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