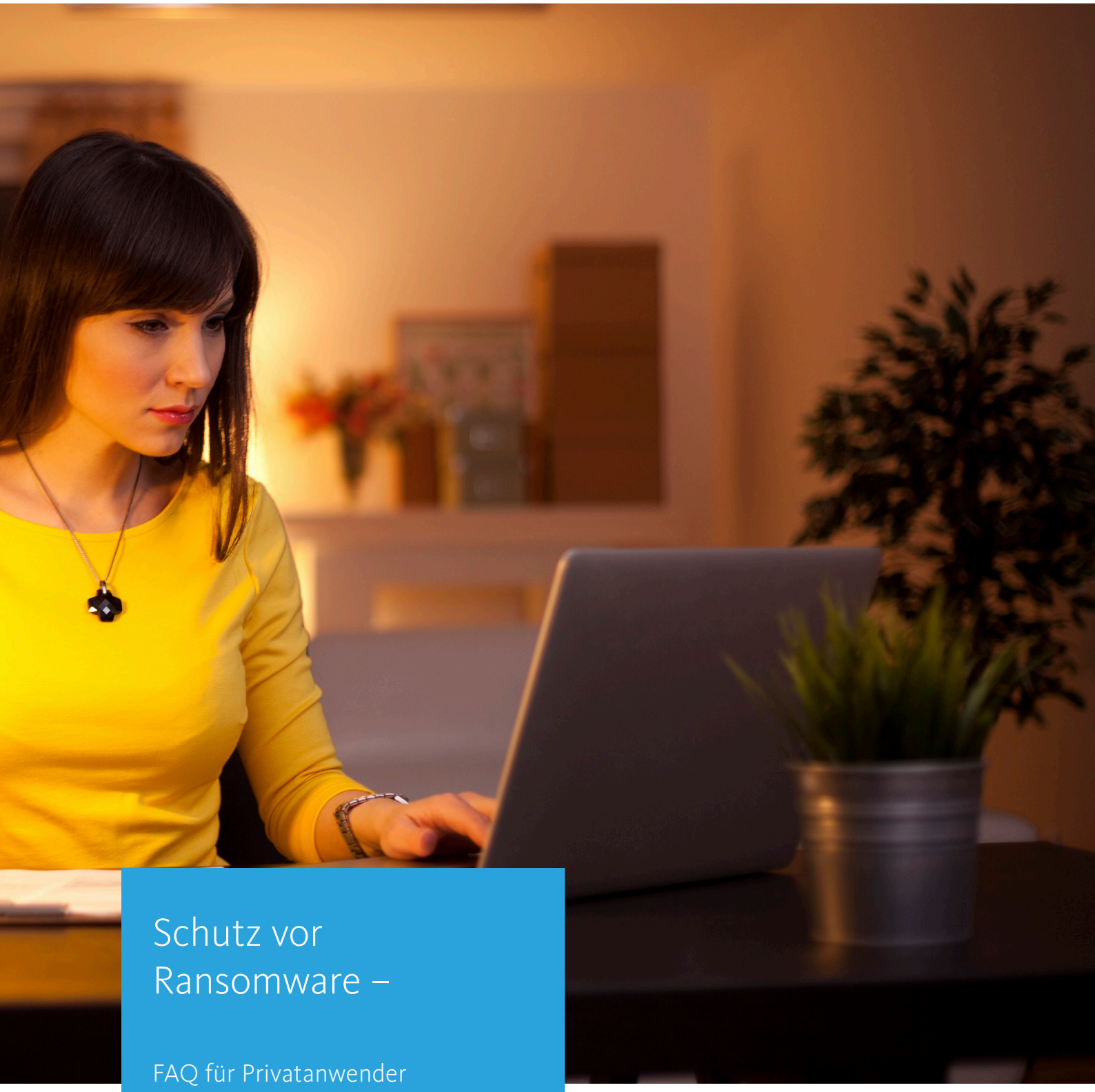
Avira



Schutz vor Ransomware –

FAQ für Privatanwender

www.avira.de

1. Was ist Ransomware?

Ransomware ist eine Erpressungssoftware, die Fotos, Videos, Musikdateien und andere Dateien auf dem Computer verschlüsselt oder den Zugriff auf das gesamte System blockiert. Für die Freigabe muss in der Regel ein „Lösegeld“ bezahlt werden, damit die Opfer wieder Zugriff auf ihre Dateien und Geräte haben.

2. Welche Arten von Ransomware gibt es?

Es gibt drei Arten von Ransomware: Encryption-Ransomware, die Dateien verschlüsselt (und unbrauchbar macht), Lockscreen-Ransomware, die den Bildschirm sperrt und Master-Boot-Record-Ransomware, die den Startbereich der Partionstabelle für BIOS-basierte Computersysteme verschlüsselt.

3. Was macht Ransomware?

Ransomware wird meistens per E-Mail oder Exploits verbreitet. Im ersten Fall sendet der Cyberkriminelle eine Phishing-E-Mail mit einem Anhang, beispielsweise an eine bestimmte Organisation. Der nichtsahnende Nutzer öffnet diesen Anhang (Word-Dokument oder eine JavaScript-Datei), weil in dem Moment der Inhalt des E-Mail-Textes trügerisch echt auf das Opfer wirkt. Der Anwender erhält beim Öffnen des Word-Dokuments dann die Nachricht, dass Makros aktiviert werden müssen, um den Inhalt korrekt anzuzeigen. Denn erst durch das Aktivieren von Makros wird die Ransomware durch Ausführen eines hinterlegten Scripts über einen Drive-by-Download unbemerkt auf den Computer heruntergeladen.

4. Was passiert, wenn Ransomware den Computer infiziert?

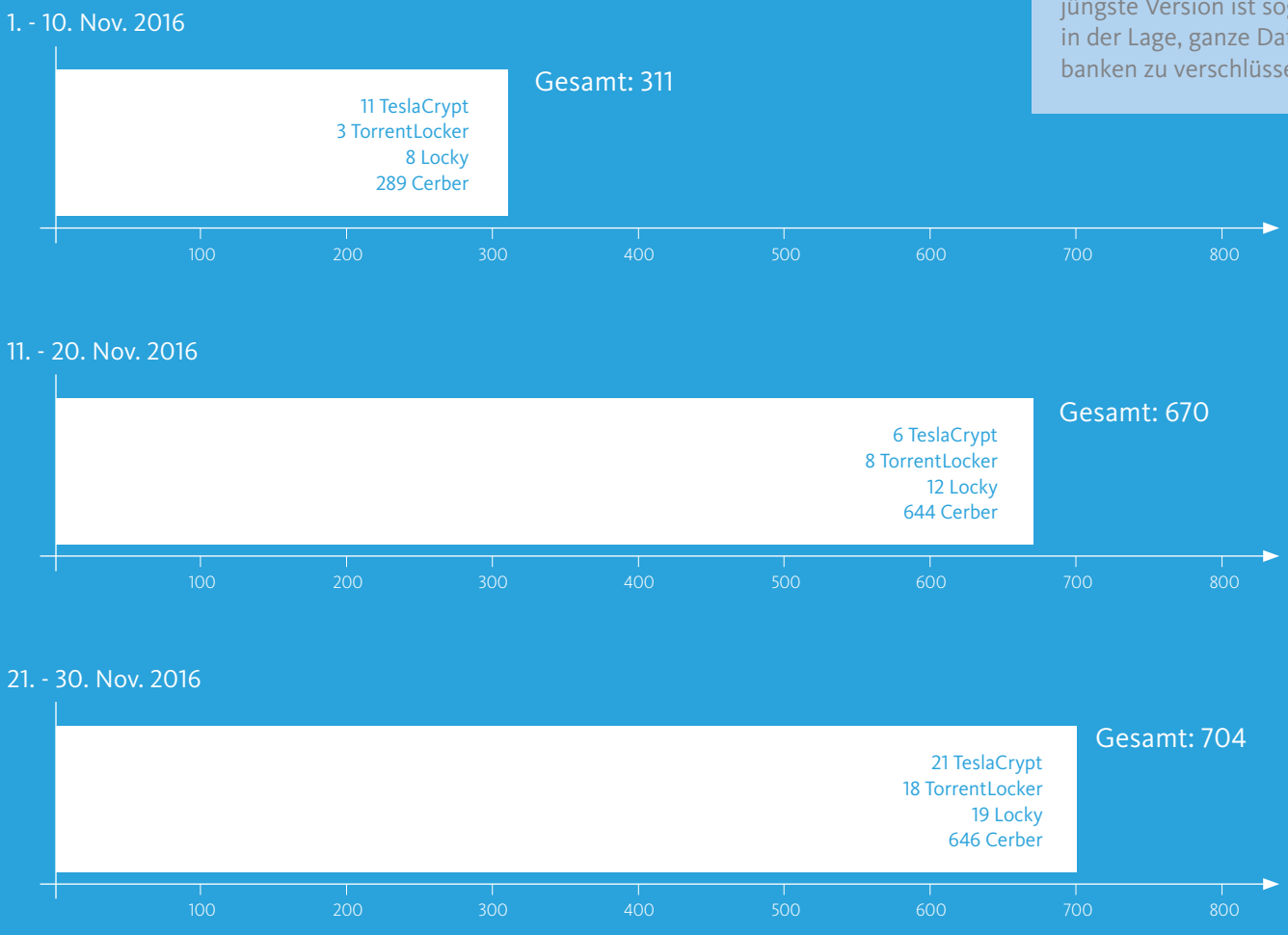
Die heruntergeladene Crypto-Ransomware verschlüsselt alle vorhandenen Dateien wie Bilder, Videos, Office-Dateien usw. Sie chiffriert sogar Daten auf Wechsellaufwerken oder Cloud-Storages, die zu dem Zeitpunkt angeschlossen sind. Nachdem alle Dateien mit einer speziellen Datei-Erweiterung verschlüsselt wurden, verlangt die Ransomware einen Geldbetrag im Austausch für die Entschlüsselung aller Dateien. Das „Lösegeld“, das häufig in Bitcoins auf einer speziellen Webseite im Darknet bezahlt werden muss, kann bis zu mehrere tausend Euro betragen. Bei Ransomware, die den Startbildschirm sperrt, sodass der Nutzer nicht mehr auf sein Gerät zugreifen kann, wird ebenfalls ein Lösegeld für das Entsprerren gefordert – etwa durch den Kauf einer UKash-Karte oder anderer digitaler Zahlungsmitteln.

5. Wie ist die aktuelle Bedrohungslage?

Ransomware-Attacken werden sich weiter fortsetzen, da das Geschäftsmodell für die Cyberkriminellen sehr lukrativ ist und viele Opfer – wohl oft auch stillschweigend – zahlen. Dieses anhaltende Geschäftsmodell wird von den Cyberkriminellen ständig weiterentwickelt. So werden mittlerweile nicht nur Windows-Programme (Portable Executable) verwendet, sondern verstärkt auch Script-Sprachen (VBS, JavaScript, Powershell) eingesetzt, um eine Malware-Klassifizierung zu erschweren. Ransomware gibt es inzwischen auch auf Android-Geräten: Der Anwender kann sein Smartphone so lange nicht nutzen, bis er sich per SMS-Zahlung freikauft. Mac-Anwender sind u.a. von der Ransomware KeRanger betroffen. Weitere bekannte Vertreter sind „Petya", „FBI Ransomware" oder „Locky", die bereits Millionen von Windows-Rechnern infiziert haben.

Ransomware – eine permanente Gefahr

Aufkommen ausgewählter Verschlüsselungstrojaner im November 2016 | Quelle: ransomwaretracker.abuse.ch



Cerber

Zu den besonders gefährlichenen Ransomware-Vertretern gehört die Cerber-Familie, die sich in der Regel als Anhang von E-Mails verbreitet. Ihre jüngste Version ist sogar in der Lage, ganze Datenbanken zu verschlüsseln.

6. Welche Sicherheitstechnologien setzt Avira ein, um Ransomware zu bekämpfen?

Es bedarf eines mehrschichtigen Sicherheitsansatzes, um die Risikofaktoren von Ransomware zu minimieren und einzudämmen. Avira hat effiziente Technologien zur Echtzeit-Erkennung und -Bekämpfung von Schadsoftware entwickelt. Wir setzen auf „State of the Art"-Technologien wie Maschinelles Lernen/Künstliche Intelligenz, Reputation, verhaltensbasierte Erkennung und Echtzeit-Analysen, um unbekannte Dateien einzustufen. Durch unsere Cloud haben unsere Nutzer immer Zugriff auf die aktuellsten Daten. Zukünftig werden durch Künstliche Intelligenz gestützte Systeme eine wesentliche Rolle spielen, wenn es um die Analyse und Einstufung von noch unbekannter Schadsoftware geht.

Fünf Tipps, wie Sie sich effektiv vor Ransomware schützen:

1

Antiviren-Software auf allen Ihren Geräten installieren

Nutzen Sie eine Virenschutzlösung auf allen Ihren Geräten (PC, Mac, Smartphones und Tablets).

Avira erkennt und blockiert alle bekannten Ransomware-Bedrohungen.

2

Vorsicht vor schädlichen E-Mails und Links

Öffnen Sie nur E-Mail-Anhänge von Absendern, die Sie kennen. Klicken Sie

ausschließlich auf Links und Social Media Posts, die vertrauenswürdig sind.

3

Alle Programme auf dem neuesten Stand halten

Installieren Sie Software-Updates und Patches immer sofort. Das erschwert es der Ransomware, den Computer zu infizieren. Achten Sie darauf, dass die Software auf allen Ihren Geräten aktuell ist, um Schwachstellen zu vermeiden. Wenn Sie unsicher sind, wie Sie Ihre Software immer auf dem neuesten Stand halten und so Sicherheitslücken vermeiden, dann hilft Ihnen ein Tool wie **Avira Software Updater**. Es alarmiert Sie über veraltete Software und erspart Ihnen die Suche nach Updates.

4

Regelmäßig Daten-Backups erstellen

Wir empfehlen Ihnen, Ihre Daten regelmäßig in der Cloud oder auf einer externen Festplatte zu sichern. Sollten Ihre Dateien dann von einer Ransomware verschlüsselt werden, können Sie Ihre Festplatte bedenkenlos formatieren. Sie haben Ihre Daten schließlich an einer externen Stelle gesichert.

5

Verwenden Sie einen Browserschutz oder besser: einen sicheren Browser wie Avira Scout

Die kostenfreie Browsererweiterung von Avira blockiert schädliche Webseiten und schützt Ihre Privatsphäre.

Avira Scout blockiert automatisch schädliche Webseiten und Phishing-Seiten und enthält eine Funktion gegen Tracking. Damit ist der Browser von Avira einer der wenigen auf dem Markt, der keine Daten darüber sammelt, welche Seiten Sie im Internet besuchen, was Sie herunterladen und online shoppen.

Über Avira

Avira, ein überdurchschnittlich wachsendes Unternehmen in Familienbesitz, wurde 1986 von dem IT-Sicherheitspionier Tjark Auerbach in Tettnang gegründet und ist einer der bedeutenden regionalen Arbeitgeber am Bodensee.

Seit nunmehr drei Jahrzehnten bietet Avira seinen Kunden selbstentwickelte Sicherheitslösungen zum Schutz vor Internetbedrohungen, Malware-Angriffen, schädlichen Programmen und Datendiebstahl. Über 100 Millionen Nutzer – vor allem Mikro- und Kleinunternehmen sowie Privatanwender – verlassen sich auf die Software von Avira und schätzen deren Zuverlässigkeit, Performance und Benutzerfreundlichkeit.

Unter den weltweit führenden Antivirensoftwareherstellern nimmt Avira Platz zwei ein. Das von Travis Witteveen geleitete Unternehmen unterhält eigene Virenlabore und stellt seine Innovationsfreude und Leistungsfähigkeit immer wieder unter Beweis, indem es zukunftsweisende Sicherheitstechnologien entwickelt. Dazu gehören der Echtzeitschutz durch cloudbasierte Malware-Erkennung oder die Webkonsole „Online Essentials“.

Avira arbeitet eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen und ist Gründungsmitglied der Initiative „IT-Security made in Germany“.

Aviras Erfahrung und vielfach ausgezeichnete Produkte und Services sind ein Beitrag, damit Menschen sich in unserer digitalen Welt frei und sicher bewegen können.

Darüber hinaus liegt Avira auch die Sicherheit in der realen Welt am Herzen: Die Auerbach Stiftung des Firmengründers unterstützt gemeinnützige und soziale Vorhaben und förderte bereits weit über 300 Projekte in den Bereichen Bildung und Erziehung, Kinder, Jugend und Familie, Altenhilfe, Behindertenhilfe sowie Kunst und Kultur.

Avira

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany
Telefon: +49 7542-500 0

Irrtümer und technische Änderungen vorbehalten. Stand: Dezember 2016

PROTECTING PEOPLE
IN THE CONNECTED WORLD

www.avira.com