OFFICE 365 SECURITY: TOP PRIORITIES FOR 30 DAYS, 90 DAYS AND BEYOND

Mark Simos
Lead Cybersecurity Architect
Microsoft
@MarkSimos

Matt Kemelhar
Global Director, Incident Response
Microsoft
Session Outline

1. LIFE ON THE CLOUD (AS SECURITY)
   What is security like when fully on Office 365?
   What’s gone?
   What’s new or changed?

2. THE JOURNEY
   How do I get the most for my security investments?
1. LIFE ON THE CLOUD (AS SECURITY)
What is security like when fully on Office 365?
   What’s gone?
   What’s new or changed?
## Responsibility Zones

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
<th>On-prem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data governance and rights management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Client endpoints</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Account and access management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Identity and directory infrastructure</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Application</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Network controls</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Operating system</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Physical hosts</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Physical network</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Physical datacenter</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

- **Always retained by customer**
- **Varies by service type**
- **Transfers to Cloud Provider**

- Microsoft | Customer
## Security Responsibilities Transfer to Office 365

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data governance and rights management</td>
<td></td>
</tr>
<tr>
<td>Client endpoints</td>
<td></td>
</tr>
<tr>
<td>Account and access management</td>
<td></td>
</tr>
<tr>
<td>Identity and directory infrastructure</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td></td>
</tr>
<tr>
<td>Network controls</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
</tr>
<tr>
<td>Physical hosts</td>
<td></td>
</tr>
<tr>
<td>Physical network</td>
<td></td>
</tr>
<tr>
<td>Physical datacenter</td>
<td></td>
</tr>
</tbody>
</table>

### Microsoft

<table>
<thead>
<tr>
<th>Security Patches (Server)</th>
<th>Attacks on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Upgrades*</td>
<td>Operating System (OS) and Admins</td>
</tr>
<tr>
<td>Service Uptime</td>
<td>Application attacks</td>
</tr>
<tr>
<td>SLA from Microsoft</td>
<td>Hardware/Firmware</td>
</tr>
<tr>
<td>Server Maintenance and Troubleshooting</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>Backup and Archive</td>
<td>Physical Attacks</td>
</tr>
</tbody>
</table>

*You still need to manage feature configuration*
"No Firewall"

Service connected directly to Internet (users and admin interfaces)

Implications

1. Authentication Security is Extremely Critical
   - Multi-factor authentication
   - Anomaly detection using
   - User and Entity Behavior Analytics (UEBA)
   - Context awareness (time, date, geolocation)
   - Integrated security intelligence

2. Tenant Security Configuration is Critical
Evolution of Visibility and Policy Enforcement

Mobile Device Management

Network Edge

Policies

[Diagram showing various icons and symbols related to network security and device management]
Must shift to policy and controls tailored for each asset type
Threats change a bit...

Notable trends:

1. **Identity Attacks**
   - Password spray
   - Brute force
   - Password re-use

2. **App/Data Layer Attacks**
   - Social engineering
   - Delegation and forwarding rule attacks
   - PowerShell scripts in attacks

For more information, see [https://aka.ms/O365attacks](https://aka.ms/O365attacks)
1. LIFE ON THE CLOUD (AS SECURITY)
What is security like when fully on Office 365?
  What's gone?
  What's new or changed?

2. THE JOURNEY
How do I get the most for my security investments?
Roadmap Outcomes
How do I quickly and efficiently protect my Office 365 Tenant?

30 DAYS
- Rapid Configuration
  - Basic admin protections
  - Logging and Analytics
  - Basic Identity Protections
- Tenant Configuration
- Prepare stakeholders

90 DAYS
- Advanced Protections for
  - Admin Accounts
  - Data and User Accounts
- Customize roadmap for your compliance, threat, and user needs
- Adapt and implement default policies and protections

BEYOND
- Adjust and refine key policies and controls
- Extend protections to on-premises dependencies
- Integrate with business and security processes (legal, insider threat, etc.)

Monitor Logs via SIEM (if applicable)

Regularly Review Alerts and Upcoming Updates
30 DAY Plan

THREAT PROTECTION
Admins
- Separate Admin Account
- Enforce MFA for admins
- Highly Secure Productivity Device

Windows 10 example: http://aka.ms/HighSecWin10

Tenant / All Users
- Enable logging + anomaly detection (Example: Microsoft Cloud App Security)

INFORMATION PROTECTION
- Evaluate example Information Protection policies
  https://aka.ms/O365DataPolicy
- = Start preparation for action in 90 day plan

IDENTITY AND ACCESS MANAGEMENT
- Enable Azure AD Identity protection
  Ensure passwords are synchronized to Azure AD
- If Federated, enforce account security (Password length / age / complexity, etc.)
- Evaluate example conditional access policies
  https://aka.ms/O365IdentityPolicy

SECURITY MANAGEMENT

Regularly Review Alerts (CASB, Threat Dashboard) and Upcoming Changes (Roadmap | Blog | YouTube)
90 DAY Plan

**THREAT PROTECTION**

Admins
- Privileged Access Workstation [http://aka.ms/cyberpaw](http://aka.ms/cyberpaw)
- Configure Azure AD PIM

Tenant / All Users
- Configure SIEM to collect logs from Federation, CASB, and Office 365

**INFORMATION PROTECTION**

- Adapt and Implement Information Protection policies [https://aka.ms/O365DataPolicy](https://aka.ms/O365DataPolicy)

**IDENTITY AND ACCESS MANAGEMENT**

- Enable and Enforce Multi-factor Authentication for all users
- Adapt and Implement Conditional Access policies [https://aka.ms/O365IdentityPolicy](https://aka.ms/O365IdentityPolicy)

**SECURITY MANAGEMENT**

- Secure Score – Identify important actions and low hanging fruit [https://securescore.microsoft.com](https://securescore.microsoft.com)
- Sharing Risks – Use CASB to identify oversharing of sensitive/internal documents
- Threat Intelligence – Conduct Attack Simulation + Industry Trends
- Compliance Status – Compliance manager (GDPR, NIST 800-171) [https://servicetrust.microsoft.com/ComplianceManager](https://servicetrust.microsoft.com/ComplianceManager)

Regularly Review Alerts (CASB, Threat Dashboard, SIEM) and Upcoming Updates
...And BEYOND

**THREAT PROTECTION**

**Admins**
- SPA roadmap for on premises AD
  [http://aka.ms/SPAroadmap](http://aka.ms/SPAroadmap)

**Tenant / All Users**
- Integrate Cloud App Security Broker (CASB) into
  - Insider threat program
  - Shadow IT GRC risks/program

**INFORMATION PROTECTION**
- Integrate AIP into insider threat risk strategy
- Refine Information Protection policies
- Office 365 DLP
- CASB policies and alerts
- Data Encryption Solution

**IDENTITY AND ACCESS MANAGEMENT**
- Refine policies and operational process
- Integrate alerts on user behavior in with insider threat program (from Azure AD Identity Protection or other capability)

**SECURITY MANAGEMENT**
- Secure Score – Continue Planning Next Actions
- eDiscovery – Integrate into legal and threat response processes

Regularly Review Alerts and Upcoming Updates
• User 2
• On-Premises Admin

• User 1
• Cloud Admin
### Questions?

**30 DAYS**
- Rapid Configuration
  - Basic admin protections
  - Logging and Analytics
  - Basic Identity Protections
- Tenant Configuration
- Prepare stakeholders

**90 DAYS**
- Advanced Protections for
  - Admin Accounts
  - Data and User Accounts
- Customize roadmap for your compliance, threat, and user needs
- Adapt and implement default policies and protections

**BEYOND**
- Adjust and refine key policies and controls
- Extend protections to on-premises dependencies
- Integrate with business and security processes (legal, insider threat, etc.)

Monitor Logs via SIEM (if applicable)

Regularly Review Alerts and Upcoming Updates
Thank you

@MarkSimos  https://aka.ms/markslist
REFERENCES
Password Spray (aka Brute Force, Hammering)

Iterate through known account names with most common passwords

Probability of account compromise by password spray: 1%

<table>
<thead>
<tr>
<th>Password</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>123456</td>
<td>password1</td>
</tr>
<tr>
<td>123456789</td>
<td>qwerthyuiop</td>
</tr>
<tr>
<td>qwerty</td>
<td>666666</td>
</tr>
<tr>
<td>111111</td>
<td>a123456</td>
</tr>
<tr>
<td>12345678</td>
<td>1234</td>
</tr>
<tr>
<td>123123</td>
<td>654321</td>
</tr>
<tr>
<td>password</td>
<td>5201314</td>
</tr>
<tr>
<td>1234567</td>
<td>123456a</td>
</tr>
<tr>
<td>12345</td>
<td>iloveyou</td>
</tr>
<tr>
<td>1234567890</td>
<td>11111111</td>
</tr>
<tr>
<td>abc123</td>
<td>159753</td>
</tr>
<tr>
<td>123</td>
<td>123123123</td>
</tr>
<tr>
<td>123321</td>
<td></td>
</tr>
</tbody>
</table>
References

- **Office 365 Updates**
  Office 365 Roadmap | O365 Update Series on YouTube

- **Office 365 Secure Score**
  https://securescore.office.com/

- **Office 365 Security Reference Configuration**
  http://aka.ms/securecampaign

- **Securing Privileged Access Roadmap**
  http://aka.ms/sparoadmap

- **Deploy Privileged Access Workstations**
  http://aka.ms/cyberpaw

- **Standards for a Highly Secure Windows 10 Device**
  http://aka.ms/HighSecWin10

- **Cloud App Security**

- **Enable Azure AD Identity Protection**
  https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection-enable
Integrating with your SIEM

Connect to your existing SIEM tool and processes

- Log Integration
- Audit Logs
- Alerts

- Windows Defender ATP
- Azure AD Identity Protection
- Azure Security Center
  - Threat Protection
  - Threat Detection
- Azure SQL Threat Detection
- Cloud App Security
- Office 365
- ATA
- Office 365 ATP
  - Email Gateway
  - Anti-malware

Powered by the Intelligent Security Graph
SIEM Integration Reference

- **Windows Defender ATP**

- **Advanced Threat Analytics**
  https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/configure-event-collection
  https://docs.microsoft.com/en-us/advanced-threat-analytics/deploy-use/setting-ata-alerts

- **Azure SIEM Integration (includes Azure AD)**
  https://aka.ms/azureSIEMintegration

- **Office 365**

- **Cloud App Security**
  https://docs.microsoft.com/en-us/cloud-app-security/siem

- **Operations Management Suite (OMS)**
  https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-api-alerts
### Other Notable Changes

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data governance and rights management</td>
<td></td>
</tr>
<tr>
<td>Client endpoints</td>
<td></td>
</tr>
<tr>
<td>Account and access management</td>
<td></td>
</tr>
<tr>
<td>Identity and directory infrastructure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network controls</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td></td>
</tr>
<tr>
<td>Physical hosts</td>
<td></td>
</tr>
<tr>
<td>Physical network</td>
<td></td>
</tr>
<tr>
<td>Physical datacenter</td>
<td></td>
</tr>
</tbody>
</table>

- PowerShell for administration (and attacks)
- Authentication flow changes (protocols, log locations, etc.)
- Log analytics easier/faster/better (with CASB anomaly detection + O365 Logs)
- Regular release of features/changes (configurable, but not customizable)

**Implications**

- Always Current Features
- Security must regularly review updates

[Office 365 Roadmap](#) | [O365 Update Series on YouTube](#)
Security Log Notes

**KEY LOG LOCATIONS**
- Azure AD – Account Authentication/Management
- Office 365 Security and Compliance Center – O365 App Usage
- SIEM integration – See reference slide

**THERE IS A DELAY FOR SOME LOGS (30-60 MINUTES)**

**ENABLING LOGS IN EXCHANGE**
- Admin and Non-Owner Logging are on by default
- Owner Logging (e.g. activities in my mailbox) must be enabled
  - Secure Score can launch script to enable this
  - Cloud App Security needs this for some anomaly detection
Observed to increase risk of security incidents

**Privilege Hygiene**
- Missing key protections for privileged accounts (see 30 day plan)
  - Includes accounts with powerful permissions (eDiscovery, HR/Compliance account)
- Multiple people sharing a single account/password
- Granting broad permissions to data (SharePoint/OneDrive)

**Tenant Configuration**
- Logging not enabled (hampers incident investigation)
- Weak password policies in on-premises AD (Federated Identity)
- Unused Security Capabilities (Advanced Threat Protection, Cloud App Security, etc.)

**Key Strategic Element(s)**
- Identify business critical data within O365
- SecureScore to measure risk exposure and progress
- Avoiding cloud features (e.g. avoiding password sync = not having leaked credential protection)