Les menaces sont toujours d'actualité dans l'OT

Cybersécurité de l'IT et de l'OT | La numérisation joue un rôle de plus en plus important dans pratiquement tous les domaines du système énergétique. Cela crée de nouvelles portes d'entrée pour les cyberattaques. Dans cet entretien, Raphael Reischuk explique où se situent les points communs et les différences entre l'IT et l'OT, et comment les EAE peuvent se protéger efficacement.

En quelques mots

Dr Raphael Reischuk est partenaire et responsable du groupe Cybersécurité chez Zühlke. Il est également membre du Conseil de l'innovation d'Innosuisse ainsi que cofondateur et membre du comité de l'Institut national de test pour la cybersécurité, le centre de compétences suisse chargé des tests indépendants des produits numériques et des infrastructures en réseau. Il a travaillé dans le domaine de la recherche à l'Université de la Sarre, à l'Université Cornell et à l'ETH Zurich.

→ Zühlke Engineering AG, 8952 Schlieren
→ raphael.reischuk@zuehlke.com

Bulletin: En quoi la cybersécurité de l'OT diffère-t-elle de celle de l'IT ?
Raphael Reischuk: Les objectifs de protection des technologies de l'information (information technology, IT) et de la technologie opérationnelle (operational technology, OT) sont fondamentalement différents, tout comme leurs finalités fonctionnelles. Pour comprendre les différences en matière de cybersécurité, il convient en premier lieu de se rappeler en quoi l'IT et l'OT diffèrent. Les systèmes IT sont conçus pour traiter, stocker et transmettre des informations sous forme de données, tandis que les systèmes OT sont destinés à contrôler des appareils physiques et des processus dans des environnements industriels tels que les chaînes de production, les réseaux énergétiques ou les installations de traitement de l'eau. La sécurité des systèmes IT réside en premier lieu dans la confidentialité, l'intégrité et la disponibilité des données, alors que pour les systèmes OT, il s'agit de garantir la sécurité (en anglais safety), la fiabilité et la disponibilité des processus d'exploitation.

La situation initiale est en outre différente pour les attaquants. Les systèmes informatiques sont typiquement utilisés et manipulés par des êtres humains, ce qui signifie que des personnes sont directement impliquées et peuvent détecter des attaques sur les ordinateurs portables, les imprimantes ou les serveurs pendant leur utilisation et, dans l'idéal, réagir rapidement. Si un smartphone chauffe excessivement ou qu'un site Web ou un service ne réagit pas comme d'habitude, il est possible de faire appel immédiatement à un « incident responder » (un intervenant en cas d'incident) et à des experts en science forensique. Les dommages portent alors généralement sur les données sous-jacentes et sur l'indisponibilité de l'infrastructure informatique. Les systèmes OT, en revanche, fonctionnent souvent sans surveillance et sans intervention humaine active ; ils reposent plutôt sur la coordination de machine à machine. Il en résulte que l'authentification des appareils et des accès ne se fait pas par une interaction dynamique des utilisateurs, mais par des informations d'identification enregistrées. En outre, les défaillances et les processus d'exploitation indésirables ne sont détectés que bien plus tard, voire pas du tout. L'élimination des vulnérabilités et des infections peut également être plus compliquée, car les appareils OT sont souvent plus difficiles à atteindre, disposent d'une alimentation en données (réseau radio avec un débit de données plus faible) et d'une alimentation électrique plus complexes ou plus limitées (fonctionnement sur batterie, énergie solaire), et ont typiquement une durée de vie plus longue que les appareils IT : ils comprennent donc plus de composants obsolètes et dépassés. Pourtant, les dommages dans ce domaine sont typiquement plus importants que pour les appareils informatiques en raison de leur impact potentiellement plus élevé sur le monde physique. Pour reprendre les mots de Bruce Schneier : « There is a fundamental difference between crashing your computer and losing an Excel sheet and crashing your pacemaker and losing your life. »

Quelle est la tendance en matière d'attaques dans le domaine de l'OT ? Observe-t-on la même croissance que dans celui de l'IT ? Ou est-ce plus calme ?
Les attaques contre les systèmes OT ont augmenté ces dernières années et révèlent des tendances inquiétantes. Il y a plusieurs raisons à cela : premièrement, les systèmes OT ont, du fait de leur finalité, un potentiel de dommages plus élevé. Alors que les systèmes informatiques sont souvent la cible de cyberattaques ayant pour objectif le vol, la manipulation ou le sabotage de données, les attaques contre les sys-

Figure : Raphael Reischuk

tèmes OT peuvent causer des dommages réels, parfois graves, dans le monde physique. Ceci rend les systèmes OT plus attrayants, tant pour les attaquants motivés par des raisons financières, qui provoquent des interruptions de production ou d'exploitation avec des attaques par ransomware et exigent une rançon pour renflouer leurs caisses, que pour les acteurs étatiques dont l'objectif est d'exercer une pression politique, de créer de l'instabilité ou de commettre des actes de guerre. Deuxièmement, la connectivité accrue entraîne une augmentation du volume des attaques, car les attaquants opèrent de plus en plus à distance, avec un sentiment d'anonymat. Troisièmement, les attaques contre les systèmes OT deviennent plus complexes et plus sophistiquées. Les attaquants utilisent des connaissances spécifiques sur les systèmes de contrôle industriels et sur les protocoles pour mener des attaques ciblées. Ils s'attaquent souvent aux chaînes d'approvisionnement pour compromettre le matériel ou les logiciels qui seront ensuite intégrés dans la technologie OT et utilisés dans les infrastructures critiques. Quatrièmement, les changements géopolitiques du pouvoir et l'augmentation de la menace internationale font intervenir des acteurs étatiques: de nombreuses attaques contre les systèmes OT sont encouragées – ou du moins tolérées – par l'État et visent à perturber des infrastructures critiques, à espionner, à interrompre l'approvisionnement en électricité et en eau, à causer des dommages environnementaux ou à mettre en danger la sécurité publique. Les dommages collatéraux et les profiteurs aggravent le problème.

Quels sont les principaux dangers dans le domaine de l'OT ?

Comme les systèmes OT commandent les processus du monde physique avec leurs actionneurs, les menaces peuvent entraîner non seulement des pertes de données ou des dommages financiers, mais aussi des dommages physiques, des problèmes de sécurité, et même des situations potentiellement mortelles. Concrètement, je vois les menaces suivantes:

Les systèmes OT sont de moins en moins exploités en tant que solution isolée, sans « Air Gap » (c'est-à-dire sans séparation entre les systèmes OT et les réseaux externes). Ils communiquent de plus en plus avec le monde extérieur connecté via des canaux publics pour envoyer des données télémétriques, recevoir des ordres de commande et des notifications, ou faire des demandes au monde extérieur. Ce degré croissant d'interconnexion permet toutefois en principe aux pirates d'accéder à distance aux systèmes critiques et de causer des dommages.

Un fait souvent sous-estimé est que l'on n'utilise, dans le domaine de l'OT, que rarement des puces spécifiques, limitées à cette fonctionnalité. Au lieu de cela, on utilise souvent – paradoxalement pour des raisons de coûts – des appareils et des processeurs tout à fait standard, dont la capacité de calcul n'est pas limitée et qui sont donc en mesure d'exécuter bien plus que la fonctionnalité réellement nécessaire. Ceci pose problème, car un pirate peut non seulement exploiter la fonctionnalité implémentée sur le système cible, mais aussi installer son propre code et l'utiliser contre les actionneurs et les autres systèmes connectés. Si, par exemple, un environnement Java non patché est disponible, il constitue un terrain idéal pour de nombreuses attaques. La sécurisation du matériel et des logiciels à usage général dans un environnement d'application limité devient donc un aspect décisif de la sécurité OT.

Les entreprises d'approvisionnement en énergie sont-elles suffisamment sensibilisées aux dangers ? Où voyez-vous des améliorations à effectuer ?

Il me semble que la sensibilisation des entreprises d'approvisionnements critiques aux dangers a généralement augmenté, comme le montrent les documents d'appel d'offres qui mentionnent de plus en plus souvent la cybersécurité comme une exigence indispensable. Néanmoins, de nombreuses petites entreprises d'approvisionnement ne sont guère en mesure de prendre des mesures exhaustives, raison pour laquelle il faut aussi s'attendre à des attaques à l'avenir. C'est notamment pour sensibiliser que j'ai fondé en 2020, en collaboration avec le Conseil d'État du canton de Zoug, l'Office fédéral de la cybersécurité et d'autres experts, l'Institut national de test pour la cybersécurité (NTC), qui s'est donné pour mission de détecter les points faibles aux endroits menacés par des dommages critiques et où le marché n'investit pas assez, et d'y remédier.

Les outils de sécurité utilisés dans le domaine de l'OT sont-ils les mêmes que ceux utilisés dans le secteur de l'IT ?

La principale différence réside dans les mécanismes sous-jacents. Certes, la plupart des principes et des paradigmes de la sécurité IT s'appliquent également au monde OT. Il existe cependant des exigences parfois plus strictes, des normes spécifiques telles que la série de normes IEC 62443 sur les réseaux de communication industriels, et des architectures de référence dédiées telles que le modèle de référence Purdue. Pour citer quelques exemples concrets: dans le domaine de l'OT, les mises à jour doivent souvent pouvoir être réalisées « over-the-air », être signées et fournir des procédures à sécurité intégrée afin de minimaliser ou d'éviter complètement les défaillances des installations d'approvisionnement et de production. Dans l'IT, les mises à jour sont souvent réalisées par des personnes qui les accompagnent tout au long du processus. Dans l'OT, elles doivent s'effectuer à distance et de manière essentiellement autonome. En outre, la détection des anomalies est importante et doit également se faire de manière aussi autonome que possible, même à distance.

Les mécanismes d'authentification diffèrent également: les procédures visant à garantir une identité d'appareil infalsifiable et non copiable, un démarrage sécurisé et la mise à disposition d'identifiants uniques sont plus importantes dans le monde de l'OT que dans celui de l'IT, où les personnes peuvent s'authentifier sur les appareils en saisissant un mot de passe ou en fournissant d'autres facteurs d'identification. De plus, les appareils OT ont souvent une puissance de calcul limitée en raison d'une alimentation électrique plus faible ou restreinte. Par conséquent, une cryptographie moins gourmande en ressources, et donc moins performante, doit souvent être utilisée.

Les architectures de système sont aussi différentes: dans le domaine de l'OT, l'architecture de type Harvard est à privilégier car, contrairement à l'architecture de von Neumann largement répandue, les données et le code du

programme y sont stockés dans des mémoires séparées. Ceci présente l'avantage que les vulnérabilités dues aux dépassements de mémoire tampon, lors desquels les données sont interprétées et exécutées comme du code de programme, sont moins facilement exploitables. Une autre différence au niveau technique réside dans le fait que les appareils OT communiquent souvent entre eux via des protocoles propriétaires développés par les fabricants d'appareils, qui ne sont pas entièrement pris en charge par les solutions de sécurité informatique. Les tests de ces solutions sont également plus complexes et moins exhaustifs.

Enfin, j'aimerais insister sur la nécessité d'une documentation complète et de la communication explicite des hypothèses en matière d'utilisation prévue. Les analyses de menaces (threat modeling) réalisées pendant le développement se basent sur des hypothèses concernant l'utilisation et les modèles d'attaquants. Si ces hypothèses ne sont pas communiquées à l'exploitant, ou si elles ne sont pas prises en compte lors de l'adaptation de l'installation, cela peut générer des situations dangereuses n'ayant pas été considérées dans le dispositif de sécurité.

Pouvez-vous nous donner quelques exemples de cas d'attaques perpétrées dans le domaine de l'OT ?

La liste est longue. Dans de nombreux cas, des systèmes informatiques ont été attaqués pour endommager des systèmes OT. Ainsi, en mai 2021, le Colonial Pipeline, l'un des plus grands pipelines de carburant aux États-Unis, a été la cible d'une attaque par ransomware. Ceci a entraîné la mise hors service temporaire de l'oléoduc et a provoqué une pénurie de carburant à grande échelle, une hausse du prix de l'essence et des achats panique dans certaines régions des États-Unis. Les exploitants ont payé une rançon d'environ 4,4 millions de dollars en bitcoins. Cette attaque et d'autres cas célèbres soulignent la croissance des cybermenaces contre les systèmes OT et les infrastructures critiques : parmi celles-ci, notamment, l'attaque peut-être la plus célèbre, Stuxnet, contre le programme nucléaire iranien (2010), les attaques de Sandworm contre l'approvisionnement en électricité de l'Ukraine (contre 230 000 Ukrainiens pendant environ six heures en 2015, et contre 700 000 Ukrainiens pendant environ une heure en 2016), et la cyberattaque Triton (2017) contre un site pétrochimique au Moyen-Orient. Les informations et les rapports ne sont toutefois souvent pas clairs : il n'a par exemple pas suffisamment pu être prouvé que la cyberattaque de la station de traitement d'eau d'Oldsmar (2021), en Floride, ait réellement été perpétrée par des cybercriminels.

Comment jugez-vous l'utilité de nouvelles plateformes Internet telles que Scion pour la sécurité de l'OT ?

En tant qu'ancien scientifique ayant travaillé au développement de Scion, de nombreux aspects positifs me viennent à l'esprit. Comme je l'ai dit plus tôt, quand on parle de sécurité, on pense généralement à la confidentialité des données, et celle-ci est généralement placée en tête des objectifs de sécurité. Dans le monde de l'OT, où la disponibilité constitue le premier objectif de sécurité, il s'agit avant tout de faire en sorte que l'infrastructure continue de fonctionner, presque indépendamment de ce qui se passe dans le monde extérieur.

En raison de ces exigences élevées en matière de disponibilité, l'utilisation de l'Internet public en tant que réseau dorsal de communication pour les systèmes OT est parfois liée à des risques élevés. L'Internet actuel est trop vulnérable aux défaillances, qu'elles soient dues à un sabotage ciblé ou à des erreurs de configuration. Les exploitants de systèmes OT ont donc souvent recours à la location onéreuse de lignes ou à des connexions MPLS. L'architecture de routage et de transfert basée sur les chemins de données de Scion rend Internet beaucoup plus résistant aux défaillances : les exploitants de systèmes OT peuvent atteindre une plus grande résilience pour le transfert de leurs données de contrôle en choisissant de manière ciblée les chemins de routage et en assurant la redondance. Scion crée ainsi une classe de connectivité qui est moins chère que les solutions à haute disponibilité actuelles, et en même temps plus fiable que l'Internet public.

Scion n'est certes pas la solution à tous les problèmes, mais il est très prometteur si les conditions sont appropriées. Il pourrait mener à des économies substantielles pour les exploitants et permettre de nouvelles applications OT considérées comme non rentables jusqu'à présent.

INTERVIEW : RADOMÍR NOVOTNÝ