

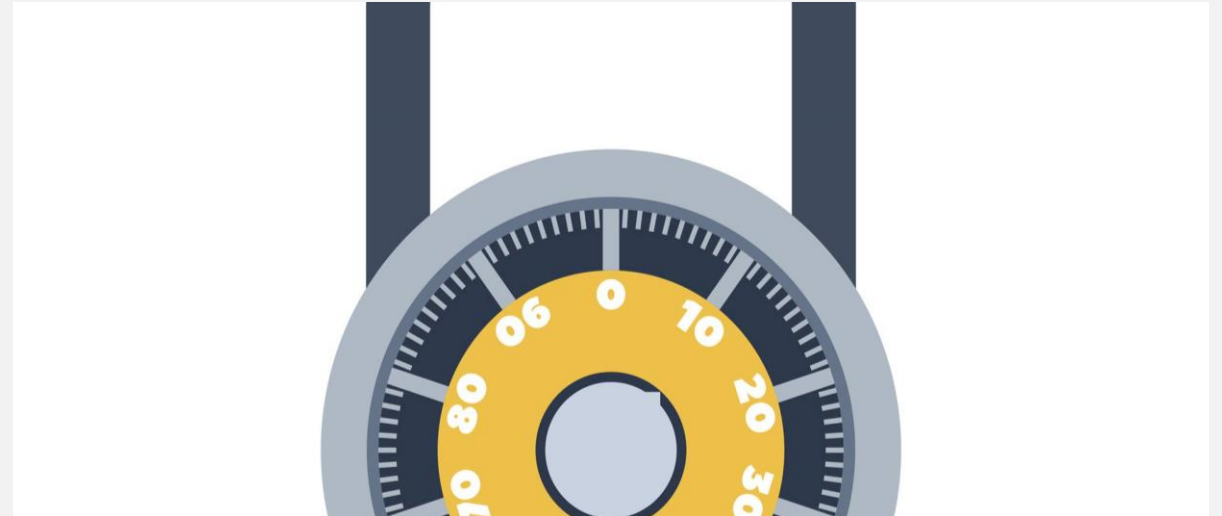


# Office 365

**Hvad nu med privacy og sikkerhed**

---

[kpmg.com/dk](https://kpmg.com/dk)





- 01 Office 365 -fælder
- 02 Særligt omkring logning
- 03 Lidt om sikkerhed
- 04 Azure Marketplace og O365
- 05 GDPR fælder



## **Den første som opretter virksomhedens Office 365 er Global Admin**

## Vær opmærksom på:

Det ser meget nemt ud:

1. Konfigurerer Azure AD Connect og synkroniser brugere og grupper
2. Flyt Exchange Oneline (hav 1 server on-prem for management)
3. Update Mailflow

Det betyder at:

1. Alle i hele verdenen din Office 365.
2. Jeres sikkerhedsarkitektur er ændret
3. Jeres AD er nu AzureAD

The following list contains examples of configuration vulnerabilities:

- **Multi-factor authentication for administrator accounts not enabled by default:** Azure Active Directory (AD) Global Administrators in an O365 environment have the highest level of administrator privileges at the tenant level. This is equivalent to the Domain Administrator in an on-premises AD environment. The Azure AD Global Administrator accounts are the first accounts created so that administrators can begin configuring their tenant and eventually migrate their users. Multi-factor authentication (MFA) is not enabled by default for these accounts.[1] There is a default Conditional Access policy available to customers, but the Global Administrator must explicitly enable this policy in order to enable MFA for these accounts. These accounts are exposed to internet access because they are based in the cloud. If not immediately secured, these cloud-based accounts could allow an attacker to maintain persistence as a customer migrates users to O365.
- **Mailbox auditing disabled:** O365 mailbox auditing logs actions that mailbox owners, delegates, and administrators perform. Microsoft did not enable auditing by default in O365 prior to January 2019. Customers who procured their O365 environment before 2019 had to explicitly enable mailbox auditing.[2] Additionally, the O365 environment does not currently enable the unified audit log by default. The unified audit log contains events from Exchange Online, SharePoint Online, OneDrive, Azure AD, Microsoft Teams, PowerBI, and other O365 services.[3] An administrator must enable the unified audit log in the Security and Compliance Center before queries can be run.
- **Password sync enabled:** Azure AD Connect integrates on-premises environments with Azure AD when customers migrate to O365.[4] This technology provides the capability to create Azure AD identities from on-premises AD identities or to match previously created Azure AD identities with on-premises AD identities. The on-premises identities become the authoritative identities in the cloud. In order to match identities, the AD identity needs to match certain attributes. If matched, the Azure AD identity is flagged as on-premises managed. Therefore, it is possible to create an AD identity that matches an administrator in Azure AD and create an account on-premises with the same username. One of the authentication options for Azure AD is "Password Sync." If this option is enabled, the password from on-premises overwrites the password in Azure AD. In this particular situation, if the on-premises AD identity is compromised, then an attacker could move laterally to the cloud when the sync occurs. **Note:** Microsoft has disabled the capability to match certain administrator accounts as of October 2018. However, organizations may have performed administrator account matching prior to Microsoft disabling this function, thereby synching identities that may have been compromised prior to migration. Additionally, regular user accounts are not protected by this capability being disabled.
- **Authentication unsupported by legacy protocols:** Azure AD is the authentication method that O365 uses to authenticate with Exchange Online, which provides email services. There are a number of protocols associated with Exchange Online authentication that do not support modern authentication methods with MFA features. These protocols include Post Office Protocol (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transport Protocol (SMTP). Legacy protocols are used with older email clients, which do not support modern authentication. Legacy protocols can be disabled at the tenant level or at the user level. However, should an organization require older email clients as a business necessity, these protocols will not be disabled. This leaves email accounts exposed to the internet with only the username and password as the primary authentication method. One approach mitigate this issue is to inventory users who still require the use of a legacy email client and legacy email protocols. Using Azure AD Conditional Access policies can help reduce the number of users who have the ability to use legacy protocol authentication methods. Taking this step will greatly reduce the attack surface for organizations.[5]

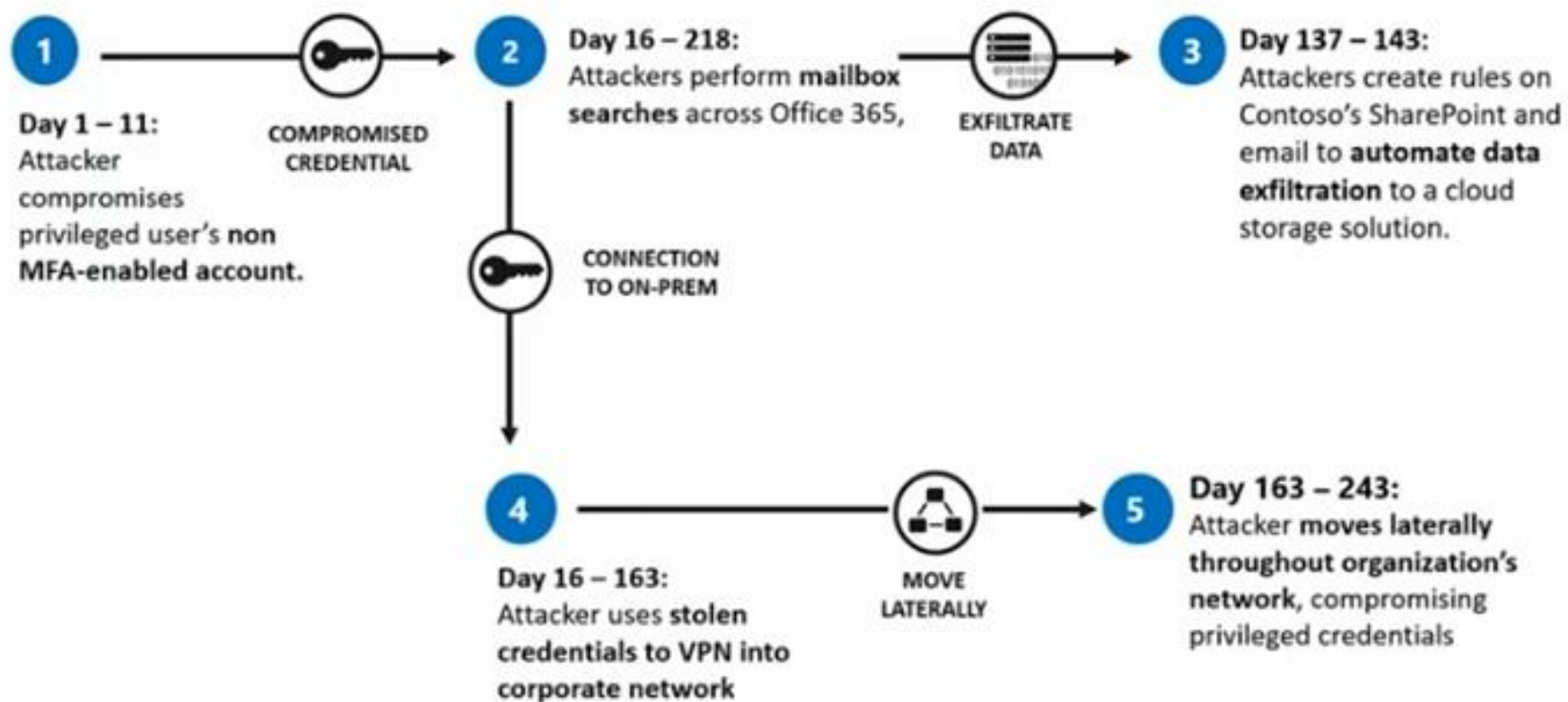
Protocol (SMTP). Legacy protocols are used with older email clients, which do not support modern authentication. Legacy protocols can be disabled at the tenant level or at the user level. However, should an organization require older email clients as a business necessity, these protocols will not be disabled. This leaves email accounts exposed to the internet with only the username and password as the primary authentication method. One approach mitigate this issue is to inventory users who still require the use of a legacy email client and legacy email protocols. Using Azure AD Conditional Access policies can help reduce the number of users who have the ability to use legacy protocol authentication methods. Taking this step will greatly reduce the attack surface for organizations.[5]



Audit Item	Category	Enabled by Default	Retention
User Activity	Office 365 Security & Compliance Center	No	90 days
Admin Activity	Office 365 Security & Compliance Center	No	90 days
Mailbox Auditing	Exchange Online	No*	90 days
Sign-in Activity	Azure AD	Yes	30 days (AAD P1)
Users at Risk	Azure AD	Yes	7 days 30 days (AAD P1) 90 days (AAD P2)
Risky Sign-ins	Azure AD	Yes	7 days 30 days (AAD P1) 90 days (AAD P2)
Azure MFA Usage	Azure AD	Yes	30 days
Directory Audit	Azure AD	Yes	7 days 30 days (Azure AD P1/P2)

\* Microsoft is gradually enabling mailbox auditing for tenants.

## Attack timeline





AAD	<ul style="list-style-type: none"> <li>• <a href="#">Dump users and groups with Azure AD</a></li> </ul>	<ul style="list-style-type: none"> <li>• Password Spray: <a href="#">MailSniper</a></li> <li>• Password Spray: <a href="#">CredKing</a></li> </ul>			
O365	<ul style="list-style-type: none"> <li>• <a href="#">Get Global Address List</a>: MailSniper</li> <li>• <a href="#">Find Open Mailboxes</a>: MailSniper</li> <li>• User account enumeration with <a href="#">ActiveSync</a></li> <li>• <a href="#">Harvest</a> email addresses</li> <li>• Verify <a href="#">target</a> is on O365, [<a href="#">DNS</a>], [<a href="#">urls</a>], [<a href="#">list</a>]</li> </ul>	<ul style="list-style-type: none"> <li>• Bruteforce of Autodiscover: <a href="#">SensePost Ruler</a></li> <li>• Phishing for credentials</li> <li>• Phishing <a href="#">using OAuth app</a></li> <li>• 2FA MITM Phishing: evilginx2 [<a href="#">github</a>]</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Add Mail forwarding rule</a></li> <li>• Add <a href="#">Global Admin Account</a></li> <li>• Delegate Tenant Admin</li> </ul>	<ul style="list-style-type: none"> <li>• MailSniper: <a href="#">Search Mailbox for credentials</a></li> <li>• Search for Content with <a href="#">eDiscovery</a></li> <li>• Account Takeover: <a href="#">Add-MailboxPermission</a></li> <li>• Pivot to On-Prem host: <a href="#">SensePost Ruler</a></li> <li>• Exchange Tasks for C2: <a href="#">MWR</a></li> <li>• Send Internal Email</li> </ul>	<ul style="list-style-type: none"> <li>• MailSniper: <a href="#">Search Mailbox for content</a></li> <li>• Search for Content with <a href="#">eDiscovery</a></li> <li>• Exfil email using EWS APIs with <a href="#">PowerShell</a></li> <li>• Download documents and email</li> <li>• Financial/<a href="#">wire</a> fraud</li> </ul>
End Point	<ul style="list-style-type: none"> <li>• Search host for <a href="#">Azure credentials</a>: SharpCloud</li> </ul>		<ul style="list-style-type: none"> <li>• Persistence through Outlook Home Page: <a href="#">SensePost Ruler</a></li> <li>• Persistence through <a href="#">custom Outlook Form</a></li> <li>• Create <a href="#">Hidden Mailbox Rule [tool]</a></li> </ul>		
On-Prem Exchange	<ul style="list-style-type: none"> <li>• <a href="#">Portal Recon</a></li> <li>• <a href="#">Enumerate domain accounts</a> using Skype4B</li> <li>• <a href="#">Enumerate domain accounts</a>: OWA &amp; Exchange</li> <li>• <a href="#">Enumerate domain accounts</a>: OWA: FindPeople</li> <li>• OWA <a href="#">version discovery</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Password Spray</a> using Invoke-PasswordSprayOWA, EWS, <a href="#">Atomizer</a></li> <li>• Bruteforce of Autodiscover: <a href="#">SensePost Ruler</a></li> <li>• PasswordSpray <a href="#">Lync/S4B [LyncSniper]</a></li> </ul>	<ul style="list-style-type: none"> <li>• Exchange <a href="#">MTA</a></li> </ul>	<ul style="list-style-type: none"> <li>• Search Mailboxes with eDiscovery searches (EXO, Teams, SPO, OD4B, Skype4B)</li> <li>• Delegation</li> </ul>	<p>Prepared by @JohnLaTwC, May 2019, v1.04</p> <p>: KILDE <a href="https://pic.twitter.com/6pas4RwHjk">pic.twitter.com/6pas4RwHjk</a></p>

# Sikkerhed

Microsoft Azure

Oversigt ▾ Løsninger **Produkter ▾** Dokumentation Priser Undervisning Marketplace ▾ Part

[Startside](#) / [Produkter](#) / [Azure Sentinel](#)

## Azure Sentinel PRØVEVERSION

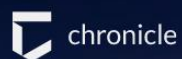
Står vagt ved din side. Intelligent sikkerhedsanalyse til hele virksomheden.

[Start uden omkostninger >](#)

[Produktoversigt](#) [Funktioner](#) [Introduktion](#) [Dokumentation](#) [Kunder](#) [Ofte stillede spørgsmål](#) [Pri](#)

Skab næste generations sikkerhedshandlinger med cloud og kunstig intelligens

Se og stop trusler, før de forårsager skad  
Azure Sentinel får du overblik over hele v  
erfaring inden for Microsoft-sikkerhed. G  
intelligens. Slip for konfiguration og vedl  
imødekomme dine sikkerhedsbehov. mens du reducerer it



**PRODUCTS**

TECHNOLOGY

APPLICATIONS

COMPANY

CAREERS



## Backstory

Extract signals from your security telemetry to find threats instantly.

We live in a digital world, but the current economics of storing and processing enterprise security data have made it not just expensive, but nearly impossible to compete against cybercrime.

But what if the scalability and economics of storing and analyzing your organization's security data were no longer an issue? Chronicle's Backstory was built on the world's biggest data



# Marketplace

## User Management Pack™ 365

AudioCodes



## User Management Pack™ 365

AudioCodes

Create

Save for later

## User Management Pack™ 365

across Skype for

Management Pack

modules called

existing Skype for

management of

operation more

control panel, and

## E-mail Converter

Kalmstrom Enterprises AB



## E-mail Converter

Kalmstrom Enterprises AB

Create

Save for later

*E-mail Converter* converts e-mails to SharePoint list items, so that it is easy for a team to organize and cooperate on them. By default, e-mails in the monitored folders are converted every 5 minutes.

Features:

- Add a ticket URL to every converted e-mail.
- Transfer attachments and inline images from e-mails to SharePoint list items on conversion.
- Map the e-mail fields to the SharePoint list columns.
- Add each e-mail concerning the same case to the first list item, instead of creating one item for each e-mail.
- Merge several list items.
- Generate an Excel report for selected SharePoint columns.

This version will work for 30 days. Then you must register *E-mail Converter* to continue using it.

Please refer to: [http://www.kalmstrom.com/products/E-mail\\_Converter/Subscribe.htm](http://www.kalmstrom.com/products/E-mail_Converter/Subscribe.htm)

Home > ManageEngine O365 Manager Plus

## ManageEngine O365 Manager Plus

ManageEngine



## ManageEngine O365 Manager Plus

ManageEngine

Create

Save for later

Want to deploy programmatically? Get started →

reporting, management, and auditing solution that helps administrators manage their Office 365 environment. The user-friendly interface allows you to manage Exchange Online, Azure Drive for Business all from one place.

figured reports on Office 365. It consolidates data from Exchange Online, eDrive for Business, and other Office 365 components into detailed reports, 365 setup. The reports can be scheduled and exported to PDF, CSV, XLS, or

ment effortless with its sophisticated features. It allows bulk user license management, bulk mailbox management, and more, substantially reducing management tasks.

365 environment to take preemptive actions and avoid dire consequences. A clear report of user activities on all Office 365 components in one place.

es happening in your Office 365 environment. O365 Manager Plus lets you see. These custom alerts save you time by eliminating the need to constantly





« X

### Choose a workspace to add to Azure Sentinel

PREVIEW

Search workspaces

+

Create a new workspace

### Log Analytics workspace

Create new or link existing workspace

Enter workspace name

\* Subscription

Azure Pass - Sponsorship

\* Resource group ⓘ

☒ Create new

☐ Use existing

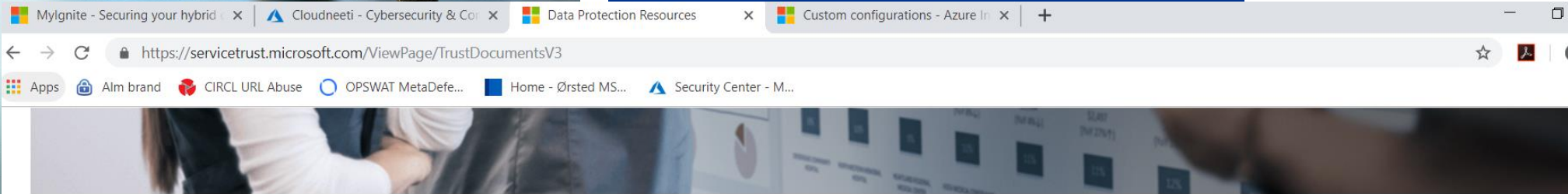
\* Location

Australia Central

\* Pricing tier

Per GB (2018)

# GDPR















## Data Protection Resources

Information about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization.

Select start date  to Select end date  Document Type  Cloud Service  Industries 

Audited Controls Compliance Guides FAQ and White Papers GRC Assessment Reports Microsoft 365 Quarterly Pulse Report Pen Test and Security Assess 

<input type="checkbox"/>	Title	Description	Date ↓	
<input type="checkbox"/>	 Office 365 - Audited Controls NIST 800_53A Rev 4  	This spreadsheet provides information about Microsoft Office 365 controls, implementation details, and audit test procedures for NIST 800-53 standard. Combining this info... <a href="#">Show more</a>	2019-05-08	...
<input type="checkbox"/>	 Office 365 - Audited Controls ISO 27001:2013  	This spreadsheet provides information about Microsoft Office 365 controls, implementation details, and audit test procedures for ISO 27001 standard. Combining this infor... <a href="#">Show more</a>	2019-05-08	...
<input type="checkbox"/>	 Office 365 - Audited Controls ISO 27018:2014  	This spreadsheet provides information about Microsoft Office 365 controls, implementation details, and audit test procedures for ISO 27018 standard. Combining this infor... <a href="#">Show more</a>	2019-05-08	...
<input type="checkbox"/>	 Office 365 GDPR control mapping 5.24.18  	Comprehensive mapping of Microsoft Service Controls to GDPR obligations for Office 365	2019-05-07	...

# GDPR

← → ↻ https://servicetrust.microsoft.com/FrameworkDetailV2/05502b9b-a729-428c-861d-4163419a36ec ☆ | 🔒 | ☰

Apps Alm brand CIRCL URL Abuse OPSWAT MetaDefe... Home - Ørsted MS... Security Center - M...

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
<b>Control ID:</b> 8.4.1 <b>Control Title:</b> Temporary files <b>Supported GDPR Article(s):</b> Article (5)(1)(c) <b>Description:</b> Article (5)(1): Personal data shall be: (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization')	6	Implemented	8/31/2018	Third-party independent auditor	✓
<a href="#">More</a> ∨					
Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
<b>Control ID:</b> 8.4.3 <b>Control Title:</b> Personal data transmission controls <b>Supported GDPR Article(s):</b> Article (5)(1)(f) <b>Description:</b> Article (5)(1): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').	6	Implemented	8/31/2018	Microsoft	✓
<a href="#">More</a> ∨					
Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
<b>Control ID:</b> 8.4.2 <b>Control Title:</b> Return, transfer, or disposal of personal data <b>Supported GDPR Article(s):</b> Article (28)(3)(g), Article (30)(1)(f)	6	Implemented	10/19/2016	Third-party independent auditor	✓



# Reading List

<https://www.blackhillsinfosec.com/red-teaming-microsoft-part-1-active-directory-leaks-via-azure/>  
<https://www.trustedsec.com/2017/08/attacking-self-hosted-skype-businessmicrosoft-lync-installations/>  
**CAS Authentication Timing Attack** <http://h.foofus.net/?p=784>  
<https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52>  
<https://www.slideshare.net/DouglasBienstock/shmoocon-2019-becs-and-beyond-investigating-and-defending-office-365> (youtube)  
<https://www.splunk.com/blog/2018/08/31/i-azure-you-this-will-be-useful.html>  
<https://docs.microsoft.com/en-us/office365/securitycompliance/detailed-properties-in-the-office-365-audit-log>  
<https://www.splunk.com/blog/2018/08/27/the-future-is-cloudy-with-a-chance-of-microsoft-office-365.html>  
<https://www.splunk.com/blog/2017/07/27/splunking-microsoft-cloud-data-part-1.html>  
<https://twitter.com/matthewdunwoody/status/1091786455851167749>  
<https://labs.mwrinfosecurity.com/blog/tasking-office-365-for-cobalt-strike-c2/>  
**DEF CON 25 - Gerald Steere, Sean Metcalf - Hacking the Cloud** (youtube, slides)  
**Business Email Compromise on O365** (<https://www.youtube.com/watch?v=JMFB4TodjkE>)  
<https://blogs.technet.microsoft.com/cloudready/2018/10/14/email-phishing-protection-guide-part-14-prevent-brute-force-and-spray-attacks-in-office-365/>  
**Andrew Johnson / Sacha Faust - Cloud Post Exploitation Techniques @ Infiltrate 2017**, <https://vimeo.com/214855977>  
<https://www.mdsec.co.uk/2017/04/penetration-testing-skype-for-business-exploiting-the-missing-lync/>  
**When Clouds Collide** (slides)  
**MS Security Intelligence Report (Volume 24)**  
**Proofpoint: Threat actors leverage credential dumps, phishing, and legacy email protocols to bypass MFA and breach cloud accounts worldwide**  
**Bypassing inline filtering by security services [O365 user voice]**  
**Hiding in Plain Sight: Using the Office 365 Activities API to Investigate Business Email Compromises by CrowdStrike**  
**Using O365 Activities API for Incident Response**  
**OFFICE365 ACTIVESYNC USERNAME ENUMERATION by GrimHacker**  
**Extracting Sign-in data from O365**  
**eDiscovery Search** <https://docs.microsoft.com/en-us/Exchange/policy-and-compliance/ediscovery/create-searches?view=exchserver-2019>  
<https://adsecurity.org/wp-content/uploads/2019/04/2019-BSidesCharm-YouMovedtoOffice365NowWhat-Metcalf.pdf>  
**2FA MITM Phishing Toolkit** [Evilginx2](#) [Tools](#)  
**ADSECURITY.ORG**

Researchers to follow:

- <https://twitter.com/fullmetacache>
- <https://twitter.com/doughsec/>
- <https://twitter.com/MadeleyJosh>
- <https://twitter.com/matthewdunwoody/>
- <https://twitter.com/mwrlabs>
- <https://twitter.com/meansec>
- <https://twitter.com/domchell>
- <https://twitter.com/vysecurity>
- <https://twitter.com/dafthack>
- <https://twitter.com/PyroTek3>
- [https://twitter.com/\\_staaldraad](https://twitter.com/_staaldraad)
- <https://twitter.com/byt3bl33d3r>



**Thomas Kristmar**  
Senior Manager, IT Advisory

KPMG P/S  
Dampfærgevej 28  
2100 København Ø

T: +45 5087 9861  
E: tkristmar@kpmg.com

**Specialeområder**  
Cybersikkerhedsrådgivning  
Etablering og drift af CERT/SOC  
Incident response  
Krisestyring og -beredskab  
Vurdering af cybertruslen

**Uddannelse og certificeringer**  
Cand.scient.pol.  
CISSP  
CISA  
"Outstanding reviewer" status



[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



This proposal is made by KPMG P/S and is in all respects subject to the negotiation, agreement, and signing of a specific engagement letter or contract as well as client and engagement acceptance in accordance with our internal procedures. KPMG P/S is a member firm of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-a-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.