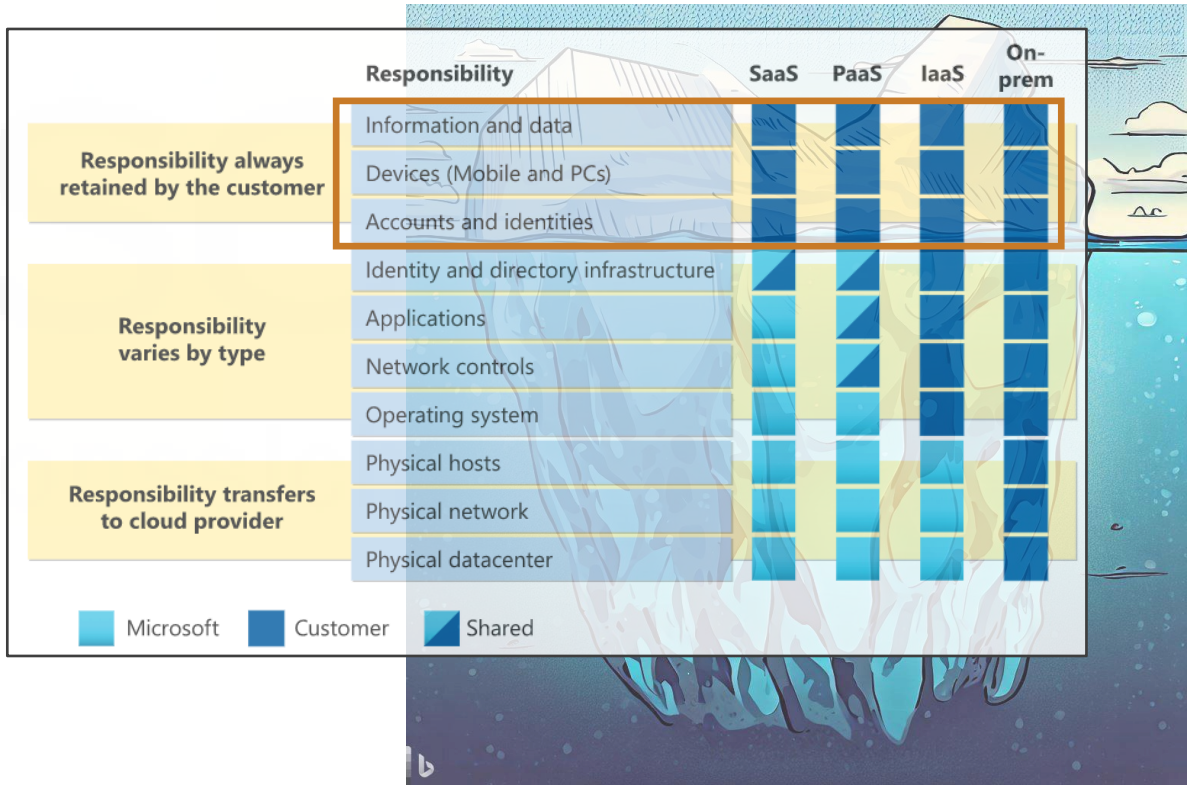
Microsoft 365 – Secure by default?

Basishärtung für Microsoft Entra ID / M365 Tenant

Bild: https://www.bing.com/images/create/ein-microsoft-azure-logo-auf-einer-grc3bcnen-wiese-d/653a3e7614e04fdf9e393076f5cdd488?id=iU2jitwXwq1UQPZ41vLrlA%3d%3d&view=detailv2&idpp=genimg&FORM=GCRIDP&mode=overlay

Cloud - Verantwortlichkeiten

- Auch mit Entra ID behalten Unternehmen die Verantwortung für Ihre Daten
- Sie müssen sich um Härtung und sichere Konfiguration kümmern
- Sie sind für Benutzerverwaltung, Awareness und den Umgang mit Zugangsdaten zuständig



Quelle: https://docs.microsoft.com/de-de/azure/security/fundamentals/shared-responsibility

M365 – Nicht sicher per Default

- Wer einen Microsoft Tenant betreibt, der muss nahezu alle Einstellungen anfassen, um einen sicheren Betrieb zu gewährleisten

- Es gibt einige Self-Assessment-Tools und gute Ressourcen, um sich dem Thema zu nähern – diese decken aber oft nicht alle Teilbereiche und Themen ab

Was muss ich tun für einen sicheren Tenant?

Muss ich wirklich was tun?!

Azure und M365 absichern – das tun?*) **)

Benutzer-Berechtigungen anpassen

- Tenant Erstellung durch Nutzer einschränken
- Subscription Ein- / Ausbringen verhindern
- LinkedIn-Verbindung unterbinden
- Portal-Zugriff einschränken
- Datenspeicherstandort festlegen

Gäste / B2B – Einstellungen anpassen

- Gäste erlaubt / verbieten / einschränken
- Einladung auf Domänen begrenzen
- B2B-Collaboration Defaults anpassen
- B2B-Trust-Settings anpassen
- Gästen das Verlassen des Tenant unterbinden

Gruppen-Konfiguration anpassen

- Security-Gruppen-Erstellung begrenzen
- M365-Gruppen-Erstellung einschränken
- Pre-/Suffix für M365-Gruppen vorgeben
- Dynamic Groups für: Gäste, bestimmte Geräte, Compliance, Usage Locations … einrichten

Geräte-Konfiguration anpassen

- Benutzer dürfen registrieren
- Benutzer dürfen joinen
- Benutzer dürfen BitLocker-Keys auslesen
- Max. Anzahl Geräte pro Nutzer festlegen
- Registrierung ohne MFA unterbinden (+ CA)

Enterprise Applications / App Registrierungen anpassen

- Registrierung durch Nutzer einschränken
- Consent durch Nutzer konfigurieren
- ServicePrincipal Zuweisungen prüfen
- Externe Verwendung von Apps prüfen
- Rollenzuweisungen für die Apps prüfen
- User-Assignments für kritische Apps vorgeben
- Graph-Berechtigungen der Apps prüfen

Zugriff prüfen und anpassen

- Passwort-Einstelllungen anpassen
- Passwort-Reset konfigurieren
- Multifaktorauthentifizierung vorgeben
- Admin-Passwort-Reset absichern
- CA-Regelwerk sicher gestalten
- Admin-Zugriffe absichern (FIDO2)
- Admin-Tier-Modell / Admin-Accounts umsetzen
- Break-Glass-User (FIDO2), Role-Assigned-Groups konfigurieren
- Umgang mit Unmanaged Devices in CA festlegen
- Umgang mit App Limitations über CA erzwingen
- MFA Strengh für CA vorgeben
- WhatIf für CA durchprobieren
- Trusted Locations definieren

Exchange, SharePoint, Teams, … kontrollieren und anpassen

- PowerAutomate deaktiveren / kontrollieren
- Teams Apps aussperren
- Teams Recording, Steuerungsübergabe, etc. deaktivieren, ..
- Gäste in Teams steuern
- Freigaben in SharePoint limitieren
- Sensitivity Labels / App Limitations konfigurieren
- EXO: Send-Domains, Anti-Spam, Anti-Phishing, Auto-Forward, Attachment-Filters konfigurieren

Logging

- Einrichtung Log-Sammlung
- Einrichtung automatisierter Alarme definieren
- Deception / „Canary“ User / E-Mail für Alarm hinterlegen

Aufräumen / „Hygiene“

- Management Groups für Subscriptions einrichten
- Nicht benutzte Gastaccounts entfernen
- Accounts ohne Manager auflösen
- Accounts ohne Usage Location auflösen
- Nicht benötigte App Registrations löschen
- Private registrierte Geräte löschen
- Geräte ohne Besitzer löschen
- Gruppen ohne Mitglieder und Besitzer löschen

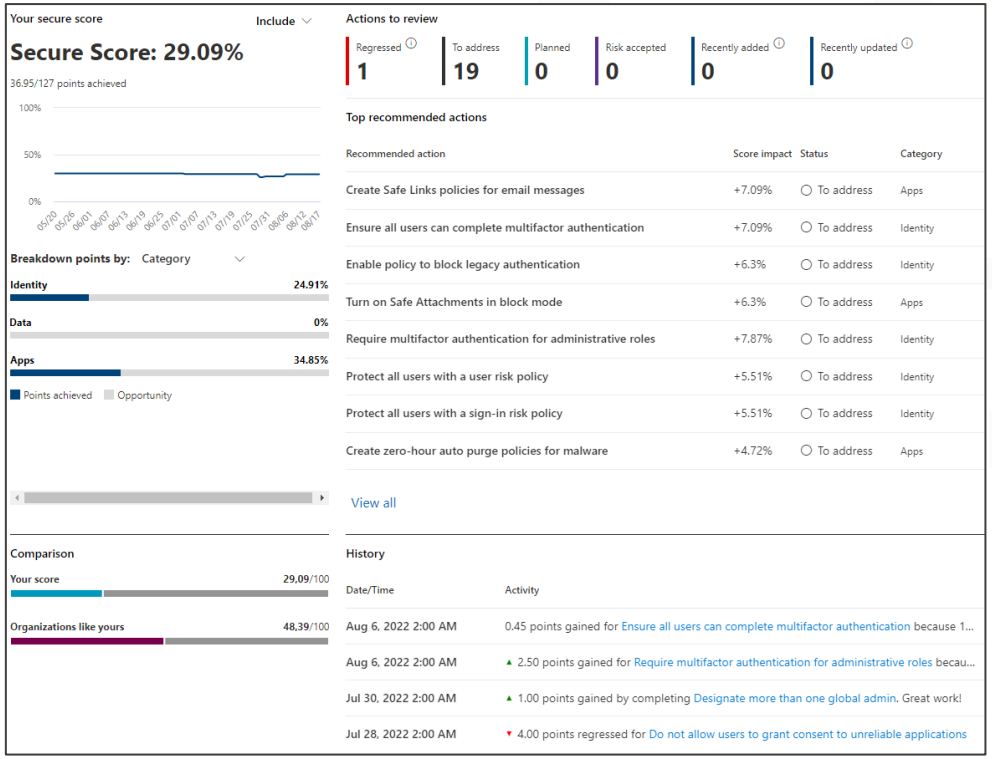
* Die Auflistung erhebt keinen Anspruch auf Vollständigkeit
** Unterstrichene Punkte sind komplexe eigenständige Themengebiete

Ausgewählte Tools für Self-Assessments

Microsoft 365 – Self-Assessments

„Build-in“ & Free

Microsoft Security Score



Fokussiert alle Bereiche im M365-Universum.
Viele MS-Feature-Empfehlungen (Defender *).

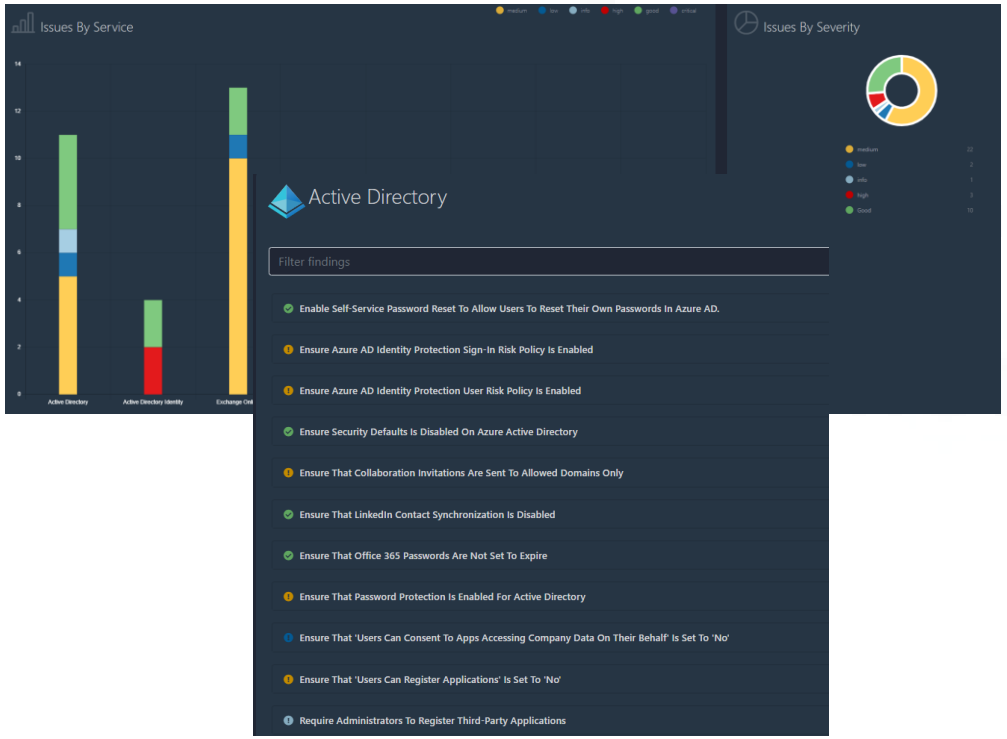
Gewichtete Ergebnisse und „Workflow“ zum Tracking des Bearbeitungsstands.

https://security.microsoft.com/securescore

Gute Grundlage, um die Empfehlungen von Microsoft durchzuarbeiten.

Microsoft 365 – Self-Assessments

Monkey 365



Fokus auf M365-SaaS-Dienste Exchange, Active Directory, Teams und co.

Ergebnisse mit Abschätzung der Kritikalität und ausführlichen Empfehlungen zur Behebung.

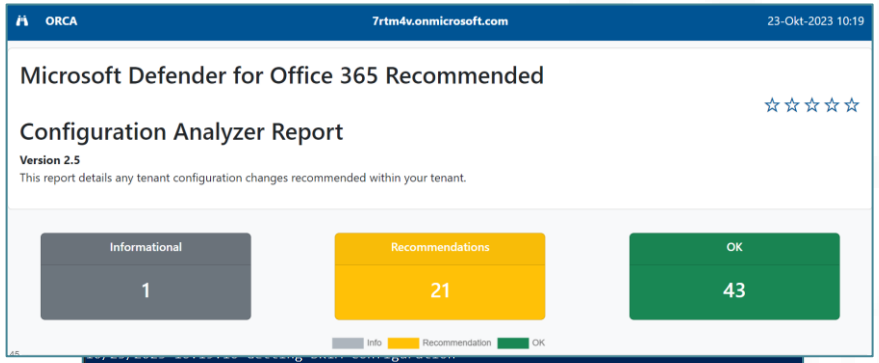
https://github.com/silverhack/monkey365

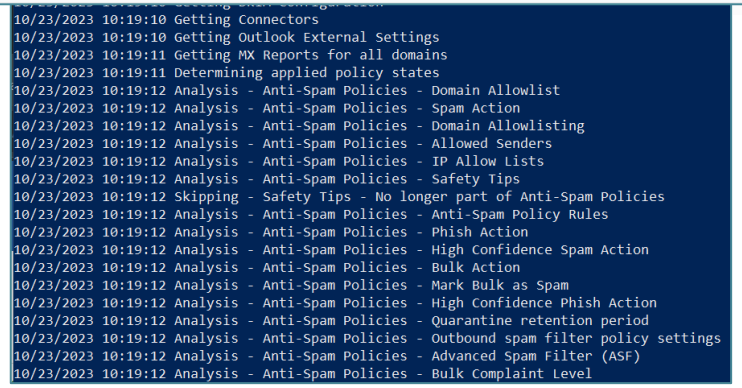
Liefert einige nützliche Empfehlungen zur Härtung einzelner Microsoft-365-Dienste.

Microsoft 365 – Self-Assessments

Einfaches Setup über PowerShell-Galerie

The Office 365 Recommended Configuration Analyzer – ORCA





Fokus auf Exchange Online Security – mit vielen Details.

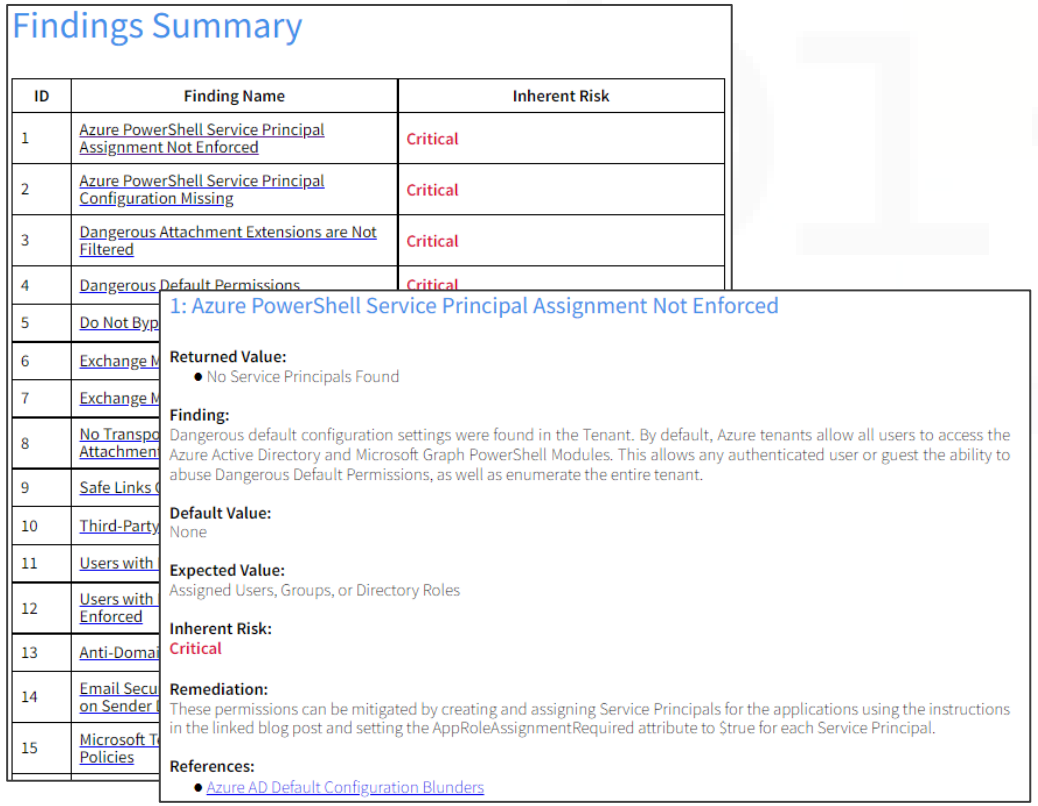
Ergebnisse in HTML-Form mit ausführlichen Empfehlungen und Gesamt-Score.

https://www.powershellgallery.com/packages/ORCA/2.2/Content/ORCA.psm1

Die wahrscheinlich detailliertesten Ergebnisse zur Nutzung der Sicherheitsfeatures rund um Defender in Exchange und co.

Microsoft 365 – Self-Assessments

365 Inspect



Findings Summary

ID	Finding Name	Inherent Risk
1	Azure PowerShell Service Principal Assignment Not Enforced	Critical
2	Azure PowerShell Service Principal Configuration Missing	Critical
3	Dangerous Attachment Extensions are Not Filtered	Critical
4	Dangerous Default Permissions	Critical
5	Do Not Byp	
6	Exchange M	
7	Exchange M	
8	No Transpo Attachmen	
9	Safe Links (	
10	Third-Party	
11	Users with	
12	Users with Enforced	
13	Anti-Domai	
14	Email Secu on Sender	
15	Microsoft T Policies	

1: Azure PowerShell Service Principal Assignment Not Enforced

Returned Value:
- No Service Principals Found

Finding:
Dangerous default configuration settings were found in the Tenant. By default, Azure tenants allow all users to access the Azure Active Directory and Microsoft Graph PowerShell Modules. This allows any authenticated user or guest the ability to abuse Dangerous Default Permissions, as well as enumerate the entire tenant.

Default Value:
None

Expected Value:
Assigned Users, Groups, or Directory Roles

Inherent Risk:
Critical

Remediation:
These permissions can be mitigated by creating and assigning Service Principals for the applications using the instructions in the linked blog post and setting the AppRoleAssignmentRequired attribute to $true for each Service Principal.

References:
- Azure AD Default Configuration Blunders

Rundumblick auf Entra ID und typische Fehler in Exchange und co.

HTML-Bericht mit über 80 Prüfpunkten und Einschätzung der Kritikalität

https://github.com/soteria-security/365Inspect

Detaillierte Ergebnisse zur Nutzung der Sicherheitsfeatures für Defender, Exchange und co.

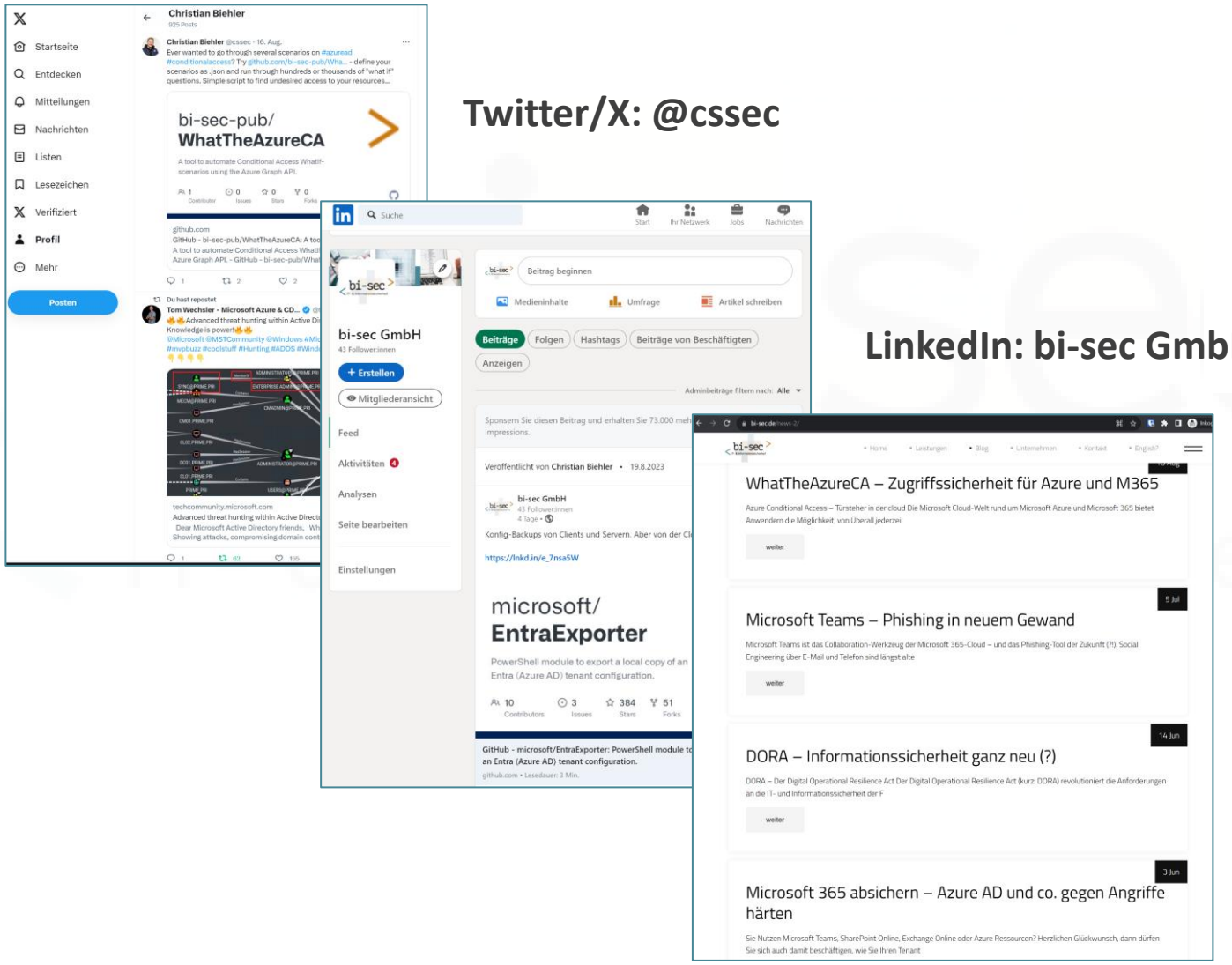
Mehr Infos und Links

Tool- & Linksliste

- Azure-Red-Team – Sammlung von Tools und Commands:
  - https://github.com/rootsecdev/Azure-Red-Team
- TREVORspray – Info-Sammlung & Brutef-Force Tool:
  - https://github.com/blacklanternsecurity/TREVORspray
- ROADtools – Token-Spiel- und Angriffswerkzeug:
  - https://github.com/dirkjanm/ROADtools
- GraphRunner – Automatisiertes Recon- und Angriffswerkzeug:
  - https://github.com/dafthack/GraphRunner
- AADInternals – Must-Know Azure AD Toolkit:
  - https://github.com/Gerenios/AADInternals
- DCToolbox – Azure AD Audit und Angriffs-Toolkit mit super Conditional Access POC:
  - https://github.com/DanielChronlund/DCToolbox

- Scriptlets zur Sammlung einzelner Infos:
  - https://github.com/bi-sec-pub/azure
- WhatTheAzureCA – Automatisiertes Durchprobieren von WhatIf-Regeln:
  - https://github.com/bi-sec-pub/WhatTheAzureCA

Stay in touch ☺



Twitter/X: @cssec

LinkedIn: bi-sec GmbH

Blog: www.bi-sec.de