ACHTUNG gefälschte E-Mails im Umlauf

Achtung

• Zur Zeit grassiert der Emotet Trojaner in vielen Unternehmens-Netzwerken. Per Email mit einem Link oder vermeintlichem Word-Dokument im Anhang verbreitet sich dieser Trojaner.

• Die gefälschten Emails sehen täuschend echt aus und erwecken den Eindruck, als würden Sie von einem Freund oder Kollegen kommen.

• Unser Securepoint Antivirus sollte den Emotet in der Regel erkennen. Es kann aber durchaus auch Varianten geben, die noch nicht erkannt werden

Aktuelle Information zur Schadsoftware Emotet

Gefälschte E-Mails im Namen von Freunden, Nachbarn oder Kollegen gefährden im Moment ganze Netzwerke: Emotet gilt als eine der größten Bedrohungen durch Schadsoftware weltweit und verursacht auch in Deutschland aktuell hohe Schäden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in den vergangenen Tagen eine auffällige Häufung an Meldungen erhalten, die im Zusammenhang mit Emotet stehen. Das Schadprogramm wird über Spam-Kampagnen verteilt und stellt eine akute Bedrohung für Unternehmen, Behörden und Privatanwender dar.

Emotet liest die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms. Das funktioniert so: Empfänger erhalten E-Mails mit authentisch aussehenden, jedoch erfundenen Inhalten von Absendern, mit denen sie erst kürzlich in Kontakt standen. Aufgrund der korrekten Angabe der Namen und Mailadressen von Absender und Empfänger in Betreff, Anrede und Signatur wirken diese Nachrichten auf viele authentisch. Deswegen verleiten sie zum unbedachten Öffnen des schädlichen Dateianhangs oder der in der Nachricht enthaltenen URL.

Ist der Computer erst infiziert, lädt Emotet weitere Schadsoftware nach, wie zum Beispiel den Banking-Trojaner Trickbot. Diese Schadprogramme führen zu Datenabfluss oder ermöglichen den Kriminellen die vollständige Kontrolle über das System. In mehreren dem BSI bekannten Fällen hatte dies große Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke neu aufgebaut werden mussten. Für Privatanwender kann eine Infektion den Verlust von Daten, insbesondere wichtiger Zugangsdaten, bedeuten.

Wie Sie sich schützen können:

• Öffnen Sie auch bei vermeintlich bekannten Absendern nur mit Vorsicht Dateianhänge von E-Mails (insbesondere Office-Dokumente) und prüfen Sie in den Nachrichten enthaltene Links, bevor sie diese anklicken.

• Bei einer verdächtigen E-Mail sollten Sie im Zweifelsfall den Absender anrufen und sich nach der Glaubhaftigkeit des Inhaltes erkundigen.

Mehr Infos:

https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html

https://www.heise.de/security/meldung/Achtung-Dynamit-Phishing-Gefaehrliche-Trojaner-Welle-legt-ganze-Firmen-lahm-4241424.html

Eindeutige ID: #1054
Verfasser: Robert Gabriel
Letzte Änderung: 2018-12-06 10:50