10 Fragen zur Informationssicherheit

1. Wann fand die letzte Informationssicherheits-prüfung in Ihrem Unternehmen statt?
2. Besitzen ihre Vermögenswerte einen angemessenen Schutz - heute wie morgen?
3. Liegt eine Definition Ihres angestrebten Informationssicherheitsniveaus vor?
4. Liegen Ihre Risiken alle innerhalb Ihres Toleranzbereichs?
5. Wird die Einhaltung Ihrer Unternehmenswerte kontrolliert?
6. Wie lauten die zuletzt durchgeführten Maßnahmen, um die Informationssicherheit in Ihrem Unternehmen zu erhöhen?
7. Befinden sich alle vertraulichen Unternehmensdaten im Unternehmensnetzwerk und können diese verschlüsselt werden?
8. Welcher war Ihr letzter Sicherheitsvorfall und wie wurde er behandelt?
9. Sind nur so viele Berechtigungen vergeben, wie Ihre Mitarbeiter zur Erledigung ihrer Aufgaben benötigen?
10. Besitzen Ihre Anwendungen alle den gleichen Schutzbedarf?

Das können wir für Sie tun

Planung

- Durchführung von Risikoanalysen u.a. nach ISO2700x-Standard, z.B. mittels IT-Sicherheits-auditierung
- Begleitung von Self-Assessments
- Bewertung und adressatengerechte Aufbereitung der Analyseergebnisse
- Unterstützung bei der Selektion geeigneter Maßnahmen und der Entscheidungsvorbe-reitung für das Management

Durchführung

- Die vereinbarten Vorgaben werden im Unternehmen umgesetzt, z.B. durch organisatorische Maßnahmen, Erarbeitung neuer Sicherheitskonzepte, Einführung geeigneter SW-, HW- oder Infrastrukturlösungen

Prüfung

- Die Maßnahmen werden hinsichtlich ihrer Zielrichtung und Wirksamkeit kontrolliert und erneut bewertet (Re-Assessment)

Handeln

- Auf Grundlage des Prüfergebnisses werden eventuelle Korrekturen eingeleitet

Vater Solution GmbH
Liebigstraße 26, 24145 Kiel

Telefon (0431) 20084 200
Telefax (0431) 20084 222
solution@vater-gruppe.de
www.vater-gruppe.de

vater
unternehmensgruppe

Informations-sicherheit

Kennen Sie Ihre Unternehmensrisiken?

vater
unternehmensgruppe

Mögliches Bedrohungsszenario Mittelstand

Rund um's Gebäude
Gebäude- u. RZ-Sicherheit
Asset Management
Netzwerksicherheit
Notfallplanung

Faktor Mensch
Informationssicherheitsstrategie
IT-Sicherheits-Audits
Awareness-Maßnahmen
Behandlung von Sicherheitsvorfällen

Informationssicherheit
Klassifizierung von Informationen
Umgang mit Datenträgern
Sondergenehmigungen

E-Mail und mehr
Sicherer E-Mail Verkehr
Virenschutz
Prevention vor Datenverlust

Daten überall
Internetnutzung
Mobile Computing
Telearbeitsplätze
Fernzugriff
Penetrationstests

Chancen und Risiken bestimmen den unternehmerischen Alltag. Je mehr Chancen genutzt und erfolgreich umgesetzt werden, desto größer ist der Wettbewerbsvorteil für ein Unternehmen. Wie sieht es allerdings mit den Risiken aus, ist z.B. die Bedrohungslage für Informationssicherheit nur ein Fall von Paranoia?

Zunehmende Datenpannen und damit drohender Imageverlust sowie grenzübergreifende Wirtschaftsspionage zwingen immer mehr Unternehmen ihre Sicherheitsstrukturen und -prozesse zu überdenken. Fragestellungen zum physischen und technischen Perimeterschutz, Zugriff auf Unternehmensdaten, Umgang mit Sicherheitsvorfällen sowie angemessenen Berechtigungsstrukturen sind häufig Anlass, sich um eine angepasste Informationssicherheitsstrategie Gedanken zu machen.

Die Optimierung des unternehmensinternen Sicherheitsmanagements führt oft vom reinen Grundschutzansatz zur risikoorientierten Steuerung. Die notwendige Risikoanalyse schafft die Möglichkeit die identifizierten Risiken innerhalb oder außerhalb des unternehmensspezifischen Toleranzbereichs zuzuordnen und damit eine zielgerichtete Risikominimierung und verlässliche Budgetsteuerung zu erreichen. Mittels definierter Risikokennzahlen wird ein transparentes Berichtswesen zur Lage der Informationssicherheit im Unternehmen geschaffen, welches die Weiterentwicklung, sowie das rechtzeitige Gegensteuern bei Fehlentwicklungen der Informationssicherheit ermöglicht.

	Workshop	Risikoanalyse	Erweiterte Risikoanalyse	Individuelle Beratung
Ziel / Inhalt	* Besprechung relevanter Handlungsfelder	* Identifikation und Einordnung von Risiken	* Identifikation von Risiken * Netzwerkpenetrationstest	* Auswahl spezieller Untersuchungsfelder
Ablauf	* Workshop	* Assessment * Interviews * Sichtprüfung	* Assessment * Interviews * Sichtprüfung * Pentest	* individuell
Ergebnisse	* ‚Landkarte` möglicher Informationssicherheitsrisiken * Vorläufige Einschätzung	* Tabellarische Zusammenfassung * Optional: Ausführliche Risikoanalyse	* Ausführliche Risikoanalyse inkl. Zusammenfassung des Ergebnisses Pentest	* Risikoanalyse über festgelegte Untersuchungsfelder
Dauer (Tage)	1-2	3-7	7-10	individuell
Ort	Kunde	Kunde / Vater	Kunde / Vater	Kunde / Vater