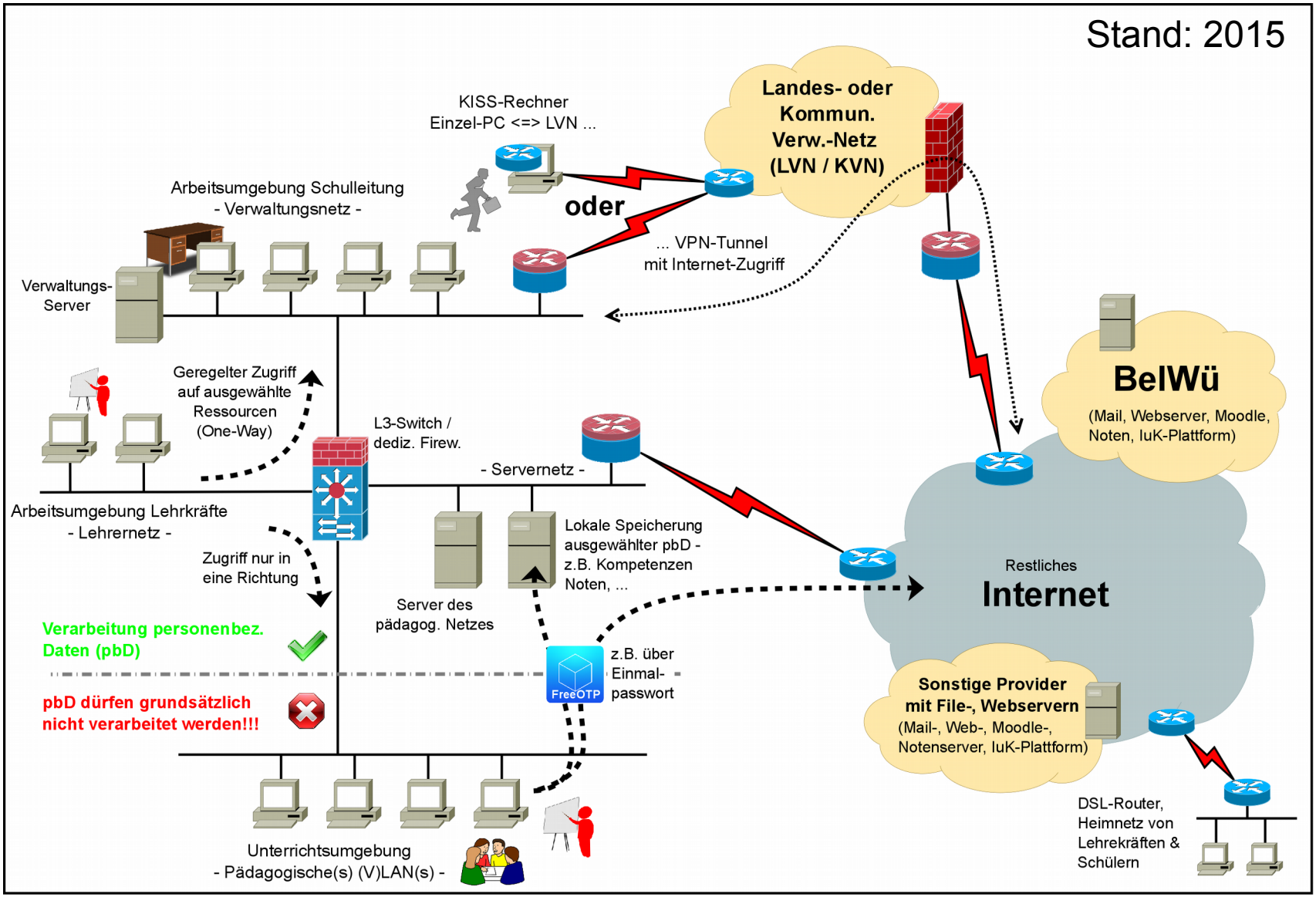
Landesakademie für Fortbildung und Personalentwicklung an Schulen

Andreas Grupp
grupp@lehrerfortbildung-bw.de

„Mobile Devices und 2-Faktor-Authentifizierung“ von Andreas Grupp ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz. http://creativecommons.org/licenses/by-sa/4.0/deed.de

Netzbrief v3 – spez. pbD im Intra- & Internet



BY-SA
A. Grupp - grupp@lehrerfortbildung-bw.de

Netzbrief v3 – Auszug …

*Zeugnisse, Lernstandsberichte, Halbjahresinformationen und vergleichbare Dokumente dürfen in der Unterrichtsumgebung **generell** nicht verarbeitet werden.*
Ist jedoch beabsichtigt, weitere personenbezogene Daten von Schülern in der Unterrichtsumgebung zu verarbeiten, beispielsweise laufende Leistungsbeurteilungen (Einteilung in Niveaustufen oder der Einsatz von Kompetenzrastern), müssen zwingend die folgenden technischen Datenschutzmaßnahmen getroffen werden.

- *Als Identitätsnachweis ist für jeden Nutzer eine Zwei-Faktoren-Authentifizierung erforderlich, die aus der Kombination von zwei verschiedenen voneinander unabhängigen Komponenten (Faktoren) besteht. Zusätzlich zum üblichen Passwort ist der Besitz eines "elektronischen Schlüssels" erforderlich. Denkbar wäre die Verwendung von Hardwaretokens oder von Einmal-Passwörtern (time-based one-time-Passwort, nach dem TOTP- bzw. OTP-Verfahren). Bei der Verwendung eines Einmalpassworts muss die Passworterzeugung zwingend auf einem zweiten Gerät erfolgen. Alternativ könnte auch eine TAN-Liste verwendet werden.*

Zusätzlich ist eigenes Server-Netz (auch als VLAN erlaubt) erforderlich. Die Datenübertraung muss zudem eine Transportverschlüsselung haben.

Zwei-Faktor-Authentifizierung?

- Erster Faktor bei der Authentifizierung
  - Benutzernamen und zugehöriges Passwort
  - Bei jedem Login gleich!
  - Häufig auch „weiteren Personen“ bekannt
- Zweiter Faktor bei der Authentifizierung
  - Zusatz-Hardware – z.B. Smartcard, Hardware-Token
    - Interoperabilität zwischen Anwendungen mäßig
  - Einmal-Passwort – z.B. auf Uhrzeit basierend
    - Time-based One-Time-Password (TOTP)
    - Am weitesten verbreitet → auf Basis des Google-Authenticator-Algorithmus

Zwei-Faktor-Authentifizierung – TOTP-Prinzip

Server

Gibt ein „Geheimnis“ vor

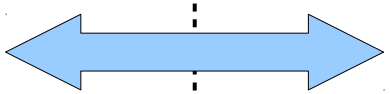
3EB4G3X5LI7ZKRWS

Client

Übernimmt „Geheimnis“

3EB4G3X5LI7ZKRWS

Einmaliger Vorgang!
Server und Client teilen sich nun ein „Geheimnis“



Benötigt hierfür keinerlei Online-Verbindung auf dem 2. Gerät! Weder Mobilfunk, noch Internet! Code wird von Hand oder per QR-Code-Scan übertragen

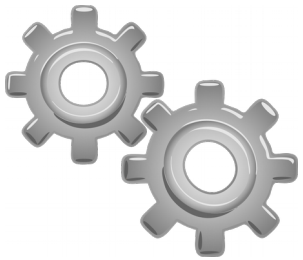
CC BY-SA
A. Grupp - grupp@lehrerfortbildung-bw.de

Zwei-Faktor-Authentifizierung – TOTP-Prinzip

Benötigt hierfür keinerlei Online-Verbindung mehr! Weder Mobilfunk, noch Internet!

Server

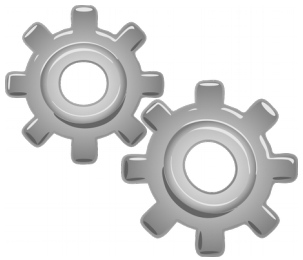
+ **3EB4G3X5 LI7ZKRWS**



640118

Client

+ **3EB4G3X5 LI7ZKRWS**



640118

Kommt der Client auf das gleiche Ergebnis?

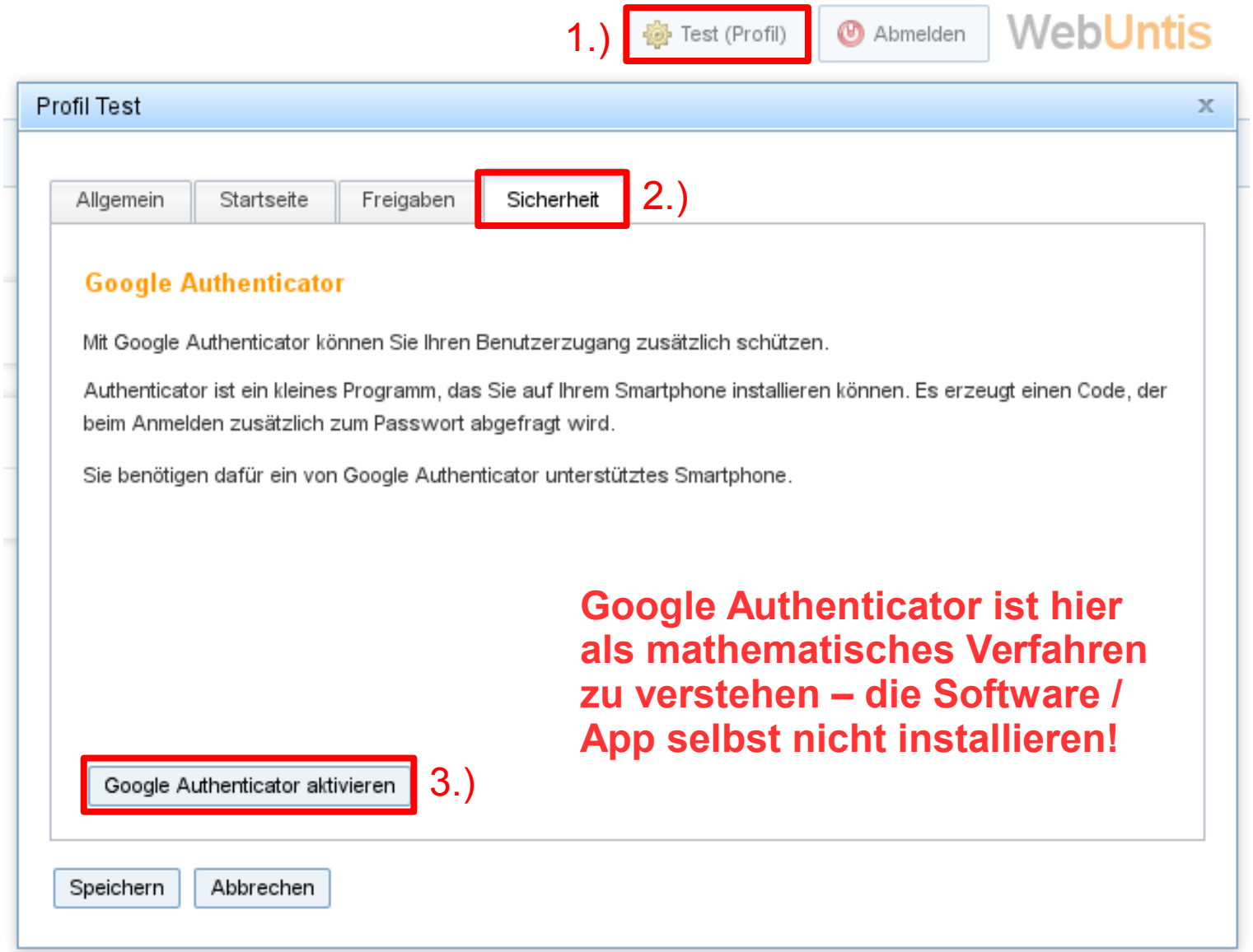
Und wo ist da nun ein „Mobile Device“?

- Woher wissen „weitere Personen“ eigentlich die Kombination „Benutzernamen / Passwort“?
- Und wo wird der 2. Faktor erzeugt? Netzbrief V3 **schreibt zweites Gerät zwingend vor**
- Zweites Gerät reduziert die Wahrscheinlichkeit, dass Angreifer beide Geräte gleichzeitig unter Kontrolle hat erheblich
- Mögliche Geräte als zweites Gerät:
  - Smartphone – egal welches Betriebssystem
  - Tablets – egal welches Betriebssystem
  - Eher weniger sinnvoll → 2. PC

Diverses! Probleme? Kosten?

- Freie, quelloffene Apps für TOTP → verfügbar
  - z.B. für Android, iOS → FreeOTP 
- Serverseitig z.B. für das Kompetenzraster in Moodle → bereits verfügbar
- Zeit auf Server u. Client muss einigermaßen synchron sein → Gewisse Abweichung ok.
- Software- Kosten für eigentliche 2-Faktor-Auth. beläuft sich auf → 0,- €
- Zweites Gerät → Kostenübernahme? Unterstützung? Beteiligung?

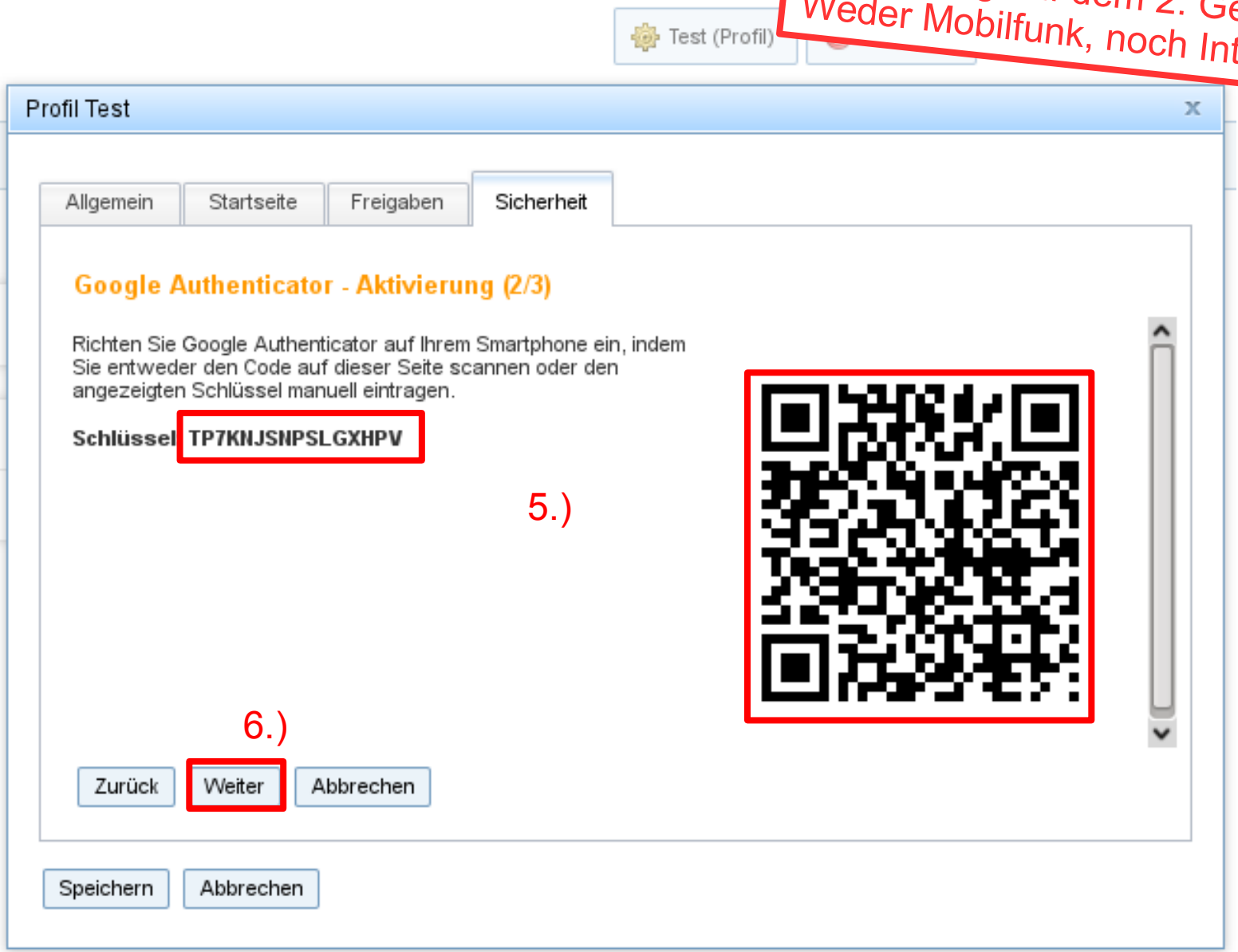
Beispiel → WebUntis



Beispiel → WebUntis

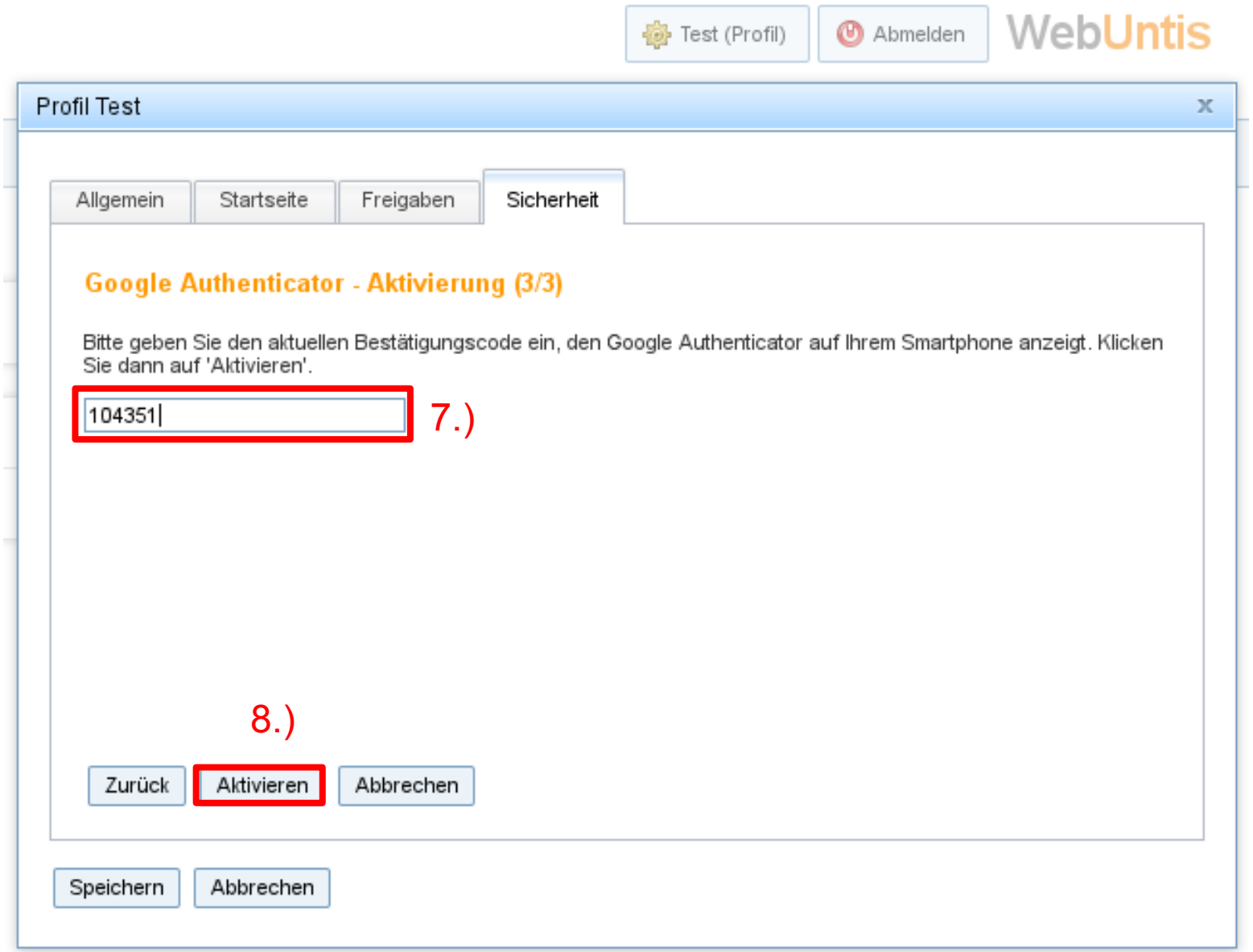
Beispiel → WebUntis

Benötigt hierfür keinerlei Online-Verbindung auf dem 2. Gerät!
Weder Mobilfunk, noch Internet!

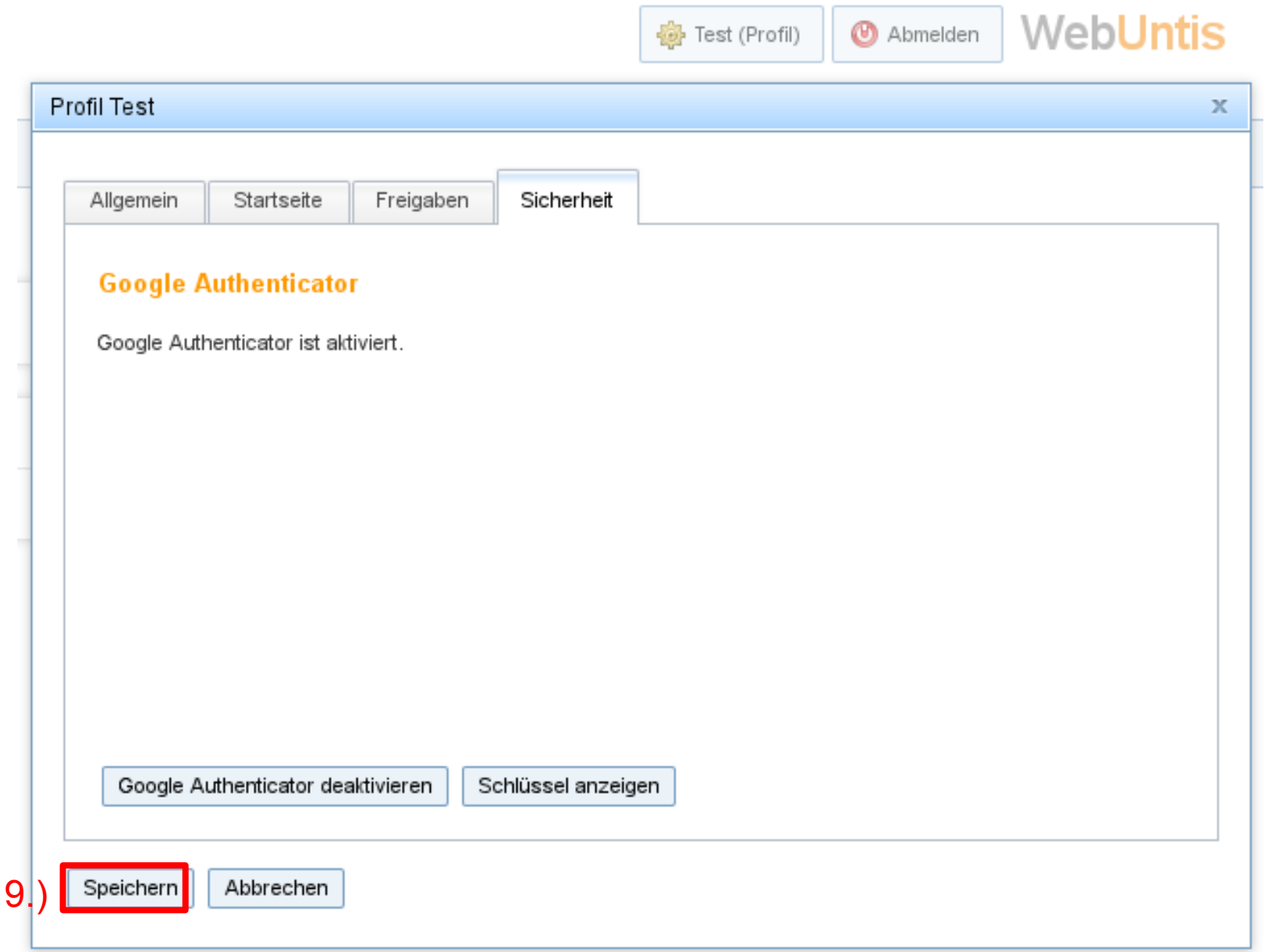


BY-SA

Beispiel → WebUntis

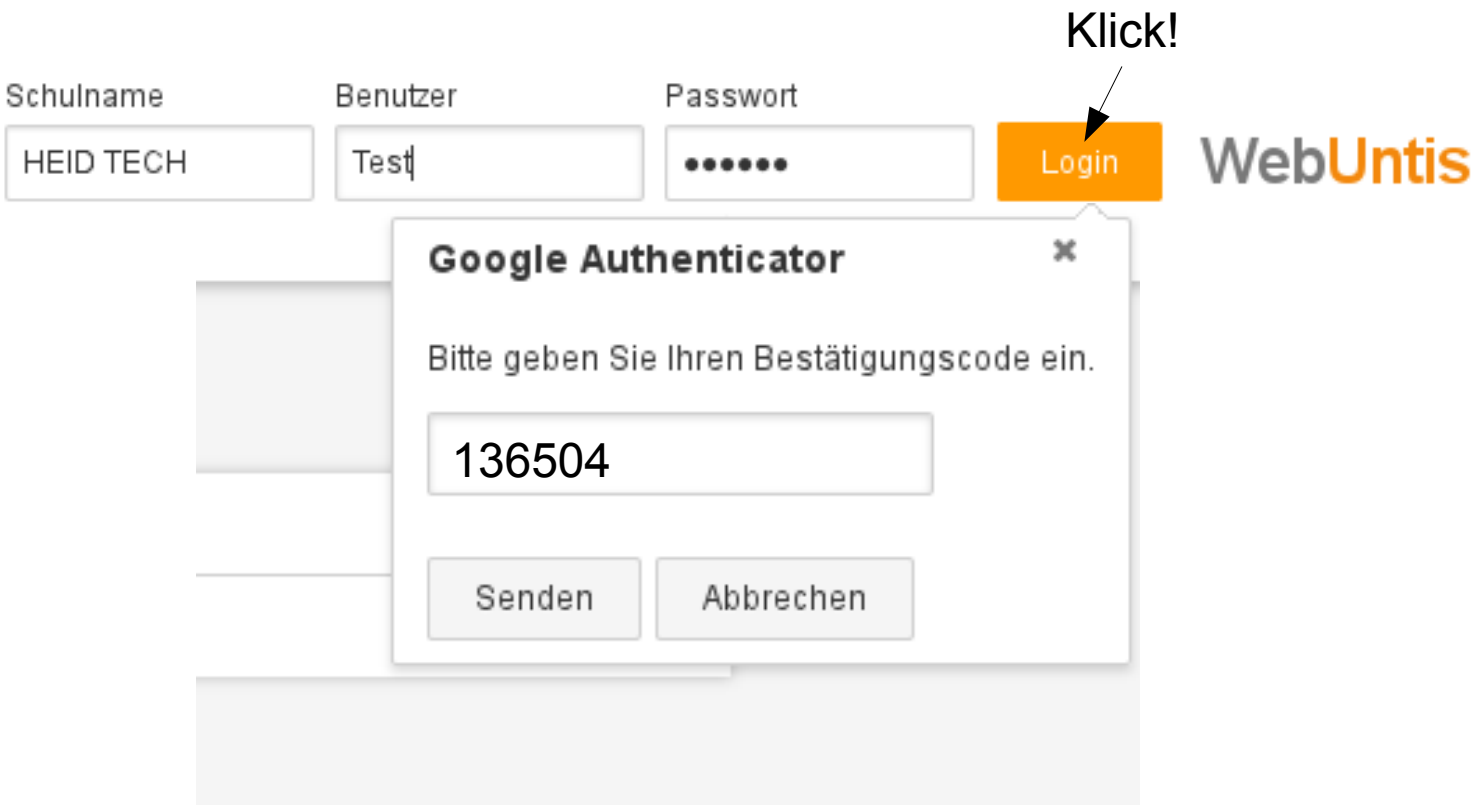


Beispiel → WebUntis



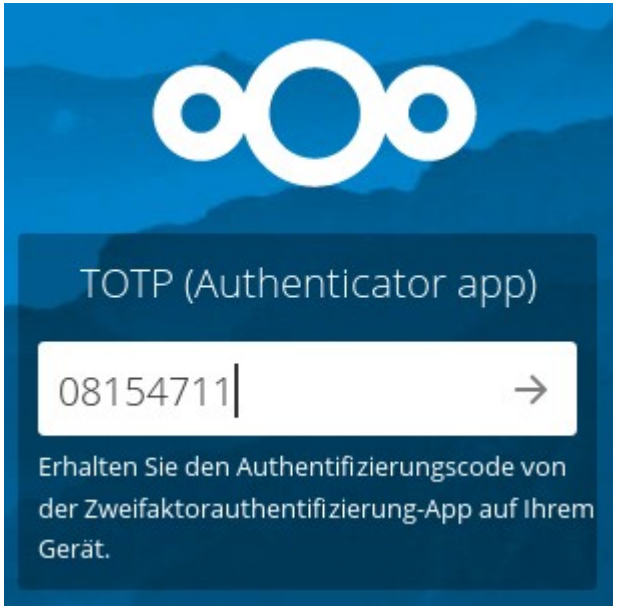
BY-SA

Beispiel → WebUntis → Login



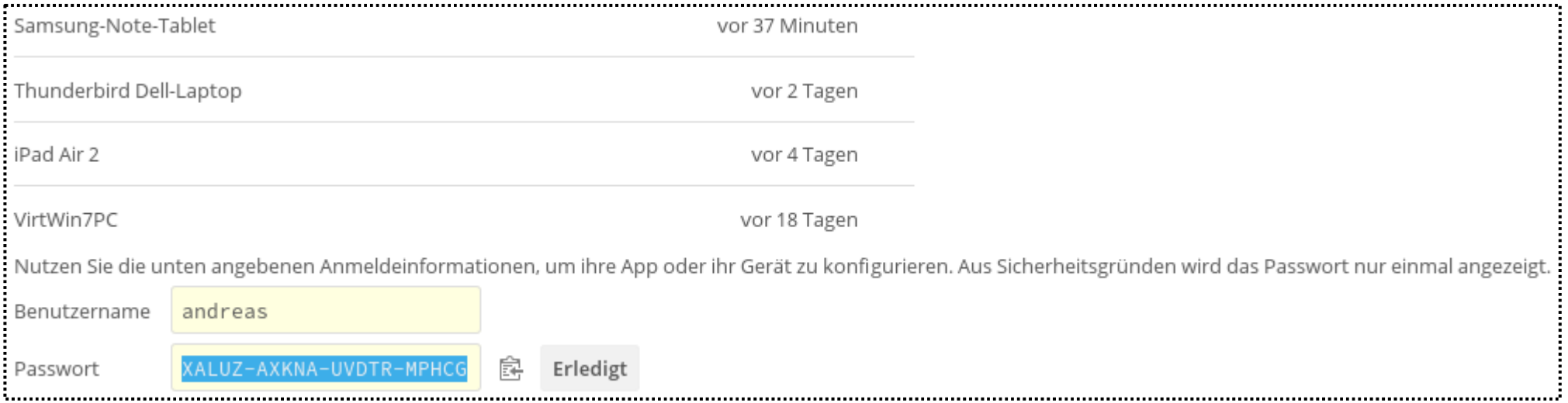
Benötigt hierfür keinerlei Online-Verbindung auf dem 2. Gerät!
Weder Mobilfunk, noch Internet!

Beispiel → Nextcloud 2FA für Weboberfläche



Beispiel → Nexcloud App-Passwort bei aktiver 2FA

Da App‘s auf mobilen Geräten die 2FA ggf. (im allgemeinen) nicht können → App-spezifisches Passwort aktivierbar, das dann keine 2FA benötigt.



Bei Geräte-Verlust, oder Verdacht auf Kompromittierung, können App-Zugänge einzeln gelöscht / neu gesetzt werden!

Weitere Tipps …

- Unbedingt den Shared Key, der Basis für den TOTP-Algorithmus ist, redundant sichern
  - z.B. im Passwort-Save „KeePass“
- Apropos „KeePass“: Über das Plugin „KeeOTP“ kann auch via KeePass das zeitbasierende One-Time-Passwort generiert werden
  - Beachten: Unter Beachtung des Netzbriefs ist zwingend ein zweites Gerät erforderlich!

Vielen Dank, ...

… haben Sie noch Fragen?