

# 10 Gebote der Internetsicherheit

für Unternehmen



# 10 Gebote der Internetsicherheit | Für Unternehmen

## 1 Etablieren Sie ein IT-Sicherheitsmanagement

Cyber-Angriffe machen immer wieder Schlagzeilen und sorgen für hohe finanzielle Schäden. Auch rechtliche Folgen und Reputationsverlust drohen betroffenen Firmen. Sichern Sie sich deshalb sowohl technisch als auch rechtlich gegen Angriffe ab. Eine professionelle Risikobewertung durch IT-Experten sowie eine zuverlässige Rechtsberatung unterstützen Sie dabei, die Datenschutzvorkehrungen in Ihrem Unternehmen den aktuellen Anforderungen anzupassen.

## 2 Verwalten Sie die Benutzerrechte Ihrer Mitarbeiter

Admin-Konten haben praktisch uneingeschränkten Zugriff auf Computer und Netzwerke. Sie können Software installieren oder Systemeinstellungen ändern. Viele Viren und Trojaner benötigen diese Admin-Rechte, um einen Rechner erfolgreich zu infizieren. Nicht jeder Mitarbeiter muss über weitreichende Berechtigungen verfügen, um seiner täglichen Arbeit nachzugehen. Erteilen Sie Benutzerrechte entsprechend der Aufgabenbereiche Ihrer Mitarbeiter und verhindern Sie so, dass Cyber-Kriminellen durch fahrlässiges oder böswilliges Handeln Tür und Tor geöffnet werden.

## 3 Setzen Sie eine Firewall ein

Unternehmen und Freiberufler mit schützenswerten Daten sollten für die Verbindung zum Internet eine professionelle Firewall verwenden. Sie schränkt unerwünschten Datenverkehr so ein, dass die Sicherheit Ihres Netzwerks erheblich gesteigert wird. Überprüfen Sie die Konfiguration der Firewall regelmäßig.

## 4 Setzen Sie eine professionelle Antiviren-Software ein

Prüfen Sie ausgewählte PCs regelmäßig mit einer Antiviren-Boot-CD. Auf der Firewall oder dem Gateway sollten mehrere Antiviren-Engines vorhanden sein.

## 5 Setzen Sie nur aktuelle Software ein

Software-Aktualisierungen (Updates) schließen gefährliche Sicherheitslücken in Betriebssystemen und Anwendungsprogrammen. Selbst kleinste Programmierfehler können es Kriminellen ermöglichen, wichtige Sicherheitsfunktionen zu umgehen und so u. a. Schadprogramme in Unternehmensnetze zu schleusen. Die meisten Software-Entwickler bemühen sich, Sicherheitslücken umgehend zu schließen und bieten regelmäßig kostenlose Updates für ihre Produkte an.

Stellen Sie sicher, dass in Ihrem Unternehmen ein zuverlässiges Update- und Patch-Management existiert. Mit veralteten Programmen gibt es keine Sicherheit!

## 6 Verzichten Sie auf ein WLAN-Netzwerk im Unternehmen

Vom WLAN-Einsatz in Unternehmen ist generell abzuraten. Sollten Sie nicht auf kabellose Netzwerke verzichten können, reicht eine standardisierte Verschlüsselung nicht aus. Professionelle EAPOL-Lösungen zur Authentifizierung sind unbedingt nötig.

# 10 Gebote der Internetsicherheit | Für Unternehmen

## 7 Sorgen Sie für Sicherheit beim Surfen & Mailen

Sollten Sie Terminalserver einsetzen, können Sie Ihren Mitarbeitern gesonderten Zugang zum Internet ermöglichen. So können Sie außerdem den Wartungsaufwand verringern und Ihre Infrastruktur zentral überwachen.

## 8 Gehen Sie vorsichtig mit E-Mails um

Bedenken Sie, dass Cyber-Kriminelle E-Mail-Absenderadressen spielend leicht fälschen können. Seien Sie stets misstrauisch und öffnen Sie E-Mail-Anlagen oder Hyperlinks nur, wenn Sie sich absolut sicher sind, dass sie tatsächlich vom angegebenen Absender stammen. Setzen Sie zuverlässige Verfahren zur E-Mail-Verschlüsselung ein, wenn schützenswerte Daten verschickt oder Rechtsgeschäfte per Mail durchgeführt werden.

## 9 Nutzen Sie das sicherste Zahlungsverkehrsverfahren

Für Einzelüberweisungen eignen sich besonders die Verfahren, bei denen ein TAN-Generator zum Einsatz kommt. Sammelüberweisungen sollten ausschließlich über signaturbasierte Verfahren wie EBICS oder HBCI mit Chipkarte durchgeführt werden. Sofern höhere Geldbeträge transferiert werden, sollten Computer, die für den Zahlungsverkehr genutzt werden, abgesichert und isoliert werden. Speichern Sie niemals Signaturen auf Computern oder im Netzwerk.

## 10 Machen Sie Ihre Mitarbeiter zu Sicherheitsexperten

Schaffen Sie ein nachhaltiges IT-Sicherheitsbewusstsein bei Ihren Mitarbeitern. Das erreichen Sie z. B. mit regelmäßigen Awareness-Maßnahmen oder einer nachhaltigen Awareness-Kampagne.



[facebook.com/8com.info](https://facebook.com/8com.info)



[www.8com.de](http://www.8com.de)



[www.8com.de/blog](http://www.8com.de/blog)



[www.awarenessshop.de](http://www.awarenessshop.de)



[xing.com/profile/Goetz\\_Schartner](https://xing.com/profile/Goetz_Schartner)