Die 10 Gebote der Internetsicherheit

1. Gebot: http://www.8com.de

Verbinden Sie Ihren Computer / Ihr Netzwerk niemals ohne Firewall / DSL-Router mit dem Internet.

Überprüfen regelmäßig die Konfiguration Ihrer Firewall / Ihres DSL-Routers.

Private Firewalls und kleine Unternehmensfirewalls können Sie kostenfrei unter www.8com.de prüfen lassen. Große Unternehmensfirewalls sollten regelmäßig professionell geprüft werden!

2. Gebot: http://www.8com.de

Surfen Sie niemals als administrativer Benutzer im Internet und/oder Senden oder Empfangen Sie E-Mails als administrativer Benutzer! Schadsoftware (Viren, Trojaner, BOTs) benötigen häufig „administrative“ Berechtigungen, damit sich diese auf ihrem Computer installieren können. Arbeiten Sie als Benutzer mit eingeschränkten Rechten und ein Großteil der Schadsoftware kann sich nicht auf ihrem Computer installieren!

Auch Administratoren dürfen niemals mit „administrativen Berechtigungen“ im Internet surfen oder E-Mails empfangen!

3. Gebot: http://www.8com.de

Setzen Sie nur aktuelle Software ein!

Alte Betriebssysteme und Anwendungssoftware *(z.B. Webbrowser, E-Mail Clients, Office Produkte, PDF-Viewer usw.)* sind meistens potentiell unsicher und können von Schadsoftware häufig einfach manipuliert werden. Achten Sie darauf, möglichst aktuelle Versionen zu verwenden.

Aktualisieren Sie permanent ihr Betriebssystem und ihre Anwendungssoftware mit den von ihrem Softwarehersteller angebotenen Sicherheitsupdates *(ggf. sollten Sie die Verträglichkeit der Updates prüfen)*. Vergessen Sie dabei auch nicht ihre Webbrowser, E-Mail Software, AntiVirus Software, PDF-Viewer, Picture-Viewer usw.

Bedenken Sie, ein einzelnes fehlendes Sicherheitsupdate kann dazu führen, dass trotz aktivierter Firewall und Antivirus Software Ihr Computer/Netzwerk gehackt wird!

4. Gebot: http://www.8com.de

Verwenden Sie eine professionelle AntiVirus Software für alle Computer (auch für ihre Server). Häufig finden Sie in Computerzeitschriften Testberichte gängiger aktueller Anti-Viren-Software-Pakte. Informieren Sie sich möglichst vor einer Neuanschaffung über die aktuelle Entwicklungen.

Empfehlenswert wäre ein sogn. „Internet Security Kit“ mit folgenden Bestandteilen:

- AntiVirus mit E-Mail Prüfung
- Anti-Spyware
- Rootkit Erkennung
- Anti-Spam
- Personal Firewall
- Boot-CD für “Offline Viren Scan des Betriebssystems“

Überprüfen Sie regelmäßig Ihren Computer mit der Antivirus Boot CD. Booten Sie dazu Ihren Computer von der Boot CD und führen Sie dann einen vollständigen Suchlauf durch!

5. Gebot: http://www.8com.de

Vorsicht vor E-Mail Anlagen!

Die meisten Schadprogramme (Viren, Trojaner usw.) gelangen immer noch per E-Mail auf die Computer der Opfer. Seien Sie vorsichtig beim Öffnen von E-Mail Anlagen. Bedenken Sie, dass heute sogar ein Foto (z.B. ein „jpg“), ein PDF-Dokument oder ein Video reicht, um ihren Computer mit Schadsoftware zu infizieren. Anders als früher, benötigt man heute keine ausführbare Datei – wie z.B. eine „exe“ oder „vbs“ mehr dazu!

Öffnen Sie nur E-Mail Anlagen von Absendern, denen Sie vertrauen!

Fallen Sie nicht auf angebliche Verträge oder „UPS-Zustellinformationen“ herein und öffnen Sie solche Anlagen nicht.

Verwenden Sie nur das Textformat für E-Mails

Verwenden Sie zum Lesen von E-Mails möglichst nur das Text-Format. Im HTML-Format kann sich gefährliche Schadsoftware verstecken!

Derzeit wird Schadsoftware zwar meistens per E-Mail Anhang verteilt, aber leider kann diese in einer HTML E-Mail im sogenannten E-Mail Body versteckt werden. In diesem Fall kann es schon ausreichen, dass Sie die E-Mail öffnen oder sogar nur in der Voransicht ansehen und die Schadsoftware kann sich unter Umständen auf Ihren Computer installieren.

Speziell hierfür sollten Sie eine einfache Schutzmaßnahme durchführen!

Stellen Sie Ihren E-Mail Client so ein, dass er E-Mail ausschließlich im "Textformat" anzeigt und nicht im "HTML-Format"!

6. Gebot: http://www.8com.de

Geben Sie niemals vertrauliche Daten weiter!

Online Betrüger versuchen auf verschiedenste Art und Weise vertrauliche Informationen (z.B. Kreditkarteninformationen, Online Banking Identitätsdaten wie PIN, TAN/iTAN usw.) von Ihnen zu ergaunern. Häufig setzen Online Betrüger dazu E-Mails ein. Diese E-Mails sollen vortäuschen, z.B. von ihrer eigenen Hausbank zu stammen. Sie werden in diesen E-Mails aufgefordert, vertrauliche Informationen bekanntzugeben! Mit diesen Informationen (z.B. PIN und TAN) werden die Betrüger dann versuchen, Ihnen Geld zu stehlen!

Vorsicht vor Betrügern!

Seien Sie prinzipiell misstrauisch, wenn jemand von Ihnen vertrauliche Daten anfordert. Ihre Bank/Sparkasse wird niemals nach Ihrer PIN und TAN fragen. E-Mails können heute leider sehr einfach gefälscht werden, so dass sie aussehen, als ob sie wirklich von Ihrer Hausbank stammen würden. Teilweise werden solche E-Mails auch vertrauliche Informationen über Sie enthalten, wie z.B. Ihren Namen und Ihre Bankverbindung, fallen Sie trotzdem nicht auf solche Betrüger rein!

Achtung!

Betrüger versuchen auch teilweise Ihnen vertrauliche Daten per Telefon und per Telefax zu entlocken!

7. Gebot: http://www.8com.de

Surfen im Internet stellt heute die größte Gefahr für Internetbenutzer dar.

Optimal wäre eine Auftrennung des Surfen und E-Mailen im Internet auf einen Computer und das Speichern von Daten und die Durchführung sensibler Transaktionen (z.B. Online Banking) auf einen zweiten Computer.

Alternativ können Sie eine Linux Boot CD für Ihren Computer verwenden und von dieser aus im Internet Surfen und E-Mails über Webmailer senden und empfangen (z.B. gmx.de, web.de, hotmail.com usw.).

Empfehlungen von Linux LIVE CDs:

- www.ubuntu.com
- www.knopper.net

Sie benötigen hierzu keinerlei Linux-Kenntnisse. Einfach den Computer von der CD starten (DSL/Kabelrouter ist eine Voraussetzung für die einfach Nutzung). Das Linux System startet dann von CD/DVD. Webbrowser öffnen und lossurfen! Selbst wenn Sie sich einen Virus oder ähnliches einfangen, beim Herunterfahren würde er automatisch entfernt werden!

Möchten Sie aber neben dem Arbeiten am Computer im Internet surfen? Dann wäre folgende Maßnahme ein sinnvoller Weg für Sie:

Erstellen Sie ein VMware oder Virtual PC Image und surfen Sie ausschließlich von diesem im Internet. Wichtig: Das Image nur über einen Player starten, so dass alle Änderungen automatisch zurückgesetzt werden.

Alternativ können Sie Ihren Computer über die Konfiguration Ihres Webbrowser absichern, aber bedenken Sie, dass diese Maßnahme nicht die Sicherheit eine Linux Boot CD oder eines Virtuellen Betriebssystem-Images erreichen kann.

Stellen Sie ihren Webbrowser auf SICHER!

Beim Surfen im Internet mit einem Webbrowser (z.B. Internet Explorer, Firefox Safari usw.) kann es vorkommen, dass Schadsoftware auf ihren Computer gelangt. Dazu kann es unter Umständen schon ausreichen, dass Sie eine Webseite öffnen, auf der sogenannte Schadsoftware hinterlegt worden ist!

Beachten Sie folgende Empfehlungen, um die Gefahren beim Surfen im Internet und beim Online Banking zu reduzieren:

1. Internet Explorer
    a. Verwenden Sie das Zonenkonzept vom Internet Explorer.
    b. Stellen Sie die Sicherheitsstufe für die Zone „Internet“ auf „Hoch“.
    c. Aktiviren Sie den „geschützten Modus“
    d. Beachten Sie, dass einige Webseiten, die gefährliche aktive Inhalte verwenden, jetzt nicht mehr vollständig dargestellt werden können. Handelt es sich um vertrauenswürdige Webseiten, dann fügen Sie diese zur Zone der „Vertrauenswürdigen Webseiten“ hinzu.
    e. Seien Sie bei Webseiten, bei denen „Dritte Personen“ eigene Inhalte wie z.B. Videos, Fotos oder auch nur Angebote (bei Auktionsplattformen) hochladen können sehr vorsichtig!

2. Firefox
    a. Der Firefox verfügt leider über kein Zonenkonzept. Die notwendige Sicherheit kann aber über das kostenfreie Add-On „NoScript“ für den Firefox Browser realisiert werden. Installieren Sie dies unbedingt!

Meiden Sie zweifelhafte Webseiten

Würden Sie freiwillig z.B. in Los Angeles/Kalifornien durch die Slums laufen? Normalerweise siegt hier der gesunde Menschenverstand und wir würden von dem Vorhaben absehen. Das gleiche gilt auch für das Internet. Nur existiert im Internet leider keine für uns Menschen sichtbare Grenze! Meiden Sie also unbedingt anrüchige oder dubiose Webseiten (z.B. Pornographie, Webseiten mit sogenannten Hacktools usw.).

Bedenken Sie eine weitere, aber sehr einfache Regel, die ihnen helfen wird, einen höheren Sicherheitsstandard im Internet zu erzielen:

Ein Gedanke vor dem Klick, das ist im Internet der Trick!

8. Gebot: http://www.8com.de

Installieren Sie niemals Software fragwürdiger Herkunft!

9. Gebot: http://www.8com.de

Schützen Sie Ihr WLAN!

Immer wieder dringen Kriminelle über WLANs in fremde Computersysteme ein und begehen Straftaten.

Beachten Sie, dass die WEP-Verschlüsselung innerhalb von 1-2 Minuten mit heutigen „Hack-Tools“ geknackt wird. Der Zugangsschutz über sogn. „MAC-Address-Filter“ kann innerhalb weniger Sekunden umgangen werden.

Verwenden Sie den Verschlüsselungsstandard WPA2 (notfalls WPA) – mit einem 63 Zeichen langen Kennwort!

10. Gebot: http://www.8com.de

Für Privatpersonen:

Informieren Sie sich regelmäßig im Internet über aktuelle Bedrohungen und Gefahren. Abonnieren Sie dazu z.B. unseren Newsletter unter www.8com.de.

Für Unternehmen:

Etablieren Sie ein IT-Sicherheitsmanagement in Ihrem Unternehmen

Immer mehr Unternehmen sind heute von einer funktionierenden IT abhängig. Im gleichen Zug nehmen die Kriminalisierung im Internet und die Ausnutzung der digitalen Angreifbarkeit von Unternehmen zu. Erpressungen von Unternehmen, Insolvenzen aufgrund von IT-Fehlfunktionen nehmen zu. Dauerhaft können sich Unternehmen nur dann sinnvoll gegen solche Bedrohungen schützen, wenn sie ein funktionierendes IT-Sicherheitsmanagement im täglichen Unternehmensablauf etablieren.

Führen Sie regelmäßig Security Audits / Penetration Tests durch!

Schlusswort

Die 10 Gebote der Internetsicherheit können nur dann den Sicherheitsstandard ihres Computers oder Ihres Unternehmensnetzwerkes sinnvoll erhöhen, wenn Sie auch alle 10 Gebote einhalten. Ähnlich wie beim Autofahren, kann Sicherheit nur durch „sichere Technik“ und entsprechendes Verhalten erzielt werden.

Haftungsausschluss

Die 10 Gebote der Internetsicherheit haben keinen Anspruch auf Vollständigkeit und können auch nicht garantieren, dass Sie damit 100%ige Sicherheit im Internet erlangen werden. Sofern Sie die Konfiguration ihres Computers nicht selbst durchführen können, empfehlen wir ihnen, Hilfe aus ihrem Freundes- oder Verwandtenkreis anzunehmen, oder einen professionellen IT-Dienstleister in ihrer Region damit zu beauftragen. Speziell für Computer und das Internet gilt folgende Aussage: „Wissen ist Sicherheit“. Bilden Sie sich regelmäßig fort. Häufig bieten Volkshochschulen sehr gute und kostengünstige Seminare zum Thema „Sicherheit im Internet“ an.

EDV Administratoren und IT-Spezialisten müssen professionell und regelmäßig fortgebildet werden. Hier reicht eine Fortbildung über die Volkshochschulen nicht mehr aus. Erkundigen Sie sich z.B. im Internet über die Qualität der angebotenen Fortbildungsmaßnahmen.