OT-Security Spezialisten: Digitale Hirten unserer kritischen Infrastrukturen

Geschrieben von Joshua Bucheli, KI Ethik Forscher und Fellow beim ForHumanity Center, in Zusammenarbeit mit Swantje Westpfahl Acting Director der ISS, Christian Fichtner Senior Cyber Security Architekt bei der Deutschen Bahn, Stefan Schillings Information Security Officer und Cloud Architect bei den Schweizerischen Bundesbahnen und Peter Kosel, Gründer von cyberunity

Vor 10 Jahren hinderte der berüchtigte PSN-Hack und -Ausfall Millionen von Gamern fast einen Monat lang daran, online zu zocken. Er kostete Sony über 170 Millionen Dollar, kompromittierte die sensiblen Daten von rund 80 Millionen Benutzerkonten und empörte Gamer auf der ganzen Welt.

Solche Vorfälle sind zwar typisch für die kostspieligen Unannehmlichkeiten, die Cybersecurity-Verstösse in der IT verursachen können. Sie verblassen aber im Vergleich zu dem, was uns bevorsteht, wenn unsere Kerninfrastrukturen von ähnlichen Angriffen heimgesucht werden.

Die IT steht oft im Rampenlicht, aber sie ist nicht die einzige Dimension der Cybersicherheit. Die Absicherung von Operational Technologies (OT) - der Hard- und Software, die physische Geräte und Prozesse in einer Infrastruktur überwacht und steuert - ist von ebenso grosser Bedeutung.

«Im Gegensatz zu den Anfängen von OT, die mehr für einen Zweck als auf einer Interoperabilität zu IT konzipiert waren, werden OT-Strukturen in einem ‘Industrie 4.0 Umfeld’ intelligenter und kommunikativer, weit über ihre physischen Grenzen hinaus. Dem stehen aber proprietäre Protokolle entgegen, die Security eher rudimentär implementiert haben und um ein

vielfaches angreifbarer sind als heutige Protokolle, die es in IT-Umgebungen gibt», sagt Christian Fichtner, Senior Cyber Security Architekt bei der Deutschen Bahn.

Schalttafeln in Fabriken. Weichen bei Transportunternehmen. Stromnetze und Systeme, die Verkehrsampeln, Industriemaschinen und Kernreaktoren-Stäbe steuern. Obwohl sie der IT etwas hinterherhinken, treten diese OT-Legacy-Systeme (veraltet, aber funktional) in das digitale Zeitalter ein - unsere kritischen Infrastrukturen ‘gehen online’.

Wo steht das Thema OT heute?

Laut Swantje Westpfahl, Co-Direktorin des Institute for Safety and Security, ist die Digitalisierung das Gebot der Stunde:

«Die OT-Branche steckt voll im Digitalisierungsprozess und sobald diese Systeme mit dem Netzwerk verbunden sind, sind sie gefährdet. Jeder will vernetzt sein, weil es vieles einfacher macht. Aber genau diese Leichtigkeit bringt auch Risiken mit sich - sowohl offensichtliche als auch undurchschaubare. Dass sich die Dinge sowohl in Richtung Automatisierung als auch in Richtung Fernsteuerung entwickeln macht die Situation noch brisanter.»

Das vielleicht drängendste Problem, mit dem OT heute konfrontiert ist, ist der wachsende ‘Awareness-Gap’, wenn es um Art und Umfang von Cyber-Bedrohungen geht:

«Die Mitarbeitenden stehen neben den Schalttafeln und denken, sie hätten alles unter Kontrolle. Aber wenn Legacy-Systeme online gehen, sind sich diese Personen oft nicht bewusst, wie einfach es ist, solche Systeme zu hacken - das stellt potenziell lebensbedrohliche Risiken dar.»

Nehmen Sie die Netzbetreiber, die die Verteilung von Strom auf nationaler und regionaler Ebene verwalten. Sobald diese online gehen und hackbar werden, können Sicherheitsverstösse katastrophale Stromausfälle bewirken, die Tage oder sogar Wochen dauern.

Betrachten wir beispielsweise die Stromausfälle in der Ukraine 2015 und 2016 oder den bereits vor 10 Jahren aufgetretenen Stuxnet-Vorfall, bei dem Zentrifugen des iranischen Urananreicherungs-Programms sabotiert wurden.

Selbst scheinbar triviale OT können Leben kosten, wenn sie Cyberangriffen ausgesetzt sind. Zum Beispiel Systeme zur Steuerung von Brauerei- und Brennereianlagen - wenn diese kompromittiert werden, könnte die Manipulation dieser Maschinen durch böswillige Parteien nicht nur die Produktion unterbrechen, sondern sogar tragische Explosionen verursachen.

Wir brauchen uns nur die Verwüstung vor Augen zu führen, die durch den 2014 erfolgten Cyber-Angriff auf einen Stahlwerk-Hochofen in Deutschland verursacht wurde, um uns das potenzielle Chaos vorzustellen, das arglistig inszenierte Stromausfälle und Industrie-katastrophen anrichten können.

Die Entwicklung der IoT-Technologie, die wahrscheinlich mit denselben Netzwerken verbunden sein wird wie die zukünftige OT, wird zweifellos auch eine entscheidende Rolle in dieser ganzen Gleichung spielen, argumentiert Swantje - ebenso die Brute-Force-Bedrohungen, die durch das Aufkommen von Quantencomputern entstehen.

Einige Nationen haben bereits konzertierte Anstrengungen unternommen, um diese Probleme anzugehen:

Israel hat die Nase vorn, wenn es darum geht, Cybersicherheit als Schulfach in das öffentliche Bildungssystem zu integrieren. Estland ist schon fast komplett durchdigitalisiert und hat die Blockchain-Technologie als Mittel zur Sicherung seiner Informations-Infrastrukturen eingesetzt. Unterdessen ist Japan bei der Behandlung von Sicherheitsbelangen im Automobilbereich führend, indem es Vorschriften wie die UN-Norm R155 /R156 sofort umsetzt und Automobile in erster Linie als IoT betrachtet.

Dennoch bleibt noch viel zu tun, und es ist absolut entscheidend, dass Unternehmen, Branchenführer und politische Entscheidungsträger Tools wie den Cyber-Demonstrator des ICBC erkennen und sich zu Nutze machen um sich besser mit diesen Themen auseinanderzusetzen:

«Im Endeffekt bringen einfache Eintrittswahrscheinlichkeit- und Risikoberechnungen alleine nicht viel. Wenn wir uns die Zunahme von Cyberangriffen in den letzten Jahren ansehen, wird deutlich, dass sie eher die Norm als die Ausnahme sein werden - und das gilt für OT genauso wie für IT», warnt Swantje.

OT-Security Spezialisten: Gefragte Fähigkeiten und Ausbildungen

Wenn es um Ausbildungen geht, sind Informatikstudiengänge mit Schwerpunkt auf IoT, SCADA und anderen kritischen Infrastrukturen für angehende OT-Sicherheitsspezialisten von grossem Vorteil (siehe z. B. den Bachelor in Information & Cyber Security Major in Technology der Hochschule Luzern).

Zertifikate und Schulungen, die speziell auf die industrielle Cybersicherheit ausgerichtet sind, wie die vom ISS' Capacity Building Center (ICBC) und Dragos, oder die GICSP-, GRID- und GCIP-Zertifikate von GIAC, verschaffen den Kandidaten natürlich einen besonderen Vorteil. Aber auch Personen mit Sicherheitszertifizierungen wie CEH, CISSP und CISM fallen positiv auf, und Abschlüsse und Zertifizierungen in ingenieurwissenschaftlichen Disziplinen sind ebenfalls von Vorteil.

Einem guten Hirten ähnlich, werden OT-Security Spezialisten unsere kritischen Infrastrukturen sicher ins digitale Zeitalter begleiten. Der Kampf um diese Infrastrukturen wird an vielen Fronten stattfinden. Daher werden Arbeitgeber ihre OT umso besser schützen können, je breiter sie ihre Talentsuche nach IT-Ingenieuren und Netzwerkspezialisten ausweiten.

«Je grösser und vernetzter das betreffende Unternehmen ist, desto wichtiger sind Mitarbeiter mit der Fähigkeit, eine ganzheitliche Perspektive auf die Frage nicht nur der IT- , sondern auch der OT-Sicherheit einzubringen», rät Swantje.

«Angehende OT-Security Spezialisten sollten daher idealerweise in der Lage sein, Fachwissen und Best Practices aus so unterschiedlichen Bereichen wie Produktion, IT-fokussierte Cybersicherheit und Risikomanagement zusammenzubringen».

In Bezug auf Hard Skills bedeutet dies folgendes: Fachwissen in den Bereichen Netzwerksicherheit, Penetration-Testing und im Aufbau von Business-Continuity-Modellen, Engineering-Know-How und ein Verständnis für das Thema Echtzeitanwendungen. Erfahrung in

der Absicherung von physischen Systemen, ICS und Grundkenntnisse in Elektrotechnik oder Maschinenbau sind ebenfalls ein grosses Plus.

Da OT allgegenwärtig ist, gibt es unzählige Einstiegspunkte in die OT-Security-Branche. Organisationen, die spezialisierte industrielle OT-Sicherheitslösungen anbieten, wie Dragos, Fortinet, InfoGuard, Secunet, Cyberbit, oder das entstehende internationale Security Operations Center Hub der VINCI Energies in Basel, sind ideale Anlaufstellen.

Dennoch dürfen die Branchen, in denen diese OT-Systeme hergestellt und schon über viele Jahre betrieben werden, nicht ausser Acht gelassen werden.

Wie Stefan Schillings, Information Security Officer und Cloud Architekt bei den SBB, betont, «Die Schwierigkeit über Jahrzehnte OT-Systeme zu betreiben und zu supporten ist gewaltig. Die Supply-Chains müssen aktiv gesichert und geprüft werden - und Änderungen an bestehenden Anlagen bedürfen sehr exakter Kenntnisse, was in Zeiten von Online-Patching eine echte Herausforderung darstellt!»

Bahnen wie die SBB, die DB und die EWS, Hersteller von Industriemaschinen wie Caterpillar Inc., ABB, Cisco und Linde AG sowie andere Unternehmen, die wichtige Infrastrukturen wie Energieunternehmen und Kernkraftwerke betreiben, werden alle die Unterstützung von OT-Security Spezialisten benötigen, wenn sie den Übergang ins digitale Zeitalter überleben wollen.

Persönlichkeit – über technisches Know-How hinaus:

«OT-Security Spezialisten erschaffen den aktuellen Sprung der Informationssicherheit, die, wie in der IT auch, immer häufiger die OT betrifft. Sie verstehen das Business und sind Vermittler zwischen OT und einer viel kleineren IT Welt. Sie sind Dolmetscher zwischen Ingenieuren und IT-Profis, vertreten OT-relevante Aspekte einer konvergierenden IT/OT-Welt und entwickeln Sicherheitskonzepte auf Basis von Greenfield, Brownfield und Darkfield Ansätzen. Denn jede OT-Umgebung ist anders und optimal an seine Aufgabe angepasst», erklärt Christian.

Aufgrund dieser vielfältigen Aufgaben ist es unabdingbar, dass OT-Security Spezialisten über Qualitäten verfügen, die über die bereits erwähnten Hard Skills hinausgehen.

Von grosser Bedeutung sind zum Beispiel Kommunikationsfähigkeiten. OT-Security Spezialisten müssen sich nicht nur dynamisch in interdisziplinären Teams eingliedern können, um Sicherheitsanforderungen zu identifizieren, sie müssen auch in der Lage sein, diese Anforderungen gegenüber Managern und C-Suite-Führungskräften im gesamten Unternehmen zu vermitteln, oder zumindest, sofern vorhanden, dem CISO.

Wachsamkeit und ausgeprägte analytische Fähigkeiten sind ebenfalls von entscheidender Bedeutung, da die Mitarbeiter täglich mit den sich ständig weiterentwickelnden Bedrohungen konfrontiert sind.

«Man muss genug Fantasie mitbringen, um die Vorstellung bei operativen Einheiten zu wecken, dass ihre Anlagen nicht unangreifbar sind. Tools wie das Mitre-ICS ATT&CK Framework können helfen, die sich weiterentwickelnden Bedrohungsszenarien besser sichtbar zu machen und verschaffen gleichzeitig den SOC-Einheiten ein besseres Verständnis über mögliche Angriffsziele und Gegenmassnahmen», ergänzt Stefan.

Woran man zudem denken sollte, sagt Swantje, ist das Durchhaltevermögen:

«Security ist von Natur aus eine heikle Disziplin, die viele immer noch als lästig empfinden. Die Menschen gehen lieber davon aus, dass die vorhandenen Firewalls ihre Netzwerke ausreichend schützen, als dass sie sich mit der Komplexität von Themen wie Remotewartung- und Access-Controls beschäftigen.»

Um dem entgegenzutreten, brauchen angehende OT-Security Spezialisten die unerschütterliche Überzeugung, dass die Arbeit, die sie leisten, entscheidend ist, um uns auf den richtigen Weg in eine sichere Zukunft zu bringen.

Wie Peter Kosel, Gründer und Talent Community Manager der cyberunity AG, abschliessend betont: «Das Thema OT-Sicherheit ist allgegenwärtig und es betrifft praktisch jeden. Ob die Digitalisierung der OT als fataler Fauxpas der Menschheit oder als eine ihrer fruchtbarsten Innovationen in die Geschichte eingeht, wird unter anderem davon abhängen, ob Unternehmen sich vorausschauend mit dem Thema beschäftigen und Talentpools aus diversen OT-Spezialisten aufbauen. Gehen die Unternehmen das Thema OT-Security und die dafür notwendige Gewinnung von Spezialisten erst dann an, wenn die Operational IT angegriffen und grössere Schäden verursacht wurden, dann werden sie grosse Mühe haben, die richtigen Persönlichkeiten kurzfristig für sich zu gewinnen.»

Peter hebt hervor, wie entscheidend es für den nachhaltigen Unternehmenserfolg in Zukunft sein wird vom herkömmlichen Rekrutierungsprozess abzuweichen, der erst dann startet wenn eine Stelle dringend besetzt werden muss. Der KNOW YOUR TALENTS-Ansatz beginnt schon weit vor der Entstehung einer Vakanz und setzt auf lebendige Beziehungen zu den zukünftigen Leistungsträgern, um sie im Bedarfsfall unkompliziert kontaktieren und gewinnen zu können.

Wer sich für ein **OT Security Training and Exercises** des ICBC interessiert, findet weitere Informationen unter folgendem **Link**: https://icbc.uniss.org