Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

RECHENZENTRUM

Newsletter des Rechenzentrums

Ausgabe Dezember 2019

Inhalt:

Wir wünschen allen Lesern Frohe Weihnachten und alles Gute für 2020!

1. Support-Ende für Windows 7 - Umstieg auf Windows 10 erforderlich

Am 14. Januar 2020 beendet Microsoft den Support für das Betriebssystem Windows 7. Aus Sicherheitsgründen ist daher ein Umstieg auf Windows 10 zwingend erforderlich. Wenn Sie also noch einen Windows 7-Arbeitsplatz an der Uni haben, kümmern Sie sich besser jetzt schon um den Umstieg auf Windows 10.

Nach dem Ende von Windows 7 liefert Microsoft keine Updates und Sicherheitsupdates mehr aus. Danach sind die Windows 7-Systeme nicht mehr ausreichend geschützt und stellen eine potentielle Sicherheitslücke sowohl für den Arbeitsplatz als auch für die Infrastruktur der Universität dar.

Wenn Sie noch einen Windows 7- Arbeitsplatz an der Uni haben:

Kümmern Sie sich rechtzeitig - am besten jetzt schon - um eine Windows 10- Installation.

Wenden Sie sich für die Installation oder mögliche Windows-Alternativen an den Netz- und IT-Verantwortlichen in Ihrem Bereich. Informationen und Tipps finden Sie auch hier:

- Infos zur Installation von Windows 10 über ein Image
- Wir bieten Kurse "Windows 10 Praxis" im KursShop an

Bei Fragen wenden Sie sich an den IT-Support.

Stets aktuelle Betriebssysteme sind ein (!) Baustein für höhere IT-Sicherheit, siehe auch **Thema 2** dieser Newsletterausgabe.

2. Der Trojaner-Vorfall und seine Folgen

(aus einBLICK vom 3.12.2019)

Im September 2019 wurden über Nacht tausende von Mails mit einem darin enthaltenen Link an Mitarbeiterinnen und Mitarbeiter der Julius-Maximilians-Universität Würzburg (JMU) verschickt. Wurde dieser Link angeklickt, öffnete sich ein Word-Dokument, welches nach einem weiteren Bestätigungsklick ein sogenanntes Makro ausführte.

Dieses lud Schadsoftware auf den Rechner und verschlüsselte anschließend die lokalen und im Netz verfügbaren Dateiverzeichnisse, darunter persönliche Laufwerke oder Institutslaufwerke.

Matthias Funken, CIO und Leiter des Rechenzentrums der JMU, erklärt im Gespräch, was genau vorgefallen ist und was User mit einem Uni-Account beim Umgang mit ihren E-Mails beachten sollten.

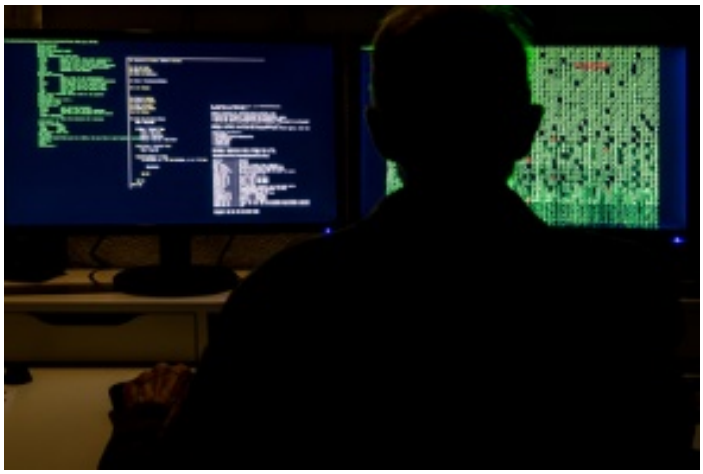

Abbildung 1: Hackerszenario (Foto: Bernd Kasper, pixelio.de)

Herr Funken, der Vorfall im September 2019 war nicht der erste Angriff auf das IT-Netz der Universität. Aber er hatte schwerere Folgen? Ja. Zum einen nimmt die Anzahl der Angriffe auf unsere Universitäts-IT kontinuierlich zu. Zum anderen haben bei diesem Vorfall erstmals in größerem Umfang Mitarbeiter den Trojaner aktiviert, indem sie den Anhang der Mail geöffnet und das darin enthaltene Makro gestartet haben. Die große Herausforderung bei den heutigen Angriffsmustern ist, dass sie dezentral und über den Menschen laufen. Zentrale und rein technische Maßnahmen reichen zum Schutz unserer Infrastruktur und Daten leider nicht mehr aus, was uns dieser Vorfall deutlich gezeigt hat.

Was ist passiert? Der aktivierte Trojaner hinterließ auf den 136 betroffenen Rechnern eine Datei mit dem Namen ‚ALL YOUR FILES ARE ENCRYPTED' in den bereits verschlüsselten Verzeichnissen, der die Nutzer dazu aufforderte, eine der verschlüsselten Dateien an eine spezielle E-Mail-Adresse zu schicken. Die Erpresser entschlüsseln diese Datei im Anschluss zum Beweis, dass sie dazu in der Lage sind. In der Folge wird mit der entschlüsselten Datei eine Lösegeldforderung überstellt, die sich nach der Größe der betroffenen Einrichtung richtet.

Von vergleichbaren Fällen wissen wir, dass eine Universität wie die JMU mit einer Lösegeldforderung im sechsstelligen Bereich zu rechnen hätte. Es stellte sich im Nachgang heraus, dass es sich bei dem Trojaner um eine sogenannte Ransomware (Erpressungstrojaner, Anmerk. d. Red.) namens ‚Buran' handelt.

Wie konnten die Forderungen der Erpresser verhindert werden? Das Rechenzentrum reagierte sofort nach Bekanntwerden der ersten Meldungen aus dem Nutzerkreis. Nach Rücksprache mit Präsidium und Datenschutz fuhren wir die Mail- und Datenserver herunter. Außerdem wurde die Verbindung zum Angreifersystem auf der Firewall der Universität gesperrt und die Datensicherungen sofort gestoppt.

Was wurde dadurch erreicht? Einerseits konnte eine weitere Ausbreitung der Verschlüsselung auf weitere Rechner und auf Netzlaufwerke verhindert werden. Andererseits konnten die betroffenen Rechner relativ schnell neu installiert und durch die Datensicherung des Vortages wieder in einen halbwegs aktuellen Stand gebracht werden. Insgesamt hat die Beseitigung der Folgen allerdings einige Wochen gedauert.

Wie können Mitarbeiterinnen und Mitarbeiter der Uni Gefahren durch Trojaner und Viren im Arbeitsalltag erkennen oder minimieren? Es gibt ein paar einfache Regeln, die man sich in unklaren Fällen immer wieder in Erinnerung rufen muss. Keine zweifelhaften E-Mails bearbeiten und beantworten. Fragen Sie sich, ob Ihnen der der Adressat einer E-Mail bekannt ist.

Seien Sie bei Dateianhängen besonders kritisch. Verwenden Sie Software und Daten aus sicheren Quellen. Verwenden Sie sichere Passwörter. Und natürlich: Geben Sie keine sensiblen Informationen, wie Login und Passwort, preis. Darüber hinaus wird das Rechenzentrum in der nächsten Zeit weitere Maßnahmen einleiten, um Zahl und Auswirkungen solcher Angriffe möglichst gering zu halten.

Das heißt, die Gefahr ist vorüber? Keineswegs. Wir können alle nur versuchen, die Wahrscheinlichkeit erfolgreicher Angriffe zu minimieren. Gänzlich verhindern lassen sie sich bei weiter steigenden Aktivitäten von Erpressern im Netz leider nicht.

3. Erneuerung des Kern-Netzwerks der JMU

Das derzeitige Kernnetz, dass alle Gebäude und Einrichtungen der JMU mit einander verbindet, ist nach über einem Jahrzehnt weitestgehend problemlosen Betriebs nun in die Jahre gekommen. Ein Großteil der Hardware der alten Cisco-Router erhält ab dem kommenden Jahr keinen Support mehr durch den Hersteller.

Auch existieren noch neuralgische Punkte im derzeitigen Netzkonzept, welche durch eine Neuausrichtung beseitigt werden sollen. Über einem Großgeräte-Antrag wurden dazu über eine Ausschreibung neue Router der Firma HPE beschafft, die nun in den kommenden Monaten sukzessive zum Einsatz gebracht werden.

Damit wird das Kernnetz dann folgendermaßen migriert:

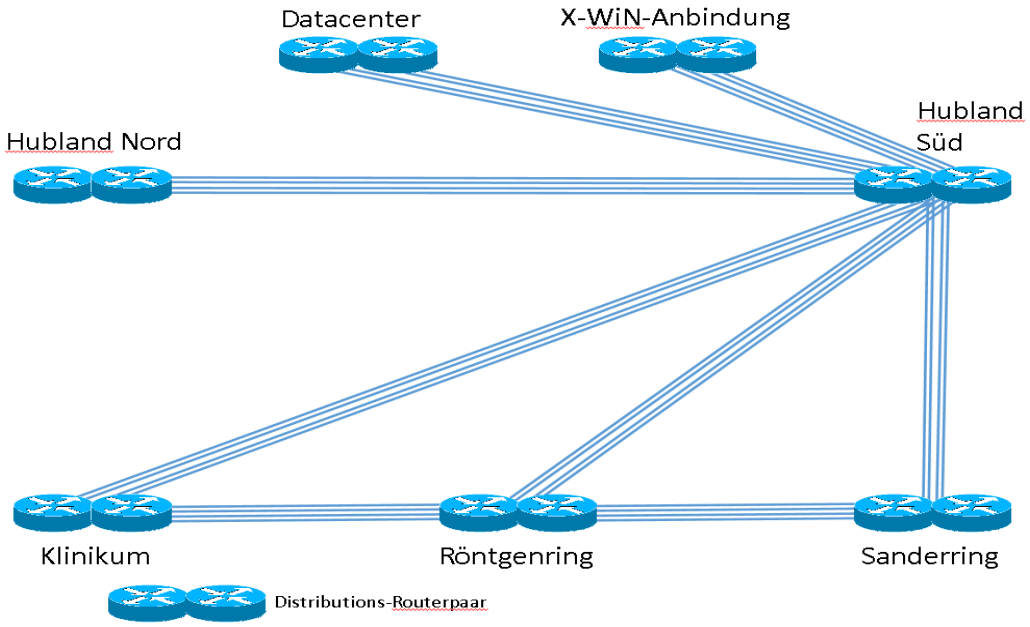

Abbildung 2: Kernnetz vor der Umstellung

Für die Umsetzung müssen dafür in einem ersten Schritt die zentralen Gebäudeswitche in den zentralen Datennetz-Verteilern (diese nannte man früher Übergaberäume) mit ihrer physischen Anbindung in das neue Kernnetz eingearbeitet werden. In einem zweiten Schritt dann wird die Wegfindung (das sogenannte „Routing“) im Netz auf den neuen Core umgestellt.

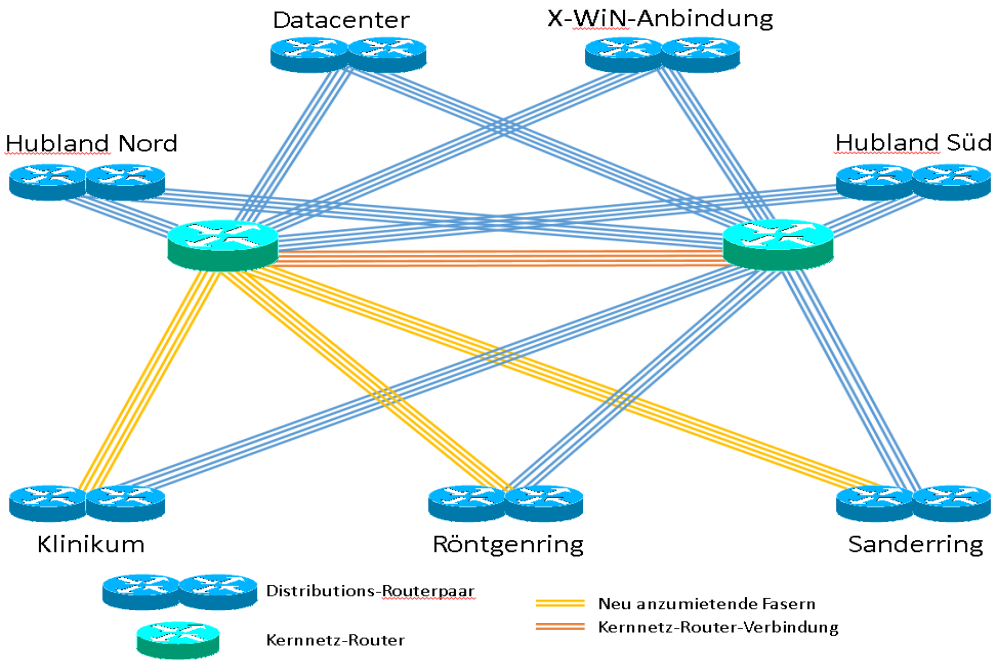

Abbildung 3: Kernnetz nach der Umstellung

Die Netzverantwortlichen in den einzelnen Gebäuden und Bereichen werden dazu jeweils vorher informiert, wobei der erste vorbereitete Schritt nur etwa ein bis zwei

Minuten am früheren Morgen in Anspruch nimmt. Der zweite Vorgang ist sogar in der Regel nicht spürbar ist (Dauer nur ca. eine Sekunde).

Das Rechenzentrum selbst ist diesen Weg bereits gegangen und hat seine Datennetze schon Anfang Dezember ohne Probleme umgezogen.

4. Datensammlung in Windows 10 verhindern

Das Betriebssystem Windows 10 ist nicht frei von Kritik, insbesondere hinsichtlich der Sammlung von Telemetrie- und Diagnosedaten durch die Unternehmensgruppe Microsoft.

Daher einige wichtige Hinweise für den täglichen Betrieb mit Windows 10.

a. Information

Microsoft informiert detailliert über die gesammelten Daten und erklärt Möglichkeiten ein Sammeln zu beschränken unter https://docs.microsoft.com/de-de/windows/privacy/windows-10-and-privacy-compliance

Das Bundesamt für Sicherheit in der Informationstechnikgibt dazu ergänzend einen umfassenden Überblick und Empfehlungen im Rahmen des Projektes SiSyPHuS https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html

b. Zentrales Management

Bitten Sie Ihre Netz- und IT-Verantwortlichen sicherzustellen, dass Ihr Windows 10 Client zentral verwaltet wird. So wird der Datenaustausch mit Servern von Microsoft bereits auf ein Minimum reduziert. Als Level für Diagnosedaten ist bereits das datensparsame "Security" festgelegt.

c. Ihre Kontrollmöglichkeiten

Microsoft ermöglicht Ihnen gesammelte Diagnosedaten einzusehen und zu löschen.

Gehen Sie dazu unter **Einstellungen > Datenschutz > Diagnose- und Feedback**. Dort gibt es die Optionen "**Diagnosedaten anzeigen**" und "**Diagnosedaten löschen**".

d. Nutzung alternativer Programme

Nutzen Sie alternative Programme, etwa für

- Den Browser: Firefox statt Internet Explorer oder Edge
- Schadsoftwareschutz: Sophos EndpointProtection statt Microsoft Defender
- E-Mail-Programme: GroupWise oder Thunderbird statt Mail

- Karten: BayernAtlas https://geoportal.bayern.de/bayernatlas/ und OpenStreetMap https://www.openstreetmap.de/
- Kommunikation: DFNConf https://www.conf.dfn.de/ statt Skype
- Büroanwendungen: LibreOffice statt Microsoft Office
- Grafik: Gimp statt Paint

e. Alternativen zu Windows 10

Sollten Ihnen diese Schutzmaßnahmen nicht ausreichen, sprechen Sie doch mit Ihrem Netz- und IT-Verantwortlichen über Alternativen. In vielen Fachbereichen ist etwa Linux als Betriebssystem im Einsatz. Computer und Notebooks im WebShop unterstützen auch Linux-Betriebssysteme. Ferner können auch Systeme mit MacOS über den WebShop beschafft werden.

5. Umzug Schulungsraum SE05 nach 1U28

Die beiden Schulungsräume im Rechenzentrum haben nun auch räumlich zueinander gefunden. Mussten sich die Teilnehmer bislang noch innerhalb des gesamten Gebäudetrakts nach dem richtigen Raum umschauen, geht das nun recht einfach.

Beide Räume (1U28 und 1U29) liegen nun direkt nebeneinander. Der größere Kursraum 1U29 hat 30 Teilnehmerplätze, der kleinere 1U28 hat 18 Plätze.

Einzig der Mac-Raum, in dem auch gelegentlich Schulungen stattfinden, liegt weiterhin im Übergang zur Physik (SE06).

Abbildung 4: Neuer Schulungsraum für IT-Kurse (Foto: RZ)

6. Personelle Veränderungen im Rechenzentrum

Anfang Dezember haben am Rechenzentrum vier neue Mitarbeiterinnen und Mitarbeiter ihre Arbeit aufgenommen:

- Frau Anne Greßer kümmert sich um das Thema Forschungsdatenmanagement.
- Frau Daniela Oechsner unterstützt den Verwaltungsbereich
- Herr Jens Roesen ist für den Aufbau einer neuen WLAN-Lösung zuständig.
- Herr Matthias Reimund arbeitet beim Thema Webshop mit.

Wir begrüßen alle vier herzlich und wünschen einen guten Einstieg in das jeweilige Betätigungsfeld.

7. Neues aus dem Geräteverleih

Der Geräteverleih des Rechenzentrums wurde – nicht zuletzt Dank der Dr. Herbert-Brause-Stiftung - mit einigen neuen Geräten ausgestattet:

- Mikrofone für das Smartphone
- USB-Aufnahmegeräte
- Weitere Funkmikrofone
- Spiegelreflexkameras
- Lautsprecher für kleine und große Veranstaltungen
- Laptops für den Videoschnitt

Nicht nur das Inventar des Geräteverleihs hat sich erneuert, sondern auch die Anordnung der einzelnen Geräte ist übersichtlicher geworden. Die gesamte Übersicht finden Sie hier:

https://go.uniwue.de/geraeteverleih

Bitte beachten Sie die Öffnungszeiten des Verleihs:

Montag bis Donnerstag	9.00 - 16.30 Uhr
Freitags	9.00 - 13.00 Uhr

8. Neuer Kurskalender für den Start in 2020

Auch für die ersten Monate im neuen Jahr wurde wieder ein attraktives IT-Kursprogramm zusammengestellt. Zusätzlich zu den immer wieder stark nachgefragten Kursen der Office-Palette und Grafik-Kursen bietet das Rechenzentrum im Rahmen der nötigen Umstellung der Arbeitsplatzrechner auf Windows 10 (Siehe auch Thema 1) folgende Kurse an:

Windows 10 Praxis

am ***22.1.2020, 9:00 bis 12:00 Uhr*** oder am ***5.2.2020, 13:00 bis 16:00 Uhr***.

Weitere Informationen mit Beschreibungen zum Kursprogramm finden Sie hier:

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

9. Öffnungszeiten zum Jahreswechsel

Das Rechenzentrum bleibt in der Zeit zwischen Weihnachten und Neujahr – wie die gesamte Universität auch – geschlossen. Die Systeme laufen selbstverständlich weiter.

Ab Donnerstag, den 2. Januar 2020 sind wir wieder für Sie da.

Ende des Newsletters Dezember 2019