Living and Working after COVID-19

IAM and its opportunities post-pandemic: key findings from the virtual roundtable hosted by iC Consult and ForgeRock

Focus of Discussion:

- IAM trends during COVID-19
- Why passwords are no longer enough
- Protection of critical infrastructures by separating OT and IT
- Effects on e-commerce and omnichannel environments
- Setting the course informed by COVID-19

After many months of working from home, falling incidence rates and rising vaccination figures are enabling the first cautious steps toward normality. But the triumph of digital workplaces and teleworking models still poses challenges for many security departments: After all, in the "new normal", the digital identities of countless employees, partners, and customers must be efficiently managed and reliably protected – both on-premises and in the cloud.

So, what should Identity & Access Management look like after the pandemic? To get to the bottom of this question, iC Consult Group GmbH hosted a virtual Excellence Talk: „Living and Working after COVID-19". The panel of invited enterprise customers talked about their experiences during the pandemic and discussed the directions their companies have taken and may take in the future.

Dr. Heiko Klarl, Chief Marketing and Sales Officer of iC Consult Group, and Gerhard Zehethofer, Vice President IOT & Technology Partnerships at ForgeRock, led the one-hour Excellence Talk. The panel focused on nine questions.

1. Even before the pandemic, many companies were struggling with data management and IAM issues. What were the main challenges?

Like any other tool, IT should be easily accessible and intuitively understood. However, this is precisely where many IAM solutions and other applications fail. One participant in the roundtable explained that a normal working day today consists of entering data (numbers and other information) into numerous masks, and processing it there. Since each program has its own functions, and thus its own strengths and weaknesses, the team is faced with a patchwork of solutions. You have to approach each program differently – and none works properly on its own.

In addition to the number of applications, the programs themselves also pose challenges for employees: Many colleagues access applications rarely, with long intervals between uses. During this time, however, the respective software has often gone through several updates, so that using it again feels completely foreign. Having to relearn how to use a program again and again frustrates employees, and wastes valuable time. It also puts an increasing strain on IT: More service requests come in, and colleagues have to be repeatedly retrained to ensure smooth workflows.

2. With the crisis, IAM became more of a focus. In addition to enterprise security, companies sought to optimize workflows and user experience. How did the participants proceed with this, and what trends will remain in the post-pandemic phase?

IAM trends during COVID-19

The roundtable agreed that a complete return to the structures and methods used before COVID19 is out of the question. Many milestones achieved during the crisis – such as the relocation of large parts of the workforce to home offices – will continue to accompany us in the future. The participants are convinced that the trend will be toward hybrid workplace models: There will be phases in which processes and deadlines demand in-person work. But there will also be times when employees can work from home. In light of this, one participant pointed out, it may also make sense to set up identity queries on several levels: Those who are in-person at the company will then need fewer factors for authentication than the employees who are working remotely.

Another participant reported that his company was already largely cloud-based prior to lockdown. The focus was on One Portal and Office 365, and on federated identities, making one login sufficient for all services. During lockdown, in particular, the company also pushed MFA solutions. After all, employees with wide-ranging access rights are often the target of phishing attacks, and each breach comes at a high cost. MFA provides additional security – and makes it easier to manage identities, too. Biometric solutions such as fingerprints are also highly popular among participants, as they combine maximum security and ease of use.

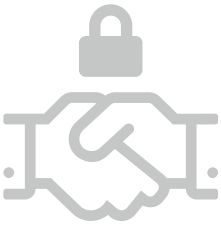
3. With the rapid adoption of cloud and IAM solutions, some employees received more access rights than they really needed. How can this be adjusted?

The pragmatic assignment of rights during the crisis must now be followed by a wave of consolidation, examining which access rights are really necessary for the individual, to what extent the broad assignment poses a security risk, and how to strengthen security again. One approach would be to use an intelligent access system. It knows which access rights are currently required and permitted, and it classifies employees accordingly.

Assistance systems are also able to automatically suggest access rights for employees by evaluating similar employee profiles and the accesses they contain. This not only facilitates the selection of rights, but also ensures that employees do not suddenly lack urgently-needed access rights.

A so-called birthright access management system automatically assigns rights if it can be clearly demonstrated that an employee must have them, based on his or her position and scope of activities. In retrospect, companies can also use so-called improvement and application processes to optimize the access profiles of their employees.

4. Has the crisis affected the separation between IAM and CIAM?



A merging of classic IAM and CIAM is on the horizon

The panel agreed that a merging of classic IAM (for employees and partners) and CIAM (for end customers) is on the horizon. In the past, these areas were clearly separated. However, with increasingly personalized consulting, employees need access to customer data more and more often. To do this, they need to be in the same system and context as the customer – this is the only way they can provide them with the best possible service and ensure a high-quality shopping experience.

One participant also emphasized that not all customers come from the homogeneous B2C area (in which all customers generally have comparable rights). Many of them come from the much more heterogeneous B2B environment and sometimes require similar rights as internal employees. This, of course, further complicates the clear separation of IAM and CIAM.

5. A study by ForgeRock has shown that many users abandon overly complicated log-in processes. Logging in should be as simple and convenient as possible – but can this be done without compromising on security?

One participant explained that every "signal" received from a user helps the company better understand that user. With each new piece of information, it becomes easier to compare the user's current and historical behavior. This, in turn, makes it easier to identify unusual behaviors that indicate foreign access. In this way, something like "invisible" IAM is created: Users whose identity is confirmed beyond doubt can dispense with passwords, for example. In particularly critical areas, it is still necessary to query other factors, but access management is generally relegated to the background.

Regarding the authentication of employees, companies need to remember that they often attract and retain good employees by offering good tools. And this includes user-friendly IAM.

6. Passwords are often criticized for not meeting today's security requirements. Why is password management so problematic?

More and more companies are refraining from using passwords to confirm identity (and thus as the key to sensitive data). The reason: problematic password management. One participant summarized it as follows: Companies usually use secure, and thus also complicated, passwords that – at least in the case of a single-user password – have to be entered several times a day. Reality shows that many employees write down this password, post it in full view at their workplace, and even pass it on to co-workers

Why passwords are no longer enough

so that they can use the same PC. In addition, the password is also shared with IT whenever there are problems with apps or the end device. In short: The password spreads and is therefore no longer secure. However, users are often not aware of this. Another participant also calls for password-free IT, since the habit of entering passwords in masks can often lead to an entry in the wrong text field, which paves the way for phishing attacks. Instead, he recommends using the smartphone as a second authentication factor. A phone is personal, and handled so frequently that the user usually notices right away if it gets lost.

7. To what extent were companies and organizations with critical infrastructure challenged by COVID-19?

Critical segments such as healthcare were particularly affected by the pandemic. One participant working in healthcare explained that about 80 percent of their staff were working from home, and this had to be managed via the cloud. In addition, the organization hired new staff on a large scale and also restructured as a result of COVID-19, so the IAM department had to set up and connect a large number of new identities in a very short time.

A participant from a utility company expressed a similar opinion: The company is striving to bring the traditional IT networks and the non-IP-based industrial networks (OT) closer together. But in view of the current threat situation in the utilities segment, the corresponding projects have been put on hold. So, although IT and OT security are still strictly separated at the moment, the company wants to enable its employees to work together smoothly. This is difficult, however, because the entire company is considered "critical infrastructure" and is thus not allowed to integrate a cloud solution. So the goal must be to divide companies subject to CRITIS into an OT area that requires special protection, and a classic, less strictly-regulated office area.

Protection of critical infrastructures by separating OT and IT

The objection was raised that such a separation between OT and IT is not completely possible: As soon as a user accesses IT and OT components via the same end device, this creates a security gap that a malicious actor can exploit. The discussion then turned to the Zero Trust approach: In order to protect such sensitive data, one way could be to have to prove "trust", and thus identity, anew each time. This would also automatically check whether the compliance of the end device corresponds to company policy.

8. How did COVID-19 impact IAM in e-commerce and omnichannel environments?

Effects on e-commerce and omnichannel environments

A recent study has shown: Customers will continue to use the opportunity to shop online even after the pandemic ends. The decisive factor for their willingness to buy is whether the right products are offered at the right time. To ensure this, the company must know the customer and collect their data, which is only possible in Europe in compliance with the GDPR. Ideally, the customer should not only be recognized online, but also in brick-and-mortar retail. The digital user experience must therefore merge with the in-store experience. The prerequisite for this is an integrated IAM system that captures the customer holistically.

It is important to note that customers are particularly willing to share data if they receive something in return – such as a higher-quality shopping experience or personal advice.

9. Are the experiences of the pandemic only a challenge? Or is there something positive to be gained?

The participants noted that the digital transformation during the pandemic entailed real, cultural changes for companies and employees. The move to working from home undoubtedly required compromises, for example regarding social interaction with colleagues, and employees also had to become more vigilant about maintaining a work-life balance. In addition, there were often technical hurdles such as overloaded networks during the day, since the entire family shared one Internet connection for work and school. Nevertheless, the COVID-19 crisis also showed the new possibilities that IT brings to the workday, and the new levels of freedom that result. The flexibility of working from home also opened up new possibilities for time management. So the pandemic was not only a challenge; it revealed alternatives. And companies should keep these in mind even after the pandemic.

Setting the course informed by COVID-19

Conclusion: The crisis fostered innovations

In the end, the participants of the virtual roundtable all agreed: Although 2020 presented them with several challenges – from the ad-hoc introduction of digital workplaces to the redefinition of identity and access management – the COVID-19 crisis also paved the way for many innovations and new approaches. A modern and comprehensive range of IAM products, such as those offered by ForgeRock, lets companies set the course for agile, scalable, and secure Identity & Access Management. Throughout the lifecycle of the IAM solution – from selection to implementation to managed service – the experts at iC Consult help their customers drive digital transformation and ensure maximum ROI from the solutions deployed.

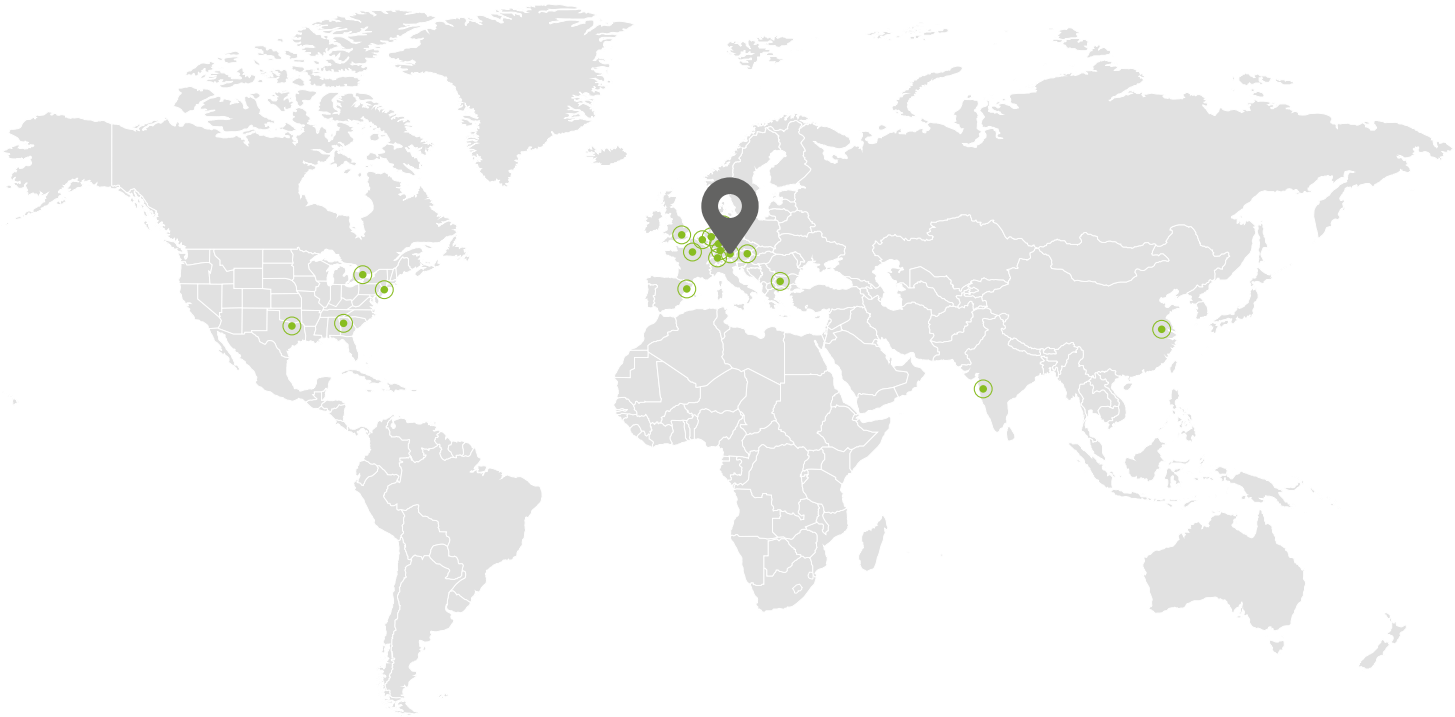
About iC Consult

iC Consult is the world's leading independent consultancy, systems integrator, and managed services provider for Identity & Access Management with more than 800 employees worldwide.

We are committed to excellence and innovation, and with the best-in-class technology in the IAM space, we provide our customers with next-level cybersecurity solutions. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations.

iC Consult is headquartered in Germany with offices in Switzerland, Austria, France, Belgium, Spain, Bulgaria, the UK, the U.S., Canada, India, and China. The world's largest brands trust in our expertise, to secure and manage their most valuable assets: their identities.

More information at www.ic-consult.com



iC Consult GmbH | Leopoldstr. 252b | 80807 München | Deutschland | sales@ic-consult.com | **www.ic-consult.com**