VORSICHT KRYPTO TROJANER

5 einfache Regeln zum Schutz

Krypto-Trojaner sind Computerviren, mit denen wir in Zukunft noch häufiger zu tun haben werden. In 2015 waren 3,1 Mio. Deutsche von einem Verschlüsselungs-Trojaner betroffen, Tendenz steigend. Sie werden meist per E-Mail oder mittels präparierter Webseiten verbreitet. Gelangt der Krypto-Trojaner auf Ihren Computer, werden alle Unternehmensdaten verschlüsselt und lassen sich nicht mehr öffnen. Den Schlüssel zum Dechiffrieren der Daten geben die Erpresser nur gegen Lösegeld preis. Im Moment gibt es noch keine Möglichkeiten, die Daten wieder selbst zu entschlüsseln.

Deshalb hier die wichtigsten 5 Regeln zur Vermeidung von Schäden. Wir empfehlen dringend diese auch an Ihre Kollegen weiterzugeben.

Vorsicht bei E-Mails mit Anhängen

1. Krypto-Trojaner kommen meistens als Anhang einer E-Mail, oft sind diese als Rechnungen oder Zahlungsaufforderungen getarnt. Das Dokumentenformat ist häufig als Word (.doc, docx, docm) abgespeichert, aber auch auch andere Office-Dokumente sind möglich. Vor dem Öffnen eines Anhangs immer Absender und oben genannte Eigenschaften prüfen. Im Zweifelsfall den Anhang NICHT öffnen und Ihre IT-Spezialisten oder Ihren IT-Dienstleister kontaktieren.

Erst Nachdenken, dann klicken

2. Erhalten Sie eine E-Mail von einer Person aus einem Unternehmen, zu dem Sie keine Geschäftsbeziehung haben, sollten Sie den Anhang auf keinen Fall öffnen. Vor allem, wenn auch die zweite Voraussetzung zutrifft: Die mit einem Virus versehenen Mails sprechen Sie nicht persönlich an sondern haben eine allgemein gehaltene Anrede (z.B. Sehr geehrte Damen und Herren).

Aktualisieren Sie Ihre Software regelmäßig

3. Sicherheitslücken, die als Einfallstor für Viren gelten, gibt es fast in jeder Software. Wird diese bemerkt, veröffentlichen die Software-Hersteller in der Regel schnell ein Software-Update, um die Lücke zu schließen.
Verfügbare Software-Updates sollten so schnell wie möglich installiert werden.

Keine zweifelhaften Links anklicken

4. Ein weiteres Risiko, sich mit einem Virus zu infizieren, sind Links in E-Mails und auf Webseiten, insbesondere auf Social-Media-Plattformen wie Facebook. Bevor Sie einem Link folgen, sollte man sicher sein, dass das Linkziel vertrauenswürdig ist.

Im Zweifelsfall nachfragen

5. Wenn Ihnen ein Anhang oder ein Link verdächtig erscheint, auf keinen Fall anklicken. Sollte die Nachricht wichtig erscheinen, lieber zuerst den Absender telefonisch nachfragen oder direkt Ihren Administrator oder IT-Dienstleister kontaktieren.
So minimieren Sie das Risiko, sich mit einem Virus zu infizieren, deutlich!

Sie benötigen Unterstützung? Sprechen Sie uns an: vertrieb@interconnect.de

InterConnect GmbH & Co. KG · Am Fächerbad 3 · 76131 Karlsruhe · Fon: 0721/6656-0 · info@interconnect.de · www.interconnect.de