DLP, Phishing, Tech Support Scams

Miten Microsoft toteuttaa tietoturvaa ja tietosuojaa? November 2018

Mikko Viitaila
@mikkoviitaila
National Technology Officer, Teknologiajohtaja
Microsoft Oy
Microsoft in Finland is a strong millennial, born 1992. 2+ million active users in Microsoft Office 365 cloud. 2,000+ partners generating 8 $ revenue per each $ by MSFT. Partner ecosystem with 40,000 tech jobs in Finland. 1,600 start-ups directly supported by Microsoft. Close to 90% of the students in Finland using Office 365. 51% of major Finnish companies using the cloud.
Agenda

- Digital Estate – Threat Landscape
- Microsoft’s Approach to Security
- DLP
- Phishing
- Tech-support Scams
The digital estate is growing
The cybersecurity landscape is rapidly changing

Cyberspace is the new battlefield

Security skills are in short supply

Virtually anything can be attacked
Your Organization in Transformation

Cloud Technology

SaaS adoption

Infrastructure as a Service

Platform as a Service

Internet of Things

Perimeter of a Modern Enterprise

1st class mobile experience
Q: WHERE IS YOUR DATA?

A: EVERYWHERE

- Devices: fixed and mobile
- SaaS apps & file shares
- On-premises file shares

On-premises

Online backup

Email

Cloud storage

SaaS apps

Mobile devices

Q: WHERE IS YOUR DATA?

A: EVERYWHERE

- Devices: fixed and mobile
- SaaS apps & file shares
- On-premises file shares

On-premises

Online backup

Email

Cloud storage

SaaS apps

Mobile devices
88% of employees use non-approved SaaS apps at work

85% of enterprise organizations keep sensitive information in the cloud

88% of organizations no longer have confidence to detect and prevent loss of sensitive data

58% have accidentally sent sensitive information to the wrong person
The challenge of securing your environment

Bad actors are using increasingly creative and sophisticated attacks.

The digital estate offers a very broad surface area that is difficult to secure.

Integrated, intelligent correlation and action on signals is difficult, time-consuming, and expensive.
Increasingly Hostile Environment

- Increased attack surface with new technologies creates new blind spots
- Attacks rising in volume and sophistication to capture illicit opportunities

Enterprise IT is Cloud Hybrid

- Cloud adoption is inevitable (Digital Transformation + industry momentum)
- Legacy systems will take years to migrate or retire

Technology Mobility and Volume is Exploding

- Increasing demand for first class experience on mobile devices
- Variance in trustworthiness of mobile devices

Pervasive Digital Transformation and IoT

- IoT adoption driving a wave of app development and cloud usage
- Enterprise PC Security strategies applies poorly to IoT devices

Increasingly Hostile Environment

- Increased attack surface with new technologies creates new blind spots
- Attacks rising in volume and sophistication to capture illicit opportunities
Microsoft’s Approach
Focusing security efforts in a complex landscape

- **Adopt identity-based protection**: Enable Seamless and secure identity and access for employees, partners and customers.
- **Apply persistent data protection**: Protect sensitive data – wherever it lives or travels.
- **Protect against sophisticated hackers**: Protect, detect and remediate against threats across the modern workplace.
- **Simplify security management**: Streamline management with built-in intelligence and recommendations.
Microsoft Security

Identities
Users and admins

Endpoints
Devices and sensors

User Data
Email messages and documents

Cloud Apps
SaaS applications and data stores

Infrastructure
Servers, virtual machines, databases, networks

Intelligent Security Graph
6.5 TRILLION signals per day
Holistic view on security...

- 200+ global cloud consumer and commercial services
- 1.2 billion devices scanned by Windows Defender
- 450 billion authentications
- 18+ billion web pages scanned by Bing
- 400 billion e-mails analyzed

The Microsoft Intelligent Security Graph
...provides new insights

1.2 billion devices scanned by Windows Defender

400 billion e-mails analyzed

18+ billion web pages scanned by Bing

200+ global cloud consumer and commercial services

450 billion authentications

Intelligence

Insights across Clients and Services

The Microsoft Intelligent Security Graph
Data Loss Prevention
Evolution of Information Protection

Microsoft Security Philosophy

- Access Controls
  - + Encryption
- + Rights Management
- + Full Lifecycle Protection (Auto Classification, SaaS)

Information Protection Trends

- Fileshare & USB stick Sprawl
- SharePoint & Email/Mobile Sprawl
- Cloud & Shadow IT Sprawl

Information Technology

- Mainframes + PCs
- + Datacenters + Mobile Devices
- + Cloud + Internet of Things (IoT)
Data Security Challenges

Reduce and manage risk of user errors
Collaboration to create new business value requires data sharing and data mobility
Critically important to prevent unauthorized disclosure, modification, or destruction

Classification is challenging
Manual user classification is impractical at scale
Large set of existing documents and more being created all the time

Data must be protected outside of the network
Data must be protected as it traverses mobile devices and cloud services
Data created outside the network must be classified and protected

Compliance & security require a complete strategy
Compliance penalties are increasing and measuring outcomes vs. methods
Need full lifecycle protection for information assets (appropriate to valuation)
Data protection & data governance go hand-in-hand

Comprehensive policies to protect and govern your most important data – throughout its lifecycle

- Unified approach to discover, classify & label
- Automatically apply policy-based actions
- Proactive monitoring to identify risks
- Broad coverage across locations
Follow data throughout its lifecycle

Users are guided to classify files, or content automatically scanned for sensitive info

Data gets protected based on policy

Data travels across various locations, shared

Data gets monitored

Data gets retired, deleted

Data gets created, imported, & modified across various locations

Detect & Apply protection based on policy information

Do you need the flexibility to apply a range of regulations and compliance factors impacting your company?

Does protection need to persist with the data, even as it travels across devices, sand apps and on-premises?

Do you have a way to ensure that labels persist with the data—wherever it travels?

Are you able to empower end-users to protect content themselves, or apply automatically based on company policies?

Do you have the right notifications and education for users about being responsible with sensitive data?
Microsoft Information Protection solutions

Protect your sensitive data – wherever it lives or travels

Discover  
Classify  
Protect  
Monitor

Across

Devices  
Apps  
Cloud services  
On-premises
Phishing
Phishing attacks are fast and hard to stop

If an attacker sends an email to **100 people** in your company...

...**23 people** will open it...

...**11 people** will open the attachment...

...and **six** will do it in the first hour.
On average, 16 malicious emails per month per user.

92.4% of malware is delivered via email.  
https://enterprise.verizon.com/resources/reports/dbir/

Fake invoices are the #1 disguise for distributing malware.  
The Phishing Landscape

Attack Spectrum

Broad ($)  
- Scams  
  - E.g. Personal Identity/Financial
- Brand Phishing  
  - E.g. Access consumer credentials
- IT/SaaS Phishing  
  - E.g. Access to org credentials and data
- Spear Phishing  
  - E.g. Wire/W2, BEC, high profile accounts

Targeted ($$$)

- Domain Spoof
- Phishing Attachments
- Credential Phishing Links
- Link to fake SaaS Apps
- User Impersonation
- Domain Impersonation
Microsoft statistics

300,000 Phish Campaigns Analyzed in 2018

8 million Business Email Compromise Attempts in 2018

20% Of users click on a malicious link in first 5 minutes

Phishing email statistics from Office 365 from January 2018 to September 2018
Anti-phish capabilities in Office 365

5 billion
Phish Emails Blocked in Office 365 in 2018

7 billion
URL clicks protected by Safe Links in 2018

11 billion
Unique items detonated by ATP sandboxing in 2018
Microsoft’s Approach

Rich signal across M365  

Artificial Intelligence

Rich client & Service Integration

Protect  
During mail flow and post delivery

Detect  
User and Admin controls

Respond  
Visibility and actionable insights
Phish email categories and anti-phish enhancements

**Domain Spoof**
- DMARC, DKIM, SPF
- Implicit Intra Org spoof detection
- Implicit Cross domain spoof detection

**Content Detonation**
- Detonate Attachments
- Detonate URLs
- Detect Text lures

**Compromised**
- Internal Safe links
- Multi factor Authentication

**Impersonation**
- Detect Look alike domains
- Detect User Display name tricks
- Detect brand impersonation

**Anti-phish Enhancements**
- Spoof Intelligence for intra-org and cross domain spoof detection
- Advanced Machine Learning Models
- Time of Click Protection (Safe links)
- Internal Safe links
- Detonation of attachments for phish/malware
- Detonation of Link Content for malware/phishing sites & attachments
- Detonation and detection of malicious files in SharePoint/OneDrive/Microsoft Teams
- Mailbox Intelligence for user contact graph
- User and Domain Impersonation protection
- Real time reporting
- Rich Insights
Normalized Phish Miss in Office 365 by Vendor, May 1 – Sep 16 2018

Mail flow volume

Office 365
Vendor 1
Vendor 2
Vendor 3
Vendor 4
Vendor 5
Vendor 6
Vendor 7
Vendor 8
Vendor 9
Vendor 10
Vendor 11

Office 365 EOP/ATP
This sender might be impersonating a domain that’s associated with your organization. Learn why this could be a risk Feedback

Your user account is going to be disabled. Login now to prevent suspension.

Go to the sign-in page, https://portal.office.com

Sincerely,
The Microsoft Office 365 Team
Phishing: Six Best Practices to apply TODAY

1. Enable ATP Safe links and Safe attachments for ALL users
2. Tune machine models tolerance for Phishing
   - Lower the phish threshold for key users
3. Review ETR Rules (Exchange Transport Rule)
   - Ensure IP/Domain allow rules include checks for authentication
4. Utilize the new reporting Add-in to gain insights
5. Enable MFA
6. Get to DMARC p=Reject
   - DMARC = Domain-based Message Authentication, Reporting and Conformance
Tech Support Scams
Tech Support: Remote Access

Go to www.teamviewer.com
Microsoft statistics
Some stats

- **FBI**: 11,000 tech-support fraud complaints in 2017 with claimed losses totaling nearly $15m, up 86 percent on reported losses in 2016. It received reports from victims in over 80 countries. [https://www.ic3.gov/media/2018/180328.aspx](https://www.ic3.gov/media/2018/180328.aspx)

- **Microsoft**: In 2017, Microsoft Customer Support Services received 153,000 reports from customers who encountered or fell victim to tech support scams, a 24% growth from the previous year. These reports came from 183 countries, indicating a global problem. [https://cloudblogs.microsoft.com/microsoftsecure/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/](https://cloudblogs.microsoft.com/microsoftsecure/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/)
Tech Support Scams – Scope of the problem

2 out of 3 people have experienced a tech support scam in the last year.

1 in 5 consumers surveyed continued with a potential fraudulent interactions; meaning they downloaded software, visited a scam website, gave the fraudsters remote access to their device, or provided credit card information or other form of payment.

Nearly 1 in 10 have lost money to a tech support scam.

Of those who continued with a fraudulent interaction, 17% of them were older than 55, while 34% were between the ages of 36 and 54.

50% of those who continued were millennials, between the ages of 18 and 34.

Source: Ipsos, Global Market Research, commissioned by Microsoft, July 2016.
An Industry Wide Problem
Protect yourself from tech support scams

• Microsoft does not send unsolicited email messages or make unsolicited phone calls to request for personal or financial information, or fix your computer.

• Microsoft will never proactively reach out to you to provide unsolicited PC or technical support → Any communication we have with you must be initiated by you.

• Don’t call the number in pop-ups → Microsoft’s error and warning messages never include a phone number.

• Report it
  • www.microsoft.com/reportascam
Jatketaan keskustelua...

Mikko Viitaila
Teknologiajohtaja, National Technology Officer (NTO)
Microsoft Oy

mikko.viitaila@microsoft.com
@mikkoviitaila
www.linkedin.com/in/viitaila
+358 40 8098757
Microsoft mission

Empower every person and every organization on the planet to achieve more