Entfernung von Malware

Bei einem aktiven Anti-Virus Programm

Wenn Malware bei aktivierten Anti-Virus Programm (On-Access-Modus) gefunden wird, können Sie die identifizierte Malware löschen.

Bei einem nicht aktiven Anti-Virus Programm

Wird Malware erst nach einem Update des Anti-Virus Programms entdeckt, bzw. nachdem Sie ein neues Anti-Virus Programm installiert haben oder Ihr Anti-Virus Programm nicht aktiv war (wöchentliche Untersuchung), ist Ihr System nicht mehr als vertrauenswürdig anzusehen.

Wenn ein System kompromittiert wurde, können alle Daten (Programme, Informationen etc.) manipuliert, an Dritte weitergeben oder bereits (Passwörter usw.) bekannt sein.

Löschen Sie auf keinen Fall die Malware! Es kann vorkommen, dass ein Anti-Virus Programm eine wichtige Datei, die infiziert wurde und nicht wiederhergestellt werden kann, komplett löscht.

Was tun bei einer Viren-Kompromittierung?

Wenn man sich sicher ist, dass das System kompromittiert wurde, müssen folgende Maßnahmen sofort durchgeführt werden:

1. Das betroffene System ist sofort herunterzufahren, um weitere Datenmanipulationen zu verhindern
2. Ein Backup des Systems mit all seinen Daten ist zur späteren Analyse zu empfehlen
   - 2.1. Das Backup zur Analyse muss zwingend von einem sauberen Medium aus geschehen (Boot-CD)
   - 2.2. Analyse des Backups
     - 2.2.1. Infektionsweg identifizieren (bei Trojanern und Würmern das Einfallstor bzw. Sicherheitslücke identifizieren)
     - 2.2.2. Wenn ein sauberes Backup des Systems existiert, können anhand von Prüfsummen Datenmanipulationen aufgedeckt werden
     - 2.2.3. Wichtige Dateien, die nicht kompromittiert wurden sind zu sichern
   - 2.3. Backup zur Beweissicherung (Betriebshaftpflicht) aufbewahren
3. Existiert ein sauberes Backup des Systems, sind folgende Maßnahmen zu treffen:
   - 3.1. Es muss garantiert sein, dass das Backup sauber ist
   - 3.2. Der Infektionsweg muss bekannt sein, damit eine erneute Kompromittierung ausgeschlossen werden kann
   - 3.3. Das saubere Backup aufsetzen
   - 3.4. Zwingend notwendig: alle Passwörter ändern
4. Existiert kein sauberes Backup des Systems, sind folgende Maßnahmen zu treffen:

4.1. Der Infektionsweg muss identifiziert werden, damit eine erneute Infektion ausgeschlossen werden kann
4.2. Wenn kein sauberes Backup zum Vergleich (Prüfsummen) von Daten-manipulationen vorliegt, sind alle Dateien und Programme als kompromittiert anzusehen
4.3. Das System neu aufsetzen
4.4. Zwingend notwendig: alle Passwörter ändern

Rösner-IT:

- ✓ sichert Ihre wichtigen Daten
- ✓ rekonstruiert Ihre Daten bei Virenbefall
- ✓ untersucht die Malware
- ✓ stellt Ihr System wieder her

Rösner-IT ♦ Lönsstr. 16 ♦ 48485 Neuenkirchen
Tel: +49 (0) 5973-90 06 52 ♦ Fax: +49 (0) 5973-90 07 98
E-Mail: info@roesner-it.com ♦ Web: www.roesner-it.com