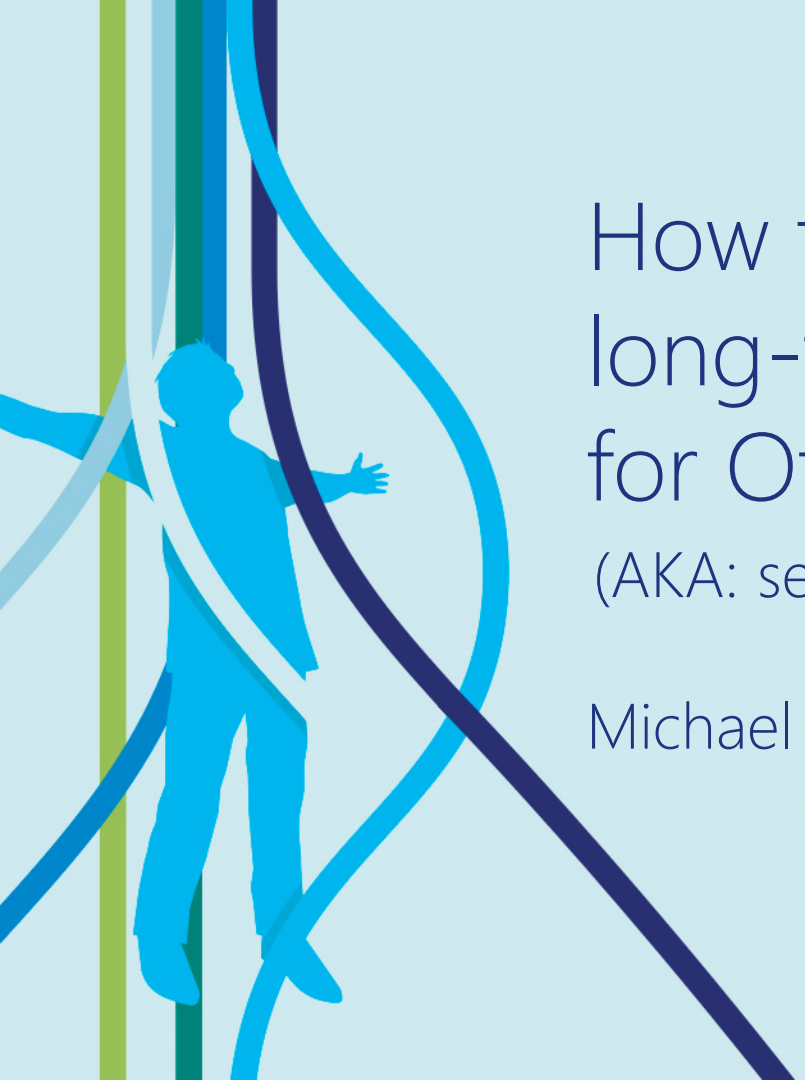


How to develop and deliver a long-term security strategy for Office 365 that works !

(AKA: security for the IT-Pro)

Michael Van Horenbeeck

Experts Live Netherlands

Michael Van Horenbeeck

Managing Partner | The Collective

Offices Apps & Services MVP

Security/EMS afficionado

@vanhybrid

Classification: Public

"There's two types of organizations: those who have been hacked, and those who don't know it yet..."

John T. Chambers

Classification: Public

Importance of a strategy

- Implementing solutions for the sake of implementing them is (rarely) a good idea.
- Adding products and features to your solution stack often means adding complexity which can affect your security/compliance baseline (negatively).

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Identify/enumerate risks/threats

- Identify threats that are applicable for your organization and 'common' in the industry. For example:
  - Is there a high(er) risk of Data Loss (e.g. *corporate espionage*)?
  - What workloads will you be using?

Classification: Public

Build your own Threat Matrix

- What is the threat/risk?
- What would the impact of the threat be?
- How likely is it going to occur (probability)?
- How can I mitigate the risk? Is there more than one approach?
- What is the cost of implementing the solution? (both licensing and effort)

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Example

Threat	Impact	Probability	Possible solution(s)
Ability to (inadvertently) share sensitive information with a non-authorized 3rd-party (via email).	High	Medium	• Prevent automatic forwarding • Implement Rights Management • Office Message Encryption • Implement Session Controls • ….

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Threats/Risks have many forms

- Data Theft / Data Loss
- Malicious software (malware, ransomware)
- Phishing
- Regulations
- …

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Compliance

Internal/External compliance requirements add a layer of complexity:

- GDPR, EAVG,…
- HIPAA (*US*)
- ISO
- PCI DSS (*Payment Card Industry*)
- …

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Type of measures

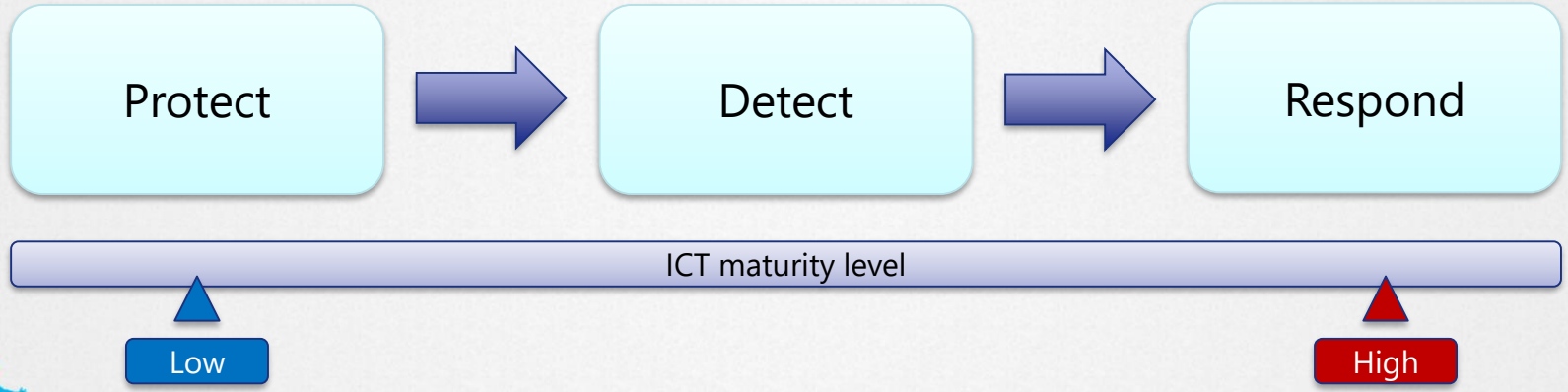
- Not all threats need to/can be mitigated with a (*technical*) solution.
- Organizational measures (*e.g. procedures*) can be effective too.
  - e.g. User training/awareness
  - IT Policy

Classification: Public

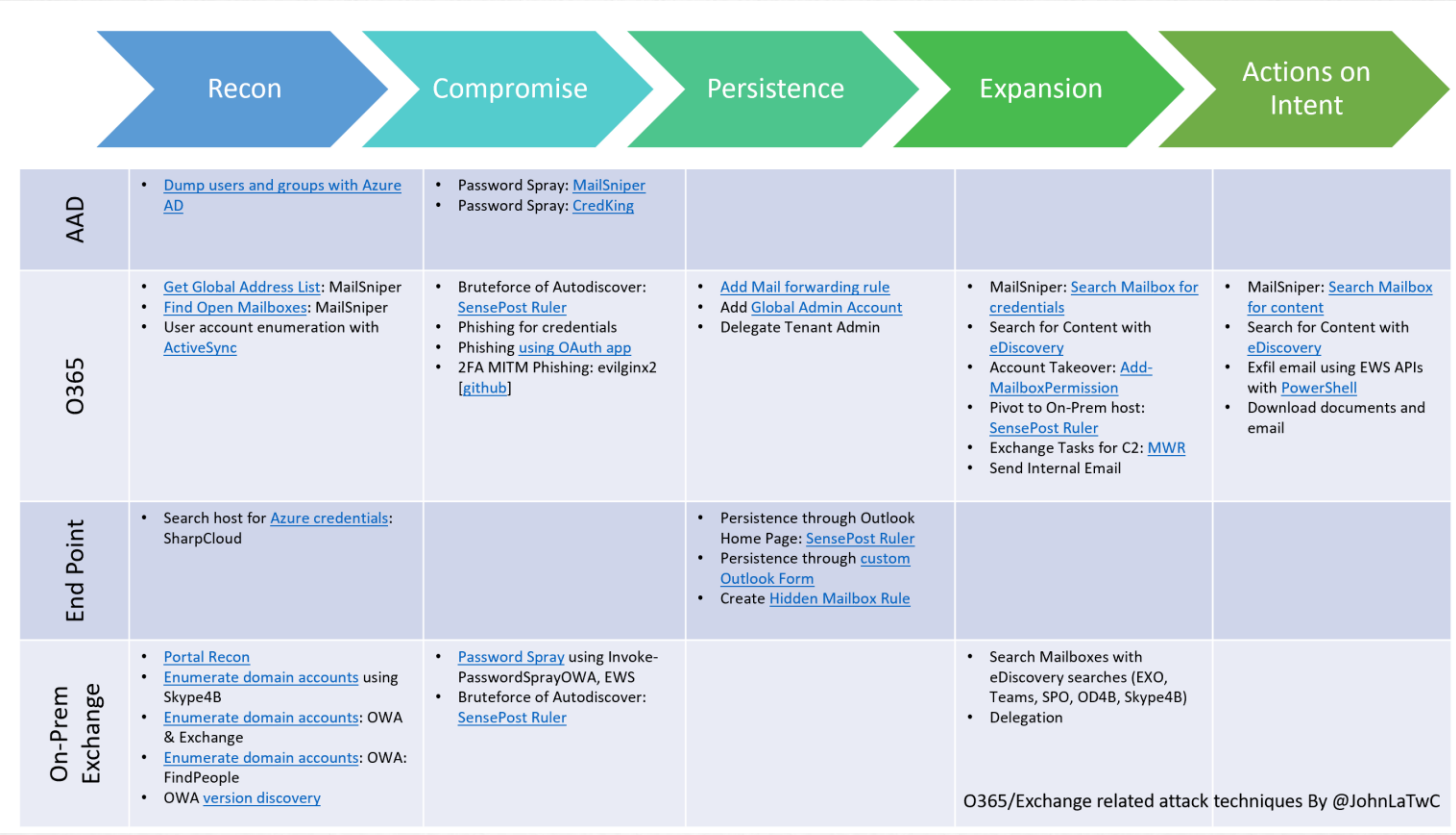
COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Framework?

Various frameworks exist to aid developing a security strategy. Choose which one fits you best (if any). Ideally, combine them.



Classification: Public



	Recon	Compromise	Persistence	Expansion	Actions on Intent
AAD	• Dump users and groups with Azure AD	• Password Spray: MailSniper • Password Spray: CredKing			
O365	• Get Global Address List: MailSniper • Find Open Mailboxes: MailSniper • User account enumeration with ActiveSync	• Bruteforce of Autodiscover: SensePost Ruler • Phishing for credentials • Phishing using OAuth app • 2FA MITM Phishing: evilginx2 [github]	• Add Mail forwarding rule • Add Global Admin Account • Delegate Tenant Admin	• MailSniper: Search Mailbox for credentials • Search for Content with eDiscovery • Account Takeover: Add-MailboxPermission • Pivot to On-Prem host: SensePost Ruler • Exchange Tasks for C2: MWR • Send Internal Email	• MailSniper: Search Mailbox for content • Search for Content with eDiscovery • Exfil email using EWS APIs with PowerShell • Download documents and email
End Point	• Search host for Azure credentials: SharpCloud		• Persistence through Outlook Home Page: SensePost Ruler • Persistence through custom Outlook Form • Create Hidden Mailbox Rule		
On-Prem Exchange	• Portal Recon • Enumerate domain accounts using Skype4B • Enumerate domain accounts: OWA & Exchange • Enumerate domain accounts: OWA: FindPeople • OWA version discovery	• Password Spray using Invoke-PasswordSprayOWA, EWS • Bruteforce of Autodiscover: SensePost Ruler		• Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B) • Delegation	

O365/Exchange related attack techniques By @JohnLaTwC

Classification: Public

Protect (prevention)

- Make sure to cover as much as you (reasonably) can; it will keep out 90%+ of the threats.
- Examples are:
  - DLP policies
  - Azure Information Protection
  - …

Classification: Public

Detect

- Effective en intelligent detection mechanisms can help you minimize damages of a breach and will reduce the time to counteract.
- Measure for gaps in your protection strategy first.
  - e.g. Windows Defender ATP
  - SIEM-integration (e.g. Sentinel)

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

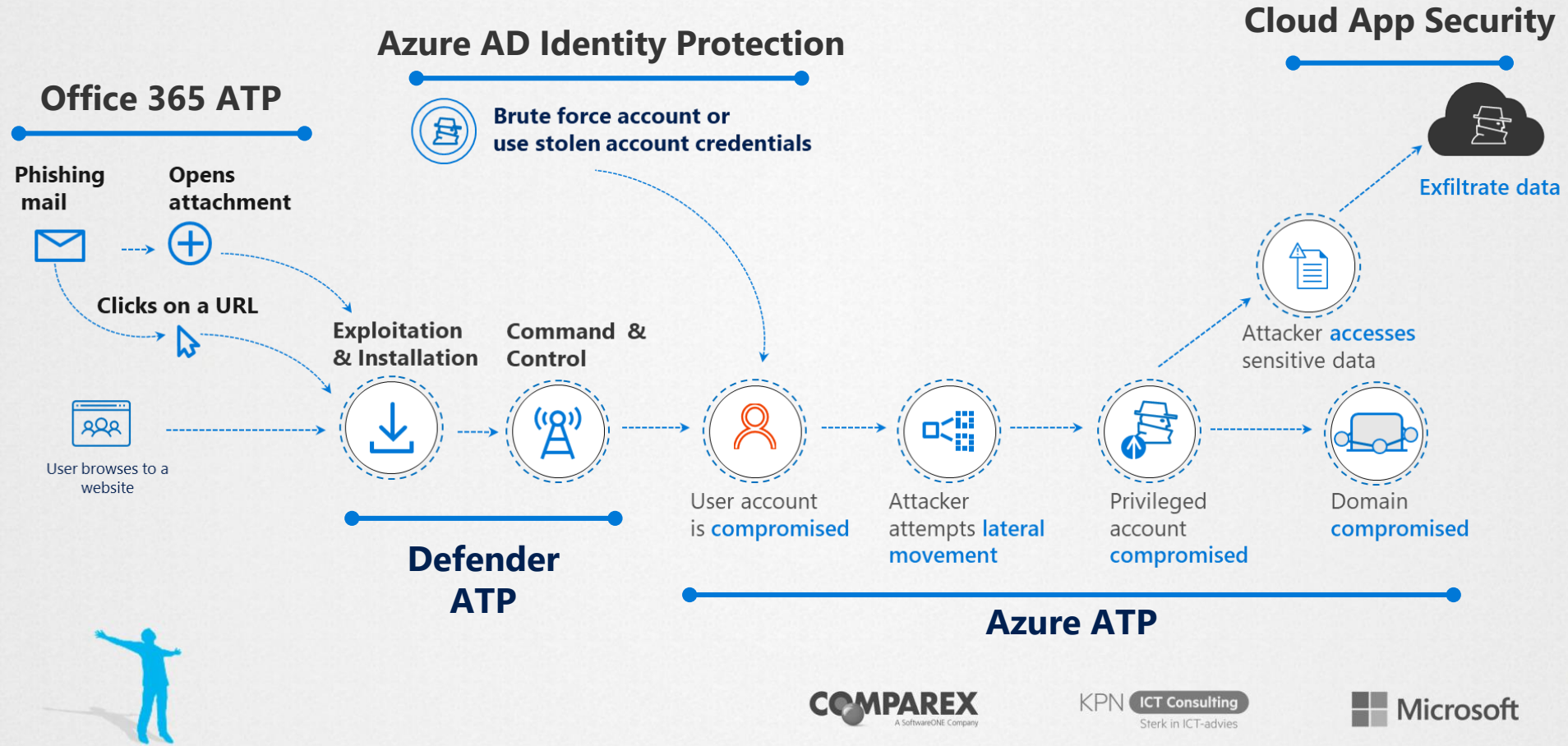
Classification: Public

Respond

Make sure to have appropriate tools and processes in place to tackle a problem head-on.

Classification: Public

MICROSOFT 365



Classification: Public

What to focus on?

Depending on your current security posture, you might want to first spend (most) efforts on developing a good/thorough defense strategy (protect)

Classification: Public

What to watch out for?

- There is a balance between cost & effectiveness.
- Some features may offer a solution, but may end up costing too much (vs. the risk exposure); proportionality principle
  - e.g. Is it really worth spending 1million to protect assets worth 100k?*
- Pareto principle also applies to cybersecurity…

MICROSOFT 365

Identifying threats & defining countermeasures

Exchange Online

Threat	Possible solution(s)
Ability to (inadvertently) share sensitive information with a non-authorized 3rd-party (via email). *Manual or automatic action.*	• Prevent automatic forwarding • Implement Rights Management • Office Message Encryption • Implement Session Controls • ….

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Exchange Online

Threat	Possible solution(s)
Potential to receive harmful payloads (e.g. Malware) via email.	• Implement Office 365 ATP • Implement Windows Defender ATP • Implement Azure Sentinel

Classification: Public

Exchange Online

Threat	Possible solution(s)
Potential to receive spoofed messages in order to trick users to 1) perform unauthorized actions or 2) click malicious links (to download payload).	• Implement Office 365 ATP • User awareness training

Classification: Public

Exchange Online/SPO

Threat	Possible solution(s)
Weak identification of the recipient (which may lead to unintended disclosure of sensitive information).	• Implement Rights Management (*w/ ability to revoke content*) • User awareness • Leverage Global Address list • Monitoring / Supervision policies • ….

Classification: Public

Exchange Online

Threat	Possible solution(s)
Potential data exfiltration through Outlook (fat client)	• Disallow users to connect multiple accounts in Outlook. • Implement rights management

Classification: Public

Exchange Online

Threat	Possible solution(s)
Potential data exfiltration through Outlook by synchronizing contents onto an insecure device (OST/PST)	• Conditional Access (only allow managed devices); limit downloading of files through managed devices only • Disable ability to take files offline in Outlook Web App

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Exchange Online

Threat	Possible solution(s)
Potential reputational damage because of spoofed domains	• Implement DKIM and DMARC • Use S/MIME • *Use Office Message Encryption*

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Exchange Online

Threat	Possible solution(s)
Lack of probative value of correspondence	• Keep message tracking logs • Use Office Message Encryption • Use DKIM/DMARC (and monitor!)

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

SharePoint Online / ODfB

Threat	Possible solution(s)
Ability to (inadvertently) share sensitive information with a non-authorized 3rd-party.	• Disallow external sharing • Create specific site(s) or libraries through which sharing is possible. • Implement Rights Management • Implement DLP Policies • Monitoring (SecOps) • Auditing & Reporting (*e.g. whom has shared what*)

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

SharePoint Online / ODfB

Threat	Possible solution(s)
Users can potentially upload/download harmful payloads (e.g. Malware)	• Implement Office 365 ATP • Deploy Defender ATP • Monitoring & Reporting

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

SharePoint Online / ODfB

Threat	Possible solution(s)
Potential data exfiltration (*to insecure devices*) through synchronizations mechanisms	• Prevent synchronization (completely, partially) • Implement Conditional Access • User Cloud App Security Session policies

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Authentication

Threat	Possible solution(s)
Risk of (successful) brute force attacks	• Relax the security restrictions... • Cloud App Security (broker for cloud applications) • Deploy MDATP (monitoring) • User awareness training

Authentication

Threat	Possible solution(s)
Use of insecure passwords	• Implement (strong) password policy • Enforce MFA • Block Legacy authentication • Implement Password Hash Synchronization (for *Insecure Password Detection*)

Classification: Public

Authentication (ADFS)

Threat	Possible solution(s)
Risk of being victim of a DDOS attack	• Implement DDOS mitigation solutions (also processes!) • Highly-available setup of ADFS • Have backup strategy available (e.g. tunnel all traffic if external access to ADFS is unavailable)

Teams

Threat	Possible solution(s)
External users may have access inadvertently access to sensitive data	• User awareness training • Implement Rights Management • Prevent external sharing • Implement Cloud App Security session controls.

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Flow

Threat	Possible solution(s)
Ability to exfiltrate data through Flow, despite DLP policies. Flow DLP policies prevent sharing data across e.g. Different connectors, but it won't stop you from reading an email and then forwarding it.	• User awareness • Implement Rights Management

Classification: Public

General

Threat	Possible solution(s)
Rogue admin	• Implement Privileged Identity Management • Proactive monitoring, reporting and alerting • Implement Alert Policy in SIEM or CAS to alert when high-privileged account is (mis)-used • Conditional Access to restrict usage of privileged accounts

Classification: Public

General

Threat	Possible solution(s)
Accidental misconfiguration by privileged accounts	• Implement Privileged Identity Management • Use automation where possible (manual actions increase the risk) • Abide to the principe of least privilege > RBAC, Privileged Access Management

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

General

Threat	Possible solution(s)
Risk of introducing (more) Shadow IT by a (too) restrictive approach of the security countermeasures; no visibility in current shadow it usage	• Relax the security restrictions... • Cloud App Security (broker for cloud applications) • Deploy MDATP (monitoring) • User awareness training

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

General

Threat	Possible solution(s)
When installing Office Pro Plus on a computer at home, data might be inadvertently visible.	• User education • Block download/installation of Office from portal • Implement Conditional Access

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

General

Threat	Possible solution(s)
User registers 3rd-party application which could exfiltrate user data	• Turn off user consents in Azure AD

Classification: Public

Other

Threat	Possible solution(s)
Microsoft has the potential to access customer data.	• Implement Customer Lockbox • Implement Customer Key (*Service Encryption)*

Classification: Public

Other

Threat	Possible solution(s)
Foreign (*US)* government might subpoena Microsoft for proprietary information.	• Don't move such data into Office 365… (*Customer Key only mitigates unauthorized snooping*)

Classification: Public

Other

Threat	Possible solution(s)
Unavailability of the Azure Information Protection client	• Monitoring • Implement Defender ATP + Azure Information Protection analytics

Classification: Public

COMPAREX A SoftwareONE Company
KPN ICT Consulting Sterk in ICT-advies
Microsoft

Other

Threat	Possible solution(s)
DLP policies don't apply immediately to newly-uploaded documents; there might be a (significant) delay	• Implement Cloud App Security (e.g. Session controls) • Implement Rights Management (document-level)

Workstation

Threat	Possible solution(s)
Default antivirus not sufficient to deal with zero-day threaths and advanced malware	• Implement Defender ATP • Integrate with e.g. Cloud App Security • Enhance w/ Intune Compliance Policy

Classification: Public

Workstation

Threat	Possible solution(s)
Windows attack surface	• Implement Intune (Security Baseline policy) • Defender ATP (Attack Surface Reduction Rules) • For Azure VMs > Azure Security Center

Classification: Public

GDPR

Threat	Possible solution(s)
Users have access to the Azure Portal through which they may be able to (easily) see other user information and/or resource information	• Restrict access to the Azure Portal for users • Implement Conditional Access / Cloud App Security to restrict access to the feature

Classification: Public

GDPR

Threat	Possible solution(s)
Personal data potentially captured without consent (and available to users) when using 'Track & Trace' in Azure Information Protection	• Prevent automatic forwarding • Implement Rights Management • Office Message Encryption • Implement Session Controls • ….

Classification: Public

GDPR

Threat	Possible solution(s)
Personal information of guest accounts centrally stored in Azure AD (no lifecycle by default). Data is potentially captured without prior consent.	• Prevent automatic forwarding • Implement Rights Management • Office Message Encryption • Implement Session Controls • ….

Classification: Public

Are you GDPR compliant?*

- GDPR is not just about implementing (technical) solutions to specific threats/scenarios.
- It's also (more) about having proper controls/processes in place to deal with subject privacy. Technical solutions aid in abiding to those controls/processes.

COMPAREX A SoftwareONE Company

KPN ICT Consulting Sterk in ICT-advies

Microsoft

Classification: Public

MICROSOFT 365

Maintaining your strategy

It's a moving target…

- **Define** a roadmap (fit-gap)
- **Update** the roadmap **regularly** (in function of new features, updates, etc.)

Classification: Public

TL;DL

Key Points

- Start by defining threats applicable to your organization/data… Define solutions from there.
- Make sure to cover all cycles(protect, detect, respond)
- Regularly revisit your strategy/roadmap as features are updated and new capabilities/solutions introduced.

Classification: Public

Next session: 11:30AM – 12:30PM

Infrastructure as Code; Azure Resource Manager - inside out

Henry Been

Experts Live Netherlands