NOSTALGIE IST FEHL AM PLATZ

Die Nachfrage für Unterstützung aus dem Bereich des Identity & Access Management steigt stetig. Experten sehen den Markt bereits heute bei knapp 10 Milliarden Dollar. Bis 2025 könnte er sich noch einmal verdoppelt haben. Die Gründe dafür liegen in mehreren sich überlagernden Trends, die fast alle mit einem Bild beginnen.

Text: **Jan-Pieter Giele;**

Zwei graue Kästen, vor denen zwei Wörter stehen: Username. Passwort.
Bitte verraten Sie es nicht weiter: Bei mir ist es die linke, obere Schublade im Schreibtisch. Die, die so quietscht, wenn man sie herauszieht. Da liegen sie wild durcheinander, die Zettel mit den Passwörtern. Nicht einfach so! Sondern doppelt und dreifach gesichert: Jeder Unbefugte wird gnadenlos ausgetrickst, weil beim Passwort nicht dabeisteht, wofür es eigentlich ist. Und der besondere Sicherheitsclou: Das Passwort ist teilweise unkenntlich gemacht! Klasse, oder? Klitzekleines Problem ist nur, dass der einzige, der bislang von diesem Kuddelmuddel verwirrt und ratlos aufgefunden wurde, der rechtmäßige Inhaber der Accounts ist.
Als wäre diese in ähnlicher Ausprägung tausendfach wiederholte persönliche Tragödie nicht Grund genug, sich mit einem modernen Zugangsmanagement-System zu beschäftigen, wächst der Druck von außen: aufgrund zunehmender technischer und rechtlicher Anforderungen einerseits sowie wachsender Betrugsversuche andererseits.

VERSCHIEDENE TRENDS – DIESELBE RICHTUNG

Eine Software, die Administratoren und Anwender dabei unterstützt, einen einfachen Zugriff auf das richtige System von der befugten Person zu organisieren. Ein Programm, das Identitäten und Zugriffsrechte auf unterschiedliche Systeme und Applikationen verwalten kann. Eine Lösung, die Nutzer schnell und sicher authentifiziert und autorisiert. Das alles sind zentrale Funktionen eines Identity and Access Management (IAM). Dass der Markt für solche Lösungen weiter kräftig wachsen wird, mag an diesem Leistungsumfang liegen. Mit Sicherheit liegt die Nachfrage jedoch auch daran, dass die Risiken für Betriebe in diesem Umfeld so vielfältig wie schwerwiegend sind.

Die Risiken für Betriebe in diesem Umfeld sind so vielfältig wie schwerwiegend.

Kaum ein Unternehmen kann es sich leisten, seine Mitarbeiter unstrukturiert Rollen und Funktionen einnehmen zu lassen. Nicht umsonst stammt ein lauter Ruf nach Unterstützung daher auch aus Richtung der Personalabteilungen. Jeder Angestellte dürfte es schon einmal am eigenen Leib erfahren haben: Die mehr oder weniger chaotische Zeit beim Eintritt in ein neues Unternehmen. Formulare für die unterschiedlichsten Zugriffsberechtigungen werden da in den ersten vierzehn Tagen in Hausposttaschen gesteckt, bis sich endlich das Gefühl von „so langsam habe ich alle notwendigen Zugänge, um arbeiten zu können“ einstellt.
Glücklich schätzt sich die Abteilungsleitung, die überall ankreuzen kann, dass der oder die Neue dieselben Berechtigungen benötigt, wie sein oder ihr Vorgänger. Dann wird schnell ein Template kopiert oder die Berechtigungshäkchen abgeschaut. Doch in einer zunehmend projektbasierten Arbeitsweise ist selbst dieser Glücksfall allenfalls noch als Krücke zu bezeichnen. Demgegenüber zentralisiert und bündelt eine IAM-Software die Verwaltung von Identitäten und Zugriffsberechtigungen und steuert die punktgenaue Authentifizierung und Autorisierung der Mitarbeiter. In dieser zentralen Zugriffskontrolle bilden die Verantwortlichen auch komplexe Regelwerke ab, und zwar ausgerichtet auf die Anforderungen ihrer individuellen Organisationsstruktur. Diese betreffen nicht nur einen Neueintritt. Auch der Austritt von Mitarbeitern oder ein Wechsel innerhalb der Organisation kann hier zentral gesteuert werden.

Zumal auch unter aktuellen Compliance- und Sicherheitsgesichtspunkten wenig Spielraum für Nostalgie bleibt. Eine IT-Abteilung, die bei Austrittsprozessen mehrere Wochen benötigt, bis alle Berechtigungen gesperrt sind, kann ein juristisches wie auch ein Daten-Risiko bedeuten. Hinzu kommt, dass bestimmte Auftraggeber, beispielsweise aus der Automobilindustrie oder der Luftfahrt-Branche verbindliche Forderungen an die Organisationsstruktur bei ihren Zulieferern und Dienstleistern stellen. Hier stehen IAM-Themen vorn im Anforderungskatalog. Aus Sicht der Unterneh-

mensleitung kann ein IAM darüber hinaus eine wichtige Säule in der Digitalisierungsstrategie des Unternehmens darstellen. Betriebe, die sich intensiv über mehrere Abteilungen hinweg mit Themen wie Losgröße 1 und Industrie 4.0 beschäftigen, sind gut beraten, sich auch im Personal- bzw. IT-Bereich mit digitalen Lösungen bei der Identitäts- und Zugangskontrolle zu beschäftigen.

HACKERANGRIFFE ERSCHWEREN

Ein nicht sauber strukturierter Umgang mit Berechtigungen und Zugängen kann noch ganz andere Geister hervorrufen, die man nur schwer oder gar nicht mehr wieder losbekommt. Schubladen mit Passwort-Zetteln, Haftnotizen mit Passwörtern oder kleine Tesafilm-Streifen mit dem Code unter die Tastatur geklebt, genauso wie zigfach genutzte Passwörter und unübersichtliche Berechtigungen – solches Fehlverhalten öffnet auch Digital-Erpressern Tür und Tor. Verschiedene Fälle haben bereits gezeigt, dass der Diebstahl von Identitäten immer häufiger zu Lösegeldforderungen führt. Administratoren schränken das Risiko – und im Schadensfall das Ausmaß – deutlich ein, wenn sie in die Lage versetzt werden, den Anwendern einfach und unkompliziert nur die Rechte zuweisen zu können, die sie auch tatsächlich zur Erfüllung ihrer Aufgaben benötigen. Im besten Fall hat der IT-Mitarbeiter die Konten vom Zeitpunkt der Generierung bis zum Moment des Löschens dauerhaft im Blick und weiß über den korrekten Nutzungsumfang Bescheid.
Um den unbefugten Zugriff auf Programme und Inhalte zu erschweren, ist es zudem mittlerweile gängige Praxis, eine sogenannte Multifaktoren-Authentifizierung zu nutzen. Dabei wird auf einem mobilen Endgerät ein zusätzlich zum Namen und Passwort abgefragter Code erzeugt. Nicht nur in Chemieanlagen und Maschinenbaufabriken, sondern auch im Consumer-Bereich wie auf Social-Media-Plattformen oder für E-Mail-Konten wird die über die Abfrage eines zusätzlichen Software-Tokens erreichte Sicherheit nach und nach zum gängigen Standard. Allerdings sind die hierzu notwendigen Initialisierungsschritte nicht jedem Mitarbeiter kommentarlos zuzumuten. Die einfache Nutzerführung und Unterstützung der Anwender durch die IT und ein IAM-System sollten ebenso zum Stand der Technik gehören wie die Methode selbst.

DATENSCHUTZ HAT AN BEDEUTUNG GEWONNEN

Die Anforderungen an eine gut durchdachte Berechtigungsstruktur quer durch das gesamte Unternehmen und sämtliche Abteilungen vom Personalressort über das Auftragsmanagement oder Marketing wurden durch die europäische Gesetzgebung noch einmal deutlich verschärft. Die Datenschutzgrundverordnung aus dem Jahr 2018 zielt darauf ab, jedem Individuum die Hoheit über Speicherung und Umgang mit persönlichen Daten zu sichern. In der Konsequenz führt das dazu, dass der Zugriff auf persönliche Informationen von Mitarbeitern, Kollegen und Kunden klar geregelt und dokumentiert sein muss. Daher ist das sogenannte Access Governance ein wichtiger Bereich innerhalb eines IAM. Diese Programmfunktionen stellen sicher, dass Mitarbeiter genau den Zugriff auf Netzwerkbereiche erhalten, den sie für ihre Arbeit benötigen – und nur auf diese. Dass diese Server physikalisch häufig nicht mehr im Keller des Unternehmens stehen, sondern in dezentralen Cloud-Lösungen bereitgehalten werden, verschärft die Bedeutung eines professionellen Umgangs mit Authentifizierung und Autorisierung noch einmal. Der Service, den solche Cloud-Lösungen bieten, darf nicht zu einem Risiko in Sachen Datensicherheit und Access-Management führen. Hier ist es ratsam, bereits früh im Evaluationsprozess auf entsprechende Funktionalitäten der anzuschaffenden Software zu achten. Denn interne Dienste und Services werden sich (zumindest teilweise) künftig deutlicher in Richtung Cloud bewegen und sollten mit einer IAM gut erreicht werden können.

ANFORDERUNG AN MENSCH UND TECHNIK

Zum Wandel der Arbeitswelt gehört ein weiterer Aspekt: Der Digitalisierung auf dem Fuße folgt, dass sich starre Arbeitszeiten auflösen, da es nicht mehr nur noch den einen Ort bzw. Arbeitsplatz gibt, an dem eine Leistung erbracht wird. War es früher nur der Verkäufer im Außendienst, sind es heute fast alle Funktionen im Betrieb, die einen Teil ihrer Arbeit mobil leisten. So steht der Betriebsleiter heute mit einem Tablet-PC vor der Anlage und steuert sie. Browser-Anwendungen ermöglichen dem Ingenieur nicht nur in Alarmfällen am

Der Service, den Could-Lösung bietne, darf nicht zu einem Risiko in Sachen Datensicherheit führen.

Laptop Maßnahmen zu ergreifen und auf die Steuerung und Bedienung von Maschinen und Anlagen zuzugreifen, ohne vor Ort zu sein.
Dass diese neue Arbeitswelt zu mehr Komplexität in den IT-Abteilungen führt, liegt auf der Hand. Der Grad an Automatisierung und Flexibilisierung macht eine technische Unterstützung und Begleitung wie durch ein IAM unumgänglich. Betrachtet man die grundlegenden Veränderungen, die in vielen Betrieben derzeit durch Digitalisierung und Industrie 4.0 geschehen, wird sich diese Entwicklung weiter fortsetzen: Betriebe werden gezwungen sein, flexibler zu produzieren, Maschinen in den Fabriken und außerhalb werden mobiler und Mitarbeiter wechselnde Rollen an unterschiedlichen Standorten einnehmen müssen.

ANALYSIEREN UND AUSWERTEN

Dabei birgt die Nutzung von zentralen IAM-Programmen und den dabei entstehenden Daten innerhalb der eigenen Struktur eine weitere Chance, wie auch das IAM-Gartner-Summit Anfang März dieses Jahres inten- siv diskutiert hat. So erlebten über 1600 Konferenzteil- nehmer, Software-Hersteller, Beratungsunternehmen und Integratoren, wie sehr sich der Markt bewegt.
Demnach wird der Fokus künftig weniger auf Authentifizierung (Wer hat Zugriff?), Autorisierung (Was darf er tun?) und Administration (Steuerung der Berechtigung) liegen. Das simple Verwalten von Zugangsberechtigun- gen, also dem traditionellen ereignisgesteuerten Vor-

DYNAMISCH AGIEREN UND KOMPLEXE BERECHTIGUNGS-REGELN SYSTEM-ÜBERGREIFEND VERWALTEN.

gang, wird vielmehr durch die intelligente Analyse von identitätsbezogenen IAM-Informationen (Konten, Berechtigungen, Eigenschaften, Verhalten etc.) ersetzt werden. Beispielsweise birgt die Verhaltensanalyse erhebliches Potenzial. Dabei werden Informationen über das Nutzerverhalten gesammelt – etwa, dass sich ein Benutzer immer zu bestimmten Zeiten in bestimmten Netzwerken an bestimmten Orten anmeldet. Erfolgt diese Anmeldung zu völlig anderen Zeiten oder in einem anderen Kontext, können vordefinierte Handlungsabläufe aktiviert werden: Zugang sperren, Alarm auslösen und separate Zugriffsfreigabe anfordern.

Hier zeigt sich ein neuer Trend mit neuen Herausforderungen, der zu weiterem Wachstum im IAM Bereich führen wird. Das sich verändernde Technologieumfeld und die aktuellen Lösungen und Prozesse müssen an die neuen Anforderungen angepasst werden. Nicht umsonst prognostizierten die Gartner-Analysten in London, dass 63 Prozent aller Unternehmen aufrüsten und mindestens eine IAM-Technologie austauschen werden. Spätestens dann ist auch hier Schluss mit Nostalgie und quietschenden Schubladen voll mit Passwort-Zetteln.◀

Hier gelangen Sie zur Autorenseite mit weiteren Links und Empfehlungen des Autors.

Bild: Tools4ever Informatik GmbH

Jan-Pieter Giele

... ist Managing Director DACH sowie Nord & Osteuropa der Tools4ever Informatik GmbH, einem der globalen Marktführer im Bereich Identity- und Access-Management. Tools4ever gehört mit mehreren Millionen verwalteter Benutzerkonten zu den marktführenden Anbietern in den Bereichen Identity- und Access-Management.

MEHR DAZU

...finden Sie unter:
www.tools4ever.de

oder lesen Sie weitere Artikel zum Thema im Blog des Unternehmens:
www.tools4ever.de/blog