IT-Security – Spielverderber oder Wettbewerbsvorteil in der vernetzten Welt?

Wenn ich meine Fantasie über das Potential der neuen großartigen Möglichkeiten der IT schweifen lasse, verblasst so mancher visionäre Science-Fiction Film meiner Jugend zu einem langweiligen B-Movie.

AI, IoT, Big Data Analytics und das Verschmelzen von OT und IT erzeugen eine Welt, in der meine individuellen Wünsche im Vorfeld erkannt werden. Mein Nutzerverhalten fließt bereits vorausschauend in Material- und Produktionsplanung in Form der Losgröße 1 ein. Und das alles, bevor die Kaufentscheidung letztendlich getroffen wird. Ich gebe zu, dass dieses Bild der Realität etwas voraus ist.

Als globaler IT-Distributor hat man den großen Vorteil, mit einem Auge an den Visionen von IT-Herstellern und ihrer schönen neuen Welt teilzuhaben zu können. Mit dem anderen Auge betrachtet man den echten Markt und seine Realität. Mit der aktuell gelebten Strategie vieler produzierender Unternehmen ist die Expedition in IoT-Welten oder gar die Koppelung von OT und IT ein Wagnis mit hohem Risiko. Diese neuen Möglichkeiten verlangen innovative Wege im Umgang mit der IT-Security.

IT-Security als ganzheitliches Konzept begreifen

Wenn man den Blick nun zurück auf den Beginn der Industriellen Revolution richtet, erkennt man, dass Unternehmen gezwungen waren, ein Qualitätsmanagement einzuführen. Nur so konnten sie im Wettbewerb bestehen. Das Produzieren von Einzelteilen, die erst zum Schluss komplett montiert werden, verträgt keine Fehler, die sich dann in tausenden Endprodukten wiederfinden.

Die IT-Security in Unternehmen steht vor einem ähnlichen Wandel. In der Vergangenheit haben wir viele verschiedene „Security Produktionsmaschinen“ eingesetzt und uns auf ihre Wirksamkeit verlassen. Diese einzelnen Maßnahmen wurden aber nie in ein ganzheitliches „Security (Qualitäts-) Konzept“ im Unternehmen eingebunden.

Mal Hand aufs Herz: Wer deckt Gelände- und Gebäudesicherheit, Personen-, Identitäts-, Rollen- oder Rechteverwaltung und Endgeräte- und Schwachstellenmanagement als Grundlage der IT-Security in einem gemanagten Prozess ab? Einzeln und in verschiedenen Abteilungen bestimmt. Aber mit diesem Ansatz verspielt man schnell wertvolle Potentiale. Haben Sie die Kontrolle über Ihr digitales und analoges Firmennetzwerk? Und wissen Sie, was jedes Ihrer vernetzten Geräte gerade macht und mit wem es kommuniziert?

Spätestens dann, wenn die Produktionsstraße mit dem IT-Firmennetz verbunden wird, sollte das „IT-Security Qualitätsmanagement“ so reibungslos funktionieren wie das Qualitätsmanagement der Produktion.

Dass die klassische Herangehensweise mit der Anschaffung von zusätzlichen „Security Produktionsmaschinen“ mehr und mehr versagt und keine ganzheitliche IT-Security Strategie darstellt, erfährt man jeden Tag aus verschiedenen Medien. Manager sind angehalten, Unternehmen immer widerstandsfähiger gegen Ausschuss und Verlust in der Produktion und somit effizienter zu machen. Die schöne neue Welt verlangt, die IT zu einem widerstandsfähigen homogenen, sich ständig verbessernden System zu wandeln, das Unternehmen und deren Kunden schützt und Schäden begrenzt. Denn wie in der Produktion gibt es auch in der IT-Security immer „Ausschuss“, der bei uns „Angriff“ heißt. Diese „Angriffe“ gilt es durch eine ganzheitliche Security Strategie abzuwehren und somit den „Spielverderber“ IT-Security als Wettbewerbsvorteil zu nutzen.

Patrick Olschewski

Patrick Olschewski ist Senior Business Development Manager für IT-Security bei Tech Data Advanced Solutions. Er berät Business Partner bei der Weiterentwicklung ihres IT-Security Geschäfts.