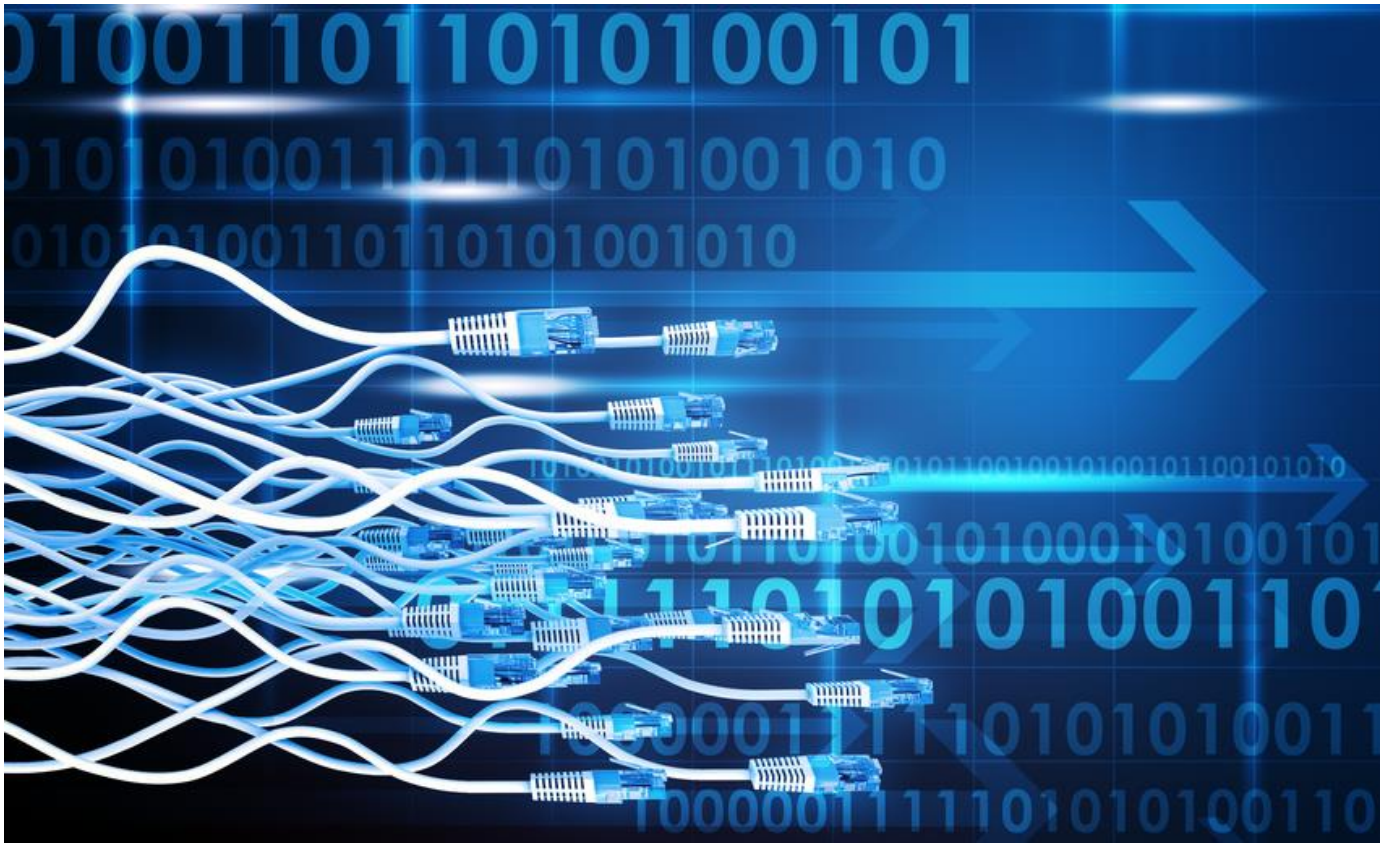

Vernetzte Wirtschaft als Gefahr: Es braucht jetzt eine Cyber Defense Strategie.

Andy Mühlheim, SATW

Industrie 4.0 und Cyber Security

Unternehmen nutzten bisher die Möglichkeiten des Internets vor allem für die Optimierung ihrer Support-, Einkaufs- und Vertriebsprozesse. Die unternehmerischen Kernaufgaben verblieben dabei weiterhin ausschliesslich innerhalb der eigenen Unternehmensgrenzen. Unter dem Begriff Industrie 4.0 findet nun seit einigen Jahren die Digitalisierung der unternehmerischen Wertschöpfungsketten statt (Abbildung 1). Dazu werden Internettechnologien in den Kernprozessen eingesetzt, welche eine prozessintegrierte Zusammenarbeit über Unternehmensgrenzen hinweg ermöglichen. Damit entsteht eine Welt des „Internet of Everything“, in welcher jeder Computer und jedes industrielle System über das Internet miteinander verbunden sind und untereinander in Echtzeit und direkt kommunizieren können. Mit Industrie 4.0 entstehen somit fragmentierte, integrierte Prozesse und Zusammenarbeitsformen über die Unternehmensgrenzen hinweg, welche sich je nach den aktuellen Anforderungen selbstständig und agil neu zusammenstellen. Industrie 4.0 bedeutet damit auch eine Abkehr von unternehmensweiten Datensilos zu globalen Datenflüssen mit Informationen, welche nur noch für den jeweiligen Moment gültig sind. Sowohl für die Wirtschaft wie auch für die Gesellschaft entstehen hierdurch neue, schier unbegrenzte Möglichkeiten und Chancen. Was aus einer rein wirtschaftlichen Sicht durchaus Sinn macht und für die Wirtschaft und die Gesellschaft einen grossen Nutzen mit sich bringt, trägt aber auch neue Risiken und Gefahren in sich. Klare und überwachbare Unternehmensgrenzen diffundieren weg und Maschinen, ja ganze Systeme, kommunizieren fast unkontrollierbar

als Teil des Internets permanent mit anderen Maschinen und Systemen. Dabei tauschen sie Daten und Informationen aus, welche direkt und in Echtzeit in die jeweiligen Unternehmensprozesse einfliessen.

In Industrie 4.0 ist ein herkömmlicher Perimeterschutz mit Firewalls und Virenschutz, wie ihn Unternehmen heute betreiben, gänzlich ungenügend geworden. Zum einen weil sich der Unternehmensperimeter durch die sich agil verhaltenden Prozessfragmente ständig ändert, zum anderen weil sich der Inhalt der Daten und Informationen, welche von den vernetzten Systemen kommen, kaum in Echtzeit prüfen lässt.

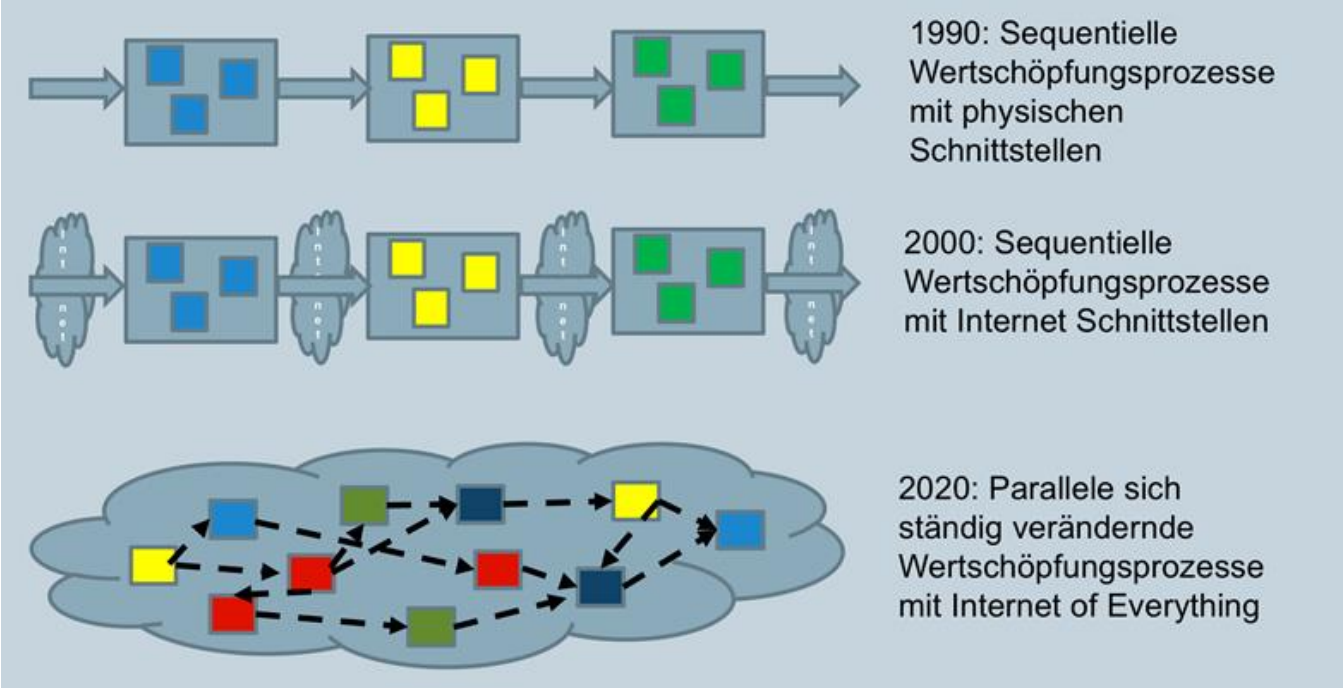

Abbildung 1: Entwicklung zu Industrie 4.0

Datenschutz und Cyber Security greifen zu kurz

Die herkömmliche IT-Security, in welche man auch Themen wie Datenschutz, Passwortschutz, Nutzung der Informatikmittel und vieles mehr hineingepackt hat, wird der neuen Situation nicht mehr gerecht. Wie es in der realen Welt üblich ist, Türen und Fenster zu schliessen und die Werte des Unternehmens korrekt zu nutzen, sind diese IT Security-Themen letztendlich nichts anderes als einzuhaltende Compliance der jeweiligen Unternehmen. Während in der bisherigen Welt Unternehmen mit der Überwachung der Einhaltung der Vorgaben sowie mit installierten Firewalls und Virenschutz bereits wesentliche Punkte für eine adäquate IT Sicherheit abgedeckt haben, braucht es nun in einem digitalisierten Umfeld eine übergeordnete Cyber Defense-Strategie. Der Grund liegt darin, dass mit der Digitalisierung die herkömmliche mit der industriellen Informatik verschmilzt und dabei die bisherige industrielle Informatik durch Internettechnologien abgelöst wird. Damit begeben sich die industriellen Prozesse in die Welt des Internets mit allen Möglichkeiten und Gefahren, welche wir bereits aus unserer bisherigen IT-Welt kennen.

Systeme am „Netz“ werden angegriffen

Versuche mit „Honey-Pots“ zeigen, dass bereits Minuten, nachdem ein neues System im Internet eingebunden ist, dieses das erste Mal „gescannt“ wird.

Honey Pots:
Als Honey-Pot wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, der die Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honey-Pot werden eingesetzt, um Informationen über Angriffsmuster und Angreiferverhalten zu erhalten. Erfolgt ein Zugriff auf einen derartigen virtuellen Dienst oder Nutzer, werden alle damit verbundenen Aktionen protokolliert [Quelle: wikipedia].

Nach kurzer Zeit erfolgen bereits die ersten Angriffe. In der sich nun rasch vernetzenden Welt werden diese Angriffe weiter zunehmen und sowohl an Quantität wie auch an Qualität massiv zulegen. Für den Schutz der industriellen Kernprozesse kommt erschwerend hinzu, dass die Investitionszyklen in der Industrie oftmals 10, 15 oder mehr Jahre betragen und die entsprechenden Systeme während dem Betrieb aufgrund ihrer Abhängigkeiten sowie den betrieblichen Anforderungen kaum aktualisiert werden können. Da für Echtzeitsysteme die Verarbeitungsgeschwindigkeit ein wesentlicher Faktor ist und eine Datenprüfung Zeit beansprucht, können industriell genutzte Systeme oft nicht mit komplexen Firewalls, Virenschutz und weiteren Massnahmen geschützt werden. Dabei verfügen die Angreifer aus der IT-Welt über die jeweils neuesten Technologien und Mittel, um Schwachstellen in Systemen aufzuspüren und auszunutzen. So treten auch immer häufiger Zero-Day-Attacken auf, welche bis zur Bereitstellung eines Security-Patches faktisch nicht abgewehrt werden können. Gerade industrielle Systeme sind dabei besonders von Zero-Day-Exploits betroffen.

Zero-Day-Exploits:
Ein Exploit ist in der elektronischen Datenverarbeitung eine systematische Möglichkeit, Schwachstellen auszunutzen, die bei der Entwicklung eines Programms nicht berücksichtigt wurden. Dabei werden mit Hilfe von Programmcodes Sicherheitslücken und Fehlfunktionen von Programmen (oder ganzen Systemen) ausgenutzt, meist um sich Zugang zu Ressourcen zu verschaffen oder in Computersysteme einzudringen, bzw. diese zu beeinträchtigen [Quelle: wikipedia].

Es muss zuerst in einer Testumgebung sichergestellt werden, dass die bereitgestellte Security-Patches keine unerwarteten Auswirkungen auf die Prozessfunktionen haben. Eine solche Prüfung kann je nach Komplexität des Prozesses mehrere Wochen dauern, wobei die Systeme während dieser Zeit gegen diese Angriffsart ungeschützt bleiben.

Cyber Security muss neu erfunden werden

Aufgrund ihrer verschiedenen Rollen in der unternehmensübergreifenden Zusammenarbeit nehmen Unternehmen ihre Bedrohungen unterschiedlich wahr. Der jeweilige Schutzgrad bemisst sich dabei an den für die Unternehmen für sich als relevant empfundenen Gefährdungen. Damit entsteht in einem vernetzten System die „Weakest Link Problematik“, welche den Schutz des Gesamtsystems auf den tiefsten Schutzgrad im System reduziert. Der Perimeterschutz der Unternehmen wird damit durchlässig oder sogar komplett ausgehebelt. Die Situation verschärft sich zusätzlich, weil Angreifer damit begonnen haben, sich über das Internet zu organisieren und auszutauschen. Ein Netzwerk von Systemen ist damit auf einmal einem Netzwerk von Angreifern ausgesetzt.

Cyber-Angriffe verändern somit aufgrund der Digitalisierung der industriellen Prozesse, ihrer globalen Ausprägung, der Einfachheit ihrer Ausführung sowie der globalen Vernetzung der Angreifer die Bedrohungslage für Unternehmen massiv. Zudem sind Cyber-Angriffe mit einer globalen Ausprägung aufgrund nicht vorhandener staatlicher Ordnungssysteme im Internet strafrechtlich kaum zu verfolgen. Und nicht zuletzt stehen hinter Cyber-Angriffen oft auch Staaten und Organisationen, welche den kaum kontrollierbaren Cyberraum für ihre eigenen Interessen nutzen. Die heute primär auf Perimeterschutz (u.a. Firewalls) ausgelegten Cyber Security-Massnahmen der Unternehmen müssen somit rasch, konsequent und umfassend an die neue Bedrohungslage angepasst werden.

Lösung Immunsystem

Auch wenn ein Land sich an der Grenze durch Grenzkontrollen schützt, gibt es trotzdem im Landesinneren eine Polizei, eine Feuerwehr und einen Notdienst. Obwohl sich der Mensch mit Schutzmitteln gegen bekannte Gefährdungen wie Hitze, Kälte oder scharfe Kanten schützt, besitzt er noch ein Immunsystem, welches Bedrohungen im Inneren des Körpers erkennt und abwehrt. In der realen Welt gibt es also schon eine Kombination aus „Perimeterschutz“ und „Schutz im Inneren“. Aus diesen Analogien kann man die Lösung für einen ganzheitlichen Schutz von vernetzten Systemen ableiten, indem man die Firewalls als Perimeterschutz beibehält und diese mit einem „digitalen Immunsystem“ ergänzt, welches Angriffe im Innern erkennt und abwehrt. Die Erkennung von Bedrohungen geschieht dabei in der systematischen Auswertung und der Suche nach Anomalien in allen wesentlichen Ereignisprotokollen aus den verschiedenen Systemlogs in Echtzeit. Aufgrund dieser Anomalien werden Rückschlüsse gezogen auf Vorbereitungen oder Durchführung von Cyber-Angriffen. Die Abwehr der Bedrohung erfolgt je

nach Angriff automatisch oder durch Spezialisten mittels geeigneter Anpassungen der Systemkonfigurationen. Inzwischen gibt es bereits SIEM-Systeme (Security Information and Event Management), welche die verschiedenen Systemlogs überprüfen, nach bekannten Mustern scannen und Meldungen absetzen, wenn Unregelmässigkeiten entdeckt werden.

SIEM:
Ein SIEM analysiert in Echtzeit Logs, bzw. Ereignisdaten aus verschiedenen Systemen welche in einem Netzwerk verteilt sind nach Spuren von potenziellen Angriffen. Dabei werden Ereignisse miteinander korreliert um Zusammenhänge und Ursachen zu ermitteln.

Diese Systeme sind jedoch insbesondere im Betrieb sehr aufwändig und teuer und werden, wenn überhaupt, oft nur von einem einzigen Systembetreuer und mit den vom Hersteller bereitgestellten Standardeinstellungen betrieben. Damit reduziert sich der Nutzen maximal auf die Erkennung von bekannten Bedrohungen sowie auf eine allfällige „post mortem“ Analyse, wenn man noch herausfinden möchte, was genau die Ursache der Systembeeinträchtigung war. Selbst dies jedoch nur unter der Voraussetzung, dass die entsprechenden Historien der Logs genügend lang gesichert wurden und noch verfügbar sind.

Ein Netzwerk, um ein Netzwerk vor einem Netzwerk zu schützen

Den Gedanken des Immunschutzes aufnehmend und weitertragend ist eine Organisation, welche Systemlogs von verschiedenen Unternehmen professionell, in Echtzeit und 7/24/365 sammelt, korreliert und nach Anomalien durchsucht. Idealerweise schliessen sich in einer solchen Organisation Unternehmen zusammen, welche in ihren Prozessen bereits miteinander vernetzt sind (z. Bsp. Energieversorger, Transport-/Logistikunternehmen, Spitäler) und vergleichbare oder ähnliche Prozesse haben. Durch die Analyse der relevanten Ereignisse aus den verschiedenen Systemlogs über die Unternehmensgrenzen hinweg können entsprechende Kosten und Ressourcen zentral geführt und geteilt werden, was einen effizienten und bezahlbaren 7/24/365 Betrieb erlaubt. Zudem können bei einem solchen Ansatz zusätzliche Fähigkeiten durch Mathematiker, Prozessanalysten und Forensiker bereitgestellt werden, die auch unbekannte Bedrohungen feststellen können, welche in den SIEM nicht in den Standardeinstellungen erkannt werden. Ein um solche Fähigkeiten erweitertes Team erlaubt auch eine Verknüpfung der Daten aus den Systemlogs mit dem Verständnis von Prozessspezialisten sowie mit OpenSource- und nachrichtendienstlichen Informationen. In der Summe ergibt dies eine äusserst effiziente kontext- und risikobasierte Erkennung von Bedrohungen und Anomalien in den Systemen in Echtzeit. Unregelmässigkeiten und Angriffe können damit im Idealfall bereits erkannt werden, bevor diese grössere Schäden anrichten. Gewonnene Erkenntnisse werden dabei mit Handlungsempfehlungen an die beteiligten Unternehmen weitergeleitet, was diesen eine rasche und adäquate Intervention an den Systemen in ihren Unternehmen ermöglicht. Nachrichtendienste profitieren ihrerseits, indem sie ihre Informationen mit Daten aus den Systemen verifizieren können und damit sicherstellen, dass sie nicht auf sogenannte „Troll Farms“ hereinfallen, welche ihre Glaubwürdigkeit untergraben wollen.

Troll Farm:
Eine Troll Farm ist eine Institution, welche unter anderem mittels gezielter Falschmeldungen und Aktivitäten vom eigentlichen Ziel eines Angreifers ablenkt, um damit den Angegriffenen oder Dritte zu ungeeigneten Handlungen zu bringen und damit dessen Glaubwürdigkeit zu diskreditieren.

Mit diesen Gedanken entsteht ein Netzwerk von Cyber Defense-Spezialisten (Abbildung 2), welche in den teilnehmenden Unternehmen, staatlichen Stellen sowie zentral in der obenerwähnten Organisation gemeinsam Hand in Hand arbeiten und sich dabei ergänzen. Durch die permanente Einbindung der Unternehmen in den Cyber Defense-Prozess können diese ihre Massnahmen laufend den aktuellen Bedrohungen anpassen und auch aufeinander abstimmen. Das Konzept, dass Unternehmen sich für Cyber Defense gemeinsam organisieren, entspricht auch dem Sinn der NCS (vom Bundesrat im Juni 2012 verabschiedete nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken), welche die Verantwortung für Cyber Security-Massnahmen in Eigenverantwortung der Industrie zuweist und von dieser geeignete Massnahmen gegen Cyberbedrohungen erwartet.

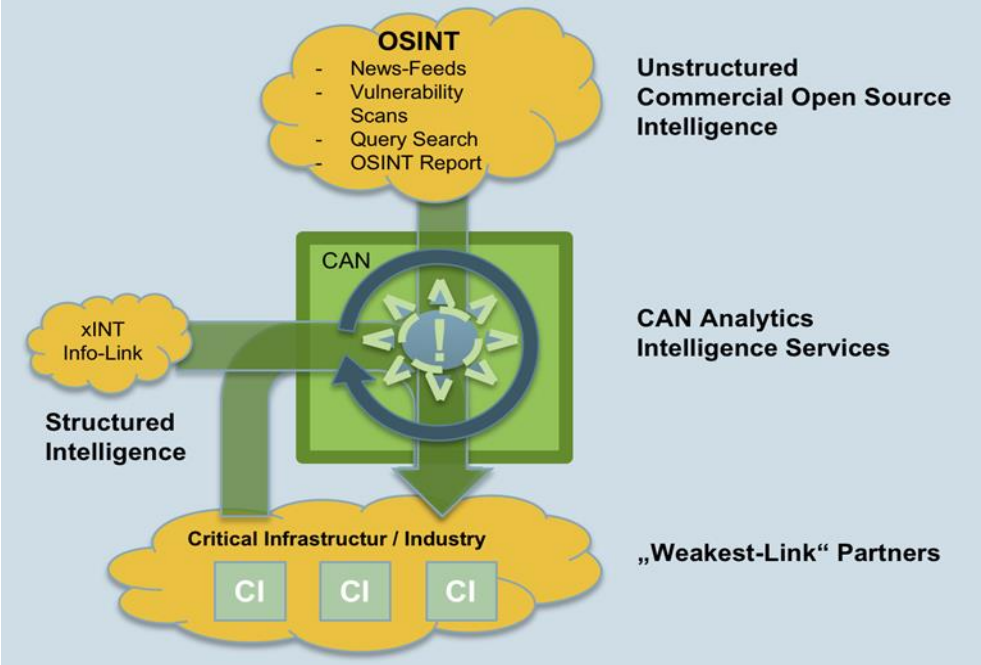

Abbildung 2: Integriertes Cyber Alert-Netzwerk
CAN: Cyber Alert Network
OSINT: Open Source Intelligence
xINT: Intelligence Service
CI: Critical Infrastructure or Industry

Cyber-Krisenmanagement als neue Kompetenz von Unternehmen

Auch bei Umsetzung aller Cyber Defense-Massnahmen werden in der vernetzten Welt vermehrt Cyber-Incidents geschehen. Es ist zwar möglich die Anzahl der Incidents und insbesondere deren Auswirkungen zu reduzieren, sie können jedoch nicht gänzlich verhindert werden. Die Fähigkeit, jederzeit zeitnah einen Cyber-Incident erfolgreich abwehren zu können, wird somit für jedes Unternehmen zu einer nicht zu unterschätzenden permanenten Aufgabe und wird unter Umständen sogar eine entscheidende Rolle spielen, ob ein Unternehmen einen Cyber-Angriff übersteht oder nicht. Eine Cyber-Krise unterscheidet sich dabei massgeblich von herkömmlichen bekannten Krisen. So kann eine konkrete Cyber-Bedrohung mehrere Monate dauern und dabei während der ganzen Zeit die Aufmerksamkeit des Managements und operative Ressourcen beanspruchen, während gleichzeitig der eigentliche Betrieb des Unternehmens aufrechterhalten werden muss. Die Entdeckung von Vorbereitungen zu einem Cyber-Angriff oder eines Cyber-Angriffs selbst muss dabei, auch innerhalb des Unternehmens, zwingend höchst vertraulich behandelt werden, da der Angreifer möglicherweise seinen Angriff zerstörerisch ausübt, sobald er feststellt, dass er entdeckt worden ist. Somit sind auch sämtliche Gegenmassnahmen über den gesamten Zeitraum höchst vertraulich und verdeckt zu führen, obwohl diese aufgrund der Vernetzung der Systeme möglicherweise zusätzlich mit Dritten abzustimmen sind. Ein solches Cyber-Krisenmanagement muss vorbereitet und wiederholt mit den involvierten Verantwortlichen geübt werden. Da ein Aufbau eines Cyber-Krisenmanagements bei einem Incident nicht mehr möglich ist, müssen entsprechende Ressourcen und Fähigkeiten bereits im Vorfeld bestimmt und verfügbar sein. Auch hier ist ein einzelnes Unternehmen kaum in der Lage, die entsprechenden Experten „auf Vorrat“ zu beschäftigen. Insbesondere, da diese Fähigkeiten rar und entsprechend teuer sind. Abgesehen davon wären solche Experten in einem einzelnen Unternehmen unterbeschäftigt und unmotiviert. Ein Pool von diversen Spezialisten über die einzelnen Unternehmen hinweg macht deshalb Sinn. Idealerweise ist dabei Cyber-Krisenmanagement eine weitere Dienstleistung der bereits angesprochenen unternehmensübergreifenden Cyber Defense-Organisation und stellt mit vordefinierten Prozessen, Prozeduren und Infrastrukturen sicher, dass ein Unternehmen bei Bedarf unmittelbar eine Krisenmanagementeinrichtung in Anspruch nehmen kann.

Fazit

Industrie 4.0 und die Vernetzung der Produktionsprozesse über die Unternehmensgrenzen hinweg ist sinnvoll, schafft immense neue Chancen für Industrie und Gesellschaft und spart letztendlich durch integrierte Wertschöpfungsprozesse massgeblich Kosten.

Unternehmen sind jedoch gut beraten, wenn sie im Rahmen ihrer Digitalisierungsprojekte eine für sie geeignete Cyber Defense-Strategie entwickeln und gleichzeitig Cyber-Krisenmanagementfähigkeiten aufbauen. Die entsprechenden Kosten sind dabei als Preis der Digitalisierung und der Industrie 4.0 Strategie der Unternehmen zu sehen. Je nach Situation wird es dabei wahrscheinlich sinnvoll oder sogar zwingend sein, Cyber-Defense und -Krisenmanagementfähigkeiten gemeinsam mit anderen Unternehmen zu entwickeln und sicherzustellen.

Die Verantwortung der Cyber-Defense und -Krisenmanagementsmassnahmen liegt bei der obersten Unternehmensführung, welche Vorgaben erstellen muss und auch die entsprechenden Mittel bereitstellen kann. Die Umsetzung der Massnahmen liegt hingegen bei den CIOs, CSOs, Risk Officers, BCM- und Krisenmanagern der einzelnen Unternehmen.

Eine Digitalisierung ohne eine begleitende Cyber Defense-Strategie und ohne ein vorbereitetes Cyber-Krisenmanagement ist heute nicht mehr denkbar. Dies gilt insbesondere für kritische Infrastrukturen wie Energie, Telekommunikation, Transport, Logistik und Versorgung, da die Betreiber dieser Infrastrukturen aufgrund der Abhängigkeiten der gesamten Industrie und Gesellschaft von diesen Basisdienstleistungen, neben den unternehmerischen Risiken, vor allem volkswirtschaftliche Risiken tragen. Weil ein Funktionieren eines Staates und einer Gesellschaft ohne eine funktionierende und permanent zur Verfügung stehende Basisinfrastruktur undenkbar geworden ist, müssten für diese Unternehmen möglicherweise sogar verpflichtende Massnahmen im Bereich Cyber-Defense geprüft werden.

Impressum
Schweizerische Akademie der Technischen Wissenschaften
www.satw.ch
April 2016
Dieser Artikel entstand für die SATW Rubrik „Im Fokus“ zum Thema Cyber Security.
Gestaltung: Claudia Schärer
Bilder: Fotolia