Sechs entscheidende Schritte, um Digitalisierung, IoT und Vernetzung sicher zu machen

Die Digitalisierung wird noch auf Jahre der bestimmende Trend im Business bleiben. Sie ist auf unterschiedliche Arten im Unternehmen wirksam. Auf der einen Seite macht sie neue Geschäftsmodelle und Produktinnovation möglich, auf der anderen Seite hilft sie bei der Optimierung der Abläufe und bei der Kostensenkung. Versteckt passiert sie auch in den Maschinen- und Fertigungsstrassen, wo die Welten der IT und der OT (Operational Technology) aufeinandertreffen. Die totale Vernetzung aller Komponenten mit dem Internet erschliesst Angreifern ganz neue Einfallstore.

Michael Ghezzo

«Vorstellung der Digitalisierung ist, dass alles zu jeder Zeit miteinander kommunizieren können soll und auf Daten von überall zugegriffen werden kann. Das erzeugt bei Security-Verantwortlichen Kopfschmerzen», Freddy Bürkli, T-Systems.

«Mit dem Ausbau von 5G wird die Verbreitung von IoT-Geräten drastisch zunehmen und zum attraktiven und bevorzugten Tummelplatz von Cyberangriffen werden. IoT-Geräte mit Verbindung zum Unternehmensnetzwerk und/oder RZ werden zur Bedrohung des gesamten Unternehmens», Rolf Herzog, CT Cinetrade AG.

Dabei kommen auch noch unterschiedlichste Produkte, Berater und Hersteller zum Einsatz. Die Technologie ist schnelllebig. Was heute ein Hype ist, wird morgen durch ein ganz anderes Konzept ersetzt. Die Implementierung muss oft schnell gehen und auf Cyber-Security-Schwächen stösst man dann erst am Schluss.

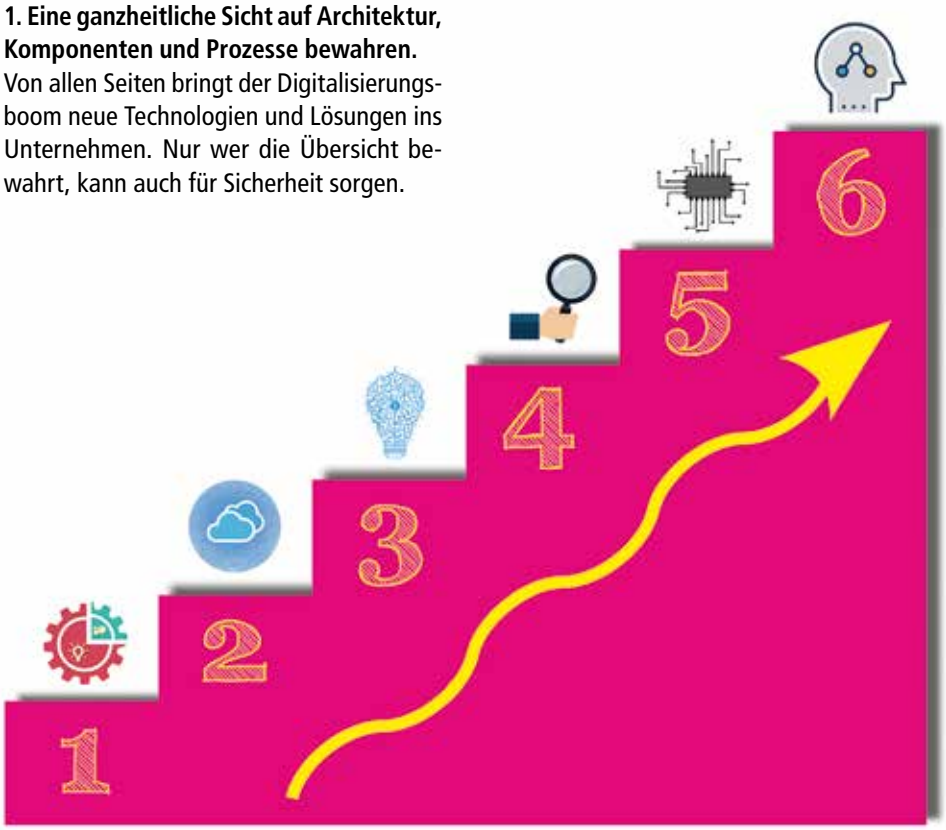
«Je mehr wir unser technisches Umfeld verändern, je mehr wie unsere Prozesse und Zusammenarbeitsmodelle digitalisieren, je mehr wir uns aus unseren (nur anscheinend so sicheren eigenen) Rechenzentren heraus in die Cloud bewegen, Edge etablieren, umso mehr nehmen die Bedrohungsszenarien zu, mit denen wir konfrontiert sind. Das Umfeld wird ganz einfach komplexer. Hybride Welten halt. Aber das ist das, was geschieht, das sind Entwicklungen, denen wir uns nicht verschliessen können und wollen. Sie sind essenziell für unseren Unternehmenserfolg. Daher müssen wir uns mit ihnen auseinandersetzen, sie aktiv angehen», Marcus Frantz, ÖBB.

Von Profis für Profis

Wer diese sechs Schritte berücksichtigt, schafft eine sichere Digitalisierung und kann trotz IoT-Einsatz ruhig schlafen:

1. Eine ganzheitliche Sicht auf Architektur, Komponenten und Prozesse bewahren.
Von allen Seiten bringt der Digitalisierungsboom neue Technologien und Lösungen ins Unternehmen. Nur wer die Übersicht bewahrt, kann auch für Sicherheit sorgen.

«Die Digitalisierung ist der Treiber, der uns mit unglaublicher Geschwindigkeit in Form von neuen Technologien und Innovationen nach vorne bringt. Gleichzeit besteht darin aber auch die Gefahr, dass wir uns durch die damit einhergehende und sehr oft unkontrollierte Vernetzung, unbemerkt Hintertüren einbauen, die es Angreifern ermöglichen, tief in unsere Landschaft vorzudringen – auch in Bereiche, die nach Best Practices der Cyber Security sehr gut geschützt sind.



Ein grosses Bedrohungsszenario sehe ich in einem Wildwuchs an unsicheren Lösungen, der oft in Schatten-IT's, vorbei an den IT-Verantwortlichen betrieben wird», Thomas Zapf, Verbund.

2. In jedem Projekt schon sehr früh die Frage nach der Sicherheit stellen.
Wenn die Cyber Security erst berücksichtigt wird, wenn das Projekt schon kurz vor dem Abschluss steht, verursacht diese unnötige Kosten und Verzögerungen, die im schnelllebigen digitalen Zeitalter den Erfolg im Wettbewerb gefährden.

«Die IoT-Elemente sind in der Regel mit dem Fokus auf ihre zentrale Funktion entwickelt und hierbei werden die Schnittstellen und möglichen Angriffsvektoren vorerst ausgeblendet», Martin Schellenberg, Schutz und Rettung Zürich.

«Die Digitalisierung im Allgemeinen öffnet Unternehmen viele Türen und neue Wege, bietet aber auch neue Angriffspunkte und zusätzliche Bedrohungen für die Unternehmen. Gerade deshalb ist es essenziell, den Sicherheitsaspekt bei fortlaufender Digitalisierung stets von Beginn an mitzuberücksichtigen», Gottfried Tonweber, EY.

«Tatsächlich kann man schon viele Problemfelder eingrenzen, wenn Security-Aspekte bereits in der Produktauswahl bzw. -entwicklung einfliessen. Da geht es um ganz simple Dinge, wie bspw. Codeüberprüfungen, um festzustellen, ob einfache Einfallslücken, wie ein simples Passwort oder schon bekannte Hersteller-Bugs, geschlossen sind», Freddy Bürkli, T-Systems.

3. Es muss nicht so bleiben, wie es war: Man sollte bestehende Abläufe beim Digitalisieren hinterfragen.
«Wer einen Sch*-Prozess digitalisiert, erhält einen digitalen Sch*-Prozess.» Das Ergebnis sind Systeme, die kaum mehr managebar sind, und Schwachstellen, die man nicht mehr wegbekommt.

«Nur weil es bisher so gemacht wurde, bedeutet es nicht zwangsläufig, dass es in Zukunft auch so gemacht werden muss. Unnötige oder schlechte Prozesse bringen eine verhängnisvolle Komplexität in die System- und Servicelandschaft, die dann langfristig vielleicht sogar zu einer kontraproduktiven Situation und höheren Kosten führen kann», Wolfgang Mayer, Hoerbiger.

4. Und wenn das Angebot noch so attraktiv ist – man sollte die Hersteller genau überprüfen.
Tolle Features, geringe Kosten, schnelle Implementierung, das versprechen die Hersteller. Standards und Zertifizierungen helfen dabei, zu überprüfen, ob auch die Anforderungen der Cyber Security gewahrt sind.

«Die zunehmende Geschwindigkeit setzt die Hersteller unter Druck, schnell neue Produkte auf den Markt zu bringen. Darunter leidet oft die Security-Qualitätssicherung und wird nicht mit der notwendigen Aufmerksamkeit behandelt, die von Kunden vorausgesetzt wird», Thomas Zapf, Verbund.

«Ob es nun ENISAs Empfehlungen ‹Good Practices for Security of Internet of Things› sind oder der NIST Draft ‹Recommendations for IoT Device Manufacturers› vom Jänner 2020. Es ist klar, dass das blinde Vertrauen zu Herstellern von IoT verschwunden ist», Wolfgang Mayer, Hoerbiger.

5. Wie ein Feuerwart denken: Bedrohte Bereiche isolieren.
Totale Sicherheit ist undenkbar. Die Kosten würden explodieren und die Funktionalität würde leiden. Wie im modernen Hausbau kann man aber in der Planung schon sicherstellen, dass im Notfall nicht gleich das ganze Hause abbrennt.

«Die möglichen Einfallstore werden noch grösser und die Isolierung überlebenswichtiger Systeme umso zentraler. Ich denke hier vermehrt wie beim Hausbau in ‹Brandabschnitten›. Wir müssen da ein oder zwei Zimmer opfern, um die anderen zu schützen. Das verbrannte Zimmer können wir dann wieder renovieren. Das ist immer noch wirtschaftlicher als das ganze Haus zu ersetzen. Mit diesem Bild vor Augen haben wir uns deshalb entschlossen diese ‹lebenswichtigen IT-Organe› physisch vom Rest zu trennen. Im Einzelfall ist das jeweils eine reine Risiko- und Wirtschaftlichkeitsabwägung», Konrad Zöschg, Flughafen Zürich.

«Netzwerksegmentierung und Jump-Hosts sind die Lösung, um die ‹sauberen Netze› von den potenziell angreifbaren zu trennen und so eine virale Verbreitung von Schadcode zu unterbinden», Gerhard Grün, Erber AG.

6. Auch wenn es ohne Partner nicht geht – man sollte sicherstellen, dass entscheidendes Know-how im Unternehmen bleibt.
Auf dem Weg zum Secure Softwareentwicklungsunternehmen – in Zeiten von Cloud und Outsourcing – darf man das Know-how über die wichtigsten Prozesse und Systeme nicht gänzlich abgeben.

«Hier muss den Herstellern der Applikationen fachlich bzw. softwaretechnisch auf Augenhöhe begegnet werden, und das ist durch den sehr starken Outsourcingtrend in den verschiedenen Industrien nicht mehr so einfach zu bewerkstelligen. Jedes Unternehmen muss auf gewisse Weise auch zu einem Softwareentwicklungsunternehmen werden. Ich erweitere diese Forderung der Digitalisierung aber in Richtung Secure Softwareentwicklungsunternehmen», Thomas Zapf, Verbund.

«Da Digitalisierung mit Automatisierung und damit früher oder später mit Ressourceneinsparung einhergeht, gibt es oft einen Wissensverlust. Deswegen sehe ich es als bedenklich, wenn zentrale und komplexe Geschäftsprozesse ohne gute Dokumentation automatisiert werden», Wolfgang Mayer, Hoerbiger. ■