Checkliste "Sicherer PC"

Zusammenfassung

Es besteht **immer die Gefahr von unbefugten Zugriffen auf Daten von außen** (Hacker, Spyware), von innen durch Beschäftigte und Gefahren durch höhere Gewalt wie etwa Feuer, Wasser usw.

Eine vollständige Sicherheit wird es nie geben. **Deshalb sollte man aus den zahlreichen Möglichkeiten der Lösungen diejenigen auswählen, welche optimale Sicherheit bieten**.

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**
- **alle sonstigen Zwecke**

1. Betriebssystem und Rechte

Die Schutzfunktionen des Betriebssystems und seiner Komponenten nutzen:

Diese sind z.B.:

- Personal Firewalls
- Anti-Spyware-Programme (z.B. Windows-Defender)
- Phishing-Filter (im IE 9: SmartScreen-Filter)
- eingeschränkte Benutzerrechte (inklusive der Benutzerkontensteuerung/ UAC - User Account Control in Windows Vista/ 7)

Im Windows-Wartungscenter werden Firewall-Einstellungen, Windows Updates, Einstellungen für Anti-Malware-Software, die Internetsicherheit und Einstellungen für die Steuerung der Accounts verwaltet.
Im Wartungscenter werden außerdem Einstellungen für die Computerwartung überwacht und Links zu Problembehandlungen sowie anderen Tools bereitgestellt, die Ihnen bei der Beseitigung von Problemen helfen können. (Quelle: Microsoft)

Diese Schutzfunktionen sollen nicht deaktiviert werden.

Die tägliche Arbeit sollte lokal nicht mit administrativen Rechten ausgeführt, sondern mit eingeschränkten Rechten der Accounts. Die Accounts können mit verschiedenen Rechten versehen werden.
Administrative Rechte benötigt man nur, um Konfigurationen vorzunehmen oder zu ändern.

Viele Schadprogramme werden erst wirksam, wenn mit administrative Rechten gearbeitet wird, dann verfügt auch dieser Angreifer über administrative Rechte.

2. Virenscanner

Der Schutz des Rechners vor Schadsoftware (Viren, Würmer usw.) erfolgt durch die Verwendung eines Virenscanners bzw. einer Software mit weitergehenden Schutzfunktionen (Anti-Spyware, Anti-RootKit, Anti-Phishing etc.). Diese Software muss permanent aktualisiert und richtig konfiguriert sein.

Es soll überprüft werden, ob folgende Einstellungen aktiv sind:

- Zugriffsscan
- mindestens wöchentlicher vollständiger Scan des Systems
- mindestens einmal täglich ein automatisches Update ausführen

Die ST-SIS - Stabsstelle für Sicherheit informationstechnischer Systeme des URZ stellt für alle Angehörigen (Mitarbeitende und Studierende) 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 die Person Angehörige/r der Hochschule ist.

Es steht ein vorkonfiguriertes Standard-Installationspaket der Universität Jena in Verantwortung der ST-SIS - Stabsstelle für Sicherheit informationstechnischer Systeme zur Verfügung.
Nach der Installation dieses Paketes sind keine weiteren Anpassungen notwendig, um einen wirksamen Schutz zu erhalten.

Immer nur einen einzigen Virenscanner auf dem Rechner installieren! Mehrere Virenscanner können sich gegenseitig negativ beeinflussen.

3. Patches und Updates

Das System stets aktuell halten, verfügbare Updates zeitnah einspielen.

Entdeckte Schwachstellen in Software-Produkten und bestimmten Hardware-Komponenten müssen schnell behoben werden, damit sie nicht durch potentielle Angreifer ausgenutzt werden können. Es ist es sehr wichtig, dass zwischen der Veröffentlichung der Patches und Updates der Hersteller und der Aktualisierung der Software der geringstmögliche zeitliche Abstand liegt.
Auch für Treiber werden Updates herausgegeben. Deshalb gelten dafür die gleichen Maßnahmen wie für das Betriebssystem und die Applikationen. Oft wird ein automatischer Update-Services angeboten.

Für die **Aktualisierung von Windows Betriebssystemen** stellt das URZ der Uni Jena einen zentralen Service von Microsoft bereit, mit dem alle angeschlossenen Rechner über das Uni-Netz mit neuen Updates versorgt werden können.

4. Passwörter

Der Zugriff auf den Rechner muss durch ein sicheres Passwort geschützt werden. Hinweise zum Generieren eines sicheren Passwortes und dem korrekten Umgang mit Passwörtern finden Sie **hier**. Es ist ein Login für das Verwaltungshandbuch HanFRIED notwendig.

Das Speichern von Passworten darf niemals unverschlüsselt auf dem Rechner erfolgen.
Alle Benutzerkonten auf dem Rechner müssen mit einem sicheren Passwort versehen sein.

5. E-Mail-Programme und Browser

Grundsätzlich soll keine Software ausgeführt werden, die als Anhang einer E-Mail zugesandt wird. Anhänge mit doppelten Datei-Extensions wie "test.pdf. exe" enthalten mit hoher Wahrscheinlichkeit schadhaften Code.

E-Mails mit der Aufforderung zur Installation von Software und/oder zur Übermittlung von Passwörtern, Kreditkartennummern, PINs, TANs etc. niemals beachten und sofort löschen.

Nicht auf E-Mails mit unerwünschtem oder zweifelhaftem Inhalt antworten oder abbestellen. Mit der Rückantwort erfährt der Absender, dass die Adresse gültig ist. Diese E-Mails sollten gelöscht oder und/oder als SPAM gekennzeichnet werden.

Unerwarteten E-Mails und insbesondere ihren Dateianhängen sollte man misstrauen. Wenn man von bekannten Absendern eine E-Mail erhält, die "nur" eine befremdliche Betreffzeile enthält, sollte man trotzdem vorsichtig sein. Sicherheitshalber beim angeblichen Absender nachfragen. Virenbefallene E-Mails täuschen in der Regel vertraute Absenderadressen vor. Nach Möglichkeit sollte die HTML-Ansicht von E-Mails deaktiviert und stattdessen die Textansicht genutzt werden. Das Fälschen von E-Mail-Absenderadressen ist relativ einfach möglich.

Angebliche E-Mails vom URZ: Unsere E-Mails sind immer in verständlicher deutscher Sprache verfasst und niemals anonym. Sie tragen immer den Namen des Verfassenden als Unterschrift. Niemals wird dazu in E-Mails/Rundschreiben aufgefordert, das Passwort anzugeben.

Ein Virenscanner sollte immer installiert sein. Viren, Würmer und Trojaner verbreiten sich häufig über E-Mail-Anhänge oder aktive Inhalte von Webseiten.

Das Deaktivieren der automatischen Anzeige bzw. das Ausführen von E-Mail-Anhängen im E-Mail-Programm wird empfohlen. Sicherheitsregeln sollten im Mailprogramm eingeschaltet werden (z.B. Outlook: Datei- Optionen - Outlook-Optionen - Sicherheitscenter: Automatische Download, Datenausführungsverhinderungsmodus aktivieren usw.).

Das automatische Ausführen aktiver Inhalte im Browser sollte abgeschaltet oder eingeschränkt werden (z.B. IE: Extras- Internetoptionen - Sicherheit - Stufe anpassen - Scripte deaktivieren; im Firefox: mittels noscript-Addon oder Extras- Einstellungen - Sicherheit oder Inhalt).

Die Kommunikation per E-Mail ist heute Standard. Für eine sichere Kommunikation müssen E-Mails mit einem Zertifikat verschlüsselt werden, damit Unbefugte diese nicht lesen können.

Informationen dazu -> hier .

Generelle Hinweise vom BSI:

Bei E-Mails auch von vermeintlich bekannten bzw. vertrauenswürdigen Absendern prüfen, ob der Text der Nachricht auch zum/zur AbsenderIn passt (englischer Text von deutschem Standort, zweifelhafter Text oder fehlender Bezug zu konkreten Vorgängen etc.) und ob die Anlage (Attachment) auch erwartet wurde.

Das BSI empfiehlt, den Versand/Empfang von ausführbaren Programmen (Extend .COM, .EXE, .BAT, ...) oder anderer Dateien, die Programmcode enthalten können (Extend .DO*; XL*, PPT, VBS...) vorher telefonisch abzustimmen. Dadurch wird abgesichert, dass die Datei vom angegebenen Absender geschickt und nicht von einem Virus verbreitet wird." (Quelle: BSI)

Der Einsatz eines Alternativbrowsers anstelle des Internet Explorers, stellt heutzutage nicht mehr generell einen Sicherheitsgewinn dar. Entscheidend ist die Verwendung der aktuellen Version, was beim Internet Explorer durch die Integration in das Automatische Update bei Windows-Systemen standardmäßig umgesetzt ist. Der Einsatz eines veralteten Alternativbrowsers gegenüber einem aktuellen Internet Explorer muss als potentielles Sicherheitsrisiko gesehen werden.

Die Sicherheit des Browsers lässt sich durch die Umsetzung der im Browsercheck beschriebenen Maßnahmen und den Einsatz von Plug-Ins, die die automatische Ausführung aktiver Inhalte verhindern, wie NoScript und Flash Block (jeweils für Firefox/Seamonkey) erhöhen. Einen zusätzlichen (wenn auch niemals 100%igen) Schutz kann der Einsatz von Plug-Ins bieten, die vor (potentiell) gefährlichen Webseiten warnen, wie WOT (Web of Trust) oder der SiteAdvisor von McAfee.

6. Software

Software aus nicht vertrauenswürdigen Quellen enthält häufig Schadsoftware. Diese Schadsoftware wird oft aktiv, ohne dass der Nutzer/die Nutzerin davon Kenntnis hat.
Deshalb sollte man ausschließlich Originalsoftware nutzen und diese möglichst direkt von der Herstellerfirma bzw. von einer vertrauenswürdigen Quelle beziehen. Für dienstliche Zwecke ist das URZ-Rechenzentrum ein kompetenter Kontakt.

Möglichst nur wirklich benötigte Software installieren.

> **Bitte beachten!**
>
> Häufig werden gerade kostenlose Programme mit Plugins und Programmen anderer Hersteller gekoppelt, d.h. diese werden bei einer Standardinstallation meist ungewollt mit installiert. Hier empfiehlt sich die benutzerdefinierte Installationsmethode mit der Möglichkeit der gezielten Auswahl der zu installierenden Software.

Auf angebliche Schutzprogramme, die oft kostenlos angeboten werden und die die Sicherheit des eigenen Systems erheblich beeinträchtigen können, sollte man verzichten und nur die Anwendungsprogramme usw., die wirklich benötigt werden, sollten installiert werden. Damit wird die Pflege und der Überblick über das eigene System erheblich erleichtert. Das nachträgliche Abschalten/ Entfernen von Diensten in Windows ist für nicht versierte Nutzer immer problematisch und führt in den meisten Fällen zu fehlerhaften Funktionsweisen.

7. Aktualität und Vorsicht

Persönliche Maßnahmen:

Für einen wirksamen Schutz ist es wichtig, informiert und sensibilisiert zu sein. Dann ist man in der Lage, die Situation realistisch zu beurteilen, passend zu reagieren und Probleme aus Unkenntnis auszuschalten.

Das Informationsangebot des URZ oder weiterer einschlägiger Quellen sollte genutzt werden. Wichtig ist es, sich zu informieren und Schulungen zu besuchen.

Man sollte sich immer aktiv abzumelden, wenn man auf einer Website eingeloggt war. Das gilt ganz besonders an öffentlichen Rechnern, z.B. in Hotels oder in Internet-Cafés. Ein Schließen der Seite ist nicht ausreichend.

Misstrauen ist hilfreich, wenn man wegen eines (vermeintlichen) Problems kontaktiert wird, um sensible Daten, wie Passwörter oder Konfigurationseinstellungen zu erfahren. Die IT-Verantwortlichen der Universität Jena fragen solche Informationen nie ab.

8. Zugriffsschutz

Der Rechner sollte nicht unbeobachtet gelassen werden, wenn man angemeldet ist. Man kann sich ausloggen, den Zugriff sperren oder einen Bildschirmschoner mit sicherem Passwort aktivieren, wenn der Arbeitsplatz verlassen wird - auch wenn es sich nur um eine vermeintlich kurze Zeitspanne handelt. Wird der Arbeitsplatz für längere Zeit verlassen, sollte der Rechner ausgeschaltet werden.

9. Datensicherung

Während oder nach Angriffen auf den PC können diese Aktionen zu Datenverlusten führen oder diese verändern oder zerstören. Aus diesem Grund ist es sehr wichtig, dass Daten regelmäßig gesichert werden.
Man sollte sich aber bewusst sein, dass durch das Umsetzen der beschriebenen Maßnahmen und der damit verbundenen Erhöhung der Datensicherheit ein 100%iger Schutz nie garantiert werden kann.

Wichtige Daten sollten auf Netzlaufwerken gespeichert oder eine zusätzliche lokale Sicherung durchgeführt werden. Außerdem sollte man das lokale Backup möglichst auch auf beweglichen Datenträgern sichern.

Ein Programm mit Erinnerungsfunktion kann in regelmäßigen Abständen an eine Datensicherung erinnern.

Checkliste zum Ausdrucken und Abhaken

außerdem:

Methoden zum sicheren Löschen von Dateien

Mit Windows gelöschte Daten sind nicht unwiederbringlich gelöscht!

Unbefugte können nicht nur digitale Bilder, private und geschäftlichen Daten wiederherstellen, durch Surfen im Internet hinterlässt man ebenfalls Spuren, durch die auf Vorlieben, den zeitlichen Zugriff auf Websites und auf Downloads Rückschlüsse gezogen werden können.

Das Bundesamt für Sicherheit in der Informationstechnik Informationen zusammengestellt.

Titel: "Checkliste "Sicherer PC""

Stand: 05..10.2021