Julius-Maximilians-
UNIVERSITÄT
WÜRZBURG

RECHENZENTRUM

Newsletter des Rechenzentrums

Ausgabe Juli 2023

1. Inhalt

Wir wünschen allseits erholsame Sommerferien!

1. WueData – ein neuer Dienst für das wissenschaftliche Arbeiten

Messwerte, Datensätze oder Grafiken - in der Wissenschaft entstehen täglich große Mengen an digitalen Forschungsdaten, aus denen Erkenntnisse gewonnen werden. Dies kann aber nur mit einer guten Organisation der Daten gelingen.

Auch die nationalen und europäischen Forschungsförderorganisationen haben ihre Anforderungen an einen transparenten und nachhaltigen Umgang mit Forschungsdaten in den letzten Jahren sukzessive erhöht. Dazu gehört unter anderem auch, die Daten am Projektende nach den FAIR-Prinzipien abzulegen.

FAIR bedeutet, dass Forschungsdaten auffindbar ("Findable"), zugänglich ("Accessible"), interoperabel ("Interoperable") und nachnutzbar ("Reusable") sein sollen - und das nicht nur für Menschen, sondern auch für Computer.

Seit Mitte Mai 2023 steht daher allen Wissenschaftlerinnen und Wissenschaftlern der Julius-Maximilians-Universität Würzburg das institutionelle Forschungsdaten-repositorium „WueData“ zur Verfügung, in dem sie ihre Forschungsdaten veröffentlichen können. Damit wird auch eine bisher bestehende Angebotslücke geschlossen.

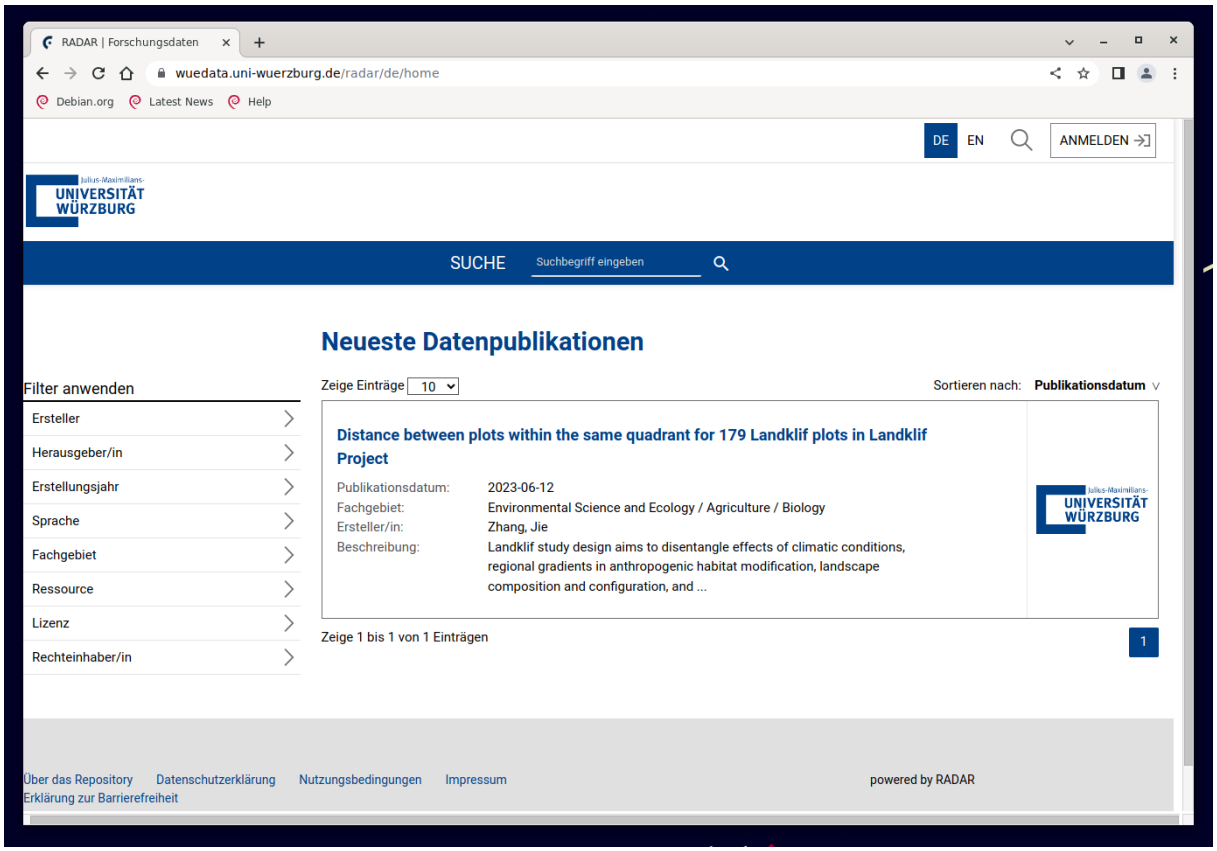

Abbildung 1: Screenshot einer Webseite aus WueData

Denn in etlichen wissenschaftlichen Disziplinen fehlt es bisher noch an fachspezifischen Datenrepositorien, in denen die wissenschaftlichen Daten nach den FAIR-Prinzipien veröffentlicht werden können. Für diese Disziplinen ist WueData als generisches Angebot der Universität eine sichere und vertrauenswürdige Alternative.

WueData ist ein gemeinschaftliches Projekt des Rechenzentrums und der Universitätsbibliothek. So werden die verschiedenen Kompetenzen rund um das Thema Publizieren von Forschungsdaten gebündelt, damit für alle Fragen eine Antwort gefunden werden kann.

Bei Fragen oder wenn Sie Interesse haben, WueData zu nutzen, wenden Sie sich bitte per E-Mail an wuedata@uni-wuerzburg.de.

2. Kollaborations- und Kommunikationsdienste - Nachtrag

In der Aprilausgabe unseres Newsletters haben wir auf eine bevorstehende Übersicht zu allen an der Uni Würzburg zur Verfügung stehenden Kollaborations- und Kommunikationsdiensten hingewiesen. Da zu einzelnen Diensten noch einige datenschutzrechtliche und sicherheitstechnische Fragen zu klären waren, konnten wir die Übersicht noch nicht abschließend zeigen.

Mittlerweile sind jedoch alle Einzelfragen geklärt und so können wir nun alle Dienste nach Kategorien sortiert auf folgender Webseite vorstellen:

Übersicht Kollaborations- und Kommunikationsdienste

3. Der Jahresrückblick 2022 ist online

Was sind die Dienstleistungen des Rechenzentrums? Welche Projekte wurden bearbeitet und fertiggestellt? Was waren bzw. sind neue Themen im IT -Umfeld? Was waren Ziele und Aufgaben? Welche besonderen Ereignisse gab es im vergangenen Jahr? Dies und mehr finden sie in unserer jährlichen Zusammenfassung.

Wir werden immer wieder gefragt, was eigentlich die Hauptaufgaben eines Rechenzentrums sind. Eine einfache und kurze Antwort darauf gibt es natürlich nicht. Daher haben wir auch für das Jahr 2022 wieder eine Zusammenfassung unserer Aktivitäten erstellt sowie auf die Besonderheiten im vergangenen Jahr hingewiesen. "Wissenswertes 2022", so der Titel unserer Jahresübersicht, ist Ende Mai erschienen und kann über die Seite

Webseite mit Publikationen des Rechenzentrums

als PDF-Datei heruntergeladen werden. Über folgenden Link gelangen Sie direkt zum PDF-Dokument: Wissenswertes 2022

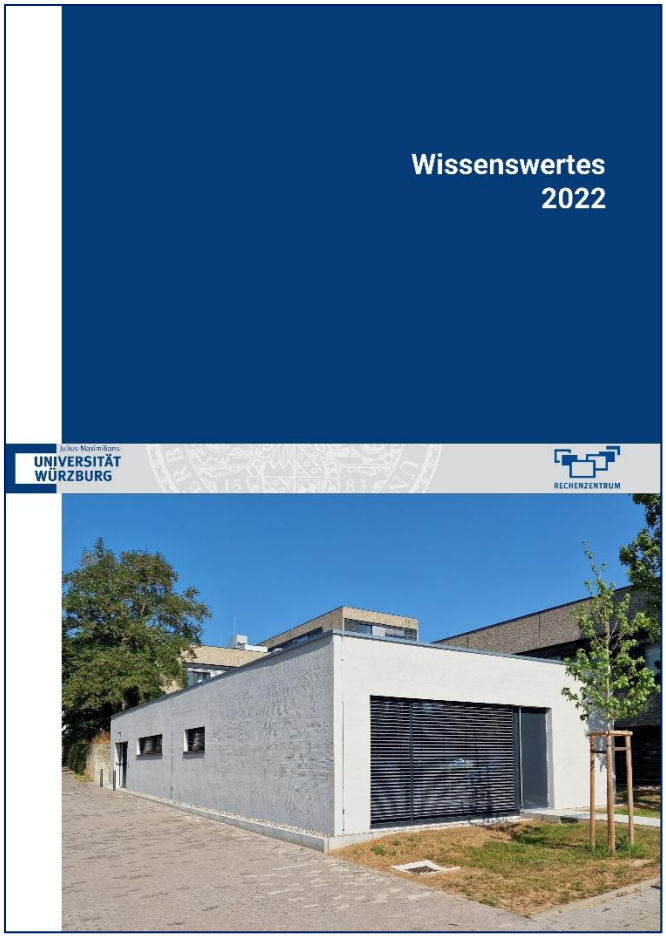

Abbildung 2: Das Cover unseres Jahresrückblicks

4. IT-Schulungen – die Sommerangebote

Auch für die Ferienmonate August und September haben wir auf Wunsch der Studierenden wieder ein attraktives Programm an IT-Kursen zusammengestellt.

Bis zum Semesterbeginn im Herbst werden zahlreiche IT-Schulungen zu Themen wie Excel, Word mit Zielrichtung wissenschaftliches Arbeiten, Photoshop, SPSS, R, HTML, TYPO3 und vieles mehr angeboten. Anmelden können Sie sich über den Kursshop. Die Kurse sind für Studierende komplett kostenlos.

Für viele der Kursthemen finden Sie kostenlose Skripte des Herdt-Verlages. Nach dem Motto „All you can read“ können sich alle Mitglieder der Universität Würzburg kostenlos aus den Skripten des Herdt-Verlags bedienen. Der Zugang erfolgt über https://herdt-campus.com/. Bitte beachten Sie, dass Sie für den Login entweder im

Netzwerk der Universität eingeloggt oder per VPN von außerhalb verbunden sein müssen.

5. Bwsyncandshare – ein neuer Dienst für die Zusammenarbeit

„Bwsyncandshare“ („Bw“ steht dabei nicht für „Bundeswehr“ sondern „Baden-Württemberg“) ist ein Dienst zum Austausch von Daten zwischen verschiedenen eigenen Endgeräten („Sync“) bzw. mit anderen Nutzern („Share“). Die Lösung ist ein DFN-Cloud-Dienst, der durch das Karlsruher Institut für Technologie (KIT) / Steinbuch Centre for Computing (SCC) bereitgestellt wird.

Sie können eine Lizenz im Webshop erwerben. Der besondere Vorteil des Dienstes ist, dass der Austausch von Daten ausschließlich bei einem Anbieter innerhalb des DFN-Verbundes verbleiben (DFN steht für das **D**eutsche **F**orschungs**N**etz) und daher eine aus Datenschutzsicht gute Alternative zu z.B. „Dropbox“ ist.

Zu gegebener Zeit werden wir den aktuell noch parallel laufenden Dienst „Teamdrive“ einstellen. Dazu werden wir rechtzeitig vor der Abschaltung nochmals informieren.

ANMERKUNG. Für die nötige Lizenz des neuen Dienstes wird eine geringe jährliche Gebühr erhoben, nähere Details dazu erfahren Sie im Webshop.

6. Neue IT-Angriffsvariante „Quishing“

Der Begriff Quishing setzt sich aus den Wörtern QR-Code und Phishing zusammen. Dabei werden anstatt Links sogenannte QR-Codes verwendet, um Menschen dazu zu bringen, sensible Informationen preiszugeben oder Malware auf ihre Geräte herunterzuladen. Was kann man tun, um sich zu schützen.

Was ist Quishing?

Quishing ist eine Variante von Phishing, der darauf abzielt, vertrauliche Informationen zu stehlen oder Malware auf das Gerät des Opfers zu übertragen. Die Angreifer erstellen QR-Codes, die das Opfer beim Scannen auf eine Website umleiten, die legitim aussieht, aber in Wirklichkeit dazu dient, Informationen zu stehlen oder Schadsoftware zu installieren.

Wie funktioniert Quishing?

Quishing macht sich das Vertrauen zunutze, das die Menschen in QR-Codes setzen. Viele Menschen gehen davon aus, dass QR-Codes sicher sind und ohne jedes Risiko

gescannt werden können. Angreifer nutzen dieses Vertrauen aus, indem sie QR-Codes erstellen, die zu bösartigen Websites führen.

Hier ist ein Beispiel dafür, wie Quishing funktionieren könnte:

1. Ein Angreifer erstellt einen QR-Code, der so aussieht, als würde er zu einer legitimen Website führen, z. B. zu einer Bank oder einem Online-Händler.
2. Der Angreifer druckt den QR-Code auf einen Aufkleber und platziert ihn an einem öffentlichen Ort, z. B. in einem Vorlesungsgebäude.
3. Ein Opfer sieht den QR-Code und scannt ihn mit der Kamera seines Smartphones.
4. Der QR-Code leitet das Opfer auf eine gefälschte Website um, die wie die legitime aussieht. Das Opfer bemerkt möglicherweise nicht, dass es umgeleitet wurde und gibt seine Anmeldedaten oder andere sensible Informationen ein.
5. Der Angreifer erfasst die Daten des Opfers und verwendet sie für betrügerische Zwecke, z.B. um unberechtigte Einkäufe zu tätigen oder auf das Bankkonto des Opfers zuzugreifen.

Wie Sie sich vor Quishing schützen können

Hier sind einige Tipps, wie Sie sich vor Quishing schützen können:

1. Wenn Sie einen QR-Code an einem öffentlichen Ort sehen, seien Sie vorsichtig, bevor Sie ihn scannen. Fragen Sie sich, ob er legitim aussieht und ob Sie der Quelle vertrauen können.
2. Verwenden Sie einen QR-Code-Scanner, der URLs anzeigt und gegebenenfalls vorher prüft. Einige QR-Code-Scanner verfügen über integrierte URL-Prüfer, die Sie warnen können, wenn eine Website verdächtig aussieht. Vermeiden Sie QR-Code-Scanner, die Sie direkt auf die Seite weiterleiten. Dies tritt bei einigen Smartphone bei der Verwendung der Kamera-Funktion auf.
3. Überprüfen Sie die Website, bevor Sie sensible Daten eingeben. Wenn Sie nach dem Scannen eines QR-Codes auf eine Website weitergeleitet werden, vergewissern Sie sich, dass es sich um eine legitime Website handelt, bevor Sie vertrauliche Daten eingeben. Überprüfen Sie die URL und achten Sie auf Anzeichen für eine sichere Verbindung, wie z. B. das Schlosssymbol in der Browserleiste.
4. Halten Sie Ihre Geräte auf dem neuesten Stand. Stellen Sie sicher, dass auf Ihrem Smartphone und anderen Geräten die neuesten Software-Updates installiert sind. Dies kann dazu beitragen, Sie vor bekannten Sicherheitslücken zu schützen.

Zusammenfassend lässt sich sagen, dass Quishing eine wachsende Bedrohung darstellt, die schwer zu erkennen sein kann. Wenn Sie obige Tipps befolgen, können Sie sich davor schützen, Opfer dieser Art von Cyberangriff zu werden. Denken Sie daran, wachsam zu bleiben und beim Scannen von QR-Codes an öffentlichen Plätzen vorsichtig zu sein.

7. Studentische Hilfskraft gesucht

Das Rechenzentrum ist eine zentrale Einrichtung der Universität Würzburg und sucht ab sofort eine studentische Hilfskraft im Bereich Medientechnik.

Der Bereich Medientechnik kümmert sich um die Ausstattung von fast 500 Seminarräumen und Hörsälen mit Vorlesungs- bzw. Veranstaltungstechnik sowie um den Betrieb verschiedener Tools für die Online-/ Hybridlehre.

Zu den wesentlichen Aufgaben gehören:

- Pflege des Datenbestands der eingesetzten Medientechnik (Open-Source-System).
- Unterstützung bei der Betreuung des Systems "OpenCast" für Vorlesungsaufzeichnung/ Streaming von Videos/ Podcasts.
- Wartung der Medientechnik in Hörsälen/ Seminarräumen.

Anforderungen:

- Hilfreich sind Kenntnisse im IT-Bereich und allgemein in der Medientechnik. Daher sollte die Bewerberin/ der Bewerber auch aus einem IT-nahen Studiengang kommen.
- Kontakt- und Ausdrucksfähigkeit, Teamfähigkeit, Eigeninitiative sowie freundliches und kompetentes Auftreten unseren Kunden gegenüber.

Sie werden von uns in die Aufgaben eingearbeitet. Daher sind wir auch an einer längerfristigen Zusammenarbeit interessiert. Die Festlegung Ihrer Arbeitszeiten (min. 20, max. 40 Stunden) kann nach Absprache flexibel gehandhabt werden.

Wir müssen darauf hinweisen, dass aus tarifrechtlichen Gründen die Beschäftigung nur während eines Bachelor-Studiengangs erfolgen kann.

Wenn Sie in einem netten Team viel Neues über IT-Systeme im Produktiveinsatz und Multimedia-Lösungen ganz praxisnah erlernen wollen, sind Sie bei uns richtig. Bei Interesse senden Sie eine Kurzbewerbung mit Lebenslauf an:

michael.tscherner@uni-wuerzburg.de

8. Sophos geht, Microsoft Defender kommt

Am 20. Juli endet aus technischen Gründen die Versorgung dienstlicher Endgeräte mit den Sophos-Sicherheitstools. Das Rechenzentrum hat allerdings schon einen Nachfolger evaluiert und wird diesen im Juli schrittweise einführen.

Die Sicherung dienstlicher Rechner vor Viren und unerlaubten Zugriff ist wichtig (Foto: Antje Delater/ pixelio.de)

Künftig wird auf dienstlichen Rechnern die Lösung "**Microsoft Defender for Endpoint**" installiert werden und so für den notwendigen Virenschutz sorgen. Diese Änderungen müssen auf allen eingesetzten Arbeitsplatzsystemen vollzogen werden und gehen mit der Deinstallation der alten Sophos-Lösung einher. Für MacOS-Rechner und dienstliche PCs, die "standalone" betrieben werden (also keine Verbindung zu unserer „Active Directory“ haben und keine sogenannten "SCCM-Client" installiert haben), gibt es eine manuelle Lösung, die Sie unter pool@rz.uni-wuerzburg.de erfragen können.

Die IT-Verantwortlichen der jeweiligen Bereiche wurden bereits frühzeitig informiert und werden vom Rechenzentrum mit allen nötigen Informationen versorgt, damit der Schutz der Geräte beim Wechsel der Sicherheitslösung nicht verloren geht. Im Allgemeinen haben Endanwender daher keine Arbeit bei der geplanten Umstellung.

Einzig Linux-Geräte werden vom neuen Schutzmechanismus aktuell noch nicht abgedeckt.

Für alle privaten Geräte gilt zudem, dass es zukünftig keinen von der Dienststelle zur Verfügung gestellten Virenschutz mehr gibt. Am besten aktivieren Sie die jeweils eingebaute Schutzsoftware (Microsoft Defender bzw. macOS XProtect). Für private Rechner können wir jedoch keinen Support leisten.

Alle weiteren Informationen finden Sie auf dieser Themenseite:

https://www.rz.uni-wuerzburg.de/dienste/it-sicherheit/it-arbeitsplatzsicherheit/sophos-anti-virus/sophos-end-of-life/

9. Kennen Sie eigentlich schon **Fragen & Antworten** in Zoom-Meetings?

Die F&A-Funktion ermöglicht, dass Teilnehmende während des laufenden Meetings Fragen stellen können. Diese können Sie anschließend direkt mündlich während des Meetings oder auch schriftlich – wahlweise öffentlich einsehbar oder privat – beantworten.

Die Vorteile gegenüber der Sammlung von Fragen über den Chat:

Die gestellten Fragen können dabei nur von Host und Co-Host gesehen werden. Außerdem können Fragen auf diese Weise übersichtlicher gesammelt, sortiert und abgearbeitet werden.

Möchten Sie das Feature verwenden, müssen Sie dieses bei der Meeting-Planung (über den Zoom-Client oder das Zoom-Webportal) aktivieren.

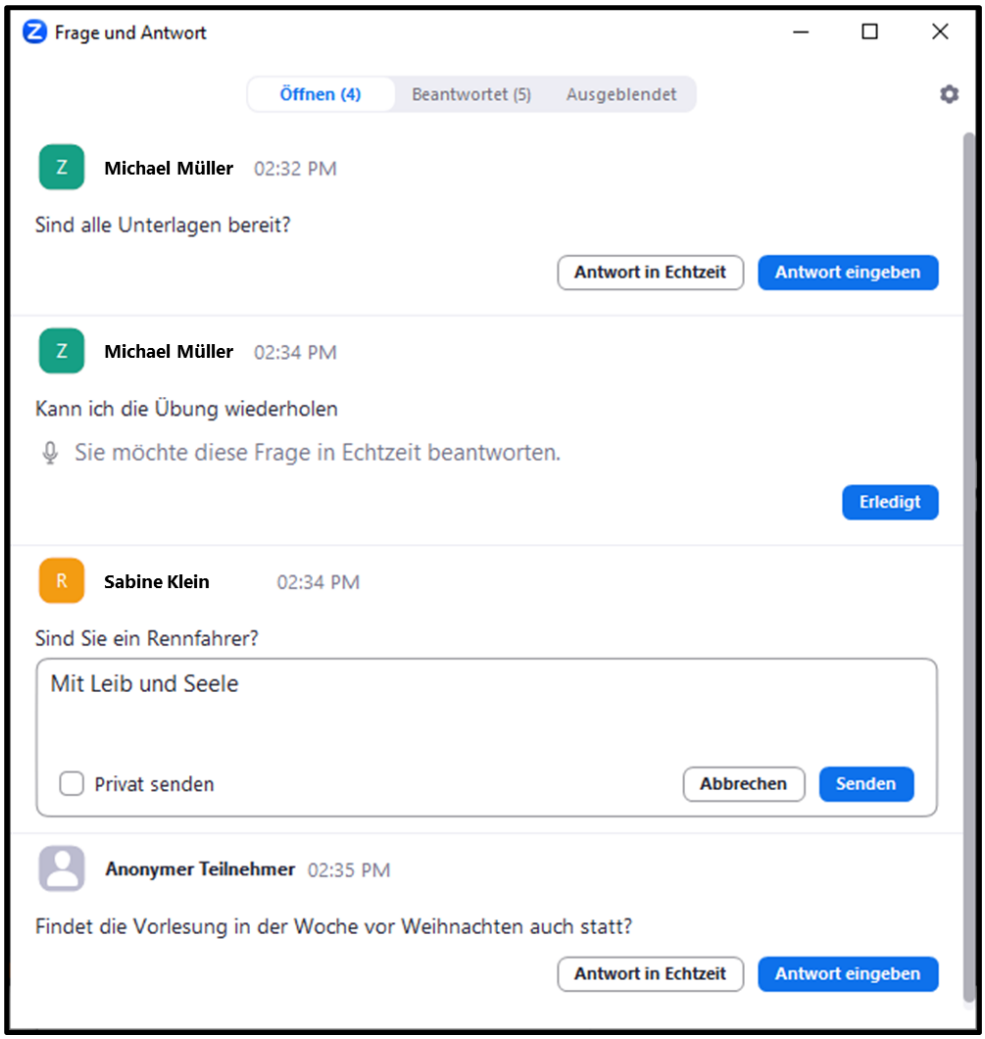

Abbildung 3: Fragen und Antworten während eines Zoom-Meetings

Wählen Sie hierzu einfach „Fragen und Antworten“ bzw. „F&A“ (je nach Version) unter den erweiterten Einstellungen aus. Im Zoom-Meeting ist die Funktion anschließend automatisch aktiv.

Weitere hilfreiche Tipps und Anleitungen zu Zoom finden Sie auch unter

go.uniwue.de/zoom-anleitungen

10. E-Mail-Weiterleitungen nach dem Ausscheiden

Nach Verlassen der Universität wird Ihr bisheriges Benutzerkonto normalerweise nach spätestens sechs Wochen gesperrt. Daher kann es nützlich sein, wenn ehemalige Kollegen in der JMU oder aber auch Kooperationspartner von außerhalb auch weiter in der Lage sind, Sie per Mail zu erreichen.

Da dies über die bisherige Dienstadresse nach 45 Tagen nicht mehr funktioniert, haben wir im User-Portal eine Funktion eingerichtet, mit der Sie eine private oder neue dienstliche Adresse hinterlegen können. Per Autoreply werden dann die Mailabsender informiert, wie Sie zukünftig zu erreichen sind.

Die Einrichtung ist in wenigen Minuten erledigt. Bitte beachten Sie lediglich, dass dieses Autoreply maximal zwei Jahre gültig ist und dann auch nicht verlängert werden kann. Weitere Informationen zu dieser Lösung und zur Einrichtung im User-Portal finden Sie auf dieser Infoseite: Einrichtung Autoreply

Mit der neuen Funktion entfällt auch das bisherige Verfahren der E-Mail-Weiterleitung nach dem Ausscheiden aus dem Dienstverhältnis.

11. IT-Sicherheit im Büro

Die Sicherheit in Büros ist ein entscheidender Aspekt der Informationssicherheit. Hier erfahren Sie, was jeder Einzelne zur Verbesserung der Informationssicherheit am Arbeitsplatz beitragen kann.

Zugriff auf PC sperren

Sperren Sie Ihren PC immer, wenn Sie Ihren Arbeitsplatz verlassen. So stellen Sie sicher, dass niemand auf Ihre Daten oder Ihre Netzwerkressourcen zugreifen kann. Hier sind einige Methoden, die Sie dazu nutzen können:

- Die schnellste und einfachste Möglichkeit, Ihren PC während Ihrer Abwesenheit zu sperren, ist die Verwendung der Tastenkombination "Windows

+ L". Wenn Sie diese Tastenkombination drücken, wird Ihr Windows-PC sofort gesperrt, und Sie werden zur Anmeldeseite weitergeleitet.
Bei iOS verwenden Sie die Tastenkombination “Ctrl + Befehlstaste +Q“

- Sie können zusätzlich den Bildschirmschoner verwenden, um Ihren PC automatisch zu sperren. Stellen Sie sicher, dass der Bildschirmschoner in den Einstellungen so konfiguriert ist, dass er sich nach einer kurzen Zeit der Inaktivität einschaltet und Sie das Passwort bei der Reaktivierung eingeben müssen.

- Bei längerer Abwesenheit sollten Sie Ihren PC ausschalten.

„Cleandesk“

Stellen Sie sicher, dass alle vertraulichen Informationen wie Passwörter, Dokumente und personenbezogene Daten in verschlossenen Schränken oder Schubladen aufbewahrt werden. Lassen Sie am besten gar keine Dokumente oder Notizen offen auf Ihrem Schreibtisch liegen.

Mobile Datenträger

Mobile Datenträger wie USB-Sticks, externe Festplatten, SD-Karten und Smartphones können sehr praktisch sein, um Dateien zu transportieren oder zu sichern. Allerdings bergen sie auch Sicherheitsrisiken, wenn sie verloren gehen oder gestohlen werden. Eine der wichtigsten Maßnahmen zur Sicherung von Daten auf mobilen Datenträgern ist deren Verschlüsselung. Durch eine gute Verschlüsselung stellen sie sicher, dass die Daten auch dann nicht verwendet werden können, wenn der Datenträger verloren geht oder gestohlen wird. Verwenden Sie dazu auf Ihren Windows-PCs z.B. die Software Bitlocker.

Vertrauliche Informationen entsorgen

Beim Entsorgen vertraulicher Informationen ist besondere Vorsicht geboten, um sicherzustellen, dass sie nicht in die falschen Hände geraten. Hier sind einige Tipps dazu:

- Papierdokumente müssen ordnungsgemäß vernichtet und entsorgt werden. Dies kann durch das Zerkleinern der Dokumente in Papier-Shreddern erfolgen. Dies verhindert das Wiederherstellen.

- Elektronische Daten müssen sorgfältig gelöscht werden, bevor Geräte wie Computer, Smartphones oder USB-Sticks entsorgt werden. Verwenden Sie dafür spezielle Programme, die Daten mehrfach überschreiben, so dass alle Informationen vernichtet werden und nicht wiederhergestellt werden können.

Vertrauliche Informationen am Drucker

Drucker können ein Risiko für die Vertraulichkeit von Informationen darstellen, wenn sie nicht richtig genutzt werden. Hier sind einige Tipps, um sicherzustellen, dass vertrauliche Informationen am Drucker geschützt sind:

- Schützen Sie den Zugang zum Drucker
  Stellen Sie sicher, dass der Zugang zum Drucker nur von autorisierten Personen erfolgen kann. Platzieren Sie den Drucker an einem sicheren Ort.
- Löschen Sie die Druckaufträge
  Löschen Sie die Druckaufträge, sobald sie gedruckt wurden, um sicherzustellen, dass sie nicht in falsche Hände geraten. Drucker speichern häufig eine Kopie der gedruckten Dokumente, was ein Risiko für die Vertraulichkeit darstellen kann.

Zusammenfassend lässt sich sagen, dass IT-Sicherheit im Büro ein wichtiger Teil Ihres Arbeitsalltags ist. Mit den oben beschriebenen Maßnahmen können Sie diese deutlich verbessern. Denken Sie daran, dass sicheres Arbeiten im Büro ein fortlaufender Prozess ist. Überprüfen und aktualisieren Sie daher regelmäßig Ihre Sicherheitsrichtlinien und -praktiken.

12. Informationen zur Sicherheits-Behandlung von Mails

Bereits seit einigen Monaten unternehmen wir Anstrengungen, im Bereich des Maileingangs verschiedene Mechanismen zu etablieren, um die Sicherheit für die Nutzenden und für die Authentizität der Mails zu erhöhen. Folgende Maßnahmen stehen dabei im Fokus:

1. **Kennzeichnung externer Mails**

Schon länger werden Mails von extern mit [EXT] gekennzeichnet. Diese Kennzeichnung wird wieder entfernt, wenn die Mail die Uni wieder verlässt, um eine Mehrfachkennzeichnung möglichst zu vermeiden. Dieser Mechanismus wurde nun dahingehend optimiert, dass Mails, die innerhalb der Uni von einem Mailsystem in ein anderes weitergeleitet werden, diese Kennzeichnung nun beibehalten.

Mehrfachkennzeichnungen durch [EXT] können leider nicht ganz vermieden werden, z.B. wenn der Betreff beim Weiterleiten oder Beantworten der Mail so umkodiert wird, dass die Markierung vom Mailsystem nicht mehr erkannt werden kann.

2. **Ablösung des Spamcheck-Dienstes „Puremessage“**

Ab 19.07.2023 werden der Sophos-Virenscanner auf dem Mailrelay und die End-User-Quarantäne „Puremessage“ (spamcheck.uni-wuerzburg.de) entfallen. Der Sophos-

Virenscanner wurde bereits durch den neuen Online-Virencheck „DFN-Mailsupport“ ersetzt.

Ab dem Stichtag werden als Spam erkannte Mails nicht mehr an „Puremessage“ ausgeliefert, sondern entsprechend gekennzeichnet und verpackt an den Benutzer ausgeliefert. (Die End-User-Quarantäne wird dann noch für eine Weile weiterbetrieben, bis alle dort vorgehaltenen Mails herausgealtert sind.)

- Mails, die von extern kommen und als Trojaner eingestuft werden, werden direkt verworfen, ohne den Absender zu informieren (Anmerkung: zurzeit werden Trojaner-Mails, die vom zentralen „Mailgate“ entdeckt werden, noch direkt abgewiesen. Dabei erzeugt der sendende Maildienst in der Regel eine Nichtzustellbarkeits-Benachrichtigung an den Absender).
- Mails, die von extern kommen und als verdächtig eingestuft werden, werden gekennzeichnet und verpackt an den Empfänger ausgeliefert. Für Exchange werden automatisch Regeln gesetzt, die diese Mails in den Junk-Ordner verschieben und nach 30 Tagen löschen. Wenn Sie also den Verdacht haben, eine Mail wurde fälschlicherweise als Spam eingestuft, können Sie sie binnen 30 Tagen selbst aus dem Junk-Ordner holen.
- Mails, die von intern kommen und als Trojaner eingestuft werden, werden verworfen und der Absender wird informiert.

Ende des Newsletters „Juli 2023“

IT-Support des Rechenzentrums

Telefonische Hotline
0931 31-85050 (auch per WhatsApp zu den Öffnungszeiten)

Mailkontakt:
it-support@uni-wuerzburg.de

Öffnungszeiten
Montag -Donnerstag: 9.00 - 16.30
Freitag: 9.00 -13.00

IT-Bereichsmanager
Ihren zuständigen IT-Bereichsmanager finden Sie auf unseren Webseiten.

Impressum

Rechenzentrum der Universität Würzburg
Am Hubland
97074 Würzburg
Deutschland
E-Mail: it-support@uni-wuerzburg.de
Internet: https://www.rz.uni-wuerzburg.de/

Die Universität Würzburg ist eine Körperschaft des Öffentlichen Rechts. Sie wird gesetzlich vertreten durch den Präsidenten Prof. Dr. Paul Pauli.

Das Rechenzentrum der Universität Würzburg ist eine zentrale Einrichtung der Universität Würzburg. Es wird vertreten durch den Leiter Matthias Funken.

Datenschutzbestimmungen
Umsatzsteueridentifikationsnummer DE 134187690
Verantwortlicher für Inhalte in diesem Newsletter gemäß § 55 Abs. 2 RStV: Matthias Funken (Anschrift siehe oben)
Zuständige Aufsichtsbehörde: Bayerisches Staatsministerium für Wissenschaft und Kunst