predica.
make IT happen

SaaS, IaaS, PaaS – how to manage and use them safely?

Regardless of offering type, be it Office 365, Azure infrastructure or service, or data analytics services, they all have one thing in common: security! At the same time, most companies still maintain on-premises software and most of their users work within a local network, based on the services provided by the Active Directory.

- How to connect the two? How to build a correct connection between our local Active Directory and on-line Microsoft cloud services?
- Once our user identities are in the cloud, how to maintain security of services and data processed there?
- What options does Azure platform offer in terms of identity and application security?
- How to store sensitive data and protect our systems and applications in the cloud?
- Which IAM model to implement? How to manage resource access, delegate access to individual services and monitor their use?

Our dedicated **Azure platform security workshop** for businesses will answer these questions and more!

We will give you practical information to help your organization design and set up cloud access, and then show you how to properly manage security mechanisms available on the platform.

This two-day workshop will give you essential knowledge and hands-on experience of the Azure platform security services.

Day 1: Identity and access in Azure. Building a hybrid access solution for on-line services

- Service access architecture between the local AD and Azure AD
- Types of objects and identities in Azure AD
- Methods of authentication and SSO configuration between AD and Azure AD (federated access, password synchronization, pass-through authentication, seamless SSO)
- Architecture and configuration of Azure AD Connect. Maintaining service accessibility and reliability
- Synchronizing objects from the local AD to Azure AD
- Configuring Azure AD: managing objects, licences and application access
- Configuring password reset for users through Azure AD
- Azure AD administrative model: built-in roles and their management
- Managing admin roles with Privileged Identity Management

Day 2: Access management, administrative model and Azure security services

- Azure AD administrative model
  - Resource management through Resource Groups
  - Delegating access to Azure resources within IaaS / PaaS
  - RBAC model in Azure
- Securing Azure IaaS services with Azure Security Center
  - Monitoring service configuration and virtual machines
  - Detecting incompatibilities with required configuration
  - Just-in-time access to Azure network resources
- Azure applications security model
  - Security model for application access to Azure resources
  - Managing security principals and application configuration
  - Managed Service Identities and their use in applications
- Managing access to sensitive information, KeyVault services
- IAM services
  - Conditional Access
  - Identity Protection