4 Stunden für die IT-Sicherheit in Ihrem Unternehmen

Sie sind der IT-Leiter im Unternehmen und verantwortlich für den reibungslosen Ablauf aller geschäftlichen Vorgänge, die von der IT unterstützt werden? Also verantwortlich für den reibungslosen Ablauf ALLER geschäftlichen Vorgänge, denn was geht noch ohne IT?
Sie denken oft, heute ging es wieder drunter und drüber, zu viele Aufträge, zu viele Supportanfragen, zu viele Probleme?
Sie würden auf jeden Fall eine Strategie begrüßen, die Ihnen das Leben als IT-Leiter leichter macht?

Dann machen Sie doch einmal den IT-Sicherheitscheck mit Wolf-IT-Architekt. Hier geht es nicht nur um Cyber-Sicherheit, Datensicherheit, Zugriffsberechtigungen und sichere Passwörter. IT-Sicherheit ist ein Managementprozess und eine Strategie, die Sie nachts wieder ruhig schlafen lässt. Mit dem IT-Sicherheitsscheck sagt Ihnen Wolf-IT-Architekt, wo Sie ansetzen müssen.

Die Abbildung zeigt Ihnen eine Auswertung des Sicherheitsschecks, die für viele mittelständische Unternehmen typisch ist.

Organisation und Personal ist gut aufgestellt. Die Verantwortlichkeiten sind klar geregelt, Zugangs- und Zugriffsberechtigungen werden nach klaren Kriterien vergeben, die Administratoren sind in vollem Umfang ihren Aufgaben gewachsen, alle Mitarbeiter werden regelmäßig sensibilisiert und geschult. Dementsprechend läuft auch der **operative Betrieb** ziemlich reibungslos. Und wenn Sie den operativen Betrieb auf die einzelnen **IT-Komponenten** herunterbrechen, sieht das Bild ebenfalls akzeptabel aus. In der Regel laufen die PC-Arbeitsplätze, die (häufig virtualisierten) Server, die Router und Switches und die geschäftlichen Anwendungen auf diesen Systemen fast immer reibungslos.

Warum haben Sie dennoch schlaflose Nächte?

Schauen Sie auf den Erfüllungsgrad der Schichten „IS-Management“, „Konzepte“ und „Detektion und Reaktion“, der mit Hilfe des IT-Sicherheitschecks ermittelt worden ist. Hier gibt es Optimierungspotenzial.

IS-Management
Informationssicherheit ist Chefsache. Der Managementprozess muss von der Geschäftsleitung initiiert und mit Resourcen ausgestattet werden. Sein Erfolg muss regelmäßig überprüft und es muss ggf. nachjustiert werden.
Dazu sollte die Rolle eines IT-Sicherheitsbeauftragten etabliert werden, der den Sicherheitsprozess steuert und die Aufgaben koordiniert.
Sicherheitsleitlinien sollten erstellt und allen Mitarbeitern zur Verfügung gestellt werden. Jeder im Unternehmen muss über den Stellenwert der IT-Sicherheit informiert sein, und worauf es in seinem Arbeitsumfeld besonders ankommt.
Es sollten Sicherheitskonzepte schriftlich niedergelegt werden für alle geschäftlichen Abläufe.
Aller Mitarbeiter müssen die für sie relevanten Konzepte kennen und danach handeln.

Konzepte
Datensicherungskonzepte sind in der Regel vorhanden und nicht das Problem.
Ein durchgängiges Kryptokonzept fehlt aber häufig. Es werden nicht alle sensiblen Geschäftsbereiche integriert. Verschlüsselung und Datensicherung spielen oft nicht reibungslos zusammen.
Der Informationssicherheit auf Dienstreisen im In- und Ausland wird eine zu geringe Bedeutung beigemessen.
Die Sicherheitsanforderungen für das Vernichten von Datenträgern mit sensiblen Daten werden unterschätzt.

Detektion und Reaktion
Sicherheitsrelevante Ereignisse werden häufig nicht erkannt. Damit geht auch die Möglichkeit verloren, darauf frühzeitig zu reagieren, also noch bevor es „anfängt zu brennen“
Wenn ein Sicherheitsvorfall eintritt, sind die Unternehmen häufig nicht vorbereitet und können nicht kurzfristig reagieren. Dann beginnen die langen und stressigen Nächte und Wochenenden.
Es fehlt ein gut durchdachter und effektiver Katalog von Maßnahmen zur Bereinigung weitreichender Sicherheitsvorfälle. Hier spielen Experten im eigenen Unternehmen, aber auch externe Experten eine wichtige Rolle. Entsprechende Einsatzplanungen und Kontaktdaten sollte der IT-Sicherheitsbeauftrage in der Schublade haben.

Der IT-Sicherheitscheck von Wolf-IT-Architekt basiert auf dem Standard des BSI IT-Grundschutz Kompendiums, dass das BSI Anfang 2018 herausgegeben hat. Der Check wird als Interview durchgeführt und dauert ca. 4 Stunden.

Danach kenne Sie die Stärken und Schwächen der IT-Sicherheit in Ihrem Unternehmen. Danach können Sie die kritischen Bereiche gezielt optimieren -und bestimmt wieder besser schlafen.

Fragen Sie Wolf-IT-Architekt. Ich unterstütze Sie mit Kompetenz und Engagement.