SECURITY-OUTSOURCING

Informationssicherheit hat in der IT-Abteilung nichts verloren

Informationssicherheit geht weit über (technische) IT-Sicherheit hinaus. IT-Security muss ein Bestandteil der Informationssicherheits-Bemühungen eines Unternehmens sein.

WIEN – Die tatsächlichen Werte eines jeden Unternehmens sind Informationen, Informationen über Produkte, Kunden, Mitbewerb, Markt, Preise und vieles mehr. Der Verlust solcher Informationen bedeutet den Verlust des Wettbewerbsvorteils. Dies kann vom Entgang eines Auftrags bis hin zum völligen Ruin reichen.
Informationen sind mehr als reine Daten, die in Rechnern liegen, sie können sich auch auf Papier finden oder in den Köpfen der Mitarbeiter stecken. Darum muss sich die Sicherheit auch auf mehr als auf rein technische Maßnahmen stützen.
Die IT-Abteilung ist gewohnt, in technischen Lösungen zu denken, wodurch etliche Problemfelder übersehen werden. Informationssicherheit wird meist auf IT-Sicherheit beschränkt, oft sogar auf reine Netzwerksicherheit. Wenn das einzige Werkzeug ein Hammer ist, so wird jedes Problem zum Nagel. Alternative Lösungswege werden nicht gesehen. Etwa 20 Prozent einer Gesamtsicherheitslösung bestehen aus technischen Maßnahmen, der Rest sind organisatorische und persönliche Maßnahmen. Beschränkt sich ein Unternehmen auf IT-Sicherheit, so sind zwangsläufig riesige Lücken offen.

SICHERHEIT VERSUS KOMFORT

Die IT-Abteilung wird bei der Frage »mehr Features« oder »mehr Security« immer Ersteres wählen. Dies ist kein Vorwurf, dies ist die ursächliche Aufgabe der IT, sie soll ja die Geschäftsprozesse erleichtern. Mehr Security bedeutet auch für die IT Abteilung Behinderung im Alltag. Warum sollten persönliche Administrator-Accounts eingerichtet werden, wo doch mit *admin* oder *root* viel einfacher zugegriffen werden kann. Wozu in unternehmenskritischen Bereichen ein Vier-Augen-Prinzip etablieren, dies ist doch nur Overhead, Administratoren sind per se vertrauenswürdig und dürfen auf alle Daten zugreifen.
Informationssicherheit bedeutet aber auch eine Art Controlling-Funktion. Passieren alle Prozesse nach den eigenen oder gesetzlichen Vorschriften? Quis custodit custodes? Die IT sollte sich nicht selbst überwachen. In Unternehmen ist daher die IT-Abteilung der falsche Ansprechpartner für Informationssicherheit, für die ganzheitliche Sicht auf Security.
Compliance Anforderungen (vgl. 8. EU Richtlinie) drängen die Geschäftsleitung in immer größere Verantwortung, in persönliche Haftung bei Ungereimtheiten in finanziellen Unternehmensdaten. Dadurch wächst der Druck gerade auf die Geschäftsleitung, ein konsistentes Bild der Gesamtsicherheit des Unternehmens zu erstellen.

VERANTWORTUNG BEI DER GESCHÄFTSLEITUNG

Die Verantwortung für Informationssicherheit liegt definitiv bei der Geschäftsleitung, dies wird gerne übersehen. Die operative Tätigkeit im täglichen Geschäft sollte daher idealerweise als Stabsstelle angesiedelt sein, jedenfalls außerhalb der IT.
Ein eigener Beauftragter für Informationssicherheit (CISO) wird in der Literatur gefordert (vgl. BSI).
Dies wirft wiederum mehrere Probleme auf.
Das meiste (wenn auch einseitige) Know-how für Informationssicherheit sitzt in der IT-Abteilung. Um Bedrohungen einschätzen zu können, ist in der Regel tiefes technisches Wissen erforderlich. Unternehmen haben oft nicht genug Auslastung für einen Sicherheitsbeauftragten als Full-Time-Job. Ständige Weiterbildung ist essentiell – Bedrohungen ändern sich rasant – aber auch kostspielig.
Ein Sicherheitskonzept ausschließlich für IT-Security zu erstellen ist daher fahrlässig, da es eine trügerische Sicherheit vorgaukelt, aber andere wichtige Themen nicht behandelt werden (vgl. ISO 27001 u. ä.).
Ein eleganter Ausweg aus dieser Zwickmühle ist das Outsourcing der Funktion des Sicherheitsbeauftragten. Ein externer Dienstleister kann durch den Blick von außen, durch seine Erfahrung und durch Objektivität zusätzliche Elemente für das Unternehmen einbringen. Mit etwa einem Tag pro Woche ist dies eine kostengünstige, aber ausgesprochen effiziente Art, das Sicherheitsniveau zu steigern. Sicherheit bedeutet nicht immer nur höhere Kosten, Sicherheitsmaßnahmen steigern die Wettbewerbsfähigkeit, mindern das Unternehmensrisiko und verbessern das eigene Image.

UMFASSENDE INFORMATIONSSICHERHEIT

Informationssicherheit ist viel mehr als (technische) IT-Sicherheit. IT-Security muss ein Bestandteil der Informationssicherheits-Bemühungen eines Unternehmens sein. Ein externer Sicherheitsbeauftragter kann für das Unternehmen einen Mehrwert bieten, der sich mittelfristig auch finanziell niederschlägt.
Effizientere Prozesse, größeres Vertrauen der Kunden und der eigenen Mitarbeiter ins Unternehmen, schnelle und gezielte Reaktion bei Störfällen, all das schützt und unterstützt das eigentliche Geschäftsfeld des Unternehmens. ***[ws/el]***

ZUR PERSON

Dr. Wolfgang Schnabl bietet mit seiner Firma »Business Protection« seinen Kunden effizientes Informations-Sicherheits-Management. Outsourcing der Funktion des Beauftragten für Informationssicherheit bietet für die Geschäftsleitung eine kostengünstige Variante, um den vermehrten gesetzlichen Bestimmungen in diesem Bereich nachzukommen.
»Business Protection« bietet mit der Dienstleistung Rent-A-CISO anderen Unternehmen diesen Mehrwert.
www.rent-a-ciso.at.