Sécurité des systèmes de contrôle industriels

La technologie opérationnelle, abrégée OT (operational technology), est de plus en plus ciblée par les cybercriminels. Cela est d'autant plus dangereux que les réseaux OT ne sont généralement pas conçus pour la cybersécurité. Ruedi Kubli, sales engineer et responsable de l'équipe Fortinet chez BOLL, explique dans une interview en quoi consiste la sécurité OT.

Ruedi Kubli, chef d'équipe Fortinet chez le distributeur de sécurité informatique BOLL.

Que signifie la technologie opérationnelle?
L'OT comprend tous les systèmes électroniques tels que les capteurs, les actionneurs, les serveurs SCADA (supervisory control and data acquisition) ou les systèmes de contrôle industriel (ICS) qui sont directement connectés aux installations industrielles, de la chaîne de production à la turbine de la centrale électrique. Dans cet environnement se déroulent des processus qui, s'ils ne sont pas contrôlés correctement, peuvent entraîner des risques physiques, voire mettre en danger la vie humaine. La sécurité de ces systèmes est particulièrement importante. Cela vaut également pour les PME: pour les hackers, il n'est pas beaucoup plus difficile d'attaquer 1000 PME qu'une grande entreprise.

En quoi les systèmes OT diffèrent-ils des systèmes IT?
Les systèmes OT sont conçus pour une longue durée de vie de dix ans ou plus. Souvent, ils ne sont pas élaborés pour des mises à jour régulières et ne disposent pas de mécanismes de sécurité tels que l'authentification ou la possibilité d'installer des agents, comme c'est souvent le cas dans la protection des terminaux informatiques. Il est ainsi difficile d'éliminer les failles de sécurité ou d'établir de nouvelles normes de sécurité.

Les réseaux OT sont-ils fondamentalement moins sûrs?
Pas forcément. Mais les réseaux OT sont traditionnellement peu segmentés – tout système peut communiquer avec n'importe qui – et le contrôle d'accès au niveau des réseaux informatiques n'est pas courant. En outre, hormis l'IP, les protocoles industriels sont également courants dans l'environnement OT, tels que Modbus, MQTT et Profibus. Les solutions de sécurité conventionnelles et les experts en sécurité informatique ne comprennent généralement pas ces protocoles.

Qui s'occupe de la sécurité des environnements OT?
Les fabricants tels que Siemens ou ABB sont traditionnellement responsables de la sécurité des installations. Ce n'est que depuis quelques années que la cybersécurité est davantage prise en compte. Mais il y a encore des aspects problématiques. Par exemple, lors du traitement des données, telles que les données de mesure des compteurs intelligents, il est souvent difficile de savoir comment et où elles sont traitées et stockées. La classification des données comme dans l'informatique n'est pas courante. C'est précisément pour cette raison que l'OT est une cible de plus en plus visée pour les attaques – les installations ne sont pas aussi bien protégées et les cybercriminels peuvent opérer sous le radar, pour ainsi dire.

Que doit apporter une solution de sécurité OT?
La visibilité et la transparence de l'infrastructure sont parmi les plus importantes. Tous les assets doivent être connus et leurs risques identifiés. En outre, il faut un contrôle d'accès rigoureux concernant l'accès depuis l'environnement informatique et entre les systèmes OT. Une segmentation fonctionnelle et cohérente dans le réseau OT est également utile. Et encore une chose: les systèmes OT fonctionnent souvent dans des environnements difficiles en termes de température, d'humidité ou de poussière – les appareils, y compris les commutateurs de réseau, doivent être robustes et capables de résister à des conditions environnementales difficiles.

Qui propose de telles solutions?
Plusieurs fabricants de réseaux et de systèmes de sécurité se spécialisent de plus en plus dans le domaine de l'OT ou rendent leurs solutions compatibles avec l'OT. Fortinet est un généraliste doté d'une approche holistique. Il étend sa structure de sécurité au monde des technologies de l'information, complétée par une base de données contenant des informations sur la sécurité de nombreux systèmes et dispositifs de ce type. Et pour le secteur des soins de santé, Fortinet travaille avec le spécialiste Medigate et intègre sa solution dans la Security Fabric.

Quels sont les produits qui jouent un rôle dans ce domaine?
En principe, les mêmes produits sont utilisés pour les environnements OT et IT, en partie dans des versions robustes adaptées et complétées par des services spéciaux pour la sécurité industrielle. Par exemple, les pare-feux et commutateurs Fortigate pour la segmentation, FortiAuthenticator pour la gestion des identités et des accès ou FortiSIEM pour la gestion de la transparence et de la sécurité.

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60

vente@boll.ch
www.boll.ch