Computer-Schädling Emotet zerstört:
Bei Systemreinigung nicht in neue Falle tappen

Die Gefahr kam meistens mit einer E-Mail, die so aussah, als sei sie die Antwort eines bekannten Kontakts. So konnte sich Emotet auf Zehntausende Rechner von Privatpersonen schmuggeln, Online-Banking manipulieren oder Passwörter ausspionieren. Auch Behörden, Krankenhäuser und Unternehmen hatten mit dem Schadprogramm zu kämpfen, denn es legte mitunter komplette Netzwerke lahm. Seit dem 26. Januar 2021 ist damit vorerst Schluss – Ermittlungsbehörden konnten die Infrastruktur des Schädlings zerstören und die international organisierte Cyber-Kriminalität schwächen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) teilt mit, dass Betroffene nun von ihren Internet-Anbietern informiert werden sollen, wenn sich Spuren von Emotet auf ihren Computern und Laptops befinden. „Nehmen Sie diese bitte ernst, bereinigen Sie Ihre Systeme", lautet der Appell der IT-Sicherheitsbehörde und der Verbraucherzentrale NRW. Sie gibt Tipps, woran Verbraucher erkennen, ob E-Mails ihrer Internet-Anbieter echt sind:

- **Stimmt der Absender?** In der Regel schicken Kriminelle die gefälschten E-Mails von Adressen, die überhaupt nichts mit dem Unternehmen zu tun haben. Hinter dem @ sollte der richtige Name des Internet-Anbieters stehen. Im Zweifel sollten sich Kunden bei ihrem Anbieter informieren, mit welcher Adresse er seine E-Mails versendet.
- **Enthält die Begrüßung den Kundennamen?** Werden Empfänger mit einer E-Mail mit ihrem Namen begrüßt, ist das keine Garantie dafür, dass die Mitteilung wirklich vom Unternehmen stammt, nach dem sie aussieht. Allerdings beginnen falsche Nachrichten häufiger unpersönlich als mit den Namen der Empfänger.
- **Gibt es Rechtschreibfehler oder seltsame Begriffe?** Die meisten Betrüger arbeiten international und lassen Texte für ihre E-Mails in etliche Sprachen übersetzen. Dabei kommt es zu Fehlern, die oft ein Indiz für Betrug sind.
- **Sollen Links angeklickt oder Anhänge geöffnet werden?** Das Ziel der meisten Phishing-Mails ist es, dass Empfänger einen Link in der E-Mail öffnen und auf einer

tipp tipp tipp tipp tipp

Frankenwerft 35
50667 Köln

Tel.: (0221) 846 188-88
Fax: (0221) 846 188-33

koeln.quartier@verbraucherzentrale.nrw
www.verbraucherzentrale.nrw

gefälschten Internetseite persönliche Daten angeben. Auch Anhänge, in denen es angeblich weitere Informationen gibt, sind bei Betrügern beliebt. Tatsächlich verbergen sich aber gerade in diesen Anhängen schädliche Programme. Deshalb: Nie auf unbekannte Links klicken oder Anhänge öffnen!

- **Gibt es Zeitdruck?** Ein gängiges Mittel von Phishing-Betrügern ist eine kurze Frist, um überstürzte Handlungen hervorzurufen. Beispiel: „Wenn Sie nicht in den nächsten 48 Stunden reagieren, dann …“ Davon sollte sich aber niemand unter Druck setzen lassen.
- **Nachfragen beim Provider!** Wer über eine Emotet-Infektion informiert wird, sollte sie ernst nehmen, aber nichts überstürzen. Bei Zweifeln daran, dass die Information echt ist, sollten Anwender bei ihrem Internet-Anbieter anrufen oder sich auf der Internetseite ihres Kundenbereichs einloggen. Oft sind auch dort die verschickten E-Mails des Providers gespeichert.

Verdächtige E-Mails können Betroffene weiterleiten an das Phishing-Radar der Verbraucherzentrale NRW. Es ist über phishing@verbraucherzentrale.nrw zu erreichen. Auf www.verbraucherzentrale.nrw/phishing gibt es fast täglich Beispiele aktueller Phishing-Mails sowie grundlegende Informationen zum Schutz vor schädlicher elektronischer Post.

Stand der Information: 28. Januar 2021

Frankenwerft 35
50667 Köln

Tel.: (0221) 846 188-88
Fax: (0221) 846 188-33

koeln.quartier@verbraucherzentrale.nrw
www.verbraucherzentrale.nrw