Basisschutz für dienstliche Windows-PCs

Zusammenfassung

Aktuelle Bedrohungen, Schutz wissenschaftlicher Forschungsergebnisse, Berücksichtigung Datenschutz und -sicherheit, gute wissenschaftliche Praxis

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**
- **Gäste der Friedrich-Schiller-Universität**

Regelungen, Gesetze und Compliance

Nutzerordnung: https://www.hanfried.uni-jena.de/vhbmedia/universitaetsrechenzentrum/regelungen-informationen/nutzerordnung-urz.pdf

Betriebs- und Benutzungsordnung für das Datennetz: https://www.hanfried.uni-jena.de/vhbmedia/universitaetsrechenzentrum/regelungen-informationen/betriebs-und-benutzungsordnung-datennetz.pdf

Informationssicherheitsrichtlinien für die Friedrich-Schiller-Universität Jena: https://www.hanfried.uni-jena.de/vhbmedia/universitaetsrechenzentrum/regelungen-informationen/it-informationssicherheitsleitlinien.pdf

Passwortverwendung und Domainintegration

Passwort

Das Passwort ermöglicht die Authentifizierung der Benutzer an verschiedenen Servern im URZ und in der Verwaltung der FSU. Das Passwort darf nur dem Besitzer der Benutzerkennung bekannt sein, um Missbrauch der Benutzerdaten zu vermeiden. Eine Weitergabe an Dritte verstößt gegen die Benutzungsregelungen.

Wie soll ein Passwort aussehen?

Vermeiden von:

- Namen oder typischen Daten: Namen berühmter Menschen oder Charaktere aus Kino und Fernsehen, Namen von Orten, Kinofilmen, Fernsehshows und -serien, Titel von Liedern, Geburtsdaten, Studienrichtung etc.

- Beispiel-Passwörter aus Hilfetexten oder Formularen
- Einträge aus Wörterbüchern oder Wörter aus irgendeiner Sprache: diese können mit modernen Passwort-Suchprogrammen erkannt werden und erleichtern auch das Erraten der Passwörter.

Verwenden von:

- mindestens acht Zeichen mit mindestens zwei Buchstaben und einer Zahl oder einem Sonderzeichen, sonst besteht die Gefahr, dass es kombinatorisch geknackt werden könnte
- folgende erlaubte Sonderzeichen:
- & ! ? * \ ' $ % : + , - < = # " @ ; > /) (_ [.] { ~ }
- Die Verwendung von Steuerzeichen (z.B. CONTROL-Sequenzen) und Umlauten wird nicht empfohlen, da dies zu unerwünschten Effekten führen kann.

Wie sieht ein gutes Passwort aus?

- eine Buchstaben-Zahlen-Sonderzeichen-Kombination, die als gebräuchlicher Ausdruck nicht vorkommt, die aber über bestimmte Assoziationen leicht zu merken ist
- eine ungewöhnliche Groß- und Kleinschreibung und bewusstes "Falschschreiben"
- das Passwort soll schnell und sicher einzugeben sein, um Mitlesen durch andere Personen bei der Eingabe zu vermeiden
- Passwörter sollten niemals aufgeschrieben (Negativbeispiel: Post-It am Monitor) oder im Rechner gespeichert werden. Falls das Passwort zur Sicherheit doch aufgeschrieben werden soll, muss der Zettel mit dem aufgeschriebenen Passwort wie z.B. einen Bankautomatcode behandelt werden, der anderen Personen nicht zugänglich sein soll.

Trotz aller Vorsichtsmaßnahmen wird ein regelmäßiger Wechsel des Passwortes, mindestens einmal monatlich, empfohlen. Zu beachten ist, dass neue Passwörter sich mindestens um vier Zeichen von den jeweils letzten fünf vergebenen Passwörtern unterscheiden müssen und dass in der Vergangenheit genutzte Passwörter nicht noch einmal verwendet werden können. Alle Passwörter, die Ihnen vom Systemadministrator zugewiesen werden, müssen sofort geändert werden!

Weitere Informationen findet man unter Sicherheit / Software.

Domainintegration

Die Integration des Windows-PCs in die FSU-Domäne wird vom Rechenzentrum empfohlen und bietet verschiedene Vorteile:

- Login über Uni-Kürzel
- automatische Einrichtung von Outlook
- ZUFS Home-Laufwerk wird automatisch eingebunden
- wichtige Sicherheitseinstellungen per Gruppenrichtlinie

Die Integration muss durch einen Administrator durchgeführt werden, welcher die entsprechende Berechtigung besitzt. Ansprechpartner ist der Administrator der zuständigen Einrichtung.

Gruppenrichtlinien

Gruppenrichtlinien stellen die einfachste Möglichkeit dar, Computer- und Benutzereinstellungen in Netzwerken, die auf einer Windows Domäne basieren, zu konfigurieren. Die mithilfe von Gruppenrichtlinien definierten Richtlinieneinstellungen werden unter Windows erzwungen. In den meisten Fällen wird die Benutzeroberfläche dieser Einstellungen deaktiviert. Da Gruppenrichtlinieneinstellungen unter Windows an sicheren Orten in der Registrierung gespeichert werden, können Standardbenutzerkonten diese Einstellungen außerdem nicht ändern. Durch das einmalige Ansprechen einer Einstellung kann diese Einstellung also auf vielen Computern konfiguriert und erzwungen werden. Wenn eine Einstellung für einen Computer oder Benutzer nicht mehr zutrifft, wird die Richtlinieneinstellung durch die Gruppenrichtlinie entfernt. Die ursprüngliche Einstellung wird wiederhergestellt und die zugehörige Benutzeroberfläche wieder aktiviert.

Windows 10 Konfiguration

Windows 10 bei Ersteinrichtung

Die folgenden Schritte gelten nur für eine Neuinstallation von Windows 10 Enterprise. Nach einem Produktupdate oder bei Anpassung eines bestehenden Windows 10-Systems startet man bei "Windows 10 konfigurieren".
Am Ende der Installation bzw. beim ersten Start eines neuen PCs wird die Ersteinrichtung von Windows 10 geladen. Hier wirbt Windows 10 mit "Schnell einsteigen" und "Express-Einstellungen verwenden".
Hiervon nicht unter Druck setzen lassen und nehmen sich die Zeit nehmen, selbst zu entscheiden, welche Daten an Microsoft gesendet werden. Deshalb "Einstellungen anpassen" auswählen. Deaktivieren von allen Einstellungen, um eine Weitergabe von Daten an Microsoft zu verhindern.

Nach diesen Einstellungen wird von Windows 10 "Wem gehört dieser PC?" gefragt. Hier "Meiner Firma" auswählen und mit "Weiter" bestätigen.
Im nächsten Schritt soll die "Art der Verbindung" ausgewählt werden. "Einer Domäne beitreten" anklicken.
Anschließend ein lokales Benutzerkonto angeben. Bitte beachten, dass nicht das Universitätskürzel als Namen angegeben wird. Es kann sonst nach einem Beitritt zur Domäne zu Fehlern beim Anmelden kommen.
Die Passwortrichtlinie muss berücksichtigt werden.

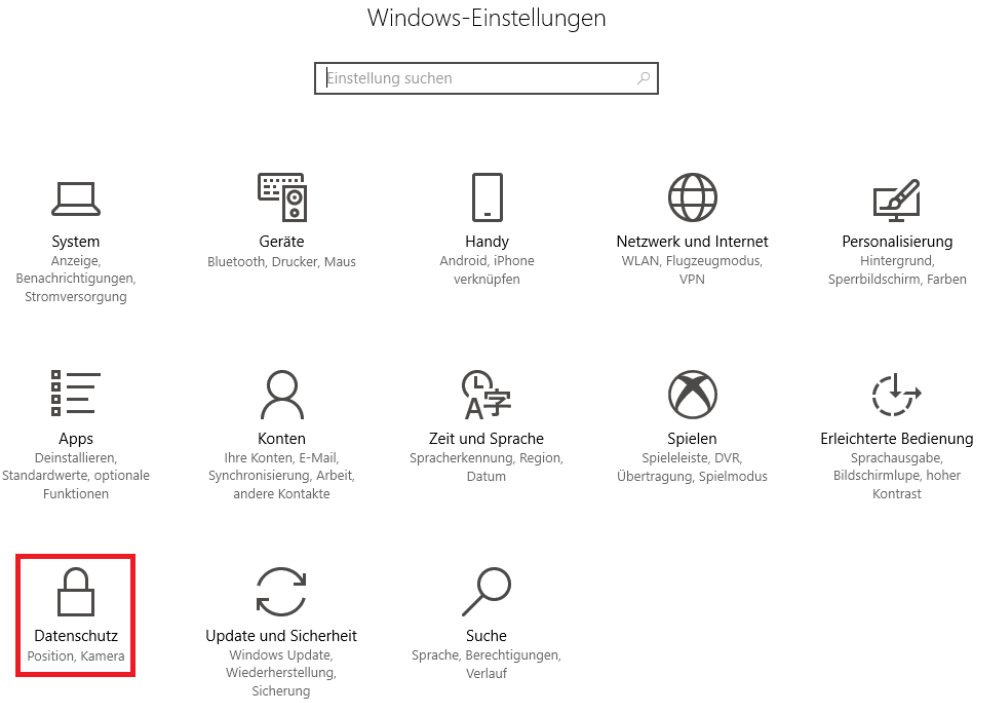
Windows 10 konfigurieren

Leider deaktiviert Windows 10 damit nur einen Teil der vielen Einstellungen, welche zur Identifizierung und Lösung von Problemen, zur Verbesserung der Dienste und Produkte und zur Personalisierung des Systems an Microsoft gesendet werden. Leider können diese nicht vollständig abgeschaltet werden. Daher muss daher durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass diese Daten nicht an Microsoft übertragen werden. Daher sind nach der Installation noch weitere Schritte nötig. Sollte Windows 10 bereits installiert sein, können hier auch nachträglich die Einstellungen der Ersteinrichtung geändert werden.

Konfiguration - Datenschutz

Wenn der PC in die Domäne integriert ist, werden die folgenden Einstellungen durch die Gruppenrichtlinien realisiert.

Im Startmenü auf "Einstellungen" klicken. In den PC Einstellungen auf die Seite "Datenschutz" gehen.



In den Datenschutzeinstellungen jeden Punkt genau durchklicken und alle Optionen, welche nicht explizit benötigen werden, deaktivieren. Bei Fragen an die Stabstelle Sicherheit informationstechnischer Systeme wenden.

Konfiguration - WLAN

Unter "Einstellungen" "Netzwerk und Internet" "WLAN" muss "WLAN-Dienste zu öffentlichen Hotspots" deaktiviert werden. Öffentliche Hotspots sind meist nur ungenügend gesichert und ermöglichen ein Abfangen des Datenverkehrs.

Windows zurücksetzen

Windows 10 bietet die Möglichkeit, das System wieder auf den Ursprungszustand zurückzusetzen. Unter "Einstellungen" "Updates und Sicherheit" "Wiederherstellung", dann auf "Diesen PC zurücksetzen" "Los geht's" gehen.
Hier hat man die Wahl zwischen "Eigene Dateien beibehalten" oder "Alles entfernen".
"Eigene Dateien beibehalten" entfernt nur Einstellungen und Programme, lässt die persönlichen Dateien jedoch auf dem PC.
"Alles entfernen" entfernt alle Einstellungen, Programme und Dateien vom PC.

Datenablage auf zentralen Fileserver oder Cloud der Universität

Zentraler Fileserver

Das Universitätsrechenzentrum stellt für Mitarbeiter und Studierende zentralen, sicheren und wiederherstellbaren Speicherplatz als persönlichen Arbeitsbereich zur Verfügung. Studierenden stehen 3 GB und Mitarbeitern 5 GB zur Verfügung. Durch das Ablegen von Daten auf einem zentralen Speicherplatz ist ein Zugriff von unterschiedlichen Geräten aus möglich:

- Über PCs im universitätsweiten Datennetz (z. B. in Büroräumen, PC-Pools)

- Mobil über Notebooks im universitätsweiten WLAN
- Außerhalb des universitätsweiten Datennetzes ist ein Zugriff über VPN (Virtual Privat Network) möglich.

Wenn sich der PC in der FSU-Domäne befindet, wird das Homeverzeichnis bereits als Netzlaufwerk angezeigt.

Weitere Informationen: persönlicher Speicherplatz (zentrales Home-Verzeichnis).

Das URZ bietet für ein gemeinsames Arbeiten innerhalb von Projekten oder Arbeitsgruppen zentralen, sicheren und wiederherstellbaren Speicherplatz in Form eines Projektverzeichnisses an. Die Größe des Speicherplatzes richtet sich nach der Größe der Einrichtung und muss mit dem zuständigen Anschlussverantwortlichen abgesprochen werden. Bei Bedarf ist eine Speicherplatzerhöhung über die maximal vorgesehene Größe zu beantragen. Eine Erhöhung ist kostenpflichtig.

Die abgelegten Daten werden stündlich via Snapshots gesichert und vier Wochen aufbewahrt. Man kann somit selbständig über Windows eine Vorgängerversion wiederherstellen.

Weitere Informationen: Speicherplatz für Arbeitsgruppen und Projekte (Projektverzeichnis).

FSU-Cloud

Als Mitarbeiter oder Emeriti der FSU Jena kann man mit der FSU-Cloud einen Online-Speicherdienst nutzen, der es ermöglicht, auf Daten von verschiedenen Rechnern und mobilen Endgeräten aus zuzugreifen bzw. Daten zwischen diesen auszutauschen. Man kann auf die in der Cloud abgelegten Daten von unterwegs einfach über einen Web-Browser oder mittels einer speziellen Client-Software zugreifen. Die Daten können zum Beispiel auch mit Forschungspartnern geteilt bzw. an Studierende weitergereicht werden (Sync & Share).

Mit dem Web-Browser erreicht ma den FSU IT-Dienst unter folgender Adresse: https://cloud.uni-jena.de

Die Daten werden außer auf den angeschlossenen Endgeräten nur im Universitätsrechenzentrum der FSU gespeichert.

In der FSU-Cloud ist ausschließlich das Speichern und Teilen von Daten aus Forschung, Lehre, Studium und Verwaltung gestattet. Es ist zu beachten, dass die FSU-Cloud nicht das hauptsächlich genutzte Arbeitsverzeichnis ersetzt und kein Archiv darstellt! Es wird darauf hingewiesen, dass lediglich Kopien in der Cloud (insbesondere im angelegten Synchronisationsverzeichnis des Cloud-Clients) abgelegt werden sollten. Die Originaldaten sollten zusätzlich lokal im Homeverzeichnis bzw. in dem zentral angebotenen Homeverzeichnis (ZUFS) des URZ gespeichert werden!

Weitere Informationen: FSU-Cloud.

Softwarebezug und Sicherheitsprogramme

Softwarebeschaffung

Studierende, Mitarbeiter, Institute und Einrichtungen können zu günstigen Konditionen und teilweise auch kostenfrei Software über das URZ beziehen. Es werden einige Softwareprodukte für die Nutzung auf privaten Arbeitsplätzen angeboten. Die meisten Angebote gelten aber ausschließlich für den dienstlichen Gebrauch innerhalb der FSU Jena.

Die Softwarebeschaffung bietet für jede/n Mitarbeiter/in und Einrichtungen der FSU Software aus Campus- und Landesverträgen an. Zur Bestellung von Software, welche nicht in den Campus- und Landesverträgen enthalten ist, das Bestellformular unter Kauf-Software verwenden. Durch abgeschlossene Rahmenverträge mit einzelnen Firmen gibt es die Möglichkeit, Produkte zu günstigeren Preisen zu erwerben. Gerne kann man sich vor einer Bestellung bei der Softwareabteilung nach Produkten und Preisen erkundigen.

Sicherheitsprogramme

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Sophos ist eine Software mit weitergehenden Schutzfunktionen (Anti-Spyware, Anti-RootKit, Anti-Phishing etc.). Diese Software muss permanent aktualisiert und richtig konfiguriert sein.

Das URZ stellt für alle Angehörigen (MitarbeiterInnen und StudentInnen) der Universität den Virenscanner von Sophos zur Verfügung. Dieser Virenscanner sollte auf allen Rechnern der Hochschule eingesetzt werden. Der Sophos-Virenscanner darf von allen NutzerInnen auch auf privaten Rechnern eingesetzt werden, solange man Angehörige/r der Hochschule sind. Es steht eine vorkonfiguriertes Standardinstallationspaket der Universität Jena zur Verfügung. Nach der Installation dieses Paketes sind keine weiteren Anpassungen notwendig, um einen wirksamen Schutz zu erhalten.

Datensicherung / Backup

Datensicherung

Es wird empfohlen, wichtige Daten auf dem Homeverzeichnis (ZUFS) des URZ zu speichern. Die abgelegten Daten werden stündlich via Snapshots gesichert und vier Wochen aufbewahrt. Man kann somit selbständig über Windows eine Vorgängerversion wiederherstellen.

Server-Backup

Das Universitätsrechenzentrum bietet Ihnen die Möglichkeit, die Server der Einrichtung in das zentrale Backup-System der FSU einzubinden. Dadurch werden die Daten des Servers in regelmäßigen Abständen gesichert und können bei Verlust wieder eingespielt werden. Es ist jedoch nicht möglich, einen Rechner komplett wiederherzustellen, da ausschließlich die Nutzerdaten gespeichert werden. Bitte beachten, dass Arbeitsplatzrechner nur in Ausnahmefällen in das Backup-System einbezogen werden können.

Ansprechpartner bei Problemen und Vorfällen

Anschlussverantwortlicher

Die Anschlussverantwortlichen sind kompetente Ansprechpartner für alle Nutzer des Computernetzes der Einrichtung bezüglich aller Fragen der Netzanschlüsse und der Zuverlässigkeit des Universitätsnetzes und seiner Dienste sowie des Internets. Durch ihre Kenntnisse vor Ort, bsw. der räumlichen Gegebenheiten, der Zugangsmöglichkeiten, insbesondere zu den Serverräumen, tragen sie wesentlich dazu bei, die Arbeit über das Netz allen Mitarbeitern entsprechend ihren Wünschen zu ermöglichen und eine hohe Verfügbarkeit zu gewährleisten. Auf Grund ihrer lokalen Kenntnisse, auch hinsichtlich spezieller Software innerhalb des Wissenschaftsbereiches, sind sie erste Ansprechpartner für die Nutzer bei Problemen. Außerdem sind die Anschlussverantwortlichen umfassend über alle Arbeiten am Netz, z. B. planmäßige Wartungsarbeiten, Neuanschluss und Umrüstung von Netzkomponenten und Software-Upgrades informiert.

Den/die Ansprechpartner/in der Einrichtung findet man hier: Liste der Anschlussverantwortlichen

IT-Servicezentrum

Das IT-Servicezentrum hilft bei Fragen gern weiter. Fragen zum UniNetz oder der angebotenen Software und Hardware, zum UniAccount oder z.B. wie man sich mit dem WLAN verbindet oder einen Sicherheitsvorfall meldet, beantwortet das IT-Servicezentrum am Ernst-Abbe-Platz 4.

IT-Servicezentrum:

Ernst-Abbe-Platz 4 / Raum 1209
07743 Jena
(03641) 9-404777
itservice@uni-jena.de

Informationsbeschaffung / Vertiefung

URZ Dienste

Betriebs- und Benutzungsordnung Datennetz

Nutzerordnung

IT Informationssicherheitsleitlinien

Autor: Hannes Günthe

Titel: "Basisschutz für dienstliche Windows-PCs"

Stand: 21.02.2023

FRIEDRICH-SCHILLER-
UNIVERSITÄT
JENA