Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 115 (2024)
Heft: 3

Artikel: Bei der OT gehen die Bedrohungen weiter = Les menaces sont toujours d'actualité dans l'OT
Autor: Novotný, Radomír
DOI: https://doi.org/10.5169/seals-1075071

Bei der OT gehen die Bedrohungen weiter

Cybersicherheit von IT und OT | Im Energiesystem spielt die Digitalisierung in praktisch allen Bereichen eine zunehmend grosse Rolle. Dadurch entstehen neue Einfallstore für Cyberangriffe. Wo die Gemeinsamkeiten und Unterschiede zwischen der IT und der OT liegen und wie sich EVUs wirksam schützen können, erläutert Raphael Reischuk im Interview.

Bild: Raphael Reischuk

Zur Person

Dr. Raphael Reischuk ist Partner und Group Head of Cybersecurity bei Zühlke. Zudem ist er Mitglied des Innovationsrats von Innosuisse sowie Mitgründer und Vorstandsmitglied des Nationalen Testinstituts für Cybersicherheit, dem Schweizer Kompetenzzentrum für die unabhängige Prüfung digitaler Produkte und vernetzter Infrastrukturen. Er hat an der Universität Saarland, der Cornell University sowie der ETH Zürich geforscht.

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

Bulletin: Wodurch unterscheidet sich die Cybersicherheit von IT und OT?
Raphael Reischuk: Die Schutzziele von Informationstechnologie (IT) und Betriebstechnologie (OT) sind – ebenso wie ihre funktionalen Zweckbestimmungen – grundverschieden. Um die Unterschiede in der Cybersicherheit zu verstehen, muss man sich zunächst die Unterschiede von IT und OT vergegenwärtigen. IT-Systeme sind ausgerichtet auf die Verarbeitung, Speicherung und Übertragung von Informationen in Form von Daten, OT-Systeme hingegen auf die Steuerung physischer Geräte und Prozesse in industriellen Umgebungen, wie Fertigungsstrassen, Energienetze oder Wasseraufbereitungsanlagen. Die Sicherheit von IT-Systemen liegt primär in der Vertraulichkeit, Integrität und Verfügbarkeit der Daten, wohingegen es bei OT-Systemen um die Gewährleistung der Sicherheit (engl. safety), Zuverlässigkeit und Verfügbarkeit der Betriebsabläufe geht.

Die Ausgangslage der Angreifer ist zudem eine andere. IT-Systeme werden typischerweise von Menschen benutzt und bedient, d.h. Menschen sind direkt involviert und können Angriffe auf Laptop, Drucker oder Server während der Bedienung erkennen und im Idealfall schnell reagieren. Erwärmt sich ein Smartphone übermässig oder reagiert eine Webseite oder ein Service nicht wie gewohnt, können Incident Responder und Forensiker sofort hinzugezogen werden. Der Schaden bezieht sich dann meist auf die zugrunde liegenden Daten und die Nichtverfügbarkeit der IT-Infrastruktur. OT-Systeme hingegen funktionieren oft unbeobachtet und ohne aktive menschliche Beteiligung; sie beruhen stattdessen auf der Koordination von Maschine zu Maschine. Dies hat zur Folge, dass die Authentifizierung von Geräten und Zugängen nicht über dynamische Benutzerinteraktion, sondern über gespeicherte Anmeldeinformationen erfolgt. Zudem werden Ausfälle und unerwünschte Betriebsabläufe erst bedeutend später oder gar nicht erkannt. Auch die Behebung von Schwachstellen und Infektionen ist unter Umständen schwieriger, da OT-Geräte oft schwerer erreichbar sind, über eine aufwendigere oder eingeschränktere Stromversorgung (Batteriebetrieb, Solarstrom) und Datenversorgung (Funknetz mit geringerem Datendurchsatz) verfügen und typischerweise eine längere Lebenserwartung als IT-Geräte haben und entsprechend über mehr veraltete und überholte Komponenten verfügen. Allerdings sind die Schäden aufgrund der potenziell höheren Auswirkung auf die physische Welt typischerweise grösser als bei IT-Geräten. Um es mit den Worten von Bruce Schneier zu sagen: «There is a fundamental difference between crashing your computer and losing an Excel sheet and crashing your pacemaker and losing your life.»

Wie sieht der Trend bei den Angriffen auf die OT aus? Gleich wachsend wie bei der IT? Oder ist es da ruhiger?
Die Angriffe auf OT-Systeme haben in den letzten Jahren zugenommen und zeigen besorgniserregende Trends. Dafür gibt es mehrere Gründe: Erstens haben OT-Systeme aufgrund ihrer Zweckbestimmung ein höheres Schadenspotenzial. Während IT-Systeme häufig Ziel von Cyberangriffen sind, die auf Datendiebstahl, -manipulation oder -sabotage abzielen, können Angriffe auf OT-Systeme reale, zum Teil schwerwiegende Schäden in der physischen Welt verursachen. Dieser Umstand macht OT-Systeme attraktiver – sowohl für finanziell motivierte Angreifer, die mit Ransomware-Angriffen Produktions- oder Betriebsunterbrechungen herbeiführen und Lösegeld fordern, um ihre Kassen aufzubessern, als auch für staatliche Akteure, deren Ziel es ist, politischen Druck auszuüben, Instabilität zu schaffen oder Kriegshandlungen zu begehen. Zweitens führt die erhöhte

Konnektivität zu einem Anstieg des Angriffsvolumens, da die Angreifer im Gefühl von Anonymität zunehmend aus der Ferne operieren. Drittens werden Angriffe auf OT-Systeme komplexer und ausgefeilter. Angreifer nutzen spezifisches Wissen über industrielle Steuerungssysteme und Protokolle, um gezielte Angriffe durchzuführen. Oft werden dabei die Lieferketten angegriffen, um Soft- oder Hardware zu kompromittieren, die später in OT-Technologie integriert und in kritischen Infrastrukturen eingesetzt wird. Viertens rufen die geopolitische Machtverschiebung und die gestiegene internationale Bedrohungslage staatliche Akteure auf den Plan: Viele Angriffe auf OT-Systeme sind staatlich gefördert – oder mindestens geduldet – und zielen darauf ab, kritische Infrastrukturen zu stören, Spionage zu betreiben, die Strom- und Wasserversorgung zu unterbrechen, Umweltschäden zu verursachen oder die öffentliche Sicherheit zu gefährden. Kollateralschäden und Trittbrettfahrer verschärfen das Problem.

Was sind die grössten Gefahren bei der OT?

Da OT-Systeme mit ihren Aktoren die Prozesse in der physischen Welt steuern, können Bedrohungen nicht nur zu Datenverlust oder finanziellen Schäden führen, sondern auch zu physischen Schäden, Sicherheitsrisiken und sogar lebensbedrohlichen Situationen. Konkret sehe ich folgende Bedrohungen:

OT-Systeme werden immer seltener als Insellösung betrieben, ohne Air Gap. Sie kommunizieren zunehmend über öffentliche Kanäle mit der vernetzten Aussenwelt, um Telemetriedaten zu senden, Steuerbefehle und Benachrichtigungen zu empfangen oder Anfragen an die Aussenwelt zu stellen. Der zunehmende Vernetzungsgrad ermöglicht es Angreifern jedoch prinzipiell auch, aus der Ferne auf kritische Systeme zuzugreifen und Schaden anzurichten.

Ein oft unterschätzter Umstand ist, dass nur selten spezifische, auf die eigentliche Funktionalität beschränkte Hardware-Chips eingesetzt werden. Stattdessen werden – paradoxerweise aus Kostengründen – häufig vollwertige Standardgeräte und -prozessoren verwendet, die in ihrer Berechenbarkeit nicht eingeschränkt sind und daher in der Lage sind, weit mehr als die tatsächlich benötigte Funktionalität auszuführen. Dies ist deshalb problematisch, da ein Angreifer auf dem Zielsystem nicht nur die implementierte Funktionalität ausnutzen, sondern beliebigen eigenen Code aufspielen kann und diesen dann gegen die Aktoren und andere angeschlossene Systeme einsetzen kann. Steht beispielsweise eine nicht gepatchte Java-Umgebung zur Verfügung, so bietet diese einen idealen Nährboden für zahlreiche Angriffe. Die Härtung von Allzweck-Hard- und Software in einer eingeschränkten Anwendungsumgebung wird daher zu einem entscheidenden Aspekt der OT-Sicherheit.

Sind die Energieversorgungsunternehmen genügend sensibilisiert bezüglich der Gefahren? Wo sehen Sie Nachholbedarf?

Mir scheint, dass das Bewusstsein bei kritischen Versorgungsunternehmen insgesamt gestiegen ist, was sich auch in Ausschreibungsunterlagen zeigt, in denen Cybersicherheit immer häufiger als unabdingbare Anforderung genannt wird. Dennoch sind viele kleinere Versorgungsunternehmen heute kaum in der Lage, umfassende Massnahmen zu ergreifen, weshalb auch in Zukunft mit Angriffen zu rechnen ist. Nicht zuletzt zur Sensibilisierung habe ich im Jahr 2020 zusammen mit dem Regierungsrat Zug, dem Bundesamt für Cybersicherheit und weiteren Experten das Nationale Testinstitut für Cybersicherheit NTC gegründet, welches es sich zur Aufgabe gemacht hat, Schwachstellen dort aufzudecken und zu beheben, wo kritische Schäden drohen, aber seitens des Marktes zu wenig investiert wird.

Kommen im OT-Bereich die gleichen Security-Tools zum Einsatz wie bei der IT?

Der Hauptunterschied liegt in den zugrunde liegenden Mechanismen. Zwar gelten die meisten Prinzipien und Paradigmen der IT-Sicherheit auch für die OT-Welt. Dennoch gibt es zum Teil verschärfte Anforderungen, spezifische Normen wie die IEC-62443-Reihe über industrielle Kommunikationsnetze und dedizierte Referenzarchitekturen wie dem Purdue Model. Um ein paar konkrete Beispiele zu nennen: In der OT müssen Updates häufig over-the-air funktionieren, signiert sein und ausfallsichere Prozeduren bereitstellen, um Ausfälle von Produktions- und Versorgungsanlagen zu minimieren oder ganz zu vermeiden. In der IT werden die Updates häufig von Menschen eingespielt und durch den Prozess begleitet. In der OT müssen sie weitgehend autonom und per Fernwartung ablaufen. Darüber hinaus ist die Erkennung von Anomalien wichtig und muss ebenfalls möglichst autonom erfolgen, auch aus der Ferne.

Im Gegensatz zur IT unterscheiden sich auch die Authentifizierungsmechanismen: Verfahren zur Sicherstellung einer fälschungssicheren und nicht kopierbaren Geräteidentität, zum sicheren Booten und zur Bereitstellung eindeutiger Credentials sind in der OT-Welt wichtiger als in der IT-Welt, in der sich Personen an Geräten durch Passworteingabe oder die Bereitstellung weiterer Faktoren authentifizieren können. Zudem haben OT-Geräte oft eine begrenzte Rechenleistung aufgrund einer schwächeren oder eingeschränkten Stromversorgung. Folglich muss häufig schwächere Kryptografie verwendet werden, da diese ressourcenschonender ist.

Auch die Systemarchitekturen unterscheiden sich: In der OT-Welt ist die Harvard-Architektur zu bevorzugen, da sie im Gegensatz zur weitverbreiteten Von-Neumann-Architektur die Daten und den Programmcode in getrennten Speichern ablegt. Dies hat den Vorteil, dass Schwachstellen durch Buffer Overflows, bei denen Daten als Programmcode interpretiert und ausgeführt werden, weniger leicht ausgenutzt werden können. Ein weiterer Unterschied auf technischer Ebene besteht darin, dass OT-Geräte häufig über proprietäre Protokolle miteinander kommunizieren, die von den Geräteherstellern entwickelt wurden und von IT-Sicherheitslösungen nicht vollständig unterstützt werden. Auch das Testen dieser Lösungen ist aufwendiger und weniger umfassend.

Abschliessend möchte ich noch auf die Notwendigkeit einer vollständigen Dokumentation und explizit kommunizierter Annahmen über den Einsatzzweck hinweisen. Die während der Entwicklung durchgeführten Bedrohungsanalysen (Threat Modeling) basieren auf Annahmen über Einsatzzweck und Angreifermodelle. Werden diese nicht an den Betreiber kommuniziert oder bei Anlagenanpassungen nicht berücksichtigt, so können gefähr-

liche Situationen entstehen, die im Sicherheitsdispositiv nicht berücksichtigt wurden.

Welche Fälle von Angriffen auf OT kennen Sie?
Die Liste ist lang. In vielen Fällen wurden dabei IT-Systeme angegriffen, um OT-Systeme zu schädigen. So wurde im Mai 2021 die Colonial Pipeline, eine der grössten Treibstoffpipelines in den USA, Ziel eines Ransomware-Angriffs. Der Vorfall führte zur vorübergehenden Stilllegung der Pipeline und verursachte eine weitreichende Treibstoffknappheit, steigende Benzinpreise und Panikkäufe in Teilen der USA. Die Betreiber zahlten ein Lösegeld von rund 4,4 Millionen US-Dollar in Bitcoin. Dieser Angriff und andere prominente Vorfälle unterstreichen die wachsenden Cyberbedrohungen gegen OT-Systeme und kritische Infrastrukturen: dazu zählen der vielleicht berühmteste Angriff, Stuxnet, auf das iranische Nuklearprogramm (2010), die Sandworm-Angriffe auf die ukrainische Stromversorgung (2015 gegen 230 000 Ukrainer für etwa sechs Stunden, 2016 gegen 700 000 Ukrainer für etwa eine Stunde), und Triton (2017) auf eine petrochemische Anlage im Nahen Osten. Häufig sind die Aufklärung und die Berichterstattung jedoch unklar, z. B. ist nicht hinreichend erwiesen, ob der Oldsmar-Wasseranlagen-Hack (2021) in Florida tatsächlich von Cyberkriminellen verübt wurde.

Wie schätzen Sie die Nützlichkeit von neuen Internet-Plattformen wie Scion für die Sicherheit in der OT ein?
Als ehemaliger Wissenschaftler hinter Scion fallen mir viele positive Aspekte ein. Wie eingangs erwähnt, denkt man bei Sicherheit in der Regel an die Vertraulichkeit von Daten und nennt dies als oberstes Sicherheitsziel. In der OT-Welt, wo die Verfügbarkeit das oberste Sicherheitsziel ist, geht es in erster Linie darum, dass die Infrastruktur weiter funktioniert, fast unabhängig davon, was mit der Aussenwelt passiert.

Aufgrund dieser hohen Verfügbarkeitsanforderungen ist die Nutzung des öffentlichen Internets als Kommunikations-Backbone für OT-Systeme mit teilweise hohen Risiken verbunden. Das heutige Internet ist zu anfällig für Ausfälle – sei dies durch gezielte Sabotage oder durch Konfigurationsfehler. OT-Betreiber greifen daher häufig auf teure Mietleitungen oder MPLS-Verbindungen zurück. Die pfadbasierte Routing- und Forwarding-Architektur von Scion macht das Internet wesentlich ausfallsicherer: Betreiber von OT-Systemen können durch gezielte Auswahl der Routing-Pfade und Sicherstellung von Redundanz eine höhere Resilienz für ihren Steuerverkehr erreichen. Scion schafft damit eine Konnektivitätsklasse, die kostengünstiger ist als heutige Hochverfügbarkeitslösungen und gleichzeitig zuverlässiger als das heutige öffentliche Internet.

Scion ist zwar kein Allheilmittel für alle Probleme, aber unter den richtigen Bedingungen sehr vielversprechend. Es könnte zu erheblichen Kosteneinsparungen für die Betreiber führen und neue OT-Anwendungen ermöglichen, die bisher als wirtschaftlich unrentabel galten. **INTERVIEW: RADOMÍR NOVOTNÝ**

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