Security Lektion 2
Malware

- ✕ Malware
- ✓ Machen Sie sich klar, welchen Malware-Angriffen Ihre Daten durch das Internet ausgesetzt sind. Dann entwerfen Sie Strategien zum Schutz.

Aufgabe

1. Malware

Sobald Ihr Rechner an das Internet angeschlossen ist, nutzen Sie Dienste eines anderen Rechners. Doch dabei kann es durchaus passieren, dass andere Nutzende Ihren Rechner ausfindig machen, die Zugangshürden überwinden und Schaden anrichten. Mit diversen Schadensprogrammen, so genannter *Malware*, werden beispielsweise Programme zum Ausspionieren installiert.

Phisher versuchen, Ihre persönlichen Bankdaten zu stehen. Sie verfolgen dazu jede Ihrer Aktionen auf Ihrem Rechner nach. Malware schädigt zudem Ihre gespeicherten Daten auf unterschiedlichste Arten mit Viren, Trojanern, Würmern oder Spyware.

Gemein ist auch das bereits in der vergangenen Lektion erwähnte *Clickjacking*, eine Technik die ebenfalls versucht, an vertrauliche Informationen heranzukommen. Dabei wird eine transparente Ebene über eine seriös aussehende Webseite gelegt. Wenn Sie auf einen vermeintlich harmlosen Link klicken, klicken Sie in Wirklichkeit auf die transparente, versteckte Ebene. Im Laufe dieses Prozesses geben Sie unter Umständen vertrauliche Informationen preis.

Mousetrapping soll verhindern, dass Sie eine Website verlassen. Entweder öffnen sich neue Fenster oder ein bereits geöffnetes Fenster lässt sich nicht mehr schließen.

Bei *Browser Hijacking* wird die Startseite präpariert. Jedes Mal, wenn Sie den Internet Explorer öffnen, erscheint als Startseite die Website eines Hijackers. Werbung, Banner, Popups, Verlinkungen zu Online-Casinos, Flirtdienste oder pornografischen Seiten erscheinen, Favoriten werden hinzugefügt. Lästig bis nervtötend sind die Varianten des Browser Hijackings, bei denen die Browser-Einstellungen so manipuliert werden, dass Sie als Nutzer oder Nutzerin diese Einstellungen nicht korrigieren können.

Solche Techniken verunsichern manche User und Userinnen so sehr, dass sie sich nicht mehr auf Links zu klicken trauen. Doch es ist wie im richtigen Leben: Da lungern Sie auch nicht in dubiosen und abgelegenen Hinterhöfen herum, lassen Handtaschen offen liegen oder geben an der Kasse Ihre Bankdaten bekannt. Verhalten Sie sich beim Surfen im WWW genauso und erkunden Sie eben keine dubiosen Seiten (Mouse-trapping wird eventuell auf Pornoseiten verwendet), füllen Sie nicht unbedacht Formulare aus und übertragen Sie Kontoinformationen nur über gesicherte Verbindungen.

Typen von Malware

- **Computerviren** sind die älteste Art von Malware. Sie verbreiten sich von einer Datei zu nächsten und infizieren diese Dateien mit dem Virus. Verteilt werden sie von uns Menschen über Dateianhänge (E-Mails), Downloads (WWW) oder durch Verwenden bereits infizierter Dateien (gerne auf USB-Sticks).
- **Makroviren** sind in ein Dokument eingebettet. Normalerweise eine tolle Möglichkeit, wiederkehrende Arbeitsabläufe zu erleichtern, kann ein Makro aber auch so programmiert werden, dass es sich in andere Dateien einnistet – um hier schädliche und / oder unerwünschte Aktionen auszuführen.
- **Bootsektorviren** werden noch vor dem Start des Betriebssystems beim Hochfahren ausgeführt.
- **Würmer** verbreiten sich in Netzwerken. Sie sind ähnlich wie Computerviren, verbreiten sich aber meist ohne menschliche Hilfe über Netzwerke.
- **Trojaner** (Trojanische Pferde) tarnen sich als nützliche Programme, führen versteckt aber bösartige Aktionen aus. Trojaner müssen vom Nutzenden installiert werden.
- Trojaner installieren gern **Keylogger**, die jeden Anschlag auf der Tastatur protokollieren. Betrüger/ -innen finden so Passwörter heraus (und Bosse überwachen so ihre Mitarbeitenden).
- Trojaner installieren auch **Backdoor-Programme.** Das sind Schadens-programme, die über Viren, Würmer oder Trojaner installiert wurden. Über diese Hintertür versuchen Dritte, Zugang zum Computer erhalten.
- **Spy- und Adware** forschen das Nutzungsverhalten aus, senden die Daten ohne Ihr Wissen und Ihre Zustimmung an Dritte, um unerwünschte Werbung zu platzieren.
- **Rootkit** ersetzt wichtige Module im Betriebssystem durch manipulierte Komponenten. Der Rechner funktioniert wie gewohnt, die Viren bleiben dabei verborgen.
- **Scareware** soll den Nutzenden verunsichern und dazu verleiten, schädliche Software zu installieren. Warnt eine gefälschte Meldung vor angeblichem Virenbefall oder ungesicherten Systemen? Durch den Download der angepriesenen Software kommt das Schadensprogramm wirklich auf den Rechner.
- **Ransomware** sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Inzwischen können diese Krypto Schadprogramme den gesamten Rechner sperren. Ob die Lösegeldzahlung den PC wieder nutzen lässt, ist fraglich.

Etwas veraltet sind sogenannte **Dialer**. Früher wurde bei Modem- oder ISDN-Verbindungen eine neue DFÜ-Verbindung ohne Wissen des Nutzenden eingerichtet. Das kostete teures Geld. Diese Mehrwert-Nummern sind schon längst von den Providern gesperrt.

Schutz vor Malware

Installieren Sie auf jeden Fall ein Antiviren-Programm. Lassen Sie diese Software am besten automatisch aktualisieren. Dann entdeckt und entfernt das Programm auch neue Viren. Beachten Sie außerdem, dass Sie mittlerweile nicht mehr auf einem PC in

der Firma arbeiten, sondern auch am Laptop Kundendaten speichern, am Smartphone eine E-Mail senden und am Tablet eine Online-Überweisung machen.

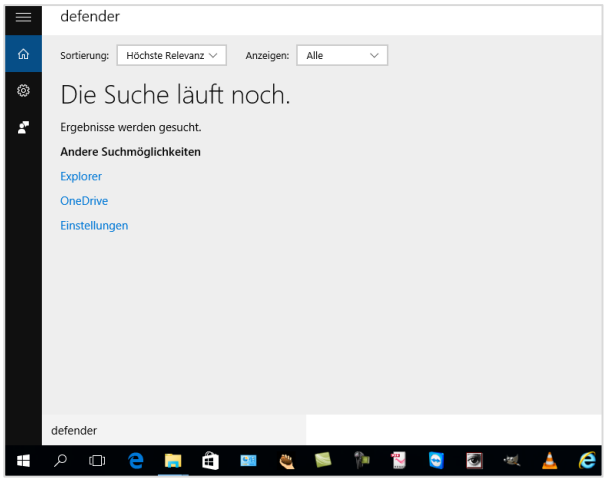
Haben Sie ältere Software auf Ihren Geräten installiert, dann entsprechen diese Versionen nicht mehr den aktuellen Sicherheitsstandards. Ein Update, sogenannte *Patches* oder das Installieren aktueller Programme kann diese bedrohlichen Sicherheitslücken wieder schließen.

Vorsicht ist geboten beim Download von Bildschirmschonern, Smileys und Emoticons oder auch Toolbars. (Was nicht heißen soll, dass die Anbietenden immer Schlechtes im Sinn haben. Doch ist es meist so.)

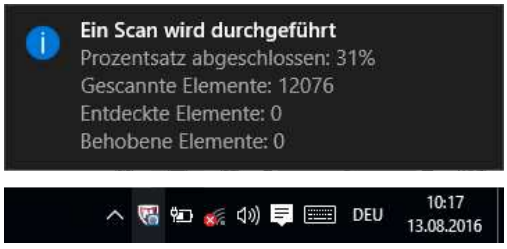
Antiviren-Software nutzen

Antiviren-Software erkennt Malware und blockiert diese Schadsoftware bereits vor dem Download. Dazu schützt handelsübliche Antiviren-Software auch E-Mails und das komplette Computersystem. Windows 10 hat standardmäßig das Programm **Defender** integriert. Neben einem Virenschutz kontrolliert dieses Programm auch das komplette System.

Starten Sie den **Defender** unter **Windows 10** über das Startmenü (siehe Abbildung).

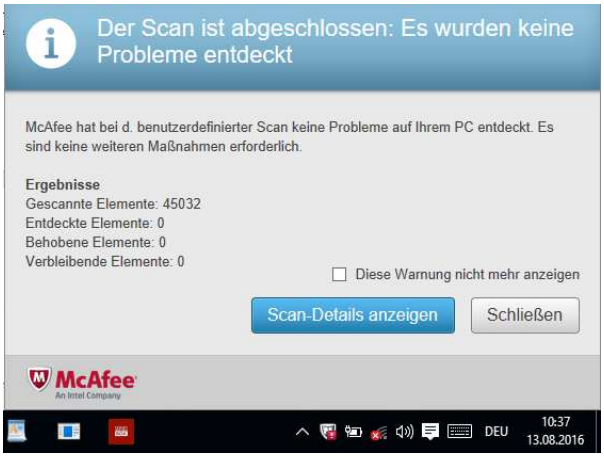


In der Taskleiste sehen Sie auf der rechten Seite einen Hinweis auf den Fortschritt des Scans (siehe Abbildung).



Ist der Scan abgeschlossen, erhalten Sie eine Information (siehe Abbildung).

Schließen Sie das Fenster.



Haben Sie ein Antiviren-Programm auf Ihrem Rechner installiert, so wird der Scanvorgang meist automatisch gestartet. Sehen Sie in der Taskleiste auf der rechten Seite nach – finden Sie hier ein Symbol für einen Virenscanner? Dann klicken Sie doppelt darauf und sehen Sie in den Einstellungen nach, welcher Zeitplan für automatische Scans eingestellt ist.

Möchten Sie einen Scanvorgang außerhalb des automatischen Zeitplans durchführen, so ist das ebenfalls möglich. Starten Sie den Virenscanner. Wählen Sie aus, ob Sie gleich den gesamten Computer prüfen möchten oder nur ein bestimmtes Laufwerk, einen Ordner oder eine Datei scannen lassen möchten.

Werden infizierte Dateien gefunden, dann wird die Antiviren-Software versuchen, diese Dateien zu löschen oder zu desinfizieren. Ist das nicht möglich, dann werden befallene oder als verdächtig erscheinende Dateien in die sogenannte *Quarantäne* verschoben. Hier wird jeder Zugriff verhindert. Sie können selber im Virenschutz-Programm bestimmen, was mit einzelnen verdächtigen Dateien geschehen soll.

Antiviren-Programme verfügen über eine Früherkennung, *Heuristik* genannt. Beachten Sie, dass diese Programme aber trotzdem Grenzen haben. Einerseits müssen Sie Antiviren-Software regelmäßig aktualisieren. So werden die aktuellen *Virensignaturen* heruntergeladen, damit auch neue Bedrohungen erkannt werden. Andererseits kann Antiviren-Software nicht vor Sicherheitslücken in den Programmen selber schützen. Aktualisieren Sie also die installierten Apps und führen Sie vorgeschlagene Software-Updates durch. Vergessen Sie dabei Ihre mobilen Geräte nicht!

Sicherheit Schritt zwei
Anti-Viren-Programm verwenden

Übung und Selbststudium

1. Sie haben eine Antiviren-Software am Rechner installiert. Wie prüfen Sie eine einzelne Datei?
2. Finden Sie gratis Antiviren-Software im Internet.
   - Installieren Sie das Programm oder nutzen Sie eine bereits auf Ihrem Gerät installierte Antiviren-Software.
   - Führen Sie einen Scan eines Ordners durch.
3. Nutzen Sie das WWW – welchen Angriffen aus dem Internet sind Sie und Ihre Daten ausgesetzt?
4. Wie schützen Sie sich vor Malware? Woran könnten Sie zweifelhafte Aufforderungen erkennen?

Testen Sie Ihr Wissen

1. Erklären Sie den Begriff Malware.
2. Was ist Browser-Hijacking?
3. Was sind Keylogger?

Notizen

Die nächste Lektion beschäftigt sich mit Netzwerken.