Digital Trust – Vertrauen in den Umgang mit Daten als Erfolgsfaktor

Mit der zunehmenden IT-Durchdringung sind Unternehmen der digitalen Welt immer stärker von der Verfügbarkeit ihrer IT-Systeme abhängig. Gleichzeitig führt der einfache Systemzugang über das Internet zu einer erhöhten Verwundbarkeit. Mit Blick in die Unternehmen haben wir jedoch das Gefühl, dass viele die Risiken der Informationssicherheit gegenwärtig unterschätzen und oftmals nicht ausreichend beherrschen.

Das öffentliche Interesse für Datenschutz und Sicherheit wächst kontinuierlich. Was müssen Unternehmen bedenken, wenn sie sich disruptiven Technologien anpassen?

Dr. Adrian Marti

Industrialisierung und Digitalisierung hielten auch auf krimineller Seite Einzug. Wie seit jeher sind Kriminelle oft *Early Adopters* neuer Technologien, um im Wettrüsten zwischen Angriff und Abwehr den entscheidenden Schritt voraus zu sein. Erheblich angestiegen sind in den letzten Jahren internetbasierte Betrügereien und die Wirtschaftskriminalität. Bemerkenswert ist insbesondere, dass der Grad organisierter Kriminalität in diesem Bereich deutlich zunahm.

Cyber-Attacken entwickeln sich zu einem profitablen Geschäftsmodell. Hochmodern ausgerüstete kriminelle Banden mit modernen Organisationsmodellen und Tools lösen einzeln agierende Cyberkriminelle ab. Die Professionalisierung der Cyber-Kriminalität schafft neue Dienstleistungen wie z. B. *Access as a Service* auf attraktive Angriffsziele inklusive Versteigerung des Zugangs zu bereits gehackten Zielen an den höchsten Bieter.

Durch die fortschreitende Verbreitung von Informationstechnologie und die zunehmende Systemvernetzung wächst die Bedrohungslage. Galt es lange Zeit, sich «nur» gegen Schadprogramme, insbesondere Viren, zu schützen, gibt es heute diverse sicherheitsrelevante Herausforderungen.

Spätestens seit der Digitalisierung gilt eine sichere und stabile IT als geschäftskritische Ressource. IT-Sicherheitsvorfälle führen demnach für die meisten Unternehmen nicht mehr nur zu einer Beeinträchtigung, sondern wirken sich potenziell geschäftsgefährdend aus. Vor dem Hintergrund der steigenden Bedeutung der Verarbeitung personenbezogener Daten in der digitalen Wirtschaft werden Datensicherheit und Datenschutz immer wichtiger. Diesbezügliche Probleme können zu einem grossen Vertrauensverlust bei Kunden und Geschäftspartnern führen, was ebenfalls geschäftskritische Implikationen nach sich ziehen kann.

Eine zeitgemässe Informationssicherheit muss potenzielle Informationssicherheitsrisiken einerseits aktiv angehen, um die Wahrscheinlichkeit ihres Auftretens möglichst klein zu halten. Andererseits muss im Schadensfall die Fortführung der Geschäftstätigkeit sichergestellt sein. Folgende Maximen können befolgt werden:

- **Risikobasierte Entscheidungsfindung**
  Informationssicherheitsverantwortliche müssen sich hin zur risikoorientierten Entscheidungsfindung bewegen. Die Umsetzung dieser altbekannten Idee ist heute dringlicher denn je. «Risk-based thinking» setzt ein Verständnis geschäftskritischer Gefahren voraus und ist Basis für eine daraus abgeleitete Priorisierung von Kontrollen und Investitionen in IT-Risiken und -Sicherheit. Mit steigender technologischer Komplexität sind die vorhandenen Mittel auf das Management der Hauptbedrohungen zu fokussieren. Risikobasiertes Denken ermöglicht es, Cybersicherheitsinvestitionen auf die Hauptrisiken auszurichten. Treiber für die Risikobeurteilung muss die Linie und darf nicht die Informatik sein.

- **Schutz der digitalen Kronjuwelen**
  IT- und Sicherheitsverantwortliche müssen ihr Augenmerk vom Schutz der IT-Infra-

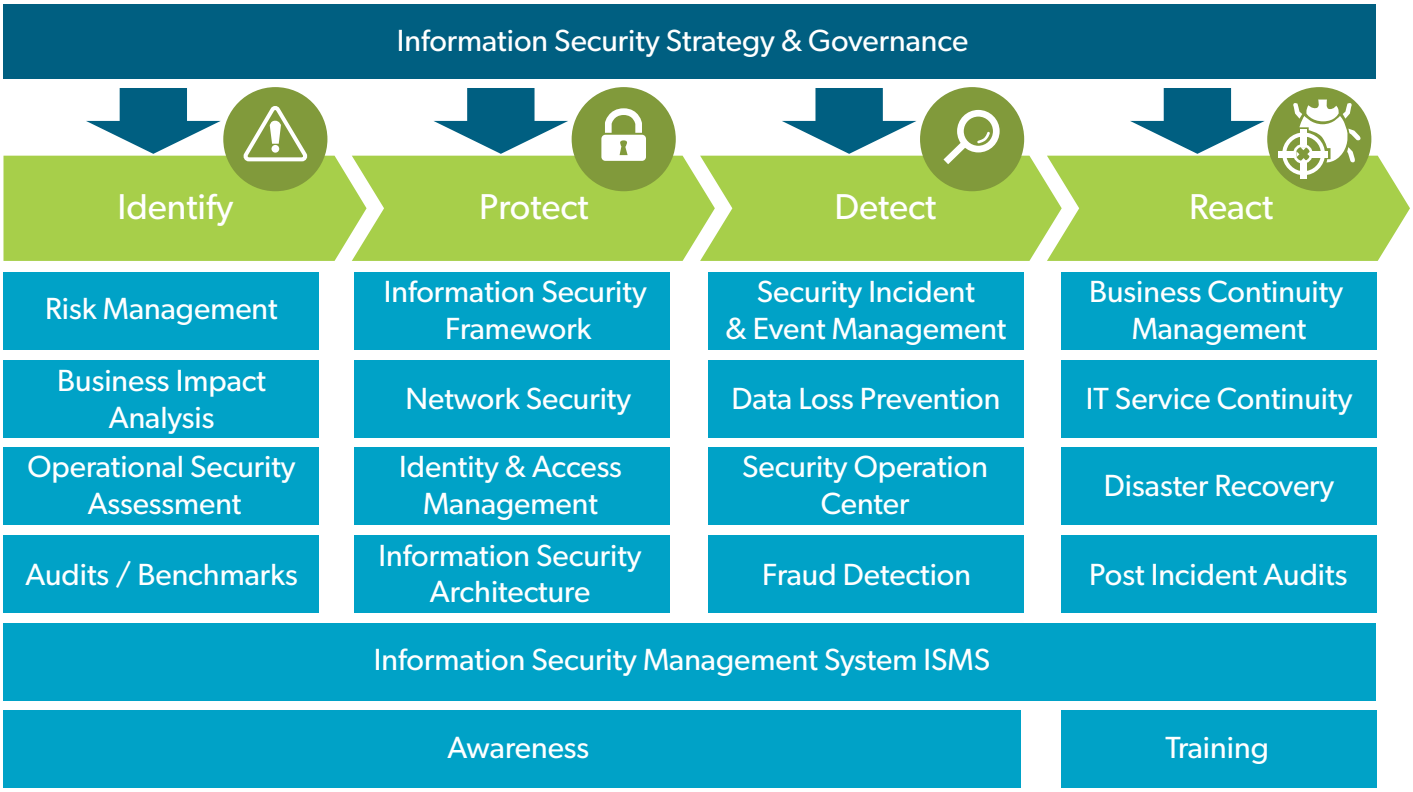

Abb. 1: Kompetenzen zur Sicherung von Digital Trust

struktur auf den Schutz geschäftskritischer Informationen lenken. In der Vergangenheit konzentrierten sich Investitionsentscheidungen auf den Schutz der IT-Infrastruktur. Von Mainframes auf Servern zu Desktops: War die Technologie sicher, war das Unternehmen sicher. Diesen Ansatz erachten wir als überholt. Mehr denn je ist heute ein «Security by Design»-Ansatz gefragt, so dass Hard- und Software bereits in der Konzeptions- und Entwicklungsphase möglichst unempfindlich gegen Angriffe gestaltet werden. Unserer Erfahrung nach ist das zwar auch bei agilen Entwicklungsmethoden herausfordernd, aber erfolgreich umsetzbar.

Für den Schutz kritischer Geschäftsergebnisse – bei Unternehmen die Kernprozesse und die damit erzielte Rentabilität, bei der öffentlichen Hand die Erfüllung öffentlicher Aufgaben – muss die Linie über eine Risiko- und Sicherheitsstrategie verfügen.

Nicht-IT-Führungskräfte behaupten gerne, dass IT-Risiko und -Sicherheit technische Probleme sind, und delegieren deren Lösung an die IT. Informationssicherheit kann jedoch nur in enger Zusammenarbeit mit der Linie erreicht werden.

- **Detektion und Reaktion statt 100%-iger Schutz**
  Die eigenen digitalen Assets zu schützen wird schwieriger: Angriffe werden raffinierter und die Zahl an Schnittstellen und Endpunkten der eigenen IT-Infrastruktur steigt. Das Ziel muss sein, ein Eindringen möglichst rasch zu erkennen und darauf zu reagieren. Benötigt werden also Fähigkeiten zur Detektion eines Angriffs, aber auch Mittel zur Verhinderung von Ausbreitung und Datenabfluss.

- ***IT Continuity & Business Continuity Management* sind wichtiger denn je**
  Neben klassischen Sicherheitsanalysen (mit Fokus auf Datenschutz und -sicherheit) sowie Ausfall- und Abhängigkeitsanalysen (mit Fokus auf der Fortführung der Geschäftstätigkeit) wird es künftig darum gehen, Menschen, Organisationen und die Gesellschaft vor autonomen Systemen mit Fehlfunktionen aller Art zu schützen. Dazu müssen die Unternehmen im Rahmen einer Risikoanalyse sämtliche kritischen Geschäftsprozesse aufspüren und für diese ein entsprechendes Notfallmanagement aufsetzen.

- **Mensch statt Technik im Mittelpunkt der Sicherheit**
  Untersuchungen zeigen, dass die meisten Gefährdungen der Informationssicherheit von innen, also den Mitarbeitenden selbst ausgehen. Erst wenn Informationssicherheit als unternehmensstrategische Aufgabe erkannt wird, entwickeln die Mitarbeitenden eine ausreichende Sensibilität für dieses Thema.