Schadsoftware: Viren, Würmer, Trojaner

Unter diesen Bezeichnungen werden allgemein „schädliche“ Programme zusammengefasst.

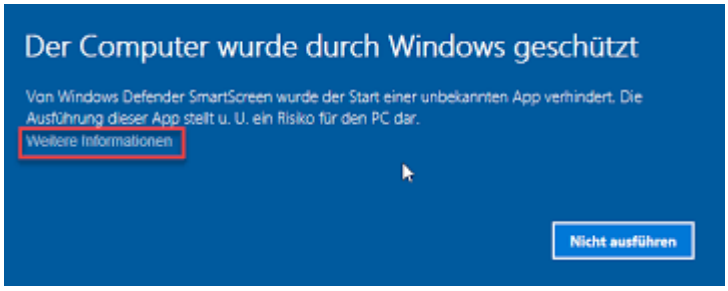
Allen ist gemeinsam, dass sie sich in deinem Computer installieren können, ohne dass du es bemerkst. Sie können sich sehr gut verstecken und dann den Computer dazu veranlassen, für dich schädliche Dinge zu tun.

Es gibt viel eher harmlose Schadsoftware, die eher harmlose Dinge tut wie den Benutzer zu ärgern oder Werbung einzublenden („**Adware**“). Es gibt aber auch sehr gefährliche, die immer wieder großen Schaden anrichtet. Sie kann zum Beispiel deine Daten ausspionieren und an irgendwen im Internet senden („**Spyware**“), oder deinen Computer für fremde Zwecke missbrauchen, z.B. (Bitcoins schürfen („**Crypto-Mine**r“).

Besonders gefährlich sind im Moment Schad-Programme, die wichtige Daten unbrauchbar machen, um „Lösegeld“ zu erpressen (“**Ransomware**“). Die Kriminellen versprechen: wenn man Lösegeld zahlt, bekommt man einen „Schlüssel“, um seine eigenen Daten wieder zu reparieren. Zahlt man nicht, sind sie verloren.

Schadsoftware installiert sich der Benutzer fast immer selbst, indem er unvorsichtig die Zustimmung zur Ausführung von ihm unbekannten Programmen gibt.

Wenn man versucht, „verdächtige“ Programme auszuführen, bekommt man von Windows eine Warnmeldung wie diese:



Sie sagt nichts darüber aus, ob das Programm schädlich ist oder nicht. Windows kann das gar nicht feststellen. Die Meldung sagt nur, dass dieses Programm schädlich sein **könnte**, du sollst also gut aufpassen. Über „Weitere Informationen“ kannst du dem Computer sagen, er soll die Datei trotzdem ausführen. Du machst das nur, wenn du sicher bist, dass sie nicht schädlich ist.

Gegenmaßnahmen:

- Installiere Programme nur, wenn du sie wirklich brauchst.
- Lass die keine Programme aufschwätzen, die Unmögliches versprechen (z.B. schnelleres Internet, ohne dafür mehr Geld zu zahlen).
- Installiere Programme nur aus vertrauenswürdigen Quellen, z.B. aus einem offiziellen Store, und lies vorher die Beschreibung und eventuelle Bewertungen genau durch. Dort steht meistens drinnen, ob das Programm schädlich ist oder nicht.
- Sei sehr vorsichtig bei „Gratis-Programmen“. Das Programmieren guter Programme ist viel Arbeit. Niemand verschenkt sie hinterher, ohne irgendwie Geld oder eine andere Belohnung dafür zu verlangen.
- Wenn du von Windows, deinem Browser oder von Office eine Warnung bekommst, dass eine bestimmte Datei „schädlich für deinen Computer sein kann“, nimm die Warnung ernst.

Versuche erst einmal, mehr zu dieser Datei herauszufinden, bis du sicher bist, dass sie harmlos ist.

- Viele (aber nicht alle) Schadprogramme werden von modernen „**Virenscannern**“ erkannt und automatisch blockiert. Alle modernen, aktuellen Windows-Versionen haben so einen Virenschutz („**Windows Defender**“, „**Windows SmartScreen**“) gratis mit dabei, es ist daher in der Regel nicht nötig, sich einen zusätzlichen Virenschutz zu kaufen.

Falsche Informationen: Hoaxe, Fake News, Propaganda

Es ist relativ einfach, Falschinformationen ins Internet zu stellen und zu verbreiten. Jeder kann das tun, und es kostet kaum Geld.

Im harmlosesten Fall machen sich die Hersteller solcher Informationen einfach lustig über jemanden, der ihren Unsinn glaubt und ihn weiterverbreitet („**Hoax**“ = „schlechter Scherz“). Manche Hoaxe richten aber auch echten Schaden an, indem sie z.B. behaupten, ganz harmlose Dinge seien gefährlich. Man solle sie deswegen nicht kaufen, wegschmeißen oder sogar zur Polizei bringen.

„Fake News“ sind dagegen frei erfundene oder bewusst veränderte und oft sehr gut nachgemachte Neuigkeiten.

Im harmlosesten Fall sind sie nur zur Unterhaltung gemacht (z.B. erfundene Promi-News), Fake-News können aber auch unschuldige Personen verleumden. Besonders beliebt ist dabei das „Herausreißen“ wirklich passierter Ereignisse oder Aussagen aus dem Zusammenhang. Es wird also weggeschnitten, was davor und danach passiert ist. Dadurch kann man aus wahren Begebenheiten neue, falsche Geschichten zusammenbauen, die auf den ersten Blick wahr aussehen.

Unter „**Propaganda**“ versteht man Nachrichten, die einseitig und falsch eine Seite gut und eine andere Seite schlecht dastehen lassen. Vieles wird einfach erfunden. Das kann man aber meistens relativ einfach feststellen, es ist „nur“ ein wenig Arbeit. „Selektive Berichterstattung“ macht es etwas geschickter: man wählt dazu aus der Fülle verfügbarer Informationen „selektiv“ nur diejenigen aus, die gut für die eigene Botschaft sind, und ignoriert gezielt alle anderen Informationen. Diese Manipulation ist schwerer zu entdecken.

Besonders anfällig für die Verbreitung von Falschinformationen sind soziale Netzwerke, weil hier der Verfasser nur schwer ermittelt werden kann, und die Verbreitung durch „teilen“ sehr schnell erfolgt.

Gegenmaßnahmen:

- Glaube sensationell formulierte, kurze Aussagen zu komplizierten Themen erst einmal nicht, ohne sie vorher genauer zu prüfen.
- Leite nichts, was wichtige Informationen verspricht, einfach mal schnell weiter. Überprüfe es vorher sorgfältig.
- Prüfe bei Behauptungen die Quelle (wer genau hat das wann und wo gesagt) und versuche, die Glaubwürdigkeit der Quelle zu beurteilen. Versuche möglichst mehrere unabhängige Quellen zu finden.

Gefälschte Webseiten

Es ist für einen guten Programmierer sehr einfach, Webseiten zu kopieren oder nachzumachen. Er kann dann unsichtbaren, schädlichen Code hinzuzufügen, und die gefälschte Seite wieder ins Internet zu stellen. Man soll sie mit der Originalseite verwechseln.

Das Ziel dieser Kopien ist es meistens, weitere schädliche Dinge vorzubereiten. So soll eine gefälschte Login-Seite dir deinen Benutzernamen und dein Passwort stehlen. Oder ein gefälschter

Store will dich dazu bringen, schädliche Software herunterzuladen und zu installieren. Oder ein gefälschter Shop will dich dazu bringen, Geld vorab für Waren zu bezahlen, die dir dann aber nie zugeschickt werden.

Gegenmaßnahmen

- Prüfe im Zweifelsfall immer, ob die Webseite, die gerade in deinem Browser angezeigt wird, wirklich echt ist (auf https achten, und die Adresse genau lesen)
- Prüfe, bevor du auf einen Link klickst, ob die Zieladresse tatsächlich die ist, die versprochen wird.
- Sei vorsichtig, wenn irgendwo eine teure Ware sensationell billig angeboten wird.
- Nütze sichere Bezahldienste wie zum Beispiel Paypal, beachte dabei aber, dass diese Dienste nicht nur sichere, sondern auch unsichere Bezahlmethoden anbieten. Paypal „Überweisung an Freunde“ ist zum Beispiel nicht sicher, „normales“ Paypal schon.
- Bezahldienste sind für dich nur sicher, wenn du ihre „Allgemeinen Geschäftsbedingungen“ beachtest. Da steht drinnen, was du selber tun musst, damit du geschützt wirst.

Phishing

Beim Phishing-Betrug versuchen Online-Betrüger, dich dazu zu bringen, ihnen vertrauliche Informationen wie Passwörter, PIN Codes, Geburtsdaten, Kreditkartendaten, Bankdaten usw. zu geben.

Meistens sprechen Phisher ihre Opfer über gefälschte Links in E-Mails an, die den Benutzer dann zu gefälschten Webseiten leiten. Beliebt ist es auch, in Anhängen an Mails Schadsoftware zu verschicken.

Gegenmaßnahmen

- Prüfe an Hand der Adresse, ob eine Mail wirklich von dem richtigen Absender stammt
- Prüfe, bevor du auf einen Link klickst, ob die Zieladresse tatsächlich die ist, die versprochen wird.
- Überlege, ob ein Mail tatsächlich Sinn macht. Hast du bei der Firma, die dir angeblich eine Rechnung schickt, wirklich etwas bestellt?
- Führe keine Mail-Anhänge aus, wenn du nicht genau weißt, was drinnen ist, egal von wem sie kommen.

Identitätsdiebstahl

Über im Internet gesammelte Daten kann man die Identität einer anderen Person annehmen, und so zum Beispiel Waren bestellen, Rechnungen bezahlen, Verträge abschließen oder auch Fake-News verbreiten. Wenn dann der Betrug auffliegt, bekommt erst einmal die wirkliche Person großen Ärger.

Die wirkliche Person kann darüber hinaus auch selber Ärger bekommen, wenn man ihr vorwerfen kann, dass sie nicht gut genug auf ihre eigenen Daten aufgepasst hat.

Gegenmaßnahmen

- Gib im Internet keine persönlichen Daten preis, wenn du nicht genau weißt, wem du sie gibst, und wozu sie verwendet werden sollen. Lies dazu die Datenschutzerklärungen.
- Bleib misstrauisch und wachsam, wenn jemand persönliche Daten von dir verlangt, auch dann, wenn die Person behauptet, dass sie dir helfen will

Spam

Spam, oder zu Deutsch „unverlangte Werbung“ ist meistens eher ärgerlich als gefährlich. Es handelt sich dabei um unerwünschte Werbung, die meistens als E-Mail zugestellt wird.

Spam wirbt oft für illegale oder minderwertige Produkte und Dienstleistungen, und kann auch für Phishing verwendet werden. Darüber hinaus klaut Spam Speicherplatz, Datenvolumen und Bandbreite, verstopft E-Mail Sever und Postfächer, und klaut nicht zuletzt deine Zeit beim Aussortieren.

Gegenmaßnahmen

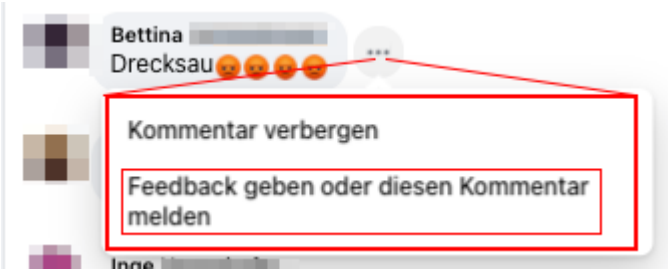
- Buche bei deinem Mail-Provider einen Spam-Blocker, oder installiere einen in deinem E-Mail Programm. Das verringert die Anzahl der Spam Nachrichten, die es bis in dein Postfach schaffen ziemlich stark. Etwa 9 von 10 Spam-Nachrichten werden richtig erkannt und entweder gleich gelöscht, oder in den Ordner „Spam“ verschoben.
- Gib deine Mail-Adresse nicht unvorsichtig weiter. Trage deine E-Mail Adresse nicht im Klartext in Webseiten, Chats oder anderen Seiten ein, wo sie dann jeder sehen und abkopieren kann.
- Lies die Datenschutzrichtlinien von Seiten, bevor du ihnen deine Daten gibst. Da muss drinnen stehen, ob deine Adresse für Werbung verwendet oder an andere Firmen weitergegeben wird.

Cybermobbing

Die Möglichkeit, sich im Internet hinter einem Kürzel (Alias, Pseudonym, Nickname) zu verstecken verleitet manche dazu, andere zu belästigen, zu verleumden oder bloßzustellen, in anderen Worten, deren **Persönlichkeitsrechte** massiv zu verletzen.

Gegenmaßnahmen

- Man kann solche Inhalte bei allen seriösen Plattformen melden, daraufhin werden sie gelöscht und der Nutzer der sie gemacht hat wird verwarnt oder gesperrt.



- Erstelle selbst keine beleidigenden Inhalte, und leite sie nicht weiter.
- Informiere das Opfer, seine Eltern oder die Schule, ggf. sogar die Polizei, über solche Inhalte. Internetplattformen haben dazu meistens irgendwo einen Button „melden“, mit dem man verdächtige Inhalte sofort an den Betreiber (Facebook, Tiktok, Youtube, usw.) melden kann.

Zusammenfassung

Viren, Würmer, Trojaner	Das sind verschiedene Arten von Schadsoftware
Schadsoftware, Schadcode	Programme die deinen Computer dazu missbrauchen, schädliche Dinge zu tun
Adware	Schadsoftware, die Werbung einblendet
Ransomware	Schadsoftware, die Lösegeld für geklaute Daten erpresst

Spyware	Schadsoftware, die persönliche Daten an Daten-Diebe im Internet sendet
Crypto-Miner	Schadsoftware, die fremde Computer missbraucht um Cryptowährungen (Bitcoins) zu schürfen
Virenscanner	Programme, die versuchen, andere Programme auf Schädlichkeit zu überprüfen
Windows Defender, Windows SmartScreen	In Windows eingebaute Schutz-Programme die versuchen, vor schädlichen Programmen zu warnen
Persönlichkeitsrechte	Rechte, die jeder Mensch hat, und die jeder andere beachten muss. Es gibt dazu eigene Arbeitsblätter.
Cybermobbing	Andere Menschen im Internet mit Hass-Kommentaren, Lügen usw. beleidigen
Spam	Werbe-Mails, die man nicht selber bestellt hat
Phishing	Jemanden dazu bringen, seine vertraulichen Daten übers Internet herauszurücken
Identitätsdiebstahl	Möglichst viele persönliche Daten zu jemandem sammeln und dann versuchen, sich im Internet oder am Telefon als derjenige auszugeben.
Persönliche Daten	Daten über jemanden, die andere nicht wissen dürfen, z.B. Passwörter, PIN Codes, Geburtsdaten, Bank-Nummern, genaue Wohnadresse, usw.
Gefälschte Webseiten	Echten Webseiten nachgemachte Kopien, die versteckten Schadcode enthalten
Hoax	„Schlechter Scherz“. Im Internet verbreitete erfundene Geschichten.
Fake News	Erfundene oder verfälschte Nachrichten
Propaganda	Manipulierte Nachrichten mit dem Ziel, eine Seite gut und eine andere Seite schlecht dastehen zu lassen
Selektive Berichterstattung	Aus den verfügbaren Informationen nur diejenigen herauspicken, die gut für die eigene Seite sind. Bei Berichten über die andere Seite nur schlechte Informationen herauspicken.