Zweifaktor-Authentifizierung

Juni 2016

Dr. Christopher Kunz, filoo GmbH

Ihr Webinar-Team

filoo®
member of Thomas Krenn Group

_ Referent: Dr. Christopher Kunz
- _ CEO Hosting filoo GmbH / TK AG
- _ Promotion IT Security
- _ Vorträge auf Konferenzen
- _ Autor von Artikeln & Büchern

_ Moderation: Stefanie Jerchel
- _ Marketing Thomas-Krenn.AG
- _ Sammelt Fragen / Feedback

filoo GmbH

member of Thomas Krenn Group

- Wir sind die Hosting-Tochter der Thomas-Krenn.AG
  - Sicheres, hochperformantes Hosting in Frankfurt
  - Mitarbeiter in Gütersloh und Freyung
- Primärer Rechenzentrumsstandort Frankfurt
  - Tier3, ISO 27001
  - Fläche in zwei Brandabschnitten
- Managed Services
  - Planung & Deployment
  - Security Services
  - Systemadministration

Agenda

filoo®
member of Thomas Krenn Group

- Zwei-Faktor-Was?! Einführung
- Übliche Verfahren
- Pro und Contra
- TOTP mit PHP
- SMS-Pin-Codes mit SimpleSMS
- Fragen

Authentiwas?

filoo®
member of Thomas Krenn Group

- Authentisierung
  - Ich lege dem System meine Credentials vor
  - Aktiv: Ich authentisiere mich
- Authentifizierung
  - Das System überprüft meine Credentials
  - Passiv: Ich werde authentifiziert
- Beides engl. Authentication, AuthN
- Autorisierung
  - Engl. Authorization, AuthZ
  - Das System vergibt Berechtigungen an authentisierte Nutzer
  - z.B. Lese/Schreibrechte
  - Passiv: Ich bin autorisiert

Faktorwiewaswo?

filoo®
member of Thomas Krenn Group

- Etwas, das ich habe
  - Smartcard, EC-Karte
  - Hausschlüssel
- Etwas, das ich weiss
  - Paßwort, PIN
  - Versteck des Ersatzschlüssels
- Etwas, das ich bin
  - Fingerabdruck, Iris-Scan
  - Persönliche Bekanntschaft (Notare)

Ein-Faktor-AuthN

filoo®
member of Thomas Krenn Group

- Benutzername und Paßwort eingeben
  - Beides etwas, das ich weiß
- „Ach, Sie kenne ich! Sie dürfen passieren.“
  - Etwas, das ich bin
- Eigenen Haustürschlüssel benutzen
  - Etwas, das ich habe
- Zahlung mit Karte ohne PIN/Unterschrift
  - Etwas, das ich habe
- SSH-Login per SSH-Key
  - Etwas, das ich habe

Zwei-Faktor-AuthN

filoo®
member of Thomas Krenn Group

- Wichtig: Zwei verschiedene Faktoren
- „Etwas, das ich habe“ + „Etwas, das ich habe“ = 1-Faktor-Authentisierung
- “Etwas, das ich habe“ + „Etwas, das ich bin“ = 2-Faktor-Authentisierung

2-Faktor-Auth, ja oder nein?

filoo®
member of Thomas Krenn Group

- EC-Karte + PIN
- EC-Karte + Unterschrift
- SSH-Key + Passphrase
- Fingerabdruck + Unterschrift
- Schlüssel + Iris-Scan
- Username, Paßwort, Sicherheitsfrage
- One-Time-Code + Paßwort
- Was denken Sie?

Drei-Faktor-Auth?

filoo®
member of Thomas Krenn Group

- Kombination von:
  - Etwas, das ich habe
  - Etwas, das ich weiß
  - Etwas, das ich bin

- Beispiele
  - Paßwort + Smartcard + Fingerabdruck
  - PIN + OTP-Code + Iris-Scan
  - EC-Karte + PIN + Personalausweis-Check

- Für webbasierte Systeme schwierig umzusetzen

MFA pro und contra

filoo®
member of Thomas Krenn Group

- Pro
  - Deutlich erhöhte Sicherheit
  - Bei richtiger Implementation schwer knackbar
- Contra
  - Gefahr des Aussperrens (Supportaufwand)
  - Manche Verfahren knackbar
  - Je nach Verfahren: Kosten

MFA einfach + günstig

filoo®
member of Thomas Krenn Group

- Einfachste Verfahren: OTP
  - One-Time Password – einmal verwendbarer (Zahlen-)Code
  - HOTP – HMAC-based OTP
  - TOTP – Time-based OTP
- TOTP ist populärstes Verfahren
  - Variante von HOTP
  - Benötigt halbwegs synchrone Zeit
  - Auch genutzt von filoo!
- Neuer Standard: FIDO U2F

Möglichkeiten für One-time-Codes

- Smart-Cards
- Security-Tokens
  - RSA SecurID
- YubiKey
  - Emuliert verschiedene Verfahren per US
  - Für alle wichtigen OS verfügbar
- FIDO U2F
- Mobile Geräte
  - Smartphone
  - SMS

FIDO U2F

filoo®
member of Thomas Krenn Group

- Standard für „Universal 2nd Factor“
  - Erarbeitet von Google und Yubico
- Zweifaktor-Authentifizierung per USB oder NFC
  - Smartphones mit NFC + App
  - YubiKey o.ä. per USB
- Kryptographisch harte Authentifizierung
  - Challenge-Response mit Signaturen
- Flexible Wahl des 2. Faktors
- Support noch ausbaufähig
  - Derzeit nur in Chrome
  - 3rd Party tools

TOTP in aller Kürze

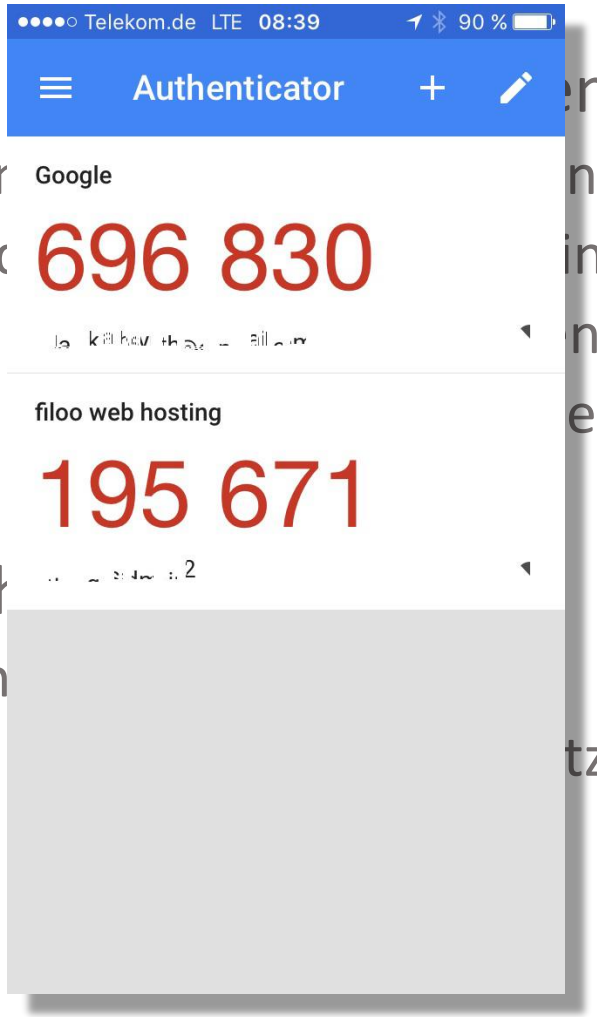
filoo®
member of Thomas Krenn Group

- Es gibt einen geheimen Schlüssel...
- Einen Timestamp (öffentlich!)
- Eine Funktion zur Code-Erzeugung (öffentlich!)
- Heraus kommt: Ein Zahlencode
- Code ändert sich alle X Sekunden (häufig: X=30)
- Überlappung gestattet, um Zeitdifferenzen auszugleichen
- Wer Ihr Paßwort stiehlt, benötigt auch den Zahlencode
- Dieser ist in der kurzen Zeitspanne nicht zu raten

TOTP-Implementationen

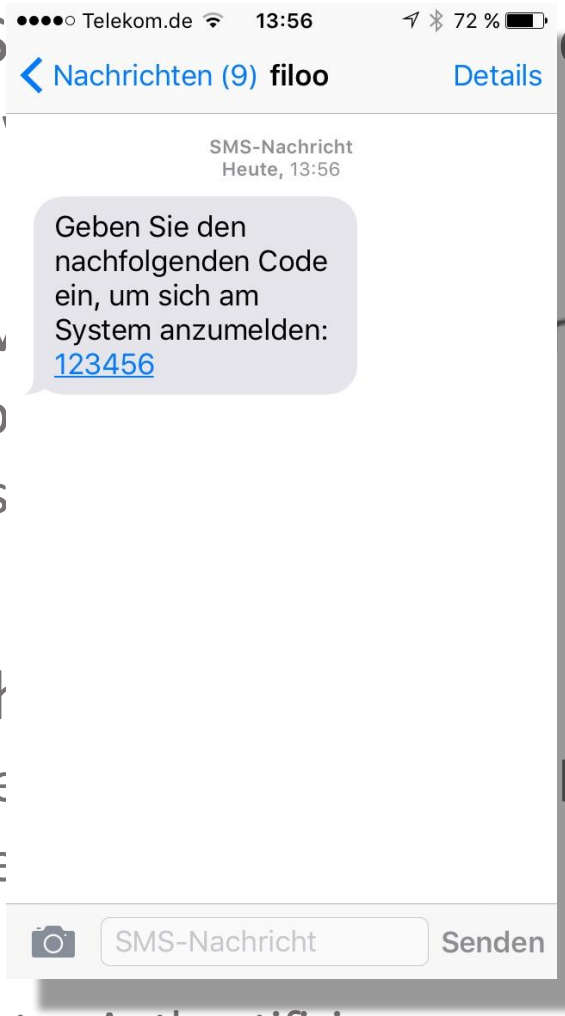
member of Thomas Krenn Group

- Server: z.B. OTP in …en
  - Referenzimplemer… lang
  - OTP-Code als Teil … ins
  - Key-Management … ntierbar
  - Wir können Ihnen … en lassen
- Client: Google Auth…
  - Für alle möglichen …
  - Kann auch für alle … tzt werden
  - Funktioniert ohne …



TOTP per SMS

- Code per SMS an S cken
  - Smartphone = „Et
- Z.B. über SimpleSM pleSMS mobile technology
  - Einfacher Aufruf p
  - https://simplesms
- Mißbrauch möglich
  - US-Carrier erlaube leitung
  - So kann 2FA ausge



Das Aussperr-Problem

filoo®
member of Thomas Krenn Group

- Zweiter Faktor verloren = Nutzer ausgesperrt
- Daher: Immer zusätzliche Möglichkeit anbieten
  - Z.B. Google Authenticator und SMS
- Ansonsten: Erhöhter Supportaufwand

Fazit

filoo®
member of Thomas Krenn Group

_ Mehr-Faktor-Authentisierung erhöht die Sicherheit

_ Recht geringe Kosten

_ Breite Nutzer-Akzeptanz

_ Leicht zu implementieren

Vorschau

filoo®
member of Thomas Krenn Group

_ Nächster Termin voraussichtlich 27.07.2016

_ Ich freue mich auf Ihre Themenvorschläge!

Vielen Dank

filoo®
member of Thomas Krenn Group

_ Ich freue mich auf Ihre Themenvorschläge und Fragen!

_ Kontaktdaten:

- _ E-Mail: chris@filoo.de
- _ Telefon: 05241/86730-0

_ Besuchen Sie filoo!

- _ https://www.filoo.de/
- _ http://twitter.com/filoogmbh