

Cyber Security als Basis der Digitalisierung

Sicher zum Erfolg

Sie gilt als Game Changer für Unternehmen und Wegbereiterin der vierten industriellen Revolution: die digitale Transformation. Doch so verlockend ihre Verheissungen auch sind – profitieren werden nur jene, die ihre Infrastruktur wirksam schützen.

→ VON FRANCO CERMINARA



DER AUTOR

Franco Cerminara
ist Chief Consulting Officer
bei InfoGuard.
→ www.infoguard.ch

Unternehmen versprechen sich viel von der Digitalisierung ihrer Geschäftsprozesse: Sinkende Kosten, höhere Effizienz und steigende Produktivität sind nur einige Beispiele. An welcher Stelle Ihrer Prioritätenliste steht die digitale Transformation in Ihrem Geschäft? Ganz oben wie bei den meisten Schweizer Firmen? Aber selbst wenn die Digitalisierung an sich für Sie nicht höchste Priorität hat, dürfte es kaum mehr einen Unternehmensentscheid geben, in den diese nicht auf die eine oder andere Art hineinspielt. Entsprechend zeigen die Wachstumsprognosen für vernetzte Maschinen und Geräte steil nach oben. Gerade im Produktionsumfeld wird in den nächsten Jahren ein Boom an internetfähigen Maschinen und Geräten erwartet. IT-Umgebungen werden dadurch immer komplexer. Eine so heterogene IT stellt Unternehmen vor grosse Aufgaben und Herausforderungen. Wie immer man die Chancen der modernen Informations- und Kommunikationstechnologien auch nutzt – etwas sollte man hierbei auf keinen Fall vergessen: die Sicherheit.

DIE FOLGEN FÜR DIE SICHERHEIT

Die Digitalisierung hat folgeschwere Auswirkungen auf die Sicherheit von Daten und IT-Systemen. Einerseits durch Lücken in der Digitalisierung von Geschäftsprozessen (analoge und digitale Prozesse laufen parallel ab), andererseits durch die erfolgte Digitalisierung. Es entstehen neue, veränderte Aufgaben, Abläufe und eingesetzte technische Systeme. Die zunehmende Digitalisierung und Vernetzung führt zu Effizienzsteigerung durch vereinfachte Prozesse, zu mehr Transparenz und zu mehr Komfort im Alltag. Gleichzeitig steigt aber auch das Bedrohungspotenzial, da

sich die Anzahl möglicher Angriffspunkte erhöht und die zu verarbeitenden Datenmengen sich vervielfachen. Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen steigt.

Doch viele Unternehmen treiben die Digitalisierung voran und stellen mitunter die IT-Sicherheit hinten an. Dies zeigt etwa die Studie «Potenzialanalyse Digital Security» von Sopra Steria Consulting. 32 Prozent der IT-Entscheider berichten darin, dass im eigenen Unternehmen neue Technologien in Einzelfällen auch dann eingeführt werden, wenn vorab noch nicht alle möglichen Sicherheitsrisiken bekannt und bewertet wurden. Dabei führen sowohl Lücken in der Digitalisierung als auch die Digitalisierung selbst zu Sicherheitsrisiken. Beides müssen Unternehmen in ihren Strategien und Massnahmen zur Cyber Security berücksichtigen. Nur dann kann die Digitalisierung tatsächlich die erhofften Vorteile bringen und nicht etwa zusätzliche Unternehmensrisiken.

ZAHL DER ANGRIFFE STEIGT

Betriebsausfälle und Cyberangriffe gehören für Unternehmen zu den grössten Business-Risiken. Speziell Cyberangriffe haben stark an Bedeutung gewonnen. Erst kürzlich hat auch die Finanzmarktaufsicht (FINMA) Cyberangriffe zum grössten operationellen Risiko für die Branche ernannt. Cyberangriffe betreffen aber auch die Industrie. Die Attacken können zu Betriebsausfällen führen, indem sie Produktionsanlagen lahmlegen oder wichtige Daten etwa mit Ransomware-Angriffen blockieren.

Der damit verbundene finanzielle Verlust, Imageschaden und Kundenschwund sind Folgen, von denen sich Unternehmen auch nach Jahren nur schwer erholen. Gerade Betriebe, die Industrie-4.0-Initiativen verfolgen, sind wegen der Komplexität ihrer IT-Landschaft anfällig für Cyberangriffe. Denn die digitale Vernetzung geht einher mit einer Evolution der Cyberkriminalität: Anzahl, Ausmass und Zielgerichtetheit von Angriffen steigen kontinuierlich.

CYBER SECURITY IST CHEFSACHE

Die Digitalisierung und die Sicherheit sind unzertrennbar miteinander verbunden – vor allem, wenn ausser Unternehmen auch versorgungskritische Infrastrukturen ins Visier von Hackern geraten. Ohne Cyber Security keine Industrie 4.0, kein Internet of Things (IoT), keine As-a-Service-Business-Modelle, keine nahtlose Partnerintegration,

«Die FINMA hat
Cyberangriffe zum grössten
operationellen Risiko
ernannt»

Franco Cerminara



Digitalisierung und IT-Sicherheit sind untrennbar miteinander verbunden

keine arbeitenden Kunden, keine Sharing Economy und kein weltweites Teamwork. Jeder Schritt in Richtung digitale Transformation löst automatisch Security-Fragen aus, die beantwortet werden müssen. Ob man will oder nicht. Und diese Fragen stellen sich nicht nur Sicherheitsverantwortliche. Sie sind Chefsache. Denn die Cyber Security betrifft geschäftskritische Prozesse, das Risikomanagement und die Compliance – also Kernaufgaben der Geschäftsführung. Die Daten von Kunden, Maschinen, Prozessen, Produkten und Innovationen müssen von unerlaubten Zugriffen und vor Verlust geschützt werden.

Die Geschäftsleitung muss sich nicht mit der Technik auseinandersetzen, aber sicherstellen, dass qualifizierte Verantwortliche und Spezialisten die erforderlichen Massnahmen ergreifen – und dass sie dafür auch die notwendigen Mittel erhalten. Zudem müssen die besonders schätzenswerten Assets durch die Geschäftsführung definiert werden. Sie muss ebenfalls festlegen, welche Ausfallzeiten für welche Prozesse tolerierbar sind und welche Daten unter keinen Umständen in falsche Hände geraten dürfen.

MEHRSCHTIG, FLEXIBEL UND MIT KULTUR

Diese Herausforderungen sind alles andere als trivial. Sie benötigen die Erarbeitung eines umfassenden Sicherheitskonzepts, das sich an immer neue Situationen anpassen lässt. Im Gegensatz zur Absicherung in der herkömmlichen analogen Welt, die über Jahrtausende komplett durchstrukturiert wurde, befindet sich nämlich die digitale Sicherheit parallel zur digitalen Transformation der Unternehmen in einem dauernden Wandel. Entsprechend mehrschichtig und flexibel wird heute auch die Cyber Security

aufgebaut. Statt einer einzelnen, möglichst hohen und dicken Mauer wird ein gestaffeltes Abwehrdispositiv errichtet, das akute Gefahren schnell erkennen, isolieren und ausmerzen kann.

STANDARDS BIETEN ORIENTIERUNG

Unternehmen sind gut beraten, sich konsequent mit aktuellen und neuen Risiken auseinanderzusetzen und der Informationssicherheit das nötige Gewicht beizumessen. Die Cyber-Security-Strategie bildet dabei den bereichsübergreifenden, strategischen Rahmen. Internationale Standards wie ISO 27001 oder das NIST Cyber Security Framework bieten dazu ein anerkanntes Modell für die Errichtung, Umsetzung, Überprüfung und kontinuierliche Verbesserung der eigenen Cyber Security.

Es hat sich gezeigt, dass gerade das systematische Vorgehen einen erheblichen Mehrwert bietet. Dazu zählen etwa ein gezieltes Risikomanagement, der Aufbau eines angemessenen Sicherheitskonzepts und einer geeigneten Security-Architektur. Dazu kommt ein weiterer entscheidender Bereich, auf den das Management einen massgeblichen Einfluss hat: Sicherheit bedingt nicht nur modernste Technik, sondern auch eine entsprechende Firmenkultur. Das Management muss diese Verhaltensnormen vorleben und deren Stellenwert Nachdruck verleihen. Eine erfolgreiche Digitalisierungskultur im Unternehmen muss zusätzlich zum kreativen Innovationsgeist immer auch ein gesundes Security-Bewusstsein hochhalten. Erst eine umfassende Cyber-Security-Strategie legt die Erfolgsbasis für die digitale Transformation des Unternehmens und schafft nachhaltiges Kundenvertrauen. ←