La sécurité OT exige un changement d'attitude

La technologie opérationnelle (OT) est aujourd'hui une cible prioritaire pour les cybercriminels. Mais de nombreux environnements OT ne sont pas suffisamment adaptés à la cybersécurité. Découvrez ci-après quels sont les défis à relever et ce qu'il faut pour assurer la sécurité OT.

La technologie opérationnelle comprend des composants électroniques tels que des capteurs et des actionneurs, des serveurs SCADA (supervisory control and data acquisition) ainsi que des systèmes de contrôle industriel (ICS), qui sont responsables de la commande et de la surveillance dans les installations industrielles et les infrastructures sensibles. Les erreurs, telles qu'elles peuvent être déclenchées par des cyberattaques, ont souvent des conséquences physiques – de la panne d'une chaîne de production à la rupture de l'approvisionnement en énergie, en passant par un danger direct pour la vie humaine. Une chose est claire: les environnements OT doivent être particulièrement bien sécurisés, ce qui n'est malheureusement que trop rarement le cas en pratique.

OT versus IT

L'OT se distingue de l'IT à bien des égards. Les réseaux OT se composent d'une multitude de composants matériels avec des firmwares intégrés, des systèmes d'exploitation propriétaires ainsi que des protocoles spécifiques à l'OT, voire propres au fabricant, qui sont plus difficiles à cataloguer et à surveiller, respectivement à actualiser, que les systèmes IT. Les systèmes OT présentent également des risques plus importants que les systèmes IT, car ils sont conçus pour une longue durée de vie (jusqu'à plusieurs décennies).

Les réseaux OT sont également moins segmentés, car ils ont été conçus à l'origine pour fonctionner de manière autonome et non pour être intégrés dans un environnement élargi. De ce fait, le contrôle d'accès a traditionnellement fait l'objet de peu d'attention. Quant aux systèmes de commande, les fabricants d'installations OT comme Siemens ou ABB n'ont pas accordé beaucoup d'importance à la cybersécurité par le passé.

Aujourd'hui, les systèmes informatiques sont tous basés sur l'IP. Il existe un énorme marché de solutions de cybersécurité pour les réseaux informatiques. En IT, on est habitué depuis longtemps à un contrôle d'accès et à une segmentation stricts, à une protection contre les menaces sur la base d'une intelligence globale des menaces, à une communication cryptée et à une transparence globale à l'aide de solutions d'inventaire, de surveillance et d'administration inter-systèmes. Mais jusqu'à présent, les solutions de cybersécurité courantes pour l'IT n'étaient pas préparées aux exigences spécifiques de l'OT.

Exigences en matière de sécurité OT

Les solutions de sécurité OT se doivent d'offrir des fonctionnalités comparables à celles des solutions de sécurité IT, complétées pour les spécificités des environnements OT. Pour cela, elles doivent maîtriser les protocoles spécifiques à l'OT et être en mesure d'inventorier et de surveiller les composants OT, y compris l'état du firmware et les vulnérabilités. Une transparence et une visibilité totale sur l'ensemble de l'infrastructure sont essentielles, de même qu'un contrôle d'accès fiable pour la communication entre l'environnement IT et OT.

Tout comme le réseau IT, le réseau OT doit être judicieusement segmenté en termes de sécurité. Pour sécuriser les composants OT individuels, il est possible de recourir à la microsegmentation individuelle, qui permet de définir précisément les autres systèmes et appareils avec lesquels un composant peut communiquer.

Les fabricants de sécurité IT sur la voie de l'OT

De plus en plus de fabricants de réseaux et de sécurité ont reconnu l'importance de l'OT et ont rendu leurs solutions compatibles avec l'OT à différents degrés. Pratiquement tous les fournisseurs de cybersécurité de renommée, dont Fortinet, Palo Alto Networks ou Kaspersky, ont entre-temps complété leurs solutions par des fonctionnalités spécifiques à l'OT ou ont lancé des solutions supplémentaires sur le marché. Sans oublier d'autres fabricants entièrement axés sur l'OT, comme Claroty.

En principe, les produits utilisés dans l'OT sont généralement les mêmes que ceux utilisés dans l'IT: pare-feux, commutateurs, points d'accès et solutions logicielles pour la gestion et la surveillance des réseaux ainsi que pour la défense contre les menaces. Et en ce qui concerne le matériel, certains fabricants proposent, en plus des appareils couramment utilisés dans l'IT, des variantes «durcies» pour les environnements hostiles avec une plage de température élargie et pour le montage dans des scénarios spécifiques à l'industrie (rail DIN).

BOLL
IT Security Distribution

BOLL Engineering AG

En Budron H15 I 1052 Le Mont-sur-Lausanne
021 533 01 60 I vente@boll.ch
www.boll.ch