CIP-Pool-Team
Juristisches Seminar
Platz der alten Synagoge 1

79085 Freiburg

Haftungshinweis: Wir weisen darauf hin, dass bei der Verwendung der von uns genannten Virenprogramme (Software, Online-Scanner, etc.) die Nutzungsbedingungen der jeweiligen Hersteller gelten.
In diesen wird u.a. davor gewarnt, dass die Verwendung von Antivirenmaßnahmen zu unerwünschten Datenverlusten oder zu einem Systemzusammenbruch führen kann.

Informationsblatt: Mein USB-Stick/ PC ist von Viren befallen,…

Bitte zunächst dieses Handout sorgfältig & komplett lesen und dann (evtl.) handeln!

1. USB-Stick säubern

Um den USB-Stick zu desinfizieren, benutze einen der CIP-Pool Rechner. Öffne den Arbeitsplatz, mache einen Rechtsklick auf das Laufwerk F: (Das ist der Laufwerks-Buchstabe deines USB-Sticks) und wähle „*Mit Sophos Anti-Virus überprüfen*“. *N*ach dem Scanvorgang müssen die Funde noch gelöscht werden. Hierzu mache einen Rechtsklick auf das blaue Schild in der Taskleiste unten rechts und wähle „Sophos öffnen“ aus. Unter „Quarantäne“ findest Du die infizierten Dateien, markiere alle und klicke auf „entfernen“. Jetzt sollte der USB-Stick erstmal wieder virenfrei sein. Zur Sicherheit benutze ihn nur an Rechnern, bei denen Du sicher bist, dass sie „sauber“ sind, z.B. im CIP-Pool.

2. Transportwege

Nun muss man sich die Frage stellen, woher die Viren kamen. Welche PCs benutze ich außerhalb der CIP-Pools (PC zuhause, Laptop oder Freunde)? Informiere die Besitzer, Freunde oder Familie darüber, dass dein USB-Stick mit Viren verseucht ist oder war und die jeweiligen PCs mit großer Wahrscheinlichkeit es nun auch sind.

PC zuhause „säubern“

1. Vorbereitung

Sichere zunächst die wichtigen Daten (z.B. Haus- oder Doktorarbeiten, Fotos, E-Mails, Linklisten, Korrespondenz, etc.)!
Brenne diese auf CD/DVD und verwahre diese erstmal sicher.

HINWEIS: Die Vorgehensweise wurde von uns getestet. In Abhängigkeit von der Schwere des Befalls können die folgenden Schritte aber dazu führen, dass Windows nicht mehr funktionsfähig ist und Daten verloren gehen. Die Durchführung der beschriebenen Maßnahmen erfolgt daher auf eigene Gefahr.

2. Diagnose

Jetzt möchtest Du Gewissheit darüber bekommen, ob Dein Rechner befallen ist. Wir haben hierfür gute Erfahrungen mit dem Online-Scanner von Kaspersky gemacht.
Öffne im Internet Explorer http://www.kaspersky.com/de/virusscanner , wähle den Kaspersky Online-Scanner aus und folge den Anweisungen. Scanne damit Deinen ganzen PC.
Das Ergebnis enthält die Information über die Anzahl der Infektionen sowie weitere Details. Die Protokolldatei sollte zur weiteren Behandlung bzw. Rekonstruktion des Virenbefalls ausgedruckt und aufgehoben werden.
Ambitionierte könne sich gerne die Details zu den gefundenen Schädlingen anschauen. Werden hierbei Keylogger oder Backdoors erwähnt, empfiehlt es sich, sämtliche Passwörter (E-Mail, Online-Banking, etc.), von einem sicheren PC (z.B. aus dem CIP-Pool) zu ändern.

3. Die Säuberung

Da nun feststeht, dass der Computer von Viren befallen ist, wird im Folgenden eine Möglichkeit vorgestellt, diese hoffentlich erfolgreich zu entfernen. Wurden die Viren unter „C:\WINDOWS\“ gefunden, sollten sicherheitshalber alle weiteren Dateien, deren Verlust schmerzhaft wäre und die in der ***Vorbereitung*** ausgelassen wurden, ebenfalls gesichert werden. **Wichtig** ist es, nach der Desinfektion des Systems die Dateien auf den Sicherungs-CDs noch einmal überprüfen zu lassen. Vorschlag auch hier: Der Kaspersky Online-Scanner.

Ein recht zuverlässiges Tool wird von TrendMicro angeboten:
Scanner: http://de.trendmicro-europe.com/file_downloads/common/tsc/sysclean.com
Virendefinition: http://de.trendmicro-europe.com/enterprise/support/pattern.php
Lade beide Dateien im CIP-Pool herunter. Diese sollten wie folgt heißen: sysclean.com und lptXYZ.zip (XYZ = Zahlenkombination). Erstelle einen Ordner, in den Du die sysclean.com und den Inhalt des Ziparchivs lpt$vpn.XYZ einfügst.
Brenne diesen Ordner nun auf eine CD.

Starte den infizierten Rechner im „Abgesicherten Modus“ (wiederholtes F8-Drücken beim Hochfahren). Lege die erstellte Anti-Viren-CD ein, kopiere den Ordner auf Deinen Computer und starte sysclean.com. Im sich öffnenden Fenster gibt es die Option: „Automatically clean infected files“(infizierte Dateien automatisch löschen). Ist der Haken gesetzt, wird beim Scannen nicht nachgefragt, bevor infizierte Dateien gelöscht werden und der Vorgang kann automatisch durchlaufen. Es werden dem Wortlaut entsprechend alle infizierten Dateien gelöscht. An dieser Stelle nochmals der Hinweis auf die Möglichkeit des Datenverlusts!

Wiederhole diesen Vorgang solange, bis keine neuen Funde auftauchen.

Starte den Rechner neu und benutze zur Sicherheit nochmals den Online-Scanner, um sicherzugehen, dass die Mühen erfolgreich waren.

Prävention

Was Du tun kannst, damit Dein PC weniger anfällig ist.

Das Wichtigste ist, immer die aktuellen Updates und Servicepacks von Microsoft zu installieren.

Servicepack: Windows XP Service Pack 2.
(http://www.microsoft.com/downloads/thankyou.aspx?familyId=049c9dbe-3b8e-4f30-8245-9e368d3cdb5a&displayLang=e)

Updates:
Hier gibt es zwei Möglichkeiten. Entweder Du öffnest mit dem Internet Explorer http://windowsupdate.microsoft.com/ oder Du lädst dir unter http://www.winhelpline.info/ in der Rubrik „Update Packs“ für Dein Betriebssystem die entsprechenden Updates herunter, indem Du einfach der angebotenen, bebilderten Anleitung folgst.

Virenscanner:
Wichtig ist zudem, einen Virenscanner zu installieren. Eine kostenfreie Version bietet Avira: http://www.free-av.de/ Das Programm sollte dann noch konfiguriert
(http://www.chip.de/bildergalerie/c1_bildergalerie_v1_20205340.html?show=33)
werden. Dieser Link dient als Hilfestellung bei Installation und Konfiguration, zusätzlich führt er einmal durchs Programm, daher ist es durchaus sinnvoll, die Anleitung einmal vollständig anzuschauen. Vor allem die Scanner- und Guardeinstellungen sind wichtig, der Rest kann vernachlässigt werden.

Bist Du bereits im Besitz eines Viren-Scanners, benutze einfach mal www.google.de und suche nach dem Namen Deiner Virensoftware, um Hilfe bei der Konfiguration und Einrichtung zu erhalten.

Der wichtigste Faktor bei der Infektion mit Viren ist Dein Umgang mit dem PC:

Benutzt Du Tauschbörsen?
Generell lautet hier der Tipp, die Finger ganz davon zu lassen!

Öffnest Du jede E-Mail von Unbekannten?
Öffne nur Anhänge von Personen, die Du kennst und lass die Finger von Anhängen unbekannter Absender, bzw. lösche einfach lieber eine E-Mail zuviel als zu wenig ☺.

Benutzt Du Daten aus dem Internet?
Archive und .exe-Dateien sollten generell vor der Benutzung auf Viren geprüft werden.

Nun wünschen wir Dir viel Erfolg bei der Bekämpfung der Viren!

Dein CIP-Pool-Team