10 Fragen zu Ransomware

Wie funktioniert ein Angriff mit Ransomware auf meine Nutzerdaten

Ransomware ist Schadcode

Sobald das Opfer den Schadcode auf seinem PC ausführt, verschlüsselt der Schädling heimlich alle Nutzerdaten, also Bilder, Videos, Musik und Dokumente.

Ist das erledigt erscheint eine Meldung mit dem Hinweis auf die verschlüsselten Daten und eine Lösegeldforderung.

Beträge zwischen 100 und 800 Euro (meist in Bitcoins) sind üblich.

Nach der Zahlung soll es einen Entschlüsselungskey geben.

10 Fragen zu Ransomware

Wie gelangt Ransomware auf meinen Rechner?

Die meisten Viren landen heute noch per Mail oder Links in Mails auf dem Rechner.

Rund 50% stecken aktuell in Office-Dateien

Verschlüsselt jede Ransomware meine Daten?

Ransomware wird meist mit Erpresserviren oder Erpressersoftware übersetzt.
Davon gibt es unterschiedliche Arten.

Die eine verschlüsselt Ihre Dateien, die andere sperrt den Zugang zu Windows.

Aktuell behaupten Erpresser per E-Mail, das Sie Passworte des Opfers kennen und Videoaufnahmen von ihm besitzen. Sie fordern also Lösegeld ganz ohne Schadsoftware.

10 Fragen zu Ransomware

Gibt es Anwender die besonders gefährdet sind?

Die Privatanwender sind momentan etwas aus der Schusslinie gerückt.

Aktuell werden Unternehmen und öffentliche Einrichtungen ins Visier genommen.

Die erzielten Lösegelder sind dann auch entsprechend höher (50.000,00 Euro)

Allerdings kursieren weiter Ransomware-Exemplare im Internet, also keine Entwarnung für Privatanwender.

10 Fragen zu Ransomware

Meine Daten wurden verschlüsselt. Soll ich zahlen?

Viele Experten raten davon ab, da ungewiss ist ob ein Schlüssel geliefert wird.

Außerdem ermutigt eine Zahlung zu weiteren Straftaten.

Mit welcher Wahrscheinlichkeit kann ich meine Daten retten?

1. Aktuelles Backup vorhanden
2. Entschlüsselungstool
3. Sie zahlen das Lösegeld (Chance 50:50)

10 Fragen zu Ransomware

Was muss ich nach einem Angriff als erstes tun?

Zunächst muss der Rechner komplett vom Schadcode befreit werden.
Dazu wird ein bootfähiger USB-Stick oder eine bootfähige Antiviren-DVD empfohlen.

z.B.: Kaspersky Rescue Disk

Wo erhalte ich in einem Schadenfall Hilfe?

Die beste Anlaufstelle ist: www.nomoreransom.org

Auch viele Hersteller von Antiviren Software bieten Entschlüsselungsprogramme an, die allerdings separat heruntergeladen werden müssen.

10 Fragen zu Ransomware

Warum funktioniert mein Entschlüsselungstool nicht?

Fast jedes Tool ist auf einen speziellen Schädling spezialisiert.

Was hilft am besten gegen Ransomware-Angriffe?

Datensicherung auf externen Medien die nur für die Dauer der Sicherung mit dem Rechner verbunden sind.

Definition: Ransomware

Der Begriff Ransomware steht für eine Spezies von Schadprogrammen, die den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld (englisch: Ransom) verlangt. Entweder sperrt ein solches Schadprogramm den Systemzugriff, so dass sich beispielsweise Programme auf einem PC nicht mehr aufrufen lassen, oder es verschlüsselt bestimmte Nutzerdaten. Besonders verbreitet ist Ransomware, die sich gegen Windows-Rechner richtet. Prinzipiell aber können alle Systeme von Ransomware befallen werden, – zum Beispiel Computer, die unter dem Desktop-Betriebssystem MacOS X laufen oder auch mobile Android-Geräte. Derzeit zielen die meisten Täter jedoch auf Windows-Systeme ab.

Bei heutigen Ransomware-Angriffen wird das Lösegeld meist in virtueller Währung wie Bitcoin verlangt – wobei die Zahlung allerdings keinerlei Garantie für die Freigabe verschlüsselter Daten oder gesperrter Systeme bietet. Das BSI empfiehlt stattdessen, dass Betroffene unverzüglich Anzeige bei der Polizei erstatten. Auch der allgemeine Ratschlag, regelmäßig Sicherheitskopien anzulegen, ist eine wirksame Ransomware-Prävention. Denn im Falle eines Angriffs lassen sich damit Datenbestände auch ohne Lösegeldzahlung rekonstruieren.