Enterprise Security with Expanded Network Boundaries

Dr. Zhijun (William) Zhang
Lead Security Architect at The World Bank Group
Data Breaches in the News

Large-scale breaches are now a regular occurrence across industry and geography

Consequences

- Erosion of client confidence
- Financial loss
- Damage to Brand
- Poor publicity
- Delays in strategically competitive initiative
- Regulatory fines

Cybersecurity is an enterprise-wide business issue requiring a risk management approach.
Information Security Threats

External Threats
- Organized Crime
- Hacktivist Group
- State or Business Sponsored Entity
- Vendor/Third-Party

Internal Threats
- Careless/Unaware User
- Malicious Privileged Insider
- Nonprivileged Insider

Attack Patterns

Crimeware
Cyber Espionage
Distributed Denial of Service
Insider and Privilege Misuse

Web Application Attacks
Business Email Impersonation (CEO Fraud)
Spear Phishing

Information Leakage
Unauthorized Use
Ransomware
The Challenge: How can we fight a set of ever-moving targets?
The Answer: Know Your Enemies

We need threat intelligence

• Vulnerability reports
• New attacks and IOCs
• New malware and signatures
• Suspicious domains
• IP addresses associated with malicious activity
• Enterprise information shared on pastebins

We need to automate threat intelligence actions

• Structured Threat Information eXpression (STIX)
• TAXII (Trusted Automated eXchange of Indicator Information)
But Information Security is NOT the Goal

• Business wants mobility
  • Traveling staff
  • Consumerization
  • Convenience and productivity

• Business wants cloud
  • Agility
  • Up-to-date capabilities
  • Service level guarantee
Control Access to Enterprise Data - Traditional

Access control to corporate data today
Controlling Access to Data in Mobile-first and Cloud-first Context

On-premises

- Users
- Devices
- Apps
- Data

Managed cloud

- Office 365
- SharePoint Online
- Exchange Online

Access control and data protection integrated natively in the apps, devices, and the cloud
Cloud-based Security is an Industry Strategy

The Promise by Microsoft

• Leverage its massive customer base to collect and analyze data
• Centrally manage security to benefit all customers
• Manage security across all Microsoft services
• Much more frequent updates and upgrades

The Pre-requisite

• “Deep adoption” of Azure AD and other cloud services
• Constantly feeding data to Microsoft cloud
Key Microsoft Cloud Services

Azure AD (positioned to be the IDaaS)
- WBG currently uses as part of Office 365
- Windows 10 devices will “domain join”
- Will become the preferred federation engine for SaaS
- Will be a central authentication/authorization engine for applications (OpenID Connect & OAuth)

Intune
- For MAM and MDM
- On-going security such as DLP

Cloud engine behind Defender, ATP, Information Protection, etc.
Windows Devices Can/Will Join Azure AD

Such devices will have much less dependency on on-premises infrastructure when accessing cloud resources.
What about Moving Your Own Apps to the Cloud?

• Enterprises focus on their own business app logic
• Cloud service providers manages compute, storage, and networking
• It can be more secure
  • Keeping humans (employees) away from systems
  • Leverage dedicated resources to take care of foundational security
  • Overall security is a shared responsibility
Summary

Leverage the power of the cloud

Leverage the intelligence of the community

Automate security controls
  • Security-as-code: baselined, version controlled, and monitored

Re-validate what you trust periodically
  • Your cloud service providers
  • Your threat intelligence sources
  • Your software suppliers
  • Your employees and contractors

Re-validate your technical controls
  • Are your security baseline code still valid?