1 Einleitung

Durch die zunehmende Vernetzung von IT-Systemen wächst die Bedrohung durch Viren stetig und schnell. Ein hundertprozentiger Schutz vor Schadsoftware ist nicht zu erreichen, aber mit einfachen Maßnahmen lassen sich viele Risiken minimieren.

Diese Handreichung soll Sie bei der Vorsorge unterstützen und auch Hilfen geben, wenn doch einmal der Fall einer Infizierung eingetreten ist.

2 Verbreitungswege

Im Folgenden sollen einmal einige mögliche Verbreitungswege für Schadsoftware genannt werden:

- E-Mails mit "verseuchten" Anhängen
  Mit einer E-Mail wird ein Anhang versendet, der zum einen interessant wie auch harmlos erscheint (z.B. ein Word-Dokument, Fotos oder auch PDF-Dokumente). In diesen Dokumenten können relativ leicht Schadprogramme versteckt werden.

- Drive-by-Downloads
  Im Grunde genommen muss der Anwender heute nicht mehr zweifelhafte und verseuchte Software ausführen, um den Rechner mit einem Virus zu infizieren. Es reicht schon aus, bestimmte manipulierte Webseiten aufzurufen. So kann man sich sozusagen im Vorbeigehen einen Virus einfangen und unbeabsichtigt Schadsoftware auf seinen Rechner herunterladen.

- Verwendung von USB-Speichergeräten
  Eine weitere recht häufige Verbreitung von Viren erfolgt durch die Verwendung von externen Speichergeräten wie z.B. USB-Sticks. Für einige Viren reicht das einfache Einstecken eines USB-Sticks in den Computer aus, damit sich diese Viren selbstständig auf den Stick kopieren. Wird der Stick nun in einen anderen Rechner gesteckt, so überträgt er sich unbemerkt auf diesen Rechner. Ein Beispiel dafür ist der recht weit verbreitete Computerwurm Conficker.

- Download von Free- oder Shareware
  Bei der Installation von kostenloser Software sollte man besonders vorsichtig sein, denn gern wird diese Software als sogenanntes trojanisches Pferd missbraucht. Neben einer sinnvollen Anwendung installiert man unbemerkt auch Schadsoftware auf seinem Rechner.

3 Erkennung der Infizierung

Häufig erkennt man über lange Zeit nicht, dass sein Rechner mit Schadsoftware infiziert ist. Die Programme schlummern still und warten darauf, dass sie aktiviert werden. Das kann zum Beispiel durch bestimmte Ereignisse wie das Erreichen eines definierten Datums oder durch entfernte Rechner, sogenannter Bot-Master, geschehen.

In den meisten Fällen kann man den Befall mit Schadsoftware jedoch erkennen durch:

- Meldungen eines installierten Antiviren-Programms
- Eine Sicherheitswarnung des Internet-Providers
- anormales Verhalten des Rechners (langsam, bestimmte Seiten im Web nicht aufrufbar)
- Funktionsunfähigkeit oder häufiges Abstürzen des Rechners
- Offensichtliche Erpressung des Nutzers (Aufforderung zur Geldüberweisung, um den Rechner wieder zu entsperren)

4 Vorbeugen ist besser als Heilen.

Die Entseuchung eines mit Schadsoftware befallenen Rechnersystems ist extrem zeitaufwändig und erfordert ein hohes Maß an Fachwissen. Besser ist es vorzubeugen:

- Information des Kollegiums über Gefahren
  Ein entscheidender Faktor für die Gewährleistung der IT-Sicherheit ist trotz aller technischen Maßnahmen immer noch der Mensch. Die meisten Fehler lassen sich vermeiden, wenn der Nutzer über die Risiken informiert ist.

- Installieren von Updates
  Ein unablässiger Schutz für das Computersystem ist die Aktualität der eingesetzten Software. Dazu müssen bei allen Programmen und natürlich auch beim Betriebssystem die relevanten Updates immer installiert werden. Damit werden wichtige Sicherheitslücken, über die das Einschleusen von Schadsoftware erfolgen kann, in den Programmen und Anwendungen geschlossen.

- Nutzen eines Antiviren-Programms
  Bis zu 30.000 neue Viren kommen täglich hinzu. Deshalb ist der regelmäßige Einsatz eines leistungsstarken Antiviren-Programms notwendig.

- Beachten von Warnhinweisen
  Die Hersteller der Betriebssysteme wie z.B. Microsoft sind daran interessiert, dass ihre Systeme zuverlässig funktionieren. Entsprechend implementieren sie von Hause aus zunehmend Sicherheitsvorkehrungen. So erhält der Nutzer weitestgehend Hinweise, wenn er sicherheitskritische Aktionen auf dem Rechner ausführen möchte. Diese wichtigen Hinweise sollten unbedingt ernst genommen und aufmerksam gelesen werden.
  Das bedenkenlose Agieren der Benutzer wird durch die Cyber-Kriminellen ausgenutzt, um Schadsoftware auf den Rechner zu platzieren.

5 Erstmaßnahmen bei Virenbefall

Trotz aller Vorsichtsmaßnahmen kann Schadsoftware auf den Rechner gelangen. Was ist zu tun?

- Trennen Sie den als befallen erkannten Rechner vom Netzwerk und nehmen Sie ihn außer Betrieb.

- Information des regionalen IT-Sicherheitsbeauftragten,
  damit er Sie bei der Lösung des Problems unterstützen kann.

- Informieren Sie alle Nutzer
  Bei einem Virenbefall im Netzwerk sind die infizierten Rechner nicht immer sofort zu identifizieren. Deshalb ist es notwendig, alle Nutzer im Netzwerk über die entstandenen Sicherheitsprobleme zu informieren.

- Alle Rechner im Netzwerk auf Viren mit verschiedenen Virenscannern prüfen
  Nicht alle Antiviren-Programme finden immer alle Viren. Deshalb wird empfohlen, verschiedene Virenscanner einzusetzen. Häufig ist das System dermaßen verseucht, dass ein Starten des Rechners mit einem anderen, virenfreien Betriebssystem erst einmal zwingend erforderlich wird. Erst dann können Antiviren-Programme erfolgreich das System scannen.

- Einbeziehung von allen Systemen (Gast-Zugänge)
  In die Betrachtungen müssen unbedingt auch Gast-Systeme eingeschlossen werden. Können z.B. im Netzwerk auch „fremde“ Geräte eingebunden werden (z.B. das private Notebook eines Kollegen)? Könnten diese Geräte möglicherweise Ursache für eine missbräuchliche Nutzung des Internet-Zugangs sein? Können diese Geräte zumindest vorübergehend aus dem Netzwerk ausgeschlossen werden?
  Grundsätzlich sind infizierte Rechner vom lokalen Netz und auch vom Internet zu trennen, um eine weitere Verbreitung der Schadsoftware zu unterbinden.

- Alle externen Datenträger wie USB-Sticks, USB-Festplatten etc. auf Viren prüfen
  Es ist fatal, wenn mit großem zeitlichen Aufwand die Systeme von Schadsoftware befreit wurden, sie dann aber durch einen verseuchten USB-Datenträger wieder infiziert werden. Deshalb müssen die verwendeten externen Speichergeräte unbedingt auch auf Virenbefall untersucht werden.
  Viele professionelle Antiviren-Programme können alle Schreib- und Lesezugriffe auf externe Speicher auf Viren überprüfen.

- WLAN-Konfiguration prüfen, ob darüber unberechtigter Netzzugang möglich ist
  Drahtlose Netzwerke bieten viel Komfort beim Netzzugang. Aber sie stellen aus Sicht der IT-

Sicherheit ein hohes Risiko dar. Ein offenes WLAN, in das sich frei alle Geräte einwählen können, ist praktisch nicht kontrollierbar. Hier können jederzeit neue Schadsoftware in das Netz eingeschleust werden. Aus diesem Grund sind WLAN-Strukturen speziell zu betrachten und abzusichern.

- Generell alle Passwörter ändern (alle Nutzer - alle Passwörter)
  Eine spezielle Kategorie von Schadsoftware ist die sogenannte Spyware. Diese Programme versuchen das System auszuspionieren und an die Passwörter der Benutzer zu kommen. Deshalb müssen unbedingt sämtliche Passwörter geändert werden. Dies betrifft die Passwörter der Benutzer und auch Systempasswörter wie z.B. die von Servern und WLAN-Routern.

- PowerLAN-Passwörter der Verschlüsselung ändern
  PowerLAN bezeichnet eine Vernetzungsmöglichkeit über die Elektro-Verteilung im Haus. Findet diese Technologie Einsatz, so müssen auch hier die Passwörter zu Verschlüsselung der Übertragung von Daten geändert werden, um die Nutzung durch Unbefugte zu unterbinden.

- Wird ein Virus auf einem Rechner entdeckt, ist die sicherste Methode eine komplette Neuinstallation des Systems, um den Virus zu entfernen.

6 Wo bekommt man Hilfen

- Ansprechpartner Regionaler IT-Sicherheitsbeauftragter
  Der Schutz von Computersystemen vor Schadsoftware ist ein wichtiger Bestandteil der IT-Sicherheit und damit eine elementare Aufgabe des IT-Sicherheitsbeauftragten. Er kann Strategien zur Vorbeugung und viele Hinweise für die Bekämpfung von Malware geben.

- im Internet
  Fast alle Informationen rund um dieses Thema findet man selbstverständlich auch im Internet. Die Hersteller von Antiviren-Programmen bieten eine große Zahl von Informationen. In einschlägigen Foren bekommt man wertvolle Hinweise und Anregungen bei sehr speziellen Problemen. Man kann mit Sicherheit davon ausgehen, dass andere die gleichen Fragestellungen haben, Lösungen schon entwickelt wurden und diese auch der Gemeinschaft zur Verfügung gestellt sind.

- kleine Linksammlung

  - www.bsi.bund.de
    Homepage des Bundesamt für Sicherheit in der Informationstechnik

  - www.buerger-cert.de
    Hier findet man sehr wertvolle Hinweise auf die aktuellen Gefahren durch Schadsoftware. Hier kann man z.B. verschiedene Newsletter beantragen, um stets zu Fragen der IT-Sicherheit aktuell informiert zu werden.

  - www.bsi-fuer-buerger.de
    Dies ist eine sehr zu empfehlende Seite, auf der verständlich viele Fragen rund um das Thema IT-Sicherheit erklärt werden.

  - www.heise.de/security
    Der Heise-Verlag stellt hier online eine sehr gute Plattform zum Thema IT-Sicherheit bereit.

  - www.botfrei.de
    Dies ist eine sehr gute Ausgangsbasis, wenn man sein System auf Viren und andere Schädlinge hin untersuchen möchte.

- Service-Firmen
  Die Suche nach Schadsoftware und deren Entfernung im Falle einer Verseuchung ist sehr zeitaufwändig und erfordert ein hohes Knowhow.
  Wenn Sie die Möglichkeiten haben, dann überlassen Sie diese Aufgaben Spezialisten.