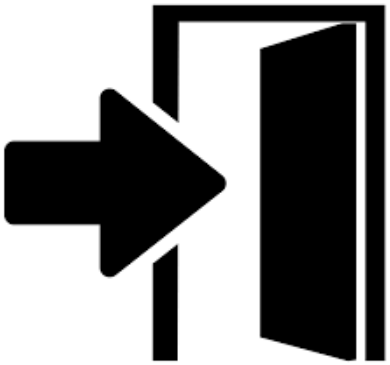
Wie teile ich sichere Passwörter?

Robert Kuhlig

- Geschäftsführer mITSM
  Munich Institute for IT Service Management GmbH
- Lehrbeauftragter der LMU München

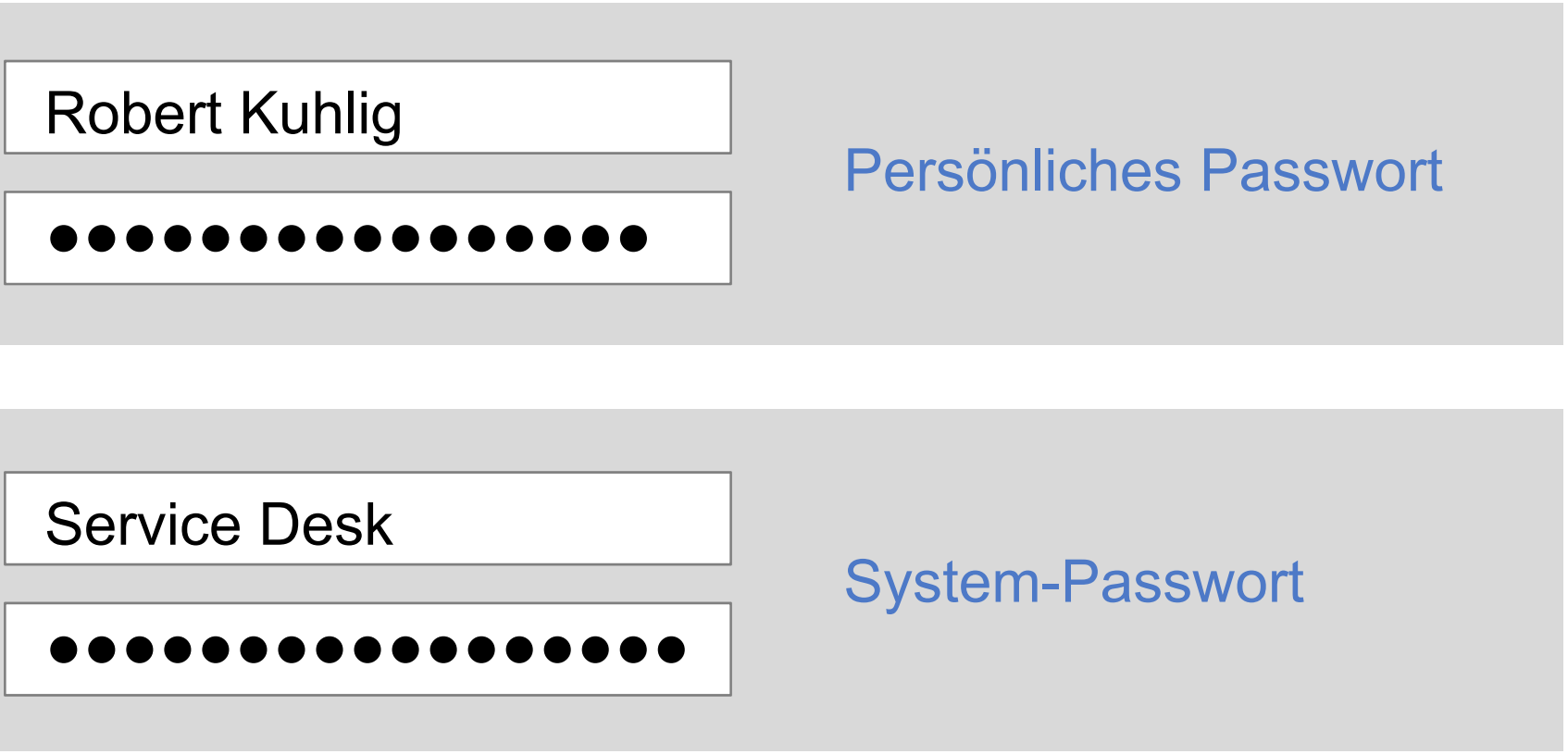
Wozu überhaupt Passwörter?



- Wer darf zugreifen?

- Wer hat zugegriffen?

Welche Passwort-Typen gibt es?



Das sichere Passwort

123456

Q=/!J=u3$bBWR%w//(=MNQ$F(§=VYS)

Empfehlungen des BSI

- Gut zu merken
- Je länger desto besser, mindestens aber 8 Zeichen lang
- Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen nutzen
- Keinen persönlichen Bezug, nicht in Wörterbüchern, keine Tastaturmuster
- Kein Ergänzen simpler Passwörter mit Sonderzeichen oder Zahlen
- Wichtige Passwörter in regelmäßigen Abständen ändern

Bundesamt
für Sicherheit in der
Informationstechnik

Empfehlungen des NIST

- Passphrasen statt Passwörter – Länge geht vor Komplexität
- Phrase darf nicht in Wörterbüchern oder Passwortlisten vorkommen
- Möglichst mit Leerzeichen
- Regelmäßiger Passwortwechsel meist überflüssig - nur bei konkretem Verdacht auf einen Angriff

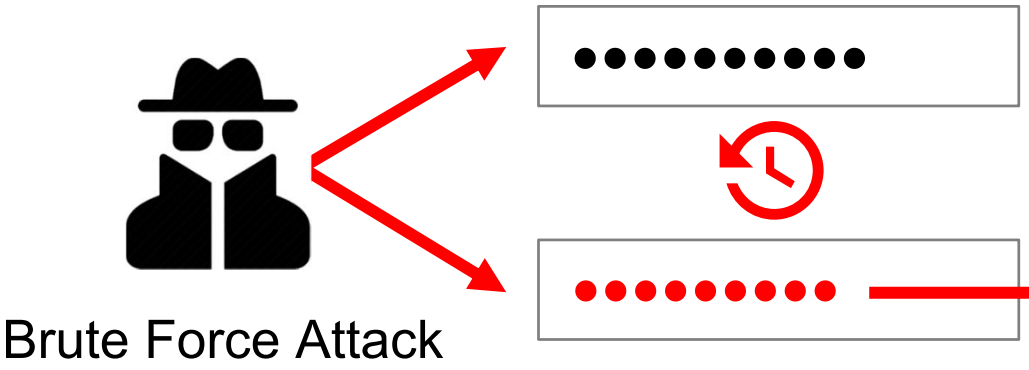
National Institute of
Standards and Technology

Das sichere Passwort

144.555.105.949.057.000 verschiedene Möglichkeiten

10 Stellen aus

52 Zeichen



Brute Force Attack

9 Stellen aus

72 Zeichen

51.998.697.814.229.000 verschiedene Möglichkeiten

Empfehlungen des BSI

- Niemals unverschlüsselt ablegen (Extremfall Zettel am Bildschirm)
- Bei vielen Zugängen einen Passwortmanager nutzen
- Wichtige Passwörter ändern (mind. einmal jährlich und bei Verdacht)
- Dasselbe Passwort nicht für mehrere Zwecke einsetzen
- Voreingestellte Passwörter ändern
- Passwörter nicht an Dritte weitergeben oder per E-Mail versenden

Bundesamt
für Sicherheit in der
Informationstechnik

Passwörter nicht an Dritte weitergeben?

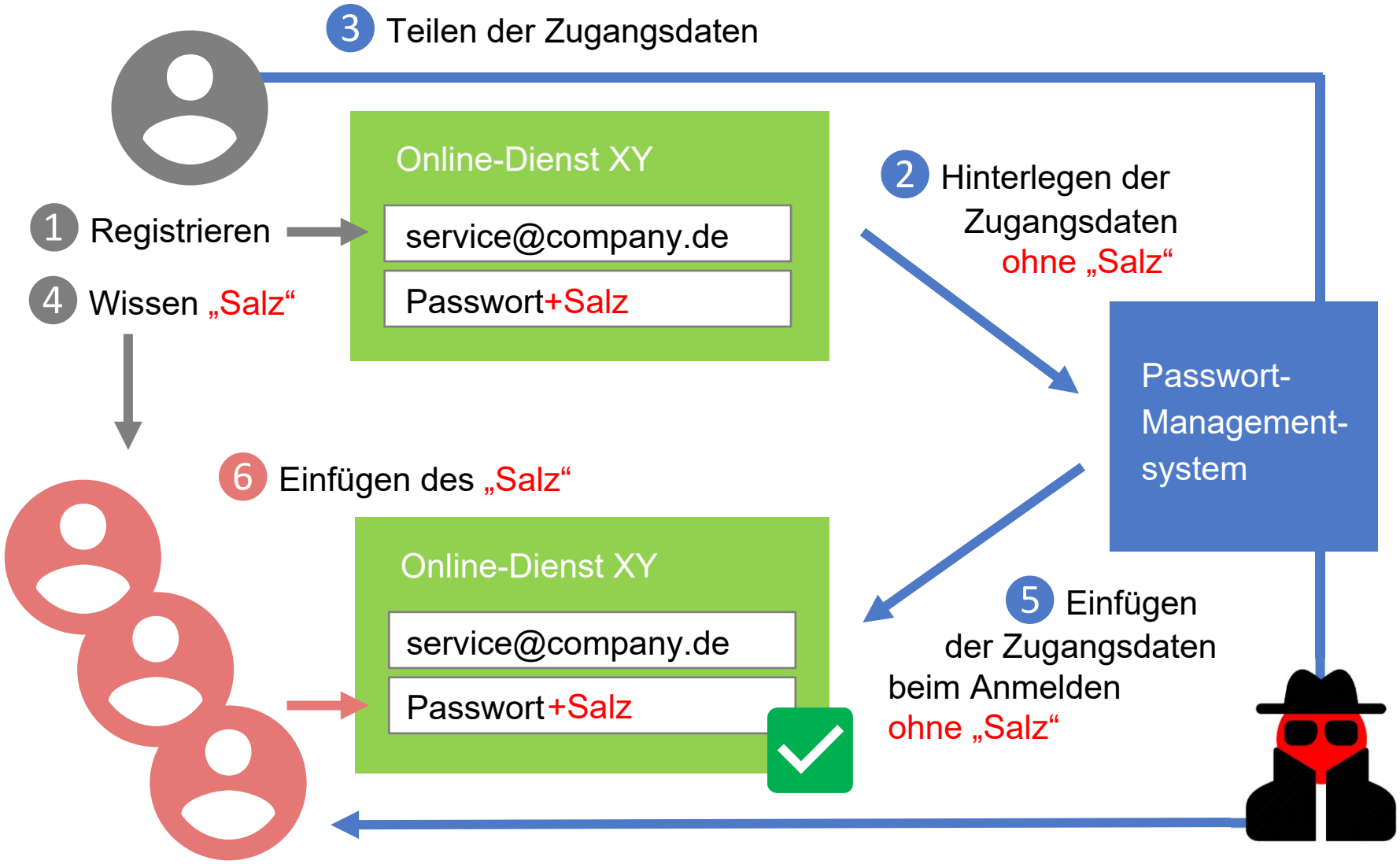
- Geht an der Realität vorbei
- Sichere Prozedur entwickeln, mit der man Passwörter teilen kann

Passwort-Managementsystem

- Speziell für die sichere Verwaltung und das Teilen von Zugängen/PW
- Von IT-Sicherheits-Experten für Nicht-Experten
- Nachweis/Historie: Wer teilt(e) mit wem welche Passwörter?

- Single point of failure: Mit dem Verlust des Master-Passworts können alle verwalteten Passwörter offenliegen.

Sichere Prozedur mit Passwort-Managementsystem



mITSM GmbH

Munich Institute for IT Service Management GmbH
Landaubogen 1
81373 München

Tel.: +49 89 55 27 55 70
Fax: +49 89 55 27 55 71
office@mitsm.de
www.mitsm.de

„Bastelanleitung“ des NIST

Einen Satz, den man sich leicht merken kann, durch ein Muster abwandeln, das nur einem selbst bekannt ist. Satz und Abwandlungs-Schema kann man sich relativ leicht merken, das Resultat wird aber in keiner Passwortliste auftauchen.

passphrasen sind sicher und leicht zu merken

Apassphrasen Bsind Csicher Dund Eleicht Fzu Gmerken!