

IT-Security Policy

Heute sind alle Ihre Geschäftsprozesse in Applikationen abgebildet und sämtliche Daten sind elektronisch gespeichert. Diese Informationen müssen zuverlässig verfügbar sein – viele für Mitarbeiter, manche aber auch für Kunden und Lieferanten. Doch was bedeutet das organisatorisch? Wer darf wann, von wo, auf welche Daten zugreifen und was darf er mit diesen Informationen tun?

Die Sicherheitsanforderungen im Zeitalter von Internetkriminalität und hartem Wettbewerb werden immer höher. Wie erreicht man, dass Unternehmensinformationen gesichert sind? Reagiert man immer dann, wenn Schwierigkeiten auftreten? Wartet man ab, bis ein Budget vorhanden ist?

Das birgt die Gefahr, dass immer erst dann gehandelt wird, wenn schon Schäden entstanden sind. Das Ziel ist, im Vorfeld Schwachstellen zu erkennen, Risiken zu minimieren und einen Plan für den Notfall griffbereit zu haben.

Gehen Sie diese Problematik in Ihrem Unternehmen systematisch an. Erstellen Sie eine IT-Security Policy, die genau festlegt, was wann zu tun ist.

Was ist dafür erforderlich?

Die Sicherheitsziele Ihres Unternehmens müssen schriftlich fixiert werden, ebenso die Maßnahmen und Richtlinien zur Verwirklichung dieser Ziele. Jeder Mitarbeiter im Unternehmen muss wissen, was zur Wahrung der IT-Sicherheit vom ihm verlangt wird.

Fragen Sie sich gerade, wann dieses neben dem Tagesgeschäft passieren soll und wer diese Maßnahmen gut planen kann und soll?

>>>

Nutzen Sie in einem „moderierten Prozess“ mit BDG Synergien: Sie bringen Ihr Fachwissen ein und wir unterstützen Sie mit unserer Erfahrung und unserem Know-How. Definieren Sie gemeinsam mit unseren Beratern Ihre Sicherheitsziele und geben Sie die unternehmensspezifischen Inhalte vor.

Diese Policy wird Ihnen auch eine Entscheidungshilfe für die Projektierung neuer Anforderungen sein: Sie legen in der Security Policy fest, was Sie wann erreicht haben müssen und möchten. Selbstverständlich müssen diese Ziele, die Maßnahmen und ergänzende Richtlinien schriftlich niedergelegt werden. Die Geschäftsführung muss sich dieser Policy verpflichten und sie im Unternehmen kommunizieren.

Eine IT-Security Policy ist auch Bestandteil eines Information Security Management Systems, wenn Sie sich nach ISO 27001 oder BSI Grundschutz zertifizieren lassen möchten.

Der Nutzen einer Security Policy geht weit über die täglichen Anforderungen hinaus: Sie gibt Ihnen Investitions- und Planungssicherheit, definiert die Sicherheitsziele und Rahmenbedingungen für Unternehmen und macht so das erreichte Sicherheitsniveau prüfbar.

Um die Security Policy im Unternehmen zu kommunizieren und alle Mitarbeiter für IT-Sicherheit zu sensibilisieren, bietet BDG mit **beware!** ein webbasiertes Trainingsprogramm. Basierend auf **open beware!**, der frei verfügbaren Einstiegsversion des Trainings, entwickelt BDG auf die Security Policy angepasste Module und Inhalte sowie eine grafische Anpassung an das Corporate Design.

Wenn Sie Interesse an unserem Angebot haben, freuen wir uns über Ihren Anruf oder Ihre E-Mail an beratung@bdg.de, wir werden uns dann umgehend bei Ihnen melden. Gerne informieren wir Sie auch über unsere weiteren Beratungsdienstleistungen:

- Unterstützung beim Aufbau eines Information Security Management Systems (ISMS) und Begleitung einer Zertifizierung nach ISO 27001
- Erstellung eines Sicherheitshandbuchs sowie ergänzender Richtlinien und Fachanweisungen
- Erstellung von Risikoanalysen und Notfallkonzepten
- Incident Management
- Business Continuity Management
- Durchführung von Security-Audits