An advanced guide through the Azure Security jungle
Eric Berg

Lead IT-Architekt – Team Azure / Team Modern Workplace

Azure, Datacenter and Modern Workplace

Azure, System Center, Windows Server and Client

info@ericberg.de

@ericberg_de | @GeekZeugs

www.ericberg.de | www.geekzeugs.de
Security Jungle?!
Intelligent Cloud Conference 2018

Maximum CONTROL

IaaS

Trusted Execution Environment

Isolated VMs

Azure Active Directory, Azure Key Vault

Maximum TRUST

PaaS

SQL Database Transparent Data Encryption, VNet Private Access

Azure control plane, just in time access, monitoring, auditing, and reporting

SaaS

Customer Lockbox

Underlying trusted platform
Security Components?!
Datacenter Security

Perimeter
- Barriers
- Fencing

Building
- Seismic bracing
- Security operations center
- 24X7 security staff
- Days of backup power

Computer room
- Cameras
- Alarms
- Two-factor access control: Biometric readers & card readers
Physical Security

- Azure regions
- access control
- video surveillance
- weight locks
- In-house disc destruction

https://cloud-platform-assets.azurewebsites.net/datacenter
Secure Multi-tenancy

- Isolates customer environments using the Fabric Controller
- Runs a configuration-hardened version of Windows Server as the Host OS
- Uses Hyper-V – a battle tested and enterprise proven hypervisor
Network Protection

- Provides logical isolation while enabling customer control

- Restricts access from the Internet, permits traffic only to endpoints, and provides load balancing and NAT at the Cloud Access Layer

- Private IP addresses are isolated from other customers
Virtual Networks / VPN

- Extension of own Datacenter to Azure
- Dedicated Express Route connection
- Management over VPN
- Network Security Group (NSG)
- Azure Software Defined Network
Azure’s DDoS defense system is designed not only to withstand attacks from the outside, but also from within.

Azure monitors and detects internally initiated DDoS attacks and removes offending VMs from the network.
Data Segregation

- Stored data accessible only through claims-based IDM & access control with private key
- Storage blocks are hashed by the hypervisor to separate accounts
- SQL Azure isolates separate account databases
- VM switch at the host level blocks inter-tenant communication
Data Protection

Data segregation
Logical isolation segregates each customer’s data from that of others.

In-transit data protection
Industry-standard protocols encrypt data in transit to/from outside components, as well as data in transit internally by default.

Data redundancy
Customers have multiple options for replicating data, including number of copies and number and location of replication datacenters.

At-rest data protection
Customers can implement a range of encryption options for virtual machines and storage.

Encryption
Data encryption in storage or in transit can be deployed by the customer to align with best practices for ensuring confidentiality and integrity of data.

Data destruction
When customers delete data or leave Azure, Microsoft follows procedures to render the previous customer’s data inaccessible.
Azure Active Directory

- Only authorized Access allowed
- MFA
- Privileged Identity Management
- Standard Protocols
- Stand-Alone or Hybrid
- Application Integration
RBAC

- Connection between Azure AD and Subscription
- Default Roles
  - Owner
  - Contributor
  - Reader
- Other Roles
  - Automation Operator
  - DevTest Labs User
  - …
- Own Roles
Azure Hierarchy

Enrollment

Country / Branch / Subsidiary

Accounts

Subscription Application1

Country / Branch / Subsidiary

Accounts

Subscription ProjektA Application2

Country / Branch / Subsidiary

Accounts

Subscription ...

Country / Branch / Subsidiary

Accounts

Subscription ...

Country / Branch / Subsidiary

Accounts

Subscription ...
„IT's not going to be easy…“

- Billing?!
- User Rights?!
- Protection?!
- Standards?!
- Audits?!
Guide?!
Azure Security Guide

- Operations Management Suite
- Azure Monitor
- Azure AD
- Azure Security Center
- Azure Investigation Dashboard
- Azure Network Watcher
- Traffic Analytics / NSG Flow
- Azure Advisor
Azure Security Center
Azure Security Center

Free for Azure Resources

- Security policy, assessment, and recommendations
- Connected partner solutions

15 $ / Month Azure and Hybrid (incl. free)

- Security event collection and search
- Just in time VM Access
- Adaptive application controls
- Advanced threat detection for networks, VMs/servers, and Azure services
- Built-in and custom alerts
- Threat intelligence
Quiz:
What is the most common attack targeting IaaS VMs?
Azure Security Center
JIT VM Access

- Known IP ranges
- 100,000 attacks/month/VM (RDP and SSH)
- Easy access to local accounts
- Always open
DEMO
Next Steps?!
Reading educates …

• Azure Virtual Datacenter Whitepaper
  • https://azure.microsoft.com/de-de/blog/azure-virtual-datacenter/

• Azure Security Overview
  • https://docs.microsoft.com/en-us/azure/security/azure-security

• Azure Trust Center
Network Security Groups
Azure AD
VPN / Express Route
Azure Security Center
Encryptio
Network Logging
Azure Monitor
Audit
Reporting
Subscriptions
Antimalware
Azure Advisor
Automation
Key Vault
Resource Policies
Network
MFA
VPN / Express Route
Encryption
Questions?!