Tipps für die Risikominderung durch strukturiertes Identity-Management

Ein effizientes und wirksames Identity-Management ist wichtiger denn je. Spätestens seit Unternehmen in der Lage sein müssen, eine breite Palette an externen Komponenten sicher in ihre IT zu integrieren und Businesspartner, Lieferanten sowie Kunden in die Geschäftsprozesse zu involvieren.

DER AUTOR

Marc Burkhard, CEO und Senior Solution Architect, ITSENSE

Ein Unternehmen muss in der Lage sein, den Zugang zu IT-Ressourcen zentral zu verwalten und jederzeit die Kontrolle darüber zu haben, wer diese wann und in welcher Weise nutzt. Eines ist sicher: Individuen mit kriminellem Potenzial, die sich zu wertvollen Informationen Zugang verschaffen wollen, haben die Zeit und den kreativen Intellekt, Schwachstellen aufzuspüren und auszunutzen. Dabei lieben sie die Herausforderung ebenso wie die Beute selbst.

Man bedenke: Die teuerste Firewall ist nutzlos, wenn Fremde oder ehemalige Mitarbeiter über kompromittierte Anmeldeinformationen, einfache Passwörter oder gar über noch aktive Benutzerkonten ungehindert auf wertvolle Ressourcen zugreifen können. Wer aber glaubt, die Bedrohung komme nur von aussen, der irrt sich. Es ist allgemein bekannt, dass die grössere Gefahr von innen droht.

Einige relativ einfache Aspekte des Identity-Managements erhöhen die Chancen erheblich, dass Angreifer aufgeben und weiterziehen. Einen Ausschnitt von Risikofaktoren und wie Sie diese vermeiden können, haben wir nachfolgend zusammengestellt:

Risiko #1 – Kompromittierte Anmeldeinformationen

Zu viele Mitarbeiter teilen ihre Anmeldeinformationen mit anderen Mitarbeitern oder arbeiten ohnehin mit gemeinsam genutzten Gruppenkonten, die statische Passwörter besitzen. Dies ist unter zwei Gesichtspunkten mit Risiken verbunden. Einerseits wird dadurch die eindeutige Nachvollziehbarkeit verhindert, wodurch im Schadensfall fehlerhafte oder gar kriminelle Handlungsfolgen keiner Person zugewiesen werden können. Andererseits sind schwache Authentifizierungsmethoden (Benutzername und Passwort) der einfachste Weg, sich Zugriff auf Ressourcen zu verschaffen. So erfolgen beispielsweise viele Angriffe auf Webseiten mit gestohlenen Anmeldeinformationen.

Die Risiken durch kompromittierte Anmeldeinformationen können durch Multi-Faktor-Authentifizierung (MFA) verhindert werden. Die Multi-Faktor-Authentifizierung (oft auch Strong-Authentication genannt) dient dem eindeutigen Identitätsnachweis eines Benutzers mittels der Kombination verschiedener und insbesondere unabhängiger Komponenten (Faktoren). Dabei handelt es sich typischerweise um Bekanntes (Passwort, PIN), Besitz (Token) oder Biometrisches (Iris, Fingerabdruck).

Risiko #2 – Der Mensch

Jeder kennt sie. Engagierte IT-Mitarbeiter, die jeden Wunsch erfüllen. Ein Anruf beim Service Desk genügt und man erhält das, was man braucht. Dies wäre aus der Perspektive des Endnutzers oder des Managements keine verwerfliche Verhaltensweise, würde dabei nicht der Faktor Mensch ein erhebliches Risiko darstellen. Nicht jeder Mitarbeiter ist gleich vertrauenswürdig. Manche Menschen nutzen Mittel und Wege, um Dinge zu erreichen, die ihre Kompetenzen überschreiten. Oder es wird darauf gedrängt, ein Anliegen schnell zu erledigen, und alle sicherheitsrelevanten Prozesse werden elegant umgangen. Ein gefundenes Fressen für Auditoren. Diese suchen am liebsten Auffälligkeiten, die leicht zu identifizieren sind. Dies wären etwa unangemessene Zugriffsberechtigungen, die einen Verstoss gegen die Trennung von Aufgaben und Verantwortlichkeiten darstellen (Seperation of Duty). Wer hat nun versagt? Der IT-Mitarbeiter verwaltet die Systeme und kann nicht wissen, wer im Unternehmen welche Aufgaben hat. Und er weiss schon gar nicht, wer was tun darf.

Das Risiko kann vermindert werden, indem die Kontrollen rund um die Entscheidungsfindung und die Umsetzung (die Provisionierung) automatisiert und dadurch Hürden für Anfragen entfernt werden. Die Aufgabe des IT-Mitarbeiters besteht nicht darin, zu entscheiden, welche Berechtigungen ein Mitarbeiter benötigt, sondern darin, dem Anfragenden schnell zu den notwendigen Berechtigungen zu verhelfen. Stellen Sie sich einen Lösungsansatz vor, bei dem der Mitarbeiter jederzeit über ein Portal unkompliziert den Zugang zu Ressourcen anfragen kann. Die Anfragen werden sofort gegen die definierten Sicherheitsrichtlinien geprüft und das hinterlegte, rollenbasierte Berechtigungsmodell (RBAC) angewendet. Anschliessend werden alle notwendigen Bewilligungsprozesse durchlaufen und bei Freigabe durch die verantwortlichen Personen automatisch umgesetzt. Ein IAM-System würde dies alles ohne Eingriff eines IT-Mitarbeiters erledigen und die Vorgänge detailliert protokollieren. So wird die IT entlastet und die Mitarbeiter erhalten ihre benötigten Zugriffe. Und das Beste: Der IT-Mitarbeiter kann seine eigentlichen Aufgaben erfüllen.

Risiko #3 – Komplexe Passwörter machen uns schwach

Die meisten tun es, auch wenn wir es nicht gerne zugeben. Wir müssen uns viele und komplexe Passwörter merken, sowohl im Geschäft als auch Privat. Wir erzeugen eine enorme Anzahl Benutzerkonten pro Jahr. Und wie helfen wir uns? Wir nutzen oftmals das gleiche komplexe Passwort, schreiben es auf und bewahren es in einer Schublade, auf einem Post-it unter der Tastatur oder in einer Notiz mit dem Namen «Passwörter» oder «vertraulich» auf. Das

Mitarbeiter haben zu viele Zugriffe, die ausgenutzt werden können. Bild: Fotolia

Risiko ist offensichtlich: Egal wie komplex das Passwort ist, wie gründlich man die Zugriffe überwacht und wie sauber man den Benutzer provisioniert, gerät das Passwort in die falschen Hände, ist das Spiel vorbei.

Diesem Risiko kann mit dem Ansatz der «Konsolidierung» begegnet werden. Wenn sich ein Mitarbeiter nur ein Passwort merken muss, steigt die Wahrscheinlichkeit, sich dieses merken zu können. Durch den Einsatz von Single-Sign-on-Technologien (SSO) kann eine sichere und einfache Nutzung mehrerer Systeme mit einem einzigen Passwort realisiert werden. Zusätzlich wird der Aufwand für Passwortrücksetzung durch die IT stark reduziert. Rund 33 Prozent von uns vergessen regelmässig Passwörter. Die Gefahr, die von aufgeschriebenen Passwörtern ausgeht, wird durch die Einführung eines zusätzlichen Faktors zur Authentifizierung massiv verringert.

Risiko #4 – Manuelle Provisionierung

In vielen Fällen können sich Mitarbeiter nach Auflösung des Arbeitsverhältnisses mit ihren Benutzerkonten weiterhin anmelden und auf wertvolle Unternehmensdaten zugreifen. Dieser Umstand ist vor allem auf ein schlechtes Berechtigungsmanagement und manuelle Provisionierung zurückzuführen. In der Praxis sind verschiedene Ausprägungen zu beobachten. Der Auszubildende, der von Abteilung zu Abteilung wandert, wodurch sich dessen Berechtigungen schrittweise in den Olymp erheben, das bequeme Kopieren von Benutzerkonten nach dem «Analog wie»-Prinzip und regelmässige Organisationsänderungen, die wie Dünger für das historische Wachsen von Berechtigungen sind. Das Resultat ist offensichtlich: Die Mitarbeiter haben zu viele Zugriffe, die ausgenutzt werden können. Die Forderung des Least-Privilege-Modells (minimale Berechtigungen für die Ausübung der Funktionen und Aufgaben im Unternehmen) konsequent anzuwenden, wird für die Security-Verantwortlichen zum Albtraum und für die IT-Mitarbeiter zum zeitaufwendigen Spiessrutenlaufen.

Abhilfe kann eine automatisierte, an den Bedürfnissen des Unternehmens ausgerichtete Provisionierung (und De-Provisionierung) schaffen. Mithilfe von Quellsystemen (wie ERP, HRM) können Ereignisse im Lebenszyklus eines Mitarbeiters automatisch und nahezu in Echtzeit abgebildet werden. Zulässige Berechtigungen werden fortlaufend und bei jedem Ereignis automatisch neu berechnet und adaptiert. Dies sollte ebenso für organisatorische Änderungen und für Änderungen am Anstellungsverhältnis gelten. Zusätzlich hilft die automatisierte Provisionierung bei der Steuerung zeitbegrenzter Berechtigungen, die oft bei Projekten oder Arbeitsgruppen benötigt werden. Alle Aktivitäten unterstehen dabei der zentralen und vordefinierten Richtlinienprüfung und erfordern bei Bedarf die Einholung oder die Bestätigung von Genehmigungen.