

Bien s'occuper son réseau OT

Sécurité

Posté par : JulieM

Publié le : 11/10/2021 15:00:00

Dans la plupart des organisations industrielles, il ne fait aucun doute que le réseau OT doit être bien plus sécurisé que le réseau informatique. Cela s'explique en partie par le fait que la disponibilité est d'une importance cruciale pour les systèmes OT, et aussi parce que les systèmes OT ont tendance à être plus anciens et plus « vulnérables ».

Cependant, il semble que les utilisateurs qui demandent une plus grande sécurité pour le réseau OT soient les mêmes qui réclament plus d'accès aux systèmes OT, depuis le réseau informatique, bien sûr. Les ingénieurs et autres utilisateurs du réseau informatique ont en effet tous besoin d'obtenir des données des systèmes OT et d'y apporter des ajustements. Mais faire communiquer SI et OT est un réel challenge.

Bien entendu, les technologies de sécurité que la plupart des organisations déploient en premier sont les pare-feux. Au début, ils peuvent sembler être la solution parfaite. Tout ce que vous avez à faire est de vous assurer de fermer tout accès au réseau OT, sauf ce qui est absolument nécessaire. Mais que se passe-t-il dans une telle configuration ?

Voici les principaux risques :

1. Les réseaux de pare-feu exécutent des logiciels et, comme tout autre logiciel, ils peuvent être piratés.
2. Les erreurs de configuration sont nombreuses.
3. Les équipes qui gèrent les pare-feu sont sous pression constante.

Pour autant, il existe un bon moyen de protéger son environnement OT : les « data diodes ». Les fournisseurs de « data diodes » peuvent dire en toute honnêteté qu'ils protègent contre toutes les attaques de l'IT vers le réseau OT. Ils peuvent le dire, car une « data diode » ne laisse passer aucun trafic.

Mais quel est le coût de cette opération ? Et par cela, nous entendons le coût de la productivité, car les utilisateurs habitués à une interaction bidirectionnelle en temps réel avec les systèmes OT réaliment soudainement qu'ils devront physiquement accéder aux systèmes qu'ils ont l'habitude d'utiliser !

Ainsi, il n'y a aucun moyen de fournir des sessions de communications bidirectionnelles en temps réel depuis l'extérieur du réseau OT. Ce qu'ils demandent, c'est la quadrature du cercle ; cela ne peut tout simplement pas être fait.

L'alternative de l'approche Electronic Air Gap

Cette approche technologique permet aux utilisateurs de réaliser des communications bidirectionnelles complètes entre les réseaux IT et OT, tout en offrant la même protection contre les attaques de couche réseau que les fournisseurs de « data diodes ».

La grande majorité des cyberattaques se propagent à travers les couches 3 et 4, respectivement les couches réseau et Transport. Des attaques comme Stuxnet, Black Energy, Wannacry, NotPetya, CrashOverride, etc. reposent toutes sur ces deux couches pour se propager.

L'Electronic Air Gap repose sur une technologie innovante. Il y a trois processus distincts en cours dans cette technologie. Ils sont implémentés sur trois circuits imprimés distincts au sein du dispositif.

Dans le premier processus, chaque paquet IP en provenance du rseau informatique est découpé des couches 1 à 4. Il ne reste que la « charge utile » : les couches 5 (Présentation) et 7 (Application). Le deuxième processus transmet la charge utile au troisième processus, sans aucune information de couche 1-4.

Dans le troisième processus, les couches 1 à 4 sont reconstruites, sans aucun code malveillant qui aurait pu s'y trouver à l'origine. Les couches 5 et 7 du paquet d'origine sont ajoutées aux couches reconstruites 1 à 4 ; le paquet entier est transmis au rseau OT.

En tant qu'Electronic Air Gap détruit puis recrée l'intégrité des couches 1 à 4 de chaque paquet IP, il rend physiquement impossible la transmission de toute attaque de rseau ou de couche de transport dans le rseau OT.

Dans le même temps, cette technologie permet aux couches 5 et 7 de chaque paquet de traverser sans entrave, de sorte qu'il n'y a aucun changement dans la charge utile du paquet. Cela signifie que les ingénieurs n'auront pas besoin de changer la façon dont ils utilisent les applications, les bases de données et les protocoles sur le rseau OT. Le rseau OT disposera désormais du plus haut niveau de protection contre les cyberattaques du rseau.

Protection contre les attaques de la couche application

La grande majorité des cyberattaques sont menées via les couches Rseau et Transport du protocole IP (couches 3 et 4, respectivement) ; ceux-ci seront tous bloqués par la technologie Electronic Air Gap. Cependant, certaines attaques utilisent la couche Application (couche 7).

Comment peuvent-ils être bloqués ?

La première méthode est le contrôle de direction. Même si certaines technologies permettent des communications bidirectionnelles sécurisées entre les rseaux IT et OT, il est toujours possible de contrôler le rseau à partir duquel la communication doit être initiée pour tout protocole, base de données ou application particulière.

Une fois la session lancée, elle sera véritablement bidirectionnelle, mais le contrôle de direction est un outil puissant pour empêcher les attaques sur le rseau OT qui proviennent du rseau informatique.

Dans les cas où l'utilisation du contrôle de direction n'est pas possible, la deuxième méthode utilisée par certaines sociétés consiste à implémenter un pare-feu de couche application en ligne avec leur Electronic Air Gap.

Le pare-feu de la couche application peut être configuré pour bloquer les attaques connues sur les applications, bases de données et protocoles particuliers trouvés sur le rseau OT.

Xavier Facchina, CEO de SECLAB