

## Sicherheit 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 stehlen. 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 so genanntes *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.

*Viren verbreiten sich von einer Datei zur nächsten und infizieren diese. Verteilt werden sie von uns Menschen über Dateianhänge (E-Mails), Downloads (WWW) oder durch Verwenden bereits infizierter Dateien (gerne auf USB-Sticks).*

*Würmer arbeiten ähnlich, verbreiten sich aber meist über Netzwerke ohne menschliche Hilfe.*

## 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.
- ▶ **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.
- ▶ **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 Schadensprogramme, 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.

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.

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

## **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.
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**

