 Die

Graphik : Shutterstock

Schad-Software über E-mails mit Thema Corna-Virus

E-Mail ist das Einfallstor Nummer Eins für Schadsoftware. Das machen sich Cyberkriminelle aktuell vor allem zunutze, indem sie wichtige Informationen oder Angebote zur Corona-Krise vorgaukeln.

Es gilt nach wie vor, dass Nutzer insbesondere im Zusammenhang mit dem Erhalt von E-Mails größte Vorsicht walten lassen sollten. E-Mails sind das bei Weitem erfolgreichste Instrument Cyberkrimineller bei virtuellen Angriffen. Sicher ist, wer Links in E-Mails nicht klickt und Anhänge aus E-Mails weder herunterlädt noch ausführt. Das gilt ganz besonders in Zeiten, in denen das neuartige Coronavirus immer mehr Menschen zwingt, von zu Hause aus zu arbeiten.

Cyberkriminelle missbrauchen Corona-Angst

So zeigt sich in der laufenden Corona-Krise, dass Cyberkriminelle verstärkt versuchen, die Angst und Unsicherheit rund um das Virus Sars-CoV-2 und die dadurch verursachte Lungenkrankheit Covid-19 zu nutzen, um Menschen zu schnellen Klicks auf fragwürdige E-Mail-Inhalte zu verleiten. Das Phänomen beschränkt sich nicht auf einzelne Regionen, sondern kann weltweit festgestellt werden, so die Sicherheitsexperten von der Tactical Defense Unit * des Software-Herstellers F-Secure.

Wenn Cyberkriminelle E-Mail-Empfänger zum Klicken auf Links oder Downloaden und Ausführen von Anhängen verleiten wollen, kommt es darauf an, diese Empfänger von der Glaubwürdigkeit des Mail-Inhalts zu überzeugen. Das ist nicht neu.

Neu ist die Thematik, mit der eben das nun versucht wird. Dabei konnten die Experten von F-Secure zwei wesentliche Aufhänger identifizieren, die die große Masse an Angriffsversuchen ausmachen: Es handelt sich zum einen um den Missbrauch legitimer Nachrichten und offizieller Warnungen, und zum anderen um angebliche Verkaufsangebote knapper Waren, wie etwa Atemschutzmasken.

Missbrauch legitimer Nachrichten

Die Menschen auf der ganzen Welt sind mindestens verunsichert, wenn es um das neuartige Coronavirus geht. Entsprechend versuchen sie, so viele Informationen wie möglich zu sammeln, um zumindest zu dem Eindruck zu kommen, das persönliche Risiko halbwegs einschätzen zu können.

In dieser emotional aufgeladenen Situationen leidet bisweilen der Sinn für die gewohnte Vorsicht. Das machen sich Cyberkriminelle aktiv zunutze, indem sie suggerieren, die Links in ihren E-Mails würden zu wichtigen, teils offiziellen Informationen leiten, die der Empfänger unbedingt zur Kenntnis nehmen müsste.

Letztlich erreicht der unvorsichtige Klicker nur, dass er vornehmlich mit Malware wie Emotet, Trickbot, Agent Tesla, Formbook, Lokibot oder Remcos RAT konfrontiert wird. Dabei handelt es sich vornehmlich um Malware, die vertrauliche Informationen, etwa per Keylogging, ausspähen will oder den Rechner fürs Krypto-Mining missbraucht. Die noch schwereren Bedrohungen können jedoch ebenso direkten Fernzugriff auf den eigenen Rechner erlangen oder eine Ransomware installieren, die die Daten des eigenen Rechners verschlüsselt und somit unzugänglich macht.

Schutzmasken-Spam

Schutzmasken und verschiedene andere Produkte der desinfizierenden Hygiene sind knapp. Das nutzen Cyberkriminelle aus, um verunsicherte Nutzer schlicht zu betrügen. Wie F-Secure herausfand, häufen sich E-Mails mit entsprechenden Verkaufsangeboten, denen nach Zahlungseingang jedoch kein Versand folgt.

Die Betreffzeilen der E-Mails suggerieren stets, ein neues Produkt oder ein sehr knappes Produkt mit geringem Lagerbestand verfügbar zu haben. Nutzer sollen sich möglichst sofort entscheiden, bevor der Vorrat aufgebraucht ist. Das verleitet offenbar viele Nutzer zum Klick und dem nachfolgenden Kaufvorgang.

Die gute Nachricht

Die gute Nachricht, sozusagen das Glück im Unglück, stellt die Tatsache dar, dass bislang zumindest keine neuen Schadsoftwaretypen aufgetaucht sind. Erfahrene E-Mail-Nutzer können sich mit den bisherigen Strategien auch vor den Corona-Angriffen schützen.

Wichtig ist vor allem eine aktuelle Ausstattung mit einer guten Sicherheits-Software. Unternehmen, die Mitarbeiter ins Homeoffice schicken, ist geraten, den Zugriff auf das Unternehmensnetzwerk in jedem Fall über ein VPN abzuwickeln.

Übrigens: Erst vor wenigen Tagen war ein Angriffsversuch aufgefallen, bei dem Malware in echt wirkenden Karten zur Coronaausbreitung versteckt worden war.

Quelle: https://t3n.de/news/malware-e-mail-angriffe-nehmen-1263952/