Fridel Rickenbacher ist Mitbegründer, Partner, Geschäftsführer und Verwaltungsrat der MIT-GROUP, einem Totalunternehmen für «Empowering for the 4th Industrial Revolution» und Informations- und Kommunikationsmanagement. Auf Bundesebene ist er als Experte und Akteur vertreten bei «Digital Dialog Schweiz» + «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS». Er ist in seiner Mission «sh@re to evolve» seit

Single Sign On SSO – Sicherheit gegen gefährdenden Passwort- und Rechte-Wildwuchs

Passwort- und Rechte-Wildwuchs und eine steigende Akzeptanz der Cloud bewirken einen verstärkten Trend zum sogenannten Single-Sign-On SSO. Diese Authentifizierungsmethode kann durch den Bedienerkomfort und die zentrale Verwaltung auch die Sicherheits- und Compliance-Anforderungen umfassend optimieren.

Beitrag von Fridel Rickenbacher

Im privaten und zunehmend auch geschäftlichen Umfeld kennt man gewisse Sign-In-Varianten über soziale Netzwerke wie Facebook, Twitter, Google, Amazon oder Microsoft als prominente SSO-Plattformen für den integrierten Zugang zu unterschiedlichen Services und Rechten.
Im Unternehmensumfeld wird SSO beispielsweise genutzt, um Nutzern einen integrierten, möglichst simplifizierten Zugriff auf eigene Web- oder Cloud-Anwendungen auf internen Servern oder in der (Hybrid)Cloud zu gewähren. Teilweise wird der Zugang mittels erweiterten Authentifizierungsmechanismen wie z.B. MFA (Multi Factor Authentication) oder 2FA (Two Factor Authentication) per Tokens, SMS, Email, Smartphone Authenticator Apps und dergleichen zusätzlich abgesichert. (ähnlich wie bei modernem eBanking).

Richtig eingesetzt generiert SSO umfassende Vorteile für die Produktivität, das IT-Monitoring und Management sowie die Sicherheitskontrolle bezüglich Compliance. Mit einem einzigen Sicherheits-Token (zum Beispiel Benutzername und Passwort), kann Nutzern der Zugriff auf mehrere Systeme, Plattformen, Anwendungen und andere Ressourcen gewährt und entzogen werden. Durch die Reduzierung auf einen Satz möglichst komplexen Zugangsdaten wird zudem die Gefahr reduziert, dass schwache, leicht zu entschlüsselnde Passwörter verwendet oder die Zugangsdaten vergessen werden. Der Support seitens IT-Servicedesk kann dadurch optimiert werden und mittels weitergehenden Self Service Optionen für z.B. Kennwort-Rücksetzung seitens Endanwender weiterentwickelt werden.
Die Reduktion der Anzahl unterschiedlichen Kennwörter und Zugangsdaten kann auch mithelfen, dass die Kennwörter nicht unerwünscht irgendwo unsicher abgelegt oder gar aufgeschrieben werden (z.B. am Bildschirm, unter der Tastatur oder unsicheren Datenablagen).
Bei der sogenannten Passwort-Hygiene wird zudem mittel SSO unterstützt oder gar per Richtlinien verhindert, dass der Anwender nicht ähnliche, nur leicht abgeänderte Kennwörter immer wieder verwendet zulasten der Gesamtsicherheit.

Solche integrierten SSO-Systeme mit integriertem Identity & Access Management (IAM) unterstützen auch mittels Workflows, Sicherheitsgruppen (anstelle z.B. individuelle Einzel-Sonder-Berechtigungen) und Richtlinien, dass bei Mitarbeiter-Eintritts- und vorallem Mitarbeiter-Austritts-Prozessen die Fehlerrate reduziert oder unerwünschte Berechtigungen verhindert werden. Solche neuen adaptierbaren Technologien helfen auch im fortwährenden Kampf gegen die Schatten Informatik (shadowIT) mittels z.B. gegebenen, zu erreichenden Mindestanforderungen an prozessuale und technologische Standards mittels erforderlichen Ablösungen, Migrationen und Upgrades von auch Legacy Systems oder Legacy Apps.

Trends wie «Bring your own device (ByoD)» sind weitere kritische Faktoren welche bezüglich der Gesamtsicherheit und deren Komplexität solche entsprechende umfassende, technische und organisatorische Massnahmen erfordern und unumgänglich machen um auf dem «Stand der Technik» (state of the art) bleiben zu können mittelfristig.

Immer mehr Menschen werden zunehmend an Geräten arbeiten, die die IT nicht mehr integriert kontrol-

Jahren als Redaktionsmitglied, Experten-Gruppen- und Verbands-Aktivist tätig bei z. B. SwissICT, s-i.ch, isss.ch, isaca.ch, bauen-digital.ch rund um Digitalisierung, Engineering, Clouds, ICT-Architektur, Security, Privacy, Datenschutz, Audit, Compliance, Controlling, Information Ethics, in entsprechenden Gesetzes-Vernehmlassungen und auch in Aus- und Weiterbildung (CAS, eidg. dipl.).

lieren kann und in Netzwerken, bei denen die IT über keinerlei Sichtbarkeit, Monitoring und Controlling verfügt. Das macht Authentifizierung zu einem entscheidenden, von Gerät und Standort unabhängigen Kontrollpunkt, um Sicherheitskontrollen wie SSO, Continuous Authentication, Multi-Faktor Authentifizierung (MFA), kontextbezogene Zugangskontrollen (conditional access), Analyse von Nutzerverhalten etc. möglich zu machen.

Der grösste Vorteil von SSO liegt in der gebotenen Skalierbarkeit, rascheren Provisionierung von Cloud-Services und zentraler Verwaltung. Durch automatisiertes Zugangsdaten-Management muss der System-Administrator sich nicht mehr händisch um all die verschiedenen Zugänge der Mitarbeiter für die einzelnen Services kümmern, die sie nutzen möchten. Das verringert wiederum die Gefahr für Fehler im Management der Authentifizierungsdaten, Berechtigungen und gibt der IT mehr Zeit, sich auf wichtigere Aufgaben zu konzentrieren zugunsten der Qualität und Gesamtsicherheit.

Entsprechende Lösungen schützen also das Business während die Anwender gleichzeitig so arbeiten können, wie es für sie am komfortabelsten ist. Alles in allem verbessert SSO, wenn es mit Mechanismen zum Risikomanagement (beispielsweise eine detaillierte, systematische Risikoanalyse aller Gruppen und Individuen vor der Rechtevergabe) geht, die Zugangssicherheit und mindert die Bedrohung durch Datenlecks oder durch Datenschutzverletzungen. (data breaches, gemäss Datenschutzgrundverordnung DSGVO / GDPR).

Den Argumenten, die für SSO sprechen, stehen aber auch einige problematische Aspekte gegenüber, die Unternehmen detailliert beachten und abwägen sollten, wenn sie erwägen, eine solche zentrale Authentifizierungsmethode einzuführen.

Ein wichtiger Punkt dabei ist, dass die Bündelung aller Zugänge unter einem Passwort dieses zu einer Art «Single-Point-of-Failure» macht. Wird dieses Passwort geknackt, kann der Schaden entsprechend potentiell enorm sein, da der Angreifer Zugang zu zahlreichen Services und Accounts erhält mit «nur einem» Login. Zwar kann die IT über das SSO-System das Passwort relativ schnell und einfach sperren. Dafür muss der Vorfall aber erst einmal bekannt sein, was unter Umständen (zu) lange dauern kann wenn kein proaktives Monitoring wie z.B. Advanced Threat Analytics / Advanced Threat Protection mitimplementiert wird je nach angestrebtem Schutzniveau.

Um dies zu verhindern, sind – wie weiter oben bereits erwähnt – komplexe, mehrstufige Sicherheitsmassnahmen notwendig. Einfache Passwörter ohne zusätzliche Sicherheitsstufen und Mindest-Komplexitätanforderungen sind einfach nicht mehr ausreichend.

Prominente Vorfälle wie der Equifax-Hack machen dies mehr als deutlich. Bei diesem Cyberangriff verschafften sich die Hacker über einen Webseite-Exploit unbemerkt Zugriff auf das System des US-Finanzdienstleisters und stahlen im Laufe von etwa zweieinhalb Monaten unbemerkt Datensätze von über 143 Millionen Kunden – darunter Sozialversicherungsnummern, Adressen und Kreditkartendaten –, bevor die Schwachstelle von der IT entdeckt und geschlossen wurde.

Um das Sicherheitsniveau entsprechend anzuheben, ist eine mehrstufige Authentifizierung nötig, die neben dem Passwort noch weitere Identifikationsmerkmale umfasst. Das ist oft die berüchtigte Kontrollfrage nach dem «Mädchenname der Mutter» oder Ähnlichem. Aber auch hier Achtung: Solche Basis-Informationen können unter Umständen je-

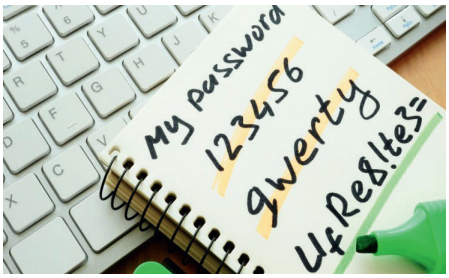

Foto: designer491 – shutterstock.com

doch relativ einfach über Recherche in den sozialen Netzwerken, Social Engineering oder Phishing- beziehungsweise Whaling-Angriffe herausgefunden werden wenn der Anwender nicht sorgsam mit diesen personenbezogenen Daten umgeht oder zu einfache Sicherheitsfragen definiert.
Hier ist entsprechend eine umfassende Mitarbeiter-Sensibilisierung rund um Themen wie CyberSecurity, Digitalisierung generell und auch rund um aktuelle Beispiele von Datenschutz-Verletzungen (data breaches) nötig.