DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 89194 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung
Zwölf Maßnahmen zur Absicherung gegen Angriffe aus dem Internet

Viele Computer von Privatanwendern, die zum Internetsurfen verwendet werden, sind nicht ausreichend gegen die Risiken der Online-Welt geschützt. Kriminelle nutzen dies, indem sie solche Rechner mit Schadprogrammen infizieren und für ihre Zwecke missbrauchen. Dadurch können Ihnen erhebliche Schäden entstehen. Zum Beispiel können die Kriminellen Ihre Daten löschen oder ausspionieren, in Online-Shops Waren in Ihrem Namen und auf Ihre Kosten bestellen, Transaktionen beim Online-Banking manipulieren oder Ihnen den Zugang zu Ihrem Bankkonto sperren. Die Kriminellen können Ihren Rechner außerdem zum Teil eines Botnetzes machen und ihn so für Cyber-Angriffe auf Unternehmen oder andere Institutionen sowie zum Versand von Spam-E-Mails einsetzen.

Einen hundertprozentigen Schutz gegen diese Gefährdungen gibt es leider nicht. Um die Risiken jedoch weitgehend einzuschränken, können Sie selbst etwas tun. Wenn Sie die folgenden Maßnahmen umsetzen, dann erhöhen Sie die Sicherheit Ihres Rechners und Ihre Sicherheit im Internet bereits erheblich. Die ersten fünf Empfehlungen (**"Kernmaßnahmen"**) sollten Sie dabei in jedem Fall umsetzen. Die weiteren Empfehlungen sind **ergänzende Maßnahmen**, mit deren Umsetzung Sie Cyber-Kriminellen weniger Angriffsfläche bieten und präventiv dafür sorgen können, Ihre Internet-Sicherheit zu verbessern und mögliche negative Folgen zu mindern.

Alle Maßnahmen sind in der Regel auch für Laien einfach umzusetzen. Wenn Sie sich dies dennoch nicht zutrauen, dann sollten Sie einen Internet-Profi oder den Hersteller Ihres IT-Systems zur Rate ziehen, der Sie dabei unterstützen kann.
Hilfestellung bietet auch das Service-Center des BSI.

Telefon 0800 2741000
Kostenlos aus dem deutschen Fest- und Mobilfunknetz
Erreichbarkeit: Montag bis Freitag von 8:00 bis 18:00 Uhr
Oder schicken Sie eine E-Mail an: mail@bsi-fuer-buerger.de

Kernmaßnahmen

- Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte **Sicherheitsupdates** für Ihr Betriebssystem und die von Ihnen installierten Programme (zum Beispiel Internet-Browser, Office, Flash Player, Adobe Reader) – idealerweise über die Funktion "Automatische Updates". Diese Funktion können Sie in der Regel im jeweiligen Programm einstellen, meist unter dem Menüpunkt "Optionen" oder "Einstellungen".
- Setzen Sie ein **Virenschutzprogramm** ein und aktualisieren Sie dieses regelmäßig, idealerweise über die Funktion "Automatische Updates"
- Verwenden Sie eine **Personal Firewall**. Diese ist in den meisten modernen Betriebssystemen bereits integriert und soll Ihren Rechner vor Angriffen von außen schützen. Dazu kontrolliert sie alle Verbindungen des Rechners in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die aus dem Internet an Ihren Rechner gesendet werden.
- Nutzen Sie für den **Zugriff auf das Internet** ausschließlich ein **Benutzerkonto mit eingeschränkten Rechten**, keinesfalls ein Administrator-Konto. Alle gängigen

Betriebssysteme bieten die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten anzumelden. Wie Sie ein einfaches Benutzerkonto einrichten, ist hier erklärt: Microsoft Windows, Mac OS X, Linux, Linux Ubuntu

- **Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Seien Sie misstrauisch.** Klicken Sie nicht automatisch auf jeden Link oder jeden Dateianhang, der Ihnen per E-Mail gesendet wird. Überprüfen Sie gegebenenfalls telefonisch, ob der Absender der Mail authentisch ist. Wenn Sie Software herunterladen möchten, dann sollten Sie dies möglichst ausschließlich von der Webseite des jeweiligen Herstellers tun.

Ergänzende Maßnahmen

- Verwenden Sie einen modernen **Internet-Browser mit fortschrittlichen Sicherheitsmechanismen** wie etwa einer Sandbox. Konsequent umgesetzt wird dieser Schutz gegenwärtig zum Beispiel von Google Chrome. Zudem sollte der Browser über einen Filtermechanismus verfügen, der Sie vor schädlichen Webseiten warnt, bevor Sie diese ansurfen. Beispiele solcher Filtermechanismen sind der Smart Screen Filter beim Internet Explorer sowie der Phishing- und Malwareschutz bei Google Chrome und Mozilla Firefox. Darüber hinaus sollten Sie nur solche Browser-Zusatzprogramme wie Plugins und Add-ons verwenden, die Sie unbedingt benötigen. Weitere Empfehlungen zur sicheren Konfiguration Ihres Browsers hat das BSI hier für Sie zusammengestellt.
- Nutzen Sie möglichst **sichere Passwörter**. Verwenden Sie für jeden genutzten Online-Dienst – zum Beispiel E-Mail, Online Shops, Online Banking, Foren, Soziale Netzwerke – ein anderes, sicheres Passwort. Ändern Sie diese Passwörter regelmäßig. Vom Anbieter oder Hersteller voreingestellte Passwörter sollten Sie sofort ändern. Wie Sie ein sicheres Passwort erstellen können, haben wir hier für Sie beschrieben.
- Wenn Sie im Internet persönliche Daten übertragen wollen, etwa beim Online Banking oder beim Online Shopping, dann sollten Sie dies ausschließlich über eine **verschlüsselte Verbindung** tun. Jeder seriöse Online-Dienst bietet eine solche Möglichkeit an, beispielsweise durch die Nutzung des sicheren Kommunikationsprotokolls "HTTPS". Sie erkennen dies an der von Ihnen aufgerufenen Internetadresse, die stets mit "**https://**" beginnt und an dem kleinen Schloss-Symbol in Ihrem Browserfenster.
- **Deinstallieren Sie nicht benötigte Programme.** Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.
- Erstellen Sie **regelmäßig Sicherheitskopien "Backups"** Ihrer Daten, um vor Verlust geschützt zu sein. Hierzu können Sie beispielsweise eine externe Festplatte nutzen.
- Wenn Sie ein WLAN ("Wireless LAN", drahtloses Netzwerk) nutzen, dann sollte dies stets mittels des **Verschlüsselungsstandards WPA2** verschlüsselt sein. Wie Sie ein sicheres WLAN einrichten können, erfahren Sie hier.
- Überprüfen Sie in regelmäßigen Abständen den **Sicherheitsstatus Ihres Computers**. Eine schnelle Testmöglichkeit bietet die Initiative botfrei des eco-Verbands.

Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/Massnahmen_gegen_Internetangriffe.html;jsessionid=37959CDA3C53B3C51F5008BF47CD7734.1_cid369