Kolumne: Chief Digital Community

Cyber Security als Schlüsselfaktor

Thomas Meier

Von der Digitalisierung profitieren langfristig vor allem diejenigen, die eine sichere IT-Infrastruktur haben. Cyber Security ist somit mehr als eine Voraussetzung für eine erfolgreiche digitale Transformation – sie ist ein Erfolgsfaktor.

Sinkende Kosten, höhere Effizienz, steigende Produktivität, mehr Umsatz, neue und grössere Geschäfte, Erweiterung der Produktpalette und des Dienstleistungssortiments und vieles mehr: Die Erwartungen an die Digitalisierung sind hoch. Was versprechen Sie sich davon? Und an welcher Stelle Ihrer Prioritätenliste steht bei Ihnen das Thema Digitalisierung? Aber selbst wenn das Thema für Sie nicht höchste Priorität hat, dürfte es kaum mehr einen Unternehmensentscheid geben, in den Digitalisierung nicht auf die eine oder andere Art hineinspielt – und das in jeder Branche. Sie haben sicher schon einmal den Begriff «industrielle Revolution» gehört. Die Wachstumsprognosen für vernetzte Maschinen und Geräte (IIoT – Industrial Internet of Things) zeigen steil nach oben. Gerade im Produktionsumfeld wird in den kommenden Jahren ein regelrechter Boom an internetfähigen Maschinen und Geräten erwartet – aber nicht nur dort. Auch öffentliche Infrastrukturen werden zunehmend digital, beispielsweise Strom- und Breitbandversorgung, ebenso wie unsere Demokratie im Sinne von elektronischen Abstimmungen. Die Herausforderung besteht in der dadurch immer komplexeren IT-Umgebung. Wie auch immer Sie die Chancen der modernen Informations- und Kommunikationstechnologien nutzen, etwas sollten Sie dabei auf keinen Fall vergessen: die Sicherheit.

Digitalisierung und ihre Auswirkungen auf die Sicherheit

Die Digitalisierung hat folgenschwere Auswirkungen auf die Sicherheit von Daten und ganzen IT-Systemen.

Zum einen entstehen durch die zunehmende Vernetzung neue Angriffspunkte, zum anderen bergen neue und veränderte Aufgaben, Abläufe und Technologien immer ein Fehlerrisiko. Bestes Beispiel hier ist die bereits genannte elektronische Abstimmung, die regelmässig aufgrund der Sicherheitsrisiken in den Medien thematisiert wird.

In Unternehmen führt die Digitalisierung und Vernetzung zu Effizienzsteigerung durch vereinfachte Prozesse, zu mehr Transparenz und Arbeitserleichterung im Alltag. Gleichzeitig steigt aber auch das Bedrohungspotenzial deutlich an, da mehr Angriffspunkte und zu verarbeitende Daten vorhanden sind. Im Umkehrschluss: Die Wahrscheinlichkeit von Cyberattacken auf Unternehmen steigt durch die Digitalisierung erheblich. Gleichzeitig erhält das Thema Cyber Security in Unternehmen immer noch zu wenig Gewicht, wie unzählige Studien und auch unsere Erfahrung zeigen. Mehr als ein Drittel der IT-Entscheider berichteten in der Studie «Potenzialanalyse Digital Security» von Sopra Steria Consulting, neue Technologien teilweise auch dann einzuführen, wenn noch nicht alle möglichen Si-

cherheitsrisiken bekannt und bewertet wurden. Fatal, aber in der dynamischen und hochkomplexen Zeit der Digitalisierung keine Seltenheit. Umso wichtiger ist es, ein Risikomanagement zu etablieren, eine effektive Cyber Security-Strategie zu erstellen und sich auf Cyberattacken so gut wie möglich vorzubereiten.

Digitalisierung und Cyber Security schliessen sich nicht aus

Damit das Risikopotenzial möglichst klein gehalten werden kann, müssen Digitalisierung und Cyber Security Hand in Hand gehen – gerade bei versorgungskritischen Infrastrukturen und sensiblen Daten. Denn diese sind ein besonders lukratives Ziel für Hacker. Aber auch wenn sie keine versorgungskritischen Infrastrukturen betreiben: Industrie 4.0, Internet of Things (IoT), X-as-a-Service-Business-Modelle, Sharing Economy, arbeitende Kunden, ortsunabhängiges Teamworking und so weiter sind ohne umfassende Sicherheitsmassnahmen langfristig nicht erfolgreich.

Sicherheitsfragen gehen jedoch nicht nur Sicherheitsverantwortliche etwas an – in erster Linie gehören sie ins Management. Wieso? Bei einem erfolgreichen Angriff sind oftmals geschäftskritische Prozesse betroffen. Ebenso geht es um das Risikomanagement und die Compliance, welche Kernaufgaben der Geschäftsführung sind. Die Daten von Kunden, Maschinen, Prozessen, Produkten und Innovationen müssen vor unerlaubten Zugriffen und Diebstahl geschützt werden. Es ist jedoch nicht erforderlich, dass das Management sich mit technischen und architektonischen Themen der Cyber Security auskennt. Es muss jedoch sicherstellen, dass Sicherheitsverantwortliche die finanziellen und personellen Ressourcen sowie das Know-how haben, um die erforderlichen Massnahmen ergreifen zu können. Ausserdem müssen sie die kritischen, besonders schützenswerten Vermögenswerte – die Kronjuwelen des Unternehmens – definieren. Dazu gehört auch festzulegen, welche Ausfallzeiten für welche Prozesse tolerierbar sind.

Weshalb Kultur ebenso wichtig ist wie Flexibilität und Mehrschichtigkeit

Um diesen Herausforderungen standhalten zu können, ist ein umfassendes, flexibles Sicherheitskonzept notwendig. Im Gegensatz zu traditionellen Prozessen ist Flexibilität besonders wichtig, denn die digitale Sicherheit muss sich der dynamischen Transformation laufend anpassen. Deswegen wird Cyber Security heutzutage auch mehrschichtig und flexibel aufgebaut. Eine möglichst hohe, dicke Mauer reicht nicht mehr aus, um Hacker aufzuhalten. Heutzutage ist ein gestaffeltes Sicherheitsdispositiv notwendig, um akute Gefahren schnell erkennen, isolieren und ausmerzen zu können. Unternehmen müssen sich konsequent mit aktuellen und neuen Risiken auseinandersetzen.

Anerkannte Modelle für die Errichtung, Umsetzung, Überprüfung und kontinuierliche Verbesserung der eigenen Cyber Security sind internationale Standards wie ISO 27001 oder das NIST Cyber Security Framework. Diese bieten ein 360-Grad-Modell für die Errichtung, Umsetzung, Überprüfung und kontinuierliche Verbesserung der eigenen Cyber Security und adressiert dabei die Bereiche: Identify, Protect, Detect, Respond und Recover. Ein solches Framework ist aber nicht nur zu Ihrem eigenen Schutz sinnvoll, sondern in einigen Branchen regulatorisch vorgeschrieben. Wichtig ist dabei ein systematisches Vorgehen, was ein umfassendes Risikomanagement, den Aufbau angemessener Sicherheitskonzepte sowie eine geeignete Sicherheitsarchitektur und Massnahmen zum Schutz, der Erkennung und Reaktion auf Sicherheitsvorfälle beinhaltet. Die Cyber Security-Strategie bildet dabei den bereichsübergreifenden Rahmen.

Hinzu kommt eine weiterer entscheidender Security-Bereich, den das Management berücksichtigen muss. Die beste Cyber Security-Strategie und die besten Technologien sind nur halb so effektiv, wenn keine entsprechende Sicherheitskultur im Unternehmen vorhanden ist. Das Management muss diese vorleben. Sicherheitsbewusste Mitarbeitende sind entscheidend, wenn es darum geht, Cyberattacken abzuwehren. In Kombination mit einer umfassenden Cyber Security-Strategie legt dies die Erfolgsbasis für die digitale Transformation des Unternehmens und schafft nicht zuletzt ein nachhaltiges Kundenvertrauen. «

Thomas Meier ist CEO der auf Cyber Security spezialisierten Infoguard AG und Vorstandsmitglied der Chief Digital Community CDC. (www.infoguard.ch, www.chiefdigital.ch).