Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

RECHENZENTRUM

# Newsletter des Rechenzentrums

# Ausgabe Oktober 2019

Inhalt:

***Wir wünschen allen Lesern einen guten Start ins neue Semester!***

1. **Krypto-Trojaner-Vorfall an der Universität**

In der Nacht vom 23. auf 24. September 2019 wurde die Universität Würzburg von Tausenden eMails geflutet, welche die Nutzer auf ein vermeintliches „eFax“ hingewiesen haben, dass über einen bereitgestellten Link heruntergeladen werden konnte.

Der Link hat dann beim Anklicken allerdings Dateien heruntergeladen, die versucht haben, einen Krypto-Trojaner auf dem jeweiligen Arbeitsplatz zu installieren. **Diese Angriffe waren teilweise erfolgreich.** Nach aktuellem Stand wurden innerhalb kurzer Zeit ca. 50 Rechner mit dem Trojaner infiziert. Bei weiteren 86 Rechnern bestand zumindest kurzzeitig die Vermutung einer Infektion.

Im Rechenzentrum startete daraufhin eine Alarmierungskette, welche aus organisatorischen und technischen Maßnahmen bestand. So wurden zunächst Universitätsleitung, Verwaltung und der Datenschutz über die anlaufenden Gegenmaßnahmen informiert.


**Abbildung 1: Auf dem besten Wege, sich einen Trojaner einzufangen! (Screenshot: RZ)**

Auf der technischen Seite wurden nach Erkennen des Gefahrenpotentials zunächst alle Fileserver, Mailserver und die Backupserver heruntergefahren. Die Firewall wurde der Bedrohungslage entsprechend konfiguriert.

Danach wurden per Twitter, RZ-Homepage und Mailingslisten der Netzverantwortlichen erste Informationen an die Nutzer verteilt und über den Zeitraum mehrerer Tage aktualisiert.

In diversen Treffen der Verantwortlichen im Rechenzentrum wurden weitere Maßnahmen sowie der Wiederanlauf der Systeme nach Beseitigung der Gefahren beschlossen.

Im Laufe des 24.09.2019 wurden schließlich die Mailsysteme wieder hochgefahren, nachdem zuvor die betreffenden Trojanermails aus den Postfächern gelöscht worden waren.

Eine Liste auffällig gewordener Rechner wurde an die Netz- und IT-Verantwortlichen ausgegeben mit der Bitte, diese Rechner vom Netz zu nehmen, sorgfältig zu kontrollieren und dann neu zu installieren.

Im Laufe des 25.09.2019 konnten dann nach und nach alle Netzlaufwerke der Fachbereiche und zentralen Einrichtungen wieder hochgefahren werden. In fünf Bereichen mussten allerdings die Laufwerke wegen bereits verschlüsselter Daten aus dem Backup wiederhergestellt werden!

In den 48 Stunden des akuten Eindringens des Trojaners gab es im IT-Support des Rechenzentrums über 400 Anrufe und ca. 230 Tickets mit Fragen zu den Vorfällen und dem weiteren Verhalten.

Zusammenfassend kann man sagen, dass die Maßnahmen weitgehend gegriffen haben und die Universität nochmal mit einem blauen Auge davongekommen ist. Allerdings gilt es festzuhalten, dass solche Vorfälle **jeder Zeit** wieder auftreten können und zudem der oder die Angreifer nur einen geringen Teil der zur Verfügung stehenden technischen Möglichkeiten ausgenutzt haben.

Der Trojaner war zum Zeitpunkt des Angriffs den üblichen Virenscannern noch unbekannt. Wir haben die Signaturen mittlerweile an einschlägige Sicherheitseinrichtungen wie das DFN-CERT weitergeben.

Das Rechenzentrum wird mit verschiedenen Maßnahmen versuchen, die IT-Sicherheit auf diese neue Bedrohungssituation auszurichten. Eine 100-prozentige Sicherheit in Sachen Viren-, Trojanern- und Phishingangriffen kann aber durch die hochintegrierte und komplexe IT unserer Zeit nicht gegeben werden.

Wichtig für Sie als Nutzer ist daher eine erhöhte und beständige Wachsamkeit, insbesondere das kritische Hinterfragen bei unbekannten Mailabsendern.

In diesem Zusammenhang sei auch wiederholt auf die Regeln und Tipps des Rechenzentrums zur IT-Sicherheit hingewiesen, die nach und nach ergänzt bzw. aktualisiert werden.

https://www.rz.uni-wuerzburg.de/dienste/it-sicherheit/goldene-regeln/

Zum Thema Phishing bietet das Rechenzentrum eine Informationsseite an (auch mit einem Erklärvideo in Englisch):

https://www.rz.uni-wuerzburg.de/dienste/kommunikation/e-mail/spam-und-phishing/"

Wir werden an dieser Stelle zukünftig immer wieder auf notwendige Maßnahmen zur IT-Sicherheit hinweisen. Weitere Informationen zu Krypto-Trojanern erhalten Sie auch hier:

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

## 2. Crypto Trojan incident at the university (English version)

In the night of 23rd to 24th of September 2019, the University of Würzburg was flooded with thousands of e-mails, which pointed out to users an alleged "eFax" that could be downloaded via a link provided.

The link then downloaded files that tried to install a crypto Trojan on the respective workstation. **These attacks were partially successful**. According to the current status, about 50 computers were infected with the Trojan within a short time. With further 86 computers the suspicion of an infection existed at least briefly.

In the computer center an alarm chain was started, which consisted of organizational and technical measures. First, the university management, administration and data protection were informed about the countermeasures being taken.

On the technical side, all file servers, mail servers and backup servers were shut down after identifying the potential danger. The firewall was configured according to the threat situation.

Afterwards, initial information was distributed to the users via Twitter, RZ homepage and mailing lists of the network managers and updated over a period of several days.

In various meetings of the responsible persons in the computer center, further measures as well as the restart of the systems after elimination of the dangers were decided upon.

In the course of 24.09.2019 the mail systems were finally restarted after the Trojan mails had been deleted from the mailboxes.

A list of conspicuous computers was distributed to the network and IT managers with the request to remove these computers from the network, check them carefully and then reinstall them.


**Abbildung 2: On the best way to catch a crypto trojan (Screenshot: RZ)**

In the course of 25.09.2019, all network drives of the departments and central facilities were gradually rebooted. In five areas, however, the drives had to be restored from the backup because the data had already been encrypted!

In the 48 hours of the Trojan's acute intrusion, IT support at the computer centre received over 400 calls and around 230 tickets with questions about the incidents and further behaviour.

In summary, one can say that the measures have largely taken effect and the university has once again escaped with a black eye. However, it should be noted that such incidents **can occur again at any time** and that the attacker or attackers have only exploited a small part of the available technical possibilities.

At the time of the attack, the Trojan was still unknown to the usual virus scanners. We have now forwarded the signatures to relevant security institutions such as DFN-CERT.

The computer centre will take various measures to adjust IT security to this new threat situation. However, 100% security in terms of virus, Trojan and phishing attacks cannot be provided by the highly integrated and complex IT of our time.

It is therefore important for you as a user to have increased and constant vigilance, in particular critical scrutiny by unknown mail senders.

In this context, the rules and tips of the data center on IT security, which are gradually being supplemented and updated, should also be pointed out repeatedly.

https://www.rz.uni-wuerzburg.de/dienste/it-sicherheit/goldene-regeln/

The computer center offers an information page on the subject of phishing (also with an explanatory video in English):

https://www.rz.uni-wuerzburg.de/dienste/kommunikation/e-mail/spam-und-phishing/

At this point, we will repeatedly point out necessary measures for IT security in the future.

(Translated with www.DeepL.com/Translator)

### 3. Support-Ende von Windows 7

Am 14. Januar 2020 endet der Support für das Betriebssystem „Windows 7“. Das bedeutet, das ab diesem Zeitpunkt von Microsoft keine Updates, insbesondere Sicherheitsupdates mehr ausgegeben werden.

Nach aktuellen Recherchen werden noch zahlreiche Windows 7-Systeme an der Universität betrieben!

Bitte denken Sie rechtzeitig daran, die Betriebssysteme Ihrer Arbeitsplätze zu erneuern. Wenden Sie sich im Zweifelsfall an Ihren Netz- und IT-Verantwortlichen für Ihren Bereich.

Stets aktuelle Betriebssysteme sind ein (!) Baustein für höhere IT-Sicherheit, siehe auch **Thema 1** dieser Newsletterausgabe.

### 4. Wussten Sie schon: „Gigamove“ für den Austausch großer Dateien?

Sicher standen Sie auch schon mal vor dem Problem, dass Sie jemandem mal schnell eine Datei schicken wollten, diese aber für eine E-Mail zu groß war? Zwar könnten Sie uni-intern für den Datenaustausch ein Institutslaufwerk verwenden, aber was ist, wenn Sie kein gemeinsames Laufwerk haben oder der Empfänger ein externer Partner ist?

In diesem Fall nutzen Sie doch einfach GigaMove.

Mit GigaMove können Sie komfortabel und schnell größere Dateien anderen Personen über eine sichere Verbindung zur Verfügung stellen. Die max. Größe einer Datei liegt bei 2 GB. Die Empfänger können auch externe Partner sein, d.h. benötigen auch keinen Account unserer Universität.

Und so funktioniert es:

Starten Sie einen Browser und melden sich mit Ihrem JMU-Account bei GigaMove an. Anschließend laden Sie Ihre Datei hoch. Es wird automatisch ein individueller Link

erstellt, den Sie Ihrem Gegenüber z.B. per E-Mail schicken. Über diesen Link kann der Empfänger sich die Datei herunterladen. Nach spätestens 2 Wochen werden die hochgeladenen Daten auf dem Server wieder gelöscht. Umgekehrt können Sie auch eine Datei von Ihrem Partner anfordern, in dem Sie ihm einen Link zum Upload schicken.

Weitere Informationen finden Sie auf unserer RZ-Homepage:

https://www.rz.uni-wuerzburg.de/dienste/zusammenarbeit/gigamove/

## 5. Akademisches Schreiben kompakt am 21.11.2019

Bereits zum vierten Mal findet am 21. November die Kooperationsveranstaltung ASK (Akademisches Schreiben Kompakt) des Rechenzentrums, der UB, dem Schreibzentrum und dem Sportzentrum statt.


**Abbildung 3: "Don't worry with word" (Foto: RZ)**

Die Veranstaltung bietet Studierenden und Doktoranden aller Fächer und Semester zahlreiche Workshops, Kurzvorträge und Beratungen rund ums wissenschaftliche Schreiben. Das Rechenzentrum wird wieder von 10 bis 19 Uhr am großen Infostand die Besucher über das umfangreiche Kurs- und Beratungsangebot des IT-Supports aufklären und insbesondere aufzeigen, welche Soft-Skills man bei den Kursen des Rechenzentrums als Studierender kostenfrei erwerben kann.

Abgerundet wird das Angebot durch den mehrmals präsentierten Vortrag "don't worry with Word", der den Studierenden zeigt, wie man die Seminar-, Master- oder Bachelorarbeit perfekt zu Papier bringt.

## 6. Jahresbericht 2018 ist erschienen

Wir werden häufig gefragt, was eigentlich die Aufgaben eines Rechenzentrums sind. Eine Antwort kann nicht durch einen Satz gegeben werden.

Daher haben wir auch für das Jahr 2018 wieder eine Zusammenfassung unserer Aktivitäten erstellt. Der Jahresbericht 2018 ist diese Woche erschienen und kann über die Seite

https://www.rz.uni-wuerzburg.de/wir/publikationen/

als PDF-Datei heruntergeladen werden.

## 7. Infoveranstaltungen des Rechenzentrums zum Beginn des Wintersemesters

Als Antwort auf diese W-Fragen gibt es in der ersten Semesterwoche die IT-Infotage des Rechenzentrums. Sie richten sich nicht nur an die Erstsemester!


**Abbildung 4: Der Support des Rechenzentrums ist zentrale Anlaufstelle für alle Fragen zu IT-Themen**

Sie wollen mehr erfahren über das Angebot des Rechenzentrums? Sie haben spezielle Fragen?

Denn an diesen Tagen informiert das Rechenzentrum speziell alle Erstsemester über seine Dienstleistungen wie Internet, WLAN, PC-Arbeitsplätze, Drucken, Software, Beratung, Kurse, Schriften und anderes mehr. Wählen Sie einen der Termine vom

**Montag, 14. Oktober bis Donnerstag, 17. Oktober**

**jeweils 13.15 - 14.15 Uhr**

**Raum: 1U29.**

Kommen Sie bequem ohne Anmeldung zu uns in den Seminarraum 1U29! Der Besuch lohnt sich vielleicht auch für Studierende aus höheren Semestern, die einfach etwas mehr über unsere vielfältigen und meist kostenlosen Dienstleistungen erfahren möchten ...

## 8. Das Herbstprogramm für IT-Kurse

Ab sofort steht das neue Herbst-Kursprogramm des Rechenzentrums online. Das RZ-Kurs-Team hat für die Monate Oktober bis Dezember wieder ein vielfältiges Paket an zahlreichen IT-Kursen geschnürt, mit dem die Studierenden oder Mitarbeiter ihre Kenntnisse auffrischen, vertiefen oder völlig neue Erkenntnisse erwerben können.

Nähere Informationen findet man auf der Webseite des Rechenzentrums, im KursShop, im Kurskalender oder bei einem Beratungsgespräch im IT-Support:

https://kursshop.rz.uni-wuerzburg.de

## 9. Tag der Lehre am 20.11.2019

Am Mittwoch, 20.11.2019, findet im zentralen Hörsaalgebäude Z6 ab 12 Uhr der Tag der Lehre statt. Auch das Rechenzentrum ist mit der Vorstellung zahlreicher Dienste sowie einem Infostand vertreten.

Unsere Vorträge und Workshops drehen sich rund um die zentralen Anwendungen WueCampus und CaseTrain sowie die Themen Vorlesungsaufzeichnung, Erklärvideos und Videokonferenzen.

Das Gesamtprogramm wird aktuell noch erstellt und gegen Ende Oktober auf der zugehörigen Webseite verbreitet:

https://www.uni-wuerzburg.de/lehre/tag-der-lehre/programm/

## 10. Neues von WueCampus

Zum Start des Wintersemesters wurde WueCampus auf die neue Moodle-Version 3.7 aktualisiert, es gibt einige sinnvolle Neuerungen, die vor allem zu einer übersichtlicheren Nutzererfahrung beitragen:

- Neuer Block „Zuletzt genutzte Objekte“ auf dem Dashboard
- Kursbeschreibung zum anklicken
- Neues ausklappbares Themenformat - dynamischer Fortschrittsbalken
- Verbesserungen bei den Mitteilungen und Foren
- und noch einiges mehr ...

Die eLearning-Plattform WueCampus ist über folgenden Link zu erreichen:

https://wuecampus2.uni-wuerzburg.de/moodle/

Ende des Newsletters Oktober 2019