Identity Security as a Service: Protect Your Identities Always and Everywhere.

In the digital world, identity protection has become increasingly important. Did you know that identities can be easily forged using today's technical resources? Classic identity access management (IAM) forms the basis and the organizational framework for identity protection. With identity security as a service, we go one step further and protect your identities always and everywhere.

Identity management ensures that the right person will have appropriate access to the resources for which they are authorized. This is easily said, but not as easily implemented.

There are a number of typical vulnerabilities and threats that will be detected by network and cloud security solutions. For identity protection, the following three vulnerabilities require special attention:

1. Unmanaged identities: Dealing with privileged access, local admin rights, impersonal accounts, and generally with the identities process (inactive identities, etc.).
2. Misconfigured identities: These include shadow administrators, service accounts, weak passwords, and poor encryption practices that facilitate access into a network.
3. Exposed identities: These include stored login credentials and access tokens that can be accessed by hackers.

How does UMB identity security as a service work?

Identity security as a service permanently monitors your identities and keeps an eye on their attack surface. Identity security as a service consists of modules, which complement each other. The following functionalities are included per module:

- Active monitoring and hardening of onPrem and Azure Active Directories(AD)
- Analyzing configuration changes on AD
- Detecting and eliminating unnecessary access rights
- Identifying critical vulnerabilities at the domain, computer, and user levels (AD and Azure AD)
- Regular auditing of relevant cloud and onPrem components - such as remote access solutions, firewall configurations, backup, printers, servers, file servers, and databases

Your advantages

- Continuous or regular testing of the security status according to best practice
- Possible attacks will be prevented at the outset
- Attackers will be stopped and cannot complete an attack

Service components

- Continuous monitoring of the AD
- Immediate customer notification in case of critical identity vulnerabilities
- Comprehensive monthly service report
- Regular audit reports on defined audits
  - Recommendations for improvement
  - Comparison of current status vs. last status

Want to feel safe all around? Contact us!

We are happy to answer your questions regarding identity as a service

Contact

Markus Kaegi
Team Leader Strategic Sales Consulting
markus.kaegi@umb.ch
+41 58 510 16 98
www.umb.ch/security