Sicherheit in einer vernetzten Produktion?!

Studie der Fachhochschule der Wirtschaft (FHDW)
Autoren: Prof. Dr. E. Koch und Prof. Dr. W. Nüßer
Stand: 15.09.2017

Inhaltsverzeichnis

Einleitung

In der IT-Sicherheitsforschung ist es üblich, die Sicherheit eines IT-Systems über ein Geflecht von Begriffen zu definieren. Eine etablierte Definition bezeichnet **Sicherheit** als die Eigenschaft eines Systems, die dadurch gekennzeichnet ist, dass die als bedeutsam angesehenen ***Bedrohungen***, die sich gegen die ***schützenswerten Güter*** richten, durch besondere ***Maßnahmen*** soweit

ausgeschlossen sind, dass das verbleibende ***Risiko*** akzeptiert wird (E. Amann, 1992). Dabei soll das Risiko verstanden werden als monotone Funktion der Eintrittswahrscheinlichkeit der Bedrohung und der Auswirkungen der Bedrohung.

Dieser Begriff der Sicherheit ist im Deutschen leider mehrdeutig. Er umfasst sowohl die Funktionssicherheit (engl. Safety), die den Schutz der Umwelt vor dem System untersucht, und die Informationssicherheit (engl. Security), die die Richtung umkehrt und den Schutz des Systems vor Einflüssen aus der Umgebung zum Thema hat.

Die IT-Branche hat seit vielen Jahren v.a. Erfahrungen mit den Bedrohungen der Güter aus der Security-Auffassung. Dazu zählen Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität, Datenschutz etc., die durch Angriffe von Hackern, kriminellen Organisationen oder gar regierungsnahen Einrichtungen beeinträchtigt werden. Die Maßnahmen, die getroffen wurden, um diesen Bedrohungen Herr zu werden, sind wohl bekannt. Hierzu zählen

- Firewalls
- Public-Key-Infrastrukturen
- Intrusion Detection und Prevention Systeme
- Virenschützer
- Etc.

Trotz dieser vielen Maßnahmen und einer ganzen IT-Sicherheits-Industrie kann jedoch nicht behauptet werden, dass es um die Sicherheit der Computer und der Daten blendend steht.

In dieses Umfeld treten nun die Initiativen und Konzepte des Internet of Things, der Cyber-Physical Systems und als spezielle, aber für Deutschland besonders wichtige Anwendung die Industrie 4.0 Initiative der Bundesregierung (BMBF, 2017). All diesen Ansätzen liegt die Annahme zugrunde, dass auch technische Systeme, die bislang nicht Teil des Internets waren, nunmehr auch in diese Kommunikation einbezogen werden. Die Vision ist die einer umfassenden Konnektivität – sei es nun im gesamten Internet oder nur bezogen auf die Produktionssysteme eines Unternehmens.

Offensichtlich stellt sich damit zumindest die Frage, welche Auswirkungen solch eine steigende Vernetzung hinsichtlich der Sicherheit dieser Systeme besitzt, wenn schon die bisherige IT-Landschaft alles andere als ein sicherer Ort zu sein scheint.

In den folgenden Abschnitten geben wir die – anonymisierten – Ergebnisse einer Studie wieder, die die Fachhochschule der Wirtschaft (FHDW) in Zusammenarbeit mit der Beratungsfirma rt-solutions.de GmbH aus Köln unter ihren Partnerunternehmen durchgeführt hat. Obwohl z.B. das BSI regelmäßig Studien zur Lage der IT-Sicherheit in Deutschland durchführt und auch der VDMA hierzu qualitativ hochwertige Aussagen macht (VDMA, 2016) (BSI, 2017), erschien uns solch eine Studie doch aus einigen Gründen sinnvoll. Zum einen erfassen selbst die großen Studien des BSI nur vergleichsweise wenig produzierende Unternehmen, die aber gerade am Stammsitz der FHDW in Ostwestfalen (OWL) (Paderborn) eine hohe Bedeutung haben. Damit eng verbunden ist der zweite Grund: eine regionale Aussage gerade für eine so wirtschaftsstarke und im Bereich der Industrie 4.0 unter anderem aufgrund des Spitzencluster it's OWL (www.its-owl.de) führende Region wie NRW war nur schwer zu erkennen. Drittens konzentrieren sich die meisten der

vorhandenen Studien nicht auf die Schnittstelle von Industrie 4.0 und Sicherheit, sondern behandeln dies nur als Teilgebiet.

Dass eine solche Studie durchaus einen wichtigen und offenen Punkt adressiert, zeigt die Tatsache, dass die Ergebnisse im September 2017 auf der internationalen Konferenz ETFA der IEEE veröffentlicht wurden.

In den folgenden Abschnitten beschreiben wir zunächst die klassische IT und dann die Operational Technology (OT), die im Produktionsbereich vorherrscht. Wir gehen dabei auch auf die Unterschiede in den vier Dimensionen Güter, Bedrohungen, Maßnahmen und Risiko gemäß der oben gewählten Definition der Sicherheit ein.

Industrie 4.0 und Security

Die klassische Information Technology (IT) ist gekennzeichnet durch eine Vielzahl unterschiedlicher Teilnehmer. Sowohl die Anzahl der Teilnehmer in den typischen Netzwerken ist gewaltig als auch die Diversität der Systeme, die über Standard-Protokolle wie IP und TCP/UDP miteinander verknüpft werden. Das reicht von großen Server-Systemen, über Desktops und Smartphones bis hin zu Mikro-Systemen wie RaspPis und embedded systems. Es entstehen damit Netzwerke mit einer hoch-dynamischen und komplexen Topologie, bei der zudem die Konfigurationen der Teilnehmer sich nahezu beliebig ändern können.

Die Sicherheitslage in dieser Welt ist bekanntermaßen oftmals bedenklich. Deshalb werden seit vielen Jahren vielfältige Werkzeuge zur Absicherung der Netzwerke eingesetzt. Nichtsdestotrotz steigt die Bedrohungslage eher, wie einige wenige Zahlen des BSI belegen mögen:

- Die Anzahl der erfolgreichen Angriffe stieg um 8% von 2014 auf 2015.
- Die Anzahl der erfolgreich angegriffenen Institutionen wuchs um 13,4% von 2014 auf 2015.
- Täglich entstehen ca. 380.00 neue Varianten von Schadsoftware.

Viele Beispiele für Angriffe oder Sicherheitslücken haben es in den letzten Jahren in die Presse geschafft. Der Heartbleed-Bug ist ein Beispiel, die Probleme des Dienstleisters Cloudflare mit unkontrollierten Memory Dumps, die Hacks von Chrysler oder die massiven DDos mit Tb/s Datenraten sind andere (Heise, 2016).

Dieser oftmals eher chaotisch wirkenden Welt der IT steht die meist deutlich statischere und geordnetere Welt der Steuerung von Maschinen, Produktionsanlagen und kritischen Infrastrukturen entgehen. Diese Operational Technology (OT) zeichnet sich durch fundamental andere Anforderungen und Eigenschaften als die IT aus. Zunächst macht es der Einsatz in kritischen Umgebungen, wie Kraftwerken, Stromversorgung oder Maschinensteuerung notwendig, dass die Safety eine dominante Rolle spielt. Zahlreiche Standards erzwingen eine hohe Schutzstufe, da die Auswirkungen bei einem fehlerhaften Verhalten z.B. aufgrund eines Cyber-Angriffs sehr gefährlich werden können. Störungen beispielsweise in der Energieversorgung können Menschenleben gefährden, sabotierte Maschinen in der Produktion sowohl Mitarbeiter im

Unternehmen als auch Nutzer der Produkte.

Auf der anderen Seite sind in der OT die Netzwerke deutlich strenger definiert, besitzen eine meist einfache Topologie und Teilnehmer, deren Konfigurationen sich ebenfalls selten verändern. Die Lebensdauer der typischen Investitionsgüter, die in der OT zum Einsatz kommen, beträgt ein Vielfaches der Lebensdauer der Consumer-Produkte, die heute das Internet dominieren. Hinzu kommt, dass über lange Jahre hinweg meist proprietäre Netzwerk-Protokolle von Siemens, Schneider, Rockwell etc. im Bereich der OT eingesetzt wurde. Aufgrund dieser weitgehenden Isolation verwundert es also nicht, dass die OT über lange Jahre hinweg nicht nur wenig Schlagzeilen hinsichtlich Safety, sondern auch im Bereich der Security machte.

Diese Unterschiede zwischen IT und OT sind in Tabelle 1 zusammengefasst.

	Klassische IT	**Control Systems (ICS, OT)**
Arbeitsumgebung	Unkritisch	Rau, Compliance wichtig
Security	hoch	niedrig
Safety	niedrig	hoch
Performance	Ziel: schnell	Ziel: Real-Time
Verfügbarkeit	Ausfälle akzeptabel	Ausfälle intolerabel
Vertraulichkeit	wichtig	oft irrelevant
Lifecycle	< 3 – 5 Jahre	> 20 Jahre
Updates	häufig, automatisiert	selten
Security-Tools (AV, FW, ...)	üblich	selten
Betrieb	ggf. mittels Outsourcing	meist im Haus

Tabelle 1: Vergleich der Eigenschaften von IT und OT

Diese Aufstellung zeigt bereits, dass IT und OT hinsichtlich ihrer Sicherheitsanforderungen sehr unterschiedlich sind. Die Tabelle 2 geht auf diese Unterschiede noch etwas genauer ein. Dabei

zeigt sie zwei unterschiedliche Anwendungsfälle der klassischen IT auf (Mail und vertrauliches Gespräch), die trotz ihrer Unterschiedlichkeit im Vergleich zur OT deutlich abzugrenzen sind.

		IT		OT
		Mail/Transaktion	**Vertrauliches Gespräch**	**Maschinen-Kontrolle**
Güter	**Menschenleben, physische Güter**	nicht direkt	nicht direkt	**wichtig**
	Vertraulichkeit	wichtig	wichtig	**irrelevant**
	Verfügbarkeit	sinnvoll	sinnvoll	**wichtig**
	Integrität	wichtig	wichtig	sinnvoll
	Authentizität	wichtig	wichtig	wichtig
	Nicht-Abstreitbarkeit	wichtig	auf keinen Fall	irrelevant
Güter	**Überprüfbarkeit**	wichtig	auf keinen Fall	irrelevant
	Forward Secrecy	evtl. wichtig	auf keinen Fall	irrelevant
Bedrohungen		sehr hoch	hoch	**bislang gering**
Maßnahmen (AV, FW…)		üblich	üblich	**selten**
Risiko		hoch	hoch	**sehr hoch**

Tabelle 2: Unterschiedliche Sicherheitsanforderungen von IT und OT

Ein besonderes Augenmerk ist dabei auch auf die möglichen Abwehrmaßnahmen zu richten. In der IT etablierte Verfahren, wie Firewalls, Virenscanner oder TLS-verschlüsselte Netzwerk-Protokolle sind oft für den Einsatz in OT-Netzwerken nicht geeignet. Solche Tools machen zum einen die Zertifizierung mancher OT-Komponenten hinfällig, da sie einen Eingriff in diese Komponenten darstellen, und haben zum anderen oftmals eine Verlangsamung von Abläufen in

der Steuerungssoftware zur Folge, die nicht akzeptabel ist. Einen Schutz vor physischen Angriffen, der in der Produktion durchaus möglich erscheint, bieten diese Werkzeuge zudem auch nicht.

Zusammenfassend kann also gesagt werden, dass bislang IT und OT getrennte Welten bilden mit unterschiedlichen Technologien, Strukturen, Gütern, Bedrohungen, Maßnahmen und Risiken (s. Abbildung 1).

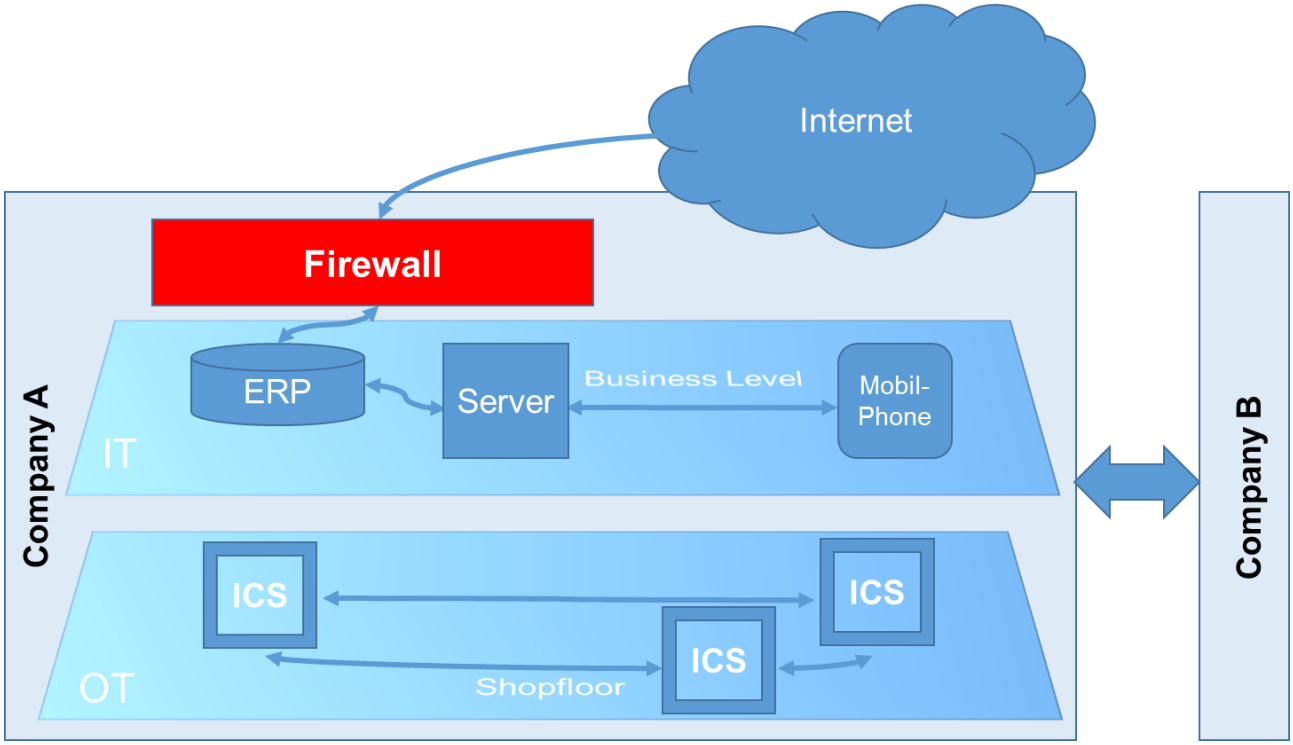

Abbildung 1: Bisherige Gestalt typischer Netzwerke: IT und OT sind getrennt

Eine Vielzahl von Studien von Gartner (2011), IHS (2015), VDMA, acatech etc. deuten nun aber darauf hin, dass die beiden Welten konvergieren. Die Technologien des Internets, wie Ethernet und IPv6, werden zusehends auch im Bereich der OT eingesetzt. Produkte von Siemens (Scalance), Beckhoff (EtherCAT), ABB etc. sind hierfür hervorragende Beispiele. Diese Entwicklung wird zum einen gefördert durch die Verfügbarkeit von hoher Rechenleistung selbst bei kleinsten Systemen (RaspPi) und zum anderen durch die oben genannten Trends und Initiativen wie IoT, CPS und Industrie 4.0: wenn eine durchgängige Vernetzung mit dem Internet gewünscht ist, liegt es nahe, die Internet-Technologien zu verwenden.

Aus Sicht der Unternehmen bietet diese Integration aller Systeme durchaus erhebliche Nutzenpotentiale. So kann zum einen eine konsistente, gemeinsame Sicht auf alle Daten des Unternehmens gewonnen werden. Wenn diese Daten zudem noch in nahezu Echtzeit analysiert und aufbereitet werden können, entstehen neuartige Möglichkeiten zur Steuerung der Unternehmensprozesse. Ansätze wie Predictive Maintenance sind nur ein Beispiel für die Optimierungsmöglichkeiten, die durch solche Datenverfügbarkeit entstehen. Auf der Basis solcher Funktionen kann weiterhin die Produktion flexibilisiert (Losgröße 1), die Erfüllung (gesetzlicher, …) Auflagen erleichtert und eine Kostenreduktion ermöglicht werden.

Insgesamt entsteht so eine Vernetzung, die nicht nur – wie in Abbildung 1 gezeigt – horizontale Kommunikationen erlaubt, sondern eine Aufweitung der Kommunikationsstrukturen auf vertikalen und unternehmens-übergreifenden Datenaustausch (Abbildung 2).

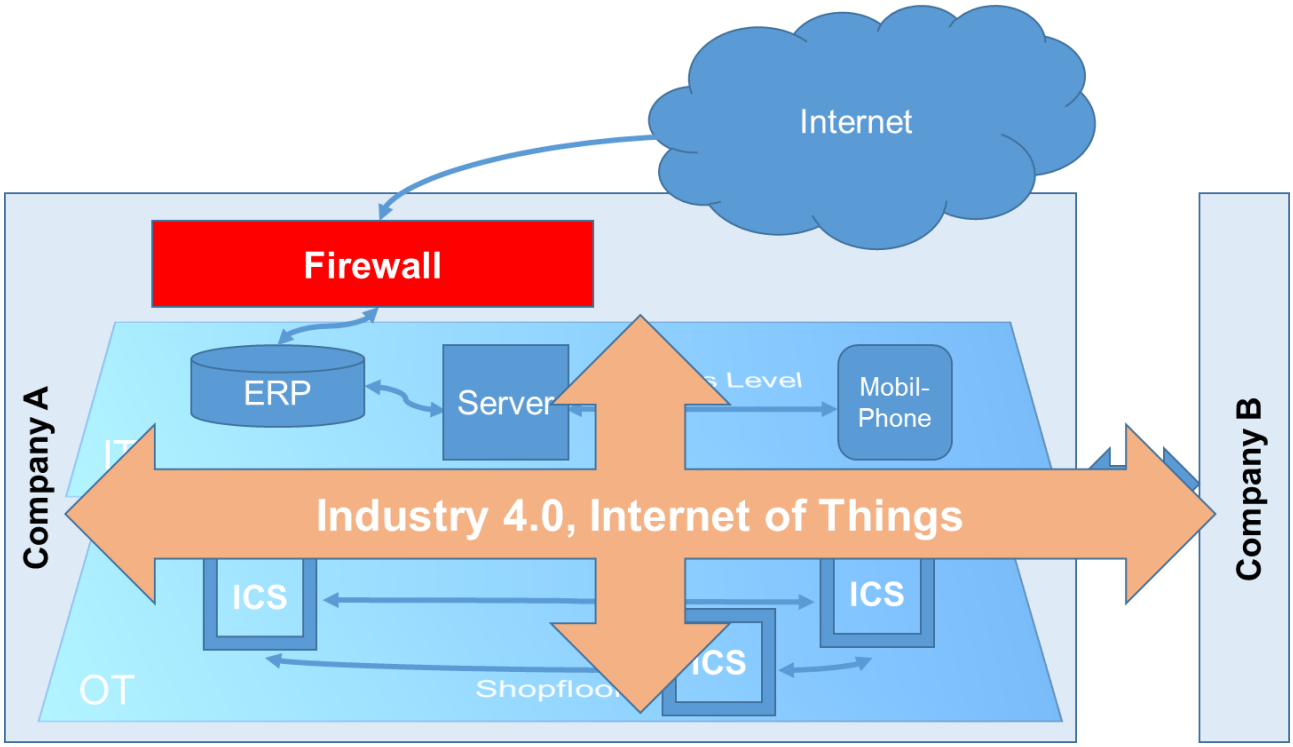

Abbildung 2: Vernetzung von IT und OT

Aus Sicht der Sicherheit hat diese Konvergenz nun beträchtliche Konsequenzen. Abbildung 3 zeigt, dass die Auswirkungen sowohl aus der IT kommend die OT betreffen als auch die umgekehrte Richtung möglich ist, in der Geräte der OT oder allgemeiner des IoT als Plattform für Angriffe auf die IT dienen können.

In der erst-genannten Richtung stellt das Internet mit seinem ungelösten Sicherheitsproblem eine besondere Bedrohung für die OT dar. Wie oben gezeigt, sind die typischen Systeme der OT nicht von Hause aus auf Security getrimmt. So gibt es in der IT-Szene das Bonmot, dass die Industrial Control Systems (ICS) „insecure by design“ seien. Tatsächlich sind viele Systeme in der OT im Einsatz, die weder Authentifizierung noch abgesicherte Protokolle verwenden. Sobald ein Angreifer die bekannten Sicherheitssysteme der IT überwunden hat, liegt die OT weitgehend offen und ungeschützt vor ihm. Andere Eigenschaften der ICS werden in den weiter unten genannten Ergebnissen unserer Studie beleuchtet. Dabei bietet die OT mit ihrem Kontakt zu physischen Objekten den Angreifern vielfache und neuartige Angriffsformen. Das Ausschalten des Stroms ist z.B. in der IT wenig spannend, da dadurch der Angriff sofort erkannt und unterbunden wird. In der OT kann dies allerdings verheerende Folgen haben. Das BSI berichtet, dass im Jahr 2014 ein Hochofen in Deutschland auf diese Weise lahmgelegt wurde – zum Glück ohne Folgen für Menschen, aber mit erheblichen Kosten (BSI, 2017). Die oftmals deutlich größeren Konsequenzen, die mit einem Angriff auf die OT verbunden sind, machen diese Systeme in den Augen vieler Angreifer zu einem besonders interessanten Ziel.

Aus Sicht der Betroffenen sind aber mitunter die unscheinbareren Angriffe mindestens ebenso bedrohlich. Eine nicht direkt erkannte Veränderung an Parametern von Produktionsmaschinen, z.B. die millimeterweise Verschiebung von Schweißnähten, kann ganze Produktchargen unbrauchbar machen. Schon kleinere Abweichungen in der zeitlichen Abfolge von Produktionsschritten verzögert unter Umständen die gesamte Produktion beträchtlich. Reparaturen sind schließlich meist nicht wie in der IT üblich mit einem Neustart des Systems getan.

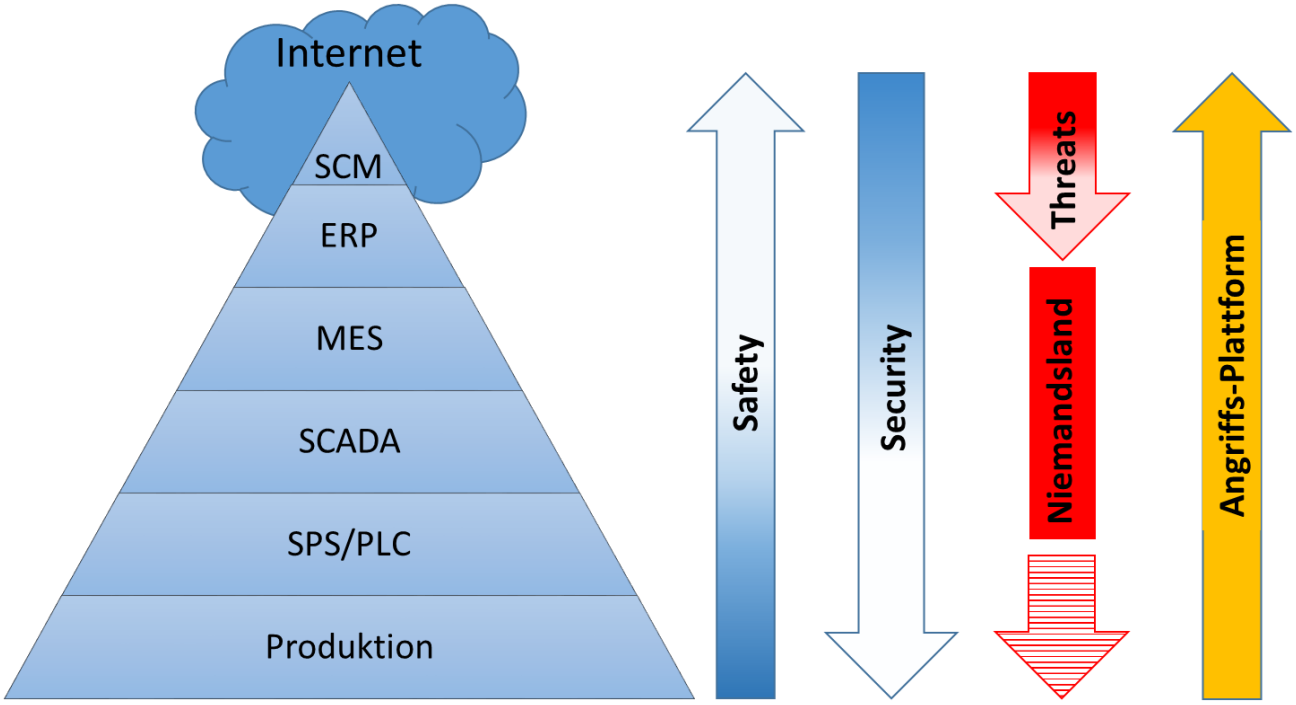

Abbildung 3: Sicherheitslage nach IT/OT-Konvergenz (ergänzt nach TrendMicro)

Aber auch die umgekehrte Richtung gewinnt in den letzten Monaten an Bedeutung. Die Geräte des OT/IoT stellen zunehmend Angriffskapazitäten zur Verfügung für Angriffe auf die IT-Systeme. Da die Geräte des IoT meist ungehärtet sind, stellen sie für Botnet-Bauer, wie Mirai, ein leichtes Ziel dar. Der größte bislang jemals gesehene DDoS-Angriff von ca. 1,1 TBit/s wurde vermutlich von einem solchen IoT-Botnet aus durchgeführt (Heise, 2016).

Insgesamt darf es also nicht verwundern, dass die Frage nach der Sicherheit im Sinne von Security gerade für den OT-Bereich eine hohe Aufmerksamkeit gewonnen hat. Die Empfehlungen des VDMA sind hierfür ein gutes Beispiel (VDMA, 2016). Doch wie steht es wirklich um die Sicherheit in der OT in den deutschen Unternehmen gerade des produzierenden Mittelstands? Wo sind die größten Mängel und wo Potentiale für eine effiziente Erhöhung der Sicherheit? Diese Fragen untersucht die Studie, deren wichtigste Ergebnisse nun genauer vorgestellt werden.

Ergebnisse der Studie

Die Studie wurde primär unter den Partnerunternehmen der FHDW durchgeführt. Aufgrund der Struktur der FHDW kamen die meisten der 30 Rückläufer aus NRW und dort v.a. aus OWL. Schwerpunkt war dabei der produzierende größere Mittelstand und einige Konzerne. Die Datenlage erlaubt sicher keine statistisch signifikanten Aussagen über eine größere Grundgesamtheit, doch gibt sie mit hoher Wahrscheinlichkeit ein qualitativ stimmiges Bild für die oben genannte Gesamtheit an. Die Grundtendenz der Ergebnisse passt sehr gut zu den Ergebnissen des BSI, geht aber an einige Stellen deutlicher und tiefer auf die Industrie 4.0 und OT-Probleme ein. Die wichtigsten Erfahrungen werden im Folgenden genauer vorgestellt und bei Bedarf durch Ergebnisse anderer Studien erweitert.

Das Sicherheitsrisiko für die OT steigt

Wie in der Einleitung beschrieben kann das Risiko im einfachsten Fall als Produkt aus Eintrittswahrscheinlichkeit und Ausmaß der Auswirkungen eines Gefährdungsfalls verstanden werden. Im vorherigen Abschnitt wurde bereits gezeigt, dass die Auswirkungen bei Angriffen auf OT-Systeme in der Regel sehr hoch sind. In den Ergebnissen der Studie sehen wir nun, dass auch die Eintrittswahrscheinlichkeit für solche Ereignisse steigt. Dies legen drei Resultate nahe:

1. Ca. 42% der befragten Unternehmen geben an, dass der Anteil der (vernetzten) ICS in ihren Unternehmen steigen wird.
2. In ca. 20% der Unternehmen werden heute IT und ICS in einem physischen Netz betrieben.
3. Die Angriffe auf ICS nehmen insgesamt zu, wie Tabelle 3 zeigt.

Damit vergrößert sich nicht nur die Angriffsfläche durch die steigende Anzahl von ICS (interner Effekt), sondern auch die externe Bedrohungslage verschärft sich. Bekannte Beispiele sind der oben genannte Angriff auf einen Hochofen, die Dragonfly-Attacke of Energieversorgen im Jahr 2013, der großflächige Ausfall der ukrainischen Stromversorgung im Jahr 2015, die Ausfälle in Stahlwerken in Brasilien 2010 und in einer Keksfabrik in Kanada 2015. Der letzt-genannte Fall verdeutlicht auf eine nur vordergründig erheiternde Weise, welche Konsequenzen ein Angriff auf ICS haben kann: der Keksteig konnte aufgrund des Ausfalls der Produktion nicht weiterverarbeitet werden und härtete in den Rohren aus. Die Anstrengungen, diese Verstopfungen zu beseitigen, waren zeitlich und finanziell beträchtlich.

Faktum	Wert	Quelle
Erfolgreiche Angriffe insgesamt	+8 % (2014 □ 2015)	BSI
Erfolgreich angegriffene Institutionen	+13% (2014 □ 2015)	BSI
Angriffsrate der KMUs	61%	Bitkom
Angriffsrate der restl. Unternehmen	54%	Bitkom
Bekannte Angriffe auf OT/ICS	2012: 138 2015: 295	ICS-CERT

Tabelle 3: Angriffe auf ICS

Doch Tabelle 3 zeigt noch mehr. Gerade KMUs können sich nicht in Sicherheit wiegen. Sie werden statistisch gesehen häufiger angegriffen als andere Unternehmen in Deutschland.

Insgesamt gesehen, erhöht also die Proliferation von ICS in Unternehmen die Gefährdungslage – eine ernüchternde Feststellung, wenn man bedankt, dass 60% der Unternehmen in ICS investieren, um eine gesteigerte Sicherheit in der Prozessführung zu erlangen.

Aktueller Zustand des OT-Netzes meist unbekannt

Nehmen wir nun einmal an, dass Angreifer sich ein konkretes OT-Netzwerk ausgesucht haben. Sind die Unternehmen heute in der Lage, solch einen Angriff zu erkennen? Im Bereich der IT haben die Erfahrungen der letzten Jahre gezeigt, dass gerade die langanhaltenden, unbemerkten und damit professionellen Angriffe (APTs = advanced persistent threats) eine der größten Gefahren darstellen.

Im Umfeld der OT zeigt sich hier eine beträchtliche Lücke:

- Weniger als 40% der Unternehmen verfügen über ein aktuelles Inventar der Systeme in ihrem OT-Netzwerk. In vielen Unternehmen geschieht die Aufnahme des Inventars noch manuell und ist damit fehleranfällig und statisch.
- Weniger als 25% der Unternehmen beobachten das OT-Netzwerk automatisiert (Monitoring).
- Es fand sich kein Unternehmen, dass automatisch eine Anomalie-Erkennung in Art eines IDS für das OT-Netzwerk einsetzt.
- Bei ca. 50% der Unternehmen waren die Möglichkeiten zur Fernwartung der Produktionsmaschinen und damit zum Zugriff auf das Produktionsnetzwerk nicht dokumentiert.

Es muss damit wohl gefolgert werden, dass mit hoher Wahrscheinlichkeit die meisten Unternehmen einen professionellen Angriff auf ihr OT-Netzwerk nicht rechtzeitig erkennen könnten.

Problematischer Update-Prozess

Nehmen wir aber einmal an, ein Unternehmen hätte einen Angriff entdeckt. Welche Abwehrmaßnahmen stehen ihm zur Verfügung?

In der OT ist ein Herunterfahren der Produktion bei weitem nicht so einfach, wie es z.B. bei Angriffen auf einen Webserver in der IT der Fall ist. Mitunter ist es aus technischen Gründen sogar unmöglich, das betroffene System innerhalb kurzer Zeit kontrolliert zu stoppen. Des Weiteren unterliegen in der OT viele Steuerungssysteme Zertifizierungen, die das einfache Einspielen von Sicherheits-Updates, das in der IT so bekannt ist, verhindern.

Können dann die ICS in einer hinreichenden Zeit auf einen sicheren Stand der Steuerungssoftware gebracht werden? Die Ergebnisse zeigen, dass auch hier die OT noch erhebliche Lücken hat:

- Nahezu kein Unternehmen hat einen systematischen und selbst-gesteuerten Prozess, um aktuelle Bedrohungen und notwendige Sicherheitspatches für die ICS zu erkennen (Sicherheitsradar).
- Ca. 80% der Unternehmen nutzen ICS unterschiedlicher Hersteller.
- Ungefähr 60% der Unternehmen aktualisieren die Steuerungssoftware ihrer ICS manuell. Selbst eine Tool-Unterstützung, wie Versionierung, scheint im Bereich der OT noch selten im Einsatz zu sein.

Das Fazit, das aus diesen Daten zu ziehen ist, beruhigt ebenfalls nicht. Wenn ein Unternehmen Ziel eines Angriff wird und diesen erkannt, sind die Reaktionsmöglichkeiten sehr beschränkt, da oftmals nicht klar ist, ob und welcher Patch helfen könnte, wie dies für die unterschiedlichen Hersteller in einer heterogenen Landschaft aussieht und wie ein Patch rechtzeitig in die ICS eingebracht werden kann. Im Vergleich zu den ca. 380.000 neuen Varianten von Schadsoftware täglich, von denen das BSI ausgeht, wirkt solch eine eher statische Struktur wenig widerstandsfähig.

Organisatorisches Bewusstsein erst in den Anfängen

Natürlich sind Sicherheitsprobleme niemals allein durch technische Maßnahmen zu beheben. Die handelnden Menschen müssen ein Bewusstsein entwickelt haben und die Organisation muss den notwendigen Rahmen für entsprechende Handlungen bieten. Auch hier zeigt sich aber, dass im Bereich der OT noch vieles Notwendige erst in den Anfängen steht:

- Weniger als 35% der Unternehmen haben dedizierte Verantwortlichkeiten für die Sicherheit von ICS definiert (ICS security officer).
- Weniger als 40% der Unternehmen führen eine routine-mäßige Risiko-Analyse der OT und ihrer ICS durch.

In vielen Unternehmen werden die Fragen der Sicherheit der OT derzeit vor allem von IT-Leuten bearbeitet – die aufgrund der oben geschilderten Unterschiede zwischen IT und OT meist eine steile Lernkurve bewältigen müssen.

Diese letzte Erfahrung führt zum nächsten Aspekt.

Kommunikative Herausforderung

Die Anforderungen an IT und OT waren und sind aus fachlichen Gründen sehr unterschiedlich. Die Ausbildung der handelnden Personen ist es ebenfalls. Auch wenn meist die Kommunikation von IT-Experten mit den Ingenieuren der OT einfacher gelingt als zwischen IT und Business, ist doch auch hier zumindest ein Abgleich der Begriffe notwendig. Paradigmen und Werkzeugen, die dem einen Bereich selbstverständlich erscheinen, sind für den anderen unter Umständen – oftmals zu Recht – tabu.

Um ein triviales Beispiel zu nennen, sind Firewalls oder Virenscanner in der IT zwar gang und gäbe, doch muss ihr Einsatz in einem Produktionsumfeld genauer betrachtet werden, da hier z.B. oft Echtzeit-Anforderungen bestehen, die so in dieser Weise in der IT unbekannt sein mögen.

Auch wenn dieser Punkt notgedrungen einen eher qualitativen Aspekt besitzt, legen doch eine Reihe von Gesprächen nahe, dass Großunternehmen regelmäßige Treffen von IT und OT durchführen, während bei KMUs dies eher seltener zu beobachten ist.

Dies mag auch mit einem weiteren Unterschied verbunden sein, der in seiner konkreten quantitativen Ausprägung sicherlich in Frage gestellt werden kann, jedoch für die Kommunikation im Unternehmen und auch die beiden folgenden Aspekte von Bedeutung ist: in nahezu allen Großunternehmen ist sich – so die Rückmeldungen – das Top Management der Bedeutung der ICS und ihrer Sicherheit bewusst. Bei den KMUs ist dieser Anteil geringer und liegt eher bei 60%.

Standards in der OT

Diese Unterscheidung nach Großunternehmen und KMUs zeigt sich auch im folgenden Bereich, der Umsetzung von Standards. Im Bereich der IT haben Standards, wie z.B. der Grundschutzkatalog des BSI buchstäblich einen (gewissen) Standard gesetzt. Auch in der OT haben sich solche Richtlinien entwickelt, die die Sicherheit der OT verbessern können. Zu erwähnen ist hier besonders der Standard IEC 62443. Doch Großunternehmen und KMUs verhalten sich diesen Standards gegenüber durchaus unterschiedlich:

- Während weniger als 35% der KMUs den BSI Grundschutz verwenden, tun dies ca. 80% der Großunternehmen.
- Beim IEC 62443 liegen die Zahlen sogar noch deutlich niedriger: weniger als 25% der KMUs und ca. 65% der Großunternehmen verwenden ihn.

Dieser Unterschied ist leicht verständlich, da Großunternehmen unter einer hohen Heterogenität leiden, während KMUs meist eine geringere Komplexität in ihren Systemen vorfinden und damit eher bereit sind, diese zu ertragen.

Dennoch überrascht, dass in einem Bereich wie der OT, der Compliance-Vorgaben seit langer Zeit kennt, selbst der Bekanntheitsgrad relevanter Normen geschweige denn die Umsetzung noch gering ist.

Prozess-Unterstützung

Ein Ergebnis einer unternehmens-internen Kommunikation und einer Betrachtung der existierenden Standards können konsistente Prozesse zur Sicherheitsbewertung und -optimierung sein. Auf der anderen Seite fördern solche Prozesse aber auch die Kommunikation zwischen den relevanten Akteuren innerhalb und zwischen Unternehmen.

Es ist deshalb zwar nicht tröstlich, doch nicht überraschend, wenn die Prozess-Unterstützung im Bereich der Sicherheit ähnlich sehr uneinheitlich ausgeprägt ist, wie die Verwendung von Standards:

- 75% der Großunternehmen verfügen über dokumentierte Prozesse im Sicherheits-Umfeld, aber nur ca. 50% der KMUs.
- Die Risiko-Bewertung ist bei Großunternehmen und KMUs ebenfalls sehr unterschiedlich

ausgeprägt. Wir bezeichnen in diesem Zusammenhang eine Risiko-Bewertung als konsistent, wenn die Unternehmen angaben, dass sie

a) regelmäßig eine Risiko-Bewertung für die IT des Gesamt-Unternehmens durchführen **und**

b) ebenso auch eine regelmäßige Bewertung für die ICS vornehmen

Im Gegensatz dazu betrachten wir eine Risiko-Bewertung als nicht-konsistent, wenn bei der Bewertung die Risiken der ICS ausgeklammert werden.
Hier zeigt sich, dass immerhin 80% der Großunternehmen solch einen konsistenten Ansatz verwenden, aber nur ca. 50% der KMUs.

Die wiederholt bemerkten Unterschiede zwischen Großunternehmen und KMUs führen uns zum letzten Punkt, der im Rahmen der Studiendurchführung immer wieder thematisiert wurde und den wir bewusst etwas provokativer und plakativer formulieren.

Die Hoffnungen der KMUs

Immer wieder scheint und schien in Gesprächen mit KMUs durch, dass KMUs Entwicklungen erhoffen, die bei Großunternehmen deutlich anders gesehen werden oder zumindest nicht ausgesprochen werden. Bewusst plakativ gesagt, hoffen KMUs, dass

- der nächste Angriff sie nicht trifft
- so komplexe Werkzeuge wie SIEMs, 2-Faktor-Authentifizierung und Anomalie-Erkennung nicht notwendig sind und werden
- weiterhin IT und OT wie bislang unabhängig verwaltet werden können.

Vor dem Hintergrund der aktuellen Lage in der IT und OT besitzen diese Hoffnungen nach unserer Auffassung – vorsichtig formuliert – nur eine sehr begrenzte Legitimation.

Empfehlungen

Was folgt nun aus diesen Ergebnissen? Welche Empfehlungen können gegeben werden? Obwohl sicherlich die meiste Arbeit in der Entwicklung von konkreten, individuellen Lösungen liegt und in der Regel einer genaueren Beratung bedarf, lassen sich doch bei aller gebotenen Vorsicht einige allgemeine Empfehlungen geben. Wir teilen diese zur einfacheren Darstellung in organisatorische und technische Punkte ein. Die Aufstellung ist sicher nicht vollständig und auch nicht direkt in dieser Reihenfolge adaptierbar. Jedoch haben wir uns bemüht, grundsätzlich vom Einfacheren zum Komplexeren zu gehen.

Organisatorisch

Organisatorische Empfehlungen umfassen alle Ansätze, die nicht direkt durch technische Hilfsmittel umgesetzt werden (müssen). Dazu zählen:
Fragen Sie nach der Sicherheit Ihrer OT … im Zweifelsfall tun Sie damit etwas Gutes.

- Reden Sie mit den Kollegen aus IT oder OT. Bereits ein Gespräch ist besser als keins … und wer weiß, was daraus wird.
- Lesen Sie die Dokumente des BSI und des VDMA.
- Definieren Sie Verantwortlichkeiten für die Sicherheit von ICS
- Prüfen Sie die Notfallpläne
- Prüfen Sie die SLA der Hersteller Ihrer Produktionsmaschinen: wie sieht es dort mit Aussagen zu Aktualisierungen etc. aus.
- Wählen Sie gute Passwörter für den Zugang zu Maschinen, die ein solches Verfahren erlauben
- Definieren Sie weitere klare Sicherheitsregeln
- Implementieren Sie erste Schritte hin zu einem Sicherheitsradar auch für OT

Technisch

Aus technischer Sicht kann eine sinnvolle Reihenfolge etwas genauer beschrieben werden:

1. Implementieren Sie eine Netzwerk-Segmentierung auch in Ihrem OT-Netzwerk. Das liefert Ihnen zumindest die Möglichkeit, Angriff eine Zeitlang einzugrenzen.
2. Dokumentieren Sie alle Zugänge zu Ihren Maschinen, auch die Fernwartungszugänge. Hier sollten auch die Authentifizierungsverfahren für den Zugang geprüft werden.
   Verlassen Sie sich dabei **NICHT** auf den Mythos der „Air Gap“ (= da, wo kein Kabel zu sehen ist, kann auch kein Zugang sein).
3. Führen Sie eine Inventarisierung Ihrer OT-Netze durch
   a. Sicherlich regelmäßig, manuell
   b. Idealerweise kontinuierlich
4. Implementieren Sie eine kontinuierliche Überwachung Ihrer OT-Netzwerke
5. Implementieren Sie eine Anomalie-Erkennung in Ihren OT-Netzwerken
6. Parallel dazu kann es sinnvoll sein, Penetration-Tests (Pentests) durchzuführen.
7. Ab einer gewissen Unternehmensgröße können auch SIEMs (Security Information and Event Management) eine wirksame Hilfe darstellen.

Falls Sie zu diesen Themen oder Aussagen Fragen haben, uns Rückmeldungen geben möchten (gerne positiv oder negativer Art) oder einfach nur das Thema spannend finden, scheuen Sie sich nicht, mit uns zu reden. Letztlich sind sichere IT und OT-Systeme für das heutige Leben essentiell. Alles, was dazu beiträgt, hat einen übergreifenden Nutzen.

Literaturverzeichnis

BMBF. (2017). *Industrie 4.0.* Von https://www.bmbf.de/de/zukunftsprojekt-industrie-4-0-848.html abgerufen

BSI. (2017). *Lageberichte.* Von https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html abgerufen

E. Amann, H. A. (6 1992). IT-Sicherheit - was ist das? *Datenschutz und Datensicherung*, S. 286-292.

Heise. (2016). *Heise Newsticker.* Von https://www.heise.de/security/meldung/Rekord-DDoS-Attacke-mit-1-1-Terabit-pro-Sekunde-gesichtet-3336494.html abgerufen

VDMA. (2016). Von https://industrie40.vdma.org/article/-/articleview/13072012 abgerufen