

Checkliste: Unternehmenswerte ganzheitlich schützen

Der Betrieb der IT im Unternehmen stellt hohe Anforderungen an Sicherheit, Zuverlässigkeit und hinsichtlich von Haftungsaspekten. Einige wichtige Maßnahmen können hier helfen, bereits im Vorfeld ganzheitlich Risiken zu erkennen, zu bewerten und mögliche Schäden vom Unternehmen abzuwenden.

Grundsätzlich zu berücksichtigende Maßnahmen

- Haben Sie festgelegt, welche Mitarbeiter sich um die Umsetzung und Aktualisierung eines Konzeptes kümmern sollen?
- Verfügen die Mitarbeiter über die entsprechende fachliche Eignung?
- Gibt es ein Vorgehen, um regelmäßig zu überprüfen, dass die Vorgaben aus dem Konzept auch eingehalten werden?
- Liegen für die von Ihnen eingesetzte Software auch gültige Lizenzen vor?
- Kennen Sie die vorgeschriebenen Aufbewahrungsfristen Ihrer Daten und haben Sie für deren Einhaltung (auch technisch) gesorgt?

Risiken und Bedrohungen erfassen

- Gibt es eine Übersicht über Ihre IT-Infrastruktur und aktualisieren Sie diese auch regelmäßig?
- Sind mögliche Bedrohungen, wie z.B. höhere Gewalt, vorsätzliche Handlungen, Fahrlässigkeit oder Fehlbedienungen in der Übersicht berücksichtigt?
- Haben Sie die Risiken unter Berücksichtigung der maximalen Schäden, der Eintrittswahrscheinlichkeit und der Sensibilität der Daten bewertet?
- Haben Sie zur Festlegung des Schutzbedarfes seriöse Quellen, wie z.B. die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI), zu Rate gezogen?
- Wurde ein Sicherheitsaudit von externen Spezialisten durchgeführt?

Wichtige Schutzmaßnahmen:

Sie sollten sich unter anderem auch folgende Fragen stellen:

- Sind Ihre Mitarbeiter in der Lage, die Bedrohungen und Risiken zu verstehen und ihre Verantwortung zu realisieren (ggf. durch Schulungen)?
- Haben Sie Maßnahmen zum Schutz der Infrastrukturen (z.B. Zugangsschutz zu Gebäuden oder einzelnen Räumen) getroffen?
- Gibt es verbindliche Vorgehensweisen bei der Zugriffskontrolle, der Wartung von Hard- und Software, der Inbetriebnahme neuer Systeme und der Datensicherung?
- Sind Notfallpläne für den Fall des Falles verfügbar (z.B. in Papierform)?

Weitere Informationen zum Thema Unternehmenswerte ganzheitlich schützen finden Sie in unserem Flyer:

„IT-Sicherheitskonzept erstellen - 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 Mitgliedschaft 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