Password Policies und ppm im OpenLDAP

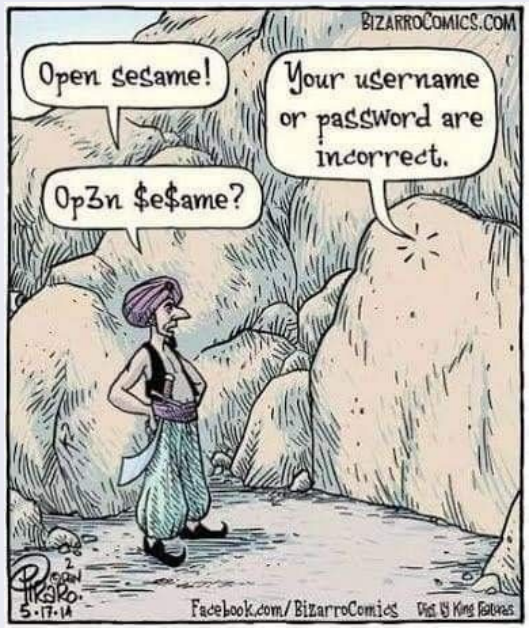
Stefan Kania

3. Juni 2025

SLAC 2025

Stefan Kania
IT-Consulting durch Training

Sichere Passwörter, ein langer, harter Weg



Seit tausenden von Jahren werden Passwörter unterschätzt

Wie sollten Passwörter sein? Aus Admin Sicht

Wie sollten Passwörter sein? Aus Admin Sicht

- ☞ Möglichst lang

Wie sollten Passwörter sein? Aus Admin Sicht

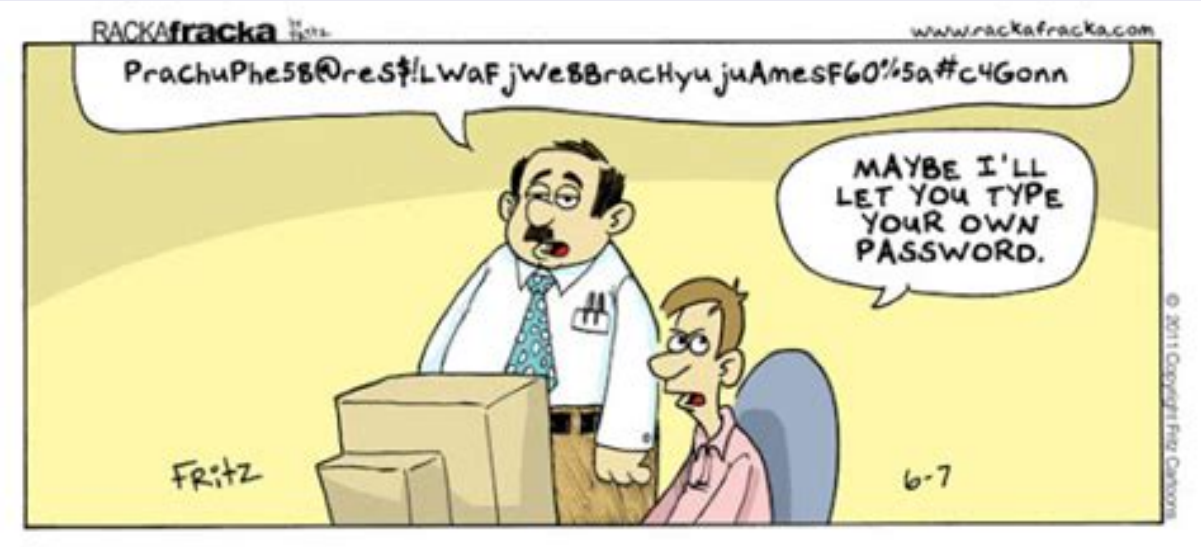
- Möglichst lang
- Möglichst komplex

Wie sollten Passwörter sein? Aus Admin Sicht

- Möglichst lang
- Möglichst komplex
- Keine Wörter

Wie sollten Passwörter sein? Aus Admin Sicht

- Möglichst lang
- Möglichst komplex
- Keine Wörter



Wie hätten es die Mitarbeiter gerne?

Wie hätten es die Mitarbeiter gerne?

- ☞ Einfach zu merken

Wie hätten es die Mitarbeiter gerne?

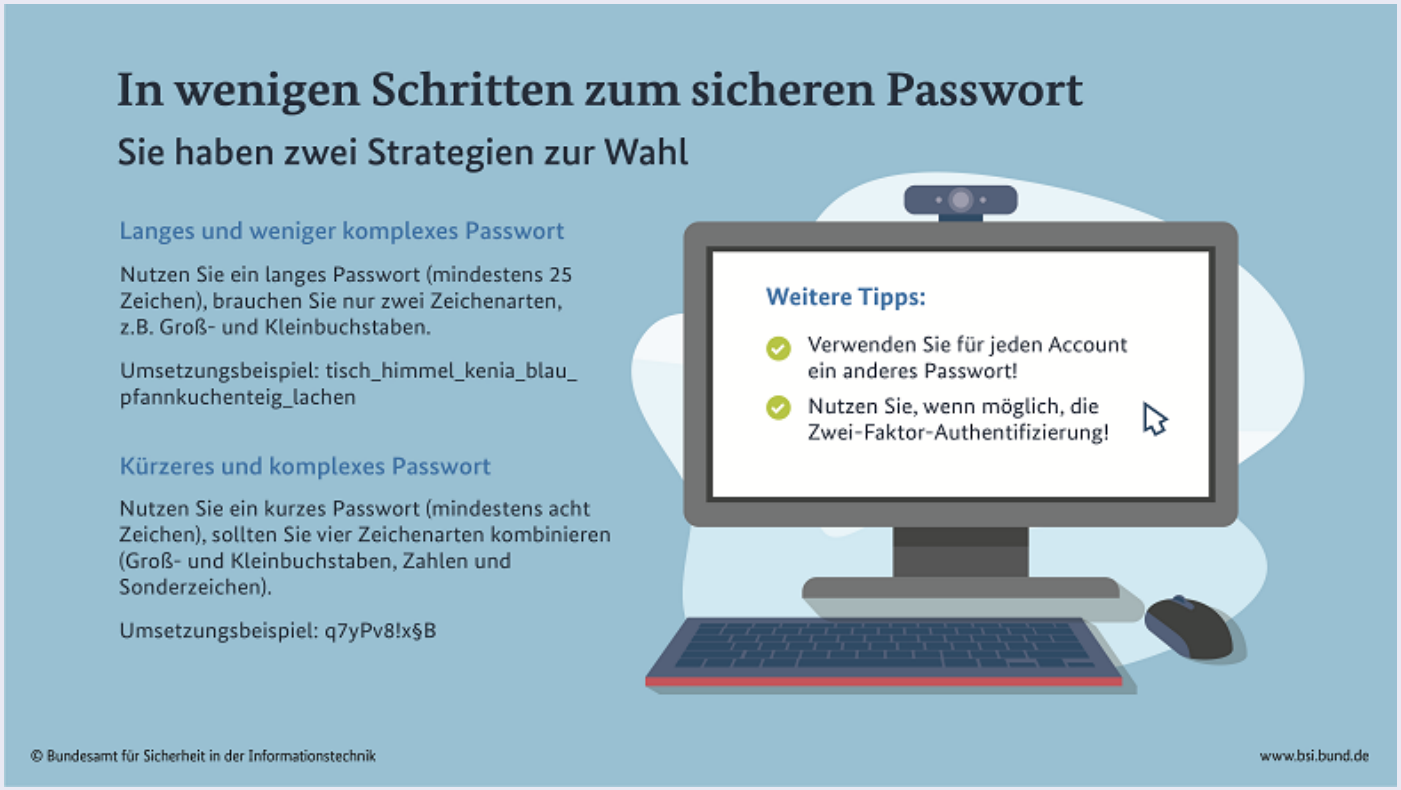
- Einfach zu merken
- Kurz

Wie hätten es die Mitarbeiter gerne?

- Einfach zu merken
- Kurz

Was sagt das BSI dazu?

Was sagt das BSI dazu?



Brute-Force Angriffe auf Passwörter

Brute-Force Angriffe auf Passwörter

Die Zeit, die ein Hacker benötigt, um dein Passwort mittels einer Brute-Force-Attacke zu ermitteln 2025

12 x RTX 5090 | bcrypt (10)

Passwortlänge (Zeichen)	nur Zahlen	nur Kleinbuchstaben	Klein- & Großbuchstaben	Zahlen und Klein-/Großbuchstaben	Zahlen Klein-/Großbuchstaben, und Symbole
4	Sofort	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	57 Minuten	2 Stunden	4 Stunden
6	Sofort	46 Minuten	2 Tage	6 Tage	2 Wochen
7	Sofort	20 Stunden	4 Monate	1 Jahr	2 Jahre
8	Sofort	3 Wochen	15 Jahre	62 Jahre	164 Jahre
9	2 Stunden	2 Jahre	791 Jahre	3k Jahre	11k Jahre
10	1 Tag	40 Jahre	41k Jahre	238k Jahre	803k Jahre
11	1 Woche	1k Jahre	2 Mio Jahre	14 Mio Jahre	56 Mio Jahre
12	3 Monate	27k Jahre	111 Mio Jahre	917 Mio Jahre	3 Mrd Jahre
13	3 Jahre	705k Jahre	5 Mrd Jahre	56 Mrd Jahre	275 Mrd Jahre
14	28 Jahre	18 Mio Jahre	300 Mrd Jahre	3 Bio Jahre	19 Bio Jahre
15	284 Jahre	477 Mio Jahre	15 Bio Jahre	218 Bio Jahre	1 Brd Jahre
16	2k Jahre	12 Mrd Jahre	812 Bio Jahre	13 Brd Jahre	94 Brd Jahre
17	28k Jahre	322 Mrd Jahre	42 Brd Jahre	840 Brd Jahre	6 Trio Jahre
18	284k Jahre	8 Bio Jahre	2 Trio Jahre	52 Trio Jahre	463 Trio Jahre

Hive Systems › hivesystems.com/password

Möglichkeiten zur Passwortverwaltung im OpenLDAP

Möglichkeiten zur Passwortverwaltung im OpenLDAP

- ☞ Hohe Sicherheit durch die Verwendung von *ARGON2* als Passworthash

Möglichkeiten zur Passwortverwaltung im OpenLDAP

- Hohe Sicherheit durch die Verwendung von *ARGON2* als Passworthash
- Passwortrichtlinien durch dass Overlay *ppolicy*

Möglichkeiten zur Passwortverwaltung im OpenLDAP

- Hohe Sicherheit durch die Verwendung von *ARGON2* als Passworthash
- Passwortrichtlinien durch dass Overlay *ppolicy*
- Komplexe Passwörter mit dem *Password Policy Modul (ppm)*

ARGON2 Passworthash

ARGON2 Passworthash

- ☞ Sicher gegen Angriffe mit spezialisierter Hardware (custom hardware attacks)GPUs

ARGON2 Passworthash

- Sicher gegen Angriffe mit spezialisierter Hardware (custom hardware attacks)GPUs
- Argon2 verwendet große Vektoren im Arbeitsspeicher

ARGON2 Passworthash

- Sicher gegen Angriffe mit spezialisierter Hardware (custom hardware attacks)GPUs
- Argon2 verwendet große Vektoren im Arbeitsspeicher
- Benötigter Speicher kann angegeben werden default 4096 KiB

ARGON2 Passworthash

- Sicher gegen Angriffe mit spezialisierter Hardware (custom hardware attacks)GPUs
- Argon2 verwendet große Vektoren im Arbeitsspeicher
- Benötigter Speicher kann angegeben werden default 4096 KiB
- Anzahl der Iterationen kann gewählt werden default 3

ARGON2 Passworthash

- Sicher gegen Angriffe mit spezialisierter Hardware (custom hardware attacks)GPUs
- Argon2 verwendet große Vektoren im Arbeitsspeicher
- Benötigter Speicher kann angegeben werden default 4096 KiB
- Anzahl der Iterationen kann gewählt werden default 3
- Mehr unter: https://de.wikipedia.org/wiki/Argon2

Overlay ppolicy

Overlay ppolicy

- Ablaufwarnung

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen
- Anzahl der Fehlversuche bis zur Sperrung

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen
- Anzahl der Fehlversuche bis zur Sperrung
- Zeit bis zur Zurücksetzung der Fehlversuche

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen
- Anzahl der Fehlversuche bis zur Sperrung
- Zeit bis zur Zurücksetzung der Fehlversuche
- maximales und minimales Kennwortalter

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen
- Anzahl der Fehlversuche bis zur Sperrung
- Zeit bis zur Zurücksetzung der Fehlversuche
- maximales und minimales Kennwortalter
- Kennwortlänge

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen
- Anzahl der Fehlversuche bis zur Sperrung
- Zeit bis zur Zurücksetzung der Fehlversuche
- maximales und minimales Kennwortalter
- Kennwortlänge
- erzwungen Kennwortänderung

Overlay ppolicy

- Ablaufwarnung
- Grace logins nach abgelaufenem Passwort
- Passwort History
- Sperre bei zu vielen falschen Anmeldeversuchen
- Anzahl der Fehlversuche bis zur Sperrung
- Zeit bis zur Zurücksetzung der Fehlversuche
- maximales und minimales Kennwortalter
- Kennwortlänge
- erzwungen Kennwortänderung
- Unterschiedlichen Policies für verschiedene Gruppen

Das password policy module (ppm)

Das password policy module (ppm)

- Neu in OpenLDAP 2.5

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert
- Vorkommen der Buchstaben kann genau beschränkt werden

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert
- Vorkommen der Buchstaben kann genau beschränkt werden
- Umfassende Regeln für die Wiederholung von Zeichen in Passwörtern

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert
- Vorkommen der Buchstaben kann genau beschränkt werden
- Umfassende Regeln für die Wiederholung von Zeichen in Passwörtern
- Cracklib kann eingebunden werden

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert
- Vorkommen der Buchstaben kann genau beschränkt werden
- Umfassende Regeln für die Wiederholung von Zeichen in Passwörtern
- Cracklib kann eingebunden werden
- Eigene Wortlisten können genutzt werden

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert
- Vorkommen der Buchstaben kann genau beschränkt werden
- Umfassende Regeln für die Wiederholung von Zeichen in Passwörtern
- Cracklib kann eingebunden werden
- Eigene Wortlisten können genutzt werden
- Zu komplexe Regeln können die Änderung fast unmöglich machen

Das password policy module (ppm)

- Neu in OpenLDAP 2.5
- Noch komplexere Regeln für Passwörter
- Bei Verwendung wird das ppolicy-Overlay übersteuert
- Vorkommen der Buchstaben kann genau beschränkt werden
- Umfassende Regeln für die Wiederholung von Zeichen in Passwörtern
- Cracklib kann eingebunden werden
- Eigene Wortlisten können genutzt werden
- Zu komplexe Regeln können die Änderung fast unmöglich machen
- Unterschiedliche Regeln für unterschiedliche Gruppen

Wie funktioniert´ es?

Wie funktioniert´ es?