IKARUS Security Software warnt: Erpresser-E-Mails drohen mit schlechten Online-Bewertungen

Das IKARUS Malware-LAB verzeichnete in den letzten Tagen eine neue Variante digitaler Erpressung: Statt mit der Verschlüsselung von Daten oder dem Versenden intimer Bilder, wird mit schlechten Online-Rezensionen gedroht. Die Opfer werden gezielt ausgesucht.
Die klassische Mundpropaganda wird vor allem im Einzelhandel immer mehr von Online-Bewertungen und den im Netz vergebenen "Sternen" abgelöst. Webshops und Websites kennen den Wert der digitalen User-Bewertungen schon längst. Nun sind auch Cyber Angreifer*innen auf den Zug aufgesprungen. Security-Experte Joe Pichlmayr, CEO von IKARUS Security Software, sieht eine neue Welle von Lösegeld-Forderungen auf Website-Betreibende zu kommen: "Für diese Form der Erpressung braucht es keine grossartigen technischen Fähigkeiten oder Infrastrukturen. Mit geringem Aufwand seitens der Erpressenden kann hoher Schaden verursacht werden."

In aktuellen E-Mails werden Unternehmen dazu aufgefordert, die eher moderate Summe von 0,1 Bitcoin (entspricht etwa 300 Euro) zu bezahlen, um negative Bewertungen und "Attacken" auf Plattformen wie Google, Booking.com, Facebook, Instagram oder Xing zu verhindern. "Die vergleichsweise niedrige Summe soll Opfer leichter zu Zahlung verleiten. Dennoch, wir raten deutlich davon ab", erklärt Joe Pichlmayr: "Ein zahlendes Opfer kann jederzeit wieder zur Kassa gebeten und einer Form von digitalisierter Schutzgelderpressung unterworfen werden - anders als im realen Leben mit Pech auch von mehreren verschiedenen Gruppen."

Einen wirksamen Schutz gegen diese neue Form der digitalen Erpressung gibt bisher kaum. "Solange mit relativ geringem Aufwand "negative" Kritiken vergeben werden können, bleibt es wohl eine Frage der Glaubwürdigkeit der Gegendarstellungen, bis Google oder andere Dienste entsprechende Services entwickeln, um rasch auf solche "Erpresser-Kritiken" zu reagieren", so Pichlmayr. IKARUS empfiehlt daher nicht nur Betroffenen: Verbreiten Sie die Nachricht!

Tipps (nicht nur) für Betroffene: Spread the word!

"Vermeiden Sie Zahlungen", rät Pichlmayr den Empfängern der Drohmails: "Posten Sie das Erpresser-E-Mail und Links zu Beiträgen über diese Erpresser-Masche unter den jeweiligen negativen Rezensionen." Je mehr potenzielle Opfer, Rezensionen-Lesende und Service-Betreibende von der neuen Ransom-Variante wissen, desto geringer der Ãœberraschungseffekt und die Glaubwürdigkeit der gefälschten Kritiken: "Missbrauchen Sie den Text aber nicht, um unzufrieden Kundenrezensionen zu relativieren!"

Informieren Sie umgehend die Betreibenden der jeweiligen Services. Motivieren Sie auch Ihre zufriedenen Stammkund*innen, Ihnen zur Seite zu stehen, beispielsweise indem Sie unangemessene Inhalte melden oder positive Bewertungen abgeben. Erstatten Sie ausserdem Anzeige bei der nächsten Polizeidienststelle. Speichern Sie dafür das ursprüngliche Erpresser-Mail (Ã–ffnen Sie die Nachricht und speichern Sie das Mail mit einem Klick auf "Datei" und "Speichern unter" auf den Datenträger) und Screenshots allfälliger bereits erfolgter Rezensionen auf einen USB-Stick. Ihre Anzeige hilft dabei, ein genaueres Bild vom Ausmass der Angriffe zu bekommen, Untersuchungen voranzutreiben und die öffentliche Awareness zu steigern.

Linktipps:

- Spam und Fake-Inhalte widersprechen den Google-Richtlinien, können als unangemessen gemeldet und müssen gelöscht werden: