Zwei Faktoren für einen sicheren Server – Teil 2

Chemnitzer Linux-Tage 2020

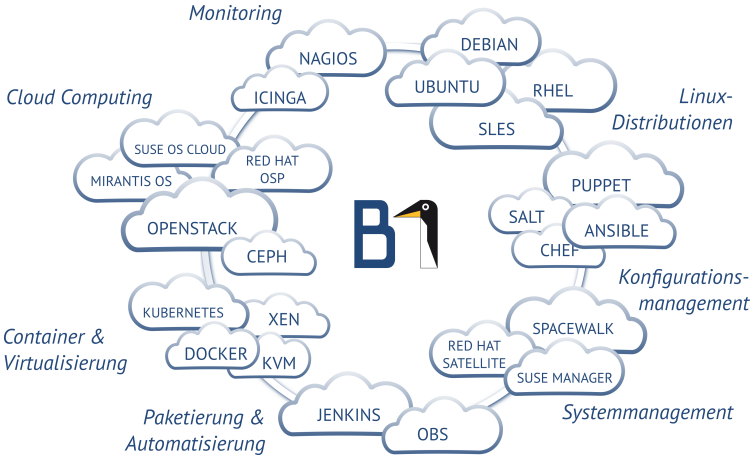
15. März 2020

Florian Winkler
Linux Consultant & Trainer
B1 Systems GmbH
winkler@b1-systems.de

Vorstellung B1 Systems

- gegründet 2004
- Linux/Open Source-Themen
- national & international tätig
- über 140 Mitarbeiter
- unabhängig von Soft- & Hardware-Herstellern
- Leistungsangebot:
  - Beratung & Consulting
  - Support
  - Training
  - Managed Service & Betrieb
  - Lösungen & Entwicklung
- Standorte in Rockolding, Köln, Berlin & Dresden

Schwerpunkte



Zwei Faktoren für einen sicheren Server, Teil Zwei

Worum geht es überhaupt?

- Wir haben einen Server, der für uns eine Web-Applikation bereit stellt, in unserem Beispiel eine Nextcloud.
- Wir wollen diese Nextcloud absichern und Zwei-Faktor-Authentisierung einrichten.
- Wie das geht, zeigen die nächsten 45 Minuten ...

Worum geht es überhaupt?

- Wir haben einen Server, der für uns eine Web-Applikation bereit stellt, in unserem Beispiel eine Nextcloud.
- Wir wollen diese Nextcloud absichern und Zwei-Faktor-Authentisierung einrichten.
- Wie das geht, zeigen die nächsten 45 Minuten ...

Worum geht es überhaupt?

- Wir haben einen Server, der für uns eine Web-Applikation bereit stellt, in unserem Beispiel eine Nextcloud.
- Wir wollen diese Nextcloud absichern und Zwei-Faktor-Authentisierung einrichten.
- Wie das geht, zeigen die nächsten 45 Minuten ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Warum das Ganze?

Einen Server bedrohen viele Gefahren:

- böse Hacker
- Skriptkiddies
- unsichere Dienste
- schwache Passwörter
- automatisierte Scans
- und, und, und ...

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe $\rightarrow$ Zwei-Faktor-Authentisierung (2FA)

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe $\rightarrow$ Zwei-Faktor-Authentisierung (2FA)

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe → Zwei-Faktor-Authentisierung (2FA)

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe → Zwei-Faktor-Authentisierung (2FA)

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe → Zwei-Faktor-Authentisierung (2FA)

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe → Zwei-Faktor-Authentisierung (2FA)

Was tun wir dagegen?

Unter anderem

- nicht benötigte Dienste abschalten, deinstallieren
- nur benötigte Pakte installieren
- `root`-Login verbieten
- Admin-Account besonders schützen
- sichere Passwörter verwenden
- zusätzliche Sicherheitsstufe $\rightarrow$ Zwei-Faktor-Authentisierung (2FA)

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Zwei-Faktor-Authentisierung (2FA)

Mögliche Faktoren sind:

- Passwort
- Kryptografische Schlüssel, z. B. SSH-Keys
- Hardware-Token, z. B. YubiKey
- One-Time-Passwords (OTP)
- Software-Token
- Biometrisches Merkmal, z. B. Fingerabdruck, Face ID
- Schlüssel (physischer Zugang)
- ...

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- ... und jetzt auch wir! ;)

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- ... und jetzt auch wir! ;)

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- ... und jetzt auch wir! ;)

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- ... und jetzt auch wir! ;)

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- ... und jetzt auch wir! ;)

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- . . . und jetzt auch wir! ;)

Webdienste

Beispiele für Web-Dienste, die 2FA unterstützen:

- Google
- Amazon
- Twitter
- GitHub
- Netcup
- ... und jetzt auch wir! ;)

2FA in Nextcloud

- für Nextcloud über entsprechende Apps sehr einfache Möglichkeit, Zwei-Faktor-Authentisierung zu nutzen
- Benutzung selbiger lässt sich für jeden Nutzer einzeln festlegen → Flexibilität
- z. B. je nach Ausstattung des Nutzers unterschiedliche Methoden, oder mehrere für einen Nutzer für mögliches Fallback auf anderes Verfahren
- lässt sich in den Sicherheits-Einstellungen für den jeweiligen Nutzer einrichten

2FA in Nextcloud

- für Nextcloud über entsprechende Apps sehr einfache Möglichkeit, Zwei-Faktor-Authentisierung zu nutzen
- Benutzung selbiger lässt sich für jeden Nutzer einzeln festlegen → Flexibilität
- z. B. je nach Ausstattung des Nutzers unterschiedliche Methoden, oder mehrere für einen Nutzer für mögliches Fallback auf anderes Verfahren
- lässt sich in den Sicherheits-Einstellungen für den jeweiligen Nutzer einrichten

2FA in Nextcloud

- für Nextcloud über entsprechende Apps sehr einfache Möglichkeit, Zwei-Faktor-Authentisierung zu nutzen
- Benutzung selbiger lässt sich für jeden Nutzer einzeln festlegen → Flexibilität
- z. B. je nach Ausstattung des Nutzers unterschiedliche Methoden, oder mehrere für einen Nutzer für mögliches Fallback auf anderes Verfahren
- lässt sich in den Sicherheits-Einstellungen für den jeweiligen Nutzer einrichten

2FA in Nextcloud

- für Nextcloud über entsprechende Apps sehr einfache Möglichkeit, Zwei-Faktor-Authentisierung zu nutzen
- Benutzung selbiger lässt sich für jeden Nutzer einzeln festlegen → Flexibilität
- z. B. je nach Ausstattung des Nutzers unterschiedliche Methoden, oder mehrere für einen Nutzer für mögliches Fallback auf anderes Verfahren
- lässt sich in den Sicherheits-Einstellungen für den jeweiligen Nutzer einrichten

2FA in Nextcloud – Beispiel

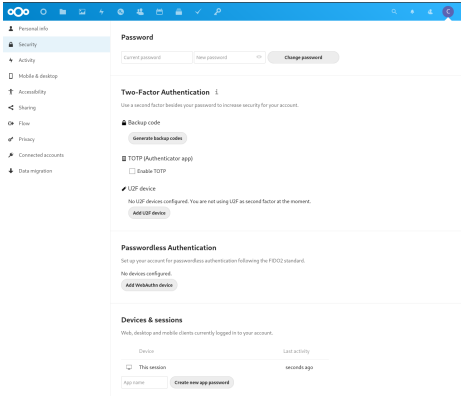


Abbildung: Sicherheits-Einstellungen

OTP-Apps

- verschiedene OTP-Apps für Mobilgeräte, die allesamt ähnlich funktionieren
- in diesem Vortrag: FreeOTP+
  - komplett Open Source
  - über fdroid erhältlich

OTP-Apps

- verschiedene OTP-Apps für Mobilgeräte, die allesamt ähnlich funktionieren
- in diesem Vortrag: FreeOTP+
  - komplett Open Source
  - über fdroid erhältlich

OTP-Apps

- verschiedene OTP-Apps für Mobilgeräte, die allesamt ähnlich funktionieren
- in diesem Vortrag: FreeOTP+
  - komplett Open Source
  - über fdroid erhältlich

OTP-Apps

- verschiedene OTP-Apps für Mobilgeräte, die allesamt ähnlich funktionieren
- in diesem Vortrag: FreeOTP+
  - komplett Open Source
  - über fdroid erhältlich

OTP-App beziehen

Google Play Store

`https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de`

Apple iTunes

`https://itunes.apple.com/de/app/google-authenticator/id388497605?mt=8`

FreeOTP+ (fdroid)

`https://f-droid.org/en/packages/org.liberty.android.freeotpplus`

OTP-App beziehen

Google Play Store

`https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de`

Apple iTunes

`https://itunes.apple.com/de/app/google-authenticator/id388497605?mt=8`

FreeOTP+ (fdroid)

`https://f-droid.org/en/packages/org.liberty.android.freeotpplus`

OTP-App beziehen

Google Play Store

`https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=de`

Apple iTunes

`https://itunes.apple.com/de/app/google-authenticator/id388497605?mt=8`

FreeOTP+ (fdroid)

`https://f-droid.org/en/packages/org.liberty.android.freeotpplus`

OTP-App für Nextcloud 1/3

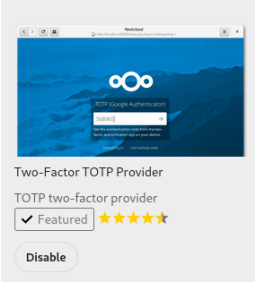


Abbildung: Two-Factor TOTP Provider

Links:

- `https://apps.nextcloud.com/apps/twofactor_totp`
- `https://github.com/nextcloud/twofactor_totp#readme`

OTP-App für Nextcloud 2/3

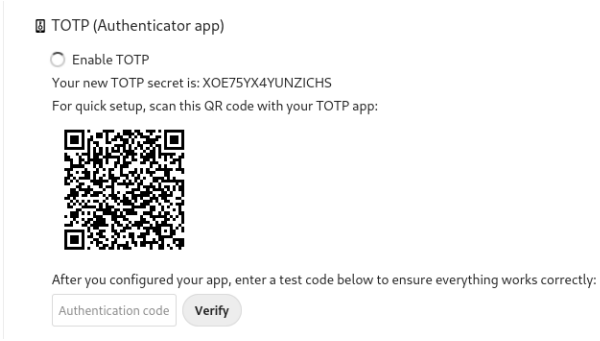


Abbildung: Two-Factor TOTP aktivieren – QR-Code scannen und Code eingeben

OTP-App für Nextcloud 3/3

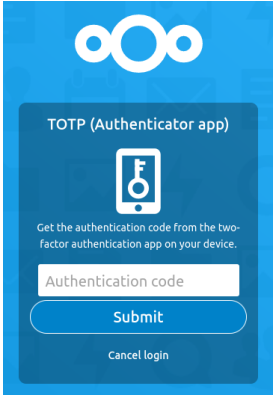


Abbildung: Login mit OTP-App – Code aus der App eingeben

U2F-Token

Abbildung: U2F-Token (Auswahl)

- Auswahl an U2F-Token mittlerweile recht groß
- wohl bekanntester Vertreter: YubiKey
- weitere: Googles Nitrokey, Solokey, verschiedene „No-Name“-Produkte
- ist Benutzung auch mit Handys, Tablets oder Laptops ohne klassischen USB-A Anschluss geplant → darauf achten, dass das Token USB-C oder NFC hat

U2F-Token

Abbildung: U2F-Token (Auswahl)

- Auswahl an U2F-Token mittlerweile recht groß
- wohl bekanntester Vertreter: YubiKey
- weitere: Googles Nitrokey, Solokey, verschiedene „No-Name“-Produkte
- ist Benutzung auch mit Handys, Tablets oder Laptops ohne klassischen USB-A Anschluss geplant → darauf achten, dass das Token USB-C oder NFC hat

U2F-Token

Abbildung: U2F-Token (Auswahl)

- Auswahl an U2F-Token mittlerweile recht groß
- wohl bekanntester Vertreter: YubiKey
- weitere: Googles Nitrokey, Solokey, verschiedene „No-Name“-Produkte
- ist Benutzung auch mit Handys, Tablets oder Laptops ohne klassischen USB-A Anschluss geplant → darauf achten, dass das Token USB-C oder NFC hat

U2F-Token

Abbildung: U2F-Token (Auswahl)

- Auswahl an U2F-Token mittlerweile recht groß
- wohl bekanntester Vertreter: YubiKey
- weitere: Googles Nitrokey, Solokey, verschiedene „No-Name“-Produkte
- ist Benutzung auch mit Handys, Tablets oder Laptops ohne klassischen USB-A Anschluss geplant → darauf achten, dass das Token USB-C oder NFC hat

U2F-Token für Nextcloud 1/3

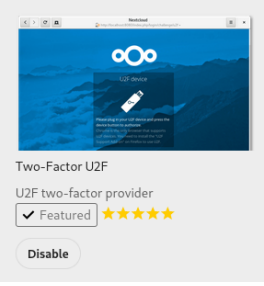


Abbildung: Two-Factor U2F

Links:

- `https://apps.nextcloud.com/apps/twofactor_u2f`
- `https://github.com/nextcloud/twofactor_u2f#readme`

U2F-Token für Nextcloud 2/3

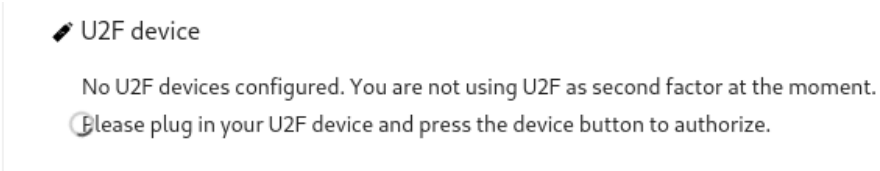


Abbildung: U2F-Token aktivieren

U2F-Token für Nextcloud 3/3

Abbildung: Login mit U2F-Token

Demo-Time

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de oder +49 (0)8457 - 931096