Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

22.07. 2019

IT-Sicherheit: Bedrohungslage in der Schweiz besorgniserregend

Von PPS

Analyse von Proofpoint zu den größten Cybergefahren in der Schweiz

(München)(PPS) **Die Gefährdungslage für Schweizer Unternehmen und Behörden in Sachen Cybersicherheit gibt weiterhin Anlass zur Sorge. Das legen Untersuchungsergebnisse von Proofpoint, einem der führenden Next-Generation Cybersecurity- und Compliance-Unternehmen, nahe. Wenig überraschend: Vor allem der Finanzsektor in der Schweiz ist für Cyberkriminelle ein attraktives Angriffsziel. Darüber hinaus gibt es eine Vielzahl von Bedrohungen, die auch Eidgenossen nicht verschonen.**

Im Verlauf der Untersuchungen zur derzeitigen Bedrohungssituation in der Schweiz, stellte das US-amerikanische IT-Sicherheitsunternehmen Proofpoint fest, dass es Hacker in der Schweiz oftmals auf die Log-in-Daten von Bankkunden abgesehen haben. Das beliebteste Werkzeug der Kriminellen dafür war in jüngster Zeit die Schadsoftware Retefe. Dabei handelt es sich um einen Banking-Trojaner, der zumeist über gezippte Datei-Anhänge verbreitet wird, die mit schadhaftem JavaScript versehen wurden oder aber über präparierte Word-Attachments. Nach einer Infektion leitet Retefe den Datenverkehr der betroffenen Banken über seinen eigenen Proxy um. Neben der Schweiz war Retefe in der Vergangenheit hauptsächlich in Österreich und Schweden aktiv – im Moment ist die Schweiz nach Datenlage jedoch offenbar das exklusive Ziel der Cyberkriminellen.

Aber auch andere Varianten von Schadsoftware gefährden derzeit Unternehmer und Verbraucher in der Schweiz. So konnten die Experten von Proofpoint beobachten, dass auch in der Schweiz Emotet vermehrt sein Unwesen treibt. Emotet war zunächst eine sogenannte „General-Purpose-Malware“, also eine Schadsoftware, die sich mit vielerlei Modulen bestücken ließ, je nach gewünschtem Verwendungszweck der Kriminellen – sei es ein Banking-Trojaner, ein Information Stealer oder ein anderer Malware-Typ. In den letzten Jahren entwickelte sich Emotet allerdings von einem Banking-Trojaner hin zu einem eigenständigen Botnet, das vielen anderen Malware-Varianten den Rang abläuft. TA542 (Threat Actor 542), die Gruppe von Cyberkriminellen hinter Emotet, verbreitet die Schadsoftware seit Anfang 2019 in Abermillionen von E-Mails, die vor allem auf den Gesundheits- und Fertigungssektor abzielen.

Ein weiterer Schädling, der die Schweiz derzeit heimsucht ist der Loader Smoke. Smoke ist ein modularer Malware-Downloader, der erstmals 2011 beobachtet wurde und gewöhnlich von russischen Cyberkriminellen bei Angriffen auf Unternehmen wie auch einzelne Nutzer verwendet wird. Verkauft wird die Malware von einer Einzelperson, die sich hinter dem Decknamen „SmokeLdr“ verbirgt und angibt, nur an russische Akteure der Black-Hat-Szene zu verkaufen. Abhängig davon, welche Module erworben werden, bietet Smoke mannigfaltige Möglichkeiten für die Hacker. Zu diesen Möglichkeiten zählen beispielsweise optionale Fähigkeiten wie ein Password Stealer, DNS-Hijackings, Key-Logging sowie die Durchführung von DDoS-Attacken (Distributed Denial of Service). Bei Angriffen in der Schweiz lädt Smoke laut der Analysen von Proofpoint jedoch nach kurzer Zeit hauptsächlich den Banking-Trojaner Retefe nach.

Doch es gibt auch erfreuliche Nachrichten: Wie Proofpoint feststellen konnte, unternahmen schweizerische Top-Unternehmen in den vergangenen sechs Monaten weitere Schritte, um sich besser gegen die sogenannte Chef-Masche beziehungsweise BEC (Business Email Compromise) zu schützen. Zu diesem Zweck implementierten insgesamt 17 der 20 im SMI gelisteten führenden Unternehmen der Schweiz den herstellerunabhängigen DMARC-Standard. Vor einem halben Jahr verfügten von den untersuchten Firmen lediglich 12 über einen DMARC-Eintrag. Dies entspricht einer Steigerungsrate von 25 Prozent und hilft den betreffenden Unternehmen dabei, sich, ihre Mitarbeiter, Partner und Kunden vor Cyberbetrug auf Basis von Domain Spoofing zu schützen – wenngleich nur vier Unternehmen auch aktiv betrügerische Mails blockieren und somit in Gänze DMARC-konform agieren.

Der öffentliche Sektor steht dem Betrug auf Basis von Domain Spoofing hingegen nahezu ungeschützt gegenüber. Nur zwei der von den 26 Kantonen genutzten Domains verfügen über einen DMARC-Eintrag. Dieses Versäumnis steigert natürlich die Gefahr, Opfer von Cyberattacken zu werden.

Näheres zu Retefe und den Smoke-Downloader hat Proofpoint in einem Blogeintrag zusammengefasst, den Sie hier im englischen Original nachlesen können:

www.proofpoint.com/us/threat-insight/post/2019-return-retefe

Über die Organisation:

Proofpoint, Inc. (NASDAQ: PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen zugleich das größte Kapital aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, verlassen sich auf Proofpoint, um ihre wichtigsten Sicherheits- und Compliance-Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren.

Pressekontakt:

AxiCom GmbH
Matthias Uhl
Infanteriestr. 11
80797 München

Tel: +49 (0)89 800 90 819
Fax: +49 (0)89 800 90 810
Email: matthias.uhl @ axicom.com
Web: axicom.de

Kategorie
IT & Software & Neue Medien
