Sichere Konfiguration für private macOS Notebooks an der ZHAW (BYOD)

Inhalt

1.1 Einführung BYOD (Bring your own Device) 2
1.2 Optionale Installation einer Virenschutzlösung mit aktivem Abonnement 2
1.3 Regelmässige Installation von Sicherheitsupdates bzw. macOS Upgrade 2
1.4 Aktivierung der Firewall des Notebooks 3
1.5 Browserschutz und Privatsphäre 3
1.6 Userkonten ohne Administrationsrechte / Sichere Passwörter 4
1.7 Regelmässige Datensicherung 4
1.8 Nutzung des Notebooks in öffentlichen Räumen der ZHAW 4
1.9 Verschlüsselung der Festplatte (FileVault) 5
1.10 Änderungsverzeichnis 5

Sichere Konfiguration für private macOS Notebooks an der ZHAW: Ventura / Monterey

1.1 Einführung BYOD (Bring your own Device)

An der ZHAW dürfen Studierende und Mitarbeitende mit privaten Geräten arbeiten.
Voraussetzung dafür ist die Einhaltung grundlegender Sicherheitseinstellungen für diese privaten Geräte.
Im vorliegenden Dokument finden Sie die Mindestanforderungen, die erfüllt sein müssen, damit Sie Ihr Gerät an der ZHAW nutzen dürfen..

1.2 Optionale Installation einer Virenschutzlösung mit aktivem Abonnement

Alle macOS Geräte haben von Haus aus die rudimentäre Virenschutzlösung xProtect und Gatekeeper installiert. Diese Lösungen bieten gegen aktuelle Bedrohungen einen grundlegenden Schutz.
Optional empfehlen wir die Nutzung einer kostenpflichtigen Virenschutzlösung.
Bedingung ist dabei, **dass diese laufend aktuell gehalten und gewartet wird bzw. ein gültiges Abonnement vorhanden ist**.

Folgende handelsübliche optionale Virenschutzprogramme sind empfohlen:

- Bit Defender Internet Security: https://www.bitdefender.de/solutions/internet-security.html
- Norton 360 Deluxe / Premium: https://ch.norton.com/products/norton-360
- Kaspersky Premium-Paket: https://www.kaspersky.de/premium
- McAfee Premium / Advanced: https://www.mcafee.com/de-de/index.html

1.3 Regelmässige Installation von Sicherheitsupdates bzw. macOS Upgrade

Hier beschreiben wir die Installation der Updates für macOS. Sicherheitsupdates müssen regelmässig installiert werden, um Ihr Notebook vor Sicherheitslücken zu schützen.
Falls Sie macOS 12 (Monterey) nutzen: Bitte aktualisieren Sie macOS auf Version 14 (Ventura).

macOS 12 (Monterey)	macOS 14/13 (Sonoma/Ventura)
1. Öffnen Sie die **Systemeinstellungen** 2. Klicken Sie auf **Software-Update** 3. Aktivieren Sie die Checkbox **Meinen Mac automatisch aktualisieren** 4. Klicken Sie auf **weitere Optionen** und aktivieren Sie alle Checkboxen 5. Falls Updates angezeigt werden, installieren Sie diese durch Anklicken von **Jetzt aktualisieren** 6. Folgen Sie den weiteren Anweisungen und Akzeptieren Sie den Softwarelizenzvertrag. 7. Die Aktualisierung wird gestartet. Es erfolgt nach einiger Zeit ein Neustart 8. Wiederholen Sie die Schritte 5-7, bis keine Updates mehr angezeigt werden. 9. Prüfen Sie regelmässig, ober Updates vorhanden sind. Installieren Sie diese umgehend.	1. Öffnen Sie die **Systemeinstellungen** 2. Klicken Sie auf **Allgemein → Software-Update** 3. Aktivieren Sie die automatischen Updates, indem Sie nach dem Klick auf das Informationslogo alle Checkboxen aktivieren. Schliessen Sie die Einstellungen mit Fertig ab und geben Sie zur Aktivierung das Systemkennwort ein. 4. Falls Updates angezeigt werden, installieren Sie diese durch Anklicken von Jetzt aktualisieren 5. Folgen Sie den weiteren Anweisungen und Akzeptieren Sie den Softwarelizenzvertrag. 6. Die Aktualisierung wird gestartet. Es erfolgt nach einiger Zeit ein Neustart 7. Wiederholen Sie die Schritte 4-6, bis keine Updates mehr angezeigt werden. 8. Prüfen Sie regelmässig, ober Updates vorhanden sind. Installieren Sie diese umgehend.

1.4 Aktivierung der Firewall des Notebooks

Da sie sich an der ZHAW in einem Netzwerk mit vielen anderen Benutzern und Computern befinden, muss zum Schutz ihres Computers bzw. Ihrer Daten und zum Schutz der anderen User die lokale Firewall aktiviert werden. Untenstehend finden Sie die Anweisungen zur Aktivierung der Firewall Lösung von macOS.

macOS 12 (Monterey)	macOS 14/13 (Sonoma/Ventura)
1. Öffnen Sie die **Systemeinstellungen** 2. Wählen Sie im Apfel Menu den Menupunkt Systemeinstellungen 3. Wählen Sie auf die Funktion **Sicherheit & Datenschutz** 4. Klicken Sie auf den **Firewall** Tab 5. Klicken Sie auf das Schloss unten links an, um Änderungen zu ermöglichen und geben sie das Systemkennwort ein 6. Klicken Sie auf Firewall aktivieren, um die Firewall zu starten 7. Schliessen Sie die Systemeinstellungen	1. Öffnen Sie die **Systemeinstellungen** 2. Wählen Sie auf die Funktion **Netzwerk → Firewall** 3. Falls die Firewall deaktiviert ist, aktivieren sie die Firewall. 4. Allenfalls müssen Sie zur Aktivierung der Firewall das Systemkennwort eingeben. 5. Schliessen Sie die Systemeinstellungen

1.5 Browserschutz und Privatsphäre

Folgende Schritte erhöhen die Sicherheit bei der Nutzung von Webbrowsern und schützen Ihre Privatsphäre im Internet:

- Prüfen Sie regelmässig, ob die Webbrowser, die Sie verwenden, aktuell sind:
  - **Safari**: Wird über das Software-Update in den Systemeinstellungen aktualisiert
  - **Firefox**: Firefox Menu → Über Firefox
  - **Chrome**: Chrome Menu → Über Google Chrome
- Benutzen Sie eine Suchmaschine die Suchanfragen anonymisiert. Empfehlungen:
  - DuckDuckGo: https://duckduckgo.com
  - Startpage: https://www.startpage.com
- Nutzen Sie einen Browserschutz für Firefox, Chrome oder Safari .
  Wir empfehlen folgende Browsererweiterungen:
  - **DuckDuckGo**: https://duckduckgo.com
    - Firefox: Erweiterung hinzufügen
    - Bei Safari muss die Erweiterung im App Store heruntergeladen werden:
      Safari Menu → Safari Erweiterungen → DuckDuckGo Privacy for Safari →
      Laden und installieren → Erweiterung in Safari aktivieren: Erweiterung aktivieren
  - **TrafficLight (Hersteller: BitDefender)**
    - Firefox/Chrome: aus dem Chrome Store bzw. den Add-Ons bei Firefox installieren
    - Safari: Die Erweiterung ist für Safari nicht verfügbar

1.6 Userkonten ohne Administrationsrechte / Sichere Passwörter

Wir empfehlen, generell mit Userkonten ohne Administratorrechten zu arbeiten.
So hat eingeschleuste Malware weniger Möglichkeiten, um Schaden anzurichten.
Zur Installation von Software, erstellen Sie ein separates Konto mit Administrationsrechten.
Userkonten ohne Adminrechte können in der Systemsteuerung erstellt werden.

Nutzen sie auf allen Accounts ihres Notebooks sichere Passwörter mit folgenden Anforderungen:

- Das Passwort hat eine Länge von mindestens zwölf Zeichen
- Das Passwort enthält Grossbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen
- Das Passwort enthält keine offensichtlichen Bezüge zu Ihrer Person (Namen, Adressen, …)

Tipp: Zur einfacheren Verwaltung von Passwörtern empfehlen wir die Nutzung eines Passwort-Managers.

1.7 Regelmässige Datensicherung

Führen sie regelmässig eine Datensicherung Ihrer Daten auf einen externen Datenträger durch. Falls Ihre Daten nur auf dem Notebook liegen und die Festplatte einen Defekt aufweist, sind sämtliche Daten auf Ihrem Gerät unwiederbringlich verloren.
Apple stellt dazu die Time Machine zur Verfügung.

1.8 Nutzung des Notebooks in öffentlichen Räumen der ZHAW

Da es sich bei der ZHAW um öffentlichen Raum handelt sind empfehlen wir folgenden Schritte:

- Sperren Sie Ihr Notebook, wenn Sie es nicht benutzen: Apfelmenu → Bildschirm sperren
- Lassen Sie Ihr Gerät nie unbeaufsichtigt.

1.9 Verschlüsselung der Festplatte (FileVault)

Sind auf Ihrem privaten Gerät sensible Daten vorhanden, welche nicht in fremde Hände gelangen dürfen, empfehlen wir Ihnen die Festplatte zu verschlüsseln.
Wichtig: Die Verschlüsselung der Festplatte birgt die Gefahr, dass bei Verlust des Wiederherstellungsschlüssels und des Passwortes Ihre Festplatte nicht mehr gelesen werden kann. Falls Sie nicht iCloud zur Wiederherstellung nutzen, ist der Wiederherstellungsschlüssel sicher zu verwahren. Die ZHAW leistet keine Unterstützung zur Wiederherstellung Ihrer Daten.

macOS 12 (Monterey)	macOS 14 (Sonoma/Ventura)
1. Aktivieren Sie Ihren iCloud Account 2. Öffnen Sie die **Systemeinstellungen** 3. Wählen Sie auf die Funktion **Sicherheit & Datenschutz** 4. Wechseln Sie in den FileVault Tab 5. Entsprerren Sie die Systemeinstellungen mit einem Klick auf das Schloss und anschliessender Passworteingabe. 6. Klicken Sie FileVault aktivieren 7. Aktivieren Sie den Radiobutton **Meinen iCloud-Account so konfigurieren, dass mein Passwort zurückgesetzt werden kann.** → Fortfahren 8. Tragen Sie das Systempasswort ein 9. Anschliessend wird die Festplatte verschlüsselt.	Wichtig: Die Nutzung von iCloud wird vorausgesetzt. 1. Aktivieren Sie Ihren iCloud Account 2. Öffnen Sie die **Systemeinstellungen** 3. Wählen Sie auf die Funktion **Datenschutz & Sicherheit** 4. Aktivieren Sie **FileVault** 5. Tragen Sie das Systempasswort ein 6. Aktivieren Sie den Radiobutton **Meinen iCloud-Account so konfigurieren, dass mein Passwort zurückgesetzt werden kann.** → Fortfahren 7. Anschliessend wird die Festplatte verschlüsselt.

1.10 Änderungsverzeichnis

Datum	Version	Wer	Änderung
15.03.2022	1.0	brmi	Dokument erstellt
13.04.2022	1.1	brmi	Dokument geprüft. Anpassung Virenschutz. Korrekturen.
15.03.2023	2.0	brmi	Diverse Ergänzungen und Anpassungen für die gesamte ZHAW
11.06.2024	2.2	brmi	Diverse Anpassungen und Korrekturen Empfehlung neu: Bit Defender Internet Security
12.06.2024	2.2.1	brmi	Optionale Virenschutzlösung als Empfehlung anstelle Obligatorium
11.07.2024	2.2.2	brmi	Kleine Korrektur: TrafficLight für Safari