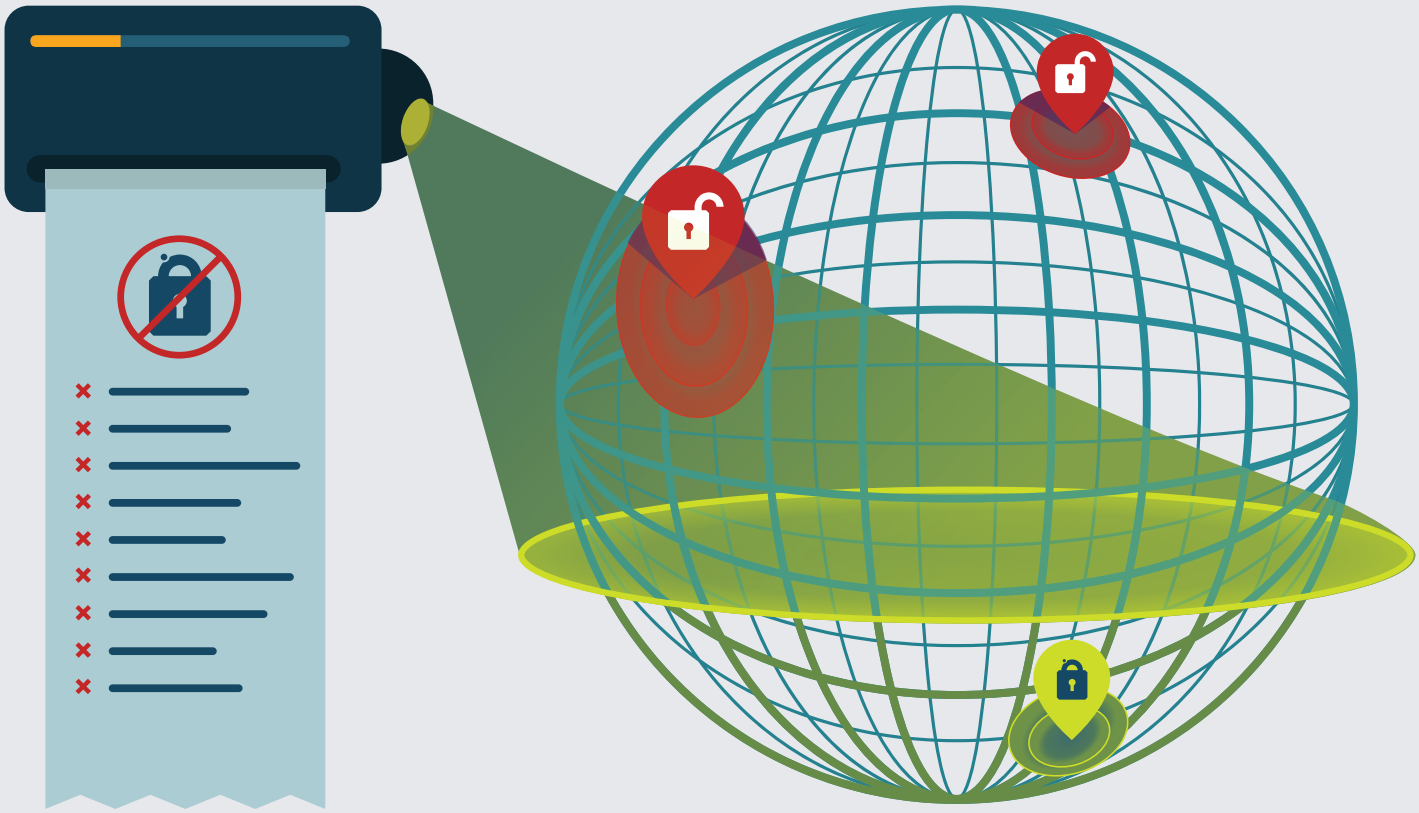
SPECOPS

Passwörter? Aber sicher!

Wie IT-Admins in Unternehmen die Passwortsicherheit erhöhen



SPECOPS

Passwörter? Aber sicher!

Wie IT-Admins in Unternehmen die Passwortsicherheit erhöhen

Totgesagte leben länger: Obwohl die Abschaffung von Passwörtern immer wieder in der Diskussion steht, führt auch künftig in Unternehmen kein Weg an ihnen vorbei. Passwörter sollen vor unbefugten Datenzugriffen schützen und somit für mehr Sicherheit sorgen. Doch sie können zum Einfallstor für Cyberkriminelle werden. Eine gute Schutzstrategie und ein modernes Risikomanagement minimieren die Gefahr, Kriminellen zum Opfer zu fallen.

Menschen vergessen schnell. Vor noch nicht allzu langer Zeit waren im Fernsehen Bilder von US-Amerikanern zu sehen, die sich Sprit in alle verfügbaren Kanister abfüllten. Vorausgegangen war ein Hackerangriff auf die Infrastruktur von Colonial Pipeline. Medienberichten zufolge zahlte das Unternehmen fünf Millionen US-Dollar Lösegeld in Bitcoins, um sich von der Ransomware zu befreien. Schnell stellte sich heraus, dass die Kriminellen für die Attacke ein VPN-Konto genutzt hatten. Das Passwort dafür wurde später in einer Sammlung geleakter Passwörter im Darknet entdeckt. Dabei hätte der Einsatz einer Software, mit der vorhandene Passwörter oder neu vergebene Passwörter regelmäßig gegen eine Liste mit bereits kompromittierten Kennwörtern überprüft werden, den Angriff womöglich verhindern können.

Mit ihrer Lösegeldforderung ließen sich die Hacker über eine Woche Zeit – und konnten sich so ungestört und unbemerkt im Netzwerk von Colonial Pipeline herumtreiben. Das FBI hat jüngst einen Großteil des Lösegelds gesichert. Das Sicherheitsgefühl der Bürger und Kunden aber dürfte nachhaltig gestört sein.

Was hat eine US-amerikanische Ölpipeline mit Deutschland zu tun? Die Antwort ist einfach: sehr viel. Die globalisierten Märkte von heute kennen kaum mehr Landesgrenzen und die Börsen haben umgehend auf die vorübergehende Benzinknappheit reagiert. Außerdem sind solche Attacken heute fast schon

Alltag. Kaum eine Woche vergeht, in der nicht irgendein Unternehmen einräumen muss, dass Daten unwillentlich abgeflossen sind. Neben dem Reputationsverlust kann das mit erheblichen finanziellen Einbußen verbunden sein. Denn die Datenschutzgrundverordnung (DSGVO) sieht bei einem Verstoß gegen Artikel 32, der bestimmte Pflichten hinsichtlich der sicheren Datenverarbeitung enthält, empfindliche Bußgelder vor.

Noch größere Schäden können entstehen, wenn Einrichtungen betroffen sind, die zu den Grundpfeilern einer Gesellschaft zählen: Energieversorger, Transportunternehmen oder Krankenhäuser. Diese sogenannten kritischen Infrastrukturen (KRITIS) müssen zwar besonders strenge Schutzmaßnahmen nachweisen, doch unantastbar sind sie keinesfalls. Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), betont: „Cyberangriffe auf kritische Infrastrukturen sind ein ernstzunehmendes realistisches Szenario auch in Deutschland."

Wie Cyberkriminelle Passwörter herausfinden

An Passwörter heranzukommen, setzt kriminelle Energie voraus. Wer diese besitzt, hat es oft vergleichsweise einfach. Nachfolgend werden die häufigsten Vorgehensweisen der Hacker vorgestellt:

- **Kauf geleakter Daten** Ob die Hackergruppe das Passwort, das sie für die Attacke auf Colonial Pipeline nutzten, im Darknet gekauft hat, ist unklar. Tatsache ist, dass sich die Angreifer später dafür entschuldigten, so vielen Menschen Unannehmlichkeiten bereitet zu haben. Ihnen sei es nur ums Geld gegangen. Solche „netten" Angreifer sind allerdings selten.

- **Credential Stuffing** Auch hierbei stehen geleakte oder anderweitig abgegriffene Passwörter im Fokus. Die Methode ist bei Hackern besonders beliebt, weil sie sich eine menschliche Schwäche zunutze macht: die des Gewohnheitstiers. Bei der Vielzahl an Passwörtern, die sich jeder heutzutage merken muss, ist die Verlockung groß, dasselbe Passwort mehrmals zu verwenden. Doch gelangt es in falsche Hände, könnte der gehackte Zugang zum Musikdienst unter Umständen ungewollt auch den Weg zum Mailkonto

oder zur virtuellen Arbeitsumgebung freimachen. Daher sollte dasselbe Passwort nie für verschiedene Dienste verwendet werden.

- **Password Spraying** Das Prinzip ähnelt dem Credential Stuffing, funktioniert aber quasi genau andersherum. Während dort versucht wird, das Passwort eines einzelnen Nutzers zu erraten, werden beim Password Spraying eines oder wenige Passwörter bei vielen verschiedenen Nutzer-Accounts ausprobiert. Hintergrund ist das Wissen, dass einige Kennwörter grundsätzlich überproportional häufig zum Einsatz kommen. Der Trick ist perfide: Während viele Systeme einzelne Nutzer nach einer bestimmten Anzahl von fehlerhaft eingegebenen Passwörtern blocken, fallen einzelne Fehlversuche bei einer großen Anzahl an Nutzern kaum auf.

- **Brute Force** Der Name ist Programm: rohe Gewalt. Durch wahlloses und unzähliges Ausprobieren werden automatisiert Zeichenkombinationen so lange getestet, bis die richtige gefunden ist. Je kürzer und schwächer das Passwort ist, desto größer ist die Chance für Hacker. Die Technik macht es heutzutage möglich, mehr als zwei Milliarden solcher Kombinationen innerhalb einer Sekunde zu testen (Quelle: Süddeutsche Zeitung)[1]. Doch mit jedem zusätzlichen Zeichen, das ein Passwort hat, wächst die Anzahl der Möglichkeiten exponentiell. Die Zeiten von „12345" sollten also längst vorbei sein.

USER HABEN WÄHREND DER CORONA-PANDEMIE DURCHSCHNITTLICH 15 NEUE BENUTZERKONTEN ERSTELLT.

82 PROZENT VON IHNEN NUTZEN IHRE PASSWÖRTER FÜR MEHRERE KONTEN.

Quelle: IBM Security Studie 2021

- **Social Engineering** Die klügsten Sicherheitsvorkehrungen nützen nichts, wenn es leicht ist, sie zu umgehen. Menschen können durch Vorspiegelung falscher Tatsachen, gutes Zureden oder Druck dazu gebracht werden, Dinge zu tun, die sie eigentlich nicht tun wollen und unter normalen Umständen nicht tun würden. Es ist der Enkeltrick der Geschäftswelt: Erst später stellt sich heraus, dass am Telefon kein Vorgesetzter, sondern eine wildfremde Person war, die Insiderinfos erbeutet hat.

[1] **So sieht ein sicheres Passwort aus:** Artikel Süddeutsche Zeitung (www.sueddeutsche.de/digital/sicherheit-im-internet-so-sieht-ein-sicheres-passwort-aus-1.2389416-0).

- **Keylogger** Solche Tools zeichnen jeden Tastaturanschlag auf und leiten ihn an ein externes Ziel weiter. Sie kommen meist durch das unachtsame Herunterladen und Öffnen einer Datei auf den Rechner. Bis sich der Virenscanner meldet, könnte schon zu viel Zeit vergangen sein. Wie beim Social Engineering zeigt sich auch bei dieser Vorgehensweise, dass technische Sicherheitslösungen zwar sehr gut sind. Ihr Nutzen potenziert sich aber noch, wenn Menschen wiederholt für drohende Gefahren sensibilisiert werden.

- **Shoulder Surfing** Klingt harmlos, ist aber eine besonders hinterhältige Art von Kriminellen, an vertrauliche Zugangsdaten zu gelangen. Wortwörtlich versuchen sie, Nutzern bei der Dateneingabe über die Schulter zu schauen. Ein Beispiel dafür ist das Erspähen der Geheimzahl bei der Nutzung eines öffentlichen Geldautomaten und der anschließende Diebstahl der zugehörigen Bankkarte.

- **Gestohlene Password Hashes** Viele Unternehmen speichern aus Sicherheitsgründen nicht die Kennwörter ihrer Kunden, sondern generieren daraus einen sogenannten Hash. Dieser ist vergleichbar mit einem unverwechselbaren Fingerabdruck. Bei jeder Eingabe wird der Hash mit dem in der Datenbank hinterlegten abgeglichen. Zahlreiche Kriminelle verfügen jedoch über sehr umfangreiche Listen von Hashes und den dazugehörigen Passwörtern. So müssen sie „nur noch“ die ihnen vorliegenden Hashes mit den gestohlenen vergleichen. Bei Übereinstimmungen entnehmen sie ihren Listen dann schnell das Klar-Passwort. Außerdem könnten sie versuchen, den Verschlüsselungscode des Unternehmens zu knacken.

- **Erraten von Passwörtern** Obwohl das heute kaum mehr möglich scheint, passiert es dennoch allzu oft. Denn viele Passwörter sind immer noch einfach zu durchschauen. Wer etwa den Namen seines Lieblingsfilms, seinen Geburtstag oder zusammenhängende Zahlenfolgen wählt, macht es Kriminellen leicht.

Warum Passwortmanager eine gute Lösung sind

Ein sinn- und wirkungsvolles Passwortmanagement ist für Admins unabdingbar. Denn je mehr Konten sie verwalten müssen, desto komplexer wird ihre Aufgabe. Das fängt schon bei der Frage an, ob häufige Passwortwechsel ratsam sind. Früher war dies eine Grundempfehlung vieler Sicherheitsexperten. Mittlerweile allerdings sind Aktionen wie der jährliche „Ändere dein Passwort"-Tag, der 2012 vom US-Technik-Blog Gizmodo ins Leben gerufen wurde, nicht mehr zeitgemäß. Der Verein „Deutschland sicher im Netz" hat sich Anfang 2020 für die Umbenennung in „Sicherer-Login-Tag" entschieden, weil aus seiner Sicht zusätzliche Sicherungen nötig sind. Dazu gehört beispielsweise die Multifaktor-Authentifizierung, also die Kombination von mindestens zwei verschiedenen Identitätsnachweisen. Das kann zum Beispiel die Eingabe eines PINs plus eines Codes sein, der auf das Mobiltelefon gesendet wird.

Tatsächlich sind die meisten Fachleute heute davon abgerückt, Nutzern nahezulegen, Passwörter häufiger zu wechseln. Dazu zählt auch das BSI, das eine entsprechende Empfehlung aus der 2020er-Ausgabe des BSI-Grundschutz-Kompendiums entfernt hat. Nun rät es zu einem Wechsel nur noch, wenn es einen Hinweis gibt, dass ein Passwort in den Besitz von unbefugten Dritten gelangt ist oder der eigene Rechner mit einem Schadprogramm infiziert ist. Auch bei Heise Security heißt es inzwischen: „Ein gutes Passwort kann man bedenkenlos über Jahre hinweg nutzen." Und bereits 2014 äußerte sich der Kryptologie-Experte Bruce Schneier eindeutig zu dem Thema:

> **„ES IST EGAL, WIE HÄUFIG ANWENDER IHR PASSWORT ÄNDERN. SEITEN, DIE DAS REGELMÄSSIG VERLANGEN, VERURSACHEN IN DER REGEL MEHR SCHADEN ALS NUTZEN.**

Die Gründe dafür liegen auf der Hand: Es zählt Qualität statt Quantität. Ein schwaches Passwort durch ein anderes schwaches zu ersetzen, nutzt nichts. Bei der Vielzahl an Passwörtern, die jeder Einzelne heutzutage benötigt, ist die Verlockung groß, bei erzwungenen Wechseln beispielsweise lediglich eine Ziffer

auszutauschen. Der Sicherheitsgewinn ist gleich null, wenn aus „FCSchalke04“ einfach „FCSchalke05“ wird.

Abhilfe können an dieser Stelle Passwortmanager schaffen. So lang oder komplex und so zahlreich die Codes auch sind: die Programme verwalten sie allesamt sicher. Die meisten dieser Tools bieten zudem die Funktion, starke Passwörter auf Knopfdruck zu generieren. Nutzer müssen sich dann nur noch ein einziges sicheres Passwort merken – nämlich das für den Passwortmanager selbst. Ein Problem bleibt allerdings bestehen: Wird der Zugang zum „Safe“ geknackt, ist der Inhalt im schlimmsten Fall einsehbar.

Welche Software Verantwortlichen die Arbeit abnimmt

Es gibt eine ganze Reihe von Sicherheitsstandards, doch wohl kaum ein Verantwortlicher für IT-Datenschutz kennt sie allesamt auswendig. Hier kann beispielsweise der Password Auditor von Specops diese Aufgabe übernehmen – und das sogar kostenfrei. Die Software scannt das Active Directory, identifiziert passwortrelevante Schwachstellen und listet sie übersichtlich in einem personalisierten Report auf. Dazu zählt unter anderem ein Check auf Konten mit kompromittierten Passwörtern: Die Software gleicht die Passwörter der Benutzerkonten mit einer Liste solcher ab, die bereits geleakt wurden. Das ist sehr wichtig, denn sind Passwörter einmal in Umlauf, gelten sie als verbrannt. Diese Aufgabe können Admins kaum selbst lösen. Specops Password Auditor kommt mit einer Liste von über 750 Millionen bereits kompromittierten Passwörtern, welche regelmäßig aktualisiert wird.

Scannen Sie mit Specops Password Auditor Ihr Active Directory auf passwortrelevante Schwachstellen.

Der durch den Read only scan des Specops Password Auditors erzeugte Report zeigt sämtliche Administratorkonten auf, einschließlich der gesperrten und nicht mehr aktiven.

DIE MEISTEN USER ÄNDERN IHR PASSWORT SELBST DANN NICHT, WENN ES KOMPROMITTIERT WURDE. WENN DOCH, IST DAS NEUE OFT SCHWÄCHER ALS DAS ALTE.

Quelle: Security and Privacy Institute der Carnegie Mellon University

Ein nicht mehr genutzter, aber noch immer funktionsfähiger Zugang, wie ihn die Hacker bei der Attacke auf Colonial Pipeline verwendeten, fällt somit schnell ins Auge. Die Praxis zeigt, dass dies eine nicht seltene Schwachstelle ist. Wechselt ein Admin beispielsweise die Arbeitsstelle, gibt es oftmals keinen klar strukturierten Offboarding-Plan, der die technische Organisation mit einbezieht. Aus den Augen, aus dem Sinn – und der Zugang schlummert vor sich hin. Häufig geht das gut, aber nicht immer. Hier besteht ein potenzielles Sicherheitsrisiko, das es unter allen Umständen zu vermeiden gilt.

Nutzer erhalten mit dem Password Auditor alle relevanten Informationen grafisch übersichtlich aufbereitet. So erkennen Verantwortliche für die IT-Sicherheit etwa auf einen Blick, wie viele und welche Nutzer Passwörter verwenden, die auf der Sperrliste mit kompromittierten Kennwörtern enthalten sind. Außerdem zeigt der Password Auditor Konten auf, die kein Passwort benötigen,

Übersichtliches Dashboard mit allen wichtigen Ergebnisses des Scans.

und überprüft darüber hinaus die Umsetzung der geltenden Password Policies – sowohl die der Default Domain als auch Fine-Grained Password Policies. Sie können zudem mit gängigen Industriestandards und den Empfehlungen von Institutionen wie dem US-amerikanischen National Institute of Standards and Technology (NIST) oder dem SANS Institute verglichen werden. Ein Farbsystem zeigt, ob alles in Ordnung ist oder Gefahr besteht.

Der Password Auditor ist eine Read-only-Anwendung. Er nimmt keine Änderungen am Active Directory vor. Der kostenfreie Check hat vor allem zwei Ziele. Er soll für mögliche Sicherheitsrisiken sensibilisieren und aufzeigen, wo dringender Handlungsbedarf besteht, um die Passwortsicherheit im Unternehmen zu erhöhen. Ein Angriff durch Cyberkriminelle kann zwar nie ganz ausgeschlossen werden, doch ein modernes Risikomanagement schließt viele Schlupflöcher. Es ist dasselbe Prinzip wie bei der eigenen Wohnung: Je höher die Hürden für Einbrecher sind, desto eher suchen sie sich ein anderes, leichteres Ziel.

TIPP Was der IT nützlich und sinnvoll erscheint, erschließt sich dem Management, dem Einkauf und dem Controlling nicht immer auf den ersten Blick. Neben einem Export der Ergebnisdaten ins CSV-Format ist der Password Auditor auch in der Lage, eine Executive Summary als PDF zu generieren. Diese kann als Entscheidungshilfe dienen, wenn es gilt, den Mehrwert von IT-Sicherheitslösungen zu verdeutlichen.

Welche Passwörter sinnvoll sind – und welche nicht

Noch immer lassen viele Unternehmen zu, dass die Mitarbeiter ihre Passwörter selbst bestimmen. Gemacht wird lediglich ein Check, ob diese mindestens acht Zeichen lang sind und sowohl Buchstaben als auch Ziffern beinhalten. Was aber zeichnet ein wirkungsvolles und starkes Passwort aus?

Manch einer dürfte die Legende von dem Reiskorn auf dem Schachbrett kennen. Darin geht es um einen Brahmanen, der das Schachspiel erfindet und es seinem tyrannischen König beibringt. Als Dank wünschte er sich lediglich ein Reiskorn auf dem ersten Feld des Schachbretts, zwei auf dem zweiten, vier auf dem dritten, acht auf dem vierten, 16 auf dem fünften. Erst später kam der Tyrann dahinter, dass es in seinem Land gar nicht so viel Reis gab, um seine Schuld tilgen zu können. Das nennt man exponentielles Wachstum. So ist es auch mit langen Passwörtern. Eine Grundregel lautet daher: Je länger, desto besser. Passwörter ab 20 Zeichen gelten den meisten Experten als sicher.

Des Weiteren sollten Passwörter keine Namen, Geburtsdaten oder andere recherchierbare Informationen enthalten. Es gibt zudem Angriffsmethoden, die gezielt versuchen, mit dem Inhalt von Wörterbüchern Passwörter zu knacken. Besser ist es also, keine Wörter zu verwenden, die darin enthalten sind. Auch das simple Anhängen von Ziffern oder unterschiedlichste Muster wie Tastatur-

FANS VON MARVEL UND DC LIEBEN PASSWÖRTER, DIE SIE MIT IHREN FAVORISIERTEN COMICS IN VERBINDUNG BRINGEN. DOCH DAMIT MACHEN SIE ES HACKERN SEHR EINFACH.

EINE NEUE UNTERSUCHUNG ZEIGT, DASS LOKI, THOR UND ROBIN DIE SPITZENPLÄTZE UNTER DEN KOMPROMITTIERTEN PASSWÖRTERN EINNEHMEN. ANALYSIERT WURDEN MEHR ALS 800 MILLIONEN KOMPROMITTIERTE PASSWÖRTER. INSGESAMT TAUCHTEN DIE 80 WICHTIGSTEN MARVEL- UND DC-CHARAKTERE MEHR ALS 1,1 MILLIONEN MAL AUF DIESER LISTE AUF.

Quelle: Eigene Untersuchung

kombinationen (qwertz) sollten vermieden werden. Das BSI nutzt ein kulinarisches Beispiel, um zu veranschaulichen, was ein starkes Passwort ausmacht: „Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!“ Wer sich die Anfangsbuchstaben merkt sowie Zahlen und Konjunktionen durch Sonderzeichen ersetzt, kommt auf „AleiPm4Z+eK!“.

Passphrasen funktionieren nach einem ähnlichen Prinzip, verzichten aber auf die Abkürzung. Sie sind daher naturgemäß viel länger als ein Passwort – und damit in der Regel auch sicherer. Das gilt umso mehr, wenn ebenfalls Sonderzeichen eingebaut werden: „Am liebsten esse ich Pizza, mit 4 Zutaten + extra Käse!“ Zudem dürfen sie auch Leerzeichen beinhalten. Ansonsten ist angezeigt, keine feststehenden Zitate wie Sprichwörter oder Liedtexte zu verwenden. Außerdem ist für jeden einzelnen Account eine separate Passphrase nötig. Sowohl starke Passwörter als auch Passphrasen minimieren die Gefahr, einem Brute Force-Angriff zum Opfer zu fallen.

Ein Wort noch zum sogenannten Leetspeak, dem Ersetzen von Buchstaben durch ähnlich aussehende Ziffern: Das Passwort P0l1z6i sieht auf den ersten Blick sehr viel sicherer aus als Polizei. Hacker sind aber in den meisten Fällen alles andere als dumm und beziehen solche Spielereien längst in ihre Angriffsstrategien ein.

Der nächste Schritt: Specops Password Policy

Wissen ist Macht. Es nutzt aber wenig, wenn man es nicht in die Praxis umsetzt. Wer mit dem Specops Password Auditor potenzielle Schwachstellen in der Active Directory-Umgebung aufgedeckt hat, für den ist Specops Password Policy genau das richtige Werkzeug, um sie zu behe-

Mit der Specops Password Policy setzen Sie starke Passwörter in Ihrer Organisation durch.

ben beziehungsweise gar nicht erst entstehen zu lassen. Die Software „kennt“ die aktuellen Empfehlungen der Sicherheitsbehörden und sorgt dafür, dass ausschließlich starke Passwörter zum Zuge kommen. So werden unter anderem Passwörter, die diesen Empfehlungen nicht entsprechen, grundsätzlich nicht akzeptiert. Gleiches gilt für bereits kompromittierte Passwörter. Password Policy unterstützt Nutzer auch dabei, Passphrasen zu formulieren, an die sie sich leicht erinnern können. Bekannte Muster wie das Voranstellen oder Anhängen von Ziffern werden dabei unterbunden, ebenso wie Leetspeak.

Darüber hinaus umfasst die Datenbank des Managed Services Breached Password Protection rund 2,4 Milliarden kompromittierte Kennwörter aus aktuellen und vergangenen Datenleaks. Das sind rund dreimal so viele wie beim Password Auditor. Außerdem ist es möglich, den individuellen Bedürfnissen angepasste Wörterbücher zu erstellen. So können Unternehmen für sie relevante Wörter wie etwa Firmen- oder Produktnamen als Bestandteile von Passwörtern ausschließen.

INFO

Sie wollen mehr über Specops Password Policy wissen? Sprechen Sie uns an, wir vereinbaren gerne einen Termin für eine Live-Demo mit Ihnen.

Specops Software ist der führende Anbieter von Passwort Management- und Authentifizierungslösungen. Specops Software schützt Ihre Geschäftsdaten, indem es schwache Passwörter blockiert und die Benutzerauthentifizierung sichert. Mit einem kompletten Portfolio von Lösungen, die nativ in Active Directory integriert sind, stellt Specops Software sicher, dass sensible Daten vor Ort und unter Ihrer Kontrolle gespeichert werden. Specops Software wurde 2001 gegründet und hat seinen Hauptsitz in Stockholm, Schweden sowie weitere Niederlassungen in den USA, Kanada, Großbritannien, Frankreich und Deutschland.

Kontaktdaten

Zentrale Schweden AB
Specops Software
Torsgatan 8
S-11123 Stockholm

Telefon: +46-8-465 012 34
Support: +46-8-465 012 50

Deutschland
Specops Software GmbH
Gierkezeile 12
10585 Berlin

Telefon: +46-8-465 012 34

www.specopssoft.com