Checkliste IT-Sicherheit und Datenschutz

im Homeoffice für Studierende und Mitarbeitende der Universität Potsdam

[Stand: 03.12.2020]

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument soll Ihnen einen kurzen Überblick zu den Themen Datenschutz und Datensicherheit für das Arbeiten im Homeoffice geben. Auch finden Sie eine 10-Punkte Checkliste zur Prüfung Ihrer Geräte und Arbeitsweise im Homeoffice. Auf der letzten Seite im Dokument sind weiterführende Internetadressen zum Thema hinterlegt.

2 Hinweise zur Datenverarbeitung

Die Universität Potsdam bietet generell eine Vielzahl von Online-Diensten, welche Mitarbeitende und Studierende bei der Arbeit von Zuhause aus unterstützt. Die meisten Dienste sind mit Ihrem UP-Account über das Internet verfügbar. Einige Dienste können ausschließlich mit Hilfe eines Virtual Private Network (SSL VPN) genutzt werden.

Die aktuelle Entwicklung, aufgrund der Covid19-Pandemie, erfordert die technischen Voraussetzungen für die Arbeit im Homeoffice in möglichst breiter Fläche zu schaffen. Damit ist der Zugriff auf diverse interne Ressourcen über das Internet verbunden und somit erhöht sich auch die Angriffsfläche für Malware (bösartige Software).

Beim Abruf Ihrer dienstlichen Daten über einen **privaten** Computer mittels E-Mail-Programm (Outlook, Thunderbird) oder dem Dateibrowser (Box.UP, File Box, sFTP) werden dienstliche Daten auf private Computer kopiert. Diese Daten sind so auch dann verfügbar, wenn der Computer nicht mit dem Uni-Netz verbunden ist.

Das ZIM muss diesbezüglich darauf hinweisen, dass diese Systemnutzung abhängig vom Zustand des Computersystems sehr risikobehaftet und daher unerwünscht ist. Nutzen Sie alternativ den Zugriff über den **Web-Browser**.

Achtung(!): Sollten sich in Ihren dienstlichen Dateien auch personenbezogene Daten befinden, ist die Nutzung ausschließlich mit dienstlichen Geräten gestattet.

Auch ohne technische Hilfsmittel besteht die Gefahr, dass Dritte Einsicht in die Daten mobiler Geräte nehmen. Dritte können beispielsweise in öffentlichen Bereichen bei ungünstiger Sitzposition den Bildschirminhalt mitlesen. Gestalten Sie daher Ihren Arbeitsplatz so, dass eine Einsicht anderen Personen nicht möglich ist. Sofern der Arbeitsplatz verlassen wird, sollte das Gerät immer gesperrt werden.

Mit persönlichen **Passwörtern** ist genauso umzugehen wie z.B. mit der PIN einer Bankkarte. Das heißt **kein hinterlegen am PC-Arbeitsplatz** (z.B. Passwort mit Haftzettel an den Monitor, Tastatur, Locher, etc. kleben) und **keine Weitergabe an Dritte**, auch nicht aus Gefälligkeit. Eine Weitergabe der Login-Daten hat zur Folge, dass diverse Schutzmaßnahmen unwirksam werden.

3 Was können Sie tun? Wie können Sie betragen?

3.1 Allgemein

Verfolgen Sie die aktuellen Meldungen und Sicherheitshinweise auf den ZIM Webseiten unter: https://www.uni-potsdam.de/de/zim/neues-stoerungen.

Prüfen Sie anhand der im Dokument angefügten Checklisten, wie Sie Ihre IT Systeme und Arbeitsweise im Homeoffice sicherer gestalten können.

Abbildung 1 ZIM Störungswebseite

3.2 Konkret

Meldung aller Vorfälle und Auffälligkeiten am Computer an das ZIM. Leiten Sie bspw. verdächtige E-Mails an **zim-service@uni-potsdam.de** weiter. Ergänzen Sie bspw. den Betreff mit „Verdächtige Mail“ oder ähnlichen Formulierungen.

3.3 Meldepflicht beim Datenschutz (DSB)

Bitte beachten Sie, dass bei sicherheitsrelevanten Vorfällen mit persönlichen Daten eine Meldung an die zuständige Aufsichtsbehörde nötig sein kann. Um diese innerhalb der gesetzlich vorgegebenen Frist von 72 Stunden zu ermöglichen, füllen Sie im Verlustfall bitte zeitnah das im Intranet abrufbare Formular zur Meldung von Verletzungen des Schutzes personenbezogener Daten aus und senden es an datenschutz@uni-potsdam.de.

4 Computer der zentralen Universitätsverwaltung

Die Computer der Verwaltung (ZUV) werden durch das ZIM zentral administriert. Dadurch werden sehr viele der hier genannten Maßnahmen bereits übergreifend umgesetzt. Sie müssen keine Änderungen an den Systemen vornehmen. Handeln Sie weiter stets sorgsam und prüfen nur die Geräte, welche Sie zusätzlich im Homeoffice verwenden.

4.1 Festplattenverschlüsselung

Um das Risiko der Verletzung von Datenschutzrechten im Falle des Verlustes eines dienstlichen Laptops oder vergleichbarer Sachverhalte zu minimieren, besteht die Notwendigkeit, die Festplatten der mobilen dienstlichen Geräte zu verschlüsseln um durch diese Maßnahme unbefugtem Zugriff vorzubeugen.

5 UP Checkliste IT-Sicherheit und Datenschutz

Vor dem Hintergrund der permanent steigenden Gefahr durch Computerviren, ist es nunmehr besonders wichtig, dass sich **Jede und Jeder** auch über die persönliche Verantwortung bewusst ist. Technische Sicherheitsmaßnahmen sind alleine nicht mehr ausreichend.

Daher: handeln Sie bitte stets sorgsam!

Wikipedia beschreibt das Thema **Datenschutz** wie folgt: „*...wird Datenschutz als Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung, Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch Schutz der Privatsphäre verstanden*. (..) *Der Datenschutz soll der in der zunehmend digitalen und vernetzten Informationsgesellschaft bestehenden Tendenz zum sogenannten gläsernen Menschen, dem Ausufern staatlicher Überwachungsmaßnahmen und der Entstehung von Datenmonopolen von Privatunternehmen entgegenwirken*.“ [Quelle: Wikipedia vom 08.01.2021]

Wikipedia beschreibt das Thema **IT-Sicherheit** wie folgt „*..als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden und -lagernden (technischen oder nicht-technischen) Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken*.“ [Quelle: Wikipedia vom 08.01.2021]

5.1 CHECKLISTE DATENSCHUTZ

Finden Sie hier den Verweis zur aktuellen Datenschutzbestimmungen für den Heimarbeitsplatz. Auch enthalten moderne Betriebssysteme **viele neue Funktionen**, **die bezüglich des Datenschutzes kritisch gesehen werden müssen**. Bspw. werden unter Microsoft Windows 10 in der Standardkonfiguration zahlreiche personenbezogene Daten (u.a. über das Surfverhalten sowie die Nutzung der Spracherkennungssoftware Cortana) gesammelt und an Microsoft Server weitergegeben. Prüfen Sie daher, ob das von Ihnen verwendete Betriebssystem in Bezug auf Datenschutz optimiert oder sogar angepasst werden muss.

Prüfung	Was	Bereich	Lösung
Hinweis	**Datenschutz**	**Datenschutz-Beauftragte/-r**	Informieren Sie sich regelmäßig über die Datenschutzbestimmungen auf den Intranet Seiten des DSB zu aktuellen Rechten und Pflichten am Heimarbeitsplatz.
	MS Windows	Betriebssystem	Zur datenschutzfreundlichen (datenarmen) Nutzung von Microsoft Windows 10 müssen umfangreiche Einstellungen zum Datenschutz vorgenommen werden, am einfachsten gelingt dies über ein vom ZIM empfohlenes Hilfsprogramm.
	MacOS iOS	Betriebssystem	Apple Systeme: Auch unter MacOS und IOS sind Datenschutzeinstellungen notwendig, um den Datenabfluss an Dritte zu minimieren.
	Android	Betriebssystem	Google Android System: Überprüfen Sie bitte folgende Einstellungen auf Android Geräten.
	Linux, Ubuntu	Betriebssystem	Einstellungen sind ggf. unter einigen Distributionen notwendig.
			☞ Ende Checkliste Datenschutz

5.2 CHECKLISTE INFORMATIONSSICHERHEIT

Testen Sie Ihr Wissen zur Informationssicherheit anhand der Checkliste. Weiterführende Information und Anleitungen zu den Themenbereichen sind Anhand der Verlinkungen abrufbar. Prüfen Sie die Geräte und Ihre Arbeitsweise im Homeoffice anhand der Liste.

Prüfung	Was	Risiko / Bereich	Lösung
Hinweis	**10 Tipps**	**IT-Sicherheit**	**Informieren Sie sich regelmäßig** auf den Seiten des **ZIM** zu aktuellen Gefahren, generellen Verhaltenshinweisen und den verlinkten Informationen vom BSI. *Selbsteinschätzung:* ☺ 😐 ☹
	1. Passwörter	Identitäts-Diebstahl	**Verwenden Sie immer unterschiedliche und sichere Passwörter** und bei Bedarf einen Passwortmanager wie bspw. KeePassXC . *Teilen Sie Ihr Passwort nicht!* ***Das ZIM fragt Ihr UP-Passwort nie persönlich ab!*** ☺ 😐 ☹
	2. Benutzung	Benutzer-Konten Steuerung	**Schränken Sie Berechtigungen auch von PC-Mitbenutzer/-innen ein**. Bspw. durch die strikte Trennung von Zugriffen für: Benutzer/-innen und Administration sowie die dienstliche und private Nutzung (bspw. auch für Kinder). ☺ 😐 ☹
	3. Aktualität	Upgrades und Updates	Halten Sie die **Software ihrer Systeme immer auf dem aktuellen Stand** (Betriebssystem, Anwendungen, Browser) ☺ 😐 ☹
	4. Antivirus und Firewall	Schadsoftware	Verwenden Sie **Antiviren Software und eine Firewall.** In den meisten modernen Betriebssystemen sind diese Programme bereits integriert und werden als ausreichend sicher eingestuft (Win10 mit Defender, SmartScreen u. Firewall). ☺ 😐 ☹
	5. E-Mail	E-Mail	Gehen Sie mit **E-Mails und deren Anhängen** sowie mit Nachrichten in sozialen Netzwerken sorgsam um. ☺ 😐 ☹
			☞ Fortsetzung auf Seite 6

☞ Fortsetzung von Seite 5

Prüfung	Was	Risiko / Bereich	Lösung
	S/MIME mit DFN-PKI	Sichere E-Mail	Optional: E-Mails werden über die UP (DFN-PKI) **digital signiert** und bei Bedarf **lokal verschlüsselt**. ☺ 😐 ☹
	6. WLAN	Daten-integrität	Sichern Sie Ihr **WLAN** ab! Personalisieren Sie den WLAN-Namen, das Router- und WLAN- Passwort. Die WLAN-Verschlüsselung muss mind. WPA2 sein, aktualisieren Sie die Firmware des Routers. Nutzen Sie auf dem Campus ausschließlich das eduroam-WLAN. ☺ 😐 ☹
	7. VPN	Daten-integrität	Um eine sichere Kommunikation im Homeoffice zu ermöglichen, sollten Sie sich ausschließlich über eine sichere VPN-Verbindung mit dem Uni-Netz verbinden. ☺ 😐 ☹
	8. WWW	Web-Browser	Erhöhen Sie die Sicherheit Ihres **Internet-Browsers**. Speichern Sie keine Passwörter, entfernen Sie unnötige Add-Ons. Vorsicht beim Download von Software aus dem Internet. Seien Sie zurückhaltend mit der Angabe persönlicher **Daten** im Internet. ☺ 😐 ☹
	9. Diebstahl	Verlust	Schützen Sie Ihre Hardware gegen Diebstahl und unbefugten Zugriff. Zur Vorbeugung unbefugten Zugriffes bei mobilen Geräten der Universität Potsdam sind immer die Datenträger zu **verschlüsseln!** Stichwort: BitLocker (To Go), Truecrypt, FileVault. Verwenden Sie keine USB-Sticks oder verschlüsseln Sie diese zumindest. ☺ 😐 ☹
	10. Sicherung	Datenverlust	Erstellen Sie regelmäßige **Datensicherungen** (bspw. FileBox od. Box.UP, beim Mac über Time Machine). ☺ 😐 ☹

☞ Ende Checkliste Informationssicherheit

Referenzen

Herausgeber: Universität Potsdam - Homeoffice Handbuch
https://www.uni-potsdam.de/de/zim/beratung-hilfe/self-service

Herausgeber: Universität Potsdam - ZIM Sicherheitshinweise
https://www.uni-potsdam.de/de/zim/beratung-hilfe/sicherheitshinweise

Herausgeber: BSI und Deutschland sicher im Netz (DsiN) - Die Cyberfibel
https://www.cyberfibel.de/

Herausgeber: Ines-IT.at – Passwortkarte, eine Anleitung
https://www.ines-it.de/wp-content/uploads/INES-IT_Anleitung_Passwortkarte_Version_1-0_Stand_07-2020.pdf

Herausgeber: HPI – Prüfen Sie, ob das eigene E-Mail-Konto bereits kompromittiert ist:
https://sec.hpi.de/ilc/search?lang=de

Herausgeber: BSI - Checklisten und Tipps
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Checklisten/checklisten_node.html

Herausgeber: Google*, SoSafe* - Kostenloser Phishing Test
https://phishingquiz.withgoogle.com/ - https://phish-test.de/
** Firmeninteresse ist vorhanden*

Herausgeber: Google- Upload und Prüfung verdächtiger Dateien
https://www.virustotal.com/gui/home/upload