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

Inhalt

Sichere Konfiguration für private Windows Notebooks an der ZHAW

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.
Die Schritte in den Kapiteln 1.2 bis 1.4 sind zwingend einzuhalten.
Die Schritte in den Kapiteln 1.5 bis 1.9 sind empfohlen.

1.2 Installation eines Virenschutzprogrammes mit aktivem Abonnement

Ein privates Notebook darf am ZHAW-Netzwerk nur mit einem aktuellen Virenschutzprogramm betrieben werden. Wir empfehlen den Einsatz des bereits in Windows 10/11 enthaltenen Virenschutztools Windows Defender Antivirus.

Öffnen Sie dazu die **Windows-Sicherheit** App. Führen sie folgenden Einstellungen durch.

- Aktivieren Sie den App- & Browserschutz
- Klicken Sie auf Viren- & Bedrohungsschutz
- Im Bereich Einstellungen führen Sie folgenden Einstellungen durch:
  - Echtzeitschutz: Ein
  - Cloudbasierter Schutz: Ein
  - Manipulationsschutz: Ein
  - Überwachten Ordnerzugriff verwalten → Überwachter Ordnerzugriff: Ein
    und Auswahl der überwachten Ordner (geschützte Ordner). Fügen Sie hier allfällige weitere Ordner hinzu.

Falls Sie bereits ein anderes Virenschutzprogramm installiert haben, können Sie dieses weiter benutzen.
Bedingung ist jedoch, **dass es laufend aktuell gehalten und gewartet wird bzw. ein gültiges Abonnement vorhanden ist.**

Die Nutzung von privaten Geräten an der ZHAW ohne gültiges Abonnement ist untersagt.
Folgende handelsübliche Virenschutzprogramme sind für die ZHAW nutzbar:

- Bit Defender Total Security: https://www.bitdefender.de/solutions/total-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

Hier beschreiben wir die Installation der Windows Updates und die Aktivierung der regelmässigen Updatehinweise. Sicherheitsupdates müssen regelmässig installiert werden, um Ihr Notebook vor Sicherheitslücken zu schützen.

- **Windows 10**:
    1. Starten Sie die **Windows Einstellungen**
    2. Klicken Sie **Update & Sicherheit**
    3. Klicken Sie **Windows Update**
    4. Klicken Sie auf **Erweiterte Optionen**
    5. Aktivieren Sie folgende Update Optionen:
        - Erhalten Sie Updates für andere Microsoft Produkte, wenn Sie Windows aktualisieren
        - Starten Sie das Gerät so bald wie möglich neu, wenn zur Installation eines Updates ein Neustart erforderlich ist.
        - Benachrichtigung anzeigen, wenn Ihr PC einen Neustart erfordert, um das Update abzuschliessen
    6. Kehren Sie zu Windows Update zurück (Pfeil nach links am oberen Rand des Fensters)
    7. Klicken Sie **Nach Updates suchen Installieren Sie alle verfügbaren Updates**
    8. Falls ein Neustart notwendig ist, führen Sie einen Neustart durch
    9. Wiederholen Sie die Schritt 7-8 bis keine Updates mehr angezeigt werden.
    10. Prüfen Sie regelmässig, ober Updates vorhanden sind. Installieren Sie diese umgehend.

- **Windows 11**:
    1. Starten Sie die **Windows Einstellungen**
    2. Klicken Sie **Windows Update**
    3. Klicken Sie auf **Erweiterte Optionen**
    4. Aktivieren Sie folgende Update Optionen:
        - Updates für andere Microsoft Produkte erhalten
        - Sich auf den aktuellen Stand bringen lassen
        - Benachrichtigung erhalten, wenn ein Neustart erforderlich ist, um das Update abzuschliessen
    5. Kehren Sie zu Windows Update zurück
    6. Klicken Sie Nach Updates suchen
    7. Falls Updates angezeigt werden, installieren Sie die Updates mit **Jetzt installieren**
    8. Falls ein Neustart notwendig ist, führen Sie einen Neustart durch
    9. Wiederholen Sie Schritt 5-8, bis keine Updates mehr angezeigt werden.
    10. Prüfen Sie regelmässig, ob Updates vorhanden sind. Installieren Sie diese umgehend.

1.4 Aktivierung der Firewall des Notebooks

Wir empfehlen, die Firewall Lösung, die mit den Betriebssystem Windows mitgeliefert wird einzusetzen. Wenn Sie eine Firewall Lösung eines Drittherstellers (BitDefender, Norton, Kaspersky…) einsetzen, müssen Sie diese immer aktuell halten.
Anweisungen zur Aktivierung der Windows Firewall:

- Starten Sie im Startmenu das Werkzeug **Windows Sicherheit**
- Klicken Sie auf **Firewall- & Netzwerkschutz**
- Prüfen Sie die Einstellungen der drei Netzwerkbereiche. Bei allen drei Bereichen muss die Einstellung **«Firewall ist aktiviert»** stehen.
    - Domänennetzwerk
    - Privates Netzwerk
    - Öffentliches Netzwerk

      Falls bei einem der drei Bereich die Firewall ausgeschaltet sein sollte, klicken Sie auf den jeweiligen Bereich und aktivieren die Firewall

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:
    - **Firefox**: Hilfe → Über Firefox
    - **Edge**: Anwendungsmenü oben rechts → Hilfe und Feedback → Infos zu Microsoft Edge
    - **Chrome**: Anwendungsmenü oben rechts → Hilfe → über Google Chrome
- Benutzen Sie eine Suchmaschine die Suchanfragen anonymisiert. Empfehlungen:
    - DuckDuckGo: https://duckduckgo.com
    - Startpage: https://www.startpage.com
- Nutzen Sie einen Browserschutz. Wir empfehlen folgende Browsererweiterungen:
    - **DuckDuckGo:** https://duckduckgo.com → Button DuckDuckGo zu ….. hinzufügen
    - **Startpage Privatsphäre-Schutz** aus dem Chrome Store bzw. den Add-Ons bei Firefox
    - **TrafficLight** aus dem Chrome Store bzw. den Add-Ons bei Firefox

1.6 Userkonten ohne Administrationsrechte / Sichere Passwörter

Wir empfehlen, generell mit Userkonten ohne Administratorrechten zu arbeiten.
So hat eingeschleuste Malware weniger Möglichkeiten, um Schäden anzurichten.
Zur Installation von Software, erstellen Sie ein separates Konto mit Administrationsrechten.

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.

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. Tastenkombination: **Windows** – **L**
- Lassen Sie Ihr Gerät nie unbeaufsichtigt.

1.9 Verschlüsselung der Festplatte mit BitLocker

Sind auf Ihrem privaten Gerät sensible Daten vorhanden, welche nicht in fremde Hände gelangen dürfen, empfehlen wir Ihnen die Festplatte mittels Bitlocker zu verschlüsseln.
BitLocker ist unterstützt in den Pro-, Enterprise und EDU-Versionen von Windows.
Wichtig: Die Verschlüsselung der Festplatte birgt die Gefahr, dass bei Verlust des Wiederherstellungsschlüssels und des Passwortes Ihre Festplatte nicht mehr gelesen werden kann.
Der Wiederherstellungsschlüssel ist darum sicher zu verwahren.
Die ZHAW leistet keine Unterstützung zur Wiederherstellung Ihrer Daten.
In folgenden Dokumenten im Internet finden Sie Anweisungen zur Nutzung von BitLocker:

- Aktivierung der Geräteverschlüsselung in Windows:
  https://support.microsoft.com/de-de/windows/ger%C3%A4teverschl%C3%BCsselung-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d
- Sichern des BitLocker Wiederherstellungsschlüssels **(zwingend, da Sie Ihr Gerät bei allfälligem Verlust des Schlüssels nicht wieder entsperren können)**:
  https://support.microsoft.com/de-de/windows/sichern-des-bitlocker-wiederherstellungsschl%C3%BCssels-e63607b4-77fb-4ad3-8022-d6dc428fbd0d

1.10 Änderungsverzeichnis

Datum	Version	Wer	Änderung
15.03.2022	1.0	brmi	Dokument erstellt
13.04.2022	1.1	brmi	Dokument geprüft. Angepasst auf Defender mit Einstellungen, aktives Abonnement, optional Bit Defender Total Security.
17.08.2022	1.2	brmi	Ergänzt: Deaktivierung Internet Explorer 11
15.03.2023	2.0	brmi	Diverse Ergänzungen und Anpassungen für die gesamte ZHAW
06.04.2023	2.1	brmi	Ergänzung BitDefender TrafficLight (Kapitel 1.5)