satw

Smart Things | Internet der Dinge

Cybersecurity – Herausforderungen für die politische Schweiz

Stand der Dinge

Das Internet der Dinge (Internet of Things, IoT) kann als intelligente Vernetzung einer globalen Infrastruktur verschiedenster «Smart Things» mit Funktionen aller Art (z.B. Temperatursensoren, Autos, Lautsprecher, Maschinen, etc.) verstanden werden. Durch die intelligente Vernetzung ist eine neue Verknüpfung von physischen und virtuellen Ressourcen mit gemeinsamen Interaktionen möglich. Die daraus entstehenden Möglichkeiten erlauben darüber hinaus auch automatisierte Aktionen auszuführen, Informationen zusammenzutragen und weiter zu verwerten.

Die Begriffe Industrie 4.0 und Operational Technology (OT) vereinen die vierte industrielle Revolution mit dem Einsatz neuer Technologien und technischen Möglichkeiten. «Industrie 4.0»[1] gilt dabei als Oberbegriff der neuen industriellen Welt, in der Maschinen untereinander verbunden und mit modernen Informations- und Kommunikationstechnologien (IKT) vernetzt sind.

Mit der Digitalisierung vernetzen sich die unterschiedlichen Welten und Architekturen der klassischen Geschäfts-IT (Information Technology) und OT zunehmend. Während die klassische IT der Informationsverarbeitung dient, werden mit der OT physische Prozesse in der industriellen Herstellung und Logistik gesteuert. In dieser Verbindung der hochkritischen OT-Systeme (z.B. Atomkraftwerke) mit IT-Systemen, die dem Internet ausgesetzt sind, entstehen neue Schadenspotentiale und Risiken.

Empfehlungen

1. Eine Übersicht der aktuellen Lage und der zukünftigen Entwicklungen im IoT-Bereich erstellen und bekannt machen, welche Best Practices bestehen (allenfalls gibt es bestehende Standards und Frameworks).
2. Eine vertiefte Forschung bzgl. IoT/OT-Security ist voranzutreiben, damit die Security mittels neuer Konzepte und Architekturen in der sehr heterogenen Umgebung auch in Zukunft gewährleistet werden kann.
3. Minimalstandards in den Bereichen IoT/OT erstellen und normieren sowie mittels entsprechender Regulationen zwingend umsetzen. Eine Zusammenarbeit mit den entsprechenden Stellen in der EU würde eine grössere Wirkung erzielen.

Deren Beherrschung und Bewältigung ist mit grossen Herausforderungen verbunden und verlangt nach neuen Konzepten.

Die neuen Technologien und die umfassende Vernetzung von OT und IT führen in Wirtschaft, Verwaltung und Gesellschaft zu grossen Entwicklungsschritten, neuen Anwendungsmöglichkeiten und innovativen Geschäftsmodellen, sofern wir die damit verbundenen Risiken angemessen und systematisch managen.

[1] Der Begriff «Industrie 4.0» adressiert weit mehr IT/OT-Technologie und bezieht sich vor allem auf neue Gesamtkonzepte wie z.B. «Smart Factory» mit umfassender Vernetzung der Systeme und Sensoren sowie Optimierung auf Basis umfassender Daten oder «Predictive Maintenance» als weiterem Themenkreis.

Herausforderungen

Es ist allgemein bekannt, dass der Einsatz neuer Technologien spezifische Risiken hervorbringt. Die flächendeckende Vernetzung von physischen und virtuellen «Smart Things» erhöht die Sicherheitsrisiken und das mögliche Schadensausmass infolge der deutlich grösseren Angriffsfläche und der steigenden Wichtigkeit von OT und IT für die Wertschöpfung. Ein erfolgreicher Angriff auf ein IoT-Gerät kann direkten Einfluss auf die reale/physische Umgebung haben und so etwa zu einem Stromausfall führen, einen Herzschrittmacher funktionsunfähig machen oder Industrieanlagen beschädigen. Diese Entwicklung führt zu höheren Anforderungen an die Sicherheit, z.B. in Form von sicherer Datenkommunikation und -speicherung. Die erhöhten Sicherheitsanforderungen werden heute oft nicht erkannt oder bewusst nicht berücksichtigt (z.B. bei IoT für die Privatanwendung) um möglichst schnell mit einem günstigen und pseudo-innovativen «Smart Thing» am Markt zu sein. Dieser Umstand bedeutet meistens, dass die Sicherheit der Geräte und die Privatsphäre der Benutzer nicht genügend gewährleistet werden können. Im Bereich der Consumer IoT (Produkte für Privatanwendung), ist bezüglich eines genügenden Sicherheitsstandards Marktversagen festzustellen.

Es muss ebenfalls beachtet werden, dass speziell im Industrieumfeld der Fokus klar auf «Safety» (z.B. Unfallvermeidung) und nicht primär auf «Security» (z.B. Schutzmassnahmen vor Angriffen) gelegt wird[2]. Des Weiteren ist speziell im OT-Bereich die Lebenszeit der verwendeten Geräte auf mehrere Jahrzehnte ausgelegt, da sie oft in harten Umgebungen hohen physikalischen Belastungen ausgesetzt sind. Im Vergleich dazu werden andere «Smart Things» je nachdem schon nach ein paar Monaten erneuert (z.B. Smart Tags). Dieses sehr grosse Spektrum an Anforderungen und Rahmenbedingungen gilt es zu berücksichtigen, um in jedem Fall genügend sichere Gesamtsysteme entwickeln und integrieren zu können.

Die heutige Praxis zeigt, dass in der Entwicklung von IoT- und OT-Systemen gängige und bekannte Konzepte (z.B. Security/Privacy by Design) und Standards (z.B. EN IEC 62443) nicht konsequent angewendet werden bzw. noch gar nicht existieren.

Die Prüfung und Zertifizierung von IT-Komponenten und -Systemen wird aktuell sowohl in der Schweiz als auch auf EU-Ebene diskutiert. In der EU wird im Rahmen des Cybersecurity Act über eine gesetzliche Regelung zur Cybersicherheitsprüfung debattiert. Die Diskussionen in der Schweiz drehen sich um ein Konzept zum Aufbau eines Prüfinstituts für vernetzte Geräte unter dem Gesichtspunkt der Cybersicherheit. Die Initiativen möchten erreichen, dass die Sicherheit und Integrität von digitalen Produkten verbindlich geregelt werden. Solche Qualitätsprüfungen durch unabhängige Stellen sind in anderen kritischen Industriesektoren wie der Medizintechnik bereits seit längerem fester Bestandteil der Produktzulassung.

[2] Safety: Geschütztsein vor unabsichtlichen Gefährdungen, also beispielsweise Hochwasser oder Unfällen, *Security*: Geschütztsein vor böswilligen Aktionen, also absichtlich von Menschen herbeigeführten Bedrohungen, einem Raubüberfall etwa oder einem Cyberangriff. https://www.endpointprotector.de/blog/was-den-unterschied-zwischen-safety-und-security-ausmacht/

Handlungsbedarf

Wie eingangs erwähnt, kann die IoT-Welt grob in zwei Bereiche unterteilt werden:

- Vernetzung aller möglicher «Smart Things» mit Funktionen aller Art
- Operational Technology (OT) / Industrie 4.0

Aufgrund der Aufteilung der genannten Bereiche ergibt sich jeweils ein anderer Handlungsbedarf pro Kategorie. Durch das mangelnde Sicherheitsbewusstsein mancher Hersteller von «Smart Things» wie auch die teilweise blauäugige Verwendung der Benutzer, ist es notwendig, diese zwei Themen mittels den folgenden Handlungsfeldern zu adressieren:

Smart Things

- Internationale Standardisierung und entsprechende Geräte-Zertifizierungen vor allem im Bereich der Sicherheit anwenden, um Transparenz (welcher Hersteller ist zertifiziert) und Sicherheit (z.B. Security/Privacy by Design) zu erhöhen. Darauf basierend eine Regulierung vorsehen, um ein genügendes Sicherheitsniveau zu erzwingen. Diese muss in mindestens einem grossen Wirtschaftsraum flächendeckend umgesetzt werden (z.B. EU), um damit eine Wirkung bei den grossen Herstellern zu erzielen.
- Das aktuell in der Schweiz diskutierte Konzept zum Aufbau eines nationalen Prüfinstituts für vernetzte Geräte unter dem Gesichtspunkt der Cybersicherheit unterstützen und nach Möglichkeiten vorantreiben.
- User-Awareness-Initiativen weiterverfolgen, um das Sicherheitsbewusstsein stetig zu erhöhen.
- Forschung im Bereich IoT/OT-Security, insbesondere bezüglich der Konzepte und Architekturen, um die Sicherheit über sehr lange Nutzungszeiträume zu gewährleisten (z.B. bei 30 Jahren Lebensdauer).

OT/Industrie 4.0

- Die zunehmende Vernetzung im OT-Bereich stellt jeden wirtschaftlichen Sektor vor Herausforderungen, da es hierbei nicht nur um die Integration neuer Systeme geht, sondern auch um die Vernetzung bestehender (alter) Systeme. Durch die hohe Diversität der zu vernetzenden Systeme, welche auch grundlegend andere Anforderungen an Safety, Verfügbarkeit und Lebensdauer haben, sind passende und umsetzbare End-to-End Security-Architekturen (z.B. Zero-Trust-Konzept[3], Micro-Segmentierung) unumgänglich. Um zusätzlich eine mögliche Verbreitung einer sogenannten Shadow-IT zu verhindern, sind die bestehenden IT-Prozesse und -Schnittstellen entsprechend anzupassen.

[3]Das Zero-Trust-Konzept definiert, das alle Verbindungen und Benutzer jederzeit überprüft werden müssen, unabhängig ob diese intern oder extern sind. Ein alleiniger Schutz von dem Netzwerkperimeter ist nicht mehr ausreichend. “Vertraue niemanden, prüfe alles”. Siehe auch Kolumne inside-IT von Roger Halbheer: https://www.inside-it.ch/de/post/satw-insights-zero-trust-sicherheit-in-zeiten-von-homeoffice-20200527

Referenzen

EN IEC 62443 - Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme ISA standards: https://www.isa.org/intech/201810standards/

SATW-Blog: Die Sicherheit vernetzter Geräte prüfen: https://www.satw.ch/de/cybersecurity/die-sicherheit-vernetzter-geraete-pruefen/

Kontakt

Nicole Wettstein
Leiterin Schwerpunktprogramm Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-herausforderungen

Impressum
Schweizerische Akademie der Technischen Wissenschaften SATW
Expertenbeiträge
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Redaktion und Grafik
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
September 2020