Checkliste Informationssicherheit

Allgemeines zum Schutz von Informationen

- ☐ Gibt es für Ihr Unternehmen einen IT-Sicherheitsbeauftragten?
- ☐ Haben Sie Ziele für Ihre Informationssicherheit definiert und wurden diese schriftlich fixiert?
- ☐ Berücksichtigen Sie diese Ziele bei allen neuen IT-Projekten?
- ☐ Haben Sie Sicherheitsmaßnahmen…
  - ☐ definiert?
  - ☐ schriftlich festgehalten?
  - ☐ priorisiert?
  - ☐ terminiert (einmalig, regelmäßig)?
  - ☐ mit Zuständigkeiten und Verantwortlichkeiten versehen?
- ☐ Wurden alle Mitarbeiter über diesen Maßnahmenplan und ihre Zuständigkeiten informiert und ist der Plan frei zugänglich? (z.B. in Form eines Mitarbeiter-Handbuchs)
- ☐ Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?
- ☐ Gibt es eine Übersicht über die wichtigsten Anwendungen und IT- Systeme?
- ☐ Haben Sie Installations- und Systemdokumentationen erstellt, die regelmäßig aktualisiert werden?
- ☐ Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen angepasst (z.B. Standard IP Adressen oder Passwörter bei Auslieferung)?
- ☐ Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?

Umgang mit E-Mail und Internet

- ☐ Ist flächendeckend Viren-Schutzsoftware im Einsatz?
- ☐ Gibt es eine Firewall und wird ihre Konfiguration und Funktionsfähigkeit regelmäßig überprüft?
- ☐ Setzen Sie eine Anti-Malware-Lösung ein…
  - ☐ für Ihre Endgeräte?
  - ☐ am Gateway - für den eingehenden Datenverkehr?
  - ☐ am Gateway – für den ausgehenden Datenverkehr?

Umgang mit E-Mail und Internet

- ☐ Haben Sie allen Systembenutzern (auch den Administratoren) Rollen und Profile zugeordnet?
- ☐ Gibt es Mechanismen, um Änderungen durch den Administrator nachzuvollziehen?
- ☐ Gibt es ein geregeltes Vorgehen beim Ein- und Austritt von Mitarbeitern, was Berechtigungen, Einweisungen etc. betrifft?
- ☐ Ist geregelt, auf welche Daten jeder Mitarbeiter zugreifen darf? Wurden Beschränkungen schriftlich definiert und an alle Mitarbeiter kommuniziert?
- ☐ Gibt es zentrale Sicherheitsrichtlinien für die Nutzung von…
  - ☐ Internet?
  - ☐ E-Mail?
- ☐ Kann Ihre Sicherheitslösung diese Richtlinien individuell für einzelne Mitarbeiter (z.B. Geschäftsführer), Gruppen (z.B. Minderjährige), Abteilungen (z.B. Vertrieb) und Standorte abbilden?
- ☐ Berücksichtigen Ihre Richtlinien den ein- und ausgehenden Datenverkehr – bei Bedarf auch unterschiedlich?
- ☐ Wurden diese Richtlinien schriftlich fixiert und alle Mitarbeiter darüber informiert?
- ☐ Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet?
- ☐ Bietet Ihre Sicherheitslösung automatisierte Alarmierungen über Verstöße?
- ☐ Wissen alle Benutzer, wie Sie sicherheitskonform handeln und Risiken bei der Nutzung von Internet und Email vermeiden?
- ☐ Sind Mitarbeiter in der Wahl sicherer Passwörter geschult?
- ☐ Wurde definiert und kommuniziert, wie mit gefährlichen Programmen (PlugIns) und aktiven Inhalten umgegangen wird?
- ☐ Wurden alle Benutzer darauf hingewiesen, dass eigene Programme oder Programme aus dem Internet nur mit Genehmigung heruntergeladen und installiert werden dürfen, oder wird dies durch eine Sicherheitssoftware gesteuert?
- ☐ Kann Ihre Sicherheitslösung den Verlust vertraulicher Daten per E- Mail oder über das Internet erkennen?
- ☐ Wie wird mit geblockten Inhalten oder Nachrichten in Quarantäne verfahren? Entscheidet allein die IT-Abteilung darüber, welche Informationen vertraulich oder unbedenklich, erwünscht oder unerwünscht sind? Oder gibt es Möglichkeiten, dies an befugte Personen/Abteilungen zu delegieren?
- ☐ Wurden WLAN-Verbindungen mit einem speziellen Netzwerkkennwort gesichert?
- ☐ Ist auf den WLAN-Komponenten die WPA-Verschlüsselung aktiviert und sind zusätzliche Authentifizierungsmechanismen aktiviert?
- ☐ Nutzen Sie Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung?
- ☐ Sind diese Mechanismen für Rechner, Programme, Anwendungen und ggf. für Internetkommunikation aktiviert?
- ☐ Kann Ihre Sicherheitslösung den Inhalt von verschlüsseltem Datenverkehr auf Gefahren scannen? Oder wird er ungeprüft durchgelassen?

Archivierung, Wartung und Backup

- ☐ Werden vertrauliche Informationen sicher verwahrt?
- ☐ Werden Arbeitsplatzrechner durch automatische Sperrung und Bildschirmschoner gesichert?
- ☐ Löschen Sie vertrauliche Informationen von Datenträgern oder Systemen bevor diese extern gewartet oder repariert werden?
- ☐ Wurde für Systeme und mobile Endgeräte definiert, welche Daten wie lange archiviert werden müssen/dürfen?
- ☐ Haben Sie Sicherungs- und Rücksicherungsverfahren dokumentiert?
- ☐ Werden Sicherheits-Updates regelmäßig oder automatisch eingespielt?
- ☐ Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?
- ☐ Gibt es ein Testkonzept für Softwareänderungen?
- ☐ Gibt es eine Backup-Strategie?
- ☐ Sind Ihre Sicherheitssysteme ausfallsicher ausgerichtet?
- ☐ Greifen Sicherheitsmaßnahmen auch beim Ausfall einzelner Komponenten?
- ☐ Gibt es einen Notfallplan, in dem alle wichtigen Notfallsituationen (z.B. Virusbefall) mit Handlungsanweisungen behandelt werden?
- ☐ Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?
- ☐ Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?

Physische Sicherheit

- ☐ Sind Ihre IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall geschützt?
- ☐ Haben Sie den Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Besteht ein ausreichender Schutz vor Einbrechern?
- ☐ Werden Besucher und Handwerker in Ihrem Haus begleitet bzw. beaufsichtigt?
- ☐ Sind Hard- und Software in einer Inventarliste erfasst?