FOTO: TRAITOV/GETTY IMAGES

Effektiver Schutz vor Ransomware

Keine Chance für Erpresser

Cyber-Ganoven setzen Anwender unter Druck, indem sie wichtige Daten verschlüsseln und danach hohe Summen für die Wiederherstellung verlangen. Dabei gibt es gute Methoden, um sich zu schützen

VON ANDREAS TH. FISCHER

Anfang des Jahres gelang Ermittlern ein bedeutender Schlag gegen die internationale Cyber-Kriminalität. Sie konnten die Server der Emotet-Bande übernehmen und mehrere Personen festnehmen. Emotet gilt als einer der gefährlichsten Schädlinge. Mit ihm war es möglich, einen versteckten Zugang auf fremden Rechnern einzurichten. Über diese Hintertüren konnten Kriminelle Ransomware ins System einschleusen.

Unter den verschiedenen Schädlingsarten, die in den vergangenen Jahren auf die Welt losgelassen wurden, zählt Ransomware zu den schlimmsten und gemeinsten Gefahren. Nach der Infektion verschlüsselt die Malware wichtige Dateien auf allen erreichbaren Datenträgern, löscht die Originale und blendet eine Lösegeldforderung ein. Die Opfer stehen vor einer Katastrophe – seien es Privatanwender, die unersetzliche Urlaubsfotos verloren haben, oder Firmen, die auf geschäftliche Daten nicht mehr zugreifen können. Ohne ein zuvor angelegtes und auch funktionierendes Backup kommen sie nicht mehr an ihre Daten – es sei denn, sie sind bereit, die teilweise sehr hohen Summen zu bezahlen, die die Kriminellen von ihnen fordern.

Gegen diese Angriffe gibt es eine ganze Reihe geeigneter Sicherheitsmaßnahmen. Sie reichen von Abwehrmethoden gegen Ransomware über eine in Windows 10 vorhandene, aber meist nicht aktivierte Schutztechnik, bis zu einem Backup-Plan. Ist das Unglück bereits geschehen, zeigen wir Ihnen auch, wo Sie Hilfe bekommen und beantworten die Frage, ob Sie zahlen sollten oder besser nicht.

Die Software[1] aus diesem Beitrag finden Sie auf der virtuellen CHIP-DVD

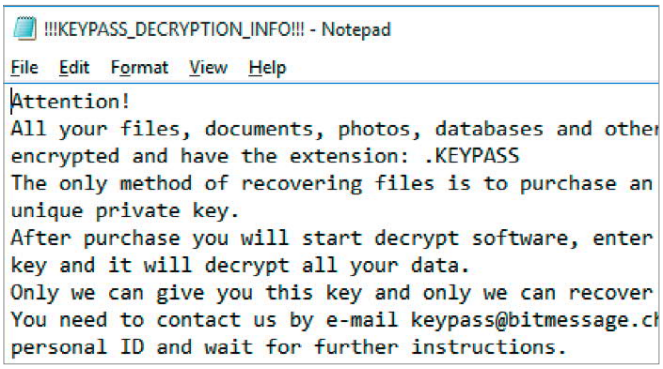
Ransomware abwehren

Im ersten Abschnitt stellen wir Ihnen Maßnahmen vor, mit denen Sie eine Ransomware-Infektion rechtzeitig verhindern, bevor ein Schädling zuschlagen und Ihre Daten verschlüsseln kann.

Spam filtern

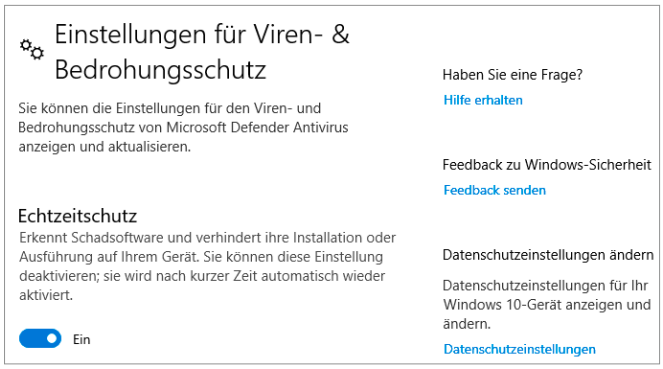
Am häufigsten gelangt Ransomware mit Hilfe von Trojanern wie Emotet auf fremde

[1]E-Paper-Leser können die virtuelle DVD unter **chip-kiosk.de/produkte** nachbestellen



QUELLE: KASPERSKY

Horrorszenario: Lösegeldforderung
Eine Ransomware hat auf diesem PC zugeschlagen und wichtige Dateien verschlüsselt. Das Opfer soll nun 300 Dollar zahlen



Grundlegende Abwehr: Virenscanner
Ein aktuelles und zuverlässiges Antiviren-Programm ist ein wichtiger Bestandteil einer umfassenden Strategie gegen Ransomware

Rechner. Dieser bereits eingangs erwähnte Schädling wird vor allem über Spam-Nachrichten verbreitet. Die meisten dieser E-Mails versenden die Kriminellen ungezielt wie mit einer gigantischen Gießkanne. Jeder der in die Hunderttausende gehenden Empfänger erhält identische Nachrichten. So kommt es etwa dazu, dass man oft gefälschte Aufforderungen von Banken und Online-Shops erhält, bei denen man gar nicht Kunde ist. Diese Mails erkennen und löschen Sie leicht. Auf keinen Fall sollten Sie aber auf einen der enthaltenen Links klicken oder beiliegende Dateien öffnen. Noch gefährlicher sind gezielte Spam-Mails.

Gegen sie hilft ein Spam-Filter, wie ihn etwa Thunderbird bereits mitbringt. Der Filter ist standardmäßig aktiv, allerdings muss er weiter trainiert werden, damit er auf Dauer gute Ergebnisse liefert und Sie vor gefährlichen Mails schützt.

Die meisten E-Mail-Dienstleister bieten eigene Spam-Filter an, die Sie teilweise aber erst aktivieren oder konfigurieren müssen. In der Regel sind diese Techniken weit leistungsfähiger als der interne Thunderbird-Filter. Sie werden von erfahrenen Spezialisten gepflegt, die etwa die aktuellen IP-Adressen von Servern einpflegen, die momentan für den Versand von Spam missbraucht werden.

Virenscanner testen

Auf einen Virenscanner sollten Sie nicht verzichten. Er überwacht alle Prozesse auf Ihrem System unauffällig im Hintergrund und schreitet bei verdächtigen Aktivitäten ein. Das funktioniert allerdings nur bei Bedrohungen zuverlässig, die er bereits kennt. Sie sollten sich daher niemals vollständig auf Ihr Antivirus-Programm verlassen und auch nicht davon ausgehen, dass es alle Infektionen verhindern kann. In den meisten Fällen reicht der von Microsoft in Windows 10 integrierte Defender aus. Ob er auch wirklich aktiv ist, können Sie mit der EICAR-Testdatei überprüfen. Diese harmlose Textdatei sollte einen Alarm auslösen, wenn Sie sie auf Ihren PC herunterladen oder kopieren.

Updates einspielen

Beim Schutz vor Ransomware sollten auch Sicherheits-Updates ganz oben auf der Todo-Liste stehen. Im Idealfall ermöglicht der jeweilige Software-Hersteller ein automatisches Einspielen der aktuellen Patches. Bei etwa Windows 10 und Programmen wie Firefox oder Thunderbird ist das der Fall. Bei anderen Anwendungen müssen Sie sich selbst darum kümmern. Auf keinen Fall sollten Sie Hinweise auf neue Aktualisierungen jedes Mal wegklicken. Eventuell werden mit dem angebotenen Update gefährliche Sicherheitslücken geschlossen, über die eine Ransomware auf Ihren Computer gelangen könnte.

Denken Sie beim Thema Updates auch an weitere von Ihnen eingesetzte Produkte wie Ihr Smartphone, Tablet, Router sowie alle anderen netzwerkfähigen Geräte. Sie können als Hintertür in Ihr lokales Netz

Spam bereits beim Provider filtern
Ergänzen Sie den Spam-Filter im Mail-Client mit einem fortgeschrittenen Filter, wie ihn die meisten E-Mail-Dienstleister anbieten

Ranshameware

Die Cyber-Bedrohungen entwickeln sich laufend weiter. Kriminelle probieren immer wieder neue Tricks aus, um an das Geld ihrer Opfer zu gelangen. Mittlerweile setzen viele Erpresser nicht mehr nur auf das Verschlüsseln wichtiger Daten. Sie klauen sie zusätzlich und drohen anschließend damit, sie im Internet zu veröffentlichen. Sicherheitsexperten gehen davon aus, dass bei zwei Drittel aller aktuellen Ransomware-Angriffe auch Daten gestohlen werden. Die Opfer sehen sich damit einer völlig anderen Lage gegenüber. Normalerweise sind Backups der beste Schutz vor Ransomware. Diese helfen aber nicht, wenn die Erpresser die geklauten Daten einer breiten Öffentlichkeit zugänglich machen wollen. Daher stammt auch der neue Begriff »Ranshameware«. In ihm steckt nicht mehr nur die »Ransom«, also die Erpressung, sondern mit »Shame« auch die Scham vor einer Veröffentlichung.

Schutz vor Ransomware in Windows 10
Der „Überwachte Ordnerzugriff“ sorgt dafür, dass die dort gelisteten Verzeichnisse nicht unerlaubt manipuliert werden können

FOTO: SHARK_749/GETTY IMAGES

Sicherung auf externe Festplatten
Kappen Sie nach dem Backup die Verbindung zwischen der externen Festplatte und Ihrem Rechner, um Ransomware auszusperren

missbraucht werden, von der sich dann Schadcode ausbreitet.

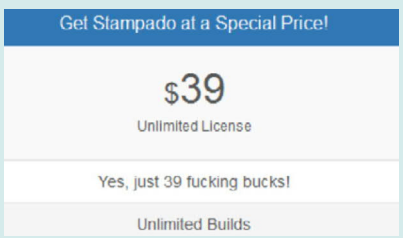
Windows-Schutz aktivieren

Seit dem Fall Creators Update, das im Herbst 2017 erschien, verfügt Windows 10 über einen integrierten Anti-Ransomware-Schutz. Standardmäßig ist er allerdings nicht aktiv, weil er unerfahrene Anwender verwirren könnte. Er verhindert den Zugriff nicht autorisierter Anwendungen auf geschützte Ordner. Die Funktion nennt sich daher auch „Überwachter Ordnerzugriff“.

Sie finden sie unter »Start | Einstellungen | Update und Sicherheit | Windows-Sicherheit | Viren- & Bedrohungsschutz«. Scrollen Sie dort bis nach unten und klicken Sie auf »Ransomware-Schutz verwalten«. Aktivieren Sie den Schalter und legen Sie anschließend über »Geschützte Ordner« fest, welche Verzeichnisse Windows vor unerlaubten Veränderungen schützen soll. Microsoft verwaltet eine nicht öffentliche Liste vertrauenswürdiger Programme, die auf diese Ordner weiterhin zugreifen dürfen. Zusätzlich fügen Sie über »App durch überwachten Ordnerzugriff zulassen« weitere Anwendungen hinzu. Anschließend kann kein Programm mehr unerlaubt und daher auch keine Ransomware mehr auf Ihre geschützten Dateien zugreifen.

Erpressung als Dienstleistung

Moderne Kriminelle gehen oft arbeitsteilig vor. Manche Gruppen wie die Emotet-Bande verschaffen anderen Ganoven den Zugang zu fremden Computern. Für diese „Dienstleistung“ bekommen sie Geld. In Untergrundforen im Darkweb lassen sich weitere Dienste mieten. Davon profitieren vor allem Einsteiger, denen noch die nötigen Kenntnisse fehlen, um etwa selbst eine eigene Ransomware zu entwickeln. Üblicherweise wird eine solche Malware wie Stampado für einen kleinen Preis verkauft, zusätzlich erhalten die Entwickler von jedem eingenommenen Lösegeld einen Anteil von etwa 30 Prozent. Das Geschäft ist also für beide Seiten sehr lukrativ.



QUELLE: SOPHOS

Das perfekte Backup

Backups sind Ihre letzte Verteidigungslinie, wenn es einem Angreifer doch gelingt, alle anderen Sicherheitsmaßnahmen zu umgehen. Es gibt dabei aber ein paar Punkte, die Sie für einen umfassenden Schutz beachten sollten.

3-2-1-Plan anwenden

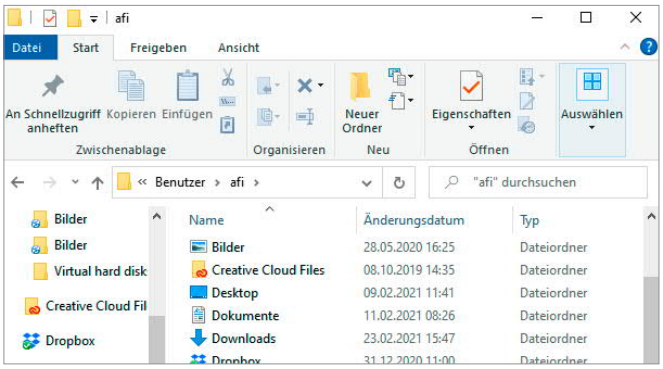
Viele Anwender sichern zumindest gelegentlich wichtige Dateien auf eine separate Festplatte. Das reicht jedoch nicht aus, um sie wirklich vor der Verschlüsselung durch eine Ransomware zu schützen. Bewährt hat sich der sogenannte 3-2-1-Plan, der folgendermaßen aussieht: Heben Sie mindestens **drei** Kopien aller wichtigen Daten auf: Eine ist das Original auf Ihrer Festplatte plus zwei separate Sicherungen. Verwenden Sie dafür mindestens **zwei** unterschiedliche Speichertechniken und verwahren Sie **eines** dieser Backups an einem anderen Ort auf. Jeden der für die Backups verwendeten Datenträger sollten Sie nach dem Sichern der Daten umgehend von Ihrem PC trennen. Sie dürfen auch nicht wie etwa ein dauerhaft verbundener NAS-Server über das Netzwerk erreichbar sein. Sonst kann eine Ransomware darauf zugreifen und Ihre Sicherheitskopien genauso wie die Originale zerstören.

Daten verschlüsseln

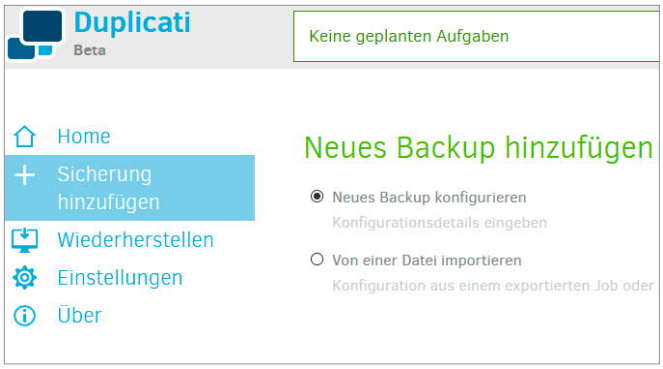
Beim Thema Verschlüsselung scheiden sich die Geister. Es hat eigentlich auch nichts mit dem Schutz vor Ransomware zu tun, ist aber trotzdem wichtig, wenn Sie einen Backup-Plan anlegen. Sicherheitsexperten raten dazu, Backups immer zu verschlüsseln. Achten Sie dabei allerdings darauf, dass Sie das verwendete Passwort nicht verlieren. Wenn Sie als Ziel für Ihre Sicherung einen Cloud-Speicher wählen, sollten Sie die Daten vor dem Hochladen auf jeden Fall verschlüsseln.

Zu sichernde Daten auswählen

Was man sichern soll, hängt davon ab, welche Daten Sie haben und wo sie gespeichert sind. Gesichert werden sollten auf jeden Fall alle wichtigen Dokumente, egal ob sie privater oder geschäftlicher Natur sind. Standardmäßig speichert Windows sie in Ihrem Benutzerordner, den Sie unter „C:\Users\Benutzername“ finden. Sie können dort alle Unterordner sichern oder Sie treffen eine Auswahl. Besonders wichtig dürfte der Ordner „Dokumente“ sein. Aber auch „Bilder“ oder „Musik“ können wichtige Daten enthalten. Wenn Sie Cloud-Dienste wie Dropbox oder OneDrive nutzen und dort wichtige Dateien ablegen,



Wichtige Daten fürs Backup ermitteln
Nehmen Sie sich Zeit, um genau festzulegen, was vor dem Zugriff durch eine Ransomware geschützt werden muss



Backup anlegen und starten
Duplicati bietet einen einfach zu bedienenden Assistenten, um neue Backup-Aufgaben vorzunehmen

sollten Sie auch diese Verzeichnisse in Ihr Backup aufnehmen.

Vorsicht bei virtuellen Maschinen oder Ihrem Downloads-Ordner! Sie sind meist sehr groß. Das verlängert die für die Backups benötigte Zeit und überschreitet möglicherweise den zur Verfügung stehenden Platz. Empfehlenswert ist es jedoch, den AppData-Ordner mitzusichern, weil dort viele Windows-Programme ihre Einstellungen sichern. Sie finden ihn im Dateiexplorer, indem Sie ins Adressfeld „%appdata%“ eintippen. Für die Sicherung Ihrer E-Mails bietet sich Mailstore Home an. Die Bedienung des für Privatanwender kostenlosen Programms haben wir bereits in CHIP 9/2019 beschrieben (als PDF auf virtueller CHIP-DVD).

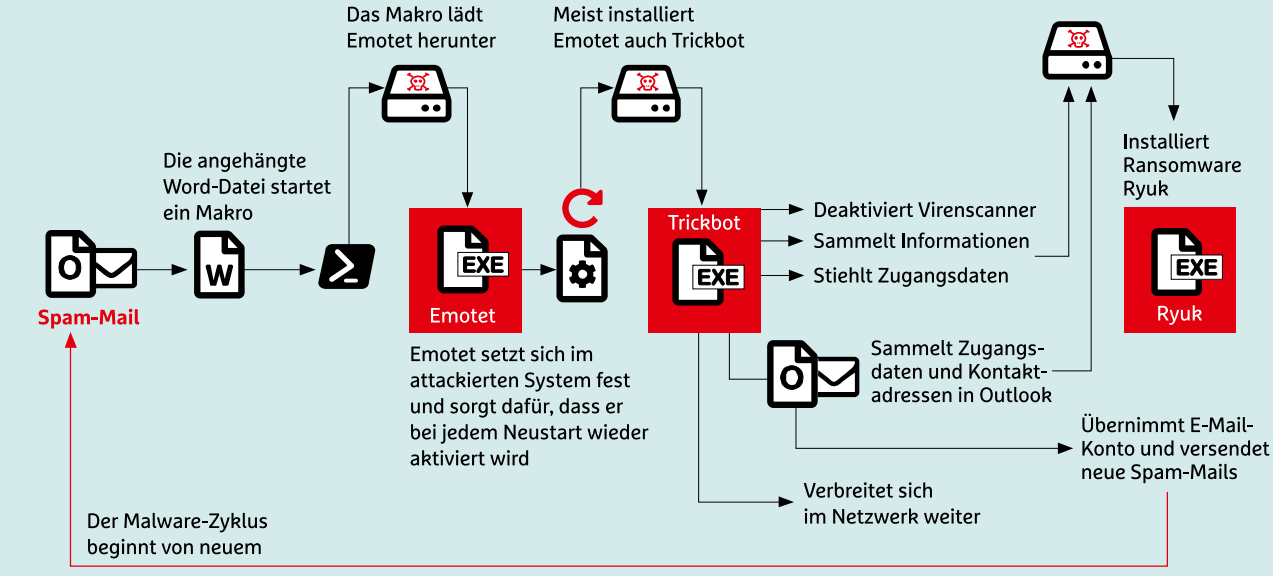
Backup anlegen

Nachdem Sie sich einen Überblick darüber verschafft haben, was Sie alles sichern wollen, starten Sie das erste Backup. Es gibt viele gute Programme für diesen Zweck. Uns hat Duplicati überzeugt, da es Open-Source-Software ist und auch von Einsteigern leicht zu bedienen ist. Installieren und starten Sie Duplicati auf Ihrem Computer. Schließen Sie dabei auch gleich den externen Datenträger an, den Sie für Ihre Sicherung verwenden wollen. Klicken Sie danach auf »Sicherung hinzufügen«, bestätigen Sie mit »Weiter« und folgen Sie dem Assistenten. Im ersten Dialog können Sie festlegen, ob Ihre Daten beim Sichern verschlüsselt werden sollen und welches Passwort („Passphrase“) Sie dafür verwenden wollen. Wählen Sie den externen Datenträger als Ziel aus. Im folgenden Dialog legen Sie fest, welche Dateien Sie sichern wollen.

Danach entscheiden Sie, ob automatische Sicherungen durchgeführt werden sollen. Das würde aber nur etwas bringen, wenn das Ziel permanent mit Ihrem Rechner verbunden ist, was beim Schutz vor Ransomware jedoch nicht sinnvoll ist. Je nachdem, wieviel Platz zur Verfügung

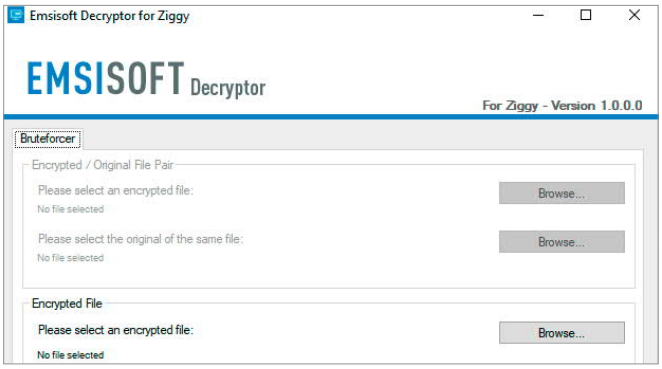
So gelangt Ransomware auf fremde PCs

Die Verbrecher hinter Emotet haben einen Rückschlag erlitten. Das grundsätzliche Vorgehen beim Einschleusen von Malware bleibt aber unverändert. Statt Emotet setzen die Kriminellen nun eben andere Schädlinge ein



QUELLE: BARKLY, CHIP

Entschlüsselungs-Tool finden
Der »Crypto Sheriff« von NoMoreRansom.org hilft Ihnen bei der Suche nach einem Tool zur Wiederherstellung der Daten



Rettung für Opfer der Ransomware Ziggy
Gelegentlich gelingt es Sicherheitsfirmen, die verwendete Verschlüsselung zu knacken und einen Decryptor zu veröffentlichen

steht und wie viele Daten Sie sichern wollen, wählen Sie zuletzt bei »Sicherungs-Aufbewahrung« entweder »Behalte alle Backups« oder »Intelligente Sicherungs-Aufbewahrung«. Dann löscht Duplicati nicht mehr benötigte Backups, sorgt aber dafür, dass immer mindestens eine Version erhalten bleibt. Bestätigen Sie zuletzt mit »Speichern« und starten Sie Ihr Backup mit »Jetzt sichern«. Der erste Durchlauf kann je nach Datenmenge und Laufwerkstempo ziemlich lang dauern.

Vergessen Sie danach nicht, den Datenträger von Windows zu trennen. Wenn Sie sich an den vorgeschlagenen 3-2-1-Plan halten wollen, legen Sie möglichst bald ein weiteres Backup auf einem anderen mobilen Datenträger an und verwahren eine der Sicherungen an einem anderen Ort.

Wiederherstellung prüfen

Bevor Sie sich nun auf der sicheren Seite wähnen, sollten Sie das Backup testen. Nur so erfahren Sie, ob sich die Daten fehlerfrei wiederherstellen lassen und ob Sie Ihrem Backup vertrauen können. Klicken Sie auf »Wiederherstellen« und wählen Sie das zuletzt angelegte Backup aus. Markieren Sie die Dateien, deren Wiederherstellung Sie testen wollen. Im folgenden Dialog legen Sie einen »Speicherort« fest. Da es nur um einen Test geht, sollten Sie dafür ein temporäres Ziel auswählen. Starten Sie den Vorgang zuletzt mit »Wiederherstellen« und prüfen Sie anschließend, ob sich die Daten ohne Probleme öffnen lassen.

Tools zum Entschlüsseln

Wenn keine der beschriebenen Sicherheitsmaßnahmen Sie vor einer Ransomware schützen konnte und Sie auch kein funktionierendes Backup besitzen, bleiben Ihnen nur zwei Möglichkeiten: Entweder Sie zahlen oder Sie haben Glück und eine Sicherheitsfirma hat genau für die Malware, die Sie ins Visier genommen hat, ein passendes Entschlüsselungs-Tool entwickelt. Die niederländische Polizei betreibt unter **www.nomoreransom.org/de** ein Portal, das in Zusammenarbeit mit Europol sowie Kaspersky und McAfee aufgebaut wurde. Auf der Webseite findet sich unter anderem ein »Crypto Sheriff«, mit dem Sie nach einem geeigneten Entschlüsselungs-Tool suchen können. Entweder Sie laden von Ihrem PC eine oder zwei verschlüsselte Beispiele hoch oder Sie kopieren den Text der Lösegeldforderung in das dafür vorgesehene Feld. Wenn Sie dort nicht fündig werden, bleibt Ihnen nur, zu warten. Die letzte Möglichkeit ist, das geforderte Lösegeld zu bezahlen. Das ist aber nicht empfehlenswert, da die Erpresser damit in ihren Handlungen bestärkt werden (siehe Kasten unten).

redaktion@chip.de

Zahlen oder nicht zahlen?

Viele Sicherheitsexperten raten dazu, eine Lösegeldforderung nicht zu begleichen. Die Realität sieht jedoch oft anders aus. Natürlich stimmt es, dass jede Zahlung die Kriminellen ermuntert, weiterzumachen und ihr Geschäft eventuell auszubauen. Außerdem besteht immer das Risiko, dass die Erpresser mit dem Geld verschwinden und die verschlüsselten Daten nicht wieder zugänglich machen oder dass in der Malware ein technischer Fehler steckt, der die Wiederherstellung verhindert. Den Kriminellen ist aber durchaus bewusst, dass sie sich damit ihr einträgliches Geschäft selbst kaputt machen würden. In der überwiegenden Mehrheit der Fälle klappt die Wiederherstellung der Daten daher. Im Grunde muss sich jedes Opfer einer Ransomware-Attacke also genau überlegen, was mehr kostet: das Eingehen auf die Erpressung oder ein Verzicht auf die verschlüsselten Daten. Viele Unternehmen kommen laut einer Umfrage des Sicherheitsanbieters Crowdstrike offensichtlich zu der Entscheidung, dass sie letzteres mehr kosten würde als die Bezahlung der Forderung. Rund 27 Prozent entschieden sich so. Die dabei geleisteten Beträge sind beachtlich. Sie liegen im Schnitt bei 1,1 Millionen Dollar. Anders sieht es jedoch aus, wenn die Erpresser auch noch Daten geklaut haben und nun damit drohen, sie bei Nichtzahlung zu veröffentlichen. Das ist laut dem Anti-Ransomware-Spezialisten Covewave mittlerweile in 70 Prozent der Attacken der Fall. Dort besteht jedoch das Risiko, dass die Erpresser nach der Begleichung ihrer Forderung ein weiteres Mal zulangen wollen. Auch soll es Fälle gegeben haben, bei denen die geklauten Daten weiterverkauft wurden, so dass andere Kriminelle ihrerseits Erpressungsversuche starteten. Bei den klassischen Ransomware-Attacken ist das anders. Da bekommen die Opfer in der Regel für ihr Geld den Schlüssel zur Wiederherstellung der Daten.