Bundesamt
für Sicherheit in der
Informationstechnik

Zunahme von erfolgreichen Cyber-Angriffen mit Emotet – BSI rät zu Schutzmaßnahmen

Ort Bonn
Datum 23.09.2019

Cyber-Angriffe mit der Schadsoftware Emotet haben in den vergangenen Tagen erhebliche Schäden in der deutschen Wirtschaft, aber auch bei Behörden und Organisationen verursacht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt daher erneut eindringlich vor dieser Schadsoftware und gibt ausführliche Hinweise zum Schutz vor Emotet. Auch Privatanwender stehen im Fokus der Angreifer, da Emotet weitere Schadsoftware nachlädt, die zu Angriffen auf das Online-Banking genutzt werden kann.

"Seit rund einer Woche wird Emotet wieder massenhaft versandt und hat binnen weniger Tage für Produktionsausfälle, den Ausfall von Bürgerdiensten in Kommunalverwaltungen und zahlreiche infizierte Netzwerke gesorgt. Man kann es nur gebetsmühlenartig wiederholen: Viele dieser Schäden sind vermeidbar, wenn IT-Sicherheitsmaßnahmen konsequent umgesetzt werden! Dazu zählt u.a. die Sensibilisierung der Belegschaft genauso wie regelmäßige Back-ups oder das Einspielen von Sicherheitsupdates", so BSI-Präsident Arne Schönbohm.

Die aktuellen Spam-Mails zur Verbreitung von Emotet werden wie zuvor mit gefälschten Absendern als vermeintliche Antworten auf tatsächliche E-Mails versendet. Sie enthalten entweder ein schädliches Office-Dokument direkt als Dateianhang oder einen Link, welcher zum Download eines solchen Dokuments führt. Über die in den Dokumenten enthaltenen Makros werden die Opfersysteme mit dem Schadprogramm Emotet infiziert. Insbesondere die in den Spam-Mails enthaltenen Zitate aus einer vorhergehenden E-Mail-Kommunikation mit dem vermeintlichen Absender lassen die bösartigen Mails dabei für viele Empfänger authentisch erscheinen und verleiten sie zum Öffnen der schädlichen Office-Dokumente.

Auf infizierten Systemen späht Emotet die Zugangsdaten für dort konfigurierte E-Mail-Konten sowie den Inhalt der Postfächer aus. Die Zugangsdaten werden anschließend dazu missbraucht, um über die kompromittierten Konten Spam-Mails zur weiteren Verbreitung von Emotet zu versenden. Dabei werden die aus den Postfächern ausgespähten E-Mail-Inhalte verwendet, um maßgeschneiderte vermeintliche Antworten an die Empfänger der Spam-Mails zu erstellen. Den eigentlichen Schaden richten die Täter mit nachgeladener Schadsoftware an. Dies ist meist zunächst ein Banking-Trojaner, der den Tätern Komplettzugriff auf das Netzwerk verschafft, bevor dann manuell bspw. ein Verschlüsselungstrojaner (Ransomware) eingesetzt wird. Dieser verschlüsselt Daten, legt ganze Netzwerke lahm und fordert Lösegeld.

In den vergangenen Tagen hat das BSI mehrere tausend E-Mail-Konten von Unternehmen und Bürgern, die durch eine Infektion mit Emotet kompromittiert und anschließend für den Spam-Versand missbraucht wurden, an die jeweils zuständigen Provider gemeldet. Die Provider wurden gebeten, die betroffenen Konten zu sperren, um einen weiteren Missbrauch für den Spam-Versand zu unterbinden, und ihre Kunden entsprechend zu informieren.

Das BSI hatte Emotet bereits im Dezember 2018 als "weltweit gefährlichste Schadsoftware" bezeichnet und zahlreiche Schutzmaßnahmen empfohlen. Das BSI warnte bereits am 05.12.2018 und 24.04.2019 vor Emotet sowie den damit verbundenen Auswirkungen wie der Verschlüsselung von Daten mittels Ransomware und stellte Empfehlungen zu Schutzmaßnahmen für Unternehmen und Bürger bereit.

Pressekontakt:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn

Telefon: +49 228 99 9582-5777
Telefax: +49 228 99 9582-5455
E-Mail: presse@bsi.bund.de

Vorangegangene BSI-Pressemitteilungen zum Thema:

- Gefährliche Schadsoftware – BSI warnt vor Emotet und empfiehlt Schutzmaßnahmen
- BSI warnt vor gezielten Ransomware-Angriffen auf Unternehmen

Seite teilen
