IT-Sicherheit als Marktchance

Wie aus notwendigen Investitionen Geschäftsmodelle entstehen können

Wir alle wollen Sicherheit. Sicherheit ist wichtig für das Überleben. Das gilt sowohl für Menschen, als auch für Unternehmen und Organisationen. In unserem Wirtschaftssystem und den bisherigen politischen und gesellschaftlichen Entwicklungen sind wir in den letzten Jahrzehnten relativ gut gefahren. Gut war meist gut, und schlecht war meist schlecht. Unsere Welt war halbwegs in Ordnung, auch, weil die Systeme einigermaßen transparent waren und wir die Mechanismen dahinter verstanden haben. Dies ändert sich gerade.
Wir sehen verstärkt, dass gut und schlecht oft eine – in vielen Augen unheilige – Allianz eingehen. Wir wollen Convenience und bezahlen mit Daten, von denen wir nicht wissen, was damit passiert. Wir kennen die Gefahren durch virtuelle Bedrohungen, schützen aber – oft aus Bequemlichkeit und Kostengründen – unsere privaten und betrieblichen Systeme nur unzureichend.

Menschen und Unternehmen sind angreifbarer, je unsichtbarer die Angriffe sind

Unternehmen sind aber zunehmend gefordert, hier aktiv zu werden, denn die größten Gefahren für den langfristigen Unternehmensbestand sind oft nicht mehr weniger Kunden oder neue Konkurrenten, sondern Viren, Trojaner und SpyWare. Große Unternehmen stellen inzwischen mehrere hundert Angriffe pro Tag auf ihre Server fest, fast alle werden glücklicherweise abgefangen. Aber geplante Angriffe (wie im Jahr 2017 „WannaCry“ oder aktuelle Sicherheitslücken in Computerchips, wie Spectre und Meltdown) hinterlassen Spuren und können sehr bald zu ernsten Gefahren werden und ganze Unternehmen bedrohen.

Natürlich reagieren Unternehmen darauf, verstärken ihren Schutz und bauen noch höhere virtuelle Mauern. Dahinter stehen oft immens hohe Kosten, die aber in einer virtuellen Welt fast achselzuckend hingenommen werden, oder sogar als „Bürde“ aufgefasst werden, die einem nicht nur Hacker, sondern auch (gutgemeint) die EU- oder nationale Gesetzgebungen auferlegen. Mit dieser Argumentation gerät IT-Sicherheit schnell in die Kategorie von Dingen, die man tun muss, aber nicht unbedingt tun will.

Von Herausforderungen zu Chancen

Wenn der Wind bläst, kann man Mauern oder Windränder bauen, lautet sinngemäß ein alter chinesischer Aphorismus. Auf IT-Sicherheit übertragen bedeutet dies nichts weiter, als zu versuchen, das Notwendige mit dem Nützlichen zu verbinden. Warum also nicht die zunehmenden Investitionen in IT-Sicherheit in andere Geschäftsmodelle integrieren und die eigenen Anstrengungen offensiv kommunizieren?

Wir sehen seit einigen Jahren einen Rückgang des Vertrauens in Unternehmen und Institutionen. Allein aus Marketingsicht ist dies sehr kritisch, denn Marken leben von Vertrauen. Ein wesentlicher Grund hierfür ist auch im intransparenten Umgang mit Daten zu sehen. Vertrauen muss also generell zurückgewonnen werden und warum sollte man dafür nicht die Investitionen in IT-Sicherheit nutzen?

Unternehmen, die sich schützen, schützen damit auch fast immer die Daten der Kunden, und dies wird zunehmend zu einem Verkaufsargument. Konsumenten haben wesentlich weniger Probleme, ihre Daten preis zu geben, wenn transparent dargelegt wird, wie diese behandelt und geschützt werden. Interne IT-Sicherheit wird damit zu einem extern nutzbaren Marketinginstrument.

Ansätze zur Umsetzung

Die Ansätze hierzu liegen in drei zentralen Bereichen:
(**a**) **Data Collection** – wie erhebe ich Daten und wie lagere ich diese Assets der Kunden? Sind sie von außen angreifbar? Kann ich mich als Kunde dagegen wehren, wenn beim Unternehmen „eingebrochen“ wird?
(**b**)**Data Analysis** – wie aggregiere ich die Daten der Kunden, wie analysiere und nutze ich sie? Hier ist zu beachten, dass dieser Schritt oft von externen Partnern durchgeführt wird. Wenn man als Unternehmen Daten an Agenturen gibt, wie sicher sind diese und wie schützen sich diese Agenturen?
(**c**) **Data Transfer** – was passiert mit Kundendaten? Werden sie (oder Teile davon) mit anderen Unternehmen geteilt oder an diese verkauft?
Wann und wie werden persönliche Daten wirklich gelöscht und sind damit für virtuelle Angriffe nicht mehr erreichbar?

Die Möglichkeiten, Windmühlen zu bauen, sind dabei nicht nur auf Kunden limitiert. So stellt z. B. die neue Datenschutz-Grundverordnung (DSGVO), die im Mai 2018 verpflichtend wurde, zwar hohe Anforderungen an Unternehmen, Mitarbeiterdaten zu schützen. Dies kann aber durchaus auch als ein Argument genutzt werden, fähige Fachkräfte anzuziehen. Denn wer möchte nicht auch lieber in einem Unternehmen arbeiten, das sorgsam mit internen und externen Daten umgeht und diese so gut wie möglich schützt?

Prof. Dr. Thomas Osburg

Prof. Dr. Thomas Osburg ist Professor für „Sustainable Marketing & Leadersgip“ und Dekan für „Automotive und Mobility Management“ an der Hochschule Fresenius in München. Daneben wirkt er als Direktor des internationalen Think Tanks „CircularKnowledge Institute“.

Mehr als 25 Jahre sammelte Prof. Osburg Erfahrungen in globalen IT-Unternehmen (Intel, Autodesk, Texas Instruments) und war in den Vereinigten Staaten, Frankreich und Deutschland für Marketing und Veränderungsmanagement verantwortlich.