Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

REGIONALES
RECHENZENTRUM

Direktor

Prof. Dr.-Ing. Stephan Olbrich

25.03.2020

Erhöhte Gefährdungslage durch Schadsoftware Emotet

In den vergangenen Monaten häufen sich die Meldungen über IT-Sicherheitsvorfälle im Zusammenhang mit der Schadsoftware Emotet – auch an deutschen Hochschulen sowie anderen öffentlichen Einrichtungen. Das RRZ betreibt effektive Maßnahmen zum Schutz der IT-Infrastruktur. Ihr bewusster Umgang mit der IT und Ihre volle Aufmerksamkeit sind dennoch notwendig.

Daher bitten wir Sie dringend, die nachfolgenden Informationen und Handlungsempfehlungen zu beachten.

Was macht Emotet?

Emotet liest die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms.

Was bedeutet das?

Empfänger erhalten E-Mails mit authentisch aussehenden, jedoch erfundenen Inhalten von Absendern, mit denen sie zuvor 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 (Bundesamt für Sicherheit in der Informationstechnik) bekannten Fällen hatte dies große Produktionsausfälle zur Folge, da ganze Unternehmensnetzwerke neu aufgebaut werden mussten. Für Sie als Nutzerin bzw. Nutzer der IT-Services der UHH sowie auch als Privatanwender kann eine Infektion den Verlust von Daten, insbesondere wichtiger Zugangsdaten, bedeuten.

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

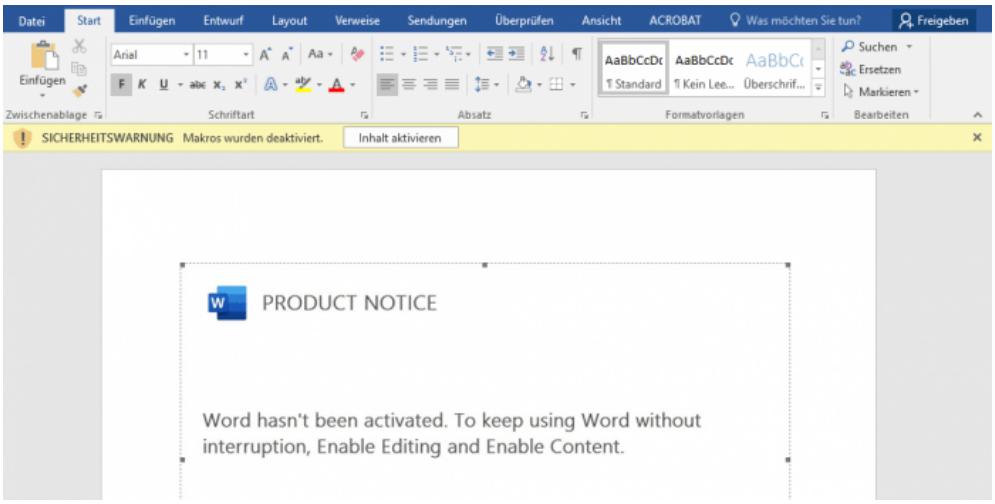
Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt den „3-Sekunden-Check“:

- Kenne ich die E-Mail-Adresse (nicht nur den Anzeigenamen) des Absenders?
- Ist der Betreff sinnvoll?
- Erwarte ich einen Anhang oder einen Link?

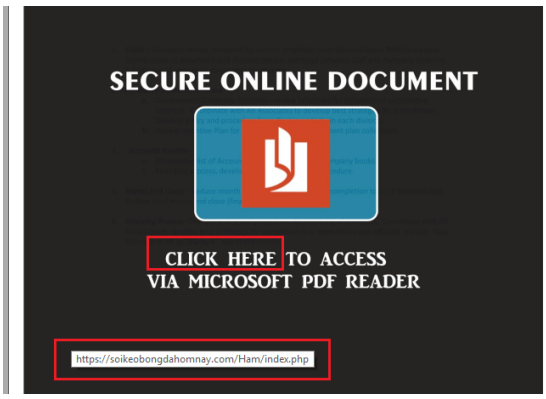
Wie erkenne ich schädliche E-Mails und wie kann ich mich schützen?

Öffnen Sie keinesfalls unvorsichtig Anlagen oder Links in E-Mails und achten Sie auf folgende Details:

- Bitte beachten Sie, dass in Ihrem E-Mail-Programm nicht immer die tatsächliche Absender-Adresse angezeigt wird. Im Text der E-Mail falsch geschriebene Wörter sowie sinnlose Buchstaben- und Zahlenreihenfolgen sind verdächtig. Fragen Sie gegebenenfalls beim vorgeblichen Absender telefonisch nach, ob die Mail von dort versandt wurde.
- Achten Sie besonders darauf, auf welche Webseiten Links in den E-Mails verweisen. Das wirkliche Ziel des Links wird Ihnen im E-Mail-Programm bzw. Web-Browser direkt am Link oder unten links angezeigt, wenn Sie den Mauszeiger über den Link bewegen.
- Öffnen Sie keine Dokumente, welche von Webseiten heruntergeladen werden, die Ihnen nicht bekannt sind.
- Sollten Sie Anhänge von E-Mails öffnen, aktivieren Sie die Bearbeitungs-Funktion erst, wenn Sie zu 100 % sicher sind, dass der Anhang und die Mail authentisch sind. Dasselbe gilt für das Speichern von Anhängen. Seien Sie lieber zu vorsichtig.
- Wenn Sie in einem Dokument aufgefordert werden, den „Inhalt zu aktivieren“ (s. u.), ist dies ein eindeutiges Alarmsignal. Sie sollten dann keinesfalls auf den Knopf „Inhalt aktivieren“ klicken.



- Wenn Sie in einem Dokument (z. B. auch in einer mit einem entsprechenden Viewer angezeigten PDF-Datei, s. u.) aufgefordert werden, einem Link zu folgen, um eine Software zum Lesen herunter zu laden, folgen Sie dieser Aufforderung bitte ebenfalls nicht.



Was mache ich, wenn mein Computer betroffen ist?

- Wenn Ihr Rechner trotz aller Vorsichtsmaßnahmen angegriffen worden ist oder Sie einen entsprechenden Verdacht haben, schalten Sie Ihren Rechner bitte sofort aus und informieren unmittelbar das RRZ. Da Ihr E-Mail-Postfach potenziell durch die Schadsoftware kompromittiert ist, nehmen Sie mit der RRZ-ServiceLine am besten telefonisch Kontakt auf (Tel.: +49 40 42838-7790).
- Lassen Sie bitte Ihr Postfach und Ihre Kennung sperren, um weiteren Missbrauch auszuschließen. Vergeben Sie bitte für sämtliche weiteren Dienste, für die Sie dieselbe Kennung verwenden, neue Passworte. Bitte denken Sie auch daran, nie dasselbe Passwort für verschiedene Dienste – insbesondere im privaten Bereich – zu verwenden.
- Da die Schadsoftware auch personenbezogene Daten überträgt, muss auch der Datenschutzbeauftragte der UHH zeitnah informiert werden, um über eine gemäß der EU-DSGVO gegebenenfalls notwendige Meldung des Vorfalls an die Datenschutzaufsicht fristgerecht entscheiden zu können (E-Mail: datenschutz@uni-hamburg.de).

Bitte beachten Sie auch die aktuellen Sicherheitswarnungen auf den Seiten des RRZ unter https://www.rrz.uni-hamburg.de/ sowie die allgemeinen Informationen zur IT-Sicherheit unter https://www.rrz.uni-hamburg.de/services/sicherheit.html.