Warnsignale für Malware-Befall der Unternehmens-IT

Wie man eine Infektion erkennen und bekämpfen kann

Malware, damit sind Viren, Würmer und Trojaner gemeint, das sind Programme, die Böses im Schilde führen. Dazu schleichen sie sich unbemerkt auf den Computer, indem sie z.B. Huckepack mit einer Datei kommen, die eigentlich harmlos aussieht. Einmal auf dem Rechner können sie vieles anrichten, vom Versand von Massenmails bis zur Protokollierung der Tastatureingaben. Gute Virenprogramme erkennen die meisten dieser Schadprogramme, aber leider nicht alle. In diesen Fällen hilft aufmerksame Beobachtung, es gibt einige Indizien, hinter denen sich meistens ein Malware-Angriff verbirgt.

Seltsames Verhalten

Man kennt ja seinen Computer, er ist ein ständig genutztes Werkzeug. Wenn der Rechner plötzlich merkwürdiges Verhalten zeigt, ist wohl von einem Befall mit Malware auszugehen. Beispielsweise werden Fenster unvermittelt geschlossen oder es öffnen sich unerwartet welche, die schwer zuordenbare Informationen anzeigen. Auch wenn sich die Startseite des Internet-Browsers ohne Zutun ändert oder neue Lesezeichen auftauchen hat man sich mit hoher Wahrscheinlichkeit infiziert.

Hohe Prozessorauslastung

Es gibt Malware, die die Rechenleistung der befallenen Computer nutzt um komplexe Aufgaben zu lösen. Das kann das Knacken von Passwörtern oder die Generierung neuer Bitcoins (eine virtuelle Währung, die als Zahlungsmittel im Internet anerkannt wird, bei Hackern sehr beliebt) sein. Das belastet den Computer aber oft über das normale Maß. Das Starten von Programmen kann sich so verlangsamen oder der kühlende Ventilator springt öfter als gewohnt an, generell leidet einfach die Performance des Systems unter dem Missbrauch.

Erhöhter Datenverkehr

Eine der Haupteigenschaften von Trojanern und Würmern ist es, dass sie sehr aktive Datensender und -empfänger sind. So kann ein Schadprogramm unter anderem einen Rechner dazu nutzen, um gewaltige Mengen an SPAM-Mails (unter anderem Betrug- oder Werbemails) zu versenden. Außerdem bringen aggressive Hacker IT-Systeme oft zum Zusammenbruch, indem sie von tausenden Computern ständig Anfragen auf den angegriffenen Server starten. Auch dafür muss der eigene Rechner vielleicht herhalten. Dies erkennt man durch ein langsameres Internet, verzögerter Seitenaufbau oder langsame Downloads sind weitere Indikatoren dafür.

Mysteriöse Dateien

Es gibt auch Schadprogramme, die sich einen Spaß daraus machen, die Dateien des Rechners innerhalb der Ordner zu verschieben. Ernster wird es aber, wenn neue Dateien installiert werden, die z.B. Tastatureingaben oder das Surfverhalten protokollieren oder wenn wichtige Files einfach verschwinden. Möglich ist auch, dass ihre Dateien plötzlich durch ein Kennwort "geschützt" werden, das der Hacker nur nach Bezahlung eines Lösegelds bekannt gibt. Änderungen in der Struktur des Dateisystems (neue Ordner, Files „wandern“) sind also ebenfalls ein mögliches Anzeichen von Malware auf dem Rechner.

Ungewöhnlicher Posteingang

Wenn im Posteingang Nachrichten über unzustellbare Mails auftauchen, die sie nie versendet haben, oder Kollegen sich über SPAM von ihrer Mailadresse beschweren, ist wohl ein Programm am Werk, das unerwünschte Nachrichten an ihre Adressbücher verschickt. Auch die Kontaktlisten von Kommunikationstools wie Facebook oder Skype werden dazu oft angezapft. In diesem Fall sollten die potentiellen Adressaten kontaktiert werden, da auch sie wahrscheinlich das Schadprogramm mittlerweile auf dem Computer haben.

Was tun?

Als erstes sollte man kontrollieren ob der Virenscanner auf dem aktuellen Stand ist und alle Sicherheitsvorkehrungen (z.B. Firewall) aktiv sind. Hat man den leisen Verdacht, dass der Rechner von Malware infiziert wurde, gibt es Diagnosetools, mit denen man die Prozessorauslastung, den Datenverkehr und vieles mehr auslesen kann. Solche Programme sind oft Teil des Betriebssystems, wem das nicht reicht, findet ein großes Angebot solcher Programme im Netz.

Erhärtet sich die Befürchtung, sollte man den Computer sofort vom Internet trennen, denn man wird nach dem Befall meist selbst zum Verteiler der bösartigen Programme. Wenn man die Malware sogar identifizieren kann (z.B. bei Windows über den Task-Manager), findet man ziemlich sicher im Internet mögliche Methoden zum Entfernen der Schädlinge. Generell sollte man bei einem Befall aber möglichst schnell einen Experten hinzu ziehen, der die richtigen Schritte einleitet, damit die Malware dauerhaft verschwindet.

Stand: 20.11.2019