Ransomware-Angriff: So schützen Sie sich

Ein Ransomware-Angriff verschlüsselt Ihre Daten, und Kriminelle verlangen Lösegeld. COMPUTER BILD erklärt, wie Sie sich schützen und im Ernstfall richtig verhalten.
Foto: iStock.com/matejmo

12.04.2023, 16:00 Uhr von Andy Voß

Ransomware-Angriffe sind ein großes Problem für Unternehmen in Deutschland, aber auch für Privatpersonen. COMPUTER BILD erklärt, wie Sie sich absichern.

INHALTSVERZEICHNIS

Ransomware verschlüsselt wichtige Daten oder stiehlt und löscht wichtige Dateien. Die Hinterleute verlangen dann für die Herausgabe Lösegeld. Das sorgt in Deutschland mittlerweile für mehr als 203 Milliarden Euro Schaden pro Jahr. Damit ist diese Schadsoftware vor allem für Unternehmen die teuerste und gefährlichste Bedrohung. Für kleinere Betriebe bedeutet sie sogar unter Umständen den Bankrott. Bei Privatpersonen sind die Lösegeldforderungen geringer – die Gefahr nicht. Wer Opfer eines Ransomware-Angriffs wird, verliert oft eine Menge privater Daten und muss den PC aufwendig wiederherstellen.

Was ist ein Ransomware-Angriff?

"Ransom" ist Englisch für "Lösegeld". Ransomware fasst daher alle Malware zusammen, bei denen die Angreifer Lösegeldforderungen stellen. In den meisten Fällen ist eine Ransomware ein Schadprogramm, das gezielt nach wichtigen Daten sucht, diese verschlüsselt und nur gegen Passwort wieder freigibt. Das Passwort bekommen Sie von den Angreifern gegen Lösegeld – zumindest in der Theorie. In der Vergangenheit gab es zudem Ransomware, die nur den Zugang zum Gerät mit einem unüberwindbaren Lockscreen blockierte. In jüngster Zeit tauchen vermehrt Erpressungsversuche auf, bei denen es nicht darum geht, Daten wiederzubekommen, sondern bei denen die Angreifer damit drohen, erbeutete Firmengeheimnisse zu veröffentlichen. Nicht direkt eine Ransomware, aber ebenfalls Erpressung sind Drohungen, kompromittierende Bilder zu veröffentlichen, wenn der Abgebildete nicht zahlt. Diese Fälle gibt es mittlerweile sehr häufig, sowohl mit echten Bildern als auch mit der schieren Behauptung, man sei im Besitz von brisantem Fotomaterial.

Arten von Ransomware

Ransomware gibt es in extrem unterschiedlichen Varianten – einige verschlüsseln lediglich, andere stehlen zuvor Daten. Einige einfache Varianten blockieren auch nur den Bildschirm und behaupten bloß, Dateien verschlüsselt zu haben. Und es gibt Ransomware für Handys. Bei einigen Lösegeldforderungen steht eine Einzelperson dahinter, bei anderen unternehmensartige Strukturen mit Support, Belohnungs-Programm und der Erstellung maßgeschneiderter Ransomware-as-a-Service. Bei kleineren Erpresserviren gibt es häufig Entschlüsselungsprogramme von Sicherheitsherstellern oder guten White-Hat-Hackern, bei professionellen Schadprogrammen nur selten.

Bei Ransomware wie LockBit erhalten Sie die Daten nur nach Zahlung wieder.
LockBit und andere große Ransomware-Netzwerke haben zudem eine Art Ehrenkodex: Kriminelle, die die Software nutzen, müssen sich an einige Regeln halten. Dazu gehört, dass die Daten bei Zahlung wieder zu entschlüsseln sind. Das ist aber längst nicht bei allen der Fall! Einige andere Ransomwares können die Daten gar nicht entschlüsseln oder es geschieht nur fehlerhaft.

Wie schütze ich mich vor Ransomware?

Die erste Schutzmauer vor Ransomware ist ein gutes Antivirus-Programm. Das erkennt die Malware im besten Fall schon, bevor sie auf den PC gelangt und Schaden anrichtet. Auch gibt es Ansätze, die gegen unbekannte Erpresserviren helfen, wie Zugriffsbeschränkungen auf private Ordner oder ständig aktuelle Sicherheitskopien aller wichtigen Daten, die automatisch ausgetauscht werden, wenn die Software ein Ransomware-Angriff erkennt. Solche ExtraSchutzfunktionen finden Sie auch in Schutzprogrammen oder manchmal in Backup-Software. Der COMPUTER BILD-Erpresserviren-Stoppe r arbeitet ebenfalls nach solch einem Ansatz: Entdeckt er verdächtige Aktivitäten, schaltet er den PC vorsichtshalber in den abgesicherten Modus.

Was mache ich bei Ransomware auf dem PC?

Hat sich auf Ihrem PC Ransomware breitgemacht, starten Sie den PC mit einer Notfall-DVD neu, etwa mit der COMPUTER BILD-Notfall-DVD. Schauen Sie dann, ob Sie noch auf Ihre Daten zugreifen können; sichern Sie diese, falls möglich. Haben Sie ein aktuelles Backup, können Sie das auch einfach zurückspielen. Schauen Sie bei Google, ob Sie mit dem Text der Erpresser-Nachricht ein Entschlüsselungsprogramm (Decryptor) finden. Wer kein Backup hat und nicht mehr an seine Daten kommt, muss sich entscheiden: Entweder die verschlüsselten Daten sind so wichtig, dass Sie es riskieren wollen, das Lösegeld zu zahlen, dann tun Sie das und folgen der Entschlüsselungsanleitung. Eine Garantie, dass Sie die Daten zurückbekommen, gibt es nicht. Oder Sie nutzen die Rettungsmedien von Antivirus-Herstellern, um die Ransomware zu beseitigen. Ihre Daten sind dann aber wahrscheinlich verloren.

Decryptor: Kostenlose Entschlüsselungs-Tools

Für einige Ransomwares gibt es Entschlüsselungs-Tools (Decryptor), die WhiteHat-Hacker oder Antivirus-Hersteller erstellt haben. Das gelingt durch Programmierfehler oder weil die Entwickler der Ransomware sich zurückgezogen und die Schlüssel veröffentlicht haben. Mit solchen Tools retten Sie Ihre verschlüsselten Daten ohne Lösegeldzahlung. Leider gibt es sie nicht für alle Ransomware-Arten. Auf der Seite NoMoreRansom.org finden Sie den Crypto-Sheriff, der ihnen dabei hilft, den richtigen Decryptor zu finden.

Lösegeld zahlen – oder nicht?

In den meisten Fällen rät COMPUTER BILD von einer Lösegeldzahlung ab. Es gibt keine Garantie, dass Sie danach Ihre Daten zurückbekommen. Und das meiste lässt sich auf anderen Wegen einfacher und günstiger wiederbeschaffen. Es gibt aber auch durchaus Ransomware-Kriminelle, die nach der Zahlung eine funktionierende Entschlüsselung anbieten. Ein weiterer Grund, der gegen die Lösegeldzahlung spricht: Sie geben den Hackern dann genau das, was sie wollen: Ihr Geld. Das motiviert zum Weitermachen. Firmen zahlen oft trotzdem, weil die Lösegeldzahlung günstiger ist, als die IT-Infrastruktur neu aufzubauen – und Daten betroffen sind, ohne die das Unternehmen nicht weitermachen kann.
Manche Betriebe fürchtet auch, dass Kriminelle bei Nichtzahlung die
Firmendaten veröffentlichen. Da könnte womöglich einiges ans Licht kommen ...

Quelle: https://www.computerbild.de/artikel/cb-Tipps-Sicherheit-So-schuetzen-Sie-sich-vor-Ransomware-Angriffen-33511527.html