Passwortsicherheit

Die richtige Strategie

[08.04.2019] Deutsche Behörden erreichen laut einer Umfrage im Umgang mit Passwörtern gute Noten. Ein Passwort-Manager kann ihnen dabei helfen, beispielsweise schwache und mehrfach verwendete Passwörter oder niedrige Sicherheits- und Passwortqualitätswerte aufzudecken.

Immer häufiger werden Behörden und Unternehmen Opfer von immer komplexer werdenden Cyber-Angriffen. Dabei fällt es den Organisationen schwer, effektive Sicherheitsrichtlinien umzusetzen. Schwache, mehrfach verwendete Passwörter stellen eine der häufigsten Sicherheitsbedrohungen dar und der laxe Umgang damit ist eine weit verbreitete schlechte Angewohnheit. Doch selbst wenn sie Passwort-Manager verwenden, haben Organisationen Schwierigkeiten oft zu quantifizieren, wie hoch ihr Risiko durch schlechte Passwortsicherheit ist. Ihnen fehlt der Einblick in das Verhalten ihrer Mitarbeiter. Und sie können nicht überprüfen, wo sie im Vergleich zu anderen Behörden oder vergleichbaren Organisationen stehen.
Einen fundierten Einblick gibt der aktuelle Globale Passwort-Sicherheits-Report des Unternehmens LogMeIn. Darin wurden die Passwortgewohnheiten der Mitarbeiter von 43.000 Unternehmen und Organisationen aller Größen und Sektoren analysiert, die den Passwort-Manager LastPass verwenden. Der Bericht zeigt nicht nur den Umgang mit Passwörtern auf, sondern bietet IT-Experten auch einen fundierten Vergleich, wie eine Organisation im Vergleich zu ähnlichen abschneidet und wie sich ihre Passwortsicherheit verbessern ließe. Der LastPass-Sicherheitswert ist ein Benchmark-Wert zwischen 0 und 100. Ermittelt wird er durch die Anzahl der mehrfach verwendeten Passwörter, die Anzahl der als nicht sicher eingestuften Seiten aufgrund von öffentlich bekanntgewordenen Datenschutzverletzungen, die Anzahl der schwachen Passwörter, die durchschnittliche Qualität jedes Passworts, die Qualität der freigegebenen Passwörter sowie den Multifaktor-Authentifizierungswert.

Sicherheitsstandards einhalten

Die Auswertung der LastPass-Daten belegt, dass die meisten Organisationen Passwortsicherheit mittelmäßig konsequent betreiben und das Passwortrisiko unabhängig von Größe, Branche und Standort ist. Je größer eine Organisation ist, desto niedriger ist aber ihr Sicherheitswert im Durchschnitt. Mehr Beschäftigte bedeuten mehr Passwörter und nicht genehmigte Apps und somit zusätzliche Gelegenheiten für Mitarbeiter, ein riskantes und gefährliches Passwortverhalten an den Tag zu legen. In größeren Unternehmen gestaltet es sich für die IT deshalb viel schwieriger, alle Beschäftigten dazu zu bringen, die Passwortsicherheitsstandards einzuhalten. In Organisationen mit kleinerem Mitarbeiterstamm ist es einfacher, sichere Passwörter und eine mehrstufige Authentifizierung für alle Mitarbeiter zu gewährleisten. Ein gutes Beispiel für die Herausforderungen, die mit der Organisationsgröße wachsen, ist die gemeinsame Nutzung von Zugangsdaten. Im Durchschnitt teilt ein bestimmter Mitarbeiter etwa sechs Passwörter mit seinen Kollegen. Bereits in einem Unternehmen mit 100 Mitarbeitern sind die Auswirkungen dessen enorm. Die gemeinsame Nutzung von Passwörtern ist sowohl für Mitarbeiter als auch für IT-Administratoren frustrierend, da die Benutzer auf die Verwendung von schwachen, aber leicht einzuprägenden Passwörtern zurückgreifen, die potenzielle Einfallstore für Cyber-Angriffe darstellen. Da Teams immer verteilter und technologieabhängiger agieren, wird es für Unternehmen immer komplizierter, aber auch unerlässlich, gemeinsame Passwörter zu schützen, zu verfolgen und zu auditieren.

Höchste Werte für deutsche Behörden

Die gute Nachricht für deutsche Behörden: Sie erreichten im Passwort-Sicherheits-Report mit Abstand den höchsten Sicherheitswert 86. Auch für Europa ist der Sicherheitswert der deutschen Behörden ein Ausrufezeichen, liegt doch der Durchschnittswert bei europäischen Behörden bei 43. Zum Vergleich: Weit abgeschlagen ist in Deutschland die Banken- und Finanzbranche mit 38 Zählern. Grundsätzlich liegen die Sicherheitswerte aller befragten deutschen Organisationen über dem weltweiten Durchschnitt. Defizite zeigen sich nur in der Multifaktor-Authentifizierung: Gerade einmal drei Prozent nutzen diese Möglichkeit, Konten zu sichern. Dabei ist und bleibt diese die optimale Vorgehensweise gegen Kontozugriffe von außen. Hierbei sind die USA Vorreiter: 65 Prozent aller Unternehmen, die mit Multifaktor-Authentifizierung arbeiten, sind dort ansässig.
IT-Sicherheit zu verbessern, ist eine kontinuierliche Aufgabe – effizienteres Passwort-Management dagegen lässt sich unabhängig von Größe, Branche und Standort vergleichsweise einfach umsetzen. Bereits ein Jahr nach der Implementierung eines Passwort-Managers, so die Analyse, können die meisten Organisationen ihren Sicherheitswert um durchschnittlich fast 15 Punkte verbessern. Außerdem werden die Produktivität, die Markenwahrnehmung und die Mitarbeiterzufriedenheit erhöht. Da immer mehr Unternehmen und auch Behörden BYOD-Richtlinien (Bring Your Own Device) umsetzen und Netzwerke für zuvor nicht genehmigte Geräte und Anwendungen öffnen, müssen IT-Führungskräfte ihre Einstellung zur Passwortsicherheit ändern. Transparenz ist der Schlüssel: Man kann Sicherheit nicht messen, wenn man kein System hat, das Einblicke in potenzielle Risikobereiche gewährt.

Leistungen des Passwort-Managers

Mit dem Log-in eines jeden Mitarbeiters bröckelt die Datensicherheit. Ein Passwort-Manager ist hierbei nicht nur ein sicheres Tor, das Hacker-Angriffe abhält, er hilft Behörden auch, die Wirksamkeit mittel- und langfristig zu beurteilen und zu kontrollieren. Ein Passwort-Manager sollte zufällige Passwörter generieren, rollenbasierte Berechtigungen auf Passwörter anwenden und Kontrolle über gemeinsam genutzte Zugangsdaten bieten. Zusätzliche Sicherheit erwirkt er durch die Multifaktor-Authentifizierung oder das Außerkraftsetzen von Zugangsdaten, wenn Mitarbeiter beispielsweise die Behörde verlassen.
Passwort-Management bedeutet Change Management. Um sie mit ins Boot zu holen, sollten Organisationen alle Mitarbeiter über Richtlinien und Best Practices informieren, den Passwort-Manager in das Sicherheitsschulungsprogramm integrieren und sicherstellen, dass alle neuen Mitarbeiter entsprechend geschult werden. Ferner sollte das Tool nebst Erläuterungen zu dessen Verwendung bereitgestellt und ein Kontakt genannt werden, an den sich die Nutzer bei Fragen wenden können. Der Fortschritt lässt sich mithilfe von Reporting-Tools überwachen. Diese decken potenzielle Sicherheitslücken wie schwache und mehrfach verwendete Passwörter, niedrige Sicherheits- und Passwortqualitätswerte oder inaktive Konten auf.

()

Stichwörter: IT-Sicherheit, Datenschutz, LastPass, LogMeIn, Passwort-Manager