Schadsoftware "emotet" und was nun?

So arbeitet die Schadsoftware "emotet" und was Sie dagegen tun können.

Die Email sieht aus wie die von einem Kollegen oder wie eine vom Chef.

Doch sie ist gefälscht. Sie enthält ein Schadprogramm, das unter dem Namen „emotet“ bekannt geworden ist.
Die Email wirkt sehr authentisch. Anrede, Absender, Betreff und Signatur sehen korrekt aus, der Text ist in gutem Deutsch verfasst. Das macht sie gefährlich.

Der Empfänger wird zum unbedachten Öffnen des Anhangs verleitet.

Zur Zeit arbeiten viele Menschen im Homeoffice. Das macht diese Form der Spam-Kampangen noch brisanter.

Zum einen ist im Homeoffice ein unbedachter Klick auf den Anhang wahrscheinlicher.

Zum anderen ist die Homeoffice-Umgebung in der Regel nicht so gut abgesichert wie der Arbeitsplatz im Büro.

Ist emotet erst einmal auf dem Rechner, beginnt er unbemerkt sein kriminelles Werk.

Er liest Email-Konten und Email-Inhalte aus. Das ist die Grundlage für seine weitere Verbreitung. Er versucht, sich über das lokale IP-Netzwerk auf andere Systeme auszubreiten. Zusätzlich versucht er, sich in den vorgefundenen WLAN-Netzwerken anzumelden. Dabei setzt er Password-Cracker ein.
Emotet baut eine Verbindung zu seinem Command and Control Server auf und lädt von dort weitere Schadsoftware nach, z.B. um Browser-Aktivitäten zu monitoren und die eingegebenen Passwörter mitzulesen. Die so entstehenden Bedrohungen sind kaum abschätzbar.

Ihre ersten Schritte für mehr Sicherheit:

- Halten Sie Betriebssystem und Anwendungen immer auf dem neuesten Stand.
- Setzten Sie Antiviren-Software ein und aktualisieren Sie diese stets.
- Führen Sie regelmäßige Datensicherungen durch, und zwar mit Hilfe eines eigens dafür eingerichteten Benutzerkontos (Stichwort: Backup-Admin).
- Arbeiten Sie unter einem nicht-privilegierten Benutzerkonto.
- Seien Sie vorsichtig mit Email-Anhängen, besonders wenn es sich um .exe oder Office-Dateien handelt.

(Kurze Frage nebenbei: warum nutzen Sie nicht lieber eine Cloud für die Zusammenarbeit auf

Dokumenten?)

- Monitoren Sie Ihr Netzwerk auf Verbindungen zu den IP's 87.106.37.146 und 45.79.223.161. Diese stehen im Verdacht, zu den Command and Control Servern zu führen.
- Sollten Sie einen Befall mit emotet erkannt haben, hilft es nur, die betroffenen Rechner neu aufzusetzten. Emotet ist dafür bekannt, dass es tiefgreifende und sichterheitsrelevante Änderungen im System vornimmt.

Den ersten Schritten müssen weitere folgen. Der Umfang der Sicherheitsmaßnahmen richtet sich nach der Kritikalität der zu schützenden Geschäftsprozesse, Daten und Systeme.

Gerne berate ich Sie. Mein Ziel ist es, für ein angemessenes Niveau der Informationssicherheit in Ihrem Unternehmen zu sorgen. Das schließt alle Homeoffice-Arbeitsplätze mit ein.

Rufen Sie mich an: 05254 9369420

oder nutzen Sie mein Kontaktformular.