2024-04-14 Schadprogramme

Immer wieder geht es um Angriffe auf die Computer und meistens um „Lücken“ oder „Schadprogramme“. Dabei handelt es sich um unterschiedliche Varianten, die immer wieder genannt werden. Um was geht es eigentlich, was sind die Unterschiede und wie kann man sich davor zumindest ein wenig schützen? Meistens bleibt es dann doch bei der Schadensbegrenzung. (DGH)

Was ist Schadsoftware?

Schadsoftware = Die Begriffe Schadprogramm oder Schadsoftware (englisch: Malware) umfassen 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: Zusammensetzung aus dem englischen *„malicious“ (*bösartig) und „*war*e“ (von Software). Es gibt zahlreiche Unterarten von Malware - zum Beispiel Viren, Trojaner, Rootkits, Würmer, Botnets, Ransomware, Adware oder Spyware. Alle Arbeiten anders und haben verschiedene Aufgaben. Ein Ziel haben sie jedoch gemein: dem Benutzer zu schaden.

Viren = ein eigenständiges Programm, das sich gegen den Willen des Nutzers auf dem PC installiert. Der Virus setzt sich in einer Software oder im Betriebssystem fest, richtet dort Schaden an und verbreitet sich anschließend weiter.
Über Webseiten und Mail-Anhänge kann der Virus direkt gestartet werden. Oftmals ist der Virus auch in einem Programm eingebaut, das den Virus nach dem Start auf das System loslässt.
Wird der Virus gestartet, sucht er verschiedenste Dateien aus, die er infiziert. Dazu können einfache Word-Dokumente, Text-Dateien, Skripte, Programmbibliotheken und alle anderen Dateien auf einem Computer gehören.

Trojaner = leiten ihren Namen vom Trojanischen Pferd ab: Als nutzbringende Anwendung getarnt schleicht sich damit ein Schadprogramm auf dem Rechner ein. Die Tarnung erfolgt meist über unauffällige Dateinamen, die beispielsweise nach Systemdateien benannt sind. Viele Nutzer wissen daher gar nicht, dass ihr Computer von einem Trojaner befallen ist. In der Regel haben Trojaner das Ziel, Passwörter und ähnliche Daten auszuspähen oder den Computer für illegale Zwecke fernzusteuern.

Würmer = kommen ohne Wirtsprogramm aus. Es handelt sich um eigenständig lauffähige Schadprogramme, die sich meist unter unverdächtigem Namen irgendwo in den Tiefen des Betriebssystems verbergen. In Aktion treten Würmer ohne Zutun der Benutzer – im einfachsten Fall etwa durch einen entsprechenden Eintrag in die automatisch ablaufende Startfunktion des Betriebssystems. Sobald der Wurm erwacht ist, könnte er beispielsweise die Kontaktordner auf dem System durchforsten und eine Kopie seiner selbst als Anhang an alle gefundenen E-Mail-Adressen versenden. Öffnet einer der Empfänger das Programm im Anhang, hat der Wurm den Sprung auf ein neues System geschafft.

Weitere Typen von Schadprogrammen: Rootkits, Botnets, Ransomware, Adware, Spyware

Schutz vor Schadsoftware

- Wenn man sich nicht sicher ist, niemals auf Links klicken oder Anhänge öffnen. Gilt insbesondere für E-Mails (unerwartete und nicht angeforderte E-Mails, evtl. E-Mail-Absender anrufen, ob die E-Mail mit Anhang von ihm stammt).

- Nur sichere Software installieren (Chip, CT, bekannte App-Stores). Im Zweifel nach der Software suchen, um evtl. mehr Informationen darüber zu erhalten (z. B. bereits gemeldete Schadsoftware).
- Nicht auf auffällige Werbebanner klicken. Wenn anschließend Fenster aufgehen, die Warnungen enthalten, immer mit dem „X“ oben rechts schließen oder Alt+F4. Niemals auf „OK“ oder „Abbrechen“ oder sonstige Buttons klicken.
- Programme und Betriebssystem durch Updates aktuell halten
- Nie ohne Virenschutz und eingeschalteter Firewall im Netz surfen. Firewall ist in der Regel standardmäßig aktiviert. Sicherheitshalber jedoch überprüfen (Windows – Einstellungen – nach Firewall suchen)

Infektionen mit Schadsoftware erkennen

- Plötzlicher Leistungsabfall
- Häufige Abstürze und Einfrieren
- Gelöschte oder beschädigte Dateien
- Pop-up-Werbung und Browser-Umleitungen
- Merkwürdige Nachrichten von den eigenen Kontakten (Nachrichten, die man selbst nicht geschrieben hat)
- Lösegeldforderungen (Ransomware, Verschlüsselung, Lösegeld für die Entschlüsselung

Aktionsplan bei Befall mit Schadsoftware

- Virenschutz schlägt Alarm (er funktioniert, entweder Löschen oder Quarantäne, Quarantäne bevorzugen, da die Dateien bei einem Fehlalarm leicht wieder hergestellt werden können), im Unternehmen, wenn vorhanden, IT-Abteilung informieren
- Mit einem anderen Gerät nach bereits bekannten Symptomen im Netz suchen.
- Rechner vom Internet trennen (Netzstecker und WLAN – Vermeidung der Weiterverbreitung)
- Wenn nichts hilft – Rechner formatieren (das lückenlose Löschen sämtlicher Daten auf dem Datenträger). Danach das Betriebssystem neu aufsetzen. Evtl. benötigt man dazu Hilfe. Backup der Daten einspielen. Hier Digitalen Ersthelfer oder BSI anrufen (**0800 274 1000)**

Doris G. Hohenwald