

## Checkliste: Netzwerke sicher administrieren

Computer-Netzwerke sind die „Lebensadern“ des Unternehmens. Ihr Schutz und damit auch der Schutz der sensiblen Unternehmensdaten ist besonders wichtig. Auf die Administration, also die Verwaltung der Netzwerke, sollten Sie besonderes Augenmerk richten.

### Haben Sie eine Übersicht über Ihr Netzwerk?

- Haben Sie eine Skizze erstellt, in der alle Komponenten des Netzwerkes genau verzeichnet sind?
  - Arbeitsplatzrechner
  - Server
  - Switches
  - Router
  - Drucker
  - Mobile Geräte (z.B. Notebook, Smartphone)
  - Ggf. private Geräte, die betrieblich genutzt werden
  - Sonstige Geräte (z.B. Scanner, Messvorrichtungen)
- Haben Sie bei allen Geräten eingetragen,
  - wer ggf. daran arbeitet,
  - an welchem Platz (Raum) sie stehen,
  - wo die wichtigen Daten gespeichert sind,
  - welche wichtigen Daten dort gespeichert sind?

### Sind Ihre Netzzugänge geschützt?

- Haben Sie dafür gesorgt, dass Ihre Netzwerkanschlüsse gesichert sind?
- Stehen alle Netzwerkkomponenten (z.B. Switches, Router) an „sicheren“ Plätzen?
- Ist sichergestellt, dass Netzwerkdosen „unter Kontrolle“ sind (d.h. nicht angeschlossen oder am „sicheren Ort“)?
- Haben Sie auf allen Netzwerkkomponenten (z.B. Router, Firewall) die Standardzugangsnamen und Passwörter geändert?
- Haben Sie sichergestellt, dass Ausdrücke von Netzdruckern nur von autorisierten Personen eingesehen werden können?

- Haben Sie zusätzliche Maßnahmen ergriffen, um Server und Fileserver besonders zu überwachen (z.B. abgeschlossener Technikraum, regelmäßige Scans)?
- Ist Ihre Internetfirewall so eingestellt, dass nur die notwendigen Zugriffe erlaubt sind und überprüfen Sie die Einstellungen auch regelmäßig?
- Überprüfen Sie regelmäßig die Sicherheitseinstellungen der Browser?
- Beim WLAN:
  - Haben Sie überprüft, ob das WLAN ständig aktiviert sein muss?
  - Ist der „Rundfunkmodus“ deaktiviert?
  - Haben Sie die stärkste mögliche Verschlüsselung für das WLAN gewählt?
  - Haben Sie den Zugang zum WLAN nur für bestimmte Gerätekennungen (MAC-Adressen) freigegeben?

### **Haben Sie für einen Basisschutz gesorgt?**

- Haben Sie für jeden PC und für jedes mobile Gerät die Basisschutzmaßnahmen ergriffen, wie z.B.
  - Viren und Trojanerschutz installiert,
  - Personal Firewall installiert,
  - getrennte Administrator- und Benutzerkonten eingerichtet,
  - regelmäßige Updates der Anwendungs-, Betriebssystems- und Sicherheitssoftware organisiert,
  - regelmäßig die Sicherheitseinstellungen der Browser überprüft?

### **Weitere Informationen zum Thema Netzwerkverwaltung finden Sie in unserem Flyer:**

*„Netzwerke sicher administrieren - 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](http://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](http://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](http://www.teletrust.de)