
SPECOPS

Specops Password Security Software

Specops Software ist der führende Anbieter von Passwort Management – und Authentifizierungslösungen. Wir schützen Geschäftsdaten, in dem wir schwache Passwörter blockieren und die Benutzerauthentifizierung sichern.

Worum geht es heute?

1. **WARUM** sind schwache Passwörter ein Problem?
2. **WAS** kann dagegen unternommen werden?
3. **WIE** sähe eine Lösung im Detail aus?

Erhöhung der Passwortsicherheit in Unternehmen

Stephan Halbmeier
Produkt Spezialist

Specops Software

Berlin, 04.11.2020

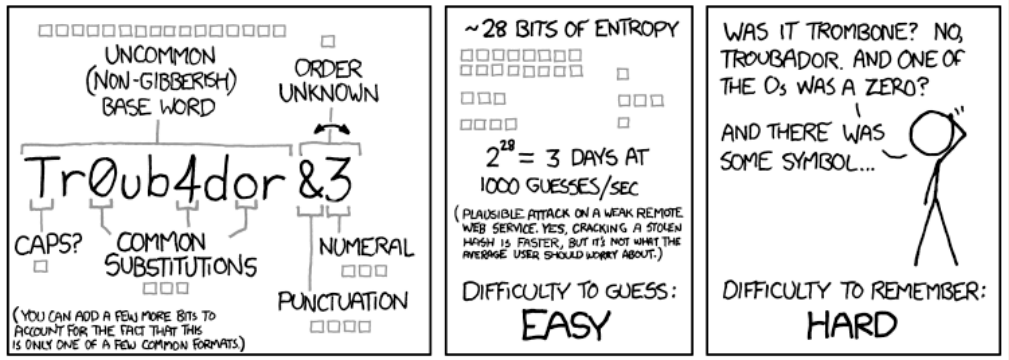
Was sind schwache Passwörter?

1. 123456
2. Ag89!+
3. 01234567890123456789
4. Sommer_2018
5. sommeruniversumvenus

123456 war 2019 das beliebteste Passwort in Deutschland gefolgt von 123456789 und 12345678

https://hpi.de/pressemitteilungen/2019/die-beliebtesten-deutschen-passwoerter-2019.html

Wie sieht die Realität aus?



Als Comic

https://xkcd.com/936/

Auf Youtube

https://www.youtube.com/watch?v=aHaBH4LqGsI

Michael McIntyre

In den letzten 20 Jahren haben wir Anwender erfolgreich trainiert, Passwörter zu benutzen, an die man sich schlecht erinnern kann, die Computer aber einfach errechnen können.

Rechtliche Grundlage

Die Authentifizierung mittels Nutzername und Passwort sowohl bei Geräten als auch Diensten stellt eine technische und organisatorische Maßnahme nach Artikel 32 DS-GVO dar. Eine sichere Authentifizierung der Nutzer ist ein Baustein, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten, Systeme und Dienste auf Dauer sicherzustellen (vgl. Art. 32 DS-GVO). Setzen Verantwortliche unzureichende technische und organisatorische Maßnahmen um, können Bußgelder bis zu 10 Millionen Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist (vgl. Art. 83 Abs. 4 DS-GVO). Verantwortliche sind also angehalten, angemessene technische und organisatorische Maßnahmen durchzuführen.

Nach wie vor stellt die Kombination aus Benutzername und Password die am häufigsten verwendete Methode da, um sich an Computersystemen anzumelden.

(Einige) Angriffsmethoden

1. Wörterbuchangriffe
2. Password Spraying
3. Trial and Error
4. Brute Force
5. Shoulder Surfing
6. Abhören der Netzwerkkommunikation
7. Man-in-the-Middle
8. Keylogger
9. Social Engineering
10. Phishing

Starke Passwörter reduzieren die Anzahl der Angriffsvektoren

Widerstandsfähigkeit


#	Passwort	Pool	Länge	Entropie	BF SC	BF PC +GPU
1	123456	10	6	~ 20 bit	< 1 sec	< 1 sec
2	Ag89!+	95	6	~ 39 Bit	< 1 sec	< 1 sec
3	01234567890123456789	10	20	~ 66 Bit	8 Minuten	43 Tage
4	P@ssw0rdP@ssw0rd	95	16	~ 105 bit	6 Mio Jahre	∞
5	Sommer_2018	95	11	~ 72 bit	7 h	6 Jahre
6	sommeruniversumvenus	26	20	~ 94 bit	> 3.000 Jahre	23 Mio Jahre
7	Djvdjfvb47643876*!43579439>	95	27	~ 177 bit	∞	∞
8	Qwertz1!	95	8	~ 52 bit	< 1 sec	4 Minuten
9	Die-13-lilablassroten-Beispielpasswoerter-nehme-ICH-nieniemals!	95	63	~ 414 bit	∞	∞

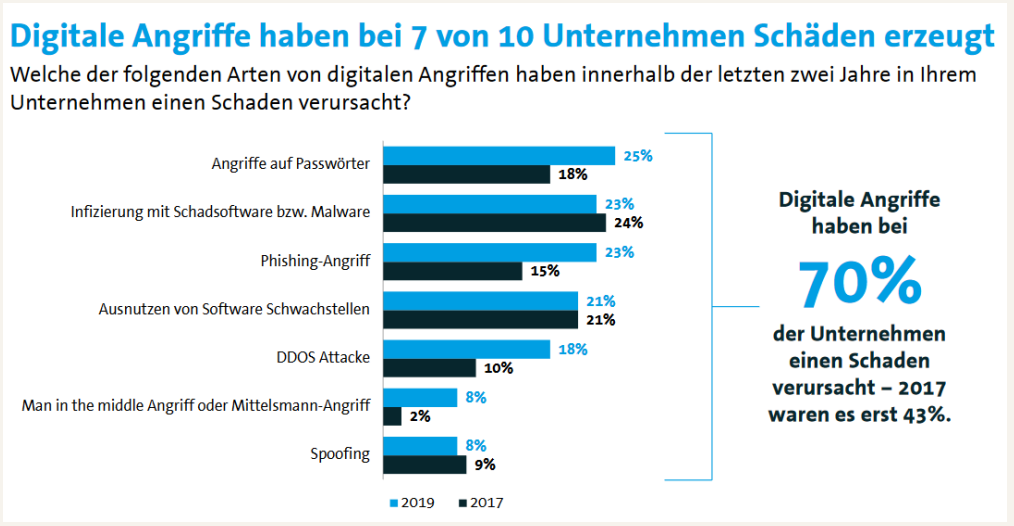
http://www.passwordstrengthcalculator.com

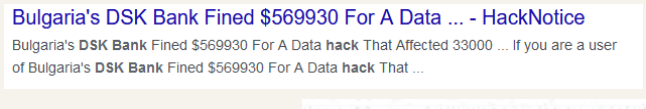
$$E = \log_2 (P) \times L$$

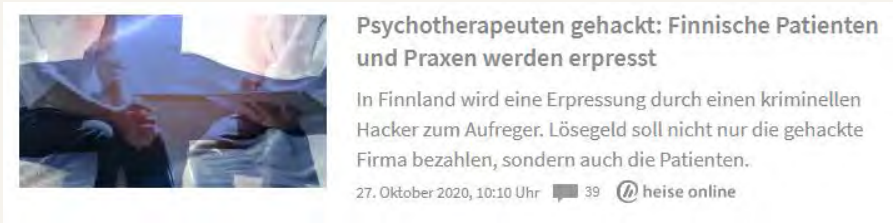
Ein (fairer) Münzwurf hat 1 Bit Entropie

Ein kompromittiertes Passwort hat 0 Bit Entropie

Warum sind schwache Passwörter ein Problem?







Schwache Passwörter sind eine Frage des „Risiko Appetits“ der IT Leitungsebene

„Hackerangriffe verursachen 102,9 Mrd. EUR Schaden jährlich in Deutschland“

bitkom „Wirtschaftsschutz in der digitalen Welt“ (2019)

Was empfiehlt das BSI?

OORP.4 Identitäts- und Berechtigungsmanagement

- Passwörter, die leicht zu erraten sind oder in gängigen Passwortlisten geführt werden, DÜRFEN NICHT verwendet werden.
- Ein Passwort MUSS gewechselt werden, wenn es unautorisierten Personen bekannt geworden ist oder der Verdacht dazu besteht.
- Das Passwort MUSS so komplex sein, dass es nicht leicht zu erraten ist.
- Das Passwort DARF NICHT zu kompliziert sein, damit der Benutzer in der Lage ist, das Passwort mit vertretbarem Aufwand regelmäßig zu verwenden.
- IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden
- Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.

Keine regelmäßige PW Änderung!

Kompromittierte Kennwörter müssen erkannt und geblockt werden!

Was empfehlen andere Sicherheitsbehörden?

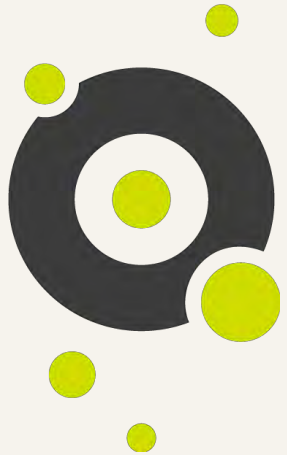
Maßnahme	Wer
Die Länge des Passworts sollte mindestens **15 Zeichen** umfassen.	HPI
Das Passwort sollte möglichst **viele verschiedene Zeichentypen** (Buchstaben, Ziffern, Sonderzeichen) sowie Groß- und Kleinschreibung mit einbeziehen.	HPI
Keine Begriffe aus **Wörterbüchern**	HPI
„Unter Berücksichtigung des **Stands der Technik**…treffen der Verantwortliche…geeignete TOMs, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten…“	DS-GVO
„Use three random words…“	NCSC (UK)
Password **length** has been found to be a **primary factor** in characterizing password strength.	NIST (US)
If the CSP or verifier disallows a chosen memorized secret based on its appearance on a **blacklist of compromised values**, the subscriber SHALL be required to choose a different memorized secret. **No other complexity requirements** for memorized secrets SHOULD be imposed	NIST (US)

Kennwörter müssen lang sein!

Kennwörter brauchen nicht komplex sein!

Kompromittierte Kennwörter dürfen nicht akzeptiert werden!

Verfahren für starke Kennwörter einführen!



1. Passwörter müssen lang sein!
2. Passwörter brauchen nicht komplex zu sein!
3. Führen Sie Passphrasen ein!
4. Privilegierte Konten mindestens 15 Zeichen!
5. Validieren Sie Kennwörter gegen Listen mit kompromittierten Passwörtern!
6. Blockieren Sie einfach zu erratenen Kennwörter durch Wortlisten!
7. Unterschiedliche Regeln für Standard –und Admin Accounts!
8. Kein regelmäßiges Ablaufdatum!
9. Sensibilisieren Sie Ihre Anwender (inklusive Admins) !

Standard Accounts:

≥ 70 Bit Entropie

Accounts mit Zugriff auf kritische Daten:

≥ 90 Bit Entropie

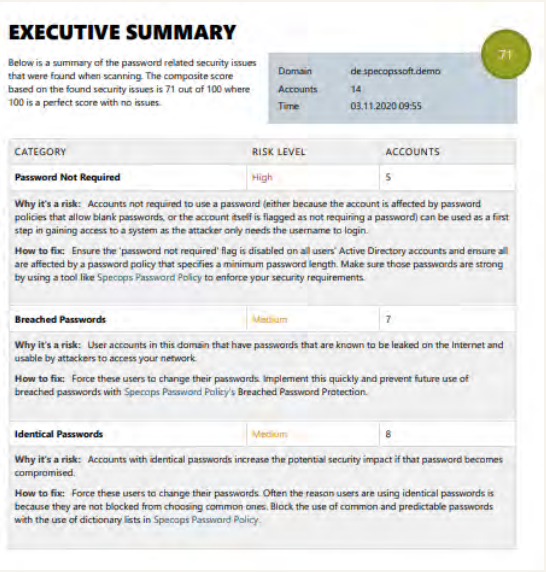
Lösungen von Specops Software

- Wir wissen **warum** schwache Passwörter ein Problem sind
- Wir sind uns einig **welche Verfahren** notwendig sind, um starke Kennwörter zu erstellen
- Wir **ahnen**, dass es ohne 3rd Party Software nicht funktionieren wird..

Specops Password Auditor

Analysiert und bewertet die Passwortsicherheit in Ihren Active Directory Services (ADDS):

- Benutzer mit kompromittierten Kennwörtern
- Konten mit identischen Passwörtern
- Konten ohne Kennwortanforderung
- Konten mit ablaufenden Kennwörtern (dynamisch)
- Der Password Auditor ist bis Jahresende kostenlos!



EXECUTIVE SUMMARY

Below is a summary of the password related security issues that were found when scanning. The composite score based on the found security issues is 71 out of 100 where 100 is a perfect score with no issues.

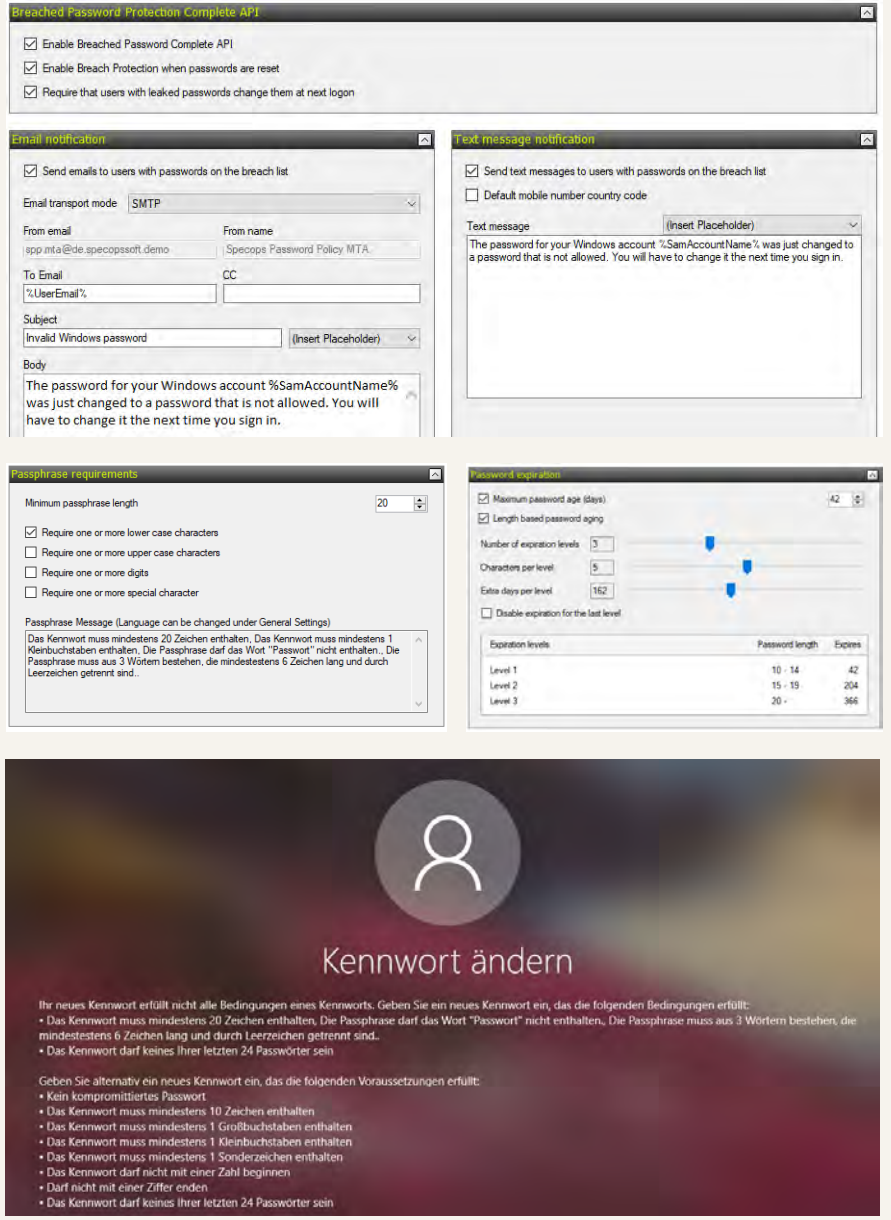
71

Domain	de.specopssoft.demo
Accounts	14
Time	03.11.2020 09:55

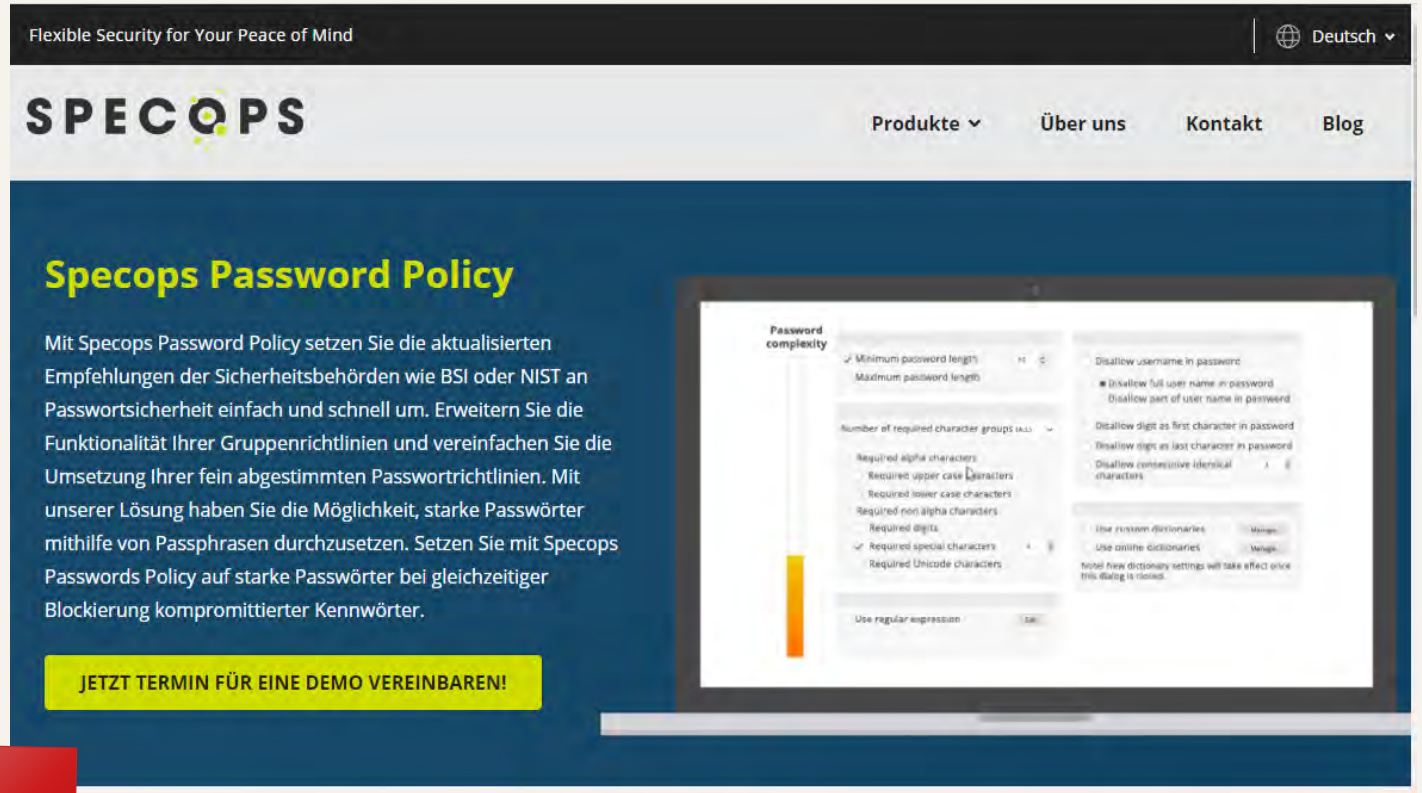
CATEGORY	RISK LEVEL	ACCOUNTS
Password Not Required	High	5
Why it's a risk: Accounts not required to use a password (either because the account is affected by password policies that allow blank passwords, or the account itself is flagged as not requiring a password) can be used as a first step in gaining access to a system as the attacker only needs the username to login.		
How to fix: Ensure the 'password not required' flag is disabled on all users' Active Directory accounts and ensure all are affected by a password policy that specifies a minimum password length. Make sure those passwords are strong by using a tool like Specops Password Policy to enforce your security requirements.		
Breached Passwords	Medium	7
Why it's a risk: User accounts in this domain that have passwords that are known to be leaked on the Internet and usable by attackers to access your network.		
How to fix: Force these users to change their passwords. Implement this quickly and prevent future use of breached passwords with Specops Password Policy's Breached Password Protection.		
Identical Passwords	Medium	8
Why it's a risk: Accounts with identical passwords increase the potential security impact if that password becomes compromised.		
How to fix: Force these users to change their passwords. Often the reason users are using identical passwords is because they are not blocked from choosing common ones. Block the use of common and predictable passwords with the use of dictionary lists in Specops Password Policy.		

Specops Password Policy

- Enthält Breached Password Protection mit derzeit 2,3Mrd kompromittierte Passwörter
- Unterstützung von Passphrasen
- Längenbasiertes Ablaufdatum
- Unterstützung von Wörterbüchern
- Benutzerfeedback bei der PW Änderung
- Als Gruppenrichtlinien konfigurierbar



Vielen Dank für Ihre Aufmerksamkeit!



https://specopssoft.com/de/produkte/specops-password-policy

Für weitere Fragen zum Thema: Registrieren Sie sich für eine Produkt-Demo auf unserer Website!