Achtung: Krypto Trojaner

Wie Sie sich mit einfachen Regeln schützen

inett

Bitte weitergeben!

Krypto-Trojaner sind Computerviren, die meist per E-Mail oder präparierte Websites verbreitet werden. Gelangen diese auf Ihren Computer, werden alle Unternehmensdaten verschlüsselt und erst gegen Zahlung eines Lösegelds wieder entschlüsselt. Derzeit gibt es technisch keine Möglichkeit, die Daten selbst zu entschlüsseln. Daher besteht ein hohes Risiko für Ihre Unternehmensdaten. Die wichtigsten Regeln zur Vermeidung von Schäden haben wir im Folgenden Zusammengefasst. Bitte geben Sie dieses Infoblatt auch an Mitarbeiter und Kollegen weiter.

① Vorsicht bei E-Mails mit Anhängen

Krypto-Trojaner kommen meist per E-Mail. Die E-Mails sind als Rechnung oder Zahlungsaufforderung gekennzeichnet und beinhalten ein Dokument im Anhang. Als Dokumentenformat kommt meist Word (.doc oder .docx, .docm) zum Einsatz, aber auch andere Office Dokumente können gefährlich sein.

Vor dem Öffnen eines Anhangs prüfen Sie bitte den Absender und den Anhang, ob die oben genannten Eigenschaften zutreffen. Öffnen Sie den Anhang der Mail im Zweifelsfalls nicht, da hierdurch der Virus aktiviert wird.

② Erst Nachdenken, dann klicken

Wenn Sie eine E-Mail von einem Unternehmen oder einer Person erhalten, mit der Sie keine Geschäftsbeziehung haben ist dies ein Hinweis auf eine gefälschte und mit einem Virus versehene Mail.

Ein weiterer Hinweis ist, dass die Mail an allgemeine Empfänger gerichtet ist und Sie nicht namentlich und persönlich in dieser Mail angesprochen werden.

③ Halten Sie Ihre Software aktuell

Nahezu jede Software besitzt Sicherheitslücken, die als Einfallstor für Viren verwendet werden kann. Wird eine Sicherheitslücke bemerkt, veröffentlicht der Hersteller einer Software meist schnell ein Update um die Lücke zu schließen.

Installieren Sie daher möglichst schnell verfügbare Software Updates, um die möglichen Einfallstore gering zu halten. Bitte beachten Sie hier aber die Freigabe von Softwareversionen für Ihr System und fragen im Zweifelsfall Ihren Administrator oder IT Dienstleister.

④ Klicken Sie keine zweifelhaften Links an

Neben Dateianhängen bergen auch Links in E-Mails und Beiträge auf Facebook und anderen Social Media Plattformen ein hohes Risiko. Bevor Sie einem Link folgen sollten Sie sich vergewissern, dass das Linkziel, also die Adresse auf die der Link zeigt, vertrauenswürdig ist.

⑤ Im Zweifelsfall nachfragen

Wenn Ihnen eine E-Mail, ein Anhang oder ein Link suspekt vorkommt, klicken Sie ihn nicht an. Wenn es Ihnen wichtig erscheint, kontaktieren Sie den Absender telefonisch und fragen nach, ob die gesendete Mail tatsächlich von ihm stammt. Alternativ fragen Sie bei Ihrem Administrator oder Ihrem IT Dienstleister nach um das Risiko zu minimieren.

Kontakt

inett GmbH
Eschberger Weg 1
66121 Saarbrücken
0681 / 410993-0
0681 / 410993-99
info@inett.de
www.inett.de