

Využití komerčních cloudových služeb pro splnění požadavků VKB

Zdeněk Jiříček, Tomáš Mirošník
Microsoft CZ/SK



Mít nebo nemít externího zpracovatele?

Je využití komerčního cloudu
slabinou nebo výhodou
z hlediska požadavků VKB č. 82/2018 Sb.
a případně GDPR?

Standards v oblasti bezpečnostních opatření

Bezpečnostní opatření ve VKB	Mapování na oblasti opatření v ISO 27001:2013 / ISO 27018:2014
§ 3 Systém řízení bezpečnosti informací	A.5 Information security policies
§ 4 Řízení aktiv	A.8 Asset management
§ 5 Řízení rizik	Viz ISAE 3000 report spol. PwC Czech: Zpráva o metodologii posuzování rizik Microsoft Online Services na základě požadavků, vyplývajících ze ZKB a VKB
§ 6 Organizační bezpečnost	A.6 Organization of information security
§ 7 Bezpečnostní role	A.6.1 Internal organization
§ 8 Řízení dodavatelů	A.15 Supplier relationships
§ 9 Bezpečnost lidských zdrojů	A.7 Human resource security
§ 10 Řízení provozu a komunikací	A.12 Operations security, A.13 Communications security
§ 11 Řízení změn	A.14.2 Security in development and support processes
§ 12 Řízení přístupu	A.9 Access control
§ 13 Akvizice, vývoj a údržba	A.14 System acquisition, development and maintenance
§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů	A.16 Information security incident management
§ 15 Řízení kontinuity činností	A.17 Information security aspects of business continuity management
§ 16 Audit kybernetické bezpečnosti	A.12.7 Information systems audit considerations; A.18 Compliance
§ 17 Fyzická bezpečnost	A.11 Physical and environmental security
§ 18 Bezpečnost komunikačních sítí	A.13 Communications security, A.13.1 Network security management
§ 19 Správa a ověřování identit	A.9.2 User access management; A.10.8 Unique use of user IDs (ISO 27018)
§ 20 Řízení přístupových oprávnění	A.9.4 System and application access control
§ 21 Ochrana před škodlivým kódem	A.12.2 Protection from malware
§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	A.12.4 Logging and monitoring
§ 23 Detekce kybernetických bezpečnostních událostí	A.12.2 Protection from malware; A.16.1.6; A.16.1.7 Security Incident Management
§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí	A.16.1 Management of information security incidents and improvements
§ 25 Aplikační bezpečnost	A.14.2 Security in development and support processes
§ 26 Kryptografické prostředky	A.10 Cryptography
§ 27 Zajišťování úrovně dostupnosti informací	A.17.1 Information security continuity
§ 28 Průmyslové, řídicí a obdobné specifické systémy	Neaplikuje se na Microsoft cloud
§ 29 Digitální služby	Aplikuje se v členském státě sídla poskytovatele (Microsoft Ireland)
§ 30 Bezpečnostní politika a bezpečnostní dokumentace	A.5 Information security policies

Microsoft cloud Trust Center: certifikace a audity

<https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings>

Global	Government	Industry	Regional
CIS Benchmark	CJIS	23 NYCRR Part 500	BIR 2012 (Netherlands)
CSA Cloud Control Matrix	CNSSI 1253	AFM + DNB (Netherlands)	C5 (Germany)
CSA-STAR-Attestation	DFARS	APRA (Australia)	CCSL/IRAP (Australia)
CSA-Star-Certification	DoD DISA L2, L3, L5	AMF and ACPR (France)	CS Mark (Gold) (Japan)
CSA STAR Self-Assessment	DoE 10 CFR Part 810	CDSA	Cyber Essentials Plus (UK)
ISO 20000-1:2011	EAR (US Export Administration Regulations)	CFTC 1.31 (US)	Canadian Privacy Laws
ISO 22301	FedRAMP	DPP (UK)	DJCP (China)
ISO 27001	FIPS 140-2	EBA (EU)	EN 301 549 (EU)
ISO 27017	IRS 1075	FACT (UK)	ENS (Spain)
ISO 27018	ITAR	FCA (UK)	ENISA IAF (EU)
ISO 27701	NIST 800-171	FDA CFR Title 21 Part 11	EU-Model-Clauses
ISO-9001	NIST Cybersecurity Framework (CSF)	FERPA	EU-U.S. Privacy Shield
SOC 1	Section 508 VPATS	FFIEC (US)	GB 18030 (China)
SOC 2		FINMA (Switzerland)	GDPR (EU)

VKB – ISMS, řízení rizik, bezp. politika

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§5 Řízení rizik (volba metodiky, posouzení rizik, volba opatření)	Posouzení rizik ochrany aktiv v rámci vymezeného ISMS	PwC Czech – zpráva o posuzování rizik v Microsoft Online Services
	Nástroj pro kontinuální řízení rizik a dokumentaci zavedených opatření	Microsoft Compliance Manager , dokumentace na aka.ms/STP
	Výběr bezpečnostních opatření / zmírnění inherentních rizik	Zapojit opatření na straně Microsoftu dle ISO 27k / NIST
§6 Organizační bezpečnost	Stanovení bezpečnostní politiky pro ISMS	Využít jako základ bezpečnostní politiku online služeb Microsoft
	Zajištění dostupnosti zdrojů pro ISMS	Smluvní závazky v „Podmínkách pro služby online“
	Pravidla pro administrátory a jejich mlčenlivost	Office 365 Lockbox , Azure Lockbox , závazek důvěrnosti, přístup jen v případě potřeby – JIT Access

Co když budu mít cloudové služby v ISMS?

ZKB č. 181/2014 Sb. a jeho VKB č. 82/2018 Sb.

- ZKB §3 – Microsoft standardně v roli poskytovatele dig. služeb (DSP)
- ZKB §4 (4) povinnost zohlednit bezp. opatření při výběru dodavatele
- ZKB §4 (5) smluvní podmínky – viz zhodnocení souladu od kanceláře Pierstone
- ZKB §5: Bezp. opatření viz Podmínky OST, ISO 27k a auditní zprávy SSAE18
- VKB §8: Řízení dodavatelů: rizika – PWC ISAE 3000 report, opatření – OST a ISO
- VKB Příloha č. 2 – hodnocení rizik: použít MS vzorové dokumenty
- VKB Příloha č. 4 – Likvidace dat do úrovně důvěrnosti 3. – „vysoká“ včetně
- VKB Příloha č. 7 – Řízení dodavatelů: viz zhodnocení souladu (Pierstone)

Česká stránka na STP Portálu

www.aka.ms/CZCR (CZ Compliance Resources)

Právní analýza souladu s požadavky ZKB

GDPR DPIA

Compliance Guides

GRC Assessment Reports

Legal Opinions

Document	Description	Report Date
 Soulad smluvní dokumentace online služeb společnosti Microsoft s požadavky na obsah smlouvy uzavírané s významnými dodavateli ve smyslu vyhlášky o kybernetické bezpečnosti	Právní posouzení souladu smluvních podmínek cloudových služeb společnosti Microsoft s požadavky vyhlášky č. 82/2018 Sb. , o kybernetické bezpečnosti na obsah smlouvy uzavírané s významnými dodavateli	2019-05-30
 Zákonné požadavky na smlouvy o poskytování cloud computingových služeb ve smyslu zákona o kybernetické bezpečnosti	Právní posouzení souladu smluvních podmínek cloudových služeb společnosti Microsoft s požadavky §4 novely Zákona o kybernetické bezpečnosti (ZKB) , účinné od 1.8.2017.	2018-06-06

Sdílená odpovědnost Správce - Zpracovatel



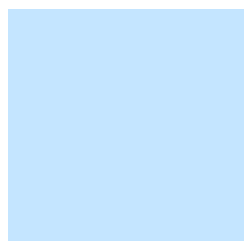
Řízení rizik na straně **Správce**

Kategorizace údajů a stanovení politik ochrany



Sdílené řízení rizik

Správa identit a řízení přístupu k údajům



Řízení rizik na straně **Zpracovatele**

Fyzická bezpečnost a infrastruktura datových center

[Shared responsibility](#) – Microsoft whitepaper

Odpovědnost	On-Prem	IaaS	PaaS	SaaS
Kategorizace údajů a politiky ochrany				
Ochrana koncových zařízení				
Správa identit a řízení přístupu k údajům				
Bezpečnost aplikací				
Síťová infrastruktura v datových centrech				
Virtuální stroje (VM)				
Fyzická bezpečnost				



Zákazník cloudu

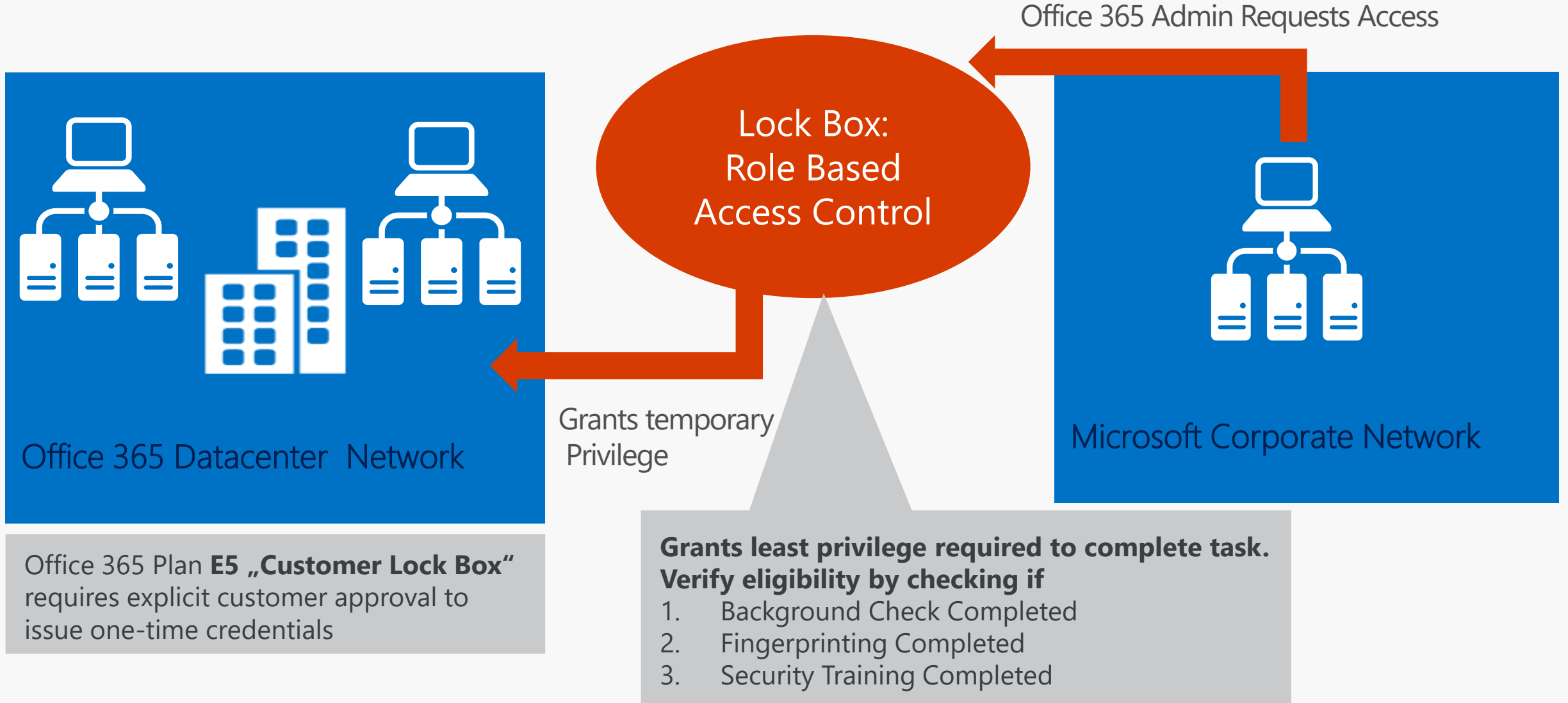


Provozovatel cloudových služeb

VKB – §4 – Řízení aktiv

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§4 Řízení aktiv (1) h) – Pravidla ochrany aktiv (1) i) – Způsoby používání aktiv (1) j) – Způsob likvidace dat	Zařadit aktiva do úrovně důležitosti	Uživatelsky přívětivé „ štítkování “ aktiv (dokumenty, emaily... Office 365 Labels)
	Stanovit přiměřená pravidla pro zabezpečení	Politiky pro automatické nastavení ochrany (dokumenty, emaily) – Azure Information Protection (AIP)
	Pravidla pro bezpečné elektronické sdílení aktiv	Nástroje pro klasifikaci dokumentů, emailů, úložišť, sdílení: Teams / Sharepoint / Outlook. s pomocí AIP
	Způsob likvidace dat v souladu s VKB Příloha č. 4	Azure, Office 365, Dynamics 365: - Úroveň střední: šifrování na úrovni média - Úroveň vysoká: šifrování s uložením klíčů v certifikovaném HSM modulu pod exkluzivní kontrolou zákazníka (KeyVault)

Restrikce přístupu na zákaznická data



VKB – Řízení provozu a komunikací

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§10 Řízení provozu a komunikací, (1) Provozní pravidla a postupy §18 Bezpečnost kom. sítí §21 Ochrana před škodlivým kódem	Sledování kyber událostí	Široké možnosti logování vč. API
	Ochrana před škodlivým kódem	Microsoft Defender ATP, O365 ATP
	Ochrana informací v celém živ. cyklu	Azure Information Protection – AIP , <u>Office 365 Data Loss Prevention (DLP) policies</u> , Intune - mobility
	Zálohování a kontrola použitelnosti	Georedundantní BC/DR, ISO 22301
§22 Zaznamenávání událostí (logy)	Logování bezpečnostních a provozních událostí	<u>Office 365 audit logging</u> a <u>mailbox auditing</u> s možností forenzní analýzy škodlivých aktivit. <u>Office 365 Alert Policies</u>
	Dlouhodobé ukládání logů (12/18 měs.)	<u>Office 365 Management Activity API reference</u> a integrace SIEM
	Synchronizace času min. 1x za 24 hod.	Ano, nejpozději každou hodinu a s přesností na 1 milisekundu.

Řízení provozu a komunikací

Sledování kyber událostí: Security Center - základ

Azure Information Protection - L x Security Center - Overview - Mic x Salvum Insula - Overview - Mic x Microsoft 365 admin center - All x Sensitivity labels - Microsoft 365 x +

https://portal.azure.com/#blade/Microsoft_Azure_Security/SecurityMenuBlade/0

Dashboard | Micros... Microsoft Lifecycle... Stay Modern - Sum... explore.ms CRM Phone Reg My Incentives (Mint) SodeXo MS SALES Azure Info Dynamics Info Lynx Iridias Office365 Manage Office 365... Elevate | LinkedIn MCP Dashboard M365 ES MyKerio Index - ITFileShare Microsoft - Office D... My Role Developm...

Microsoft Azure Search resources, services, and docs (G+)

Home > Security Center - Overview

Security Center - Overview

Showing 2 subscriptions

Subscriptions What's new

Getting things ready for your subscriptions. This may take a few minutes...

Policy & compliance

Secure score

350 OF 515

Review your secure score >

Regulatory compliance

ISO 27001	13 of 20 passed controls
Azure CIS 1.1.0	13 of 17 passed controls
PCI DSS 3.2.1	35 of 41 passed controls

Subscription coverage

1 TOTAL

6 Covered resources

Fully covered: 1, Partially covered: 0, Not covered: 0

Resource security hygiene

Recommendations

8 TOTAL

3 Unhealthy resources

High Severity: 5, Medium Severity: 2, Low Severity: 1

Resource health by severity

1 Compute & apps resources	2 Data & storage resources
1 Networking resources	2 Identity & access resources

Threat protection

Security alerts by severity

No security alerts

0 Attacked resources

Security alerts over time

No security alerts

0 High severity, 0 Low severity

Make alert data available to your SIEM

You can make Security Center alerts available to a SIEM connector

Set up SIEM connector >

Review and improve your secure score

Review and resolve security vulnerabilities to improve your secure score and secure your workload

Learn more >

New - Advanced threat protection for Storage accounts

Security Center can now protect your Storage accounts by detecting unusual and potentially harmful attempts to access or exploit Storage accounts.

Learn more >

Create a resource

Home Dashboard All services FAVORITES Azure Active Directory Monitor Cost Management + Billing Security Center Intune App Protection Advisor Intune Azure AD Identity Protection Azure Information Protection... Enterprise applications Key vaults Managed Desktop Service Health Management groups Application security groups Azure Sentinel Identity Governance Conditional Access Azure AD Domain Services Groups Application Insights Data Box Edge / Data Box ... Policy Free services Alerts Devices

Policy & Compliance: Coverage, Secure score, Security policy, Regulatory compliance

Resource Security Hygiene: Recommendations, Compute & apps, Networking, IoT Hubs & resources, Data & storage, Identity & access, Security solutions

Advanced Cloud Defense: Adaptive application controls, Just in time VM access, Adaptive network hardening, File Integrity Monitoring

Threat Protection: Security alerts, Security alerts map (Preview)

Automation & Orchestration: Playbooks (Preview)

Řízení provozu a komunikací

Pokročilé sledování kyber událostí: Azure Sentinel

The image displays the Microsoft Azure portal interface, specifically the Azure Sentinel workspace and the Logic Apps Designer.

Azure Sentinel Overview (Left Panel):

- General:** Overview, Logs, News & guides.
- Threat management:** Incidents, Workbooks, Hunting, Notebooks.
- Configuration:** Data connectors, Analytics, Playbooks, Community, Workspace settings.

Events and alerts over time: A chart showing 54 events and 54 alerts over the last 24 hours.

Potential malicious events: A map showing the geographical distribution of events.

Logic Apps Designer (Right Panel):

The Logic Apps Designer shows a workflow for handling Azure Security Center alerts:

- When a response to an Azure Security Center alert is triggered** (Trigger)
- Create incident in Service Now(Preview)** (Action)
- Post message to SOC channel(Preview)** (Action)
- Send approval email** (Action)
- Condition:**
 - And** (Logic)
 - Selected...** (Connector)
 - is equal to** (Comparison)
 - Block user and IP** (Action)
- If true:**
 - Block user in Azure AD** (Action)
 - BlockIP Paloalto** (Action)
- If false:**
 - Close incident in Service Now(Preview)** (Action)

The workflow is designed to automatically respond to security alerts by creating incidents, notifying the SOC, and blocking malicious users and IP addresses.

Rízení
Ochrana
Microsoft

Microsoft Defender Security Center

Machines > mariepracovni

Domain: AAD joined
OS: Windows 10 x64
Version: 1903
Build: 18362
Risk level: No known risks
Exposure level: Medium
Health state: Active

Active alerts: 0
Active incidents: 0
Azure ATP alerts: Machine not found at Azure ATP
First seen: Apr 28, 2019, 1:22:52 PM
Last seen: Sep 25, 2019, 10:03:49 AM
IP addresses: See IP addresses info

Manage Tags Collect investigation package Run antivirus scan Restrict app execution Isolate machine Consult a threat expert Action center

Active alerts 180 days

Risk level: No known risks
We don't see new malicious activity on this machine

Logged on users 30 days
1 logged on user
Most frequent: marie
Least frequent: marie
See all users

Alerts Timeline Security recommendations Software inventory Discovered vulnerabilities Missing KBs

Event time	Event	Additional information	User	Entities
Sep 25, 2019, 10:03:49.522 AM	EXCELEXE renamed MM přehled práce září 2019.xls		mariemirošniková	explorer.exe > EXCELEXE > MM
Sep 25, 2019, 10:03:44.289 AM	EXCELEXE renamed MM přehled práce září 2019.xls		mariemirošniková	explorer.exe > EXCELEXE > MM
Sep 25, 2019, 10:03:33.867 AM	SearchIndexer.exe created process SearchProtocolHost.exe		system	services.exe > SearchIndexer.exe
Sep 25, 2019, 10:03:32.886 AM	EXCELEXE renamed MM přehled práce září 2019.xls		mariemirošniková	explorer.exe > EXCELEXE > MM
Sep 25, 2019, 10:03:32.880 AM	EXCELEXE modified MM přehled práce září 2019.xls		mariemirošniková	explorer.exe > EXCELEXE > MM
Sep 25, 2019, 10:03:02.234 AM	OfficeClickToRun.exe successfully established connection with 104.45.3.37:443 (o...		system	services.exe > OfficeClickToRun.exe
Sep 25, 2019, 10:02:59.625 AM	EXCELEXE successfully established connection with 104.47.8.31:443 (eur03.oscs.p...		mariemirošniková	explorer.exe > EXCELEXE > 104.
Sep 25, 2019, 10:02:59.412 AM	iexplore.exe successfully established connection with 172.217.23.238:443 (www.y...		mariemirošniková	iexplore.exe > iexplore.exe > 172.
Sep 25, 2019, 10:02:57.661 AM	EXCELEXE successfully established connection with 40.101.137.2:443 (outlook.off...		mariemirošniková	explorer.exe > EXCELEXE > 40.1
Sep 25, 2019, 10:02:57.199 AM	EXCELEXE successfully established connection with 52.109.32.32:443 (ocws.office...		mariemirošniková	explorer.exe > EXCELEXE > 52.1
Sep 25, 2019, 10:02:57.166 AM	EXCELEXE successfully established connection with 13.107.18.11:443 (substrate.o...		mariemirošniková	explorer.exe > EXCELEXE > 13.1
Sep 25, 2019, 10:02:56.750 AM	smartscreen.exe successfully established connection with 40.114.224.200:443 (eu...		mariemirošniková	svchost.exe > smartscreen.exe >
Sep 25, 2019, 10:02:56.715 AM	EXCELEXE successfully established connection with 52.109.88.5:443 (odc.officeap...		mariemirošniková	explorer.exe > EXCELEXE > 52.1
Sep 25, 2019, 10:02:56.484 AM	excel.exe created Shell link (shortcut) file MM přehled práce září 2019.LNK		mariemirošniková	explorer.exe > excel.exe > MM p
Sep 25, 2019, 10:02:56.445 AM	excel.exe created Shell link (shortcut) file MM přehled práce září 2019.LNK		mariemirošniková	explorer.exe > excel.exe > MM p
Sep 25, 2019, 10:02:55.390 AM	svchost.exe successfully established connection with 40.90.137.125:443 (login.live...		system	services.exe > svchost.exe > 40.9
Sep 25, 2019, 10:02:55.259 AM	vsserv.exe successfully established connection with 52.18.188.24:443		system	services.exe > vsserv.exe > 52.18
Sep 25, 2019, 10:02:55.185 AM	explorer.exe created Shell link (shortcut) file MM přehled práce září 2019.lnk		mariemirošniková	userinit.exe > explorer.exe > MM
Sep 25, 2019, 10:02:40.983 AM	WINWORD.EXE created file ~\$RD0531.docx		mariemirošniková	explorer.exe > WINWORD.EXE >
Sep 25, 2019, 10:02:40.980 AM	WINWORD.EXE renamed ~WRD0531.docx		mariemirošniková	explorer.exe > WINWORD.EXE >
Sep 25, 2019, 10:02:40.959 AM	WINWORD.EXE created file ~\$RD0527.docx		mariemirošniková	explorer.exe > WINWORD.EXE >

Excel Entities Graph

Process name: EXCELEXE
Execution time: Sep 25, 2019, 10:02:55.060 AM
Path: c:\program files (x86)\microsoft office\root\office16\excel.exe
Integrity level: Medium
Access privileges (UAC): Restricted
Process ID: 1188
Command line: "EXCELEXE" "C:\Users\MarieMirošniková\Desktop\MM přehled práce září 2019.xls"
SHA1: 6490a5897c31e43393c0fba365a08611340867c
SHA256: 1c99988914e689a06f2f14047be501add0558731242806
Signer: Microsoft Corporation
Issuer: Microsoft Code Signing PCA 2010

MM přehled práce září 2019.xls
File name: MM přehled práce září 2019.xls
Folder path: C:\Users\MarieMirošniková\Desktop
SHA1: 87ce64ca7239fec8ed65b966f9ae95e1269114fb
SHA256: ecc2bfaf3d113966e6430c5fd74af6f0ebcd3f5c9e397

Řízení provozu a komunikací

Office 365 ATP

The screenshot displays the Office 365 Security & Compliance center interface. The left sidebar shows the navigation menu with categories like Microsoft 365 security, Policies, Alerts, Reports, Secure score, Hunting, Classification, and more resources. The main content area is titled "Safe links" and shows a summary of the policy configuration. A yellow banner at the top states: "Reports for this feature just got better. Check out the new [report](#) in the Security and Compliance Center for an enhanced reporting experience."

The "Safe links" page includes a section for "Policies that apply to the entire organization" with a table showing the "Default" policy. Below this, there is a section for "Policies that apply to specific recipients" with a table showing the "Ochrana mě" policy. A modal window titled "Ochrana mě" is open, showing the configuration for this policy. The modal includes a "general" tab and a "settings" tab. The "settings" tab is active, showing options for "Select the action for unknown potentially malicious URLs in messages" (On), "Apply real-time URL scanning for suspicious links and links that point to files" (checked), "Wait for URL scanning to complete before delivering the message" (checked), "Apply safe links to email messages sent within the organization" (checked), "Do not track when users click safe links" (unchecked), and "Do not let users click through safe links to original URL" (checked). There is also a section for "Do not rewrite the following URLs:" with a text input field and a plus button. The modal has "Save" and "Cancel" buttons at the bottom.

The "Ochrana mě" policy summary on the right shows the following settings:

- Settings:
 - Do not track when users click safe links: Disabled
 - Do not let users click through safe links to original URL: Enabled
- Applied to:
 - Office 2016 on Windows: Enabled

The "Ochrana mě" policy details on the right show the following configuration:

- Enabled
- Relative priority: 0
- Applied to:
 - If the message:
 - Is sent to a member of group "tomas@miroslav.cz" or "jakub@miroslav.cz" or "laura@miroslav.cz" or "marie@miroslav.cz" or "tom@miroslav.cz"
 - recipient's address domain portion belongs to any of these domains: "miroslav.cz" or "miroslavova.cz"
 - Take the following actions:
 - Apply safe links policy "Ochrana mě".
 - Except if the message:
- Summary
 - Safe attachments URL Scanning: Enabled
 - Wait for URL scanning to complete before delivering the message: Enabled
 - Apply safe links to email messages sent within the organization: Enabled
 - Do not track when users click safe links: Disabled
 - Do not let users click through safe links to original URL: Enabled

Řízení provozu a komunikací

Ochrana informací v celém životním cyklu

AIP – Azure Information Protection

The screenshot shows the Azure Information Protection - Labels page. The left sidebar contains the Azure portal navigation menu with options like 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES', and various Azure services. The main content area is titled 'Azure Information Protection - Labels' and includes a search bar, a 'Columns' button, and a table of labels. The table has columns for 'LABEL DISPLAY NAME', 'POLICY', 'MARKING', and 'PROTECTION'. The labels listed are 'Rodna cisla', 'Secured by Tom', and 'Protection templates'. There is also a '+ Add a new label' link.

LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Rodna cisla			...
Secured by Tom			...
Protection templates			...

Řízení provozu a komunikací

Ochrana informací v celém životním cyklu

DLP M 365

The screenshot displays the Microsoft 365 security center interface. The left sidebar shows the navigation menu with options: Home, Alerts, Reports, Secure score, Hunting, Classification, Sensitivity labels, Retention labels, Sensitive info types (selected), and Label analytics. The main content area is titled 'Sensitive info types' and includes a description: 'The sensitive info types here are available to use in your security and compliance policies. These include a large collection of types we provide, spanning regions around the globe, as well as any custom types you have created. Manage sensitive info types in the Office 365 Security & Compliance Center'. Below this is a table listing various sensitive info types.

Name	Type	Publisher
Australia Passport Number	Entity	Microsoft Corporation
Australia Tax File Number	Entity	Microsoft Corporation
Azure DocumentDB Auth Key	Entity	Microsoft Corporation
Azure IaaS Database Connection String and Azure SQL Connec...	Entity	Microsoft Corporation
Azure IoT Connection String	Entity	Microsoft Corporation
Azure Publish Setting Password	Entity	Microsoft Corporation
Azure Redis Cache Connection String	Entity	Microsoft Corporation
Azure SAS	Entity	Microsoft Corporation
Azure Service Bus Connection String	Entity	Microsoft Corporation
Azure Storage Account Key	Entity	Microsoft Corporation
Azure Storage Account Key (Generic)	Entity	Microsoft Corporation
Belgium National Number	Entity	Microsoft Corporation
Brazil CPF Number	Entity	Microsoft Corporation
Brazil Legal Entity Number (CNPJ)	Entity	Microsoft Corporation
Brazil National ID Card (RG)	Entity	Microsoft Corporation
Canada Bank Account Number	Entity	Microsoft Corporation
Canada Driver's License Number	Entity	Microsoft Corporation
Canada Health Service Number	Entity	Microsoft Corporation
Canada Passport Number	Entity	Microsoft Corporation
Canada Personal Health Identification Number (PHIN)	Entity	Microsoft Corporation
Canada Social Insurance Number	Entity	Microsoft Corporation
Chile Identity Card Number	Entity	Microsoft Corporation
China Resident Identity Card (PRC) Number	Entity	Microsoft Corporation
Credit Card Number	Entity	Microsoft Corporation
Croatia Identity Card Number	Entity	Microsoft Corporation
Croatia Personal Identification (OIB) Number	Entity	Microsoft Corporation
☒ Czech Personal Identity Number	Entity	Microsoft Corporation
Denmark Personal Identification Number	Entity	Microsoft Corporation

A detailed view of the 'Czech Personal Identity Number' is shown on the right. It includes the following details:

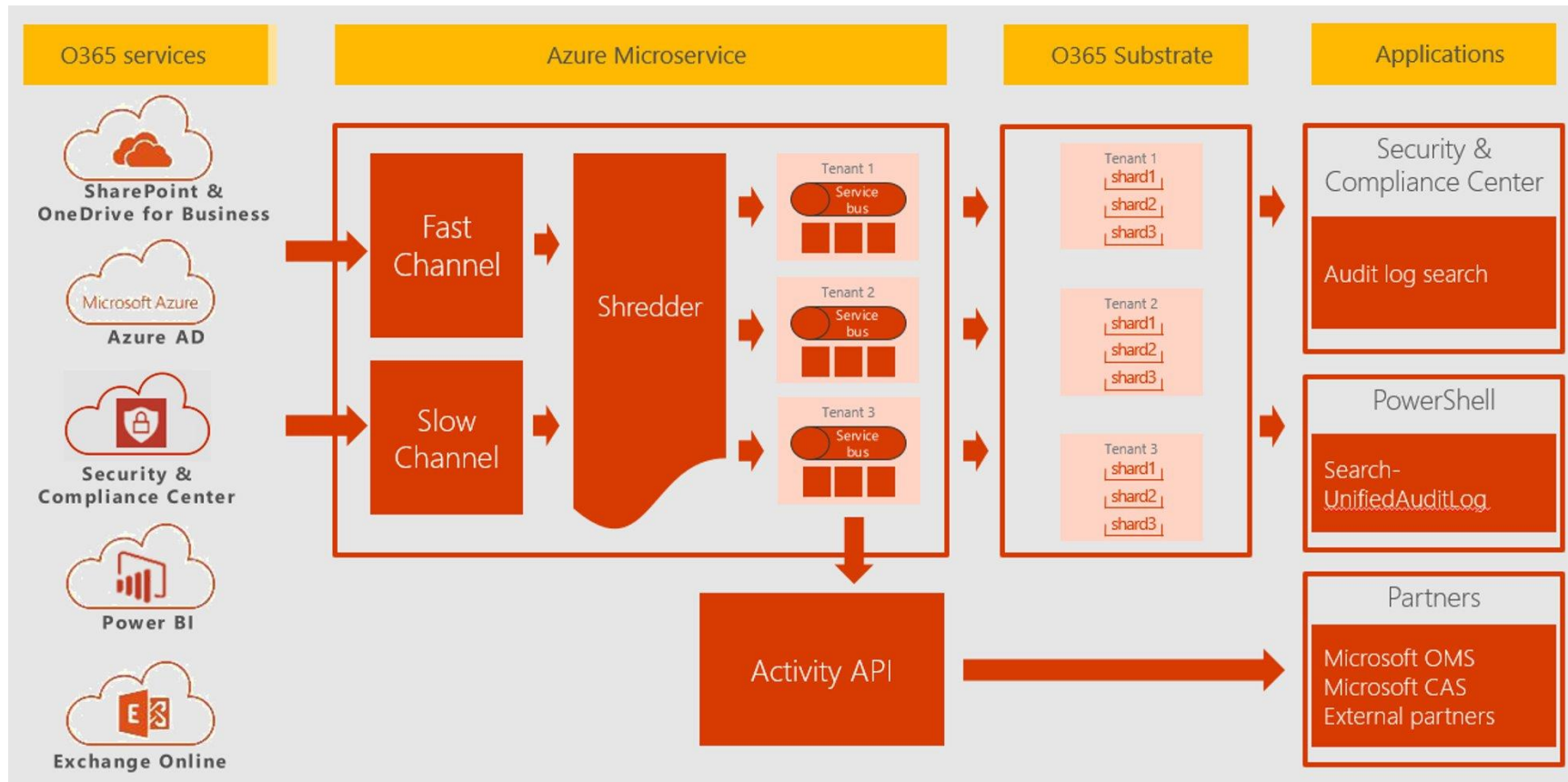
- Description:** Detects Czech Personal Identity Numbers
- Type:** Entity
- Publisher:** Microsoft Corporation

The interface also shows a 'Close' button at the bottom right of the details panel.

Řízení provozu a komunikací

Dlouhodobé ukládání logů

Office 365 Management Activity API reference a integrace SIEM



Salvum Insula - Overview - Micr...Microsoft 365 admin center - All...Alert policies - Security & Compl...

Dashboard | Micros...Microsoft Lifecycle...Stay Modern - Sum...explore.msCRMPhone RegMy Incentives (Mint)SodeXoMS SALES Azure InfoDynamics InfoLynxIndiasOffice365Manage Office 365...Elevate | LinkedinMCP DashboardM365 ESMyKerioIndex - ITFileShareMicrosoft - Office D...My Role Developm...

Office 365 Security & Compliance

Home

Alerts

Dashboard

View alerts

Alert policies

Manage advanced alerts

Permissions

Classification

Data loss prevention

Records management

Data governance

Supervision

Threat management

Mail flow

Data privacy

Search

eDiscovery

Data Investigations

Reports

Service assurance

Home > Alert policies

Alert policies

Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications. [Learn more about alert policies](#)

+ New alert policy

Search

Filter

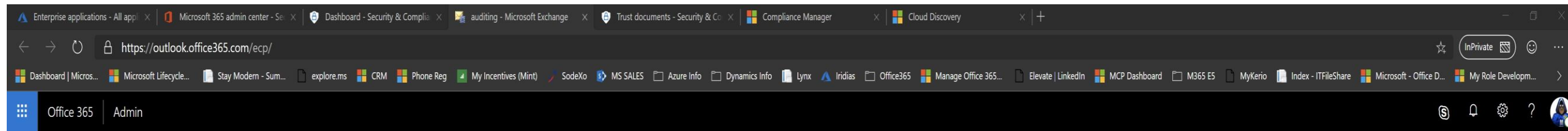
☐	Name	Severity	Type	Category	Date modified	Status
☐	MS-500 policy	Medium	Custom	Data governance	9/12/19 11:24 PM	...
☐	Suspicious email sending patterns detected	Medium	System	Threat management	-	...
☐	Elevation of Exchange admin privilege	Low	System	Permissions	-	...
☐	Email messages containing malware removed after delivery	Informational	System	Threat management	-	...
☐	Malware campaign detected and blocked	Low	System	Threat management	-	...
☐	Email reported by user as malware or phish	Informational	System	Threat management	-	...
☐	Unusual volume of file deletion	Medium	System	Data governance	-	...
☐	Unusual external user file activity	High	System	Data governance	-	...
☐	eDiscovery search started or exported	Medium	System	Threat management	-	...
☐	Malware campaign detected in SharePoint and OneDrive	High	System	Threat management	-	...
☐	Creation of forwarding/redirect rule	Low	System	Threat management	-	...
☐	User restricted from sending email	High	System	Threat management	-	...
☐	Unusual increase in email reported as phish	High	System	Threat management	-	...
☐	Unusual volume of external file sharing	Medium	System	Data governance	-	...
☐	Email messages containing phish URLs removed after delivery	Informational	System	Threat management	-	...
☐	Messages have been delayed	High	System	Mail flow	-	...
☐	Tenant restricted from sending email	High	System	Threat management	-	...
☐	Malware campaign detected after delivery	High	System	Threat management	-	...
☐	A potentially malicious URL click was detected	High	System	Threat management	-	...

19 item(s) loaded.

Řízení provozu a komunikací

Logování bezpečnostních a provozních událostí

Office 365 audit logging a mailbox auditing s možností forenzní analýzy šlodivých aktivit.



Exchange admin center

dashboard in-place eDiscovery & hold **auditing** data loss prevention retention policies retention tags journal rules

recipients

permissions

compliance management

organization

protection

advanced threats

mail flow

mobile

public folders

unified messaging

Use these reports and audit logs to view information about mailboxes accessed by someone other than the owner and changes made by administrators to your Exchange organization. You can also export search results to a file that is sent to you or other users. [Learn more](#)

Run a non-owner mailbox access report...

Search mailbox audit logs for mailboxes that have been opened by someone other than the owner. You have to enable mailbox audit logging for each mailbox that you want to run a non-owner mailbox access report for. If mailbox audit logging isn't enabled for a mailbox, you won't get any results for it when you run this report. [Learn more](#)

Run an administrator role group report...

Search the admin audit log for changes made to role groups, which are used to assign administrative permissions to users. [Learn more](#)

Run an In-Place eDiscovery & Hold report...

Search the admin audit log for changes made to In-Place eDiscovery searches and In-Place Holds. [Learn more](#)

Run a per-mailbox Litigation Hold report...

Search the admin audit log to determine if a Litigation Hold was enabled or disabled for a user's mailbox. [Learn more](#)

Export mailbox audit logs...

Export entries from mailbox audit logs about non-owner access to user mailboxes. Audit log entries are saved to an XML file that is attached to a message and sent to the specified recipients within 24 hours. [Learn more](#)

Run the admin audit log report...

View entries from the admin audit log about configuration changes made by administrators in your organization. [Learn more](#)

Export the admin audit log...

Export entries from the admin audit log for any configuration change made to your organization. Audit log entries are saved to an XML file that is attached to a message and sent to the specified recipients within 24 hours. [Learn more](#)

Run the external admin audit log report...

View entries from the admin audit log about configuration changes made to your Exchange Online services by Microsoft or by a delegated admin. [Learn more](#)

VKB – Řízení přístupu

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§12 Řízení přístupu §19 Správa a ověřování identit §20 Řízení přístupových oprávnění §22 Zaznamenávání událostí uživatelů a administrátorů	Vícefaktorová autentizace, příp. politiky pro silná hesla	<u>Identity and device access policies, MFA, strong password policies</u>
	Přidělování privilegovaných oprávnění jen na nezbytně nutnou úroveň/dobu, pravidelný přezkum přidělených oprávnění	<u>Azure AD Privileged Identity Management, Privileged Access Mgmt in O365</u>
	Kontrola cizích přístupů do mailboxu	Audit <u>non-owner mailbox access</u>
	Kontroly neúspěšné manipulace s účty nebo oprávněními	<u>Office 365 Alert Policies, Data Loss Prevention reports and Microsoft Cloud App Security</u>
	Řízení oprávnění na úrovni aktiva	Azure Information Protection – AIP

Řízení přístupu

Vícefaktorová autentizace, příp. politiky pro silná hesla, MFA

Salvum Insula - Identity Secure Score

Multi-factor authentication | Cloud Discovery

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/IdentitySecureScore

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Salvum Insula - Identity Secure Score

Salvum Insula - Identity Secure Score

Learn more | Troubleshooting and support | Got feedback?

Search (Ctrl+/)

Overview

Getting started

Manage

- Users
- Groups
- Organizational relationships
- Roles and administrators
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Notifications settings

Security

- Overview (Preview)
- Identity Secure Score
- Conditional Access
- MFA
- Risky users (Users flagged for ri...
- Risky sign-ins (Preview)
- Risk detections (Risk events)

Monitor and improve your identity security score. To view your overall score, go to Microsoft Secure Score.

Last updated 9/25/2019, 2:00:00 AM

Your Identity Secure Score

186/223

Your score is above the average for your company's industry.

Salvum Insula

Consumer industry company average

Typical 6-99 person company

Change industry

Improvement actions

Download Columns

Search to filter items...

NAME	SCORE IMPACT	USER IMPACT	IMPLEMENTATION COST
Require MFA for Azure AD privileged roles	0	Low	Low
Require MFA for all users	11	Moderate	Moderate
Do not allow users to grant consent to unmanaged applications	10	Moderate	Low
Designate fewer than 5 global admins	0	Low	Low
Designate more than one global admin	5	Low	Low
Use limited administrative roles	0	Low	Low
Do not expire passwords	0	Moderate	Low
Delete/block accounts not used in last 30 days	1	Moderate	Low
Enable policy to block legacy authentication	0	Moderate	Moderate
Turn on sign-in risk policy	0	Moderate	Moderate
Turn on user risk policy	0	Moderate	Moderate
Register all users for multi-factor authentication	0	High	High
Enable self-service password reset	0	Moderate	Moderate
Enable Password Hash Sync if hybrid	10	Low	Low

Show score for last

7 days 30 days 60 days 90 days

Řízení přístupu

Přidělování privilegovaných oprávnění jen na nezbytně nutnou úroveň/dobu, pravidelný přezkum přidělených oprávnění

Azure AD Privileged Identity Management , Privileged Access Management in Office 365

The screenshot displays the Microsoft 365 admin center interface. The left sidebar shows the navigation menu with options like Home, Users, Devices, Groups, Resources, Billing, Support, Settings, Services & add-ins, Security & privacy, Organization profile, Partner relationships, Setup, Reports, Usage, Security & compliance, Health, Admin centers, Security, Compliance, Device Management, Azure Active Directory, Exchange, SharePoint, Teams, and All admin centers. The main content area is divided into two sections: 'Security & privacy' and 'Permissions'.

Security & privacy settings:

- Password policy:** Set the password policy for all users in your organization. Days before passwords expire: Never. Days before a user is notified about expiration: Never.
- Privacy profile:** Set the privacy statement of your organization. Organization privacy statement: not set. Organization privacy contact: tomas@miroslav.cz.
- Customer Lockbox:** Set requirements for data access. Require approval for all data access requests: On.
- Sharing:** Control access for people outside your organization. Let users add new guests to the organization: On.
- Privileged Access:** Set scoped access for privilege tasks and data access within your organization. Approvals for privilege tasks: On. Manage access policies and requests.
- Let your people reset their own passwords:** You can turn it on in the Azure AD admin center. After you turn on self-service password reset, you need to send users to the following website so they can set up their alternate phone number or email address. Don't lose access to your account.

Permissions page:

Manage who in your organization has access to the Microsoft 365 security center to view content and perform tasks. You can also assign Microsoft 365 permissions in Azure Active Directory.

Admin role	Users	Description
Yleinen järjestelmävalvoja	1	Voit hallita kaikkia Azure AD- ja Microsoft-palveluiden ominaisuuksia, jotka käytät Azure AD- käyttäjätietojia.
Yhteensopivuuksien järjestelmävalvoja	0	Luo ja hallitsee yhteensopivuuksia.
Yhteensopivuuksien järjestelmävalvoja	1	Voit lukea ja hallita yhteensopivuuksienkäytöstä ja -raportista Azure AD:ää ja Office 365:ää.
Suojausoperaattori	0	Luo ja hallitsee suojatapahtumia.
Suojatietojen lukija	0	Voit lukea suojatietoja ja -raportista Azure AD:ää ja Office 365:ää.
Suojauksen järjestelmävalvoja	1	Suojauksen järjestelmävalvoja voi lukea ja hallita suojatapahtumia ja -raportista.

Řízení přístupu

Kontroly neúspěšné manipulace s účty nebo oprávněními

Office 365 Alert Policies, Data Loss Prevention reports and Microsoft Cloud App Security

The screenshot displays the Microsoft Cloud App Security console. The left sidebar contains navigation options: Dashboard, Discover, Investigate, Control, and Alerts. The main area is titled 'Edit anomaly detection policy' and shows a built-in policy named 'Suspicious inbox manipulation rule'. The policy description states: 'A suspicious inbox rule was set on a user's inbox. This may indicate that the user account is compromised, and that the mailbox is being used to distribute spam and malware in your organization.' The policy is categorized under 'Threat detection' and has a scope of 'All users and groups'. The 'Alerts' section shows settings for sending alerts via email, text message, or Flow. The 'Governance' section shows options to notify, suspend, or CC additional users. The policy was modified a few seconds ago.

Cloud App Security

Edit anomaly detection policy

This is a built-in anomaly detection policy. Learn more about it | Send us feedback

Policy name *

Suspicious inbox manipulation rule

Description

A suspicious inbox rule was set on a user's inbox. This may indicate that the user account is compromised, and that the mailbox is being used to distribute spam and malware in your organization.

Category *

Threat detection

Scope

All users and groups

Alerts

Use your organization's default settings

☐ Send alert as email

☐ Send alert as text message

Save these alert settings as the default for your organization

☐ Send alerts to Flow

Create a playbook in Flow

Governance

All apps

☐ Notify user

CC additional users

☐ Suspend user

For Azure Active Directory users

Office 365

Suspend user

Suspend user

The rule was modified a few seconds ago

After the policy is created, it takes a week to learn your baseline before this policy generates alerts. We secure your data as described in our privacy statement.

Update Cancel

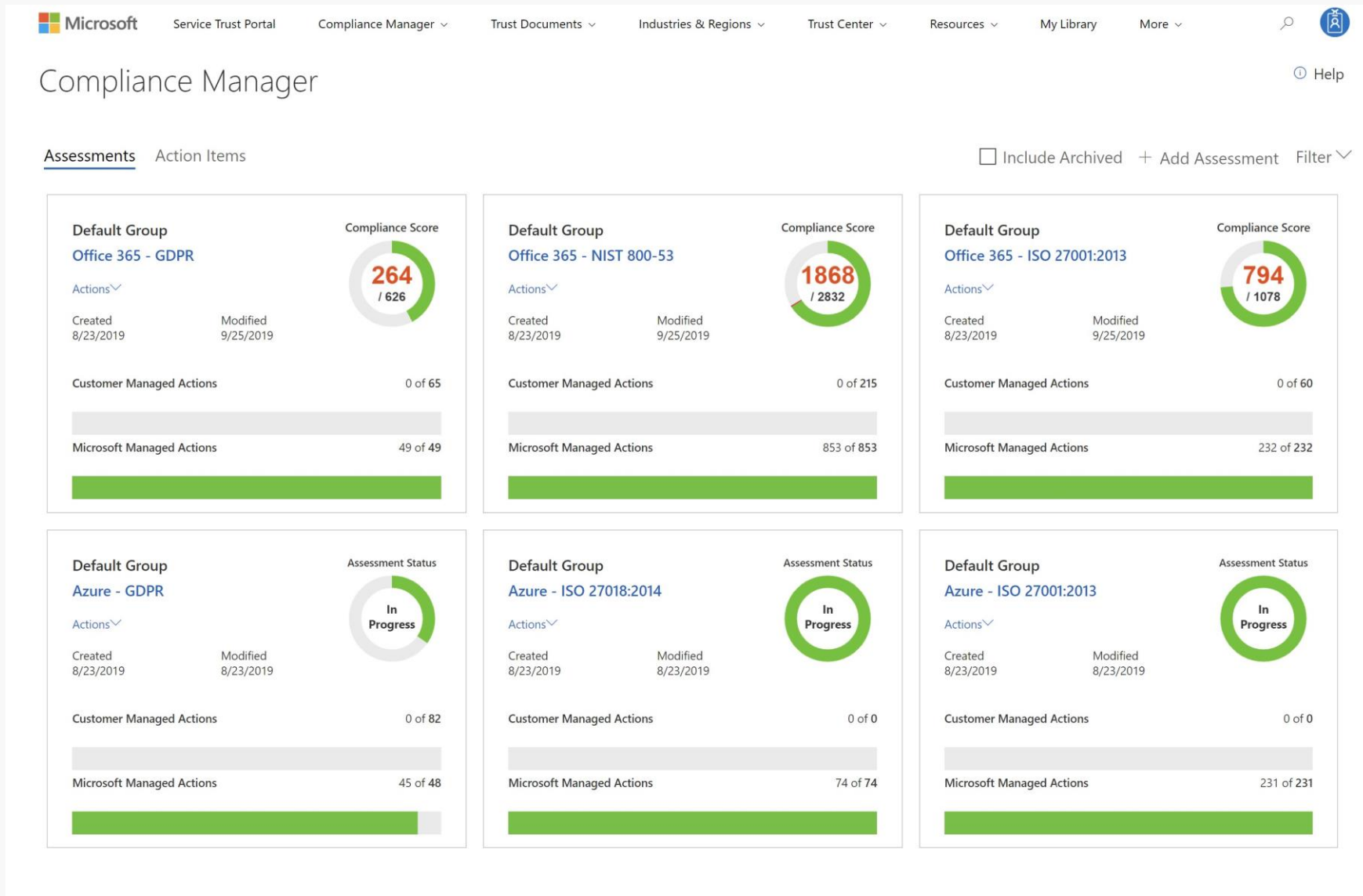
The screenshot displays a list of alerts in the Microsoft Cloud App Security console. The table has columns for Severity, Date, and a menu icon. The alerts are sorted by date, with the most recent at the top.

Severity	Date	
Low	9/10/19, 5:56 PM	
Medium	8/28/19, 10:38 PM	
Medium	7/16/19, 7:43 PM	
Low	7/2/19, 11:19 AM	
Low	7/2/19, 11:19 AM	
Medium	5/4/19, 9:18 AM	
Low	4/9/19, 9:01 AM	

Microsoft Compliance Manager

Microsoft Compliance Manager

Dohled nad stavem zvolených opáření v reálném čase – [blog](#); [Main page](#); [2 min video](#)



More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: 6.11.1 Control Title: Securing application services on public networks Supported GDPR Article(s): Article (5)(1)(f), Article (32)(1)(a) Description: Article (5)(1): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). Article (32)(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data	8	Implemented	8/31/2018	Third-party independent auditor	

More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: 6.7 Control Title: Cryptography Supported GDPR Article(s): Article (32)(1)(a) Description: Article (32)(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data	3	Implemented	8/31/2018	Third-party independent auditor	

More

Customer Managed Controls

0/7 Assessed

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: 7.2.1 Control Title: Identify and document purpose Supported GDPR Article(s): Article (5)(1)(b) Description: Article (5)(1): Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')	6	No related articles found	TM Manage Documents	Planned	Enter Date	Enter Date	Select
Control ID: 7.2.2 Control Title: Identify lawful basis Supported GDPR Article(s): Article (10), Article (17)(3)(a), Article (17)(3)(b), Article (17)(3)(c), Article (17)(3)(d), Article (17)(3)(e), Article (18)(2), Article (22)(2)(a), Article (22)(2)(b), Article (22)(2)(c), Article (5)(1)(a), Article (6)(1)(a), Article (6)(1)(b), Article (6)(1)(c), Article (6)(1)(d), Article (6)(1)(e), Article (6)(1)(f), Article (6)(3), Article (9)(1), Article (9)(2)(b), Article (9)(2)(c), Article (9)(2)(d), Article (9)(2)(e), Article (9)(2)(f), Article (9)(2)(g), Article (9)(2)(h), Article (9)(2)(i), Article (9)(2)(j), Article (9)(3), Article (9)(4) Description: Article (10): Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. Article (17)(3)(a): Paragraphs 1 and 2 shall not apply to the extent that processing is	6	GDPR: 7.2.3, 7.3.1, 7.3.4, 7.3.5, 7.3.7, 7.3.8	Assign Manage Documents	Select	Enter Date	Enter Date	Select

- Řízení přístupů, provozu a komunikace je pomocí cloudových nástrojů mnohem agilnější a poskytuje větší možnosti, zejména s ohledem na analýzu pomocí AI
- Nasazení cloudových prostředků dohledu a ochrany je rychlejší a pružnější

Děkujeme za pozornost!