Advertorial

L’accès à distance sécurisé redéfini pour les environnements OT (Operational Technology)

Les solutions de gestion des accès privilégiés (PAM) n’offrent pas une sécurité suffisante pour les applications industrielles et les infrastructures sensibles. Une plateforme RPAM spécialement conçue pour l’OT convenant à tous les environnements OT et gérant même les systèmes isolés.

Un contrôle d’accès strict est un impératif absolu, notamment dans les environnements industriels (Operational Technology). En effet, une cyberattaque réussie peut non seulement avoir des conséquences financières et porter atteinte à la réputation de l’entreprise, mais également avoir une issue littéralement catastrophique. Même la mise en danger de vies humaines peut potentiellement faire partie des conséquences d’une cyberattaque réussie. Dans ce contexte, les accès à distance, par exemple de prestataires de services externes ou de collaborateurs travaillant à domicile, doivent être contrôlés sans faille, au même titre que les accès de collaborateurs et d’applications internes.

Les solutions PAM ne suffisent pas

Dans les environnements informatiques, on utilise à cet effet des solutions de gestion des accès privilégiés (PAM). Toutefois, les fonctionnalités des solutions PAM courantes ne suffisent souvent pas à répondre aux exigences des environnements OT. Les solutions PAM ne comprennent généralement pas les protocoles OT spécifiques et ne peuvent pas tenir compte comme il se doit des systèmes hérités quasi omniprésents dans les environnements OT, ni des installations hors ligne. D’autant plus que de nombreuses solutions PAM fonctionnent sur la base d’agents. Il faut alors installer un composant logiciel sur les systèmes contrôlés, ce qui d’une part, comporte un nouveau risque de sécurité et d’autre part, n’est pas du tout possible sur les systèmes OT typiques, conçus pour une grande longévité et stabilité. Par ailleurs, les solutions PAM fonctionnent souvent avec un composant cloud qui n’est pas toléré dans les environnements hors cloud ou hors ligne. →

Advertorial

Cyolo PRO contrôle l'exploitation plutôt que l'accès des utilisateurs
Fondé en 2019 par un ancien RSSI d'une entreprise de production mondiale et deux hackers éthiques, le spécialiste de la sécurité Cyolo s'est attaqué au problème du contrôle des accès pour les environnements OT et est considéré comme un innovateur leader du marché dans ce domaine. L'entreprise compte déjà de nombreuses entreprises industrielles de renom parmi ses clients.
La plateforme Cyolo PRO (Privileged Remote Operations) va bien au-delà du contrôle d'accès classique. Elle ne se contente pas de contrôler l'accès des utilisateurs au réseau et aux systèmes, mais surveille l'ensemble des connexions des identités vérifiées aux applications et systèmes OT via des appareils autorisés.
En plus des fonctions d'une solution PAM axée sur l'accès à distance (RPAM), Cyolo PRO regroupe les fonctionnalités d'accès à distance sécurisé (SRA) et de Zero Trust Access (ZTA) dans une plateforme sans agent et indépendante de l'infrastructure. La simplicité et la grande facilité d'utilisation ont été les priorités lors du développement. Par conséquent, Cyolo PRO combine toutes les fonctions sous un toit holistique et rend superflu le passage d'un outil à l'autre.

Adapté à toutes les infrastructures
Qu'il soit natif cloud, hors cloud ou hors ligne: Cyolo PRO convient à tous les environnements OT, indépendamment de l'infrastructure existante. Il peut donc être déployé comme solution sur site, dans le cloud ou de manière hybride. La solution offre une gestion centralisée basée sur l'emplacement et prend en charge la conformité aux exigences de gouvernance et légales telles que NIS-2/IEC 62443.
En outre, elle étend l'authentification forte des identités avec une gestion granulaire des accès et des actions selon le principe du «moindre privilège», ainsi que l'authentification multi-facteurs et l'authentification unique aux applications héritées qui ne sont pas conçues pour cela.
Cyolo PRO se passe de composante cloud et évite ainsi un risque de sécurité supplémentaire. De plus, les utilisateurs ne subissent pas les latences typiques d'un détour par le cloud. En outre, la solution peut être utilisée dans des environnements complètement isolés et donc pour des applications particulièrement sensibles qui dépendent d'un air gap bien défini.

BOLL
IT Security Distribution

BOLL Engineering SA
Jurastrasse 58
5430 Wettingen

Tél. 056 437 60 60
info@boll.ch
www.boll.ch

→ **boll.ch/cyolo**