IT-Sicherheit im Zeitalter der Industrie 4.0

zeitimblick.info/

Peter 8.6.2017

Können Sie sich noch an „Stuxnet“ erinnern? Vor einigen Jahren geisterte dieser Computerwurm durch die IT-Anlagen der Industrie, in AKW´s und durch die Medien. Damals erhielt die Welt einen Blick durch ein „Wurmloch“ in die Zukunft des Cyber-War.

Diese Zukunft hat längst begonnen, besagtes Schadprogramm zeigte aber schon **2010** was auf uns zu kommt. Damals wurden zB. Steuerungsanlagen manipuliert, Frequenzumrichter kompromittiert oder gar die Uranzentrifugen angegriffen.
Es geht hier also nicht um die kleinen privaten Computer-Problemchen, sondern dieser Artikel beschreibt einen gefährlich hohen Level von Cyber-Kriminalität.

Stuxnet, bzw. dessen Wegbereiter, Klone und Versionen richteten immensen Schaden an und bis heute weiß man nicht wirklich wer dahinter steckt. Man weiß aber, die eigentlich ab 2007 gestartete Schad-Software war sehr ausgefeilt, den Auftraggebern musste es einen mehrstelligen Millionen Betrag gekostet haben.

Mit USB Stick ganze Fabrik lahmgelegt!

Hohe Kosten entstehen natürlich auch auf der anderen Seite, beim Umsetzen der Maßnahmen für industrielle IT Sicherheit. Dabei ist die Ursache oft banal: Ein Mitarbeiter lädt in der Hektik des Alltags irrtümlich Schadcode herunter, ein anderer infiziert gar absichtlich die Systeme seiner Firma. Alles schon vorgekommen, ein USB Stick reicht um ganze Fabriken zu (zer)stören.

Der unaufhaltsame Weg des Codes beginnt etwa bei einem ungepatchten Windows-PC , über das Netzwerk bis zu den Fertigungsanlagen. Jene sind ebenfalls längst untereinander vernetzt, sowie auch mit den Terminals der Mitarbeiter verbunden.
Die entpackten Methoden und Funktionen können sich lange ruhig verhalten, aber eines vorprogrammierten Tages arbeiten sie im Sinne der Cyber-Kriminellen und gegen ihre Besitzer.

Klar, jedes Unternehmen setzt erst mal auf die eigenen IT-Leute, man versucht diese Sache nicht publik werden zu lassen. Denn Kunden, Lieferanten und Partner werden wenig begeistert sein.
Studien schätzen, dass sich von 1000 betroffenen Firmen höchstens 100 – 200 melden.

Doch ich kann aus eigener Erfahrung (DDos Attacken) sagen: Solche Vorkommnisse sollte man den zuständigen Behörden melden und vor allem: sich **Hilfe externer Spezialisten holen**! Die interne IT ist auf die Betriebsabläufe fokussiert und eventuell nicht voll auf das vorbereitet was der Industrie 4.0 blühen kann und wird!

Das Internet der Dinge in der Industrie

Das „***Internet of Things***“ (kurz IoT) beschränkt sich keineswegs auf digitale Armbänder mit Tracking-Funktion, intelligente Kühlschränke oder vernetztes Kinderspielzeug.

Dieses Konzept ist auch in der Industrie angekommen: „***Industrial Internet of Things***“ (IIoT) ist die Kommunikation von Maschinen untereinander, die Datengewinnung- und deren Verwertung sowie Kommunikations- und Automatisierungstechnologien.
Dadurch erreicht man höchste Effizienz, weil die stets dokumentierten Prozesse quasi in Echtzeit optimiert werden können und im Endeffekt soll es natürlich auch den Gewinn erhöhen.

Doch es ist eine herber Verlust, wenn sich die „Dinge“, von der Werkzeugmaschine bis zum Industrieroboter gegen ihre Operatoren wenden. Hier ist guter Rat teuer, weil viel wert – aber nicht unbezahlbar!

„*Data as a Service*„? Was ist den „*Daas*“ schon wieder?

Schließlich seien noch die immensen Datenmengen erwähnt, welche das Industrielle Internet der Dinge produziert: „*Mehr Sensorik und Aktorik, ‚intelligente Maschinen und Systeme‘ produzieren unendlich viele Daten die gesammelt, analysiert und wieder bereitgestellt werden müssen. Diese Daten sollten zusammengeführt werden, um die Produktion effizienter, kostengünstiger etc. zu gestalten.*„, so ein Sprecher von www.yokogawa.com.

Genau diese Zusammenführung, Analyse und Bereitstellung von Daten in Form einer Servicedienstleitung wird als „***Data as a Service***“ (DaaS) bezeichnet.

Dies alles zeigt, wie oben erwähnt – man sollte sich helfen lassen, externe, spezialisierte Dienstleister haben da mehr Know-how. Denn diese konzentrieren sich auf genau diese Aufgaben. Die eigene, interne IT hat genug mit den Kernaufgaben der betriebsinternen Abläufe zu tun.

Dabei folgen diese Profis meist einem recht logischen Prinzip, teilen das Sicherheitskonzept für Automatisierungssysteme auf vier Ebenen auf:

- **Physische Sicherheit & Netzwerksicherheit**,
  z. B. Zugangsbeschränkungen bzw. -überwachung für Computer- und Schalträume; Firewall zwischen Leitsystem-Bus und anderen Netzwerken, z. B. Büro- oder Drahtlosnetzen, VPN-Zugänge;
- **Sicherheit von Servern und Applikationssoftware**,
  z.B. Whitelisting, Antiviren-Software & Systempflege (Updates, Upgrades, Patches);
- **Sicherungs- und Wiederherstellungsoptionen**,
  z. B. (automatisches) Erstellen von Backups, Backupverwaltung;
- **Lebenszyklus-Management**,
  Anpassung der Sicherungs- und Schutzmaßnahmen an den aktuellen Stand der Technik und die spezifische Bedrohungslage.

Man ist also nicht allein mit seinen digitalen Sorgen, es gibt immer wo Hilfe; Man muss aus der Menge an Anbietern nur die richtigen Leute herausfinden, denn diese sind noch selten.
Aber: Lesen Sie zeitimblick.info, hier zeigen wir die echten Profis auf und enttarnen Dampfplauderer …