Informatik und Dienstleistungen

Aktuelle Bedrohungen Windows

Erpressungstrojaner Jaff: Vorsicht vor Mails mit PDF-Anhang.

Derzeit sind vermehrt E-Mails mit manipulierten PDF-Dokumenten im Umlauf. Wer das Dokument unter Windows öffnet, kann sich die Ransomware Jaff einfangen.

Dieser Schädling verschlüsselt Daten und verlangt für die Freigabe ein Lösegeld in Höhe von rund 2 Bitcoin (ca. CHF 4'500.-). Sobald die Dateien verschlüsselt sind, weisen diese die Dateiendung .wlu auf und lassen sich nicht mehr öffnen: Ein Foto heisst dann z. B. "Ferien.jpg.wlu".

Wie bei Ransomware üblich, wird die Schadsoftware per E-Mail verteilt. Im Gegensatz zu vergleichbaren Trojanern sind es dieses Mal keine Word-Dokumente, sondern manipulierte PDF-Dateien, die im Anhang mitgeschickt werden.

Präventive Massnahmen

- Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten. Auf unserer Homepage www.ocom.ch/dienstleistungen/ratgeber finden Sie alles zum Thema Datensicherung.

- Seien Sie immer vorsichtig bei verdächtigen E-Mails, welche Sie unerwartet bekommen oder welche von einem unbekannten Absender stammen. Befolgen Sie hier keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links.

Aktuelle Bedrohungen Apple

Unbekannte sperren iPhones sowie Macs – und fordern Lösegeld.

Apple-Nutzer werden mit Hilfe der iCloud-Fernsperrfunktion erpresst: Angreifer sperren den Zugang zu iPhones und Macs aus der Ferne mit einem PIN – und fordern Lösegeld.

Derzeit bedienen sich Unbekannte offenbar wieder verstärkt Apples Systemfunktion "Mein iPhone suchen" respektive "Meinen Mac suchen" für Erpressungsversuche. Hierbei werden gehackte Zugangsdaten benutzt, um sich in den iCloud-Account des Opfers einzuloggen und dessen Geräte aus der Ferne zu sperren. Zusätzlich wird eine Nachricht mit einer E-Mail-Adresse zur Kontaktaufnahme übermittelt, die dann Lösegeld für eine Freischaltung fordert – derzeit umgerechnet rund CHF 50.- , bei Nichtbezahlung

OCOM AG Informatik und Dienstleistungen
Englisch-Gruss-Strasse 6, Postfach 556, 3902 Brig-Glis
OCOM STORE Kantonsstrasse 21, 3902 Brig-Glis
T 027 922 10 10, F 027 922 10 11, ocom@ocom.ch, www.ocom.ch

steigt der Wert immer höher. Ob die Erpresser die Geräte nach einer Zahlung tatsächlich wieder freigeben, bleibt unklar.

In einem uns vorliegenden Fall wird als Kontaktadresse help.apple.us@gmail.com genannt.

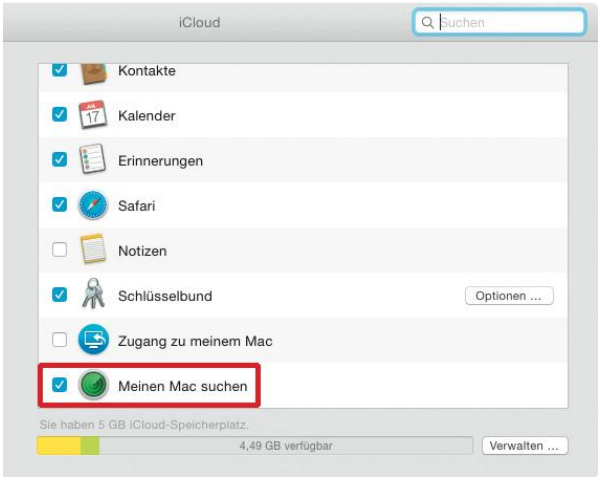
Die Masche ist nicht neu: Erpressungswellen über die iPhone- respektive Mac-Fernsperre gibt es seit mehreren Jahren immer wieder.

Fernsperrung besonders unangenehm für Mac-Nutzer

Heikel ist die Situation vor allem für Mac-Nutzer: Hier kann ein Angreifer mit Kenntnis der Apple-ID respektive der iCloud-Zugangsdaten den Mac stets mit einer eigenen PIN sperren – und zwar auf Firmware-Ebene. Der Mac lässt sich dann nur noch mit diesem PIN entsperren. Apples Fernsperrfunktion ist standardmässig aktiviert, sobald man sich auf einem iPhone oder Mac bei iCloud anmeldet.

Präventive Massnahmen

- Schalten Sie besonders beim Mac die «Meinen Mac suchen» Funktion aus. Wählen Sie „Apple" > „Systemeinstellungen" und klicken Sie auf „iCloud".
- Erstellen Sie regelmässig eine Sicherungskopie (Backup) Ihrer Daten z. B. über Apples eigenes Backup Programm Time Machine. https://support.apple.com/de-ch/HT201250



- Seien Sie immer vorsichtig bei verdächtigen E-Mails, welche Sie unerwartet bekommen oder welche von einem unbekannten Absender stammen. Befolgen Sie hier keine Anweisungen im Text, öffnen Sie keinen Anhang und folgen Sie keinen Links.
- Erstellen Sie ein sicheres iCloud Passwort. Tipps für ein sicheres Passwort finden Sie in unserem Ratgeber unter https://www.ocom.ch/data/File/Ratgeber-Passwort.pdf

Bei Fragen oder Unklarheiten können Sie sich gerne bei uns melden.

OCOM AG Informatik und Dienstleistungen
Englisch-Gruss-Strasse 6, Postfach 556, 3902 Brig-Glis
OCOM STORE Kantonsstrasse 21, 3902 Brig-Glis
T 027 922 10 10, F 027 922 10 11, ocom@ocom.ch, www.ocom.ch