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

Drive-By-Downloads, die Internetseite als Virenschleuder

Drive-by-Downloads: Die Internetseite als Virenschleuder

Sicherheitsbewusste Anwender vermeiden Internetseiten, die auch nur im Entferntesten gefährlich sein könnten. Doch auch das Ansurfen eines vermeintlich sicheren Webauftritts kann im Malware-Fiasko enden. Immer mehr Websites werden ohne Wissen des Betreibers von Hackern gezielt manipuliert und mit Malware bestückt. Der alleinige Besuch einer solchen Webseite reicht schon aus, um den eigenen PC zu infizieren. Dafür ist nicht einmal eine Benutzeraktion notwendig, wie beispielsweise das Starten eines Downloads. Diese sogenannten „Drive-by-Downloads" haben die E-Mail als häufigsten Verbreitungsweg von Malware inzwischen abgelöst.

Uhlemann empfiehlt:

1. Nutzen Sie immer die aktuelle Browser-Version!
2. Aktualisieren Sie alle Plug-ins wie beispielsweise den Flash Player oder den Adobe Reader. Zusätzliche Sicherheit bieten Browser-Erweiterungen, die (gefährliche) Skripte erst nach Freigabe durch den Anwender zulassen (NoScript für Firefox).
3. Selbstverständlich sollte Ihre Antivirensoftware (wie ESET) Web-Traffic und Web-Downloads überprüfen und Schädlinge sicher herausfiltern können.

USB-Sticks: Schnell mal einen Computer infizieren

Smartphones, Apple-Notebooks, Netbooks mit Linux und USB-Sticks: Viele Anwender setzen ihr privates Equipment auch gerne mal am Arbeitsplatz ein. Das Vorführen der aktuellen Urlaubsbilder vom USB-Stick oder das Synchronisieren von Outlook-Daten mit dem Handy führen jedoch schnell zum Virenbefall. Denn oftmals ist auf den mobilen Geräten keine Sicherheitssoftware installiert. Cyberkriminelle wissen das und missbrauchen mobile und/oder nicht Windows basierte Betriebssysteme als Überträger ihrer Malware. Die Schädlinge verbergen dabei die Anwesenheit vor ihrem „Wirt", der von ihrer Existenz nichts ahnt. Denn Apple oder Linux gilt gemeinhin als immun vor Viren. Dieser Irrglaube wird bestraft, wenn der Kontakt zum Windows-Netzwerk hergestellt ist und die eingeschleuste Malware ihre kriminellen Machenschaften startet.

Uhlemann empfiehlt:

1. Nutzen Sie Antivirensoftware auf allen Ihren Geräten. Vertrauen Sie nicht den Mythen, dass Mac-Rechner und Smartphones nicht gefährdet sind. Dies ist schlichtweg falsch.
2. Deaktivieren Sie die Auto-Run-Funktion in Windows, die angeschlossene Wechseldatenspeicher sofort öffnet und Malware in die Karten spielt.
3. Scannen Sie Ihren USB-Stick oder Speicherkarten regelmäßig auf Viren.