Passwort-Management

Sesam, schließe dich

[26.10.2023] Erstes Einfallstor für Cyber-Kriminelle sind oft unsichere Passwörter. Ein solides Passwort-Management bietet daher einen wirksamen Schutz vor Cyber-Angriffen. Tools zur Passwortsicherheit helfen dabei.

Die Konnektivität innerhalb von Organisation und in den Geschäftsprozessen hat viele Vorteile. Die digitale Transformation macht viele Organisationen aber auch anfällig für Attacken von Cyber-Kriminellen. Insbesondere Kommunen geraten zunehmend ins Visier von Cyber-Kriminellen. Ein Beispiel: Im Jahr 2021 musste eine deutsche Kommune aufgrund eines Hacker-Angriffs den Katastrophenfall ausrufen. Die IT-Infrastruktur war von einem Trojaner befallen, der die Dateien verschlüsselte. Dadurch wurde der Landkreis Anhalt-Bitterfeld in Sachsen-Anhalt lahmgelegt. Die Auszahlung von Sozial- und Unterhaltsleistungen war über eine Woche lang nicht möglich. Solche Ransomware-Angriffe zielen in erster Linie auf die Verschlüsselung aller Daten ab, die nur durch die Zahlung eines Lösegelds wieder rückgängig gemacht werden kann. Die Auswirkungen eines Angriffs können weitreichend und verheerend sein. Ist der Ransomware-Angriff erfolgreich, haben Kommunen innerhalb kürzester Zeit keinen Zugriff mehr auf wichtige Dokumente und Systeme – in manchen Fällen sogar auf ihr gesamtes Netzwerk. Die Produktivität kann für einige Tage bis hin zu mehreren Wochen zum Erliegen kommen. Auch im Jahr 2023 sind solche Vorfälle leider keine Ausnahme.

Erster Angriffspunkt: Passwort

Für die Kommunen ist es daher höchste Zeit, sich besser gegen Cyber-Attacken zu schützen. Die negativen Folgen sind vielfältig: Vom Abfluss personenbezogener Daten, die jede Organisation erhebt und deren Schutz gesetzlich geregelt ist, über den Diebstahl interner Daten bis hin zum Totalausfall von Systemen oder dem Entzug von Kapital durch Betrug. Bei den zahlreichen Cyber-Angriffen auf Kommunen sind die Beschäftigten und die von ihnen verwendeten schwachen Passwörter der erste Angriffspunkt. Schließlich sind Passwörter immer noch die häufigste Methode, um sich im Netzwerk zu authentifizieren. Sofern ausreichend starke Passwörter verwendet werden, ist diese Authentifizierungsmethode auch heute noch effektiv und sicher. Durch den Faktor Mensch kann sie aber auch zu einer Schwachstelle innerhalb der IT-Sicherheitskette werden – nämlich dann, wenn schwache oder kompromittierte Passwörter verwendet werden. Haben sich Cyber-Kriminelle erst einmal über ein solches Zugang verschafft, stehen ihnen Tür und Tor zu allen Daten offen. Die Durchsetzung von starken und nicht kompromittierten Passwörtern ist daher wichtiger denn je und sollte nicht dem Zufall überlassen werden. Vor diesem Hintergrund gilt es im ersten Schritt zu prüfen, ob die dokumentierten Anforderungen an die Passwortsicherheit den aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entsprechen.

Bestandsaufnahme der Passwörter

Ausgangspunkt für ein starkes Passwort-Management ist eine Bestandsaufnahme, der im Unternehmen verwendeten Passwörter. Bei diesem Sicherheits-Assessment helfen Tools wie der Specops Password Auditor, der die Benutzerkonten im Active Directory auf alle passwortrelevanten Schwachstellen analysiert, indem er die Hash-Werte der Benutzerkonten-Kennwörter scannt und mit einer Datenbank von mehr als einer Milliarde kompromittierter Passwörter abgleicht. Zudem gilt es, technische und organisatorische

Maßnahmen zu implementieren, die im Idealfall den Einsatz starker Passwörter organisationsweit garantieren. Starke Passwörter sind schwer zu erraten, nicht bereits kompromittiert und schwer zu knacken. Eine einfache und effektive Methode ist die Verwendung von Passphrasen zur Generierung starker Kennwörter. Die Durchsetzung dieser und weiterer moderner Richtlinien, wie zum Beispiel längenbasierte Ablaufdaten für Kennwörter, kann durch den Einsatz eines Third Party Tools wie Specops Password Policy oder eines externen Passwortfilters für das Active Directory sichergestellt werden.

IT-Support entlasten

Es kommt häufig vor, dass Mitarbeitende ihre Passwörter zurücksetzen müssen, was dann einen Großteil der Arbeitszeit der IT-Administration oder des Helpdesks in Anspruch nimmt. Um den IT-Support zu entlasten, nutzen einige Organisationen inzwischen einen Self-Service. Leider werden bei diesem Verfahren zum Zurücksetzen von Kennwörtern viele Fehler gemacht. So sind die Sicherheitsfragen, mit denen die Identität des Nutzers beim Passwort-Reset überprüft wird, oft zu einfach und können in Zeiten von Social Media auch von Dritten leicht beantwortet werden. Um dem entgegenzuwirken, gibt es sichere Verfahren zum Zurücksetzen von Passwörtern, so etwa Specops uReset, mit dem Nutzer ihre Passwörter zurücksetzen können, ohne den Helpdesk kontaktieren zu müssen. Dieses Verfahren aktualisiert nicht nur das Passwort im Active Directory, sondern auch in den lokal zwischengespeicherten Anmeldeinformationen, den so genannten Cached Credentials des Computers. Dadurch wird verhindert, dass das Nutzerkonto gesperrt wird, wenn keine Verbindung zum Domain Controller der Organisation möglich ist. Das Verfahren gewährleistet durch Sicherheitsfeatures wie Multi-Faktor-Authentifizierung und Geo-Blocking ein hohes Sicherheitslevel für die Prüfung der Nutzeridentität und auch einen Passwort-Reset von überall und zu jeder Zeit.
Cyber-Angriffe durch Kriminelle nehmen weltweit zu, mit zum Teil dramatischen Folgen für Kommunen und Bürger. Diese sind jedoch nicht machtlos. Durch den konsequenten Einsatz von Tools zur Erhaltung der Passwortsicherheit können sie sich vor Cyber-Angriffen schützen.

()

Dieser Beitrag ist in der Ausgabe Oktober 2023 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Passwort-Management, Specops