Agenda

- Data Security and Backups
- Multi-Factor Authentication
- Microsoft Threat Protection suite
- Examples and Key Takeaways

Global Attacks are Increasing

Risk of cyber attacks can cost business up to $3 **trillion a year**[1]

Cybercrime extracts between **15-20%** of the value created by the Internet[2]

91% agree consumers have **lost control** over how personal information is collected and used by companies[5]

More than 800M individual records were breached in 2013[4]

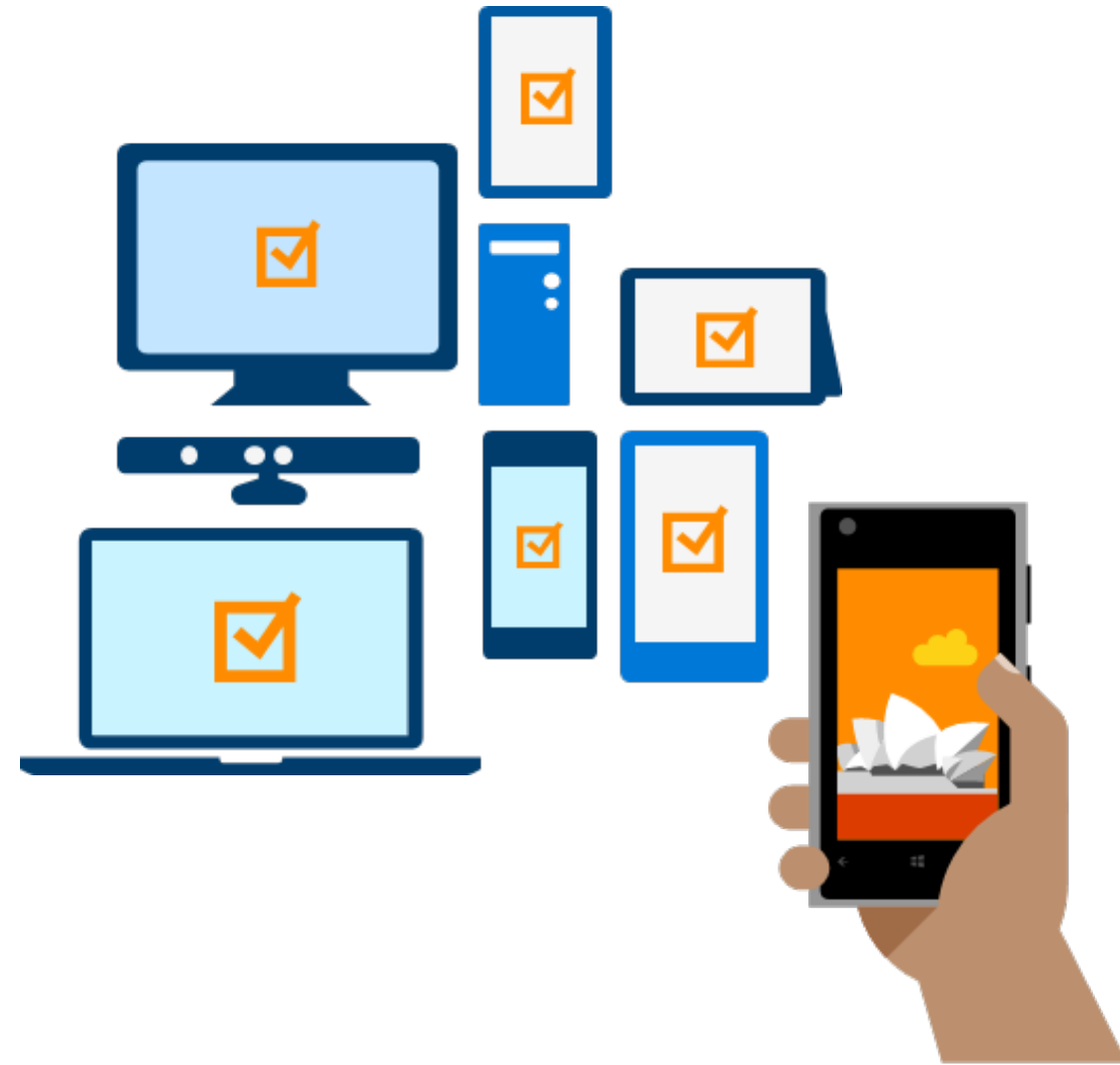The number of recorded data breaches **increased 78%** in 2014[3]

Data Security and Backups

- Protection from malware, crypto

- Protects against downtime, loss of data, failed recoveries

- Education for quick recovery

Multi-Factor Authentication

- Something You Have, You Are, and You Know

- Eliminates 99% of unauthorized access

Identity Protection

- Who's accessing the account

- Alerts to IT for strange mail flow rules

- Odd location access

- New device access

Examples

"Someone was **fooled by the email from the CEO**, and used his corp card to send the iTunes gift cards. We lost about $5,000."

—Adam A., video game rentals, 150 employees

"The only reason **we caught it** was that it was a 6 digit sales order and our sales orders are a 7 digit."

— Joe B, food distribution, 250 employees

"We saw that it was moving through the network drives, **encrypting files**, starting with Z: drive and moving down"

— Jerry K, import/export, 250 employees

"They **got someone's password**, and sent an email to our CFO, who sent the $40,000 wire transfer."

— Bob K., property management, 150 employees

Microsoft Threat Protection suite protects

- Email and collaboration with Office 365 ATP

- Identities with Azure ATP and Azure AD Identity Protection

- Endpoints with Microsoft Defender ATP

- Applications with Microsoft Cloud App security

Office 365 Advanced Threat Protection

- ATP Safe Attachments protects against unknown malware and viruses

- ATP Safe Links protects your users from malicious URLs

- Office 365 ATP also helps detect and block files that are identified as malicious in SharePoint, OneDrive and Microsoft Teams

Azure ATP and Azure AD Identity Protection

- Azure ATP leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats

- Azure ATP provides insight on compromised identities and malicious insider actions directed at your organization

- Azure ATP and Azure AD assist with improving identity security posture

Microsoft Defender Advanced Threat Protection

- Next-generation protection by using advanced behavioral analytics and Machine Learning

- Identifies vulnerabilities with installed software: both Microsoft and third party

- Shows active threats out in the world and how this impacts your organization

- Assists with reducing the attack surface

Gartner magic quadrant for endpoint protection platforms

Microsoft Cloud App Security (MCAS)

- Discover and control the use of Shadow IT

- Assess the compliance of your cloud apps

- Provides the whole story in a threat investigation

Microsoft Secure Score

- Assess your organization's security posture across its entire digital estate

- Assess your current security posture and identify potential improvements

- Identify where to improve your security posture using threat-prioritized insights and guidance

Microsoft Intune

- Implement configuration changes per security recommendations

- Enforce compliance and conditional access policies

Key Takeaways

1. Education is the best protection for cyber security

2. Have a way to monitor when your business account has "abnormal" access

3. Enable MFA if you want to be sure all access to that account will require approval from your cell phone

4. Install Security tools to protect your data on your desktop and servers

5. Make sure you are using backup systems that are not outdated to protect against ransomware

Questions

360visibility.com