CYBERSICHERHEIT FÜR OT & KRITISCHE INFRASTRUKTUREN

Die Digitalisierung durchdringt Wirtschaft und Gesellschaft – und auch Bereiche wie OT. Physische Safety und Cybersicherheit sind zentrale Aspekte. Cyberabwehr hat daher auch in OT-Umgebungen hohe Priorität.

→ **VON MARKUS LIMACHER**

OT- VS. IT-SICHERHEIT

Die OT-Welt wird zunehmend digitaler. Dabei treffen zwei Welten aufeinander: die Automatisierung (OT) und die Informationstechnologie (IT). Mit (I)IoT und Industrie 4.0 entstehen neue Sicherheitsrisiken, da nun technische Systeme angreifbar sind, die bislang nicht mit dem Internet verbunden waren. Fehlfunktionen oder Manipulationen könnten irreversible Schäden in der physischen Welt verursachen, die nicht einfach behoben werden können.

Die Vision ist eine umfassende Konnektivität und Nutzung des entstehenden Synergiepotentials – sei es im gesamten Netzwerk oder nur auf die Produktionssysteme eines Unternehmens bezogen. Die Realität bedeutet jedoch die Zusammenführung zweier komplexer Welten mit ebenso komplexen, teilweise veralteten oder fehlerbehafteten Schnittstellen. Während sich die IT auf Vertraulichkeit, Informationssicherheit und Datenschutz konzentriert, liegt der Fokus der OT auf der Verfügbarkeit der Maschinen und Anlagen sowie dem Schutz von Mitarbeitenden und der Umwelt. Die Gewährleistung der Safety ist in kritischen Umgebungen wie Kraftwerken, Stromversorgung oder Maschinensteuerung elementar.

Aufgrund der ursprünglichen Isolation der beiden Welten voneinander (keine Verbindung OT und IT oder nur isolierte Kommunikation und manuelle Schnittstellen) überrascht es nicht, dass die OT nach Etablierung von Produkttests, Konsumentenschutzmechanismen usw. über viele Jahre hinweg nicht nur wenig Schlagzeilen hinsichtlich Safety machte, sondern vor allem keine im Bereich der Security – mit Betonung auf «machte». Mit zunehmender Vernetzung der Umgebungen und der wachsenden Digitalisierung der Steuerung physischer Systeme durch komplexe Systeme wachsen die beiden Welten stärker zusammen und geraten damit ins Visier von Hackern.

STEIGENDE GEFAHR DURCH CYBERATTACKEN AUF OT

2022/23 fanden in verschiedenen europäischen Ländern gezielte Cyberangriffe auf kritische Infrastrukturen statt. Mehr als 20 Unternehmen, die Teile einer nationalen Energieinfrastruktur betreiben, wurden in koordinierten Aktionen angegriffen. Hierbei wurden betriebsführende OT-Komponenten kompromittiert. Ungewöhnlich war die Gründlichkeit der Angriffe. Die Angreifer hatten präzise Kenntnisse darüber, welche Unternehmen sie ins Visier nehmen würden. Es wird vermutet, dass staatliche Akteure beteiligt waren.

Vielfältige Bedrohungsszenarien sind im Energiesektor denkbar, wobei auch KI eine immer wichtigere Rolle spielen kann: schwerwiegende Angriffe auf SCADA-Systeme und Ransomware, verbesserte Erpressungstaktiken, Echtzeitdatenanalysen zur Erkennung und Manipulation kritischer Marktlagen im Stromhandel, das Erbeuten und Analysieren von Kunden-, Benutzer- und Log-Daten sowie täuschend echte Interaktionen, die Menschen zu negativen Handlungen verleiten. Solche und weitere Risiken erfordern eine umfassende Sicherheitsstrategie.

Berücksichtigt werden sollten unter anderem Supply-Chain-Bedrohungen aufgrund der Beschaffung unsicherer Komponenten und Dienstleistungen, insbesondere über Ländergrenzen hinweg. Gleichzeitig bedarf der unbefugte Fernzugriff auf dezentrale Komponenten wie Smart Meter besonderer Aufmerksamkeit. Die Nichteinhaltung von Sicherheitsstandards kann weiter rechtliche Konsequenzen haben und Angriffe wie beispielsweise auf die physische Regeltechnik können irreversible Schäden verursachen, was maximale Sicherheit und Redundanz erfordert. Angesichts der zunehmenden Angriffe auf OT-Umgebungen gibt es klare Empfehlungen für Betreiber kritischer Infrastrukturen:

- Exposition von Diensten: Die Sicherstellung, dass nur notwendige Dienste dem Internet ausgesetzt sind, insbesondere nach Sicherheitswarnungen wie bei VPN-Schwachstellen.
- Vulnerability Scans: Regelmässige Scans können Sicherheitslücken aufdecken und sicherstellen, dass Vereinbarungen mit Lieferanten eingehalten werden.
- Aktualisierung: Interne Prozesse zur zeitnahen Umsetzung von Sicherheitspatches (oder kompensierenden Massnahmen), basierend auf frühzeitigen Warnungen zu bekannten Schwachstellen, sind entscheidend.
- Geräteidentifikation: Die Identifikation aller Geräte im Netzwerk ist relevant, um Angriffspunkte zu minimieren.
- Event-Analyse: Die sorgfältige Sammlung und Analyse von Events und Logs auf Sektor- oder Branchenebene hilft, spezifische Angriffsmuster zu erkennen.
- Netzwerkeingaben kartieren: Alle Netzwerkeingaben zu den OT-Systemen müssen sorgfältig inventarisiert/kartiert werden, um unbekannte Angriffspunkte zu minimieren.
- Segmentierung: Netzwerke sollten so segmentiert sein, das Angriffe isoliert werden können, insbesondere gegenüber unbekannten Schwachstellen.
- Lieferantenmanagement: Eine klare Kommunikation und Vereinbarungen mit Lieferanten, vor allem bezüglich Sicherheitsupdates und der Zugänge, sind wichtig.
- Notfallplan: Ein gut durchdachter und getesteter Plan sowie Notfallverfahren sind unerlässlich, um auf Kompromittierungen effektiv zu reagieren und kritische Betriebsprozesse aufrechtzuerhalten.

OT-SICHERHEIT FÜR DIE GEWÄHRLEISTUNG DER SAFETY

Die Digitalisierung erfordert eine verstärkte Zusammenarbeit von IT und OT. Bei der Entwicklung oder der Integration neuer Maschinen oder Anlagen sollten Sicherheitsaspekte im Betriebs- und IT-Kontext vorab geklärt werden.

Dies unterscheidet sich deutlich von einer klassischen IT-Umgebung, da die Laufzeit oft über 20 Jahre beträgt, was die Aktualisierung von Firmware, Betriebssystem und APIs sowie den Einsatz von Sicherheitsmassnahmen erschwert.

Zunehmende Bedrohungen in OT und kritischen Infrastrukturen erfordern eine umfassende Sicherheitsstrategie. Die Zusammenarbeit mit Sicherheitsexperten, Regierungsbehörden und der Industrie ist entscheidend, um kritische Infrastrukturen vor komplexen Bedrohungen zu schützen. Eine systematische Cybersicherheit erfordert die Entwicklung von Richtlinien, Investitionen in Technologie, Schulungen der Mitarbeitenden, den Aufbau einer Cybersicherheitskultur, proaktive Massnahmen und kontinuierliche Anpassung an die Risikosituation. Auch der Zero-Trust-Ansatz kann im OT-Umfeld besonders effektiv sein.

Mehr denn je sollten Verantwortliche auf Führungsebene angemessene Budgets und Ressourcen bereitstellen, und die Wahrnehmung der Verantwortung des Managements bezüglich Cybersicherheit und Datenschutz sind entscheidend. Auch Crypto Agility sollte in den Fokus rücken, um langfristig auf Bedrohungen reagieren zu können. ←

Dieser Beitrag wurde von der **InfoGuard AG** zur Verfügung gestellt und stellt die Sicht des Unternehmens dar. Computerworld übernimmt für dessen Inhalt keine Verantwortung.

Zum Autor

Markus Limacher, Head of Security Consulting, ist seit 2013 bei der InfoGuard tätig und verfügt über 30 Jahre Erfahrung in der IT- und Cybersicherheit. Zu Limachers Schwerpunkten gehören die Erarbeitung von Cybersicherheitsstrategien, Sicherheits- und Risikoanalysen, der Aufbau und Betrieb von Informationssicherheits-Managementsystemen, die Durchführung von Tabletop Exercises sowie die umfassende Beratung von Kunden verschiedener Branchen.

Über InfoGuard:
Die InfoGuard AG, mit Hauptsitz in Baar/Zug sowie Niederlassungen in Bern, München und Wien, ist spezialisiert auf umfassende Cyber Security. Ihre 360°-Expertise reicht von Cyber Defence Services und Incident Response Services über Managed Security & Network Solutions bis hin zu Penetration Testing & Red Teaming sowie Security Consulting Services.

Mehr Informationen:
www.infoguard.ch

infoGuard
SWISS CYBER SECURITY

Cybersicherheit ist zentral - auch in OT-Umgebungen.

Bild: kan77/123RF.com