

„Schaltzentrale“ Netzwerk

Computer-Netzwerke entwickeln sich immer mehr zu Schaltzentralen in Unternehmen. Sie sind die Lebensadern Ihres Unternehmens, in denen die wichtigen Unternehmensdaten fließen, wie z.B. digitale Informationen über Kunden und Lieferanten oder auch Konstruktionszeichnungen und Produktionsdaten, die für den Betrieb des Unternehmens unerlässlich sind. Darüber hinaus ist das Netzwerk eine Kommunikationszentrale, die Ihre Mitarbeiter miteinander verbindet und via Internet für den Zugang nach „draußen“, z.B. mit externen Geschäftspartnern, sorgt.

Netzwerke administrieren

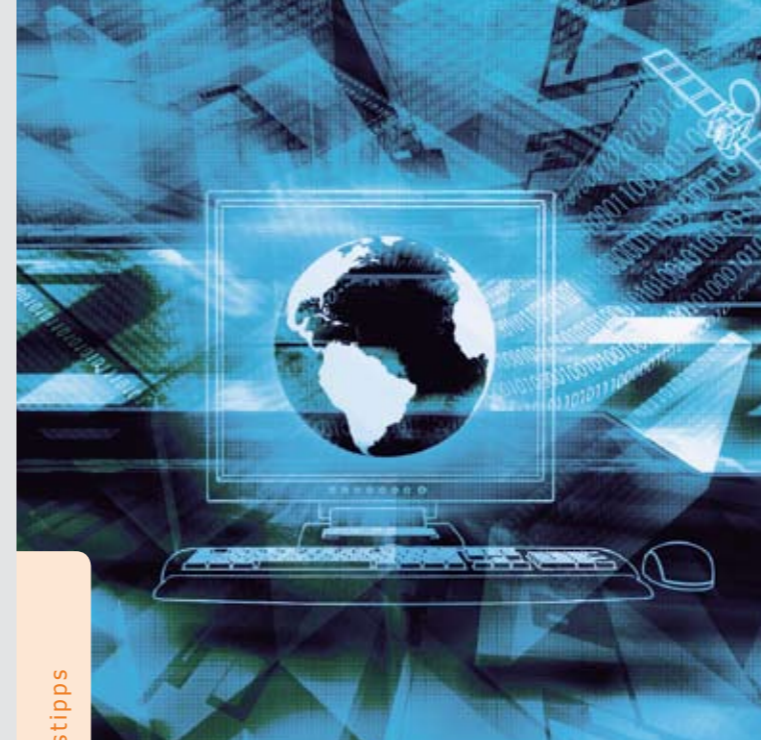
Was passiert, wenn die Netzwerke einmal ausfallen, sich technische Probleme einschleichen, Fehlbedienungen auftreten, oder sich Hacker von außen Zugriff verschaffen? Grundsätzlich sollten Unternehmensdaten nicht in falsche Hände geraten. Damit Ihr Netzwerk angemessen geschützt ist, dürfen nur diejenigen einen Zugriff auf die zum Teil sensiblen Daten haben, die es auch sollen und die die Daten zum Arbeiten unbedingt benötigen. Besondere Bedeutung kommt hierbei der Administration, also der Verwaltung, der Netzwerke zu.

Wir geben Ihnen an dieser Stelle einige grundsätzliche Tipps, um Ihr Netzwerk so zu administrieren, dass es sicher und zuverlässig funktioniert.



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.



Praxistipps

Aus der Praxis für die Praxis

Netzwerke sicher administrieren

10 Praxistipps für kleine und
mittlere Unternehmen und
das Handwerk

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages



TeleTrust

TeleTrust – Bundesverband IT-Sicherheit e.V. ist Partner des Begleitprojektes „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerkes Elektronischer Geschäftsverkehr und veranstaltet bundesweit „Stammtische“ rund um das Thema Informationssicherheit.

TeleTrust ist mit mehr als 130 Mitgliedern aus Wirtschaft, Wissenschaft und Verwaltung ein führendes Kompetenznetzwerk in Fragen der IT-Sicherheit in Deutschland und Europa.



Impressum

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.

Herausgeber:

TeleTrust – Bundesverband IT-Sicherheit e.V.,
Chausseestraße 17, D-10115 Berlin

Konzeption und Redaktion:

Hans-Joachim Bierschenk, Harald Kesberg

Grafik und Gestaltung:

Karl-Heinz Kottenhahn

Druck:

Buersche Druck- und Medien GmbH

Bildnachweis:

Danielle Bonardelle/Fotolia.com, Nmedia/Fotolia.com,
.shock/Fotolia.com

Stand: 12/2011

10 Tipps, die wirklich helfen

Wie können Sie Ihr Netzwerk zuverlässig administrieren?

10 grundlegende Praxistipps helfen Ihnen, Ihre Netzwerke zu planen und zu schützen.

Die Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen und dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Tipps rund um das Thema Datensicherung und Datensicherheit finden Sie unter www.ec-net.de und www.kmu-sicherheit.de.

Das Computer-Netzwerk ist eine sensible Schaltzentrale Ihres Unternehmens, das gut geplant und administriert werden sollte.



Wie plane und administriere ich mein Computer-Netzwerk?

Die Basis für die Sicherheit Ihres Netzes ist die Rechteverwaltung. Die hierfür zuständige Person ist der Administrator, der unumschränkte Rechte besitzt, um auf alle Systeme zugreifen zu können. Der Administrator eines Netzwerks, eines PCs oder einer Mehrbenutzer-Software ist zuständig für die Installation der Software und verwaltet die Benutzer (Konten anlegen und löschen, Rechte vergeben oder entziehen).

Das Administrator-Passwort ist als „Top Secret“ zu behandeln. Denn schlüpft ein Angreifer in die Rolle des Administrators bzw. erschleicht sich dessen Rechte, kann er tun und lassen was er will. Für die Administration sollten Sie entweder entsprechend ausgebildetes Personal haben oder externe Spezialisten hinzuziehen.

- + Tipp 1: Netzwerk planen**
Eine Administration beginnt mit einer Übersicht des vorhandenen oder geplanten Netzwerkes, damit Sie wissen, was Sie schützen müssen, und die richtigen Maßnahmen treffen können.
- + Tipp 2: Netzskizze anfertigen**
Zeichnen Sie eine Netzskizze mit Arbeitsplatzrechnern, Servern, Netzwerkkomponenten (Router, Switches, etc.). Tragen Sie bei jedem PC ein, wer daran arbeitet. Tragen Sie bei allen Geräten ein, an welchem Platz sie stehen und wo die wichtigen Daten gespeichert sind.

Wie schütze ich die Rechner in meinem Netzwerk?

Zunächst sollten Sie für jeden PC Basisschutzmaßnahmen ergreifen. Dazu gehören die Installation eines Viren- und Trojanerschutzes und einer „personal firewall“. Ein Benutzer sollte genau die Rechte haben, die er zur Erfüllung seiner Aufgaben braucht.



- + Tipp 3: Getrennte Benutzerkonten einrichten**
Richten Sie für jeden Nutzer eines PCs, Servers oder eines Softwaresystems eingeschränkte Benutzerkonten ein. Benutzen Sie das Administratorkonto nur zur Installation und Konfiguration.
- + Tipp 4: Firewall einstellen**
Prüfen Sie (als Administrator), ob die Einstellungen Ihrer „personal firewall“ Ihren Sicherheitsanforderungen genügen.
- + Tipp 5: Regelmäßige Updates durchführen**
Sorgen Sie für den aktuellen Stand der Betriebssystem- und Anwendungssoftware und führen Sie (Sicherheits-)Updates durch.

Wie schütze ich die Zugänge in meinem Netzwerk?

Mit einem offenen und unzureichend eingerichteten Netzwerk ist es prinzipiell jedem möglich, auf Ihre Daten zuzugreifen. Deshalb ist besonders auf den Schutz der Netzzugänge zu achten. Ein Netzzugang kann über das LAN (vom angeschlossenen PC oder Notebook), eine Funkverbindung (WLAN, Bluetooth, etc.) oder das Internet (über Ihren Router) erfolgen.

Schutz der LAN- und WLAN-Zugänge

Ein „Switch“ oder „Hub“ stellt die Verbindung zwischen den Rechnern des Netzwerkes untereinander her, der ggf. auch den Funkanschluss anbietet – eine lokale „Vermittlungsstelle“ für PCs.

- + Tipp 6: Netzwerkanschlüsse schützen**
Sorgen Sie dafür, dass Netzwerkanschlüsse nicht jedermann zugänglich sind. Daher stellen Sie Switches, Hubs oder Router niemals an frei zugänglichen Stellen auf (Flurbereich, etc.).

- + Tipp 7: Regelmäßig Passwörter ändern**
Ändern Sie regelmäßig auf allen Netzwerkkomponenten (z.B. Router, Firewall) die Standardzugangsnamen und Passwörter.
- + Tipp 8: WLAN absichern**
Aktivieren Sie das WLAN nur bei Bedarf und deaktivieren Sie den „Rundfunkmodus“. Wählen Sie für Ihren WLAN Zugang eine starke Verschlüsselung (z.B. WPA/PSK) aus und lassen Sie nur Ihnen bekannte Geräte zu.

Neben den PCs und Netzwerkkomponenten können im Netz noch weitere Geräte wie Server, Fileserver (NAS) und auch Drucker angeschlossen sein. Da sich auf Servern und Fileservern in der Regel gemeinsam genutzte Software und Daten befinden, bedürfen diese besonderer Aufmerksamkeit. Bei Netzdruckern ist sicherzustellen, dass die Ausdrücke (z.B. Personalakten) nur von autorisierten Personen eingesehen werden können.

Schutz des Internetzugangs

Der Internetzugang erfolgt über einen Router, hinter dem eine Firewall angeschlossen sein sollte. Oft sind die Funktionen in einem Gerät kombiniert (Firewallrouter).

- + Tipp 9: Internetfirewall einstellen**
Stellen Sie Ihre Internetfirewall so ein, dass nur die notwendigen Zugriffe erlaubt sind. Überprüfen Sie die Einstellungen regelmäßig und ziehen Sie ggf. einen Spezialisten hinzu.
- + Tipp 10: Browser-Einstellungen überprüfen**
Überprüfen Sie auch unbedingt regelmäßig die Sicherheitseinstellungen (Administrator) Ihres Browsers.