IT-SERVICE
ZENTRUM

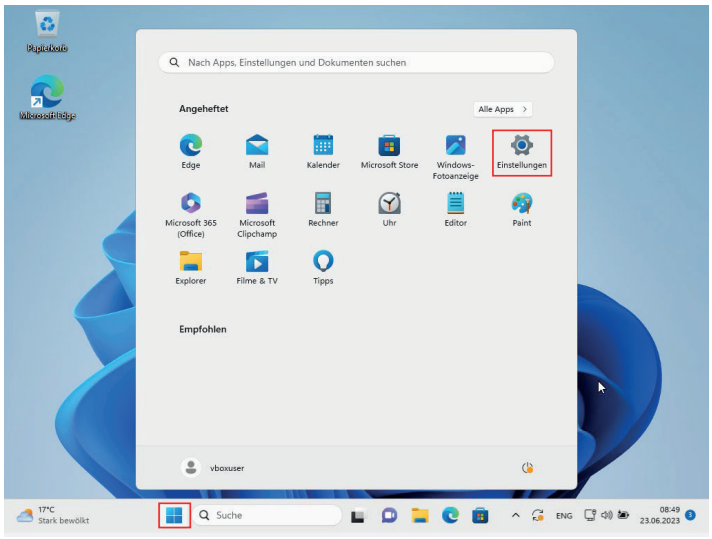
ANLEITUNG

Windows Defender 11

Das IT-Servicezentrum hat Ihnen eine Anleitung für die Einstellungen des Windows Defenders erstellt, damit Sie die Einstellungen selbst übernehmen können.

Bitte beachten Sie das die Einstellung **CLOUDBASIERTER SCHUTZ** unter Punkt 8 nur zu aktivieren ist, wenn sie Microsoft365 wie Office 365, Teams usw. haben.

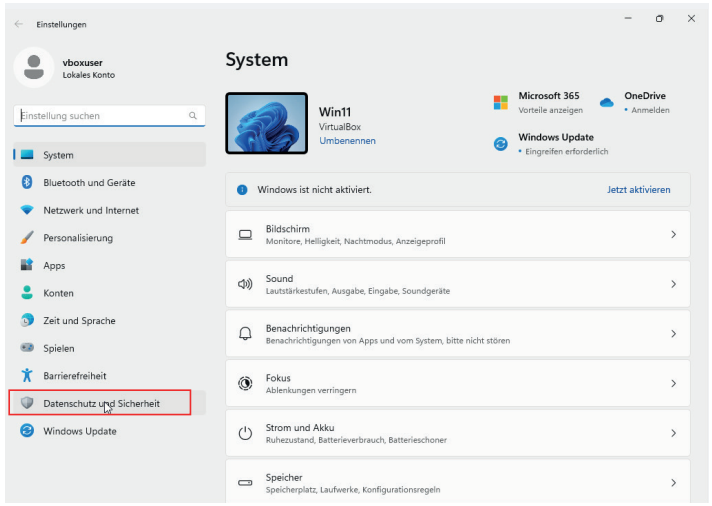
1. Klicken sie auf Windows/Start
2. anschließend auf das Zahnradsymbol (Einstellungen)



2

1

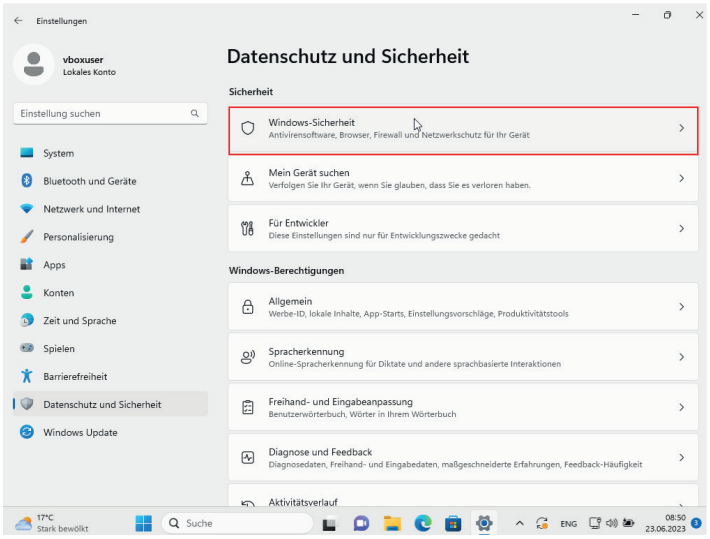
3. Klicken sie auf „Datenschutz und Sicherheit“.



3

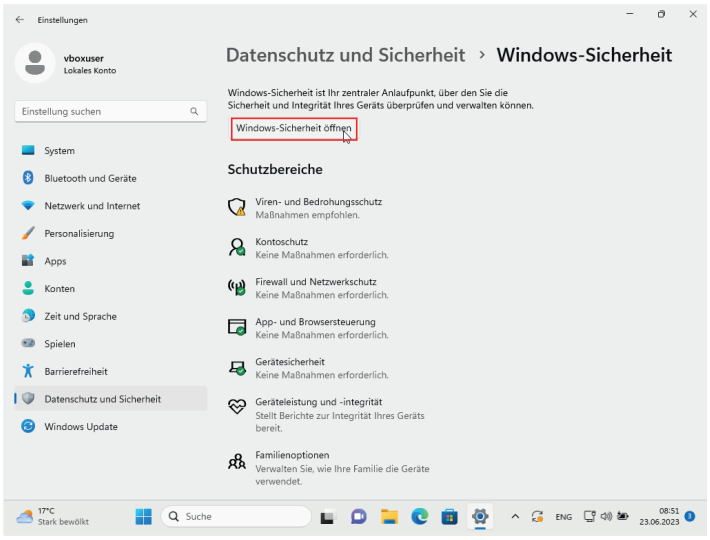
4. Nun klicken sie Auf der linken Seite auf „Windows-Sicherheit“.

4



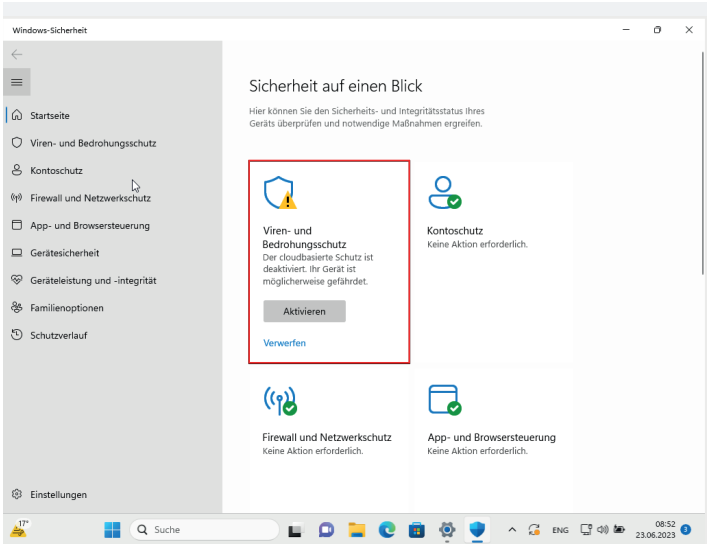
5. Klicken sie im nächsten Schritt, oben den Button „Windows-Sicherheit öffnen“.

5



6. Klicken sie auf „Viren- & Bedrohungsschutz“.

6

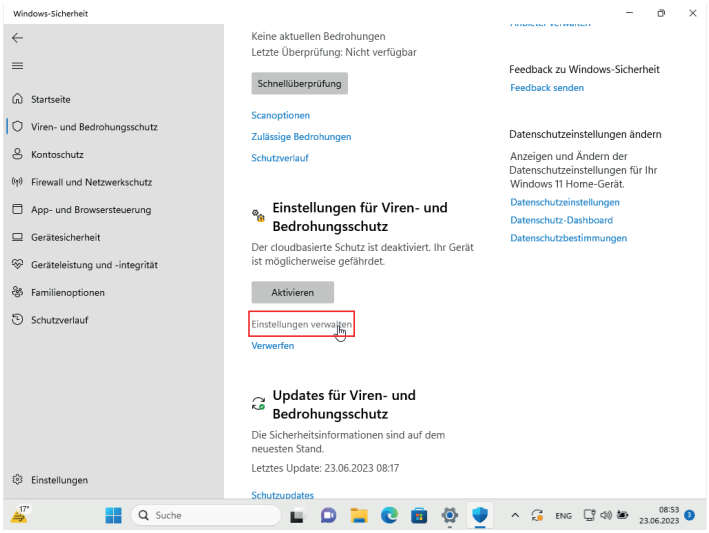


7. anschließend klicken sie unter „Einstellungen für Viren- & Bedroh-ungsschutz“ auf den Text „Einstellungen verwalten“.

Folgende Einstellungen sind hier zu tätigen:

- „Echtzeitschutz“ aktivieren.
- „Cloudbasierter Schutz“ deaktivieren.
- „Automatische Übermittlung von eispielen“ deaktivieren.
- „Manipulationsschutz“ Aktivieren.

7

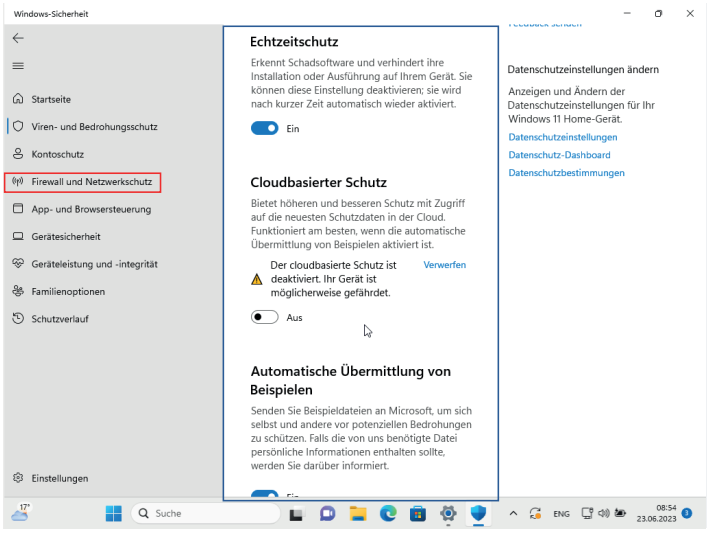


8. Wenn sie alle Einstellungen getätigt haben, klicken sie auf der linken Seite auf „Firewall - & Netzwerk-schutz“.

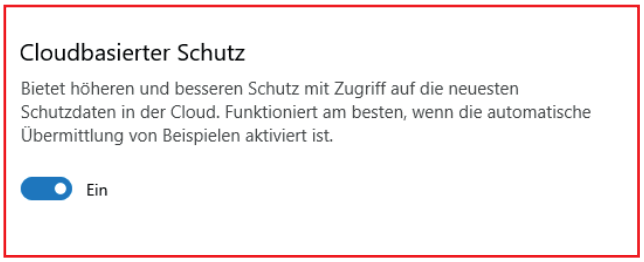
Folgende Einstellungen sind hier zu tätigen:

- „Domänennetzwerk“ Firewall aktiv.
- „Privates Netzwerk“ Firewall aktiv.
- „Öffentliches Netzwerk“ Firewall aktiv.

8



Die Einstellung Cloudbasierter Schutz ist nur zu aktivieren, wenn sie Microsoft365 wie Office 365, Teams usw. haben.

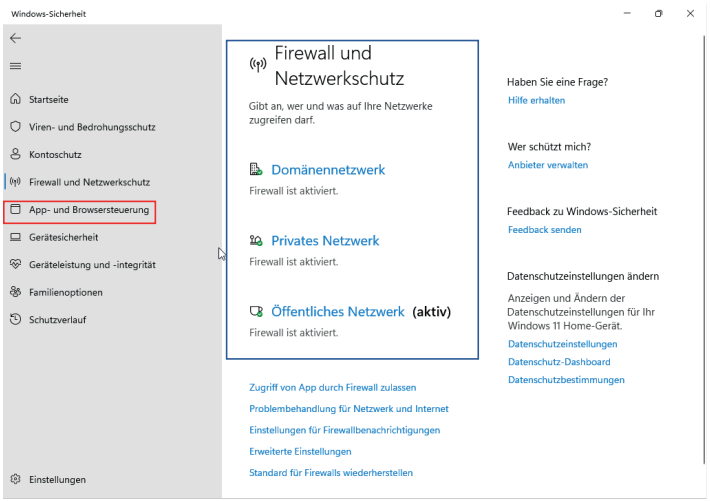


Wenn Sie den Cloudschutz deaktivieren meldet Windows das Ihre Gerät möglicherweise gefährdet ist. Das liegt daran das ohne Cloudschutz keine verdächtigen Dateien zur erweiterten Prüfung in die Microsoft Cloud geschickt werden.

Wenn Sie der MS Datenschutzvereinbarung im ITS Portal zugestimmt haben, darf der Cloudschutz aktiv sein, sonst müssen Sie ihn aus rechtlichen Gründen deaktivieren

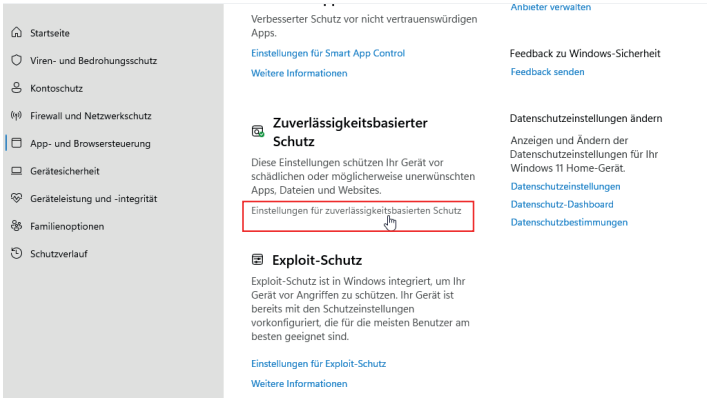
9. Wenn die Einstellungen bei ihnen so aussehen, klicken sie auf der linken Seite auf „ App- & Browsersteuerung“.

9



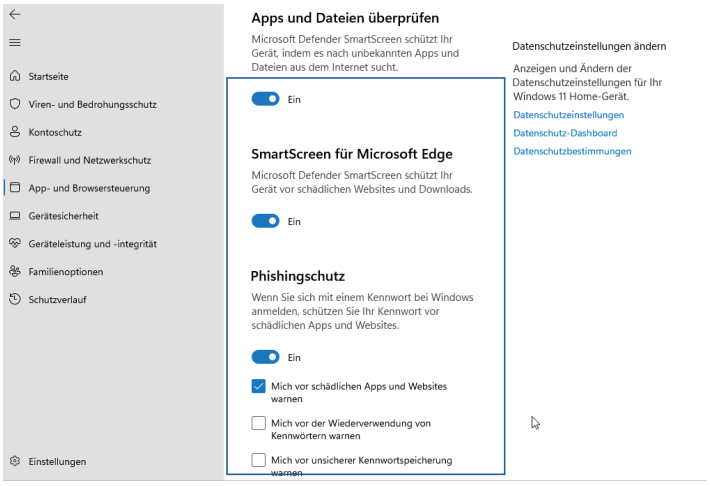
10. Klicken sie unter „Zuverlässigkeitsbasierter Schutz“ auf „Einstellungen für zuverlässigkeitsbasierten Schutz“.

10



Folgende Einstellungen sind hier zu tätigen:

- „Apps und Dateien überprüfen“ aktivieren.
- „Phishingschutz“ aktivieren und „Mich vor schädlichen Apps und Websites warnen“
- „SmartScreen für Microsoft Edge“ aktivieren.
- „Potenziell unerwünschte Apps werden blockiert“ deaktivieren.
- „SmartScreen für Microsoft Store-Apps“ aktivieren.



Wenn sie die Einstellung wie angegeben vorgenommen haben, können sie die Fenster schließen.

Noch Fragen?

Falls Sie trotz dieser Anleitung noch weitere Fragen zum Thema Mailappliance haben – kein Problem!
Sie können sich gerne per Mail **(ITS-Security@uni-bayreuth.de)**
an uns wenden.

Oder nutzen Sie unser Supportformular bzw. unseren ITS-Chatbot
unter **its.uni-bayreuth.de**.