Tipps gegen Malware, Phishing und Werbung in Windows

Was ist Malware?

Als Schadprogramm, Schadsoftware oder zunehmend als englisch **Malware** – malicious (bösartige) Software – bezeichnet man Computerprogramme, die entwickelt wurden, um, aus der Sicht des Opfers, unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Die Eingangstore für Malware sind hauptsächlich E-Mails und Webbrowser.

Die Schadfunktionen sind gewöhnlich getarnt, oder die Software läuft gänzlich unbemerkt im Hintergrund. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die technische Kompromittierung der Sicherheitssoftware und anderer Sicherheitseinrichtungen (wie z.B. Firewalls und Antivirenprogramme) eines Computers sein, aber auch das ungefragte Sammeln von Daten zu Marketingzwecken. Es ist bei mancher Malware auch üblich, dass eine ordnungsgemäße Deinstallation mit den generell gebräuchlichen Mitteln fehlschlägt, so dass zumindest Softwarefragmente im System verbleiben. Diese können möglicherweise auch nach der Deinstallation weiterhin unerwünschte Funktionen ausführen.

Software zum Schutz vor Malware

Diverse Ereignisse im Bereich Cybersicherheit haben grosse Aufmerksamkeit erregt und unsere Verwundbarkeit aufgezeigt. Die prominentesten Beispiele sind: Anhaltende Angriffswellen von Malware, welche alle Daten der Opfer verschlüsseln und nur gegen Bezahlung wieder freigeben («**Ransomware**»), Datenlecks mit Millionen von betroffenen Nutzerkonten (auch in der Schweiz), die den Missbrauch persönlicher Daten ermöglichen, sowie die anhaltende Flut von Schwachstellen in Software, die einen Angriff begünstigen.

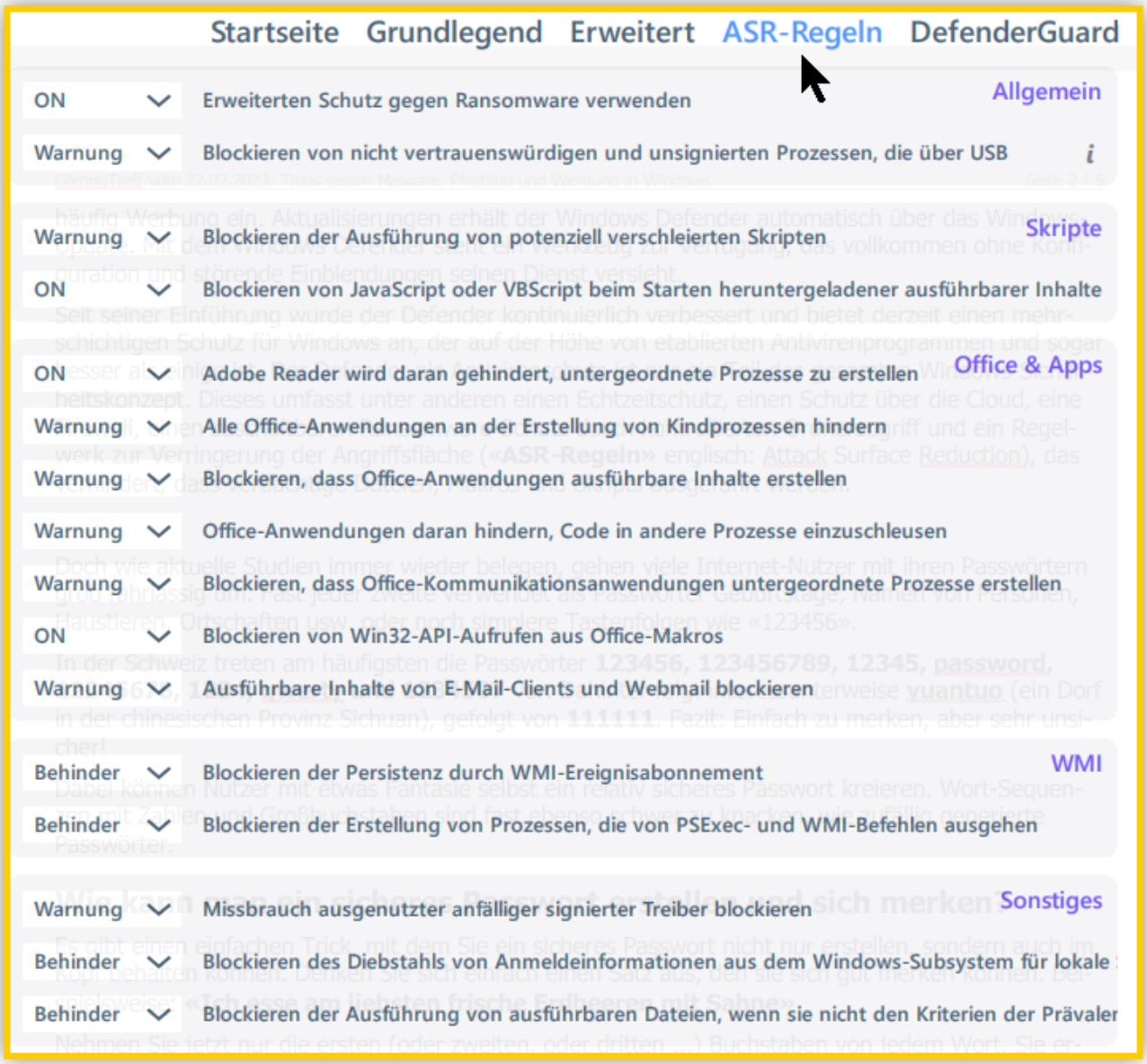
Die wichtigste Schutzbarriere zur Abwehr von Malware ist ein Antivirenprogramm. Davon gibt es duzende, sowohl kostenfreie als auch kostenpflichtige. Seit Windows 8 ist der Microsoft Defender in allen aktuellen Windows Versionen integriert und kostenlos einsetzbar. Trotzdem fragen sich viele Nutzer, ob sein Schutz ausreicht, oder ob sie besser einen anderen Virenscanner installieren sollten.

Der Defender bietet einen optimalen Schutz für Windows

Da der Defender fester Bestandteil des Betriebssystems ist, wird er nach der Installation von Windows automatisch aktiv und läuft immer im Hintergrund. Über das Windows-Update erhält er automatisch Aktualisierungen. Dabei ist das Tool sehr unauffällig. Andere Antivirenprogramme fallen durch Pop-Ups störend auf. Besonders kostenfreie Tools blenden häufig Werbung ein. Mit dem Windows Defender steht ein Werkzeug zur Verfügung, das vollkommen ohne Konfiguration und störende Einblendungen seinen Dienst versieht.

Seit seiner Einführung wurde der Defender kontinuierlich verbessert und bietet derzeit einen mehrschichtigen Schutz für Windows an, der auf der Höhe von etablierten Antivirenprogrammen und sogar besser als einige ist.

Der Defender als Antivirenschutz ist nur ein Teil des gesamten Windows-Sicherheitskonzepts. Dieses umfasst unter anderem einen Echtzeitschutz, besonders rasche Abwehrmassnahmen über die Cloud, eine Firewall, einen zuschaltbaren Ransomware-Schutz durch kontrollierten Ordnerzugriff und ein *Regelwerk zur Verringerung der Angriffsfläche* («**ASR-Regeln**», engl. *Attack Surface Reduction*), um die Ausführung von verdächtigen Dateien, Makros und Skripts zu verhindern.



Aus dem Gesagten sollten Antivirenprogramme, die nach der Windows-Einrichtung zur Installation angeboten werden (z.B. McAfee) abgelehnt werden. Werden solche Programme doch installiert, lassen sie sich nachher sehr schwer restlos deinstallieren. Ausserdem können sie oft Probleme bei Windows-Updates verursachen (Update kann nicht zu Ende ausgeführt werden, Systemabsturz, Verhinderung eines Neustarts, usw.).

Cyberkriminalität ist hier zu bleiben

Cyberkriminalität (engl. «**cybercrime**») bezeichnet alle Straftaten, die moderne Informationstechnik und elektronische Infrastrukturen (aus-)nutzen. Die fortschreitende Digitalisierung der Gesellschaft führt zu immer neuen IT-Anwendungen, die die Bandbreite der Gelegenheiten für Straftaten im Bereich Cyberkriminalität stetig anwachsen lässt. Zu den am weitesten verbreiteten Methoden von Cyber-Kriminalität gehören u.a.:

- Schadprogramme (und alle Unterarten)
- Identitätsdiebstahl
- Spam und Phishing
- Botnetze
- Social Engineering

Cyberkriminalität zielt meist darauf ab, informationstechnische Systeme mit Malware aktiv zu infizieren oder sich von gutgläubigen Menschen unfreiwillig hereinbitten zu lassen mit dem Ziel

- Zugangsdaten oder persönliche Daten auszuspionieren,
- Dateien und Daten zu verschlüsseln und Lösegeld zu erpressen oder
- die Kontrolle über das System zu übernehmen.

Es gibt keinen absoluten Schutz vor Cyberangriffen, aber es ist ratsam bei E-Mails stets wachsam zu bleiben, bereitgestellte Sicherheitsupdates immer umgehend zu installieren und einen aktuellen Virenschutz zu haben.

E-Mail als Eintrittstor für Cyberangriffe

In der heutigen Zeit ist die E-Mail als Kommunikationsmittel nicht mehr wegzudenken, sie ist zu einem unserer wichtigsten Instrumente der Kontaktnahme geworden. Leider nutzen auch Kriminelle immer wieder diesen Ansatz, um Einzelpersonen und Unternehmen erheblichen Schaden zuzufügen. Die meisten Schadprogramme werden als Anhang oder Link in einer E-Mail verteilt. Technische Massnahmen wie Antivirensoftware oder Spam-Filter können in den meisten Fällen eine Infektion verhindern. Leider können die Cyberkriminelle die Effektivität dieser Mittel durch die Verwendung von zufällig wechselnden Absenderadressen aushebeln. In solchen Fällen ist der E-Mail-Empfänger auf seine Wachsamkeit und seinen gesunden Menschenverstand angewiesen, um die Gefahr abzuwehren.

Aktuellen Untersuchungen zufolge werden weltweit täglich *fünfzehn Milliarden Spam-E-Mails* verschickt (mit «**Spam**» ist der *massenhafte Versand von unverlangten Werbemails gemeint*). Dabei handelt es sich bei *1 von 99 E-Mails* um einen Phishing-Versuch.

Phishing (engl. «**Password**» + «**fishing**») ist eine der populärsten Social-Engineering-Angriffsvarianten. Bei dieser Betrugsform wird per E-Mail, Textnachricht oder Anruf/Sprachnachricht das Ziel verfolgt, bei den Opfern ein Gefühl der Dringlichkeit, Neugier oder Furcht zu erzeugen, welches sie dazu verleitet, vertrauliche Informationen preiszugeben, auf Links zu bösartigen Websites zu klicken und Malware-verseuchte Anhänge zu öffnen.

Schutzmassnahmen gegen Phishing-Angriffe

Moderne Webbrowser und E-Mailprogramme verfügen über Schutzmassnahmen gegen Spam und Phishing. Leider werden diese durch den Einfallsreichtum der Cyberkriminellen sehr oft ausgehebelt und der Nutzer ist auf sich allein gestellt. Der beste Schutz vor Phishing-Angriffen besteht aus einer Kombination von **Wachsamkeit**, einem **gesunden Mass an Misstrauen** sowie einigen **praktischen Handlungsweisen** im Umgang mit E-Mails und dem Internet.

- Banken und seriöse E-Commerce-Firmen fordern **nie** per E-Mail, dass Sie vertraulichen Informationen preisgeben sollen. Löschen Sie solche Nachrichten sofort.
- Überprüfen Sie stets die Adressleiste in Ihrem Browser. Am besten tragen Sie die Adressen zu häufig besuchten Login-Seiten in die Favoritenliste Ihres Browsers ein
- Klicken Sie niemals auf Links in einer dubiosen E-Mail. Versuchen Sie im Zweifelsfall stattdessen, die im E-Mail-Text genannte Seite über die Startseite der betreffenden Organisation zu erreichen.
- Starten Sie niemals einen Download-Link direkt aus einer E-Mail heraus, von deren Echtheit Sie nicht hundertprozentig überzeugt sind. Laden Sie, wenn möglich, Dateien und Programme stets direkt von der Anbieterwebsite herunter.
- Prüfen Sie E-Mails mit Dateianhängen kritisch und öffnen Sie keine Anhänge, wenn Sie nicht von der Echtheit des Absenders überzeugt sind.
- Geben Sie keinesfalls vertraulichen Zugangsdaten wie Passwörter, Kreditkarten- oder Transaktionsnummern in ein E-Mail-Formular ein. Wenn Sie sich nicht sicher sind, ob eine E-Mail vielleicht berechtigterweise nach vertraulichen Daten fragt, fragen Sie am besten telefonisch bei dem genannten Anbieter nach.
- Kontrollieren Sie, ob die Website gesichert ist, bevor Sie persönliche Daten eingeben: Die URL sollte mit „http**s**://“ und nicht nur mit „http://“ starten. Eine verschlüsselte Verbindung erkennt man zudem am Vorhängeschlosssymbol links neben dem Adressfeld des Webbrowsers.
- Verwenden Sie für jede Anwendung ein anderes Login und ändern Sie regelmäßig Ihre Passwörter.
- Führen Sie Onlinebanking und E-Commerce-Transaktionen nur auf Ihrem eigenen Computer aus.
- Kontrollieren Sie regelmäßig den Saldo Ihres Bankkontos damit Sie bei unbefugten Abbuchungen schneller reagieren und Ihre Bank unverzüglich informieren können.
- Halten Sie Ihre Software (Betriebssystem, Webbrowser und E-Mail-Programm) stets aktuell und verwenden Sie eine Virenschutzsoftware mit aktuellen Virensignaturen und eine Firewall.
- Installieren Sie Webfilter, die Ihren Sperrkatalog stetig um gefälschte Webseiten erweitern. Moderne Webbrowser greifen auf Datenbanken mit bekannten Phishing-Seiten zu und warnen bei deren Aufruf davor.

Einige Erkennungsmerkmale von Phishing-Mails

- Sie als E-Mailempfänger stehen in keiner Beziehung zum E-Mailabsender und sind kein Kunde der als Absender angegebenen Bank oder Firma.
- Die Absenderadresse unterscheidet sich von der bekannten Firmenadresse.
- Die URL sieht der echten Adresse ähnlich, enthält aber unübliche Zusätze wie Zahlen: *189z-sparkasse.com* oder *ab-bank.kundenservice.de*
- Die Anrede ist unpersönlich wie beispielsweise „Sehr geehrter Kunde“.
- Akuter Handlungsbedarf wird vorgetäuscht. Zum Beispiel „Wenn Sie nicht innerhalb der nächsten zwei Tagen eine Verifikation durchführen, wird Ihr Konto gesperrt.“ In diesem Fall sollten Sie sich bei dem jeweiligen Dienst direkt einzuloggen und prüfen, ob die E-Mail real ist. Öffnen Sie keinesfalls Links oder Anhänge.
- Über ein in die Mail eingebundenes Formular oder über einen Link werden vertrauliche Daten abgefragt.
- Die Mitteilung enthält sprachliche Ungenauigkeiten oder ist in schlechtem Deutsch verfasst.
- Der Text enthält kyrillische Buchstaben oder falsch aufgelöste/fehlende Umlaute wie „a“ statt „ä“ bzw. „ae“.

Folgendes Video der deutschen *Bundesanstalt für Sicherheit in der Informationstechnik* fasst die wichtigsten Phishing-Fakten zusammen:

Werbung im Internet als Fluch und Gefahr

Werbung ist allgegenwärtig und begegnet uns täglich auf verschiedenste Weise: auf Plakaten, in Inseraten, (un-)adressierten Postwurfsendungen, Prospekten, Fernseh- und Radiospots und im Internet, hier insbesondere auch in sozialen Netzwerken und Online-Games.

Werbung im Internet ist ein Multimilliarden-Geschäft, der von Google konzipiert, ständig verfeinert und monopolisiert wird. Google verfolgt Nutzer und sammelt massenhaft Daten über ihre Surfgewohnheiten, um die Wirkung von Werbeanzeigen auf sie zu optimieren. Google finanziert sich über Werbung, und Nutzerdaten seien die Währung im Anzeigengeschäft, schrieb vor rund zehn Jahren die Harvard-Professorin Shoshana Zuboff und gab dem Google-Geschäftsmodell einen treffenden Namen: ***Überwachungskapitalismus***.

Für viele ist Google der einfachste Weg, um bestimmte Software zu finden, aber Cyberkriminelle haben dies in den letzten Monaten gefährlich gemacht. Wenn man nach einem bestimmten Programm sucht und auf eines der obersten Google Suchergebnisse klickt (in der Regel eine Anzeige, nicht das oberste Ergebnis), kann der Link zu einer Webseitenimitation führen, die Schadware anstelle des gesuchten Programms liefert. Bekannte Programmnamen, wie MSI Afterburner, Bitwarden, Grammarly, Blender, Gimp, Adobe Reader, Microsoft Teams, OBS, Slack, Thunderbird und viele andere sind bisher so missbraucht worden. Die betrügerische Webseite sieht genauso aus wie die offizielle Download-Seite der Software.

Man sollte seine Anwendungen ausschliesslich von der Webseite des Herstellers herunterladen, sofern man diese kennt. Alternativ kann man die Software von einem seriösen Softwareportal wie **Wintotal.de** oder **PCtipp.ch** herunterladen.

Um die Gefahr von infizierten Anzeigen und die Werbeflut zu entkommen, kann man einen Ad-Blocker installieren, der verhindert, dass Werbung angezeigt wird. Als positive Nebenwirkung werden die Webseiten im Webbrowser schneller geladen. Zu empfehlen sind **uBlock Origin** und **Malwarebytes Browser Guard**. Wie diese Erweiterungen im Mozilla Firefox und im Windows Edge installiert werden, zeige ich online.

Quellen und Internetadressen

Deutsches Bundesamt für Sicherheit in der Informationstechnik: Aktuelles über Cyberrisiken.

Nationales Zentrum für Cybersicherheit NCSC, Schweiz: Aktuelle Vorfälle in der Schweiz.

Die Windows Sicherheit-App: Beschreibung und Konfiguration der App für Windows-Sicherheit.

Security Insider.de: Tipps und Tricks zu Microsoft Defender.

';--have i been pwned ?: (Übersetzt in etwa «Wurde ich erwischt?»): Website, auf der Nutzer überprüfen können, ob ihre persönlichen Daten durch Datenlecks kompromittiert wurden.

PCtipp.ch: Aktuelle News, Tests und Praxisanleitungen zu Computer, Tablets, Smartphones, Unterhaltungselektronik, Software und Apps. Sichere Downloads geläufiger Anwendungen.

WinTotal.de: Das Portal für Windows-News, Software und informative Artikel. Sichere Downloads.