Ulrike Ruge

Infektionsbeseitigung

Sofortmaßnahmen

Sie müssen davon ausgehen, dass das Schadprogramm Passwörter und Zugangsdaten ausgespäht hat. Begeben Sie sich daher umgehend an einen von Schadprogrammen sauberen Rechner und ändern alle wichtigen Passwörter, die Sie im Internet benutzen. Prüfen Sie weiterhin Ihre Kontoauszüge auf fehlende oder falsche Buchungen. Ähnlich sollten Sie bei allen Kundenkonten - beispielsweise bei Online-Händlern und Auktionshäusern verfahren, um auszuschließen, dass ein Unberechtigter in Ihrem Namen Geschäfte getätigt hat.

Rechner säubern oder neu aufsetzen?

Die Beseitigung von Schadprogrammen ist immer eine heikle Sache. Es gibt inzwischen mehr bösartige als gutartige Programme. Die Hersteller von Viren-Schutzprogrammen haben es daher nicht leicht, alle Bedrohungen zu erkennen und dann auch im Falle eines Falles zu entfernen. Aktuelle Schadprogramme werden in den ersten Stunden/Tagen nicht gefunden. Kein Fund des Viren-Schutzprogrammes bedeutet somit nicht, dass der Rechner nicht doch infiziert ist

Wenn Sie Ihren Rechner beispielsweise geschäftlich oder für Bankgeschäfte nutzen, müssen Sie auch nach einer beseitigten Infektion sehr vorsichtig sein, da nie hundertprozentig sicher ist, dass das Schadprogramm vollständig entfernt wurde.

Häufig verändern Schadprogramme auch sicherheitsrelevante Einstellungen des Betriebssystemes, die nicht immer einfach rückgängig gemacht werden können.

Um auf Nummer Sicher zu gehen, spielen Sie ein vertrauenswürdiges komplettes Backup des Rechners von einem Zeitpunkt vor der Infektion zurück oder installieren Sie den Rechner neu.

10 Dinge, die Sie bei einer Infektion tun sollten:

1. Bei Verdacht auf einen Schadprogramm-Befall sollten Sie die Arbeit schnell, aber wie gewohnt beenden. Vor allem gilt: Keine Panik!
2. Schalten Sie den Computer aus.
3. Wenn Sie kein Experte sind, holen Sie sich lieber den Rat eines solchen ein. Manchmal ist zur Beseitigung von Schadprogrammen besondere Fachkenntnis erforderlich, da diese sich in ihrer Arbeits- und Wirkungsweise stark unterscheiden können.

u.ruge@uni-oldenburg.de * 04 41/36 10 95 66 * 0151 59 46 96 10

4. Stellen Sie die Bootreihenfolge im BIOS so ein, dass in der Boot-Reihenfolge das CD-Laufwerk an erster Stelle aufgeführt ist. (Normalerweise ist der Rechner so voreingestellt, dass er als erstes von der Festplatte bootet Bootreihenfolge ändern.) Legen Sie eine viren-freie System- beziehungsweise Boot-CD in das CD-Laufwerk ein und booten Sie den Rechner von dieser CD.
5. Bei Windows 10 müssen Sie über Einstellungen – Updates -
6. Überprüfen Sie den PC mit einem Sicherheits- Schutzprogramm. Achten Sie hierbei darauf, dass die so genannten Viren-Signaturen (der Teil des Viren-Schutzprogramms, der die Schadprogramme aufspürt) auf einem aktuellen Stand ist. Ansonsten besteht die Gefahr, dass ein "aktuelles" Schadprogramm nicht gefunden wird!
7. Sichern Sie Ihre Daten, falls noch nicht geschehen.
8. Entfernen Sie das Schadprogramm abhängig vom jeweiligen Typ. In der Regel macht Ihr Anti-Viren-Programm das automatisch. Sollte das nicht klappen, so können vom Hersteller der Anti-Viren-Programme mitgelieferte Viren-Datenbanken Hilfestellungen geben. Darin sind die Funktionsweise und die Behebung oftmals detailliert beschrieben.
9. Lassen Sie die Festplatte und alle anderen Datenträger noch einmal überprüfen, um sicherzugehen, dass das Schadprogramm auch wirklich komplett entfernt wurde. Stellen Sie die Boot-Reihenfolge des Rechners anschließend wieder so ein, dass als erstes von der Festplatte gebootet wird.
10. Sollte das Schadprogramm Daten gelöscht, verschlüsselt oder verändert haben, versuchen Sie, die Daten aus den Datensicherungen und die Programme aus den Sicherungskopien der Programme zu rekonstruieren.
11. Versuchen Sie abschließend die Ursache der Schadprogramm-Infektion festzustellen. Ist die Quelle auf Original-Datenträger zurückzuführen, dann sollten der Hersteller informiert werden. War die Ursache eine Datei oder E-Mail, dann benachrichtigen Sie den Ersteller oder Absender der Datei. Wenn Sie Daten von einem infizierten Rechner verschickt haben, dann warnen Sie auch die Empfänger Ihrer Daten.

u.ruge@uni-oldenburg.de * 04 41/36 10 95 66 * 0151 59 46 96 10