INFEKTION MIT SCHADPROGRAMMEN: CHECKLISTE FÜR DEN ERNSTFALL

Ein Schadprogramm ist eine Software, die unerwünschte und meist schädliche Funktionen auf einem infizierten PC, Smartphone oder anderem internetfähigem Gerät wie einem Router ausführt. Oft gelangt Schadsoftware unbemerkt auf ein System, z. B. beim Surfen im Internet oder beim Öffnen von Dateianhängen.

Cyberkriminelle nutzen Schadsoftware beispielsweise für Datendiebstahl, Onlinebetrug oder digitale Erpressung. Das bedeutet auch: Wenn die Schadsoftware es den Kriminellen einmal erlaubt, auf das infizierte Gerät zuzugreifen, können sie mitunter etwa Spam-Nachrichten verschicken oder Passwörter mitlesen.

SO ERKENNEN SIE SCHADPROGRAMME

Wenn Sie einen Sperrbildschirm mit einer Zahlungsforderung sehen, handelt es sich zweifelsfrei um einen Erpressungsversuch mit sogenannter Ransomware. In anderen Fällen können Sie Ihr Gerät jedoch trotz Schadsoftware weiterhin nutzen. Gefährlich ist, dass womöglich Kriminelle zum Beispiel auf Ihre Daten zugreifen können, ohne dass Sie dies mitbekommen. Hinweise sind etwa Meldungen Ihres Antivirenprogramms oder die Anzeige Ihnen unbekannter Programme.

Ebenso deutet es auf ein Schadprogramm hin, wenn ein Gerät langsamer als gewohnt läuft, öfter abstürzt oder der Akku sich schneller entlädt. Auch werden möglicherweise in Ihrem Namen Spamnachrichten an Ihre Kontakte verschickt oder ohne Ihr Zutun andere Aktivitäten wie das Öffnen von Webseiten ausgeführt. In manchen Fällen lassen sich auch Dateien nicht mehr ändern oder abspeichern, Updates werden nicht mehr automatisch heruntergeladen.

DAS SOLLTEN SIE TUN, WENN…

… auf Ihrem Gerät ein Schadprogramm installiert wurde oder Sie dies vermuten:

- ✓ **Trennen Sie das Gerät vom Netzwerk:** Schalten Sie das WLAN aus und entfernen Sie das Netzwerkkabel, falls Sie ein solches verwenden.
- ✓ **Starten Sie einen Virenscan:** Führen Sie auf dem Gerät einen Offline-Virenscan durch. Achten Sie darauf, dass Sie für Ihr Virenschutzprogramm alle verfügbaren Updates installiert haben.
- ✓ **Setzen Sie das System neu auf:** Aufgrund der möglichen Änderungen am System durch das Schadprogramm sollte grundsätzlich eine Neuinstallation des Betriebssystems vorgenommen werden. Smartphones und Tablets sollten Sie auf Werkseinstellungen zurücksetzen.
- ✓ **Ändern Sie Ihre Passwörter:** Beginnen Sie mit dem E-Mail-Konto, das Sie zum Zurücksetzen anderer Passwörter benötigen. Aktivieren Sie außerdem die Zwei-Faktor-Authentisierung für alle Benutzerkonten, für die dies möglich ist.

Eine umfangreiche Schritt-für-Schritt-Anleitung für die Infektionsbeseitigung von Schadsoftware auf PC, Smartphone und Tablet sowie weiteren smarten Geräten finden Sie auf:

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei

… Sie mit Ransomware erpresst werden:

Mithilfe von Ransomware verschlüsseln Kriminelle Daten auf den Geräten ihrer Opfer oder sperren den Systemzugriff. Sie unterbinden also, dass ihre Opfer wie gewohnt auf ihre Daten und ihr System zugreifen können. Für die Freigabe wird ein Lösegeld verlangt.

- ✓ **Kein Lösegeld zahlen:** Dass die Täterinnen und Täter Ihren Zugang wiederherstellen, ist nicht garantiert. Auch ermutigen Sie Kriminelle so zu weiteren Forderungen und Angriffen.
- ✓ **Anzeige bei der Polizei erstatten**: Wenden Sie sich direkt an eine zentrale Ansprechstelle für Cybercrime. Eine Übersicht finden Sie unter: www.polizei.de.
- ✓ **Entschlüsselung prüfen:** Eine Zusammenstellung kostenfreier Entschlüsselungstools gibt es auf www.NoMoreRansom.org. Das Projekt wird von Europol-EC3 in Zusammenarbeit mit behördlichen und privatwirtschaftlichen Partnern betrieben.
- ✓ **Setzen Sie das System wie oben beschrieben neu auf und ändern Sie ebenso Ihre Passwörter.**

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR SCHADPROGRAMMEN

- › **Updates durchführen:** Installieren Sie regelmäßig und zeitnah alle bereitgestellten Sicherheitsupdates. Aktivieren Sie möglichst die Einstellung „automatische Updates“.
- › **Schutzprogramme nutzen:** Aktivieren Sie Ihr Antivirenprogramm sowie Ihre Firewall. Halten Sie auch diese mithilfe von regelmäßigen Sicherheitsupdates auf dem neuesten Stand.
- › **Nutzerkonten einrichten:** Verwenden Sie beim alltäglichen Arbeiten nur ein Benutzerkonto mit reduzierten Rechten. So verhindern Sie, dass Schadprogramme Administratorenrechte erhalten und auf diesem Weg breiten Handlungsspielraum erlangen.
- › **Anhänge und Links prüfen:** Seien Sie vorsichtig beim Öffnen von Links und Anhängen beispielsweise aus E-Mails oder Chatnachrichten — auch bei vermeintlich bekannten Absendern. Deren Angabe kann in den meisten Fällen einfach gefälscht werden.
- › **Vorsicht bei Downloads:** Laden Sie beispielsweise Programme und Apps nur aus vertrauenswürdigen Quellen herunter.
- › **Daten sichern:** Legen Sie regelmäßig Back-ups wichtiger Daten an. Sollten Ihre Daten von Unbefugten verschlüsselt oder beschädigt werden, können Sie diese dann vergleichsweise einfach wiederherstellen.

Mehr Informationen rund um Cybersicherheit:
www.bsi.bund.de/VerbraucherInnen

Mehr Informationen für Opfer von Internetkriminalität:
www.polizei-beratung.de/opferinformationen/cybercrime/

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen,
dass Sie
sicher leben.
Ihre Polizei