Nutzerzertifikate für die vertrauliche E-Mail-Kommunikation - Umsetzung und Verfahren

Norman Walther

Agenda

- Notwendigkeit digitaler Zertifikate
- Fakten TU-Dresden
- Problemstellung: Zertifikate in die Fläche
- Umsetzung
- Einrichtung
- Abschluss / Ausblick

Notwendigkeit digitaler Zertifikate - Abstract

In der heutigen Zeit ist eine sichere und vertrauliche E-Mail-Kommunikation wichtiger denn je. Bei der Flut an Spam- und Phishing-Mails, die jeden Tag im Postfach landen, ist es wichtig zu wissen, was echt ist und was nicht. Eine E-Mail lässt sich leicht manipulieren und gibt schlimmstenfalls falsche Tatsachen wieder.

Um dieses Problem zu lösen, sollen persönliche Nutzerzertifikate eingesetzt werden. Durch dieses Zertifikat kann sichergestellt werden, dass der Absender einer E-Mail auch tatsächlich die Person ist, für die sie sich ausgibt.

In diesem Vortrag wird die Umsetzung des Prozesses besprochen sowie die großflächige Verbreitung von Nutzerzertifkaten an der TU Dresden, um möglichst viele Personen mit einem persönlichen Zertifikat auszustatten.

Projektname: EVAZert (Einfache Verfahren zur Anwendung von Zertifikaten)

Fakten TU-Dresden

Gliederung:

- 5 Bereiche (je Bereich 1 Bereichsleiter/-in)
    - 17 Fakultäten (mehrere IT-Administrator/-innen je Fakultät)
- Zentrale Universitätsverwaltung (mehrere IT-Administrator/-innen)

Personen:

~ 30.00 Studierende
~ 8.000 Beschäftigte

Problemstellung: Zertifikate in die Fläche

- Vorgaben vom DFN
  - Identitätsprüfung (Merkmale, Gültigkeit)
  - Nur geschultes Personal für Zertifikatsausstellung (jährliche Schulung)
  - Technische Aspekte (Privater Schlüssel,...)

- Organisatorische Probleme
  - Verpflichtung zur Nutzung von Zertifikaten
  - Zertifikate nur für Angestellte
  - Wer führt Identitätsprüfung durch (zusätzlicher Arbeitsaufwand)
  - Dokumentation (Aufbewahrung,....)

- Technische Probleme
  - 2-Faktor Beantragung (PIN-Brief)
  - User-Interface (Self-Service)
  - Zertifikatserzeugung und -aufbewahrung (Speicherfrist)

Umsetzung - Organisatorische Probleme

- Verpflichtung zur Nutzung von Zertifikaten
  - Festlegung in IT-Ordnung zur Nutzung eines digitalen Zertifikats für wissenschaftliches und nicht-wissenschaftliches Personal

- Zertifikate nur für Angestellte
  - Verfahren nur für Angestellte der TU-Dresden (SAP & Personalnummer)

- Wer führt Identitätsprüfung durch (zusätzlicher Arbeitsaufwand)
  - *Initiale Idee Identitätsprüfung im Personaldezernat bei Neueinstellung durchzuführen → gescheitert (Überlastung)*
  - Auslagerung an lokale IT-Admins → dadurch große Anzahl an prüfberechtigten Personen (~60)
  - IT-Admins geben RZ-Login aus und PIN für Zertifikatsbeantragung

- Dokumentation (Aufbewahrung,....)

Umsetzung - Technische Probleme

- 2-Faktor Beantragung (PIN-Brief)
  - Nutzername + Passwort nicht ausreichend
  - Zweiter Faktor notwendig zur Zertifikatsbeantragung (zum Zeitpunkt des Projektes keine großflächige 2FA-Lösung im Einsatz)
  - Nutzer-/in erhält von Admin nach Identitätsprüfung einen PIN-Brief (Hydalampapier, ähnlich wie bei Banken)

- User-Interface (Self-Service)
  - Erweiterung Self-Service-Portal zum Management von Zertifikaten
  - Anmeldung per Nutzername + Passwort + PIN
  - Mitarbeiter-/innen können über Self-Service-Portal komplette Beantragung tätigen sowie Zertifikat abrufen

- Zertifikatserzeugung und -aufbewahrung (Speicherfrist)
  - Zertifikat wird auf einer speziellen Appliance erzeugt
  - Aufbewahrung für 12 Wochen bevor es gelöscht wird (DFN-Policy)

Einrichtung

- Zertifikat wird als PKCS#12 (.p12) bereitgestellt
  - Einfacher Import in Windows-Zertifikatsspeicher

- Teilweise umständliche Einrichtung im E-Mail Programm/Browser

- Einführung der Software „Volksverschlüsselung“ vom Fraunhofer SIT Darmstadt
  - autom. Import & Einrichtung aller gängigen E-Mail Programme und Browser

- Erleichterung für Nutzer in heterogener Struktur

Abschluss / Ausblick

- Bisher ca. ~4500 Zertifikate ausgestellt seit 2019

- Positive Rückmeldung der Mitarbeiter und Admins nach anfänglicher Unsicherheit

- Umstellung Prozess aufgrund von Ablösung DFN durch TCS

- regelmäßige Identitätsprüfung nicht mehr notwendig
  - → nur einmalig bei Einstellung oä. ohne Vorgabe über konkrete Dokumentation
  - → Identitätsprüfung muss nicht von einer speziellen Person durchgeführt werden
  - → Nutzer kann sofort neues Zertifikat erstellen (Vereinfachung Workflow)

Vielen Dank!