



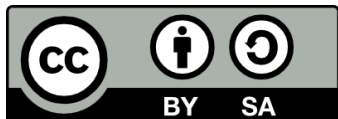
**Landesakademie für Fortbildung und  
Personalentwicklung an Schulen**



**Andreas Grupp**  
grupp@lehrerfortbildung-bw.de

## **Mobiles Lernen mit Tablets**

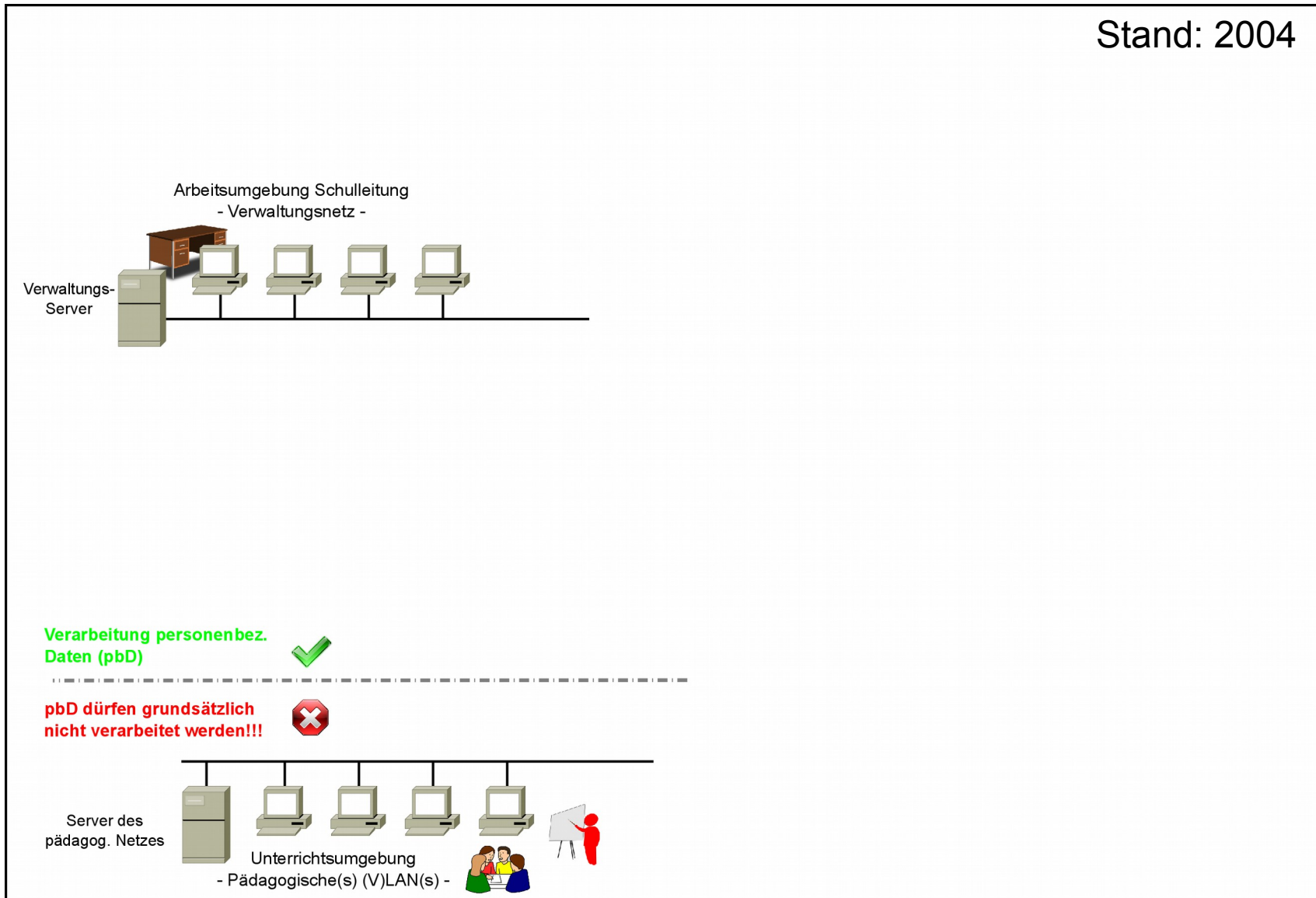
### **Esslingen, 20.10.2015**



„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>

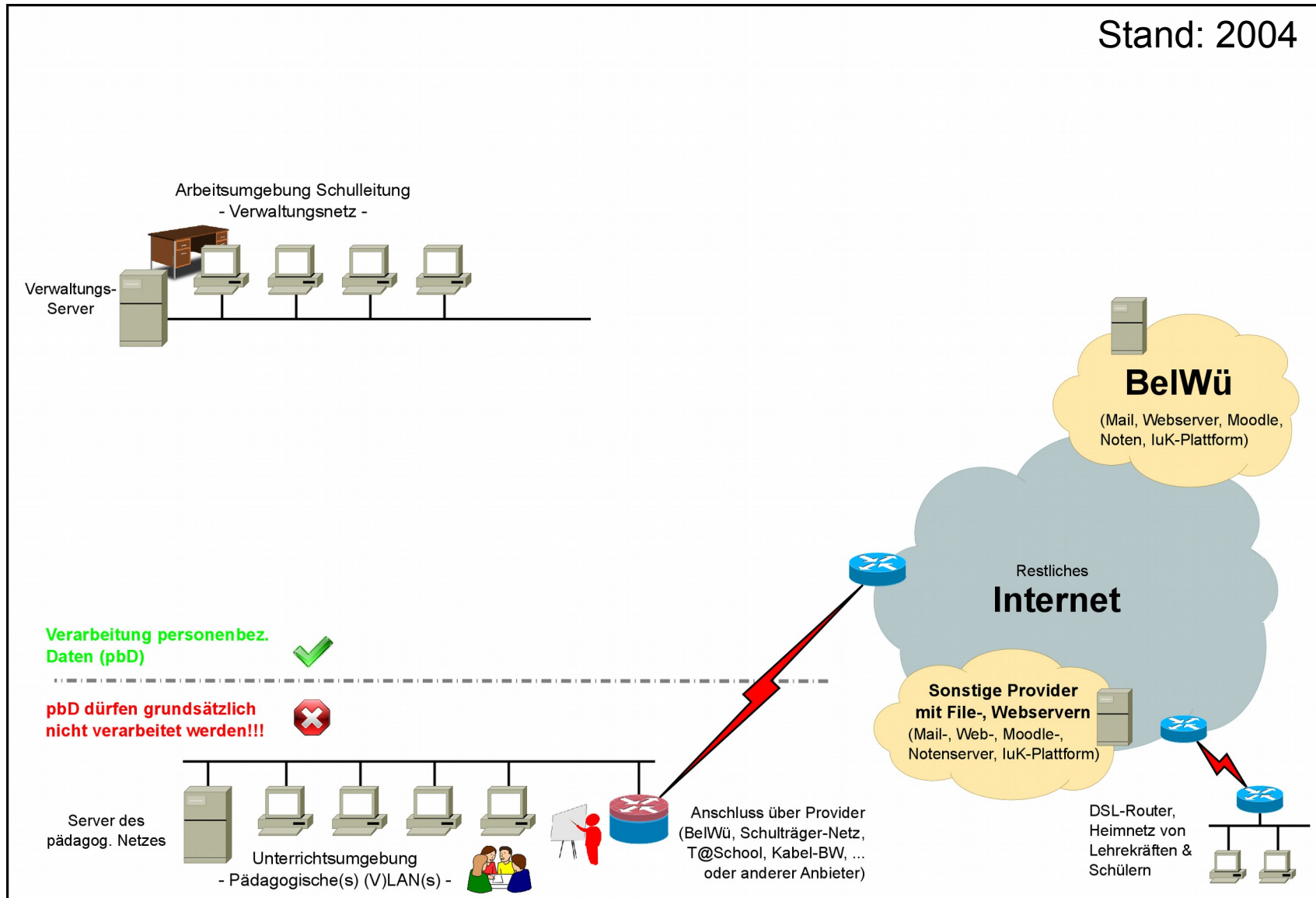


Stand: 2004



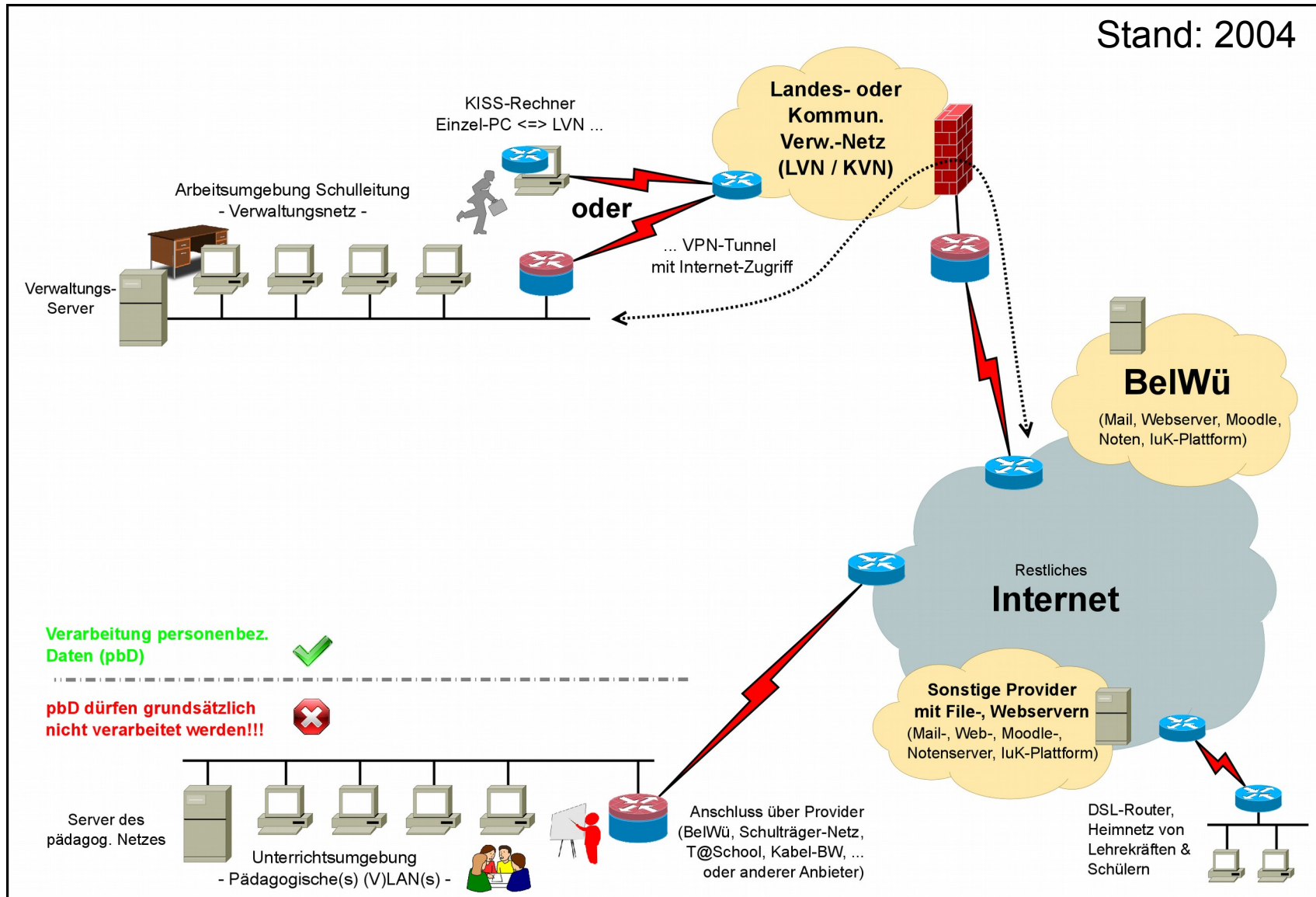


Stand: 2004





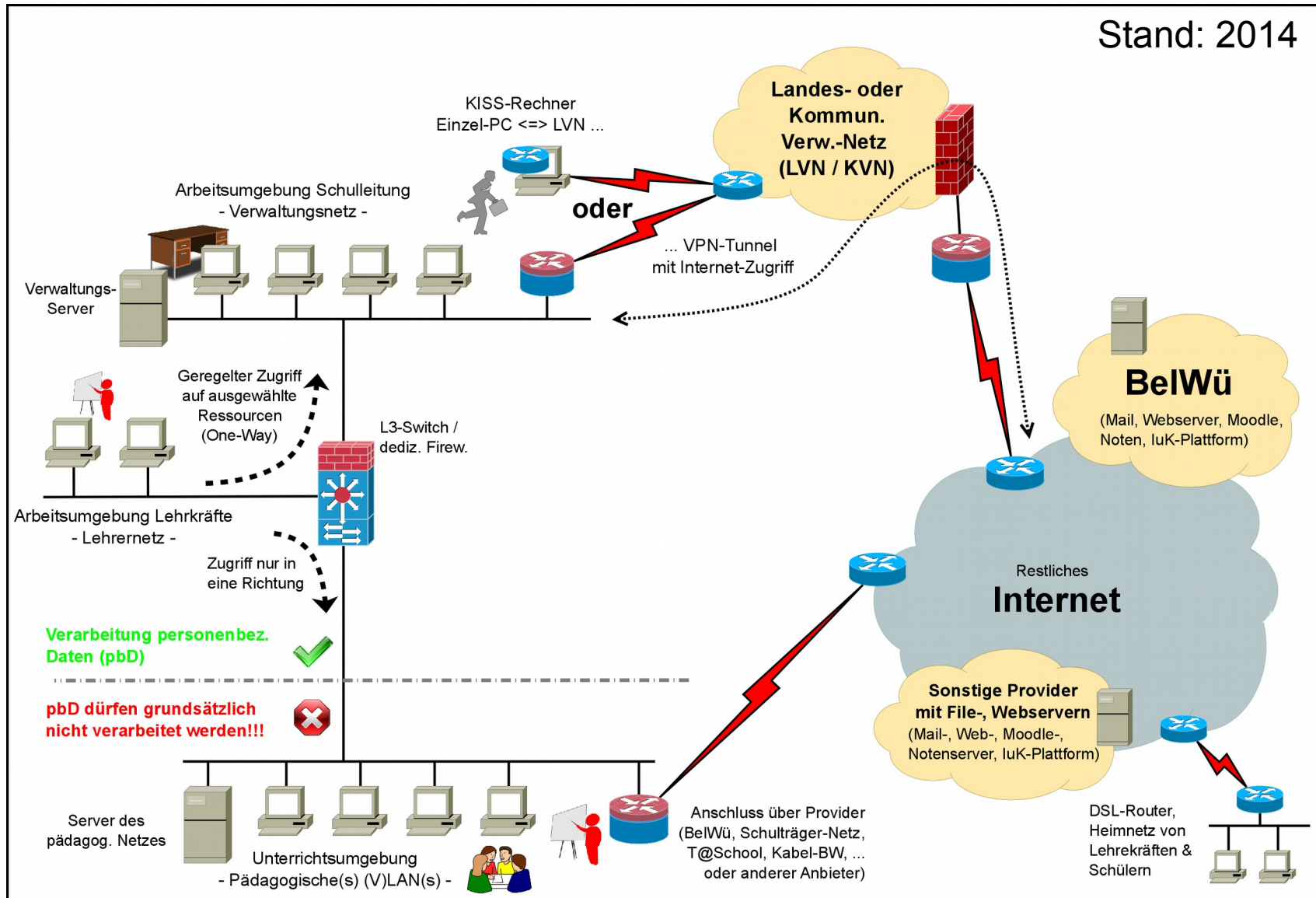
Stand: 2004





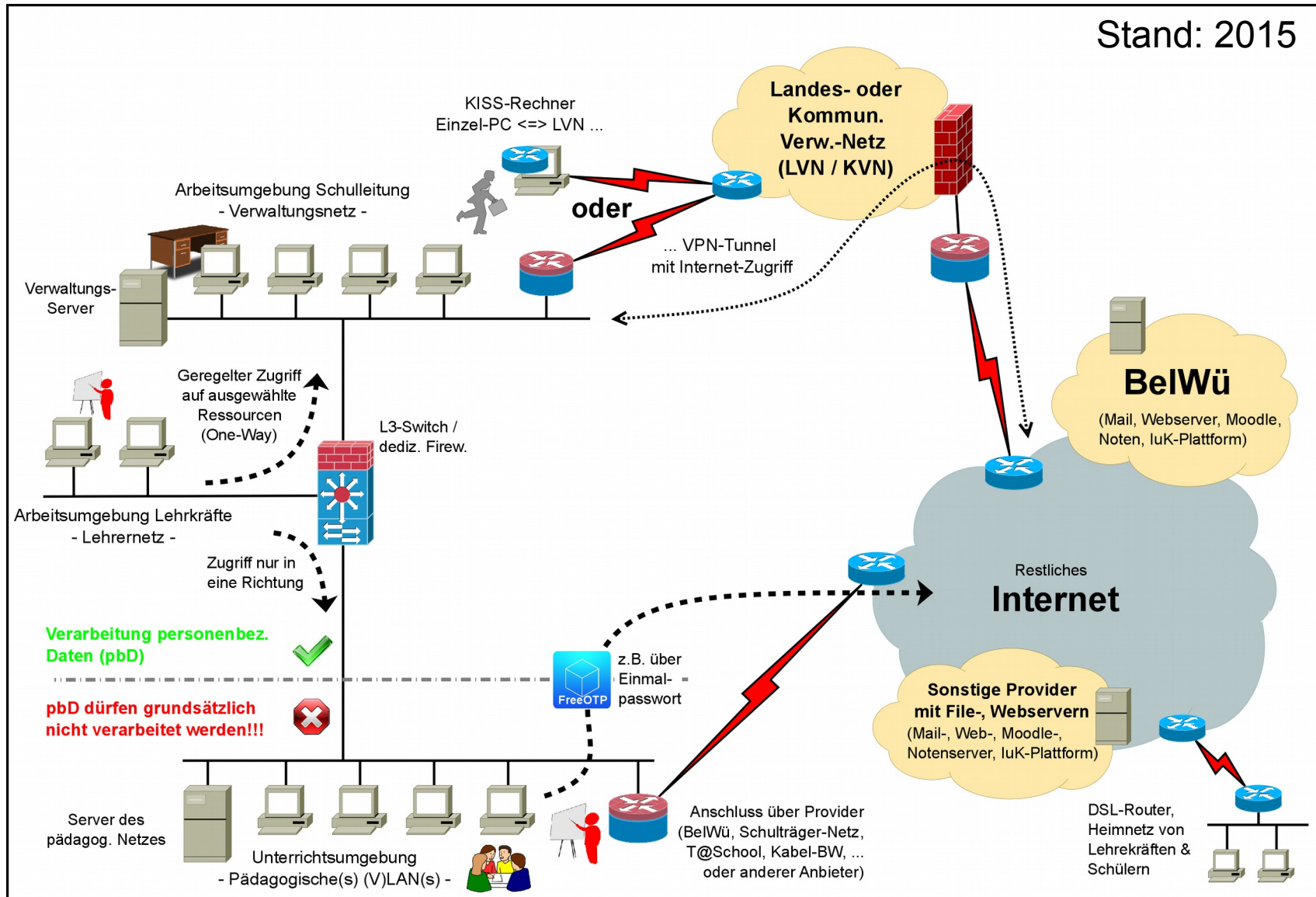


Stand: 2014



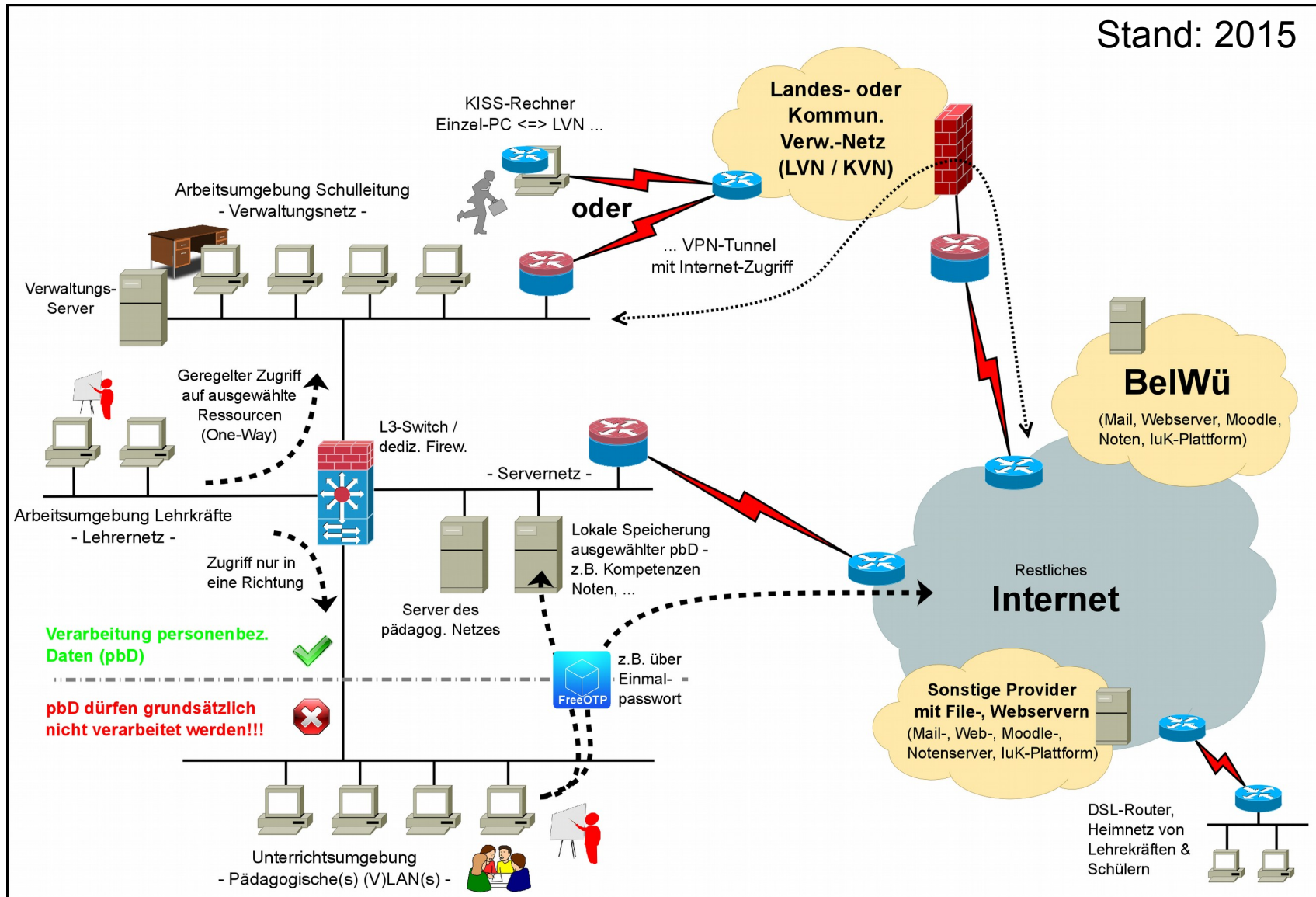


Stand: 2015





Stand: 2015







- **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







## Server

Gibt ein „Geheimnis“ vor

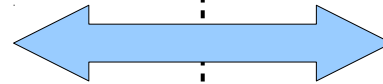
**3EB4G3X5LI7ZKRWS**

## Client

Übernimmt „Geheimnis“

**3EB4G3X5LI7ZKRWS**

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





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

## Server

## Client



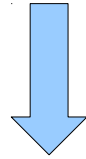
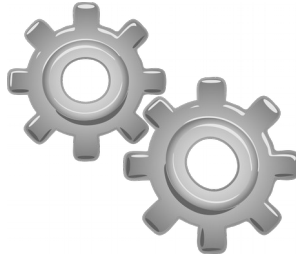
+

3EB4G3X5  
LI7ZKRWS

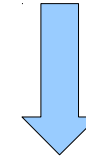
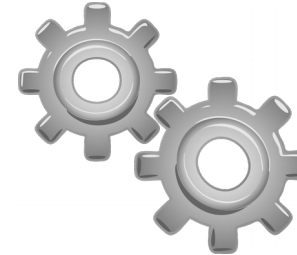


+

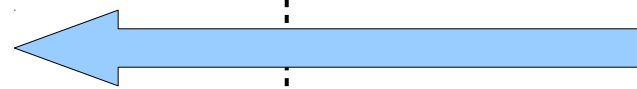
3EB4G3X5  
LI7ZKRWS



640118



640118



**Kommt der Client auf das gleiche Ergebnis?**






- 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





- 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?





1.)  Test (Profil)  Abmelden **WebUntis**

Profil Test x

Allgemein Startseite Freigaben **Sicherheit** 2.)

**Google Authenticator**

Mit Google Authenticator können Sie Ihren Benutzerzugang zusätzlich schützen.

Authenticator ist ein kleines Programm, das Sie auf Ihrem Smartphone installieren können. Es erzeugt einen Code, der beim Anmelden zusätzlich zum Passwort abgefragt wird.

Sie benötigen dafür ein von Google Authenticator unterstütztes Smartphone.

**Google Authenticator aktivieren** 3.)

Speichern Abbrechen





⚙️ Test (Profil)

🔴 Abmelden

WebUntis

Profil Test ✕

Allgemein Startseite Freigaben **Sicherheit**

### Google Authenticator - Aktivierung (1/3)

Bitte installieren Sie die Google Authenticator Anwendung auf Ihrem Smartphone.

Eine Anleitung zur Installation des Authenticators auf Android, iOS oder BlackBerry Geräten finden Sie hier: [Google Authenticator Installation](#).

Im Internet finden Sie auch Apps für Windows Phone.

4.)

Zurück **Weiter** Abbrechen

Speichern Abbrechen



Profil Test

Allgemein Startseite Freigaben **Sicherheit**

### Google Authenticator - Aktivierung (2/3)

Richten Sie Google Authenticator auf Ihrem Smartphone ein, indem Sie entweder den Code auf dieser Seite scannen oder den angezeigten Schlüssel manuell eintragen.

Schlüssel **TP7KIJSNPSLGXHPV**

5.)

6.)

Zurück **Weiter** Abbrechen

Speichern Abbrechen





### Profil Test

Allgemein Startseite Freigaben **Sicherheit**

#### Google Authenticator - Aktivierung (3/3)

Bitte geben Sie den aktuellen Bestätigungscode ein, den Google Authenticator auf Ihrem Smartphone anzeigt. Klicken Sie dann auf 'Aktivieren'.

7.)

8.)



⚙️ Test (Profil)

🔴 Abmelden

WebUntis

Profil Test

Allgemein

Startseite

Freigaben

Sicherheit

## Google Authenticator

Google Authenticator ist aktiviert.

Google Authenticator deaktivieren

Schlüssel anzeigen

9.)

Speichern

Abbrechen



Schulname Benutzer Passwort

HEID TECH Test

.....

**Klick!**

Login WebUntis

**Google Authenticator** x

Bitte geben Sie Ihren Bestätigungscode ein.

136504

Senden Abbrechen



**... haben Sie noch Fragen?**

