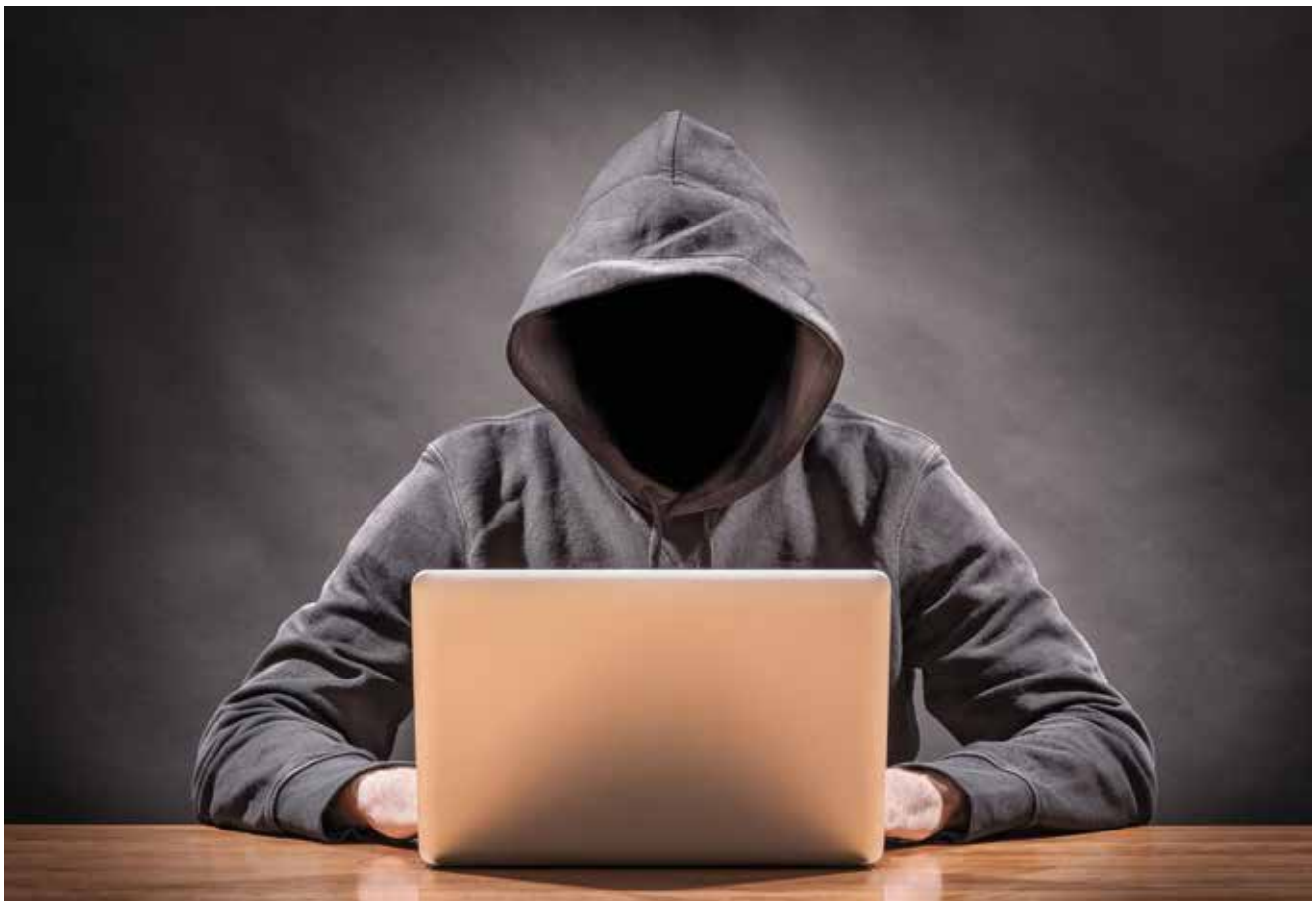

# Kidnapping auf dem Rechner – Ihre Dateien im Visier der Ransomware

Von Markus Kirchner – ED Computer & Design

Cyber-Kriminelle haben eine neue, sehr lukrative Masche für sich entdeckt: Die so genannte Ransomware wird auf einem Computer eingeschleust und verschlüsselt schnell alle wichtigen Dateien. Anders als beispielsweise bei Spyware ist hier nicht der Diebstahl von Daten das Ziel sondern die finanzielle Bereicherung auf Kosten der Opfer. Sind die Dateien erst einmal verschlüsselt, ist der Zugriff auf diese mit herkömmlichen Mitteln fast unmöglich. Die verschiedenen Versionen dieser Schadprogramme nutzen meist eine leistungsstarke Verschlüsselung, welche nur mit dem richtigen Key, den in der Regel nur die Kriminellen besitzen, rückgängig gemacht werden kann.

Meist werden nicht nur Dateien verschlüsselt, sondern auch detaillierte Anweisungen des Verursachers, wie die Daten wieder entschlüsselt werden können, übermittelt. Dass das Ganze nur nach Zahlung eines entsprechenden Obolus von Statten geht, versteht sich von selbst. In den meisten Fällen wird nach einer Zahlung sogar wirklich der korrekte Schlüssel zur Verfügung gestellt. Schließlich soll der Zahler für eventuelle spätere Infektionen bei Laune gehalten werden.

## Viele Schutzmaßnahmen schlagen gar nicht erst Alarm

Doch wie kommt es dazu, dass so viele Leute von diesen Erpressungstrojanern befallen werden? Auch von Unternehmen, die im Regelfall einen besseren Antiviren-Schutz im Einsatz haben als Privatpersonen, war schätzungsweise schon ein Drittel betroffen. Der übliche Weg, durch den die Schadsoftware eingeschleust wird, ist per E-Mail. Dabei geben sich diese E-Mails

oftmals als Rechnung oder dergleichen aus und wirken dabei sehr authentisch. Als Absenderadresse kann eine bekannte oder sogar eine hausinterne Mailadresse angezeigt werden. Im Anhang befinden sich dann Office-Dokumente oder Archive, die unter Umständen selbst noch gar nicht infiziert sind. Diese Tatsachen führen dazu, dass nicht nur Laien in die Falle tappen.

Sobald diese Dateien geöffnet werden, startet im Hintergrund ungesehen ein Skript, welches die Schadsoftware herunterlädt und installiert. Aufgrund dessen schlagen viele Schutzmechanismen gar nicht erst Alarm. Des Weiteren wird die Ransomware immer wieder leicht abgeändert, so dass diese in den Datenbanken der Antiviren-Software Hersteller nicht mehr zu den bekannten Signaturen passen und dadurch nicht direkt erkannt werden.

Kaspersky Lab bietet als erster Hersteller eine progressive Lösung an. In der neuen Version von Kaspersky for Windows Server gibt es ein sogenanntes AntiCryptor Modul, welches genau auf die Erkennung dieser Art von Schadsoftware ausgerichtet ist. Sobald durch einen Teilnehmer im Netzwerk verdächtiges Verhalten beim Zugriff auf den Server festgestellt werden, blockt das Modul die Verbindung zum Server und informiert den Administrator über den Vorfall. Dadurch wird die Gefahr unterbunden, dass ein Client mit Zugriff auf Ressourcen des Servers, diesen über den Netzwerkzugriff verschlüsselt. Noch immer gibt es keinen Schutz für den Arbeitsplatzrechner, doch wenn alle Daten zentral abgelegt und Datensicherungen vorhanden sind, kann der mögliche Schaden minimiert werden.

## Welche Maßnahmen schützen?

Selbstverständlich sollten Sie Ihre Antiviren-Software immer auf dem neuesten Stand halten. Das gilt sowohl für die Programmversion als auch für die Aktualität der Signaturen. Optimal ist eine Konstellation mit Zugriff auf Cloud Dienste, um den höchsten Grad an Erkennung zu gewährleisten. Dadurch ist die Aktualität der Datenbanken sichergestellt.

E-Mails mit Anhang sollten immer als extrem kritisch betrachtet werden und nur bei einem wirklich sehr hohen Plausibilitätsgrad sollten diese Anhänge geöffnet werden. Vorsicht ist also besser als Nachsicht. Im Zweifelsfall sollten Sie sich daher an Ihren IT-Dienstleister wenden. Sollte widererwarten doch ein schädlicher E-Mail Anhang geöffnet werden und es zur Verschlüsselung des Arbeitsplatzes kommen, hilft eine gute Backupstrategie dabei, Datenverlust zu vermeiden. Dabei sollte auch darauf geachtet werden, ein Backup anzulegen, welches extern oder zumindest getrennt vom Netzwerk gelagert wird. Sonst besteht die Gefahr, dass die unerwünschte Verschlüsselung vom Ursprungspunkt der Infektion auf weitere Geräte im Netzwerk übergreift.

## Was ist zu tun?

Als Betroffener ist es wichtig, zu wissen, dass viele der Verschlüsselungen im Laufe der Zeit geknackt werden. Sollte ein Gerät befallen und die darauf befindlichen Daten vom Verlust bedroht sein, ist noch nicht zwangsweise Hopfen und Malz verloren. Allerdings ist aufgrund der Lukrativität für die Verursacher nicht zu erwarten, dass dieses Geschäft in naher Zukunft eingestellt wird. Darum ist es momentan umso wichtiger, gut vorbereitet und achtsam zu sein.

Indem Sie sich unangreifbar machen, helfen Sie indirekt, den Übeltätern den Wind aus den Segeln zu nehmen. Durch fehlende Lösegeld-Zahlungen wird das finanzielle Fundament brüchig und diese Art der Geldmacherei letztendlich unprofitabel.