Bayerisches Landesamt für
Datenschutzaufsicht

Ansbach, den 18. Dezember 2019

Pressemitteilung

Weihnachtspost vom Hacker –
Warnung vor neuer Emotet-Infektionswelle

Nach den Erkenntnissen des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) infizieren sich derzeit zahlreiche Organisationen mit dem Emotet-Trojaner. Die Malware verursachte bislang bereits einen erheblichen wirtschaftlichen und datenschutzrechtlichen Schaden. Das BayLDA warnt daher alle Verantwortliche – egal ob Unternehmen, Arzt, Handwerker etc. – eindringlich und empfiehlt, besonders aufmerksam bei eingehenden E-Mails zu bleiben. Dies bezieht sich auch auf Weihnachtsgrüße von vermeintlich bekannten Kommunikationspartnern. Links oder Anhänge dürfen nicht sorglos geöffnet werden. Sollte es zu einer Infektion kommen, ist eine Meldung bei der Datenschutzaufsichtsbehörde verpflichtend.

Erklärung: Was ist Emotet?

Bei Emotet handelt es sich um eine Schadsoftware, die aktuell als eine der gefährlichsten Bedrohungen im Internet einzustufen ist. Der Grund dafür ist, dass der Schädling bei einer Infektion neben den E-Mail-Kontakten auch die Kommunikation ausliest und sich dann auf dem E-Mail-Weg weiterverbreitet. Ist Emotet erst einmal in die IT-Systeme eingedrungen, werden andere Schadprogramme nachgeladen. Dazu gehört beispielsweise Malware, die Zugangsdaten ausspäht und den Cyberkriminellen einen Zugriff auf die IT-Infrastruktur gewährt. Außerdem wird so eine weitere Verbreitung im gesamten Netzwerk des Opfers möglich. Oft wird auch ein Verschlüsselungstrojaner nachgeladen, sogenannte Ransomware, der nach einer gewissen Zeit sämtliche Dateien verschlüsselt, um Lösegeld zur Wiederherstellung der Dateien zu erpressen. Emotet verursacht dadurch einen enormen Schaden.

Symptome: Wie erkennt man Emotet?

Der Trojaner ist in der Lage, authentisch aussehende E-Mails zu verschicken. Emotet erlangt die entsprechenden Informationen durch das Auslesen der E-Mail-Korrespondenz. So werden gezielt E-Mails verschickt, die scheinbar von bereits bekannten Kontakten kommen und darüber hinaus auch Auszüge aus einer früheren Kommunikation enthalten. Der Empfänger wird dabei direkt angesprochen. Sprachlich sind solche E-Mails in einem relativ fehlerfreien Deutsch geschrieben.

Ein Erkennungsmerkmal ist, dass im Absenderfeld der Name nicht zur angezeigten E-Mail-Adresse passt. Auffallend ist zudem ein sehr kurzer Text sowie Dateianhänge oder eingefügte Links mit der Aufforderung, diese zu öffnen. Die Schadsoftware verbirgt sich dann entweder im angehängten Dokument oder auf der verlinkten Website. Sollte man im eigenen Posteingang eine solche Nachricht erkennen, ist der angegebene Absender im Idealfall zu informieren. Oft weiß der genannte Kontakt nämlich nicht, dass bei ihm eine Infektion mit Emotet vorliegt und in seinem Namen Schadsoftware per E-Mail verbreitet wird.

Anschrift
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

Telefon +49 (0) 981 180093-0
Telefax +49 (0) 981 180093-800
E-Mail presse@lda.bayern.de
Webseite www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz
oder Bahnhof der Stadt- und
Regionallinien

Prävention: Wie schützt man sich vor Emotet?

Eine wichtige Schutzkomponente vor Emotet-Dateianhängen stellt das Deaktivieren von Makros in Office-Anwendungen dar. Auch sollten alle ohnehin erforderlichen Sicherheitsaspekte im digitalen Umfeld berücksichtigt werden: Installation von Sicherheitsupdates für das Betriebssystem und die Anwendungen, regelmäßige Backups der Daten, Einschränkung von administrativen Benutzerrechten und ggf. zusätzliche Sicherheitssoftware.

Der entscheidende Sicherheitsfaktor bleibt letztendlich der Mensch, d. h. der Anwender, bei dem die Angriffsnachricht eintrifft. Aus diesem Grund ist die Sensibilisierung aller Mitarbeiter für die Verantwortlichen nicht nur im eigenen Interesse sinnvoll, sondern auch eine organisatorische Pflicht. Nur so kann vermieden werden, dass bei vermeintlich bekannten Absendern Dateianhänge sorglos geöffnet oder Links geklickt werden.

Reaktion: Wie verhält man sich bei einer Infektion?

Rechner in Netzwerken müssen zunächst isoliert werden. Es ist davon auszugehen, dass ein infiziertes System vollständig neu aufgesetzt werden muss, damit gewährleistet werden kann, dass alle Schadkomponenten entfernt wurden. Alle bei dem betroffenen System genutzten Zugangsdaten sind im Regelfall zu ändern, da diese abgegriffen werden konnten, z. B. auch die über den Webbrowser verwendeten Passwörter.

Bei einer Emotet-Infektion liegt datenschutzrechtlich gesehen eine Sicherheitsverletzung vor, die nach Art. 33 DS-GVO bei der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden zu melden ist. Bayerische Verantwortliche aus dem nicht-öffentlichen Bereich können ihre Meldung über einen Online-Service beim BayLDA durchführen:

- www.lda.bayern.de/datenschutzverletzung

Um die Ausbreitung von Emotet zu stoppen, ist es wichtig, dass das Umfeld über die eigene Infektion informiert wird. Bestehende Kontakte bzw. Kommunikationspartner werden mit hoher Wahrscheinlichkeit auf Grund der abgegriffenen Daten attackiert und können sich nur durch eine solche Information gezielt auf den personalisierten Angriff vorbereiten. Datenschutzrechtlich besteht nach Art. 34 DS-GVO sogar eine Verpflichtung zur Benachrichtigung der Betroffenen, falls ein hohes Risiko für diese vorliegt – bei einer Emotet-Infektion ist davon auszugehen.

Das BayLDA stellt auf der eigenen Website allgemeine Informationen zum angemessenen Umgang mit Schadcode zur Verfügung und verweist auch auf die Websites des Bundesamts für Sicherheit in der Informationstechnik (BSI):

- www.lda.bayern.de/schadcode
- www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Emotet/emotet.html
- www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/emotet.html

Der Präsident des BayLDA, **Thomas Kranig**, schätzt die aktuelle Gefährdungslage wie folgt ein:

> *„Emotet beschäftigt uns als Datenschutzaufsichtsbehörde zwar schon seit vielen Monaten, derzeit jedoch besonders intensiv. In regelmäßigen Abständen erhalten wir fast schwungartig Meldungen von infizierten Organisationen, bei denen nicht nur der Tagesablauf durcheinandergewirbelt wird, sondern teilweise der ganze Betrieb stillsteht. Egal ob Anwaltskanzlei, Arztpraxis oder Großunternehmen – die Schäden waren bislang meist als gravierend einzustufen. Emotet bedroht also jeden Nutzer, dienstlich wie privat. Leider werden die gefälschten E-Mails und die Angriffsmasche immer besser. Dass die Angreifer jetzt kurz vor Weihnachten den Schädling sogar als Weihnachtsgruß getarnt versenden, mag bei Vielen die Vorfreude auf die Weihnachtszeit trüben. Es bleibt die Hoffnung, dass sich die Schutzmaßnahmen und die Warnung vor Emotet in einem schnelleren Tempo ausbreiten als Emotet selbst."*

Thomas Kranig
Präsident