Agenda

X:00 am  Welcome and Intro: *Allen Jenkins & Josh Krodel*
Defense In Depth – Leveraging Microsoft Technology Solutions

- Security Fundamentals
- Defense in Depth Strategies
- Microsoft Solutions Review

X:45 am  Wrap-Up
Welcome and Introduction

• Allen Jenkins
  • 30+ years in IT / 20+ years at SyCom

• CISA – Certified Information System Auditor
• GSLC – GIAC Security Leadership Certification
• GSEC – GIAC Security Essentials Certification

• Dual Role at SyCom as CISO & VP of Consulting
  • Make us more secure
  • Make our customers more secure
Welcome and Introduction – Microsoft Info

• Josh Krodel
  • 20 years in IT / 7 years at SyCom
  • MCSE – Microsoft Certified Systems Engineer
Concerns over Confidentiality, Integrity and Availability of Critical Information Technology Assets
ALL Important, but…which is most high priority???

Prioritization of Approach based on what is important to organization – generally speaking…

• Confidentiality = Health Care, Gov

• Integrity = Finance

• Availability = E-commerce
Security Fundamentals

- Malicious or Criminal Attack: 47%
- System Glitch: 25%
- Human Error: 28%
Security Story – Chapter 2
Security Story - Chapter 6
This was not fiction, this really has been reported and there are other stories, like the Russian Group Energy Bear that used similar attacks to take over MUCH of the electric grid of the US in 2018 by compromising small utility companies.

There is NO Silver Bullet, but a layered approach might have helped…like:
There is NO Silver Bullet, but a layered approach might have helped…like:

• Security Awareness Training around Phishing
There is NO Silver Bullet, but a layered approach might have helped…like:

- Security Awareness Training around Phishing
- Possible Advanced Threat Protection Tools to aid with recognizing the Phishing attacks
There is NO Silver Bullet, but a layered approach might have helped…like:

• Security Awareness Training around Phishing
• Possible Advanced Threat Protection Tools to aid with recognizing the Phishing attacks
• Possibly some DNS protections or application whitelisting functions to disallow the “Password Reset” program
There is NO Silver Bullet, but a layered approach might have helped…like:

- Security Awareness Training around Phishing
- Possible Advanced Threat Protection Tools to aid with recognizing the Phishing attacks
- Possibly some DNS protections or application whitelisting functions to disallow the “Password Reset” program
- Some DLP tools to help find/thwart data ex-filtration
There is NO Silver Bullet, but a layered approach might have helped…like:

• Security Awareness Training around Phishing
• Possible Advanced Threat Protection Tools to aid with recognizing the Phishing attacks
• Possibly some DNS protections or application whitelisting functions to disallow the “Password Reset” program
• Some DLP tools to help find/thwart data ex-filtration
• Possibly some network segmentation/isolation to keep critical data assets more protected
There is NO Silver Bullet, but a layered approach might have helped…like:

- Security Awareness Training around Phishing
- Possible Advanced Threat Protection Tools to aid with recognizing the Phishing attacks
- Possibly some DNS protections or application whitelisting functions to disallow the “Password Reset” program
- Some DLP tools to help find/thwart data ex-filtration
- Possibly some network segmentation/isolation to keep critical data assets more protected
- Possibly some better vendor controls in place (in the case of breaches like Energy Bear and the Target breach, vendor controls were weak)
Agenda

X:00 am  Welcome and Intro: Allen Jenkins & Josh Krodel
          Defense In Depth – Leveraging Microsoft Technology Solutions

          • Security Fundamentals
          • Defense in Depth Strategies
          • Microsoft Solutions Review

X:45 am  Wrap-Up
Defense in Depth Strategies
Defense in Depth Strategies
Defense in Depth Strategies

Uniform Protection
Defense in Depth Strategies

• Most common approach
Defense in Depth Strategies

• Most common approach

• Equal security for all components of network
Defense in Depth Strategies

• Most common approach

• Equal security for all components of network

• Can be effective as a STARTING POINT, to deploy standard security protections as a baseline
Defense in Depth Strategies
Defense in Depth Strategies

Protected Enclaves
Defense in Depth Strategies

• Consider building secure areas within your infrastructure to protect assets
Defense in Depth Strategies

• Consider building secure areas within your infrastructure to protect assets

• Applies different levels of protection based on criticality of need
Defense in Depth Strategies

• Consider building secure areas within your infrastructure to protect assets

• Applies different levels of protection based on criticality of need

• Usually associated with network segmentation
Defense in Depth Strategies
Defense in Depth Strategies

• Build an architecture that focuses on critical information

• Can come to life as
  • Disk encryption
  • Host based segmentation
  • Networking and access controls
  • Software Defined Networking
  • Multi-tiered applications
  • Logical access controls and using principle of least privilege
  • Network traffic encryption
  • Etc., etc.
Defense in Depth Strategies
Defense in Depth Strategies

Data Classification
Defense in Depth Strategies

SAN

Data
Defense in Depth Strategies

- Web App
- Database
- Operating System
- Virtualization
- SAN
- Data
Defense in Depth Strategies
Defense in Depth Strategies
Defense in Depth Strategies
Defense in Depth Strategies
Defense in Depth Strategies

• Build protections based on specific threat vectors
• Build protections based on specific threat vectors

• Things like
  • USB sticks
  • Email attachments
  • Hackers
  • Natural Disasters, like hurricanes, all present concerns

• Each has a different set of strategies for protection
• Build protections based on specific threat vectors

• Things like
  • USB sticks – GPO’s/Data Loss Prevention
  • Email attachments
  • Hackers
  • Natural Disasters, like hurricanes, all present concerns

• Each has a different set of strategies for protection
Defense in Depth Strategies

• Build protections based on specific threat vectors

• Things like
  • USB sticks – GPO’s/Data Loss Prevention
  • Email attachments – Email threat protections – Office365 ATP
  • Hackers
  • Natural Disasters, like hurricanes, all present concerns

• Each has a different set of strategies for protection
Defense in Depth Strategies

• Build protections based on specific threat vectors

• Things like
  • USB sticks – GPO’s/Data Loss Prevention
  • Email attachments – Email threat protections – Office365 ATP
  • Hackers – Logical Access Controls (accounts/passwords)
  • Natural Disasters, like hurricanes, all present concerns

• Each has a different set of strategies for protection
Defense in Depth Strategies

• Build protections based on specific threat vectors

• Things like
  • USB sticks – GPO’s/Data Loss Prevention
  • Email attachments – Email threat protections – Office365 ATP
  • Hackers – Logical Access Controls (accounts/passwords)
  • Natural Disasters, like hurricanes, all present concerns – DR planning/Cloud solutions

• Each has a different set of strategies for protection
Defense in Depth Strategies - Summation

• Consider the specific environment and build the corresponding protections

• A combination of approaches is probably the best

• Use a Risk Based approach to assess Risks and then develop the appropriate Defense strategy to mitigate the Risks...
Agenda

X:00 am  Welcome and Intro: *Allen Jenkins & Josh Krodel*
Defense In Depth – Leveraging Microsoft Technology Solutions

• Security Fundamentals
• Defense in Depth Strategies
• Microsoft Solutions Review

X:45 am  Wrap-Up
Traditional security management doesn’t scale

5B unique threats per month*
Increasing # security solutions to manage
Only capacity for 10 alerts per day

*The Microsoft Intelligent Security Graph data
Deliver and manage enterprise-ready devices

**Windows AutoPilot**
Get new devices up and running fast without re-imaging, powered by the cloud
Automatically configure settings, security policies, and install apps like Office 365

**Mobile Device Management with Microsoft Intune**
Security policy enforcement for mobile devices and apps
Selective wipe of corporate data such as apps, email, management policies, and networking profiles from user devices while leaving personal data intact

**Windows Hello for Business**
Get better protection when you unlock your device with a look or a touch, even on devices you’ve never signed in to before

**Microsoft Store for Business**
Find, acquire, manage, and distribute apps including custom line-of-business apps to Windows 10 devices
Intelligent threat protection built-in, not bolted-on

Windows Defender Antivirus
Detect fast-changing malware variations using behavior monitoring and cloud-powered protection

Windows Defender Credential Guard
Isolate and protect credentials from a full system compromise
Configure easily with existing management tools

Windows Defender System Guard
Maintain system integrity during boot time, runtime, and remote access to avoid compromised devices

Windows Defender Advanced Threat Protection
Protect endpoints from cyber threats, detects advanced attacks and automates security incidents to improve security posture
Secure and contain business information

Azure Information Protection
Persistent data classification and protection that ensures data is protected at all times, regardless of where it’s stored or with whom it’s shared
Safe sharing with people inside and outside of your organization
Simple, intuitive controls for data classification and protection
Deep visibility and control of shared data for users and IT

BitLocker
Encrypt sensitive information and protect against unauthorized access

Microsoft BitLocker Administration & Monitoring
Use tools to provision, enforce, report compliance and recover BitLocker-protected data

Office 365 Advanced Threat Protection
Help protect against unknown malware and viruses
Provide real-time, time-of-click protection against malicious URLs
Deliver rich reporting and URL trace capabilities with Click Tracing
Manage the on-going threat landscape

**Azure Advanced Threat Protection**
Monitor users, entity behaviour, and activities with learning-based analytics
Protect user identities and credentials stored in Active Directory
Identify and investigate suspicious user activities and advanced attacks throughout the kill chain
Provide clear incident information on a simple timeline for fast triage

**Cloud App Security**
Complete visibility into employee cloud app usage and Shadow IT
Ongoing risk detection, powerful reporting, and analytics on users, upload/download traffic, usage patterns, and transactions for discovered apps
Granular-level control and data policies for on-going data protection in cloud apps

**Attack Simulator**
Run realistic attack scenarios in your organization
Three kinds of attack simulations are currently available: display name spear-phishing attack, password-spray attack, brute-force password attack

**Secure Score**
Analyzes your organization's security based on regular activities and security settings in Office 365
Welcome and Intro: Allen Jenkins & Josh Krodel

Defense In Depth – Leveraging Microsoft Technology Solutions

• Security Fundamentals
• Defense in Depth Strategies
• Microsoft Solutions Review

Wrap-Up
Wrap-Up

• Remember Security Fundamentals
  • Confidentiality, Integrity, and Availability

• Consider Defense In Depth Strategies
  • Uniform Protection, Secure Enclaves, Information Centric, Threat Vector

• Analyze and Deploy Appropriate Toolsets
Q&A
THANK YOU FOR JOINING US!

Connecting More Than Technology