

Kennwortrichtlinien vs. Passwort Compliance



Stephan Halbmeier
Product Specialist | Outpost24



OUTPOST24 - Größter Europäischer Anbieter für Cyber-Security-Assessment Lösungen



Vulnerability
Management

Application &
Network Security

Penetration
Testing



Cyber Threat
Intelligence



External Attack
Surface
Management



Password Security

Self-Service
Password
Management

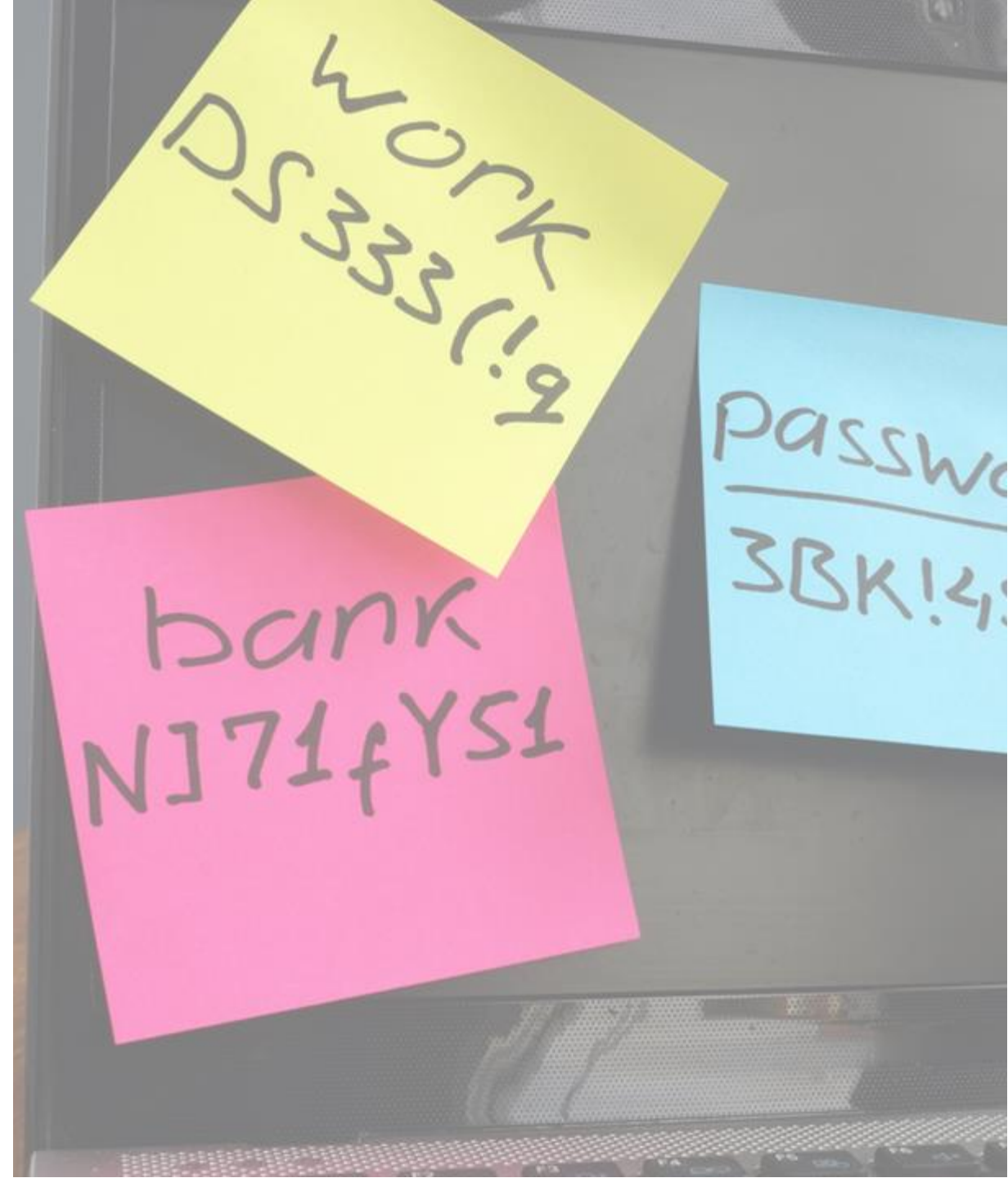
Regulatorische Anforderungen und Empfehlungen

Wer	Maßnahme
DS-GVO	„Unter Berücksichtigung des Standes der Technik ...treffen der Verantwortliche...geeignete TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten...”
BSI IT-Grundschutz	○ „Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden.“ ○ „Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.“ ○ IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern.
NIST	“Password length has been found to be a primary factor in characterizing password strength.”
CIS	“Teaching users techniques like passphrases will result in longer, more secure passwords.”

Was sind schwache Kennwörter?

Kandidat 1	Ferien1!	95/8
Kandidat 2	sommeruniversumvenus	26/20
Kandidat 3	DHZlplkö3457+#!?GHKU	95/20

- 1) Alle Kennwörter sind angemessen stark
- 2) Alle Kennwörter sind gleich schwach
- 3) Kandidat 1 ist das schwächste Kennwort
- 4) Kandidat 2 ist das schwächste Kennwort
- 5) Kandidat 3 ist das schwächste Kennwort



Password Hash Brutforce Theorie & Praxis

```
(tester@demowkst4)-[~]
$ john --incremental --min-len=8 --max-len=8 --format=RAW-MD4 hashlist-md4-95-8 --fork=4 --mask=?u?w
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 256/256 AVX2 8x3])
Node numbers 1-4 of 4 (fork)
Press 'q' or Ctrl-C to abort, almost any other key for status
1 0g 0:00:00:40 0.00% (ETA: 2023-08-02 23:22) 0g/s 41499Kp/s 41499Kc/s 41499KC/s Gspbloot..Rspblot7
4 0g 0:00:00:40 0.00% (ETA: 2023-08-04 09:22) 0g/s 41040Kp/s 41040Kc/s 41040KC/s Wm0m20rt..Mm0m21rl
3 0g 0:00:00:40 0.00% (ETA: 2023-08-04 03:24) 0g/s 41120Kp/s 41120Kc/s 41120KC/s Hl007cd6..El007ckz
2 0g 0:00:00:40 0.00% (ETA: 2023-08-04 01:40) 0g/s 41143Kp/s 41143Kc/s 41143KC/s Tkh2bnmj..Fkh2bnel
Ferien1!      (?)
2 1g 0:00:01:54 DONE (2023-03-29 09:52) 0.008755g/s 37191Kp/s 37191Kc/s 37191KC/s Aerien15..Yerien0x
3 0g 0:00:02:00 DONE (2023-03-29 09:52) 0g/s 37664Kp/s 37664Kc/s 37664KC/s H1aa2k1d..E1aa2k30
4 0g 0:00:02:00 DONE (2023-03-29 09:52) 0g/s 37613Kp/s 37613Kc/s 37613KC/s In0m42ts..Un0m46nn
1 0g 0:00:02:00 DONE (2023-03-29 09:52) 0g/s 37812Kp/s 37812Kc/s 37812KC/s Llsocz8q..Klsocznc
Waiting for 3 children to terminate
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```




BlueLiv Threat Compass Credential Module

Empfehlungen für starke Passwörter

- Passwörter müssen lang sein – Führen Sie Passphrasen ein!
- Passwörter brauchen nicht komplex zu sein!
- Privilegierte Konten mindestens 15 Zeichen!
- Validieren Sie Kennwörter gegen Listen mit kompromittierten Passwörtern!
- Blockieren Sie einfach zu erratene Kennwörter durch Wortlisten!
- Unterschiedliche Regeln für Standard- und Admin Accounts!
- Lassen Sie Passwörter ablaufen!



Warum sind schwache Passwörter ein Sicherheitsrisiko?

Gesundheit Nord bestätigt Cyber-Angriff und Datenabfluss

Die Bremer Kliniken im "Gesundheit Nord"-Verband sind Opfer eines Cyber-Angriffs geworden, bestätigt der Verband jetzt. Es sind Daten abgeflissen.

Lesezeit: 3 Min.  In Pocket speichern

   25



(Bild: Daniel Jedzura/Shutterstock.com)

Cyber-Attacke über SolarWinds: Angreifer hatten Zugriff auf Microsoft-Quellcode

Microsoft hat eingeräumt, dass die Angreifer im Fall SolarWinds sehr tief in die konzerninternen Netzwerke eingedrungen und bis zum Quellcode gelangt sind.

Lesezeit: 4 Min.  In Pocket speichern

   262



(Bild: Panuwatccn/Shutterstock.com)



Specops Password Auditor



Specops Password Policy



Fragen & Antworten

Vielen Dank für Ihre Aufmerksamkeit

Für weitere Fragen zum Thema: <https://specopssoft.com/de/kontakt/>

Produkt-Demo: <https://specopssoft.com/de/produkte/specops-password-policy/>

E-Mail: stephan.halbmeier@specopssoft.com

LinkedIn: <https://www.linkedin.com/in/stephanhalbmeier>

