Ronald Eikenberg

Online-Abzocke

Antworten auf die häufigsten Fragen

Viren-Alarm auf dem Smartphone

? Beim Surfen beginnt mein Android-Smartphone zu vibrieren und meldet innerhalb des Browsers, es sei mit einem Virus infiziert. Abhilfe soll die Installation einer Virenschutz-App schaffen. Ist da was dran?

! Nein, es handelt sich um eine gleichermaßen unseriöse wie aggressive Form der Werbung, die Sie zur Installation bestimmter Apps verleiten will. Sie können den Browser-Tab mit dem Warnhinweis getrost schließen. Falls Sie die beworbene App bereits installiert haben, können Sie über die Einstellungen eine Deinstallation anstoßen. Das sollten Sie insbesondere dann auf jeden Fall tun, wenn die App nicht über den Play Store installiert wurde.

SMS-Warnung nach eBay-Kleinanzeige

? Kurz nachdem ich eine Annonce bei eBay-Kleinanzeigen reingestellt habe, trafen auf meinem Handy zwei SMS-Nachrichten mit einer „eBay-Kleinanzeigen Konto Sicherheitswarnung" ein. Die Nachrichten verweisen auf eine Website, bei der ich mich einloggen soll. Ist das eine bekannte Betrugsmasche oder sind die Nachrichten echt?

! Offenbar versuchen Online-Ganoven, an Ihre Zugangsdaten zu kommen. Die Abzocker missbrauchen die bei eBay-Kleinanzeigen hinterlegte Rufnummer für einen Phishing-Versuch. Es besteht kein Handlungsbedarf; löschen Sie die Nachrichten einfach. Es kursieren ähnliche SMS- und WhatsApp-Nachrichten, die beispielsweise vorgeben, dass man bei einem Gewinnspiel den Hauptgewinn gezogen hat. Es handelt sich dabei meist um Betrugsversuche oder Kettenbriefe. Seien Sie bei Kurznachrichten genauso skeptisch wie bei E-Mails.

Microsoft-Support ruft an

? Mich hat jemand angerufen, der angeblich beim Microsoft-Support arbeitet. Er behauptet, mein Rechner sei mit einem Schädling infiziert und bietet mir seine Hilfe bei der Entfernung an.

! Der Anrufer will Ihnen Geld aus der Tasche zu ziehen. Callcenter-Mitarbeiter – oft aus dem asiatischen Raum – rufen zufällig Telefonanschlüsse an und versuchen den Angerufenen davon zu überzeugen, dass sein Rechner infiziert ist. Anschließend verschafft sich der Anrufer Fernzugriff auf den PC; etwa, indem er den Angerufenen zur Installation von TeamViewer animiert. Dann diagnostiziert der Anrufer das vermeintliche Problem unter Vortäuschung falscher Tatsachen. Geht es schließlich um die Lösung, bittet der Anrufer sein Opfer in spe zur Kasse und fragt nach dessen Kreditkartendaten. Will man nicht zahlen, kann es passieren, dass der Anrufer den Rechner blockiert. Microsoft hat mit der Angelegenheit nichts zu tun.

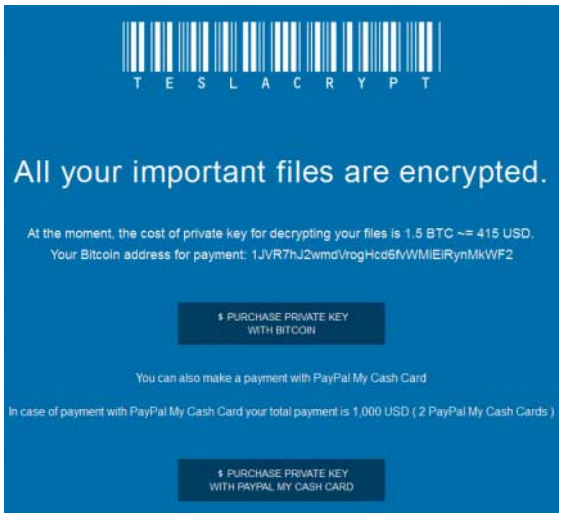
Lösegeld zahlen?

? Mein Rechner ist mit einem Schädling infiziert, der behauptet, meine persönlichen Dateien verschlüsselt zu haben. Erst nach Zahlung von 400 US-Dollar bekomme ich angeblich wieder Zugriff darauf. Kann ich meine Daten retten, ohne das Lösegeld zu zahlen?

! Diese Frage kann man nicht pauschal beantworten – aber die Chancen stehen schlecht. Es kommt darauf an, welchen Schädling Sie sich eingefangen haben – und in welcher Version. Während für einige Verschlüsselungs-Trojaner wie Bitcryptor kostenfreie Entschlüsselungswerkzeuge im Netz kursieren (siehe c't-Link), haben Sie bei vielen aktuellen Erpressungs-Trojanern Pech. Wer keine Backups hat, kann die betroffene Platte mit Tools wie ShadowExplorer nach Schattenkopien der ursprünglichen Daten durchsuchen. Möglicherweise fördern auch Datenrettungsprogramme wie Recuva noch Originale zu Tage. Allzu große Hoffnungen sollten Sie sich nicht machen, da mittlerweile viele Schädlinge diese Rettungsmöglichkeiten gezielt eliminieren. Führt kein Weg zum Ziel, sollten Sie die chiffrierten Dateien aufheben. Möglicherweise wird in Zukunft eine Methode bekannt, die Verschlüsselung zu knacken.

Die Zahlung des Lösegelds ist ein potenzieller Weg, die Daten aus dem Nirwana zurückzuholen. Eine Garantie dafür, dass der Online-Ganove anschließend tatsächlich den zur Entschlüsselung nötigen Krypto-Schlüssel herausrückt – und die Entschlüsselung gelingt –, gibt es allerdings nicht. Lernen Sie aus dem Vorfall und sichern Sie künftig regelmäßig alle Daten, auf die Sie nicht verzichten können. Sie können die Daten zum Beispiel in der Cloud oder auf einem USB-Speicher sichern, welcher nicht ständig mit dem Rechner verbunden ist.

c't Erste Hilfe gegen Verschlüsselungs-Trojaner: ct.de/y99n



Hat ein aktueller Erpressungs-Trojaner das digitale Hab und Gut verschlüsselt, kann man versuchen, mit Recovery-Tools zu retten, was noch zu retten ist.

Online-Shop geknackt

? Ein Online-Shop, bei dem ich vor Jahren eingekauft habe, hat mich per Mail darüber informiert, dass sich Kriminelle Zugriff auf die Kundendaten verschafft haben. Was muss ich jetzt tun?

! Ihr Passwort ist jetzt verbrannt und in den Händen von Online-Ganoven. Wenn Sie das im Shop genutzte Passwort bei mehreren Diensten eingesetzt haben, müssen Sie es überall ändern. Legen Sie bei dieser Gelegenheit für jeden Dienst ein – zumindest geringfügig anderes – Passwort fest, damit Sie beim nächsten Vorfall nicht erneut die Runde machen müssen. Machen Sie sich darauf gefasst, dass Sie Phishing-Mails mit persönlicher Anrede erhalten werden, die gut auf Sie zugeschnitten sind. Falls auch Zahlungsinformationen kopiert wurden, sollten Sie Ihre Kontoauszüge und Kreditkartenabrechnungen in den folgenden Monaten besonders aufmerksam kontrollieren. (rei@ct.de)