importance capitale – →

dès qu'un accès externe a lieu, toute la chaîne de communication doit être cryptée jusqu'au terminal qui y accède.

Une fois que le réseau est ouvert vers «l'extérieur», le moment et la fréquence de l'accès ne sont plus réglables et contrôlables par les barrières physiques. Les solutions d'accès à distance doivent donc permettre une surveillance et une journalisation complètes des activités afin d'identifier et de comprendre les actions suspectes. L'absence de ces fonctions rend difficile l'identification des attaques et la réalisation d'une analyse médico-légale en cas d'incident. Une surveillance inexistante peut avoir pour conséquence que des activités malveillantes passent inaperçues.

VPN, ZTNA et PAM

Pour faire face à ces problèmes de sécurité, différentes approches peuvent être mises en œuvre. Trois approches prometteuses sont présentées ci-dessous: virtual private network (VPN), zero trust network access (ZTNA) et privileged access management (PAM).

Un réseau privé virtuel (VPN) offre une connexion cryptée sécurisée entre les appareils d'accès à distance et les appareils OT. L'utilisation d'un VPN permet de protéger les communications réseau contre les tentatives d'interception potentielles et la manipulation des données. Mais également d'authentifier et d'autoriser les utilisateurs. Cela garantit que seules les personnes de confiance ont accès au réseau. En mettant en place un VPN, les entreprises veillent à ce que l'accès à distance aux appareils OT reste sécurisé et protégé. Toutefois, cela ne garantit pas que l'ensemble de la chaîne de communication soit cryptée, car le trafic peut être transféré en clair après le point d'accès VPN. En outre, dans le cas d'un VPN, c'est généralement l'ensemble du réseau qui est partagé, et pas seulement des utilisateurs individuels sur des appareils individuels. Ainsi, un seul employé d'une entreprise de maintenance externe peut avoir accès à un grand nombre d'appareils de l'infrastructure sensible.

La continuité du concept VPN et la régulation plus approfondie de l'accès au réseau se nomme ZTNA. Il s'agit d'une approche moderne de la sécurité des réseaux, basée sur le principe de «l'accès de confiance». Avec l'approche «accès au réseau zero trust», les utilisateurs sont en principe toujours vérifiés et autorisés – indépendamment de l'endroit où ils se trouvent ou de l'appareil à partir duquel ils accèdent. ZTNA permet un contrôle granulaire de l'accès aux appareils OT et minimise le risque d'accès non autorisé. En implémentant ZTNA, les entreprises peuvent s'assurer que seuls les utilisateurs autorisés ont accès aux appareils OT qui leur sont attribués, indépendamment de leur emplacement.

La gestion des accès privilégiés (PAM) est, en plus des solutions réseau, une solution de sécurité qui surveille et contrôle l'accès aux comptes et ressources privilégiés. En implémentant PAM, les entreprises peuvent s'assurer que seuls les utilisateurs autorisés ont accès aux appareils OT. PAM permet un contrôle granulaire des autorisations et des méthodes d'authentification, ce qui réduit le risque d'attaques par des données d'accès volées ou compromises. Le système PAM est ici le seul point d'entrée pour tous les systèmes importants. Outre les systèmes cibles, il est possible de définir les protocoles et les restrictions. Il est par exemple possible d'interdire le partage du presse-papiers et du media player dans le protocole Microsoft Remote Desktop. Cela permet de garantir d'une part que le travail n'est pas entravé et d'autre part que le risque de fuite de données est minimisé.

Une stratégie de sécurité (OT) complète est nécessaire

L'accès à distance aux appareils OT permet aux entreprises de maintenir leurs processus commerciaux. Cependant, il comporte également des risques de sécurité importants. En implémentant des solutions de sécurité telles que PAM, VPN et ZTNA, les entreprises peuvent optimiser au maximum la sécurité de leurs systèmes OT. Il est important de noter qu'aucune technologie individuelle ne suffit à elle seule à couvrir tous les risques de sécurité. Une stratégie de sécurité globale, combinant différents mécanismes de protection, est nécessaire pour protéger efficacement les systèmes OT. À une époque où l'accès et le travail à distance sont de plus en plus fréquents, il est primordial que les organisations gardent un œil sur la sécurité et prennent les mesures adéquates pour éliminer autant que possible les risques de sécurité potentiels. Seules des solutions de sécurité appropriées permettent aux entreprises de garantir que l'accès à distance aux appareils OT soit toujours sécurisé et protégé.

La sécurité OT assurée par un partenaire compétent

Le distributeur de sécurité informatique BOLL, connu aussi bien pour les produits qu'il représente que pour ses spécialistes hautement qualifiés, dispose précisément d'un large éventail de solutions dans son portefeuille pour ces cas d'application. Ainsi, les systèmes PAM des fabricants Fudo, Claroty et WALLIX répondent aux exigences concernant l'organisation sécurisée de l'accès à distance. Les solutions ZTNA sont également prises en charge par les spécialistes de BOLL. On peut citer entre autres les solutions des fabricants Fortinet et Palo Alto Networks. En outre, il existe également un produit complet de Claroty pour la surveillance du statut des firmwares et des configurations, qui améliore considérablement la traçabilité dans les installations correspondantes et apporte ainsi de la visibilité dans ce domaine.

Entretien avec Marcel Schick →

Entretien avec Marcel Schick, expert en sécurité OT, BOLL Europe GmbH

Selon vous, quels sont les défis à relever en matière de sécurité des connexions de téléassistance?
L'accès à distance aux appareils OT est sans aucun doute une mesure importante pour garantir la continuité des activités (même pendant une pandémie). Cependant, cela implique également des risques de sécurité importants. L'un des principaux défis consiste à garantir une authentification et une autorisation sécurisées des utilisateurs. Des mots de passe faibles ou l'absence d'authentification multifactorielle, ainsi que des réseaux non réglementés, peuvent permettre à des personnes non autorisées d'accéder à des appareils OT.

Quelles sont les solutions que vous recommandez pour faire face à ces problèmes de sécurité?
Il existe différentes solutions que les entreprises devraient envisager. Une mesure importante est la mise en œuvre de la gestion des accès privilégiés (PAM). Cela permet de contrôler et de surveiller l'accès aux comptes et ressources privilégiés. Un contrôle granulaire des autorisations et une authentification sécurisée sont essentiels pour minimiser le risque d'attaques par des données d'accès volées.

Une approche moderne que je recommande, outre le système PAM, est l'accès au réseau zéro trust (ZTNA). Il s'agit d'implémenter un «accès de confiance». Cela signifie que les utilisateurs doivent toujours être vérifiés et autorisés, indépendamment de leur emplacement ou de leur appareil. ZTNA offre un contrôle granulaire de l'accès aux appareils OT et minimise le risque d'accès non autorisé.

Quelles autres mesures les entreprises devraient-elles prendre pour garantir la sécurité de leurs systèmes OT?
Outre les solutions mentionnées, les entreprises sont invitées à développer une stratégie de sécurité globale qui combine différents mécanismes de protection. Une mise à jour régulière des logiciels et des micrologiciels sur les appareils OT est essentielle pour combler les failles de sécurité. En outre, une surveillance continue du trafic réseau devrait être mise en place afin de détecter toute activité suspecte. La formation et la sensibilisation des collaborateurs sont également primordiales. Il faut informer et former le personnel aux bonnes pratiques de sécurité et signaler immédiatement toute activité suspecte. Une stratégie complète de réponse aux incidents doit être mise en place afin de pouvoir réagir rapidement et de manière appropriée en cas d'incident.

Un grand merci pour vos précieuses informations, Monsieur Schick. Pour conclure, souhaitez-vous transmettre quelques mots à nos lecteurs?
De rien, c'était avec un grand plaisir! J'invite vivement les entreprises à développer une stratégie de sécurité globale et robuste, dans laquelle les environnements OT et IT sont considérés et protégés ensemble. Outre les mesures techniques, il convient d'établir une culture de sécurité positive et d'investir dans la formation et le perfectionnement réguliers des collaborateurs afin de renforcer la conscience de la sécurité. En outre, des contrôles réguliers (par des organismes internes et externes) permettent de vérifier le niveau de sécurité actuel et, en cas d'urgence, une équipe de réponse aux incidents doit être disponible pour prendre les (contre-)mesures appropriées. En bref, la sécurité est à considérer comme un processus global, dans lequel les mesures techniques et organisationnelles interagissent de manière optimale et intègrent le facteur humain.

Marcel Schick, expert en sécurité OT, BOLL Europe GmbH

BOLL
IT Security Distribution

BOLL Europe GmbH
Ringstrasse 3
89081 Ulm

Tél +49 (0)731 85 07 48 23
info@boll-europe.de
www.boll-europe.com

→ **boll.ch**