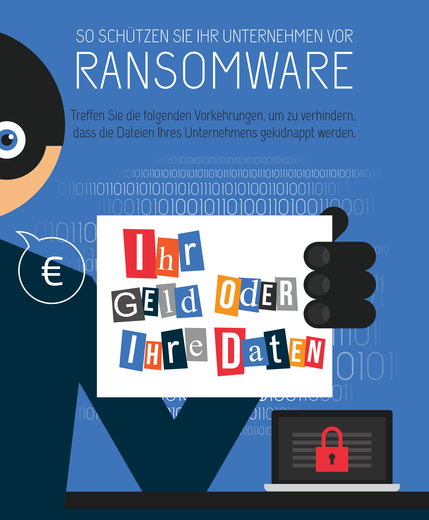
SO SCHÜTZEN SIE IHR UNTERNEHMEN VOR

RANSOMWARE

Treffen Sie die folgenden Vorkehrungen, um zu verhindern, dass die Dateien Ihres Unternehmens gekidnappt werden.



Drei Ebenen von Ransomware

Ransomware ist eine besonders bösartige Software, die Ihr System oder Daten sperrt, bis Lösegeld bezahlt wurde.

Niedrige Gefahr

Scareware

Falsche Antiviren-Tools melden Schadsoftware-probleme und verlangen Geld, um diese zu beheben.

Mittlere Gefahr

Ransomware, die den Browser oder Bildschirm sperrt

Betrüger geben sich in Nachrichten fälschlicherweise als Strafverfolgungs-behörden wie das FBI oder eine Justizbehörde aus. Sie behaupten, dass auf Ihrem Computer illegale Aktivitäten festgestellt wurden, weshalb Sie eine Geldstrafe bezahlen müssen.

Höchste Gefahr

Verschlüsselnde Ransomware

Sie werden in Pop-up-Nachrichten darauf hingewiesen, dass Ihre Dateien verschlüsselt wurden und dass Sie innerhalb einer bestimmten Frist ein Lösegeld bezahlen müssen, um die Dateien zurückzuerhalten.

Wie gefährlich ist verschlüsselnde Ransomware für Ihr Unternehmen?

Daten

Ransomware kann die wichtigsten Dateien Ihres Unternehmens verschlüsseln, unter anderem Buchhaltungs- und Gesundheitsdaten oder vertrauliche Kundendaten. Auf die verschlüsselten Dateien haben Sie keinen Zugriff mehr – außer Sie bezahlen das Lösegeld.

Häufigkeit

Jahr für Jahr werden Millionen von Ransomware-Angriffen auf kleine und große Unternehmen gestartet.*

*NPR, All Things Considered, 22.2.2016

Unternehmensruf

Bei einigen neuen Formen von Ransomware besteht für Unternehmen nicht nur die Gefahr, dass Dateien verschlüsselt werden, sondern auch, dass diese online verbreitet werden.

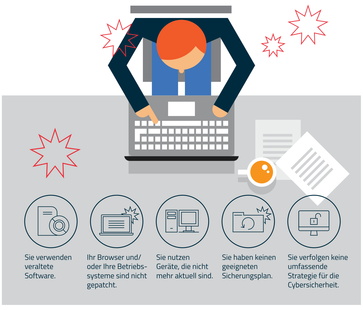
Geld

Im Februar 2016 bezahlte das Krankenhaus Hollywood Presbyterian Hospital einen Betrag von 17.000 $, um Patientendaten von Hackern zurückzubekommen. Nach Schätzungen in dem Bericht "Verizon Data Breach Investigations Report" können Unternehmen bei einem Verlust von 1.000 Datensätzen davon ausgehen, dass sie mehr als 67.000 $ verlieren werden. Mit zunehmendem Ausmaß der Datenschutzverletzung steigen auch die Kosten für das Unternehmen – exponentiell.

Lösegeld bezahlen oder nicht?

Das FBI und andere Strafverfolgungsbehörden empfehlen Privatpersonen und Unternehmen, das Lösegeld zu bezahlen. Dies ist der einfachste Weg, um wieder an die Dateien zu kommen. Experten für Cybersicherheit raten hiervon jedoch ab. Es gibt keine Garantie dafür, dass Sie nach der Zahlung des Lösegelds tatsächlich wieder Zugriff auf Ihre Dateien erhalten. Außerdem werden Sie so zum Ziel für künftige Schadsoftwareangriffe.

Fälle, in denen Ihr Unternehmen gefährdet ist



- Sie verwenden veraltete Software.
- Ihr Browser und/oder Ihre Betriebs-systeme sind nicht gepatcht.
- Sie nutzen Geräte, die nicht mehr aktuell sind.
- Sie haben keinen geeigneten Sicherungsplan.
- Sie verfolgen keine umfassende Strategie für die Cybersicherheit.

Proaktive Vorbeugung

Der beste Schutz besteht in der Vorbeugung. Treffen Sie die folgenden Vorkehrungen, um zu verhindern, dass Ransomware Ihr Unternehmen schädigt.

1 System patchen

Halten Sie Browser, Betriebssysteme und andere Softwareanwendungen stets aktuell.

2 Nutzer schulen

Das Social Engineering ist einer der häufigsten Wege, auf dem Computer mit Ransomware infiziert werden. Schulen Sie Ihre Nutzer darin, Phishing-Kampagnen, verdächtige Websites und andere betrügerische Aktivitäten zu erkennen.

3 Dateien sichern

Erstellen Sie in regelmäßigen Abständen Sicherungskopien von Ihren Daten, und speichern Sie diese außerhalb Ihres Unternehmens.

- Speichern Sie Sicherungsdateien auf keinen Fall auf einem zugeordneten Laufwerk. Bestimmte Formen von Ransomware können Dateien sogar über nicht zugeordnete Netzlaufwerke verschlüsseln.
- Stellen Sie bei einer Sicherung auf einem USB-Speichermedium oder einer externen Festplatte sicher, dass die Geräte physisch vom Computer getrennt sind.
- Wir empfehlen eine Speicherung auf einem sicheren Cloud-Server mit starker Verschlüsselung und Multifaktor-Authentifizierung.

4 In eine mehrstufige Sicherheit investieren

Durch die Installation von mehreren Ebenen zum Schutz der Cybersicherheit können Sie Ransomware-Angriffe erkennen und blockieren, bevor diese Schaden anrichten. Für einen optimalen Schutz empfehlen wir folgende Ebenen:

- Firewall
- Anti-Exploit
- Antiviren-programm mit aktiver Überwachung
- Antischad-software
- Anti-Ransomware

Was können Sie tun, wenn Sie infiziert wurden?

Wenn Sie Ihre Dateien verantwortungsvoll gesichert haben, besteht noch Hoffnung. Durchsuchen Sie Ihre Sicherungsdateien auf einem anderen PC, der nicht infiziert wurde, nach Schadsoftware. Scannen Sie dann den infizierten Computer, um diesen von allen Spuren von Ransomware oder anderer Schadsoftware zu befreien. Wenn Ihre Sicherungsdateien „sauber" sind, können Sie diese auf Ihrem Computer wiederherstellen.

Machen Sie den ersten Schritt für eine proaktive Vorbeugung, und testen Sie Unternehmensprodukte von Malwarebytes. Weitere Informationen hierzu finden Sie unter **malwarebytes.com/business**.

Malwarebytes