Cyber-Erpressung wird immer häufiger

Immer mehr Computer werden mit sogenannter Ransomware infiziert. Dabei verschlüsseln Krypto-Trojaner die Daten auf dem Rechner und geben sie erst gegen Zahlung eines Lösegeldes, meist in Bitcoin, wieder frei. Während in der Vergangenheit hauptsächlich Windows-Rechner im Visier krimineller Hacker standen, können sich seit Kurzem auch Mac-Nutzer nicht mehr sicher fühlen.

„Die Fälle von Erpresser-Software nehmen weltweit zu“, erklärt Götz Schartner vom Verein Sicherheit im Internet e. V. und Mitveranstalter der Initiative SpardaSurfSafe, und führt aus: “Sowohl für Privatanwender als auch für Unternehmen stellt Ransomware eine der größten Gefahren im Netz dar, denn im Gegensatz zu anderer Malware wie Keyloggern oder Banking-Trojanern brauchen Krypto-Trojaner keine Administratorenrechte, um sich festzusetzen. Es reicht der Zugriff auf die Daten des Rechners. Hinzu kommt, dass Bitcoins die Abwicklung der Zahlungen deutlich vereinfacht haben und ein hohes Maß an Anonymität garantieren. Das macht derartige Angriffe natürlich besonders interessant. Bislang beschränkte sich das Problem auf Computer mit dem Betriebssystem Windows, doch in der vergangenen Woche ist nun erstmals auch ein funktionierender Krypto-Trojaner für Apples OS X aufgetaucht.“

Das derzeit erfolgreichste Schadprogramm dieser Art ist Locky, das sich sowohl über Phishing-Mails mit Word-Anhang als auch über JavaScript verbreitet. Hat sich der Trojaner erst einmal eingenistet und ist aktiv geworden, bleibt dem Nutzer nur noch die Zahlung des Lösegeldes, um wieder Zugang zu seinen Daten zu erhalten. „Derzeit gibt es keine Möglichkeit, die Verschlüsselung durch Locky zu umgehen, außer man zahlt. Glücklicherweise scheint es auch unter Hackern eine Art Ganovenehre zu geben, denn bislang ist uns kein Fall bekannt, bei dem die Zahlung nicht zum gewünschten Ergebnis geführt hat“, so Schartner. Wer Sicherheitskopien auf einem externen Speicher hat, kann sich glücklich schätzen, denn im Moment ist das die einzige Möglichkeit, ohne Lösegeld wieder an seine Daten zu kommen. Doch auch hier sehen Experten bereits ein Problem, denn in Zukunft könnte Ransomware auch tiefer in die Systeme eindringen und ein Back-up unmöglich machen.

Davor warnen auch die amerikanischen Sicherheitsexperten von Palo Alto Networks, die in der vergangenen Woche den ersten funktionstüchtigen Krypto-Trojaner für Apples OS X entdeckten. Die KeRanger genannte Malware hatte sich an den Download der Software von Transmission angehängt, einem beliebten BitTorrent-Programm. Künftige Versionen von KeRanger könnten durchaus auch auf Time-Machine-Daten zugreifen und dort Daten verschlüsseln. Dadurch wäre es unmöglich, den Rechner zurückzusetzen und die Daten aus dem Back-up wiederherzustellen.

„Derzeit gibt es keinen wirksamen technischen Schutz vor Krypto-Trojanern“, warnt Schartner. „Umso wichtiger ist es,

Internetnutzer darüber aufzuklären, dass sie Vorsicht walten lassen müssen. Das Programm SpardaSurfSafe widmet sich genau dieser Aufgabe, denn es klärt Schüler, Eltern und Lehrer über die Gefahren im Netz auf – nicht nur in unseren Live-Hacking-Vorträgen zu Beginn des Programms, sondern konstant beispielsweise über unsere Webseite www.spardasurfsafe-bw.de."

Zum Schutz vor Krypto-Trojanern empfiehlt der Verein Sicherheit im Internet e. V.:

- Erstellen Sie regelmäßige Back-ups. So können Sie die meisten Ihrer Daten wiederherstellen.
- Vorsicht bei Dateianhängen! Öffnen Sie diese nur, wenn Ihnen der Absender persönlich bekannt ist. Auch bei vermeintlich vertrauenswürdigen Absendern wie Ihrer Bank kann es sich um Phishing-Mails handeln!
- Laden Sie Software nur von vertrauenswürdigen Seiten herunter. Das allein ist allerdings noch kein Schutz vor einer Infektion, wie KeRanger zeigt – die kompromittierte Datei hatte sogar ein Mac-Sicherheitszertifikat. Es empfiehlt sich, mit der Installation einer neuen Software-Version zusätzlicher Programme einige Tage zu warten. Bis dahin sind Virusinfektionen meistens erkannt und behoben.

Zahlen oder nicht zahlen, das ist hier die Frage

Doch was tun, wenn das Kind bereits in den Brunnen gefallen ist und man die gefürchtete Erpressernachricht auf dem Bildschirm sieht? Die Empfehlungen des FBI in den USA und des BSI in Deutschland gehen auseinander. Während das FBI vorschlägt, das Lösegeld zu bezahlen – die Verschlüsselung wäre zu ausgereift und man könne da nichts tun – rät das BSI, den Forderungen nicht nachzugeben, denn es gäbe keine Garantie, dass die Erpresser Wort halten. „Wer die Möglichkeit hat, seine Daten ohne große Verluste aus einem Back-up wiederherzustellen, sollte sich die Zahlung sparen.", erklärt Götz Schartner. Denn ist ein Unternehmen erst einmal als erpressbar bekannt, werden diese Informationen auch unter den Kriminellen ausgetauscht.

Bild: © agsandrew / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4942329/steigende-gefahr-durch-cyber-erpressung/