Bild: pazitivstudija /iStock.com

Sécurité des infrastructures critiques

Avec la numérisation, les systèmes de commande et les infrastructures critiques (technologie opérationnelle ou operational technology, OT), jusqu'ici isolés, s'ouvrent au monde extérieur et se retrouvent soudainement exposés aux cyberattaques. Face à cette évolution, il est impératif de disposer d'une sécurité OT efficace.

Les infrastructures techniques sensibles – qu'elles soient indispensables au fonctionnement d'un pays ou d'une entreprise – ont une histoire qui remonte à plus de 150 ans. Au début de l'industrialisation, les installations telles que les machines de production ou les centrales électriques étaient commandées manuellement à l'aide de composants purement mécaniques tels que des interrupteurs et des régulateurs. Au 20e siècle, des systèmes de surveillance et de commande électriques et électroniques sont venus s'y ajouter, puis de plus en plus des logiciels: On parle alors de technologie opérationnelle (en anglais operational technology, OT).

L'OT a longtemps fonctionné dans le cadre de systèmes fermés: les machines, les capteurs, les actionneurs et les systèmes de contrôle provenaient chacun d'un fabricant particulier, utilisaient des voies de communication et des interfaces utilisateur dédiées, étaient isolés des autres installations et du monde extérieur et ne pouvaient guère être «piratés» sans intrusion physique – la sécurité des infrastructures telles que les installations de production, l'approvisionnement en énergie, les systèmes médicaux, les systèmes de transport et la technique du bâtiment résultait de «l'air gap» avec le reste du monde.

L'ère numérique modifie l'OT et la sécurité OT

Avec la numérisation, les choses ont radicalement changé. Les systèmes OT – composants invidividuels PLC (programmable logic controller), interrogation et commande de capteurs et d'actionneurs, systèmes de contrôle industriels (ICS), système SCADA global (supervisory control and data acquisition) pour la gestion de tout l'environnement OT – sont aujourd'hui mis en réseau, collaborent avec des systèmes IT et peuvent être contrôlés à distance. Outre les normes des fabricants, les systèmes OT misent aussi de plus en plus sur des protocoles spécifiques mais standardisés, comme Modbus, BACnet, IEC-104 DNP3, MQTT et OPC, voire TCP/IP.

Autrement dit, «l'air gap», traditionnellement très apprécié en matière de sécurité, est de l'histoire ancienne, notamment en raison de l'utilisation croissante d'outils d'accès à distance pour la manipulation des systèmes OT. L'ouverture accrue de ces systèmes augmente la surface d'attaque. Par conséquent, les systèmes OT doivent être protégés au moins aussi soigneusement que les systèmes IT. Mais, l'OT n'étant pas l'IT, des mesures de sécurité en partie distinctes sont nécessaires à différents niveaux du modèle Purdue, qui reste pertinent pour les systèmes de contrôle industriels.

Aux deux premiers niveaux – le terrain des différents actionneurs et capteurs tels que les vannes, les pompes ou les capteurs de pression et de température et le niveau de commande avec les composants tels que les PLC, les RTU et les IPC –, il s'agit de surveillance et de commande directes des processus physiques, qui s'effectuent en partie manuellement via des tableaux de commande et en partie via la communication M2M (machine-to-machine) par le biais de protocoles spéciaux. Ce n'est qu'à partir du troisième niveau, celui de la gestion des processus, que la connexion avec des systèmes IT tels que les serveurs SCADA entre en jeu. Ces derniers coopèrent à leur tour avec les systèmes informatiques des niveaux supérieurs, du niveau de gestion de l'exploitation avec les MES (manufacturing execution systems) pour l'industrie et les systèmes comparables pour d'autres infrastructures jusqu'au niveau de l'entre-

prise avec les systèmes informatiques connus, tels que l'ERP et le CRM.

Défis de la sécurité OT

Les sécurités IT et OT sont confrontées au même défi: pour pouvoir évaluer les risques, il faut d'abord savoir dans les moindres détails comment l'infrastructure est construite. Il s'agit ensuite de comprendre la surface et les voies d'attaque possibles. Ce n'est qu'ainsi que l'infrastructure peut être protégée de manière adéquate dans une étape ultérieure.

Il est frappant de constater que toute une série de thèmes de sécurité IT sont également très pertinents pour la sécurité OT. Par exemple, un inventaire complet de tous les systèmes et appareils, l'analyse des informations de log et le fait de savoir quels systèmes et appareils communiquent avec d'autres et comment. La sécurisation des différents systèmes et domaines par la segmentation du réseau, l'authentification forte et le cryptage des communications en font également partie. Et c'est là que se trouve déjà le premier défi spécifique à l'OT: traditionnellement, l'OT n'est guère segmentée, tout au plus simplement authentifiée, et à peine chiffrée. Vous trouverez plus d'informations sur les différences entre la sécurité OT et la sécurité IT dans l'interview ci-contre.

Options pour la sécurité OT

Le programme de distribution de BOLL comprend aussi bien des fournisseurs connus de solutions de sécurité IT que des spécialistes de la sécurité OT, qui proposent des solutions de sécurité orientées OT dans différents domaines fonctionnels. Pour la segmentation, mais aussi pour la protection contre les logiciels malveillants et la détection des menaces, les fabricants de pare-feu comme Fortinet et Palo Alto Networks proposent du matériel spécial pour les environnements difficiles. Les solutions de Palo Alto (basées sur le cloud) et de Claroty (cloud ou sur site) permettent de réaliser un inventaire fiable. Les plateformes de gestion des accès privilégiés (PAM) comme celles de Fudo Security ou de Claroty offrent la meilleure protection pour l'accès à distance et la traçabilité de toutes les opérations, tandis que Fortinet et Palo Alto Networks proposent également un accès à distance sécurisé.

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

INTERVIEW AVEC ROLF BAMERT, SPÉCIALISTE OT, BOLL ENGINEERING

Quelle est la différence entre OT et IT en termes de risques de sécurité?

Les incidents de sécurité dans les infrastructures critiques ont une portée potentiellement beaucoup plus grande. En cas d'incident informatique, une entreprise perd de l'argent, sa réputation et éventuellement des clients. En cas d'incident dans une infrastructure d'approvisionnement, des personnes peuvent être blessées ou même mourir, et des dommages environnementaux peuvent survenir. Si l'approvisionnement en eau de Zurich est contaminé, la santé de centaines de milliers de personnes est en danger.

Et qu'est-ce qui différencie la sécurité OT de la sécurité IT?

Comparé à l'IT, que l'on peut considérer comme un bateau à moteur maniable, l'OT s'apparente davantage à grand navire pétrolier. Chaque changement de cap demande des efforts et du temps et doit être soigneusement planifié. Les systèmes OT sont conçus pour une longue durée de vie et une fiabilité maximale et sont souvent exploités sans changement pendant des années. Les mesures de sécurité doivent également en tenir compte.

Concrètement, cela signifie quoi?

Les systèmes OT présentant des vulnérabilités ne peuvent pas être mis à jour ou supprimés aisément, et les appareils ne peuvent pas être patchés régulièrement comme les systèmes IT, sans éventuellement perturber leur fonctionnement – par exemple un poste de commande d'aiguillage de l'infrastructure ferroviaire ou des systèmes de gestion du trafic. Toute interruption est indésirable et pourrait avoir des conséquences négatives. Il est donc recommandé d'user de solutions de contournement telles que le «virtual patching», avec des systèmes de protection placés en amont, afin d'éviter que les menaces ne parviennent jusqu'à l'appareil.

Dans l'IT, les menaces et les vulnérabilités sont souvent traitées de manière automatisée. Qu'en est-il dans l'OT?

Une mise en œuvre automatique n'est pas efficace dans le monde de l'OT, car une connaissance détaillée du processus est nécessaire pour déterminer les mesures requises: si la vanne X est soudainement fermée en raison d'une alarme de sécurité, cela pourrait faire échouer tout le processus – tandis que dans un autre processus, cela n'aurait peut-être aucun effet. Autre exemple: il se peut que la mise à jour du firmware d'un élément ne soit pas nécessaire, car l'élément en question n'a que peu d'importance pour le fonctionnement.

L'accès à distance pour la maintenance et la gestion est de plus en plus courant dans l'OT. De quoi faut-il tenir compte?

Il y a un élément primordial: le contrôle d'accès et la surveillance doivent être aussi stricts que pour l'accès physique à un centre de données ou à une centrale électrique, c'est-à-dire une authentification forte avec plusieurs facteurs et de la biométrie, ainsi que la surveillance et l'enregistrement de toutes les sessions à distance – comme sur un site où l'on est aussi strictement contrôlé et accompagné.