Checkliste: Faktor Mensch

Technische Lösungen wie etwa Firewalls oder Virenscanner reichen alleine nicht aus, um Unternehmen vor den Gefahren aus dem Internet, vor Datenverlust und unbefugtem Zugriff zu schützen. Wenn Mitarbeiter sorglos und nachlässig mit Daten, Programmen und Rechnern umgehen, helfen auch die besten technischen Schutzmaßnahmen nichts. Erforderlich ist ein grundlegendes Verständnis für die Bedeutung von IT-Sicherheit. Informieren Sie Ihre Mitarbeiter über mögliche Gefahrenquellen, damit sie lernen, sich richtig zu verhalten. Die Checkliste kann Ihnen dabei helfen.

Vorbereitung

Bevor Sie Ihre Mitarbeiter über mögliche Gefahrenquellen und den richtigen Umgang mit Daten informieren, sollten Sie sich in einem ersten Schritt selbst einen Überblick verschaffen, wo Risiken für Ihre IT stecken, und Richtlinien für ein „sicheres“ Verhalten der Mitarbeiter formulieren. Diese Richtlinien sind Anweisungen, die beschreiben, wie ein Mitarbeiter sich im Umgang mit der IT im Unternehmen verhalten soll. Halten Sie diese sehr knapp (manchmal genügt ein Satz) und verzichten Sie auf Fachkauderwelsch.

- ○ Haben Sie Ihre schutzbedürftigen Daten identifiziert, z.B. Personaldaten (Verpflichtung aus Datenschutzvorschriften), Kundendaten, kaufmännische Daten (z.B. Angebote, Rechnungen, Einkaufsdaten) und technologische Daten (z.B. Konstruktionsdaten, Fertigungsdaten)?
- ○ Haben Sie festgelegt, wer auf welche Daten Zugriff hat und haben muss bzw. soll (Liste)?
- ○ Haben Sie festgelegt, wer für welche Anwendungen autorisiert sein muss bzw. soll (Liste)?
- ○ Haben Sie (einfache) Benutzerrichtlinien erstellt?
    - □ Passwortrichtlinie (regelt z.B. Art, Erzeugung, Geheimhaltung und Erneuerung von Passwörtern)
    - □ Internetrichtlinie (regelt z.B. ob und wie das Internet genutzt wird, Browser-Einstellungen, Hoch- und Herunterladen von Daten und Software)
    - □ E-Mail-Richtlinie (regelt z.B. den Umgang mit bekannten und unbekannten Absendern, mit Anhängen und den Einsatz von Signaturen und Verschlüsselung)
    - □ Datenträgerrichtlinie (regelt z.B. den Einsatz, Art, Aufbewahrung, Verschlüsselung, Weitergabe und Löschung bzw. Vernichtung von Datenträgern)
    - □ Installationsrichtlinie für Hard- und Software (regelt, ob und wie Hardware und Software installiert werden)

- ☐ Zutrittsrichtlinie (regelt den Zutritt zu Betriebsgelände und Räumen für Personal und Betriebsfremde)
- ☐ Arbeitsplatzrichtlinie (regelt z.B. die Sperrung des PCs, den Verbleib von Unterlagen auf dem Schreibtisch auch bei kurzer Abwesenheit)
- ☐ Richtlinie für mobile Geräte (regelt z.B. die Nutzung, Aufsicht und Aufbewahrung, Anbindung an das Unternehmensnetz, Verschlüsselung und Wartung bzw. Updates mobiler Geräte)
- ☐ Richtlinie für externe Zugriffe (regeln z.B. den Zugriff auf das Firmennetzwerk von zu Hause oder unterwegs)
- ☐ Weitere

○ Haben Sie konkrete Verantwortlichkeiten für die Umsetzung der Richtlinien vergeben?

Kommunikation – Mitarbeiter richtig ansprechen

Am Besten lernt der, der es aus eigenem Interesse und mit Freude tut. Gefragt sind daher praktische, anschauliche Beispiele, die die Risiken im Unternehmen aufzeigen und Lösungen anbieten. Motivieren Sie Ihre Mitarbeiter, indem Sie sie aktiv beteiligen, einbinden und Verantwortlichkeiten vergeben.

- ○ Leben Sie als Chef das Thema IT-Sicherheit selber vor?
- ○ Wissen Sie, wieviel Ihre Mitarbeiter über IT-Sicherheit wissen?
- ○ Können Sie den Sinn der Richtlinien plausibel erläutern?
- ○ Haben Sie Ansprechpartner benannt, die Rückfragen von Mitarbeitern beantworten können?
- ○ Haben Sie Maßnahmen geplant oder getroffen, um die Richtlinien in Erinnerung zu rufen?
  - ☐ z.B. Plakate, wohldosierte Erinnerungsmails, Kontrollen
- ○ Haben Sie Maßnahmen geplant oder getroffen, um das IT-Sicherheitsbewusstsein zu vertiefen?
  - ☐ z.B. Schulungen, Hinweis auf Publikationen, Lernspiele

Weitere Informationen zum Thema Mitarbeitersensibilisierung finden Sie in unserem Flyer:

„IT-Sicherheit, Faktor Mensch – 10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk"

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: www.kmu-sicherheit.de

TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrusT entwickelte sich zu einem bekannten Kompetenznetzwerk und trägt seit 2011 die Bezeichnung „TeleTrusT – Bundesverband IT-Sicherheit e.V.“. Heute umfasst TeleTrusT mehr als 130 institutionelle Mitglieder. Die Mitgliederschaft setzt sich aus Industrie, insbesondere mittelständischen Unternehmen, Bundesbehörden, Forschungseinrichtungen und thematisch verwandten Organisationen aus Deutschland, Österreich, der Schweiz, Belgien, Frankreich und Großbritannien zusammen, was die allgemeine Bedeutung des Themengebietes IT-Sicherheit unterstreicht. TeleTrusT hat Gemeinnützigkeitsstatus. In Arbeitsgruppen zu aktuellen Themen der IT-Sicherheit und des Sicherheitsmanagements findet interdisziplinärer Erfahrungsaustausch statt. TeleTrusT äußert sich zu technischen, politischen und rechtlichen Fragen, organisiert Veranstaltungen und Veranstaltungsbeteiligungen und ist Trägerorganisation der „European Bridge CA“ (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates „TeleTrusT Information Security Professional“ (T.I.S.P.). Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Weitere Informationen finden Sie unter: www.teletrust.de