Gefahren bei Online-Werbung und E-Mails

-Abwehrmöglichkeiten-

Inhalt:

Die Gefahren von Online-Werbung

2017 hat Google 112 Millionen Werbungen entfernt, die schädliche Software, Viren und Tracker installieren wollten, um die Online-Aktivität zu monitoren (zu verfolgen). Die Anzahl und die Frequenz solcher Werbung steigt jedes Jahr. Pop-ups spielen dabei eine gro0e Rolle.

Pop-ups sehen normalerweise wie unschuldige Werbung aus. Sie gehören meistens zur normalen Ausstattung von Webseiten, aber die wirklichen Absichten können auch schädlich sein.

Beispiel:

Schädliche Pop-ups sind unter anderem für nachfolgende Dinge verantwortlich:

- Installation von Spyware oder Ransomware
- Tracking der Online-Aktivitäten
- Installation von Malware

All das kann passieren, ohne dass man überhaupt auf die Werbung klicken musst. Die schädlichen Inhalte werden installiert, während sich die Seite lädt. Die Technik ist auch als Advertising bekannt.

Fachworterklärungen folgen.

Begriffsklärung

Ein **Pop-up** ist ein Element einer grafischen Benutzeroberfläche. In der Regel werden Pop-ups eingesetzt, um zusätzliche Inhalte anzuzeigen oder eine bestimmte Interaktion abzufragen. Typischerweise „springen“ Pop-ups auf und überdecken dabei andere Teile der Benutzeroberfläche.

Als **Spyware** (*Spähprogramm*, *Spionagesoftware* oder *Schnüffelsoftware*) wird üblicherweise Software bezeichnet, die Daten eines Computernutzers ohne dessen Wissen oder Zustimmung an den Hersteller der Software oder an Dritte sendet. Auch werden sie dazu benutzt, dem User über Werbeeinblendungen Produkte anzubieten.

Ransomware (*Erpressungstrojaner*, *Erpressungssoftware*, *Kryptotrojaner* oder *Verschlüsselungstrojaner)* sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.

Als Schadprogramm, Schadsoftware oder zunehmend als **Malware** bezeichnet man Computerprogramme, die entwickelt wurden, um, aus Sicht des Opfers, unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. (Auszug: Wikipedia)

Abwehrmöglichkeit: Werbeblocker

Als Werbeblocker (auch Werbefilter oder englisch ad blocker) wird ein Programm bezeichnet, welches dafür sorgt, dass auf Webseiten enthaltene Werbung dem Betrachter nicht dargestellt wird. Solche Werbung kann auf verschiedene Arten vorkommen, beispielsweise als Bilder, Videos, Texteinfügungen und Pop-ups. (Auszug: Wikipedia)

Beispiele für Werbeblocker


uBlock


AdGuard


Brave Browser


AdFender


Ghostery.

Der Webbrowser Opera hat einen eingebauten Werbeblocker.

Beispiel eines Werbeblockers

Adblock Plus ist eine Browsererweiterung für Mozilla Firefox, Google Chrome, Opera und Android zur Entfernung aller aufdringlicher Werbung, wie YouTube Video Werbung, Facebook Werbung, Banner, Pop-ups, Pop-unders, Hintergrundwerbung, etc.

Adblock ist ein sogenanntes Add-on und wird auch als solches installiert. Sie finden dieses nach der Installation z. Beispiel in Firefox in den „Einstellungen“ bei „Add-ons“.

Wie funktioniert Adblock Plus?
Um Werbung blockieren zu können, benötigt Adblock Plus sogenannte Filter. Standardmäßig kommt Adblock Plus ohne jegliche Filter aber es schlägt beim ersten Start eine Filterliste vor. Mit diesen Filtern kann es spezifische Anfragen von Webseiten blockieren, üblicherweise Anfragen zur Auslieferung einer Werbung.

Schadsoftware-Abwehr bei Webinhalten

Webinhalte stehen an zweiter Stelle der Infektionswege, E-Mails an der Spitze !

Abwehrmöglichkeiten:

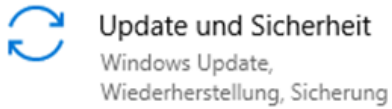
a) Die **Internet-Browser** (hier Firefox) bieten bereits Abwehrmechanismen.

Einstellmöglichkeiten hierzu finden sich im Menu „EINSTELLUNGEN“,
und dort in: 

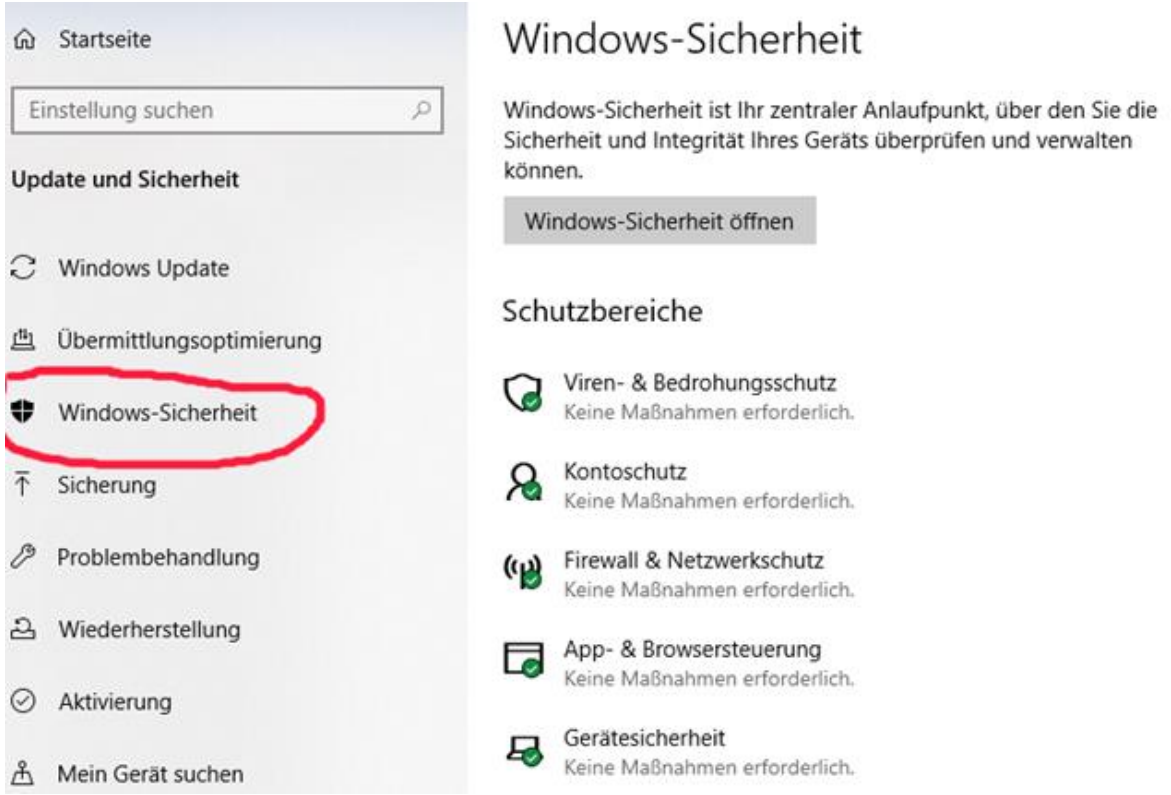
Hier können unter anderem eingestellt werden:
- Verbesserter Schutz vor Aktivitätenverfolgung
- Schutz vor betrügerischen Inhalten und gefährlicher Software
- „Nur-HTTPS-Modus“ Einstellung bietet eine sichere, verschlüsselte Verbindung zwischen Firefox und den von Ihnen besuchten Websites.

b) Besonders **Virenschutzprogramme** bieten umfassende Möglichkeiten zur Schadsoftware-Abwehr.

c) Beim **Betriebssystem** WIN 10 ist eine solche Abwehrmöglichkeit bereits an Bord.

Sie finden in „Einstellungen“: 

Dort können der Viren- und Bedrohungsschutz, Kontoschutz, Firewall und Netzwerkschutz, App- und Browsersteuerung und die Gerätesicherheit eingestellt werden.



Schadsoftware-Abwehr bei verdächtigen E-Mails

In verdächtigen E-Mails können auch zusätzlich zu den genannten Schadprogrammen Viren, Würmer, Trojaner und Phishing Mails und andere aktiviert sein!

Würmer - Sind Schadprogramme mit der Eigenschaft, sich selbst zu vervielfältigen, nachdem sie einmal ausgeführt wurden.
Phishing - Der Versuch an Ihre Zugangsdaten zu gelangen.
Trojaner - Sind Computerprogramme, die als nützliche Anwendungen getarnt sind, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt.

Betreiben Sie keinen Windows-Rechner ohne aktuelle Antiviren-Software mit aktuellen Virendefinitionen und aktuellen Sicherheits-Updates!

- Offensichtlich unseriöse Mails von unbekannten Absendern sofort löschen.
- Auch bei vermeintlich vertrauenswürdigem Absender misstrauisch sein. Absender können gefälscht sein oder dem Adressbuch eines infizierten Rechners entstammen.
- Öffnen Sie nur Dateien oder E-Mail-Anhänge, von denen Sie zweifelsfrei wissen, dass sie virenfrei sind.
- Öffnen Sie keine HTML-Dateien oder Bilddateien unbekannter Herkunft.
- Geben Sie niemals Passwörter oder andere Zugangsdaten weiter.
- Ändern Sie bei Betrugsverdacht sämtliche relevanten Passwörter.

Gefahren bei Online-Werbung und E-Mails -Abwehrmöglichkeiten-

Haben Sie noch Fragen ?

Kontaktieren Sie uns: compcaf-schoeckingen@posteo.de
oder Tel. 07156-3071972 (AB).

Wir sind persönlich für Sie da:
Jeden Dienstag von 15:00 bis 18:00 Uhr,
im Alten Rathaus in Schöckingen,
bitte melden Sie sich an.