Technologies opérationnelles : une surface d'attaque grandissante

Les infrastructures critiques qui sous-tendent notre mode de vie moderne continuent d'être attaquées. Le piratage du réseau électrique ukrainien en 2015 a mis en lumière cette triste réalité, et depuis lors, les menaces n'ont cessé de croître en nombre et en sophistication.

Ces derniers mois, les cybercriminels ont multiplié les attaques contre les compagnies d'énergie ou encore les installations de distribution d'eau ; exploitant souvent les technologies opérationnelles (OT) connectées à internet pour atteindre les systèmes de contrôle industriels.

En conséquence, il est urgent de déployer les mesures adéquates pour réduire l'exposition des technologies opérationnelles et des systèmes de contrôle industriel (ICS). Il s'agit notamment de sécuriser les accès à privilèges, que les hackers ciblent systématiquement au sein des infrastructures critiques. En les compromettant, ou en les dérobant, les cybercriminels obtiennent un accès de niveau administrateur aux ressources OT connectées. Ils peuvent alors perturber les services critiques, corrompre les systèmes OT et IT, anéantir les terminaux et les serveurs et, au final, mettre des vies humaines en danger.

La convergence OT-IT, une surface d'attaque grandissante

L'OT comprend les systèmes matériels et logiciels qui surveillent et contrôlent les équipements et les processus physiques. Il s'agit d'environnements hautement spécialisés, avec une technologie propriétaire qui n'est pas familière à la plupart des individus, en dehors des opérateurs et des ingénieurs qui travaillent avec eux. Les systèmes OT sont souvent protégés par un « air gap » (en les isolant physiquement du réseau informatique), ou segmentés à partir de réseaux extérieurs pour des raisons de sécurité et de disponibilité.

Mais à mesure que les entreprises multiplient les opérations à distance et externalisent de nombreuses tâches, notamment l'entretien et la maintenance des équipements, la connectivité devient essentielle, et les technologies OT et IT continuent de converger.

Cette convergence peut présenter de nombreux défis, le premier étant que les systèmes OT – dont beaucoup sont âgés de plusieurs décennies – n'ont tout simplement pas été conçus pour résister aux attaques hautement ciblées et sophistiquées d'aujourd'hui. Étant donné que ces systèmes sont de plus en plus connectés, la surface d'attaque s'est considérablement étendue.

La possibilité que des États-nations ou des employés malveillants dérobent, ou détournent, des identifiants à privilèges pour obtenir l'accès à des systèmes de contrôle industriel critiques est une préoccupation majeure. De plus, des outils open source accessibles au public peuvent être utilisés par les attaquants pour effectuer des reconnaissances, localiser les ressources OT connectées et planifier leur mission.

Protéger les accès à privilèges dans les environnements OT

Bien qu'il n'existe pas de solution miracle pour la cybersécurité des OT, la gestion des accès à privilèges contribue à assurer une protection contre les menaces et à réduire considérablement l'impact d'une attaque.

Pour sécuriser tous les accès à distance et comptes d'utilisateurs requis et approuvés, il suffit de suivre plusieurs étapes :

Interdire l'utilisation de mots de passe par défaut sur tous les appareils, y compris les dispositifs de contrôle et les équipements OT. Il s'agit de la première chose à faire après avoir intégré un nouvel appareil OT dans l'environnement. Il en va de même pour les appareils IoT connectés au domicile des utilisateurs, tels que les routeurs ou les imprimantes, surtout s'ils travaillent à distance.

Supprimer, désactiver ou renommer tout compte système par défaut dans la mesure du possible, en particulier ceux qui ont des privilèges élevés ou un accès à distance. Ensuite, il convient d'identifier les utilisateurs qui ont besoin d'un accès à privilèges et/ou à distance — ou les utilisateurs qui pourraient devenir privilégiés sous certaines conditions — et mettre en place des contrôles stricts qui permettent à ces utilisateurs de rester productifs, mais aussi de travailler en toute sécurité.

Appliquer une politique rigoureuse de sécurité des mots de passe. La mise en œuvre efficace d'une politique de sécurité passe en grande partie par une approche forte et cohérente visant à sensibiliser les employés aux risques de cybersécurité et à l'importance fondamentale de protéger les mots de passe.

Soulager l'utilisateur en stockant tous les mots de passe et identifiants à privilèges du compte dans un référentiel chiffré. Ensuite, une rotation automatique de ces identifiants conformément à la stratégie en vigueur est à mettre en place, pour rationaliser les workflows des administrateurs et des utilisateurs.

Déployer une authentification à deux facteurs (MFA) pour toutes les connexions à distance. Un compte a moins de 99,9 % de chances d'être compromis si la MFA est en place. La mise en place de la MFA devrait constituer une priorité.

Enfin, il est conseillé de mettre en œuvre un programme de surveillance continue et minutieuse du système qui détecte les anomalies. Cela peut aider les organisations à identifier des cyber-tactiques malveillantes ; comme celle du type « living off the land », dans laquelle les attaquants détournent un accès à privilèges pour prendre position sur le réseau, se font passer pour des utilisateurs autorisés et utilisent ensuite des outils ou des fonctionnalités natives existant dans l'environnement OT pour accomplir leur mission.

En effet, alors que les systèmes OT et IT sont de plus en plus interconnectés, les sociétés d'infrastructures critiques doivent faire de la gestion des accès à privilèges une priorité pour lutter

contre des attaquants hautement organisés et bien financés.