bellco IT-SYSTEMHAUS
Marc Schröder & Kai von Ohlen GbR
Mühlenstraße 31, 27356 Rotenburg (Wümme)
Tel.: 04261-966306 / Fax: 04261-966307 / E-Mail: service@bellco.de

WESHALB UNTERNEHMEN EINE BASISPRÜFUNG BZW. AUDITIERUNG IHRER IT- UND INFORMATIONSSICHERHEIT DURCHFÜHREN LASSEN SOLLTEN

Für mich ist es immer wieder eine Gradwanderung Unternehmer und Geschäftsführer für dieses wichtige Thema zu sensibilisieren. Einerseits schüre ich ungerne die Ängste Anderer, Andererseits aber muss ich auf bestehende Gefahren hinweisen, welche zu erheblichen Schäden und Konsequenzen führen können.
Auch die gesundheitliche Vorsorge funktioniert nur, indem man die möglichen Risiken beschreibt, niemand geht gerne zum Zahnarzt, hier nennt man das „Prophylaxe".
Auch weiß ich, dass das Thema IT-Sicherheit und Datenschutz in deutschen mittelständischen Unternehmen äußerst „stiefmütterlich", meist aus wirtschaftlichen Gründen, behandelt wird und dies sich dringend ändern muss. Der beste Weg für eine neutrale Betrachtung und Bewertung der Gegebenheiten sind Fakten. Als Auditor gebe ich lediglich diese und Gesetze „zum Besten", verwechseln Sie dies bitte nicht mit meiner persönlichen Meinung.

Folgend nur ein paar Punkte, die den erforderlichen Handlungsbedarf erkennen lassen:

1. Nur 43% der Unternehmen in Deutschland sind ausreichend auf Cyberangriffe oder sonstige IT-Ausfälle vorbereitet, haben also kein wirksames Notfall- und Sicherheitsmanagement.
2. Nicht nur die persönliche Haftung der Unternehmer und Geschäftsführer ist spätestens mit dem Inkrafttreten der EU-DSGVO im Mai 2018 eine ernstzunehmende Entscheidungsgrundlage für eine wirksame IT- und Informationssicherheit.
3. In Deutschland entsteht jährlich ein wirtschaftlicher Schaden in Höhe von 50-60 Mrd. Euro (das sind knapp 2% des Bruttoinlandsprodukts) NUR durch Cyberkriminalität – steigende Tendenz. Zur Schadenseindämmung hat die Bundesregierung eigens hierfür eine Behörde ins Leben gerufen.
4. Gleich mehrere Gesetze bilden die Grundlage bei Entscheidungen für einen gesetzeskonformen Einsatz von IT in Unternehmen. Um nur ein paar zu nennen: EU-DSGVO (europäische Datenschutzgrundverordnung), IT-Sicherheitsgesetz, IT-Grundschutz, GoBD (Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung…), BDSG (Bundesdatenschutzgesetz), die Richtlinien des BSI (Bundesamt für Sicherheit in der Informationstechnik), z.B. die DIN_ISO 27001 als maßgeblicher Zertifizierungsstandard.
5. Die Grundlage für Datenschutz ist die IT-Sicherheit, wenn diese nicht gewährleistet ist (z.B. durch geeignete technische und organisatorische Maßnahmen), sollte man zu allererst diese umsetzen.
6. IT-Sicherheit und Datenschutz ist ein Prozess, kein Projekt, also fest zu integrierende Abläufe.
7. Auch die Versicherungswirtschaft verlangt „vermehrt" Nachweise über den Zustand interner Sicherungsmaßnahmen für die Risikobewertung von Versicherungsschutz in Unternehmen.
8. Jede Maßnahme, die die IT-Sicherheit und den Datenschutz betreffen, muss adäquat dokumentiert sein, um der gesetzlich verankerten **Nachweispflicht** und **Beweislastumkehr** zu entsprechen. Dies zu ignorieren wäre zumindest Fahrlässig und kann fatale Folgen haben.

Für eine branchenunabhängige Messbarkeit der informationstechnischen Sicherheit in Unternehmen ist die IT-Basisprüfung (wir nennen das auditQ) mittels einer Auditierung ein hervorragendes und kostengünstiges Instrument. Sie wird in Anlehnung an die DIN_ISO_27001 des BSI, der DSGVO und der IT-Sicherheitsgesetze durchgeführt. Sie beinhaltet 96-114 Fragen in 14 Prüfgruppen und ist Verfahrensakkreditiert.
Die Geschäftsführung erhält einen detaillierten Ergebnisbericht mit Maßnahmen- und Umsetzungsempfehlungen und einer zugeordneten Risikobewertung. Außerdem erhält das Unternehmen nach Abschluss ein Gütesiegel, welches als Nachweis benutzt werden kann. Gerne begleite ich Sie natürlich im Anschluss bei den durchzuführenden Umsetzungsmaßnahmen (z.B. erstellen und Führen eines unternehmensweiten Dokumentationsstandards).

Lassen Sie sich von mir in Angemessenheit einer sachlichen Risikobewertung beraten, damit Sie im Fall der Fälle agieren statt nur reagieren können. Für weitere Fragen stehe ich natürlich gerne zur Verfügung.