CONSALTA
your success is our passion
AZURE SALES STAR PROGRAM IN CEE

PLANNING AZURE INFRASTRUCTURE SECURITY - AZURE ADMIN ACCOUNTS PROTECTION & AZURE NETWORK SECURITY

MAR 2017

IGOR SHASTITKO

WWW.CONSALTA.SI
About Consalta

Every business deserves an opportunity to grow! We support IT companies at growing their business in the Cloud. We are the Cloud Business Enablers!

- 1000+ CLIENTS
- 200+ ONSITE ENGAGEMENTS
- 180+ WEBINARS
- 40+ COUNTRIES
- 4,84 RATING
IGOR SHASTITKO

ROLE
• Senior Infrastructure/Security Consultant

WORK
• Microsoft Partners
• Microsoft Learning Centers
• Microsoft MCS

BACKGROUND
• Computer Science
• MCSE/MCT
• Geek 😊

PLEASURE
• Family
• Video Blogging
• Gadgets & technologies
Azure Sales Star program – Sessions – 10AM (CET)

- **FEB 6, 2017**
  Azure Security Scenarios - Overview of Main Scenarios for Security Projects

- **FEB 9, 2017**
  New Partner Opportunities to Plan Cloud/Hybrid Identity Projects

- **FEB 13, 2017**
  Fine-Tune The Details of Planning Hybrid Identity Protection

- **FEB 16, 2017**
  Provide a Full Management Experience for Hybrid Infrastructure

- **FEB 20, 2017**
  Secure Mobile Users Planning: Mobile Device Management (MDM) Scenarios Comparison

- **FEB 27, 2017**
  Implementing Microsoft Intune to MDM

- **FEB 27, 2017**
  Planning Data Access & Protection in Hybrid Infrastructure

- **MAR 1, 2017**
  Planning Hybrid Data Protection at the File Level

- **MAR 6, 2017**
  Planning Azure Infrastructure Security

- **MAR 9, 2017**
  Planning Azure Infrastructure Security – Data Protection in Azure
Agenda for the following 45’

- **Security Discussion**
  - Are Cloud Solutions protected?

- **Customers Case Study**
  - How to start fast

- **Azure IaaS Security**
  - Identity & Networking

- **What is next**
  - Webinars and resources
Cloud IaaS Solutions security threats

1. THE RESEARCH
2. NEW IDEAS
3. THE GAP
4. THE PLAN
5. THE CHANGE
6. THE EVALUATION
THE MAIN QUESTION IS:

ARE CLOUD SOLUTIONS PROTECTED?
“Drivers for using Cloud services are diverse. Most companies deciding for Cloud look at scalability, agility, and cost savings as part of their cloud strategy. However, many of these companies wonder if staying secure and private is an attainable reality or if they are compromising their business by transitioning to the Cloud.

Microsoft, Cloud Security Architecture
ATTACKS AGAINST CLOUD ADMINISTRATORS

Targeted attacks against on-premises and cloud infrastructures alike often focus on IT administrators. The intent is to take control of an email account that has a high probability of containing credentials that can be used to gain access to the public cloud administrator portal.

PIVOT BACK ATTACKS

A pivot back attack occurs when an attacker compromises a public cloud resource to obtain information that they then use to attack the resource provider’s on-premises environment. Public facing endpoints in the cloud are often under constant brute force attack through protocols such as Remote Desktop Protocol (RDP) and Secure Shell (SSH).
The cyber kill chain: On-premises and in the cloud

The cyber kill chain is a model defined by analysts at Lockheed Martin to aid decision making with regard to detecting and responding to threats.

**CYBER KILL CHAIN ATTACK**

- **Reconnaissance** - Account enumeration
- **Compromised Credential** - Abnormal working hours or location
- **Lateral Movement** - Abnormal authentication or resource access
- **Privilege Escalation** – Log Audit
- **Domain Dominance** - Remote execution
# Defense-in-Depth security discussion

<table>
<thead>
<tr>
<th>Security layer</th>
<th>Includes...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Access control list (ACL), encryption (Encrypting File System [EFS], BitLocker), data classification with RMS</td>
</tr>
<tr>
<td>Application</td>
<td>Application design using the security development lifecycle, antivirus, application hardening</td>
</tr>
<tr>
<td>Host</td>
<td>Operating system hardening, authentication, update management, host intrusion detection system</td>
</tr>
<tr>
<td>Internal network</td>
<td>Network segmentation, network encryption (Internet Protocol security [IPSec]), network intrusion detection system</td>
</tr>
<tr>
<td>Perimeter</td>
<td>Firewalls, network access control, network access protection (NAP)</td>
</tr>
<tr>
<td>Physical security</td>
<td>Guards, locks, tracking devices, surveillance cameras</td>
</tr>
<tr>
<td>People, policies, processes</td>
<td>Security awareness training, documentation, banners, warning signs</td>
</tr>
</tbody>
</table>
Azure IaaS Solutions’ protection pillars

1. THE RESEARCH
2. NEW IDEAS
3. THE GAP
4. THE PLAN
5. THE CHANGE
6. THE EVALUATION
Azure Security Infrastructure

Start to discuss this topics with customers in any hybrid/public cloud Azure IaaS project

**MANDATORY ACTIONS**

- Admin access protection in Azure IaaS
- Azure IaaS virtual networks/network access protection to Azure IaaS
- Data protection in Azure
- Antivirus/antimalware protection in Azure IaaS
- Monitoring of security for Azure IaaS, VMs, hybrid infra
Admin access protection

- Hybrid Identity solution/project
- Modernization of existing local identity infrastructure with modern technologies, e.g. authentication silos, Microsoft ATA etc.
- Modernization of existing administration procedures, processes and on-premises admin account protection (PAW)
- Planning Role Based Access Control (RBAC) and procedures in general
STEP 1: Monitoring Azure AD sign-in activities

Discovering compromised identities with Azure Active Directory Identity Protection

- **Detect** vulnerabilities and risky accounts
- **Investigating** risk events
- Risk-based **conditional access policies**
STEP 1A: Azure Active Directory Identity Protection

Planning vulnerabilities detection

- **Multi-factor authentication** registration not configured
- **Unmanaged cloud apps** (with Cloud App Discovery)
- **Security Alerts** (with Privileged Identity Management)

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>RISK LEVEL</th>
<th>COUNT</th>
<th>VULNERABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Low</td>
<td>14</td>
<td>Unmanaged apps discovered in last 7 days</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>382</td>
<td>Users without multi-factor authentication registration</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>8</td>
<td>Redundant administrators increase your attack surface</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>17</td>
<td>Weak authentication is configured for role activation</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>15</td>
<td>Too many global administrators increase your attack surface</td>
</tr>
</tbody>
</table>
STEP 1B: Azure Active Directory Identity Protection
Planning risk events investigation and supported events type

- Leaked credentials
- Sign-ins from anonymous IP addresses
- Impossible travel to atypical locations
- Sign-in from unfamiliar locations
- Sign-ins from infected devices
- Sign-ins from IP addresses with suspicious activity
STEP 1C: Azure Active Directory Identity Protection
Planning risk-based conditional access policies

- Policy to mitigate risky sign-ins by blocking sign-ins or requiring multi-factor authentication challenges.
- Policy to block or secure risky user accounts.
- Policy to require users to register for multi-factor authentication.
STEP 2: manage, control and monitor Admins’ access

Azure AD Privileged Identity Management

- See which users are Azure AD administrators
- Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune
- Get reports about administrator access history and changes in administrator assignments
- Get alerts about access to a privileged role
STEP 3: protect administrative accounts on-premises

Authentication Policies and Authentication Policy Silos as good way to modernization AD

- Good point to start modernization on-premises
- An **authentication policy silo controls** which accounts can be restricted by the silo and defines the authentication policies to apply to the members.
- An **authentication policy** defines the Kerberos protocol ticket-granting ticket (TGT) **lifetime properties** and authentication **access control conditions** for an account type.
  - The **TGT lifetime** for the account, which is set to be non-renewable.
  - The **criteria that device accounts need to meet** to sign in with a password or a certificate.
  - The **criteria that users and devices need to meet** to authenticate to services running as part of the account.
- Required Windows Server 2012 R2 or later
STEP 4: Modernization of existing local identity infrastructure with modern technologies

Protection on-premises against modern attack types - Securing privileged access & PAW

- Security Privileged Access Roadmap: Stage 1
  - Separate Admin account for admin tasks
  - Privileged Access Workstations (PAWs) Phase 1: Active Directory admins
  - Unique Local Admin Passwords for Workstations
  - Unique Local Admin Passwords for Servers

- Security Privileged Access Roadmap: Stage 2
  - PAW Phases 2 and 3: all admins and additional hardening
  - Time-bound privileges (no permanent administrators)
  - Multi-factor for time-bound elevation
  - Just Enough Admin (JEA) for DC Maintenance
  - Lower attack surface of Domain and DCs
  - Attack Detection

- Security Privileged Access Roadmap: Stage 3
  - Modernize Roles and Delegation Model
  - Smartcard or Passport Authentication for all admins
  - Admin Forest for Active Directory administrators
  - Code Integrity Policy for DCs (Server 2016)
  - Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric)

[Diagram of Attack and Defense]

https://aka.ms/privsec
**STEP 5: Protection against cyber kill chain attacks**

**Planning & deploy Microsoft Advanced Threat Analytics**

- Abnormal resource access
- Account enumeration
- Net Session enumeration
- DNS enumeration
- Directory Services enumeration (ATA 1.7)

- Abnormal authentication
- Abnormal resource access
- Pass-the-Ticket
- Pass-the-Hash
- Overpass-the-Hash

- Skeleton key malware
- Golden ticket
- Remote execution
- Malicious replication requests

- Abnormal working hours
- Brute force using NTLM, Kerberos or LDAP
- Sensitive accounts exposed in plain text authentication
- Service accounts exposed in plain text authentication
- Honey Token account suspicious activities
- Unusual protocol implementation
- Malicious Data Protection Private Information (DPAPI) Request

**Reconnaissance**

**Compromised Credential**

**Lateral Movement**

**Privilege Escalation**

**Domain Dominance**

- MS14-068 exploit (Forged PAC)
- MS11-013 exploit (Silver PAC)
Virtual Networks protection in Azure

Safe and extend your Network Engineers experience with Azure Projects

- Remote Access to IaaS/VMs & hybrid connections solutions
- Network architecture and Network Security Groups planning in Azure IaaS
- VM network security audit
- Virtual Network Security Appliances – well known network security solutions in Azure Marketplace
STEP 6A: Virtual Networks protection’s Best Practices

- Subnet your networks based on security zones.
- Use Network Security Groups carefully.
- Use site-to-site VPN to connect Azure Virtual Networks.
- Configure host-based firewalls on infrastructure as a service (IaaS) virtual machines.
- Configure User Defined Routes to control traffic.
- Require forced tunneling.
STEP 6B: Virtual Networks protection’s Best Practices

- Deploy virtual network security appliances - network security capabilities provided by virtual network security appliances include:
  - Firewalls
  - Intrusion detection and prevention
  - Vulnerability management
  - Application control
  - Network-based anomaly detection
  - Web filtering
  - Antivirus protection
  - Botnet protection
- Create perimeter networks for Internet-facing devices.
- Use ExpressRoute.
STEP 6C: Virtual Networks protection’s Best Practices

- Optimize uptime and performance.
  - HTTP-based load balancing
  - External load balancing
  - Internal load balancing
  - Global load balancing

- Disable management protocols to virtual machines. Disable access to WinRM, RDP and SSH protocols. Other options can have to be used to access VMs for remote management:
  - Point-to-site VPN
  - Site-to-site VPN
  - ExpressRoute

- Enable Azure Security Center. Azure Security Center helps optimize and monitor network security by:
  - Providing network security recommendations.
  - Monitoring the state of your network security configuration.
  - Alerting you to network-based threats both at the endpoint and network levels.
Customer Case Studies

1. THE RESEARCH
2. NEW IDEAS
3. THE GAP
4. THE PLAN
5. THE CHANGE
6. THE EVALUATION
Customer Case Study - Thaicreate

- Thaicreate is Thailand’s most popular online collaboration forum for web and mobile application developers.
- Thaicreate is the largest online community of application developers in Thailand, with over 92,000 registered participants.
- **To improve the reliability and scalability** of the thaicreate.com website, the owner deployed the PHP-MySQL site with the infrastructure-as-a service (IaaS) provider, Microsoft Azure.
- With automatic load-balancing, rapid scaling, and overseas caching, the site is easy to maintain and cost-efficient, helping Thaicreate expand abroad and host new, rich-media content.
- **Robust security and privacy policies.** Thaicreate users’ data is secure and private. Microsoft data centers comply with key industry standards for reliability and security, including ISO/IEC 27001:2005. Also, Azure is bound by the published Microsoft Privacy Principles, which set out the limitations on how Microsoft may collect and use customer data.
What's NEXT?

1. THE RESEARCH
2. NEW IDEAS
3. THE GAP
4. THE PLAN
5. THE CHANGE
6. THE EVALUATION
Azure Sales Star program – Sessions

FEB 6, 2017
Azure Security Scenarios - Overview of Main Scenarios for Security Projects

FEB 9, 2017
New Partner Opportunities to Plan Cloud/Hybrid Identity Projects

FEB 13, 2017
Fine-Tune the Details of Planning Hybrid Identity Protection

FEB 16, 2017
Provide a Full Management Experience for Hybrid Infrastructure

FEB 20, 2017
Secure Mobile Users Planning: Mobile Device Management (MDM) Scenarios Comparison

FEB 23, 2017
Implementing Microsoft Intune to MDM

FEB 27, 2017
Planning Data Access & Protection in Hybrid Infrastructure

MAR 2, 2017
Planning Hybrid Data Protection at the File Level

MAR 6, 2017
Planning Azure Infrastructure Security

MAR 9, 2017
Planning Azure Infrastructure Security – Data Protection in Azure

NEXT
Azure Sales Star program - Resources

CHECK ALL THE SESSIONS AND ANNOUNCEMENTS

https://partner.microsoft.com/pl-pl/training/AzureSalesStarProgram#kick_off-session

...AND REGISTER SOON!

CHECK OUR LATEST THINKING – AZURE SALES STAR BLOG

https://partner.microsoft.com/pl-pl/training/azuresalesstarprogram/security-can-be-the-primary-reason-for-cloud-adoption

...AND MORE TO COME!
Azure IaaS/on-premises infra security resources

- **Securing Privileged Access** - [https://aka.ms/privsec](https://aka.ms/privsec)
- **Privileged Access Workstations** – [http://aka.ms/cyberpaw](http://aka.ms/cyberpaw)
- **Azure Role-Based Access Control (RBAC)** - [https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure](https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure)
1. THE RESEARCH

2. NEW IDEAS

3. THE GAP

4. THE CHANGE

5. THE PLAN

6. THE EVALUATION

Brought to you by Consalta
Thank you for your attention!