E&P CONSULTING

Today’s challenges in Identity and Access Governance

Oliver Lukačovič

Manager | Head of IAM

ol@eberhardt-partner.com

Agenda

Identity and Access Governance

IAG (Identity and Access Governance) is a top priority on every IT managers list these days. IAG is crucial to enable new agile business models by allowing fast and controlled access of all types of users to all types of IT resources and services. Without an IAG in place it is almost impossible to achieve regulatory compliance or to ensure IT governance.

Most current IAG implementations focus on the on-premises infrastructure which worked in the past. Today IAG requires to support external users over on-premise and Cloud applications by still ensuring regulatory compliance. On the other hand there are several new opportunities modern IAG have to offer: hybrid management on-premise and Cloud, risk- and context-based authentication and authorization, integration with IT service management to name a few.

If you build your IAG around an on-premise, security-in-the-depth philosophy you might not be able to answer current challenges. The IAG industry is evolving very fast and strategies and best practices formulated 5 years ago might not be valid anymore.

A few years ago, the IAG market exploded into enterprise, consumer and IoT centric IAG systems. This separation was maybe wrong and is now harmful for many IT organizations. We have accepted that we do not know what technology brings in the future. But we have also to accept that we do not know how work will be organized in the future. Trends like home office, DevOps, agile management, share economy and so on have a huge impact on your IAG strategy.

Therefore, a company should implement a dynamic IAG that serves employees, customers, partners and devices equally today.

Modern identity management

Besides people, in times of Artificial Intelligence more and more services and devices are assigned identities across networks. Identity services should be simple, flexible, scalable and fulfill their main purpose to quickly and securely verify identities and access privileges.

Today’s solutions must link devices and mobile and social apps to a single security platform that works all the time, everywhere, on premises or off in the cloud. This is the standard that customers, citizens, and students expect, and CIOs and their businesses, (as well as governments and universities), must identify vendors that can provide it because these methods of consumer engagement directly drive revenue. Customers might deposit checks from their phone, order a service through a cloud app, or make a purchase from a laptop that recognizes their identity, and shares the right information with the vendor.

Identity and access management tools are a necessity for managing trust relationships with parties inside and outside of a company – relationships that are now tied directly to the business’ top line.

Consumers and things must be considered equally to employees. In the past IAG systems were designed for employees only with their primary user account situated in one, on-premise central user repository (e.g. Active Directory). Modern identity management must manage access privileges for all stakeholders across a variety of devices.

Today’s challenges

As a result, the following **challenges** should be put into consideration when planning an Identity and Access Governance system:

SECURITY: Flexible work forces and mobile devices making it difficult to ensure security. For example, logging in from different devices might be correct but not at the same time from different locations. In uncertain circumstances an IAG system might consider a password is not enough and ask for a second authentication factor.

SOLUTION: An IAG system must take the context of an authentication into consideration by imbedding an identity analytic solution or a SIEM system.

REQUIREMENTS: Constantly changing compliance requirements are often difficult to implement even with an IAG System. For example, the implementation of the European GDPR had been expensive and stressful for most companies.

SOLUTION: Design the IAG System not only for current needs but instead implement it from the beginning as mandatory enterprise-wide identity broker with a flexible API.

OPPORTUNITIES: IAG systems have always been considered a costly necessity. Now IAG systems are an important business enabler. Without an IAG system for example a cloud-based business strategy could not be realized. Companies will miss business opportunities if their IAG solution takes too long to deploy, adapt, or respond to user events. The cloud, social media, mobility, and new business models are revolutionizing enterprises and IAG systems should play an important part to help businesses to seize new opportunities.

SOLUTION: IT Manager should also consider speed, ease of use and scalability additional to implementation and cost of deployment.

SHIFT: The industry focus is shifting from on premise solution to cloud services. The workforce consists not any longer solely on employees but also on partners, suppliers, customers, services and devices signing in from anywhere in exponentially growing numbers.

SOLUTION: Every IAG system should be designed to be instantly scalable in terms of technology, services and licensing.

WORKFORCE: Perimeter-based security is not sufficient anymore. The corporate workforce must be able to work from anywhere.

SOLUTION: The security model should not only regulate data storeed on company premises, but also by SaaS providers or cloud applications.

IMPLEMENTATION: A large group of IAM implementations are based on a monolithic architecture. Despite the products ability to handle service requests too many provisioning tasks are still done via file transfer. This has a negative effect on IT service delivery in many aspects.

SOLUTION: Build an open, service oriented IAG architecture that can offer IAG services to other applications.

If you feel not too confident with your IAG after considering these six challenges changes are that you should review your current IAG.

IAG (Identity and Access Governance) is a top priority on every IT managers list these days. IAG is crucial to enable new agile business models by allowing fast and controlled access of all types of users to all types of IT resources and services. Without an IAG in place it is almost impossible to achieve regulatory compliance or to ensure IT governance.