Gegen Systembrüche!

Risikomanagement und tragfähige Sicherheitsarchitekturen als Schlüsselfaktoren für Sicherheit

Die meisten IT-Infrastrukturen sind mit der Zeit gewachsen und bestehen aus vielen unterschiedlichen Technologien und Systemen, die sich nur schwer managen lassen. Hinzu kommen zahlreiche Insellösungen, Datensilos und Organisationseinheiten im Unternehmen, die noch nicht zusammenarbeiten. Die ideale Voraussetzung für Cyber-Attacken, Manipulationen und Sabotagen. Noch dazu vergessen viele, die IT-Architekturen mit der Prozesssicherheit zu verknüpfen. Doch was lässt sich dagegen machen?

Von Tim Cappelmann, AirITSystems

Heterogen gewachsene IT-Infrastrukturen sind keine Seltenheit, sondern Alltag in deutschen Unternehmen. Schließlich sollen die teuren IT-Systeme möglichst lange erhalten bleiben – und nicht mit jeder neuen Technologie ausgemustert werden. Dennoch sorgen diese fragmentierten IT-Landschaften für höhere Risiken und erleichtern es Hackern, ins Unternehmensnetzwerk einzubrechen. Je mehr Systembrüche, desto größer wird das Risiko eines Hackerangriffs.

Kampf den Systembrüchen

Wer seine Unternehmenswerte schützen möchte, braucht ein durchdachtes Risikomanagement und tragfähige Sicherheitsstrukturen. Insellösungen und Datensilos sind dabei besonders zu beachten. Hier ist viel Sorgfalt gefordert. Denn Systembrüche zu beseitigen, hat verschiedene Dimensionen: in der Technik, bei Prozessen und in Bezug auf die Gesetzgebung.

Technologisch gesehen ermöglicht Automation durch ineinandergreifende Systeme ein Wachstum an Schnelligkeit. Bei der Anatomie heutiger Angriffe ist dies unabdingbar. Gleichzeitig ermöglicht es eine bessere Steuerung im Risikokontext und Budgets werden gezielter eingesetzt. Jeder Systembruch bringt Zufall in das System und erhöht so die Fehlerwahrscheinlichkeit.

IT-Lösungen machen daher nur vernetzt Sinn: Firewall, Cloud und Endpunkt arbeiten zusammen. Nur mit einer durchgängigen Security-Automation (Security Orchestration, Automation and Response, SOAR) und ohne blinde Flecken durch Insellösungen kann man ohne ausufernden Personalaufwand noch angemessen reagieren.

Prozesssicherheit ist Sicherheit

Prozessual und organisatorisch betrachtet, resultiert eine Vernetzung der Prozessabläufe mit der Technik zudem in mehr Effizienz. Auch hier können Brüche beseitigt werden. Schließlich ist eine Excel-Abfrage an die IT „welche Updates wurden eingespielt“ heutzutage nicht mehr tragbar.

Normen, Anforderungen, Gesetze bilden die externe Sicht der Prozesssicherheit, die es zu berücksichtigen gilt. Sie wollen zum überwiegenden Teil das Gleiche: gesteuerte Maßnahmen und Risikoorientierung. Ob Datenschutz, NIS-2 oder was auch immer – alle treffen sich beim Risikomanagement wieder. Wer also seine Daten ohne Systembrüche bereitstellt, kann mit einem durchgängigen Informationssicherheits-Managementsystem (ISMS) und der Verzahnung mit der Technik alle Anforderungen mit einem Managementsystem abdecken und braucht nicht für jede Anforderung eine eigene Lösung zu suchen.

Der Ball liegt beim Risikomanagement

Durch die NIS-2-Verordnung und das KRITIS-Update wird wieder einmal deutlich, wie wichtig es ist, dass Informationssicherheit unternehmensübergreifend gesehen werden muss – und eben nicht nur eine Aufgabe der IT ist.

Im Vordergrund steht das Risikomanagement. Es entscheidet, welchen Bausteinen welches Gewicht zugeteilt wird, damit notwendige Maßnahmen entsprechend schnell bei Störungen und Schwachstellen greifen. Denn umfassende Sicherheit muss vor allem managebar sein.

Für die sichere Konfiguration von IT-Systemen sowie Vorgaben zu Prozessen der Betriebsführung ist es empfehlenswert, ein ISMS einzusetzen – in der NIS-2-Verordnung wird sogar explizit das „Management und Offenlegung von Schwachstellen [der informationstechnischen Systeme]“ gefordert.

Blinde Flecken

Obwohl umfassende Informationssicherheit die Einbeziehung aller Organisationseinheiten eines Unternehmens voraussetzt, scheitert das Konzept häufig an der Umsetzung und an falschen Erwartungen. Gerade die Implementierung eines ISMS wird oft nicht vorbehaltlos übernommen. Schnell kommt der Verdacht auf, dass es sich dabei nur um eine „lästige Dokumentation“ handelt, die abgelegt und vergessen wird.

Darüber hinaus herrscht häufig der Irrglaube, dass Informationssicherheit nur eine Sache der IT sei und mit den anderen Organisationen nichts zu tun hätte. So sind die Folgen in einem Krankenhaus beispielsweise, dass die Sicherheitsregeln auf die Verwaltungs-IT angewandt werden, aber nicht auf die am gleichen Netzwerk angeschlossenen IT-Geräte der Medizintechnik. Auch das Facility Management und die dazugehörige Gebäudesicherheit, wie zum Beispiel Videokameras, Brand- und Einbruchsmeldeanlagen oder Zutrittskontrollen, können leicht vergessen werden. Es entstehen sogenannte „blinde Flecken in den Managementsystemen“, die dazu führen, dass nur eine fragmentierte Informationssicherheit etabliert werden kann. Aus diesem Grund ist es umso wichtiger, dass die Verantwortung für die Sicherheit bei der Geschäftsführung angesiedelt ist. Diese hat vor allem die Aufgabe, für eine umfassende Sicherheit zu sorgen.

Sicherheitsstrategien, die Risiken minimieren und Ziele erreichen

Jedes Unternehmen hat individuelle Risiken und benötigt somit auch ein tragfähiges Schutzkonzept – angepasst an die Risikolandkarte. Trotz aller Individualität lassen sich IT-Sicherheitsmaßnahmen bausteinartig zu einer umfassenden Sicherheitsarchitektur kombinieren. AirITSystems nutzt hierfür die Methodik der „Building Blocks“. Neben technologischen Blöcken wie beispielsweise Firewalls, Endpoint Protection, Backup und Restore, sollten auch Betriebsprozesse und Managementsysteme, Reporting, Meldeprozesse und Berichtswesen in das Gesamtkonzept eingefügt werden.

Das Ziel einer funktionierenden und umfassenden Informationssicherheit ist nicht, wie viele denken, der perfekte Schutz. Diesen gibt es nicht. Vielmehr geht es darum, die Resilienz des Unternehmens so weit zu stärken, dass es sich selbst organisieren und Maßnahmen einleiten

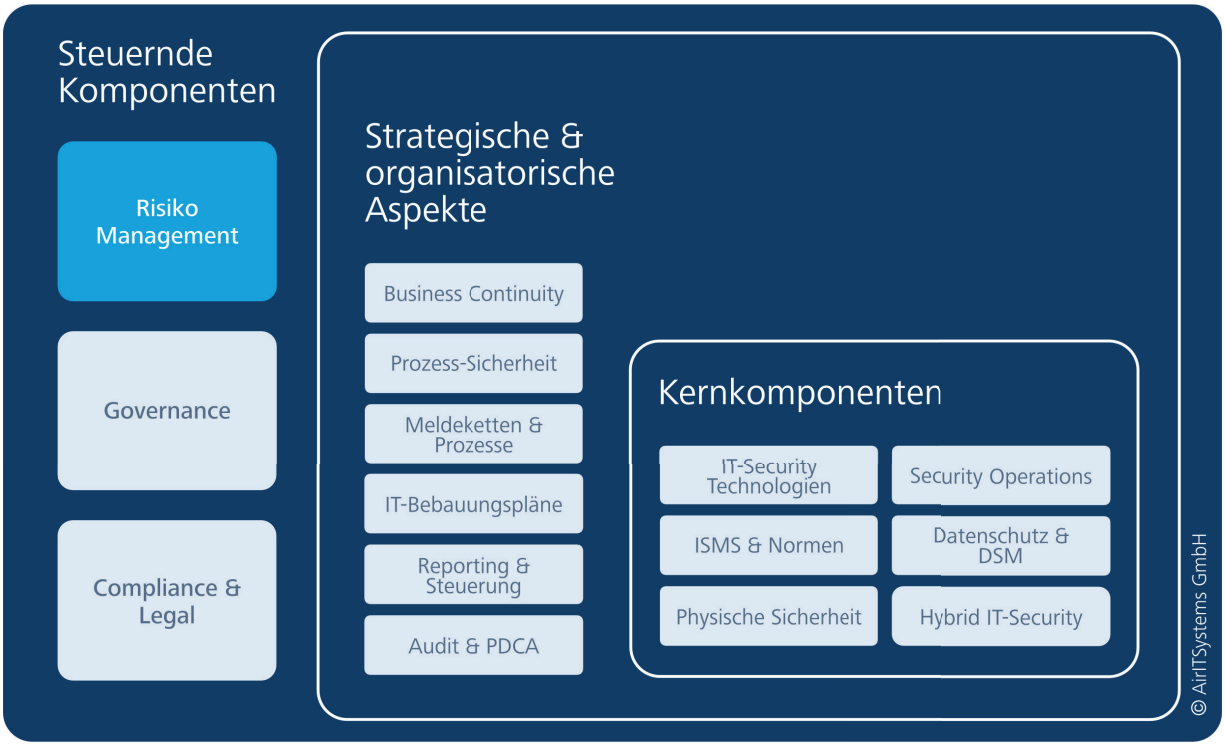

Abbildung 1: Risikomanagement im Fokus – tragfähige Sicherheitsarchitekturen als Unternehmensbasis (Bild: AirITSystems)

kann, wenn unvorhergesehene Ereignisse eintreten. Vertraulichkeit, Integrität, Verfügbarkeit und weitere Schutzziele sind hier zu nennen. Dabei ist es wichtig, Wissenssilos zu vermeiden und flexibler zu werden.

Damit rückt auch das Business-Continuity-Management (BCM) in den Fokus. Notfallhandbücher und Krisenorganisationen bestimmen Prozesse und Verantwortliche. Am Ende ist entscheidend, wie gut das Team aus unterschiedlichen Organisationen zusammenarbeiten kann, um sich selbst zu schützen.

IT und Organisation müssen zusammenwachsen

Die Grenzen zwischen der IT und den restlichen Organisationen in einem Unternehmen behindern derzeit noch jede Sicherheitsstrategie. Zu lange galt die IT-Abteilung nur als einer von vielen ausführenden Dienstleistern, die von der Geschäftsführung gesteuert wurden (Stichpunkt Business IT-Alignment). Durch die digitale Transformation hat sich vieles verändert, und es wurde klar, dass IT-Sicherheit vielmehr übergreifende Informationssicherheit ist, die für jede Abteilung und Organisation eine große Rolle spielt.

Deshalb gilt: Controller an den Tisch! Alle Beteiligten müssen gemeinsam im Team agieren und sich ihrer Verantwortung bewusst werden. Das Risikomanagement bildet die Klammer – Informationssicherheit, Datenschutz und IT-Sicherheit werden zu eins.

Aller Anfang ist leicht

Für AirITSystems ist Informationssicherheit mehr als nur IT-Sicherheit. Es geht darum, Risiken für das eigene Unternehmen zu bewerten und entsprechende Maßnahmen abzuleiten. Eine ganzheitliche Sicherheitsstrategie beinhaltet nicht nur IT-Sicherheitsarchitekturen, sondern schließt physische Sicherheit, genauso wie die Prozesssicherheit, mit ein. Denn allein mit vorher festgelegten Abläufen steht Sicherheit auf einem verlässlichen Fundament. Aus diesem Grund folgt AirITSystems dem eigenen Leitsatz „Audit – Plan – Build – Run“.

Hierfür wurden eigene Sicherheitslösungen wie beispielsweise AirIT-ONE entwickelt – ein Software-Tool zum Aufbau und Betrieb von Managementsystemen. Auch das „Business IT-Alignment“-Konzept oder die NIS-2-Gap-Analyse helfen Unternehmen, mit umfassenden Sicherheitsinitiativen schnell an den Start zu gehen. ■