# Konto gesperrt, Horrorrechnung, Operation nicht mehr möglich? - Ihr Beitrag zum Schutz vor Erpressungstrojanern (Ransomware)

Autoren: Eberhard Kiesche/Christof Scharrer Stand: 09.07.2021; siehe SZ v. 7.7.2021, S. 15

In jüngster Zeit haben Ransomware-Attacken drastisch zugenommen. Erpresser-Trojaner verbreiteten sich per Mail und infizieren zehntausende Rechner. Auch deutsche Krankenhäuser wurden 2016 Opfer von Ransomware-Angriffen. Einer Studie zufolge zahlt jedes dritte Opfer von Erpressungssoftware das geforderte Lösegeld. Behörden wie z.B. das Bundesamt für Sicherheit in der Informationstechnik (BSI) raten davon ab und empfehlen, stattdessen Anzeige bei der Polizei zu erstatten.

Kaum ein Tag vergeht in den Nachrichten, in dem nicht vor einer neuen Variante von Erpressungstrojanern (Ransomware) gewarnt wird. Doch was genau tun diese Trojaner eigentlich? Und warum sollten Sie wissen, wie Sie sich davor beruflich und privat schützen können? Erpressungstrojaner verschlüsseln Ihre Dateien, Bilder und Videos. Sie können mit Ihren eigenen Daten nichts mehr anfangen. Zwar bieten einige Erpresser gegen anonyme Zahlung einer Geldsumme an, Ihnen den Code zur Entschlüsselung zu übersenden. Ob sie das allerdings tun, wenn die erpresste Summe gezahlt ist und ob hinterher alles wieder so funktioniert wie vorher, ist nicht sicher.

Wenden Sie sich bei einem Angriff im Unternehmen/in der Behörde stets an Ihre IT-Abteilung oder an den Verantwortlichen und erstatten Sie unverzüglich Meldung. Werden Sie im privaten Umfeld Opfer eines Erpressungsvirus, wenden Sie sich an die Polizei und suchen Sie auch im Netz nach der verwendeten Virus-Variante. Für etliche dieser Programme sind die Schlüssel inzwischen bekannt.

Mit den nachfolgenden Tipps können Sie das Risiko einer Infektion Ihres Computers oder von Netzwerken im Unternehmen und auch im privaten Umfeld verringern:

- Da Erpressungs-Trojaner überwiegend per E-Mail-Anhang verbreitet werden, lassen Sie hier besondere Sorgfalt walten.
- Sollten Sie in einer E-Mail einen unerwarteten Anhang vorfinden, mit dem Sie nicht gerechnet haben - auch wenn er wie eine harmlose Excel-Tabelle oder sonstige Office-Datei aussieht - klicken Sie niemals darauf, sondern halten im Zweifel erst Rücksprache mit dem Absender, ob er Ihnen diese Datei wirklich gesendet hat. Noch mehr gilt dies natürlich für E- Mails mit Dateianhang von Ihnen völlig fremden Absendern.
- Die meisten Trojaner werden erst beim Ausführen eines E-Mail-Anhangs aktiv. Das heißt, beim Empfang eines unerwarteten Anhangs müssen Sie noch nicht in Panik verfallen.
- Office-Dokumente (Word, Excel, Powerpoint etc.) können Makros enthalten. Diese zu öffnen ist genauso gefährlich wie das Ausführen einer .exe-Datei! Makros können Code aus dem Internet nachladen und ausführen. Sollten Sie der Datei also nicht hundertprozentig vertrauen, erlauben Sie auf keinen Fall die Ausführung der enthaltenen Makros.
- Dasselbe gilt für das Versenden von Office-Dokumenten. Wenn es sich vermeiden lässt, sollten Sie keine offenen Office-Dokumente versenden - schon aus dem Grund, dass jeder problemlos den Inhalt Ihres Dokuments verändern kann. PDF-Dokumente sind die etwas bessere Option.

- **Regelmäßige** Updates installieren (für die gesamte Hardware PC + Smartphones + Tablets): Halten Sie die eigenen privaten Geräte stets auf dem aktuellen Softwarestand - also die Updates von Betriebssystem und Programmen - regelmäßig einspielen.
- ***Regelmäßige Backups*:** Wer seine Daten regelmäßig sichert, muss keine Angst vor Erpressern haben, sondern kann in der Regel den Rechner neu aufsetzen und die Daten wieder herstellen (WICHTIG: Das Speichermedium mit den Backups ist getrennt vom PC Rechner aufzubewahren).
- **Nur Sicherungen, die auch funktionieren, erfüllen ihren Zweck**. Bei wertvollen Daten schadet es also nicht, hin und wieder zu prüfen, ob diese auch ohne Probleme wieder hergestellt werden können.

Links:

https://www.nomoreransom.org/de/index.html

https://www.heise.de/tipps-tricks/Was-ist-Malware-4614964.html https://www.heise.de/tipps-tricks/So-schuetzen-Sie-sich-vor-Erpresser-Trojanern-3879963.html

https://www.heise.de/tipps-tricks/Ransomware-So-entfernen-Sie-Verschluesselungs-Trojaner-3907507.html

https://de.wikipedia.org/wiki/Penetrationstest_(Informatik)

## Ergänzung am 9.7.2021 (nach dem Angriff auf den IT-Dienstleister Kaseya) - Tipps für professionelle Anwender:

- Setzen Sie Firewalls ein, die auf dem neuesten Stand der Technik sind.
- Virenscanner sind unerlässlich und einzusetzen.
- Setzen Sie interne Systeme ein, die überwachen, welche Daten wohin gehen und überprüfen bzw. aktualisieren Sie regelmäßig Ihre vorhandenen möglichst strengen Zugriffskonzepte (beschränkt auf need to Know).
- Bei einem unbefugten Nutzen z.B. von USB-Sticks sollte stets Alarm ausgelöst bzw. die Nutzung von USB-Sticks weitgehend verboten werden.
- Schulen Sie ihre Mitarbeiter regelmäßig (mindestens jährlich) hinsichtlich der internen Datenschutzvorschriften und Datensicherheitsvorkehrungen (IT-Richtlinie).
- Regelmäßige Backups sind enorm wichtig. Eingesetzte Technik und Sicherheitskopien sind regelmäßig zu überprüfen und vor allem zu testen, ob die Wiederherstellung von Ihren Daten wirklich funktioniert.
- Systeme mit direkter Netzverbindung gegen die „Klassischen“ (Code Injection, SQL-Injection.....) Angriffsvektoren sichern und Gegebenenfalls Penetrationstests durchführen.

Stand: 10.07.2021