it-sicherheit stumm

Informations Sicherheit

rechtliche und wirtschaftliche Hintergründe

Warum eigentlich...

Informations-Sicherheit?

RISIKEN

Ohne Informations-Sicherheit gefährden Sie Ihre Existenz

Ein Ausfall der IT birgt Risiken, die häufig übersehen werden - bis die Situation plötzlich eintritt. Hier einige Beispiele:

- eingespielte Arbeitsabläufe werden gestört
- Produktion und Lieferung verzögern sich
- kein Kundenkontakt möglich, da Telefon-anlage und Email-Verkehr unterbrochen
- Rechnungen können weder eingebucht noch gezahlt - aber auch nicht erstellt! - werden

Die Folgen sind Umsatzeinbußen, unzufriedene Kunden und Strafzahlungen für Lieferausfälle. Kurz: der IT-Ausfall kostet Geld und vor allem Vertrauen.

Das wertvollste Kapital eines Unternehmens - Image und Geschäftsbeziehungen - ist gefährdet.

Informations-Sicherheit bedeutet Rechtssicherheit

Neben den wirtschaftlichen Risiken ist ein Unternehmen auch aus rechtlicher Sicht zur Informations-Sicherheit verpflichtet.

Zahlreiche gesetzliche Vorgaben fordern einen angemessenen Schutz Ihrer IT. Diese haben wir nachfolgend für Sie zusammen gefasst.

Wer die für sich zutreffenden gesetzlichen Bestimmungen nicht einhält, kann nicht nur Geld durch Bußgelder, Schadenersatz-forderungen oder teurere Kredite verlieren.

Auch das persönliche Vermögen und das Ansehen als Geschäftsführer stehen auf dem Spiel - das gilt übrigens auch für Bürgermeister!

Verfahren richten sich nicht nur gegen das Unternehmen, sondern auch persönlich gegen die verantwortliche Führung einer Organisation. Selbst Haftstrafen sind nicht ausgeschlossen.

Um diese Risiken zu vermeiden benötigen alle IT-Betreibenden ein rechtlich anerkanntes Management- System für Informations-Sicherheit.

ISO 27001 ist der internationale Standard, in Deutschland ist er als **IT-Grundschutz** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) etabliert.

Solch ein ISMS einzuführen bedeutet personellen und finanziellen Aufwand. Soweit richtig!

Aber: wir zeigen Ihnen, wo Sie Prioritäten setzen müssen, um Ihre Ziele möglichst effizient zu erreichen. Übrigens, geht es hier nicht nur um Zielerreichung, sondern auch um Perspektiven für die Zukunft, zum Beispiel zur Erschließung neuer Märkte oder für Investionen!

it-sicherheit stumm

Die Vorgabe, Informations-Sicherheit nachweisen zu müssen, leitet sich aus verschiedenen rechtlichen Grundlagen ab:

Datenschutzgesetz |

- Informations-Sicherheit ist als technische und organisatorische Maßnahme in den Datenschutz-gesetzen des Bundes und der Länder verankert. Ein Verstoß kann als Straftat gelten und Bußgelder, Schadensersatzansprüche und sogar Haftstrafen zur Folge haben.
  Verantwortlich ist die Geschäftsführung, und zwar persönlich.
- Aber vor allem: Ihre Kunden erwarten von Ihnen den sensiblen Umgang mit ihren Daten!
  Und Kunden sind Ihr größtes Kapital ...

Neue gesetzliche Anforderungen |

- Unternehmen, die die Grundversorgung sicher stellen (z.B. Energie, Wasser, Entsorgung, Banken, Krankenhäuser, Logistik, Banken, Telekommunikaton) müssen aufgrund des IT-Sicherheitsgesetzes ausreichende IT-Sicherheit gewährleisten.
- Alle anderen Unternehmen sollten dies aus Eigeninteresse tun. Nur so bleiben Sie auf Dauer wettbewerbsfähig. Fehlende Informationssicherheit kann also Ihre Existenz gefährden.

Zivilrecht |

- Wer IT betreibt, hat nach BGB die Verkehrsicherungspflicht: diese beinhaltet sowohl die Organisations- als auch die Aufsichtspflicht für den Umgang mit IT.
  Das bedeutet, es sind nicht nur Regelungen zu treffen, sondern auch ihre Einhaltung zu kontrollieren.
- Gemäß BGB ist die Geschäftsführung persönlich haftbar!
  Der Schadensfall kostet also nicht nur Geld, sondern auch Ihr Image ...

Risikomanagement |

- Risikomanagement ist nach KonTraG für mittlere und große Kapital-gesellschaften vorgeschrieben. Informations-Sicherheit ist ein Bestandteil des Risikomanagements.
- Wer kein Risikomanagement betreibt, steht dadurch nahezu automatisch in der Haftung bei Schadensfällen, denn die Beweislast liegt beim Unternehmen.

Innovation |

- Einige innovative Dienstleistungen, z.B. für Smart Metering, sind nur bei nachgewiesenem ISMS möglich. Sie sichern sich dadurch Zukunftsmärkte.
- Aber auch ohne gesetzliche Vorgaben können Sie durch ein funktionierendes ISMS flexibler auf neue Anforderungen reagieren. Weil Sie wissen, welche Risiken Sie vermeiden müssen.

Wirtschaftsprüfungen |

- IT-Sicherheit wird mitbetrachtet, fehlende IT-Sicherheit kann ein Testat verhindern.
- Auch wer nicht auf das Vertrauen der Finanzmärkte angewiesen ist, möchte sich nicht unbedingt dem Vorwurf nicht ordnungsgemäßen Wirtschaftens aussetzen.

Kreditvergabe |

- Bei Kreditvergaben sind Banken nach Basel II zur Risikobewertung verpflichtet (Stichwort „Rating“). Dabei ist nachweisbare IT-Sicherheit auch eines der Rating-Kriterien.
- Informations-Sicherheit vereinfacht und vergünstigt somit Kredite, mangelnde Informations-Sicherheit verteuert oder verhindert sogar die Kreditvergabe.

Leistungsnachweis |

- Der Nachweis eines ISMS kann z.B. bei IT-Dienstleistern den wiederkehrenden, internen Aufwand für die Auditierung durch Kunden reduzieren.
- Solch ein Leistungsnachweis dient aber auch immer mehr zu Werbezwecken und ist oft ein Verkaufsargument!

ANFORDERUNGEN

it-sicherheit stumm

Mein Name ist Stefan Stumm.

Nahezu seit Beginn meiner beruflichen Tätigkeit in 1989 bin ich mit IT-Sicherheit befasst.
Während meiner Zeit als Berater beim BSI (Bundesamt für Sicherheit in der Informations-Technik) habe ich den **IT-Grundschutz mit entwickelt**.
Als ich 1999 mein eigenes Beratungsbüro gründete, war der Schwerpunkt daher natürlich bereits gesetzt.

Zudem bin ich seit dem Jahr 2006 **BSI-lizenzierter IT-Grundschutz Auditor und Revisor**. Dabei gehöre ich zu den wenigen Auditoren, die über tatsächliche Prüfpraxis verfügen.

Aber vor allem sehen unsere Kunden uns als **praxisnahe Unterstützung bei der Konzeption** ihrer standardkonformen IT-Sicherheit. Der vorwiegende Teil unserer langjährigen Kunden sind Unternehmen aus dem Bereich der Ver- und Entsorgung, Krankenhäuser, Rechenzentren, Landes- und Kommunal-Behörden sowie mittelständische Unternehmen aus allen Branchen.

Und was können wir für Sie tun?

Hier einige Beispiele unserer Tätigkeitsfelder ...

Mit dem **ISC Initial-Sicherheits-Check** bieten wir eine günstige Einstiegsprüfung an, mit der die Bewertung Ihres IT-Sicherheits-Status an einem Tag ermittelt wird.

Unsere **Beratungen mit Workshop-Charakter** zu allen Grundschutz-relevanten Themen setzen zielgenau da an, wo Sie aus eigener Kraft nicht effizient weiter kommen - und zwar in dem Umfang, den Sie zu dem Zeitpunkt benötigen.

Viele dieser **Workshops** führen wir auch als zeitsparende, kostengünstige Veranstaltungen mit kleiner Teilnehmerzahl durch. Fragen Sie einfach nach den nächsten Terminen!

Als IS-Revisor übernehmen wir die externe **Revision** Ihrer Konzeption.
Sollten Sie keine Beratung wünschen, sondern lediglich einen vertrauenswürdigen Auditor suchen, stehe ich natürlich auch für ein **Audit** zur Verfügung.

Machen Sie sich auch unsere flexibel gestaltete und kundennahe Arbeitsweise zu Nutzen.

IT-Grundschutz in handlichen Paketen.

So wird die große Herausforderung der Einführung eines ISMS für Sie überschaubar, finanzierbar und somit real.

NEUGIERIG GEWORDEN ?

it-sicherheit stumm

Rochusstraße 16
50129 Bergheim

Mobil 0177 8072315
Fon 02238 303318
Fax 02238 303319

info@stumm-it-sicherheit.de
www.stumm-it-sicherheit.de