Comment maintenir la continuité des opérations OT en étendant la méthode Zero Trust aux environnements OT

La connectivité des machines OT expose les réseaux industriels à des vastes, avancées et lucratives cyberattaques que les cybercriminels peuvent exploiter. L'extension de la méthode Zero Trust aux environnements OT garantira des opérations plus sécurisées, résilientes et automatisées.

Parmi les déclarations Zero Trust suivantes, laquelle s'applique à votre entreprise ?

- L'adoption d'une méthodologie Zero Trust est une priorité absolue pour nous
- Nous reconnaissons que le modèle Zero Trust est bénéfique pour l'entreprise et l'intégrons dans les développements et les initiatives
- Nous considérons le Zero Trust sur une base ad hoc, lorsque les circonstances l'exigent, mais ce n'est pas une priorité
- Je ne suis pas sûr/je ne sais pas

Source : Enquête Security d'IDC 2022 (n = 700)

Comment votre entreprise protège-t-elle ses déploiements IIoT ?

64 %	52 %	47 %	43 %	42 %	40 %	33 %	29 %	1 %
Sécurité des terminaux	Passerelle de sécurité en périphérie	Contrôle d'accès au réseau (NAC)	ICP ou autres solutions d'identité des appareils	Pare-feu de l'industrie	Sécurité intégrée dans l'appareil/ capteur	Architecture Zero Trust	Détection et prévention des intrusions	Autres ; merci de préciser

Source : Enquête Security d'IDC 2022 (n = 233)

Le Zero Trust est une priorité de la feuille de route sécurité. 41 % des entreprises adoptent la méthodologie zero trust comme une priorité absolue, avec une stratégie et des objectifs définis et le soutien de la direction pour les nouveaux investissements et initiatives. Cependant, le Zero Trust n'est pas un produit, une solution ou un réseau spécifique que l'on peut acheter ; il s'agit d'une approche stratégique de la sécurité, ce qui la rend difficile à mettre en œuvre. À l'heure actuelle, seul un tiers des entreprises exploitent le Zero Trust pour protéger leurs déploiements IIoT.

Le Zero Trust

L'architecture Zero Trust repose sur le principe du refus d'accès par défaut à toute demande d'accès au réseau. Cela nécessite une surveillance constante des menaces pour l'entreprise, une maintenance continue de l'environnement et comme il s'agit d'un cadre qui va au-delà d'une solution technique, un alignement des solutions sur les exigences de gouvernance et de conformité.

Le Zero Trust est une initiative de premier plan pour la plupart des entreprises, car les modèles commerciaux évoluent et les entreprises vont de l'avant avec leurs initiatives DX. Le Zero Trust est une stratégie à l'échelle de l'entreprise visant à réduire l'exposition au risque global pour l'entreprise. Face à l'augmentation des migrations vers le cloud d'applications d'entreprise et le nombre croissant d'appareils connectés au réseau (actifs IoT et OT), l'efficacité des protections périmétriques traditionnelles de l'infrastructure diminue. Les entreprises éprouvent des difficultés à faire face aux perturbations permanentes tout en sécurisant les utilisateurs, les appareils, les ressources et les applications. Cela augmente les inefficacités opérationnelles ainsi que le risque de failles de sécurité.

Qu'est-ce que cela signifie pour l'OT ?

En matière de sécurité informatique, la confidentialité est au sommet du triangle CIA (confidentialité, intégrité, disponibilité). Cependant, dans les environnements OT, la disponibilité devient l'aspect le plus critique, ce qui nécessite un changement dans les stratégies de gestion des risques.

L'extension d'une méthodologie Zero Trust aux déploiements OT peut améliorer la sécurité et réduire les risques, mais elle nécessite une compréhension complète de toutes les ressources du réseau, et pas seulement des terminaux informatiques traditionnels. Cela permettra aux entreprises de prendre des décisions de segmentation afin de réduire la surface d'attaque et les risques globaux sans affecter la disponibilité.

Les machines connectées peuvent très facilement devenir le maillon faible ou le point d'entrée de toute entreprise. L'extension d'une méthodologie Zero Trust aux déploiements OT peut améliorer la sécurité et réduire les risques, mais elle nécessite une compréhension complète de toutes les ressources du réseau, et pas seulement des terminaux informatiques traditionnels. Cela permettra aux entreprises de prendre des décisions de segmentation afin de réduire la surface d'attaque et les risques globaux sans affecter la disponibilité.

Étendre le Zero Trust à l'OT dès maintenant : Conseils pour commencer

- Le Zero Trust doit aller au-delà des définitions traditionnelles des utilisateurs et de l'identité pour inclure tous les appareils et toutes les ressources.
- Assurer une visibilité approfondie du réseau pour identifier et surveiller chaque appareil (y compris les communications de données vers/depuis où, de qui/quoi).
- Automatiser l'application des politiques ainsi que la détection et le blocage des menaces.
- Segmenter le réseau pour appliquer les principes Zero Trust à tous les environnements en créant des zones : l'entreprise, l'IoT et l'OT peuvent être séparés.
- Confiner les appareils vulnérables, non sécurisés ou non patchés connus dans des zones plus éloignées afin de réduire la surface d'attaque.

L'avis d'IDC

La convergence de l'informatique et de l'OT a été une tendance irrépressible au cours des dernières années. C'est l'occasion pour de nombreuses entreprises de s'orienter vers des opérations décisionnelles plus résilientes afin de répondre aux exigences opérationnelles futures. L'informatique et l'OT communiquent et s'intègrent de plus en plus alors qu'ils étaient auparavant considérés comme deux entités distinctes ; conjointement, ils peuvent améliorer les performances opérationnelles des entreprises et combler le fossé historique entre les processus opérationnels et commerciaux, tout en ouvrant l'OT à un paysage de cybermenaces vaste et avancé.

L'adoption d'une approche Zero Trust, non seulement pour l'infrastructure informatique traditionnelle, mais aussi pour les environnements OT, avec des autorisations d'accès granulaires au niveau des applications, augmentera la connectivité sécurisée et l'interopérabilité entre l'informatique et l'OT, tout en réduisant les risques et les menaces pour l'ensemble de l'activité.

Message du sponsor :

L'approche OT Zero Trust de TXOne protège les entreprises contre les cyberattaques très efficaces qui sont devenues une menace courante pour le commerce. Appliquez facilement les politiques OT Zero Trust grâce à des **solutions adaptées aux ICS**.