FAQs aus den sozialen Medien der Ruhr-Universität

Stimmt das Emotet-gerücht?

Es ist noch nicht geklärt, ob es sich um Emotet handelt.

Soll man bis Montag auf Programmzugriffe verzichten?

Aktuell stehen die Dienste RUB-Mail, Moodle, RUBCast, ZOOM, Matrix (Riot) weiterhin zur Verfügung.

Muss ich alle verknüpften Konten und Accounts auf den Geräten aufheben/entfernen?

Über Netzwerk angebundene Laufwerke der RUB sollten getrennt werden. Mailaccounts können nach aktueller Einschätzung erhalten bleiben.

Kann VPN genutzt werden?

Ja, aber Verbindungen zu Netzlaufwerken sollten aktuell nicht aufgebaut werden.

Kann schon ein Schaden entstanden sein, wenn der PC mit dem VPN gestern oder vorgestern verbunden war?

Nach aktuellem Kenntnisstand ist nicht davon auszugehen.

Kann Sciebo genutzt werden?

Ja, Sciebo ist ein Cloud Dienst und dieser ist nicht betroffen.

Kann die RUB-APP genutzt werden?

Ja.

Kann das Programm Finanzinfo genutzt werden?

Nein, dies steht aktuell nicht zur Verfügung.

Ist es sicher, die RUB-Homepage und das Newsportal zu besuchen?

Ja, diese können weiter mit dem Browser besucht werden.

Funktioniert der Login bei Office wegen des Angriffs nicht mehr?

Office365 ist ein Microsoft Cloudprodukt, welches unabhängig von der RUB arbeitet und deshalb aktuell auch nicht betroffen ist.
Für den dienstlichen Gebrauch steht Office365 allerdings aktuell nicht zur Verfügung.

Kann Microsoft Office genutzt werden?

Lokal ist dies möglich. Ein Zugriff auf Netzlaufwerke sollte vermieden werden

Darf man über H.I.R.N zugreifen?

Ja, das Netzwerk kann genutzt werden, aber auch hier sollte keine Anbindung an Netzlaufwerke vorgenommen werden.

Wurden Login ID-Daten geklaut?

Die Analyse steht noch aus.

Sind Dateien auf den Servern/Laufwerken betroffen?

Ja, Serversysteme sind verschlüsselt worden aber nach jetzigem Kenntnisstand sind keine Nutzerdaten betroffen.

Sind Inhalte von Mails und Postfächern gelesen worden?

Dafür gibt es nach jetzigem Analysestand keine Anhaltspunkte.

Sind Webserver betroffen und ist es sicher, sich am jeweiligen CMS anzumelden?

Die von IT.SERVICES betriebenen CMS-Systeme sind nicht betroffen.

Können Linux basierte System auch korrumpiert werden?

Grundsätzlich ja, aber uns ist nach aktuellem Stand kein System bekannt.

Wenn eine Weiterleitung von Rub-Mail eingerichtet wurde, sind dann auch andere Postfächer betroffen?

Nach jetzigem Kenntnisstand sind RUB-Postfächer durch diesen Vorfall nicht betroffen. Trotzdem bekommt die RUB weiterhin Spam- und Phishingmails, die aber von dem Vorfall unabhängig sind. Vorsicht bleibt hier also weiterhin geboten.

User können in moodle sehen, wie viele Personen online sind. soll das so sein?

Hier sehen wir keinen Zusammenhang mit dem Cyberangriff.