Erfolgreich Ramsonware bekämpfen

Dokumentation PERSoft, Schweizer Str. 30, 52428 Jülich, Tel (02461) 348 770

Was ist Ransomware?

Als Ransomware wird eine Software bezeichnet, die Daten auf Ihrem PC verschlüsselt. Anschließend verlangt der Verursacher Geld, meist in Form von Bitcoins, um die betroffenen Dateien wieder zu entschlüsseln.

Wie gelangt die Software auf Ihren PC?

Die Software kann über E-Mails, Downloads, Webseitenbesuch oder unsichere Remote Desktopverbindungen und Fernwartungen in das System gelangen. Denkbar sind auch genutzte Sicherheitslücken des Betriebssystems und der installierten Software, die sich Hacker für die Umsetzung der Ransomware zu Nutze machen.

Wichtig: Meist setzt der eingeloggte Benutzer die Software selbst in Gang, indem er zum Beispiel E-Mails oder Anhänge unkritisch öffnet und damit einen für den ahnungslosen Anwender nicht sichtbaren ausführbaren Code genehmigt. Die Techniken dazu sind sehr ausgefeilt. Sie sind jedoch nicht Thema des Aufsatzes. Die erfolgreiche Umsetzung gelingt jedoch meist nur, weil vor allem menschliche Neugierde und Schwächen mehr dazu beitragen als den meisten Anwendern bewusst ist. Das folgende Beispiel verdeutlicht das Wirkprinzip.

Wie schaffen Sie erste Abhilfe?

Bei E-Mails:

Falls Sie eine ungerechtfertigte Rechnung oder sogar Mahnung per E-Mail zugestellt bekommen, ist der erste Gedanke, den Irrtum aufzuklären und der Sache nachzugehen. Also öffnen Sie die E-Mail und eventuelle Anhänge, um sich zu informieren. Oder Sie erhalten eine Bewerbung, obwohl Sie gar keine Stelle ausgeschrieben haben. Oft werden diese E-Mails geöffnet und aus Interesse und Neugierde „inspiziert“.

Dieses Verhalten ist fatal! Kontrollieren Sie E-Mails im Vorschaufenster auf sprachliche Auffälligkeiten, Stimmigkeit von Informationen und vor allen Dingen, über welche E-Mailadresse das Schreiben versendet worden ist. Ist sie wirklich von der Domain des Unternehmens (z.B. @firma.de) oder Ansprechpartners versendet worden? Oft finden Sie in der Zustelladresse eine Liste von Empfängern, ein deutlicher Hinweis auf Massenmails. Solche E-Mails können Sie unzweifelhaft löschen!

Bei Webseiten:

Auch Pornoseiten oder fragwürdige Downloadportale von Kaufsoft- und Freeware stellen ein erhebliches Sicherheitsrisiko dar. Ihr Besuch wird meist aus Scham verschwiegen. Die Portale von kostenfreien Downloadangeboten sind jedoch äußerst effektiv bei der Verbreitung von Viren, auch von Ransomware. Die Folgekosten solcher Aktionen sind meist wesentlich höher als der Kauf einer Software verursacht hätte, nämlich die für die Neueinrichtung Ihres Systems oder für die gar nicht zu empfehlenden Zahlung des Entschlüsselungshonorars mit durchschnittlichen Kosten in Höhe von 2500 US-Dollar. Denn auch wenn Sie eine Zahlung geleistet haben, heißt das nämlich nicht, das Sie den Entschlüsselungscode auch bekommen werden.

Schließlich können sogar Webseiten von seriösen Anbietern gehackt worden sein. In Unwissenheit des Betreibers sorgen dessen Webseiten so für ungewollte Verbreitung. Große Webhoster setzen diesem Treiben jedoch einen Riegel vor und sperren betroffene Internetseiten oder der Seitenbetreiber selbst setzt Sicherheitssoftware ein. Auch große Suchanbieter warnen vor unsicheren Seiten. Dennoch jeder Webseitenbesuch unterliegt einem gewissen Restrisiko in der Sache. Auch Ergebnisse von Suchmaschinen können Sie auf unseriöse Seiten leiten, falls Sie Warnhinweise missachten oder diese fehlen sollten. Meiden Sie – aus rechtlichen und Datenschutzgründen – möglichst Webseiten aus Nicht-EU Staaten.

Bei Fernwartungssoftware:

Der Einsatz von Fernwartungssoftware setzt sich auch im Privatbereich immer mehr durch. Dabei wird meistens ein PC für den Internetzugang rund um die Uhr betrieben, um auf die Ressourcen jederzeit aus der Ferne über das Internet zugreifen zu können.

Wie man den sicheren Zugriff auf diesen PC umsetzt, beschreibt der Artikel *Sichere Remote Desktop Verbindungen*.

Darüber hinaus sollten Sie den Zugriff auf diesen PC jedoch auch zeitlich beschränken. Gerade unserer „Freunde“ der Ransomware greifen gerne in den frühen Morgenstunden PCs an (2:00h bis 5:00h Ortszeit). Es empfiehlt sich, den PC täglich über das BIOS des Rechners (in dessen APM Einstellungen) morgens einzuschalten. Abends kann er über Software heruntergefahren werden.

Das BIOS des PCs rufen Sie unmittelbar nach Einschalten des PCs durch Drücken der Entf- oder F2-Taste. Manchmal werden auch andere Tastenkombinationen dazu benutzt (ESC- oder F8-Taste). Suchen Sie in den Menüs Einstellwerte für das automatische Starten. **Verstellen Sie sonst bitte keine anderen Werte**! Eventuell fährt ansonsten Ihr PC nicht mehr hoch.

Das Herunterfahren erledigt der Befehl shutdown -s -t:30. Diesen Befehl können Sie über die *Aufgabenverwaltung* von Windows automatisieren. Bei der eingestellten Zeit fährt der PC dann nach 30 Sekunden Vorwarnzeit herunter.

Ein ausgeschalteter PC bietet keinen Angriffspunkt für Hacker. Nötigenfalls schalten Sie ihn manuell ein und aus. Wir gehen allerdings bei dem Vorschlag der Automatisierung der Start- und Ausschaltvorgänge davon aus, dass Sie nicht unter Schlaflosigkeit leiden.

Einsatz spezieller Antivirensoftware

Wir empfehlen den Einsatz von Malwarebytes. Der Viren- und Schadsoftwarescanner überwacht ihr Gerät und die ablaufenden Prozesse sehr wirksam. Er verhindert die Umsetzung von Ransomware und anderer Schädlinge zuverlässig und blockiert entsprechende Aktionen.

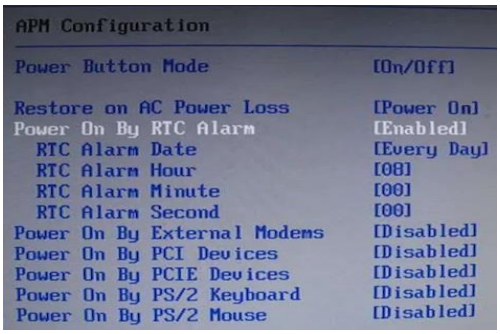
Was hilft beim Befall von Ransomware?

Kurz gesagt: Unmittelbar nichts mehr.

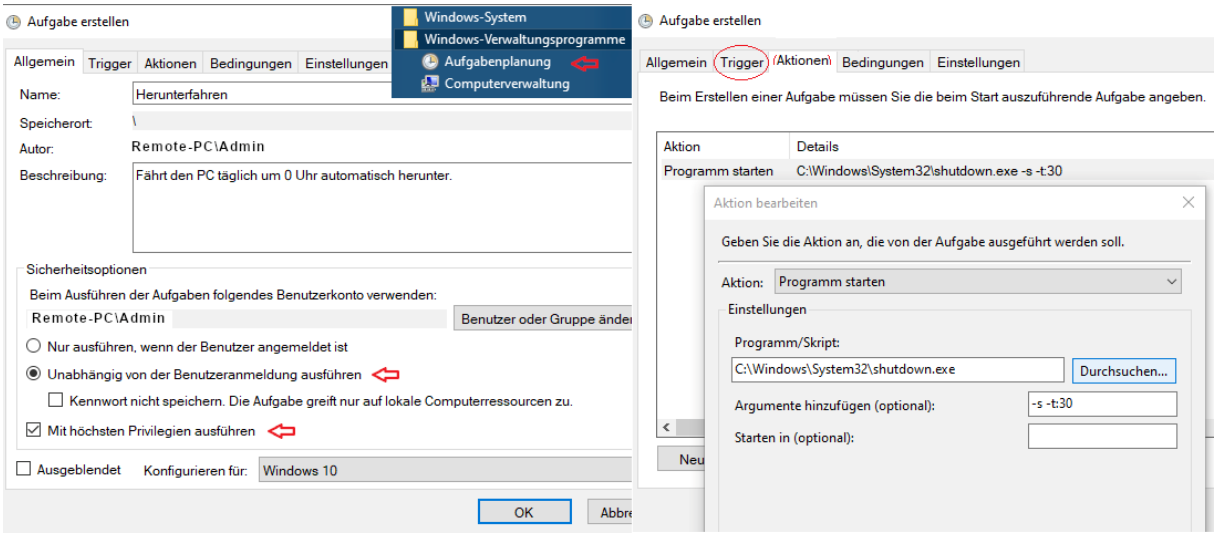
Moderne Ransomware verschlüsselt so wirksam, dass Sie selbst zur Entschlüsselung Monate bräuchten, vielleicht Jahre. **Der einzig wirksame Schutz besteht darin, regelmäßig Backups durchzuführen**, zumindest Ihrer Daten. Im Bedarfsfall können Sie diese wiederherstellen. Die diversen im Internet veröffentlichten Entschlüsselungsprogramme greifen nicht und können den Entschlüsselungscode moderner Ransomware nicht knacken.

Empfehlungswert ist auch die Backupsoftware Arcronis True Image. Sie kann nicht nur Daten, sondern auch die komplette Einrichtung Ihres Systems effizient sichern. Im Falle der Fälle können Sie direkt die komplette Einrichtung Ihres PCs wiederherstellen, selbst auf anderer Hardware und zu jedem Sicherungszeitpunkt. Aktuelle Arconis-Versionen bieten zudem eine Schutzvorrichtung gegen Manipulationen an den Backup-Dateien (Arcronis Active Protection). Backups sollten am besten auf eine externe Festplatte abgespeichert werden. Diese sollte nur während des Backups am System angeschlossen sein. So hat Ransomware keine Chance, auch Backup-Dateien zu verschlüsseln!

Ergänzende Abbildungen zum Beitrag



Empfohlene APM Einstellung des BIOS
Restore on AC Power Loss: On RTC Alarm Date: Every Day



Herunterfahren-Aufgabe erstellen: Unter Trigger wird die tägliche Zeit zum Herunterfahren eingestellt