verbraucherzentrale
Nordrhein-Westfalen

SCHADPROGRAMME

So schützen Sie sich.

WAS SIND SCHADPROGRAMME UND WAS KÖNNEN SIE ANRICHTEN?

Der Begriff „Schadprogramm“ oder „Schadsoftware“ (englisch: Malware) umfasst alle Arten von Computerprogrammen, die mit dem Ziel entwickelt wurden, Daten auszuspähen, Dritten unbefugten Zugriff auf IT-Systeme zu ermöglichen oder fremde Systeme über unterschiedlichste Kanäle zu infizieren. Malware ist dabei der Oberbegriff für eine Vielzahl an Bedrohungen, die entsprechend der verursachten Schäden in verschiedene Kategorien eingeteilt werden können:

- **Infektionen zum Zweck des Datendiebstahls:** Tastatureingaben (z. B. Passwörter) werden aufgezeichnet (Keylogger), der Computer oder das mobile Gerät wird nach sensiblen persönlichen Daten wie Passwörter und Zugangsdaten durchsucht oder Überweisungsdaten werden abgefangen (Banking Trojaner), der Zugriff auf Mikrofone und Kameras ist möglich (Spyware). Mit den gestohlenen Daten können Accounts übernommen, Identitäten in sozialen Netzwerken gestohlen und Bankdaten missbraucht werden.

- **Infektionen zum Zweck der Kontrollübernahme** (Integration in ein Bot-Netz): Von Bot-Netzen spricht man dann, wenn mehrere infizierte Systeme per Fernsteuerung zusammengeschlossen und zu bestimmten Aktionen missbraucht werden. Die Kontrolle über internetfähige Geräte aus der Ferne ermöglicht es dem Angreifer, das übernommene System unbemerkt für seine Zwecke zu missbrauchen. So kann er damit z. B. Internetseiten lahmlegen (DDoS), Spam versenden oder Online-Banking-Betrug begehen.

- **Ransomware**: Daten werden verschlüsselt, um den Nutzer zu erpressen. Ein Zugriff auf die Daten ist nicht mehr möglich. Für die Entschlüsselung wird dann ein Lösegeld (eng. Ransom) gefordert. Zusätzlich wird bei betroffenen Firmen häufig auch mit der Veröffentlichung der Daten gedroht.

- **Adware**: Als Adware werden Programme bezeichnet, die sich über Werbung finanzieren. Adware-Programme verändern dafür etwa die Browsereinstellungen, sodass sich beim Surfen plötzlich vermehrt Pop-up-Fenster mit unerwünschter Werbung öffnen oder sich die Startseite beim Öffnen des Browsers ändert. Zudem können auch persönliche Daten ausgespäht werden.

- **Scareware**: (von engl. to scare, jemanden ängstigen): Hierbei wird dem Benutzer beispielsweise suggeriert, sein Gerät sei mit einem Schadprogramm infiziert. Auf diese Weise soll er verunsichert und dazu verleitet werden, ein Programm, das den Schaden angeblich behebt, herunterzuladen. Dieses Programm enthält aber erst die eigentliche Schadsoftware.

Schadprogramme sind häufig multifunktional und im Stande, zusätzliche Schadprogramme nachzuladen, die weitere Schäden anrichten. Sie entwickeln immer bessere und intelligentere Methoden sowie Angriffsvektoren, vor denen Sie sich so gut es geht schützen sollten.

- **Phishing:** Dabei handelt es sich um einen Angriffsvektor zum Zweck des Datendiebstahls. Nutzer werden beispielsweise über Links in E-Mails oder sozialen Netzwerken auf manipulierte oder gefälschte Internetseiten gelotst, die den Originalseiten der echten Anbieter täuschend ähnlich sehen. Ziel ist es, dem Nutzer Passwörter, Kreditkartendaten oder andere vertrauliche Informationen zu entlocken. Die Delikte reichen vom „einfachen“ Datendiebstahl über illegale Kontoabbuchungen bis hin zu Angriffen auf kritische Infrastrukturen.

- **Smishing:** Mit überzeugenden SMS sollen Nutzer dazu verleitet werden, auf einen Link zu klicken. Vorwand kann zum Beispiel ein nicht zustellbares oder nicht ausreichend frankiertes Paket sein. Der Link leitet zum Download einer Schadsoftware oder zu Phishing-Seiten, auf denen Sie dann sensible Informationen preisgeben sollen.

- **Pharming:** Bei dieser Methode werden Host-Einträge (Textdateien, die Host-Namen mit zugehörigen IP-Adressen speichern) auf einem infizierten System geändert. Internetbrowser werden durch Schadprogramme so manipuliert, dass die Webseiten-Anfragen eines Nutzers auf betrügerische Webseiten umgeleitet werden. Dort werden dann Benutzernamen, Passwörter oder Kreditkartendaten erfasst oder Schadprogramme auf dem Gerät installiert.

WIE MAN SICH SCHADPROGRAMME EINFANGEN KANN

Grundsätzlich können sich alle elektronischen Geräte mit Schadprogrammen infizieren, die entweder mit dem Internet verbunden sind oder einen Wechseldatenträger besitzen. Kriminelle gehen bei dem Versuch, Nutzern ein Schadprogramm unterzujubeln, ganz verschiedene Wege. Besonders beliebt sind folgende Möglichkeiten:

- **Schadsoftware im E-Mail-Anhang:** Sie erhalten eine E-Mail, die angeblich von einem vertrauten Anbieter, wie zum Beispiel Ihrer Hausbank stammt. Der E-Mail beigefügt ist eine Datei, die ein Schadprogramm enthält. Achtung bei Dateiformaten wie .exe oder .scr oder doppelten Dateiendungen wie „pdf.exe“. Falls Sie eine solche Datei öffnen, wäre das bildlich gesehen so, als ob Sie einem Einbrecher selbst die Haustür öffnen und ihn hereinbitten. Vermeintlich harmlos wirkende Verlinkungen im Text einer E-Mail können ebenfalls auf infizierte Webseiten leiten. Eine weitere gängige Methode von Kriminellen ist es beispielsweise, PDFs oder Office-Dokumente über dynamische Inhalte und Makros zu

einem Einstieg in Ihr System zu machen. Ein Makro ist eine Abfolge von Befehlen und Anweisungen, um eine Aufgabe automatisch auszuführen. Um unnötige Risiken zu vermeiden, sollten Makros bei nicht vertrauenswürdigen Dokumenten deaktiviert werden.

- **Drive-By-Download:** Die Infektion erfolgt durch das Aufrufen einer manipulierten Internetseite. Doch auch seriöse Webseiten können durch manipulierte Werbebanner mit Schadcode verseucht sein. Das Schadprogramm wird ohne Interaktion des Anwenders alleine durch das Aufrufen der Seite installiert, indem die Täter noch nicht geschlossene Sicherheitslücken ausnutzen. Eine offene Sicherheitslücke ist wie ein schräg stehendes Fenster, durch das ein Einbrecher in das Haus einsteigen kann.

- **Malspam und Social Engineering:** Schädliche Links und Dateianhänge können Sie zum einen per E-Mail, zum anderen aber auch als Nachricht in sozialen Netzwerken erhalten. Zum Beispiel schickt Ihnen jemand, den Sie vermeintlich kennen, eine Rechnung oder ein Foto zu oder empfiehlt eine interessante Internetseite, die er gefunden hat. Durch das Öffnen der Datei oder Anklicken des Links wird das Schadprogramm installiert.

- **Wechseldatenträger:** Geräte wie USB-Sticks oder externe Festplatten können infizierte Dateien enthalten. Wenn Sie nun Daten zwischen zwei Geräten zum Zwecke des Datenaustausches beispielsweise mittels USB-Stick übertragen, kann ein Schadprogramm von einem infizierten Gerät auf das andere bisher nicht befallene Gerät übertragen werden.

- **Netzwerke:** Sie sind eine weitere Gefahrenquelle (etwa öffentliches WLAN), da Sie nicht wissen können, ob und wie diese gesichert sind. In Hotels, bei der Nutzung von Hotspots, aber auch bei Computern und mobilen Geräten von Freunden und Bekannten sollten Sie daher entsprechend vorsichtig sein und fremde Netze und Geräte nach Möglichkeit meiden.

WIE SIE SICH IM VORFELD SCHÜTZEN

Cyber-Kriminelle versuchen, Schadprogramme möglichst unbemerkt auf ein System zu schleusen. Im Unterschied zu früher gefährden heutige Schadprogramme nicht nur Computer im engeren Sinne, sondern haben prinzipiell jedes softwaregesteuerte und vernetzte System im Visier. Neben Smartphones und Tablets gilt dies insbesondere für Router und auch für internetfähige Geräte wie digitale Heizungsthermostate oder ein über das Internet steuerbares Garagentor.

- Halten Sie insbesondere das Virenschutzprogramm, den Internetbrowser und das Betriebssystem stets auf dem neuesten Stand. Führen Sie die notwendigen Updates zeitnah automatisch durch oder installieren Sie Updates bei Bedarf bewusst manuell, um Sicherheitslücken zu schließen.

- Seien Sie beim Öffnen von Mails mit Anhängen vorsichtig. Ganz gleich, ob es sich um scheinbar ungefährliche Dateien wie Bilder, Dokumente oder sonstige Dateien handelt. Wenn Sie sich nicht sicher sind oder keine Mail erwarten, fragen Sie sicherheitshalber beim Absender nach. Suchen Sie in diesem Fall selbst nach den Kontaktmöglichkeiten und antworten Sie nicht einfach der Absenderadresse.

- Klicken Sie niemals auf Links in unaufgefordert zugesandten E-Mails. Häufig leiten diese auf infizierte Webseiten. Wenn Sie diese aufrufen, können Sie sich bereits mit Schadsoftware infizieren. Geben Sie die gewünschte Internetadresse des echten Anbieters stattdessen per Hand in die Adresszeile Ihres Browsers ein oder gehen Sie über gespeicherte Favoriten, sofern Sie einen Webanbieter regelmäßig nutzen.

- Seien Sie misstrauisch, wenn Sie E-Mails mit fremdsprachigem Betreff oder einer neugierig machenden Betreffzeile (z. B. aus dem Erotikbereich) erhalten. Das

alleine reicht als Indiz aber leider nicht mehr aus, da die Phishing-Mails auch sprachlich zunehmend besser werden.

- Seien Sie besonders kritisch bei ausführbaren Programmdateien mit den Endungen .exe, aber auch .bat, .com oder .vbs. Damit der Dateityp zu sehen ist, sollten Sie die Standardkonfiguration Ihres Rechners entsprechend anpassen. Achtung: Auch komprimierte Archivdateien, die beispielsweise auf .zip enden, können ausführbare Programme enthalten und sollten daher nie ungeprüft geöffnet werden.

- Stellen Sie die Sicherheitseinstellungen Ihres E-Mail-Programms so ein, dass kein Script automatisch ausgeführt wird.

- Aktivieren Sie keinesfalls Makros, falls Sie dazu aufgefordert werden.

- Formatierte HTML-E-Mails können schadhafte Inhalte enthalten. Deshalb sollten wichtige Nachrichten ausschließlich im „Nur-Text-Format“ geschrieben und vor allem gelesen werden.

- Verschicken Sie keine aus unsicherer Quelle oder per E-Mail zugesandte Anhänge (Attachements). Sonst helfen Sie am Ende noch unbewusst und ungewollt dabei mit, Schadprogramme zu verteilen.

- Seien Sie in sozialen Netzwerken bei Mitteilungen und Angeboten von Ihnen nicht bekannten Teilnehmern skeptisch. Prinzipiell gelten dieselben Sicherheitshinweise wie beim Umgang mit E-Mails. Aber auch bei Nachrichten von Bekannten oder Freunden sollten Sie nicht unkritisch jeden Link anklicken.

Weitere Hinweise finden Sie auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter: **bsi.bund.de/VerbraucherInnen**

WIE SIE IHREN COMPUTER AUF SCHADPROGRAMME ÜBERPRÜFEN UND VON IHNEN BEFREIEN

Kriminelle sind sehr kreativ, wenn es darum geht, Schadprogramme bei Nutzern zu verbreiten. Stellen Sie ungewöhnliche Aktivitäten fest (zum Beispiel werden von Ihrem E-Mail-Konto automatisch E-Mails an Ihre Bekannten versendet) und hegen den Verdacht, dass Ihr Computer mit Schadsoftware befallen ist, untersuchen Sie Ihren Computer mit einem extern gestarteten Betriebssystem. Diese Vorgehensweise ist empfehlenswert, da aktuelle Virenschutzprogramme wichtig sind, aber keine 100-prozentige Sicherheit bieten. Wird ein Befall von Schadsoftware angezeigt, sollten Sie folgende Schritte durchführen, um Ihr Gerät von ungebetenen „Gästen“ zu befreien:

1. Trennen Sie das Gerät vom Netzwerk.

2. Sichern Sie Ihre persönlichen Daten wie Dokumente, Bilder, Musik usw. auf einem externen Medium (USB-Stick oder externe Festplatte). Sind die Dateien durch Ransomware verschlüsselt und es ist kein Backup vorhanden, bewahren Sie die verschlüsselten Daten auf, da diese ggf. zu einem späteren Zeitpunkt entschlüsselt werden können.

3. Installieren Sie das Betriebssystem neu.

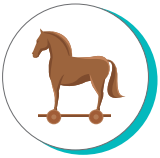
4. Versehen Sie das System mit einer aktuellen Antivirensoftware und prüfen Sie, ob Betriebssystem und Anwendungen in der aktuellsten Version installiert sind. Achten Sie auf die ständige Aktualisierung der Software.

5. Prüfen Sie Ihre auf dem externen Medium gesicherten Daten auf Schadsoftware. Installieren Sie keine Programme aus Backups, da diese infiziert sein könnten.

6. Ändern Sie bei allen Online-Zugängen (E-Mail, soziale Netzwerke usw.) Ihre Passwörter.

7. Prüfen Sie nach dem notwendigen „Reset“ mit dem aktualisierten Virenschutzprogramm, ob sich auf der externen Festplatte mit den persönlichen Daten noch ein Schadprogramm befindet.





WO SIE HILFE BEKOMMEN

- Beim Bundesamt für Sicherheit in der Informationstechnik unter:
  www.bsi.bund.de/VerbraucherInnen

- Bei Ihrer örtlichen Polizeidienststelle sowie unter:
  www.polizei-beratung.de

- Beim Phishing-Radar der Verbraucherzentrale Nordrhein-Westfalen unter:
  www.verbraucherzentrale.nrw/phishing

- Bei Ihrem E-Mail-Provider

- Technische Hilfe bekommen Sie auch auf den Internetseiten einschlägiger Fachzeitschriften.

- **www.nomoreransom.org**

- HPI Identity Leak Checker Desktop des Hasso-Plattner-Instituts:
  https://sec.hpi.de/ilc/

- Identity Leak Checker der Universität Bonn:
  https://leakchecker.uni-bonn.de/

EXKURS – BOT-NETZWERKE

Computer können über die Installation von Schadprogrammen in sogenannte Bot-Netzwerke aufgenommen und deren Ressourcen für weitere kriminelle Aktionen missbraucht werden. Der so infizierte Computer wird von nun an von Kriminellen ferngesteuert. Die Betrüger verwenden beispielsweise die gespeicherten Kontaktinformationen von Freunden und Bekannten aller infizierten Computer, um diese zum Versenden von Phishing-Mails zu nutzen. Eine andere Einsatzmöglichkeit von Bot Netzen sind DDoS-Attacken *(Distributed Denial-of-Service attack)*. Dabei werden die Computer innerhalb des Bot-Netzes dazu genutzt, gleichzeitig so viele Anfragen an einen Server zu stellen, bis dieser seinen Dienst nicht mehr leisten kann. Dieses Problem kann mit einer Tür zu einem Geschäft verglichen werden, welche durch tausende von Menschen versperrt wird, sodass echte Kunden keine Chance mehr haben, in das Geschäft zu gelangen. Diese Angriffe können so weit gehen, dass sie den jeweiligen Server und damit den Service des Anbieters zum Totalabsturz bringen und für Stunden und sogar Tage ausfallen lassen. Da viele Firmen auf die Funktionalität und Erreichbarkeit ihrer Server angewiesen sind, lassen sich einige auf diese Weise erpressen. Nicht zuletzt, da es bei einem DDoS-Angriff durch ein Bot-Netzwerk nahezu unmöglich ist, den echten Angreifer ausfindig zu machen, sollten Firmen im Vorfeld Dienstleistungen des Internet-Service-Providers zur Abwehr solcher Angriffe in Anspruch nehmen. Der Angriff erfolgt ohne das Wissen der eigentlichen Computerbesitzer, die jedoch bei einer polizeilichen Ermittlung grundsätzlich auch ins Visier der Fahnder geraten können.

In Kooperation mit dem
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesamt
für Sicherheit in der
Informationstechnik

IMPRESSUM

Herausgeber:
Verbraucherzentrale NRW e.V.
Mintropstraße 27, 40215 Düsseldorf

Bildnachweis: © jemastock - Fotolia.com
Stand: Dezember 2021

Gedruckt auf 100% Recyclingpapier

verbraucherzentrale
Nordrhein-Westfalen