

«Drive-By-Infektion»

Information und Prävention



Drive-By-Infektion

Unter Drive-By-Infektion versteht man die Infektion eines Computers mit Malware (z.B. Viren, Trojaner) allein durch den Besuch einer Webseite. Das alleinige Ansurfen einer betroffenen Webseite genügt, um den Computer zu infizieren. Dabei werden Schwachstellen des Browsers oder dessen Plugins ausgenutzt.

Verwenden Sie zu Ihrem Schutz ein stets aktualisiertes Betriebssystem und aktualisierte Software (Browser, inkl. Plugins und anderer Programme).

Gefahr durch Drive-By-Infektion:

- Ein Computer wird alleine durch den Besuch einer verseuchten Webseite mit Schadcode infiziert, d.h. der Besucher braucht keinen Download zu starten oder explizit etwas zu installieren.
- Auch seriöse, bekannte und oft besuchte Webseiten könnten mit Schadcode infiziert sein.
- Firewalls bieten diesbezüglich keinen Schutz.

Am besten können Sie sich schützen, indem Sie:

- immer die aktuellen Versionen des Browsers sowie dessen Plugins (z.B. Adobe Flash Player, JavaScript etc.) verwenden
- das Betriebssystem sowie alle installierten Programme (z.B. Adobe Acrobat Reader) aktuell halten
- stets den Virenschanner aktualisieren
- regelmässig die Festplatte auf Viren überprüfen
- nach Möglichkeit die Skriptsprachen (JavaScript, ActiveX etc.) im Browser deaktivieren

Webseiten prüfen

Norton (Symantec) stellt auf der Webseite <https://safeweb.norton.com> einen Dienst zur Verfügung, mit welchem Sie den Status der Sicherheit (und allfällige Bedrohungen) bekannter Websites erfahren können.

Weitere Informationen: www.ebas.ch/drivebyinfection

«eBanking – aber sicher!» bietet E-Banking-Anwendern nützliche Sicherheitsinfos

eBanking aber sicher!

Auf der kostenlos zu nutzenden Webseite www.ebankingabersicher.ch finden Sie weitere praxisnahe Informationen über notwendige Massnahmen und Verhaltensregeln für eine sichere Anwendung von E-Banking-Applikationen.



Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz