Leben und Arbeiten nach COVID-19

**„Das IAM-Management nach COVID-19 und die Möglichkeiten, die daraus entstehen“:
Die wichtigsten Erkenntnisse des virtuellen Roundtables von iC Consult und ForgeRock**

Im Fokus der Diskussion:

- IAM-Trends während der COVID-19-Pandemie
- Warum Passwörter nicht mehr zeitgemäß sind
- Schutz kritischer Infrastrukturen durch die Trennung von OT und IT
- Auswirkungen auf E-Commerce und Omni-Channel
- Weichenstellungen im Zuge von COVID-19

Nach vielen Monaten im Homeoffice ermöglichen sinkende Inzidenzwerte und steigende Impfzahlen erste vorsichtige Schritte in Richtung Normalität. Doch der Siegeszug der Digital Workplaces und der Teleworking-Modelle stellt viele Security-Abteilungen immer noch vor Herausforderungen: Immerhin gilt es im New Normal, die digitalen Identitäten unzähliger Mitarbeiter, Partner und Kunden effizient zu verwalten und zuverlässig zu schützen – On-Premises und in der Cloud.

Wie also soll das Identity & Access Management nach der Pandemie aussehen? Um dieser Frage auf den Grund zu gehen, veranstaltete die iC Consult Group GmbH einen virtuellen Excellence Talk zum Thema „Leben und Arbeiten nach COVID-19“. Die Runde aus geladenen Enterprise-Kunden sprach über ihre Erfahrungen in der Pandemie und erörterte, welche Richtungen ihre Unternehmen eingeschlagen haben und möglicherweise noch einschlagen werden.

Dr. Heiko Klarl, Chief Marketing und Sales Officer der iC Consult Group, und Gerhard Zehethofer, Vice President IOT & Technology Partnerships bei ForgeRock, führten durch den einstündigen Excellence Talk. Im Mittelpunkt der Runde standen neun Fragestellungen.

1. Schon vor der Pandemie rangen viele Unternehmen mit Problemen im Bereich Datenverwaltung und IAM. Welche Herausforderungen standen dabei im Fokus?

Wie jedes andere Werkzeug sollte auch IT leicht zugänglich sein und intuitiv verstanden werden. Genau an diesem Punkte scheitern aber zahlreiche IAM-Lösungen und andere Anwendungen. Ein Teilnehmer des Roundtables erklärt, dass ein normaler Arbeitsalltag heute daraus bestehe, Daten, Zahlen und andere Informationen in unzählige Masken einzugeben und dort zu verarbeiten. Da jedes Programm seine eigenen Funktionen und damit auch seine eigenen Stärken und Schwächen mitbringt, stehe das Team vor einem regelrechten Patchwork von Lösungen. Für jedes Programm müsse man umdenken und keines funktioniere richtig für sich allein.

Neben der Zahl der Anwendungen stellen auch die Programme selbst die Mitarbeiter immer wieder vor Herausforderungen: Viele Kollegen nutzen Anwendungen nur sporadisch, also in langen zeitlichen Abständen. In dieser Zeit hat die jeweilige Software aber oft mehrere Updates durchlaufen, sodass sich die erneute Nutzung völlig fremd anfühlt. Die Bedienung eines Programms nach einer Pause jedes Mal neu erlernen zu müssen, frustriert die Mitarbeiter und bindet zeitliche Ressourcen. Auch die IT wird dadurch zunehmend beansprucht, da mehr Service-Anfragen eingehen und Kollegen immer wieder neu angelernt werden müssen, um reibungslose Workflows zu garantieren.

2. Mit der Krise rückte IAM verstärkt in den Fokus. Neben der Sicherheit des Unternehmens galt es auch, die Workflows und die User-Experience zu optimieren. Wie gingen die Teilnehmer dabei vor, und welche Trends werden auch in der Post-COVID-Phase erhalten bleiben?

IAM-Trends während der COVID-19-Pandemie

Die Runde ist sich einig, dass eine vollkommene Rückkehr zu den Strukturen und Methoden vor COVID-19 ausgeschlossen ist. Viele Meilensteine, die in der Krise vollbracht wurden – etwa die Verlagerung weiter Teile der Belegschaft ins Homeoffice – werden uns auch in Zukunft begleiten. Die Teilnehmer sind überzeugt, dass der Trend dabei zu hybriden Workplace-Modellen gehen wird: Es wird Phasen geben, in denen Arbeitsabläufe und Termine die Mitarbeiter zwingen, in Präsenz zu arbeiten. Genauso werden sie phasenweise aber auch im Homeoffice bleiben. Ein Teilnehmer weist darauf hin, dass es vor diesem Hintergrund möglicherweise auch sinnvoll sein wird, die Identitätsabfragen mehrstufig aufzusetzen: Wer im Unternehmen präsent ist, wird dann weniger Faktoren zur Authentisierung benötigen als Mitarbeiter im Homeoffice.

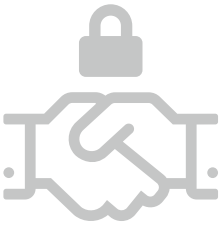
Ein anderer Teilnehmer berichtet, dass sein Unternehmen bereits vor den Lockdowns weitgehend cloudbasiert gearbeitet hat. Im Fokus standen One Portal und Office 365, und man habe sich auf Federated Identities konzentriert, damit ein Login für alle Dienste ausreicht. Gerade während des Lockdowns pushte das Unternehmen darüber hinaus MFA-Lösungen: Da die Anmeldedaten von Mitarbeitern mit weitreichenden Zugriffsrechten oftmals Ziel von Phishing-Attacken sind und jeder Breach mit hohen Kosten verbunden ist, bietet MFA zusätzliche Sicherheit und erleichtert auch das Management der Identitäten. Auch biometrische Lösungen wie Fingerprints stehen bei den Teilnehmern hoch im Kurs, da sie ein Höchstmaß an Sicherheit und Bedienkomfort vereinen.

3. Durch die schnelle Einführung von Cloud- und IAM-Lösungen konnte es leicht geschehen, dass Mitarbeiter mehr Zugriffsrechte erhielten, als sie tatsächlich benötigen. Wie lassen sich diese wieder anpassen?

Auf die pragmatische Rechtevergabe in der Krise muss nun eine Konsolidierungswelle folgen, bei der überprüft wird, welche Zugriffsrechte wirklich für den Einzelnen notwendig sind, inwiefern die Sicherheit durch die breite Vergabe gefährdet ist und wie die Security wieder verstärkt werden kann. Eine Möglichkeit ist es dabei, ein Intelligent Access System zu nutzen. Dieses weiß, welche Zugriffsrechte ein Mitarbeiter tatsächlich braucht und haben darf, und stuft ihn dementsprechend ein.

Assistenz-Systeme sind darüber hinaus in der Lage, für Mitarbeiter automatisch Zugriffsrechte vorzuschlagen, indem sie ähnliche Mitarbeiterprofile auswerten und sich an den darin enthaltenen Zugriffen orientieren. Dies erleichtert nicht nur die Auswahl der Rechte, sondern sorgt auch dafür, dass es Mitarbeitern nicht plötzlich an dringend notwendigen Zugriffsrechten fehlt.

Ein sogenanntes Birthright Access Management vergibt automatische Rechte, wenn es sich eindeutig belegen lässt, dass ein Arbeitnehmer aufgrund seiner Position und seines Tätigkeitsbereichs über bestimmte Zugangsrechte verfügen muss. Im Nachhinein können Unternehmen zudem so genannte Improval- und Beantragungsprozesse nutzen, um die Zugriffsprofile ihrer Mitarbeiter zu optimieren.



Zunehmende Verschmelzung von klassischem IAM und CIAM

4. Hat sich die Krise auf die Trennung zwischen IAM und CIAM ausgewirkt?

Die Diskussionsrunde ist sich einig, dass sich eine Verschmelzung von klassischem IAM (für Mitarbeiter und Partner) und CIAM (für Endkunden) anbahnt. Früher waren diese Bereiche klar getrennt. Mit zunehmend personalisierter Beratung benötigen die Mitarbeiter jedoch immer öfter Zugriff auf Kundendaten. Dafür müssen sie sich im gleichen System und Kontext wie der Kunde bewegen – denn nur so können sie ihn optimal betreuen und ein hochwertiges Einkaufserlebnis sicherstellen.

Ein Teilnehmer unterstreicht darüber hinaus, dass längst nicht alle Kunden aus dem homogenen B2C-Bereich entstammen (in dem alle Kunden in der Regel vergleichbare Rechte haben). Viele von ihnen stammen aus dem wesentlich heterogeneren B2B-Umfeld und benötigen mitunter ähnliche Rechte wie interne Mitarbeiter. Auch dies erschwert natürlich die klare Trennung von IAM und CIAM.

5. Eine Studie von ForgeRock hat gezeigt, dass viele Nutzer allzu komplizierte Anmeldevorgänge abbrechen. Der Log-in soll so einfach und komfortabel sein wie möglich – aber geht dies ohne Abstriche bei der Sicherheit?

Ein Teilnehmer erklärt, dass jedes Signal, das man von den Nutzern erhält, zum Verständnis des Nutzers beiträgt. Mit jeder neuen Information wird es einfacher, das aktuelle und das historische Verhalten des Users zu vergleichen. Und dies wiederum erleichtert es, ungewöhnliche Verhaltensweisen zu identifizieren, die auf einen fremden Zugriff hindeuten. Auf diese Weise entsteht beinahe so etwas wie ein „unsichtbares Identity & Access Management", bei dem Nutzer, deren Identität zweifelsfrei bestätigt wird, etwa auf Passwörter verzichten können. In besonders kritischen Bereichen ist zwar nach wie vor die Abfrage weiterer Faktoren nötig, aber grundsätzlich tritt das Zugriffsmanagement in den Hintergrund.

Mit Blick auf die Authentisierung der Mitarbeiter ist zu bedenken, dass Unternehmen gute Mitarbeiter oft nicht zuletzt durch gute Tools gewinnen und halten. Und dazu gehört eben auch ein benutzerfreundliches IAM.

6. Passwörter stehen oftmals in der Kritik, heutigen Security-Anforderungen nicht mehr gerecht zu werden. Warum ist das Passwort-Management so problematisch?

Immer mehr Unternehmen sehen davon ab, Passwörter zur Bestätigung der Identität (und damit als Schlüssel zu sensiblen Daten) zu nutzen. Der Grund: das problematische Passwort-Management. Ein Teilnehmer fasst es wie folgt zusammen: Unternehmen nutzen meist sichere, und damit auch komplizierte Passwörter, die – zumindest im Fall eines Single-User-Passwortes – mehrmals täglich eingegeben werden müssen. Die Realität zeigt, dass viele Mitarbeiter dieses Passwort notieren, es offen einsehbar am Arbeitsplatz drapieren oder sogar an Mitarbeiter weiterreichen, damit diese den gleichen PC nutzen können. Zusätzlich teilt es der Mitarbeiter außerdem auch mit der IT, sobald es Probleme mit Apps oder dem Endgerät gibt. Kurz: Das Passwort verbreitet sich und ist damit nicht mehr sicher. Dies ist den Usern jedoch oftmals nicht bewusst.

Warum Passwörter nicht mehr zeitgemäß sind

Ein weiterer Teilnehmer fordert ebenfalls eine passwortlose IT ein, da der Gewöhnungseffekt, Passwörter in Masken einzutragen, oftmals zum Eintrag in ein falsches Textfeld führen kann, was Phishing-Attacken den Weg bereitet. Er empfiehlt, stattdessen das Smartphone als zweiten Authentisierungsfaktor zu nutzen. Dieses personalisierte Gerät werde so häufig benutzt, dass dem User ein Verlust in der Regel sofort auffällt.

7. Inwiefern waren Unternehmen und Organisationen im Bereich der kritischen Infrastrukturen durch COVID-19 besonders herausgefordert?

Kritische Segmente wie Healthcare waren besonders von der Pandemie betroffen. Ein Teilnehmer aus dem Gesundheitswesen erklärt, dass bei ihnen etwa 80 Prozent der Mitarbeiter ins Homeoffice versetzt wurden, die es dann über die Cloud zu managen galt. Zusätzlich stellte die Organisation in großem Umfang neues Personal ein und führte im Zuge von Corona eine Umstrukturierung durch, sodass die IAM-Abteilung unzählige neue Identitäten in kürzester Zeit einrichten und anbinden musste.

Ähnlich äußert sich ein Teilnehmer aus einem Versorgungsunternehmen: Eigentlich sei man bestrebt, die klassischen IT-Netze (IT) und die nicht IP-basierten Industrienetze (OT) näher zusammenzuführen. Doch mit Blick auf die aktuelle Bedrohungslage im Versorgungssegment habe man die entsprechenden Projekte vorerst zurückgestellt. Obwohl IT- und OT-Security momentan also noch streng getrennt sind, will das Unternehmen seinen Mitarbeitern eine reibungslose Zusammenarbeit ermöglichen. Dies sei aber schwierig, weil das gesamte Unternehmen als kritische Infrastruktur bewertet wird und daher keine Cloudlösung integrieren darf. Das Ziel müsse es deshalb sein, KRITIS unterliegende Unternehmen künftig in einen besonders zu schützenden OT-Bereich und einen klassischen, weniger streng regulierten Office-Bereich zu untergliedern.

Schutz kritischer Infrastrukturen durch die Trennung von OT und IT

Es kommt der Einwand, dass eine solche Trennung zwischen OT und IT nicht vollständig möglich sei: Sobald ein Anwender über das gleiche Endgerät auf IT- und OT-Komponenten zugreift, entsteht eine Sicherheitslücke, die ein böswilliger Akteur nutzen kann. Die Diskussion wendet sich dann zum Zero-Trust-Ansatz: Um solch sensible Daten zu schützen, könnte es ein Weg sein, das „Vertrauen" und damit die Identität jedes Mal aufs Neue beweisen zu müssen. Dadurch werde automatisch auch überprüft, ob die Compliance des Endgerätes der Firmen-Policy entspricht.

8. Wie wirkte sich COVID-19 auf das Identity & Access Management in E-Commerce- und Omni-Channel-Umgebungen aus?

Auswirkungen auf E-Commerce und Omni-Channel

Eine aktuelle Studie belegt: Kunden werden auch nach COVID-19 weiterhin die Möglichkeit nutzen, online ewinzukaufen. Für die Bereitschaft zum Kauf ist dabei entscheidend, ob die richtigen Produkte auch zur richtigen Zeit angeboten werden. Um dies zu gewährleisten, muss das Unternehmen den Kunden kennen und dessen Daten sammeln, was in Europa allerdings nur unter Einhaltung der DSGVO möglich ist. Im Idealfall sollte der Kunde dabei nicht nur online bekannt sein, sondern auch im stationären Einzelhandel. Die digitale User-Experience muss also mit dem Instore-Erlebnis verschmelzen. Die Voraussetzung dafür ist ein integriertes IAM-System, das den Kunden ganzheitlich erfasst.

Wichtig dabei: Die Bereitschaft, Daten zu teilen, ist auf Seiten der Kunden besonders hoch, wenn sie dafür etwas zurückbekommen – etwa ein besonders hochwertiges Einkaufserlebnis oder persönliche Beratung.

9. Sind die Erfahrungen der Pandemie nur eine Herausforderung? Oder kann man daraus auch etwas Positives gewinnen?

Die Teilnehmer stellen fest, dass die digitale Transformation während der Pandemie für Unternehmen und Mitarbeiter einen echten Culture Change bedeutete. Der Wechsel in das Home-Office erforderte zweifellos Kompromisse, beispielsweise mit Blick auf die soziale Interaktion mit den Kollegen, und die Mitarbeiter mussten auch wesentlich stärker darauf achten, die Work-Life-Balance aufrechtzuerhalten. Hinzu kamen vielfach technische Hürden wie überlastete Netzwerke, weil sich die ganze Familie tagsüber für Arbeit und Schule das heimische Internet teilte. Dennoch zeigte der „COVID-Schwung" auch, welche neuen Möglichkeiten die IT im Arbeitsalltag bietet und welche neuen Freiheitsgrade sich daraus ergeben. Zudem brachte die Flexibilität des Home-Office auch ein deutlich freieres Zeitmanagement mit sich. COVID-19 war also nicht nur eine Herausforderung, sondern bot auch neue Optionen, die Unternehmen auch nach der Pandemie im Blick behalten sollten.

Fazit: Die Krise war auch ein Wegbereiter für Innovationen

Weichenstellungen im Zuge von COVID-19

Am Ende sind die Teilnehmer des virtuellen Roundtables einer Meinung: Auch wenn das Jahr 2020 sie vor etliche Herausforderungen stellte – von der Ad-Hoc-Einführung von Digital Workplaces bis hin zur Neudefinition des Identity & Access Managements – bereitete die Krise auch den Weg für viele Innovationen und neue Lösungsansätze. Eine moderne und umfassende IAM-Produktpalette, wie sie etwa ForgeRock bietet, ermöglicht es den Unternehmen heute, die Weichen für ein agiles, skalierbares und sicheres Identity & Access Management zu stellen. Während dem gesamten Lifecycle der Identity und Access Management Lösung – von der Auswahl über die Implementierung bis hin zum Managed Service – helfen die Experten der iC Consult ihren Kunden dabei die digitale Transformation voranzutreiben und einen maximalen ROI der eingesetzten Lösungen zu sichern.