NIS2 nebo nZoKB?

Petr Vlk
Microsoft MVP
Microsoft 365 Enterprise Security Architect @ KPCS CZ
KPCS vlk@kpcs.cz

NIS2
nZoKB

1. listopad 2025

- Vstupuje v platnost a startuje nám 60 a 365 dní

Zákonná povinnost

- Neznalost firmy a povinné osoby neomlouvá

Přímá odpovědnost a povinnosti vedení

- Přímé zapojení do kybernetické bezpečnosti

Organizační a technická opatření nejen v IT

- Směrnice, postupy, procesy, lidé, služby, krabičky

Ptáte se proč?

Network Information Security Directive 2 (NIS2) v EU

Česká transpozice do nového **Zákona o kybernetické bezpečnosti** (a podobně v EU)

Zajištění minimální úrovně odolnosti proti útokům v kybernetickém prostoru napříč členskými státy.

DORA, CER, Digitální služby…

Co je NIS2?

- NIS2 je novou direktivou EU v oblasti kybernetické bezpečnosti, vstoupila v platnost 17. ledna 2023 a nyní mají členské státy provést transpozici do lokálního práva
- Jejím cílem je zavést povinné minimální bezpečnostní standardy napříč důležitými ekonomickými subjekty a kritickými službami v EU
- Výsledkem má být snížení rizika vzniku a omezení dopadů bezpečnostních incidentů a zvýšení kybernetické bezpečnosti v celé EU
- Poskytuje vodítka, politiky, procedury, standardy pro technická a organizační bezpečnostní opatření nejen v oblastech detekce, řešení a hlášení incidentů, zvyšování bezpečnosti systémů, zavádění kryptografických prostředků, bezpečného ověřování, školení uživatelů, certifikace služeb a dalších oblastí informačních systémů
- Přináší nové povinnosti pro organizace a povinnost jejich aplikace, kdy nesoulad může být trestán pokutou až 10 milionů euro nebo 2 % z čistého obratu (dle toho, co je vyšší) nebo odnětím licence k provozování služby nebo pozastavení výkonu statutárního orgánu
- Rozděluje subjekty jako „**poskytovatele regulované služby**“ do dvou skupin a to „**Essential**“ (vyšší povinnosti) a „**Important**“ (nižší povinnosti).

nZoKB: NIS2 a Česká republika?

- Byl zcela přepracován Zákon o kybernetické bezpečnosti
  - Zákon podepsán prezidentem, zveřejněn, vstoupí v platnost 1. listopadu 2025
  - Obsahově kopíruje metodiky, postupy a opatření ISO 27001, vyhlášky ještě chybí
- Subjekty určené jako KII budou vždy v režimu Essential
  - Budou na ně kladeny nejvyšší nároky
  - NÚKIB získává širší pravomoci a kontrolní mechanismy
- Následně začíná subjektům ze strany regulátora běžet přechodné období pro implementaci změn (lhůta pro zavedení) od **transpozice v délce 12 měsíců od sebeurčení nebo určení ze strany regulátora či odběratele a 60 dnů do evidenčního hlášení po platnosti zákona**
- Nutnost určení dopadů a aktivní spolupráce s regulátorem, nová evidence subjektů a povinnost součinnosti (poskytnout zdroje) při řešení incidentů a stavu ohrožení
- Propaguje výjimky pro konkrétní subjekty, **povinnosti a řízení dodavatelů**, sledujete například **varování** a **ochranná opatření obecné povahy**?

nZoKB a NIS2 a možný další postup?

- **Sebeurčení** nebo **určení** společnosti
  - Velikost organizace a regulovaná služba (ohrožení zdraví, dopad na chod dne…)
  - Explicitní povinnosti pro konkrétní subjekty (domény, DNS, hostingy…)
- Logicky se nabízejí dvě možnosti řešení a přípravy:
  - Evoluční rozvoj dotčených oblastí
    - Nastartování směřování systému řízení bezpečnosti, technických opatření a procesů společnosti, tak aby v roce 2025 až 2026 byla společnost v souladu s novou verzí Zákona o kybernetické bezpečnost (a tedy vybraných standardů ISO 27001)
  - Odstartování projektu/programu zajištění souladu s NIS2
    - Zadání komplexního projektu/programu, kdy jeho odpovědností bude zajistit nastavení souladu v jednotlivých oblastech tj. od řízení bezpečnosti až po změny procesů společnosti a implementaci technologií

Směrnice, procesy, technologie, opatření…

- Nově NÚKIB bude disponovat silnějšími kontrolními mechanismy.
  - Jakými jsou kontrola na pracovišti, bezpečnostní audity, nutnost certifikace klíčových komponent a systémů, možnost vyžádání si informací k posouzení stavu opatření a stavu kybernetické bezpečnosti organizace, aktivní skenování, vyžádání si důkazů a součinnosti v rámci šetření a reakce na kybernetické incidenty, finálně dle zákona a vyhlášek.
  - Projděte si zákon a jeho vyhlášky na další povinnosti a konkrétní náležitosti.
- Opatření směřují na správnou implementaci technologií, procesů a postupů pro zajištění jednotlivých kontrol:
  - **Analýza rizik a dopadů**
  - **Bezpečnostní politiky**
  - **Šifrování a správa kryptografických klíčů (HSM a MIP)**
  - **Ochrana dat a přístupu k informacím (MIP a DLP)**
  - **Bezpečná autentizace a MFA (Azure AD MFA)**
  - **Logování a audit přístupů a aktivit (SIEM)**
  - **Analýza chování uživatelů, aplikací, zařízení, procesů (EDR)**
  - **Bezpečnostní procedury a postupy (EDR, MDO, DLP, MIP)**

NIS2 a Microsoft

- V cloudu v dobrých rukách
- Ale na cloudu nezáleží
- A cloud to nevyřeší…

- Závisí na kontextu
- Závisí na nastavení
- Závisí na organizaci

NIS2 principle	Microsoft solutions
Governance	Microsoft Defender CSPM, Entra, Microsoft Purview Compliance Manager
Risk management	Microsoft Defender XDR, Microsoft Purview Insider Risk Management
Asset management	Microsoft Defender XDR, Microsoft Purview Data Lifecycle Management
Supply chain	Microsoft Defender XDR, Entra, Microsoft DevOps
Service protection	Microsoft Defender XDR
Identity & access	Entra
Encryption	Microsoft Purview Information Protection
System security	Microsoft Defender XDR
Resilient networks	Azure Network Security
Staff awareness	Office 365 Phishing Simulation and Learning Paths, Microsoft Purview in-app notification & policies
Security monitoring	Microsoft Sentinel, Microsoft Purview Insider Risk Management
Proactive security	Microsoft Defender XDR
Response and recovery	Microsoft Defender XDR, Azure Backup and Recovery, Microsoft Purview Insider Risk Management (Adaptive Scopes)
Incident reporting	Microsoft Purview e-Discovery & Audit

Řízení bezpečnosti: Zero Trust

A NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

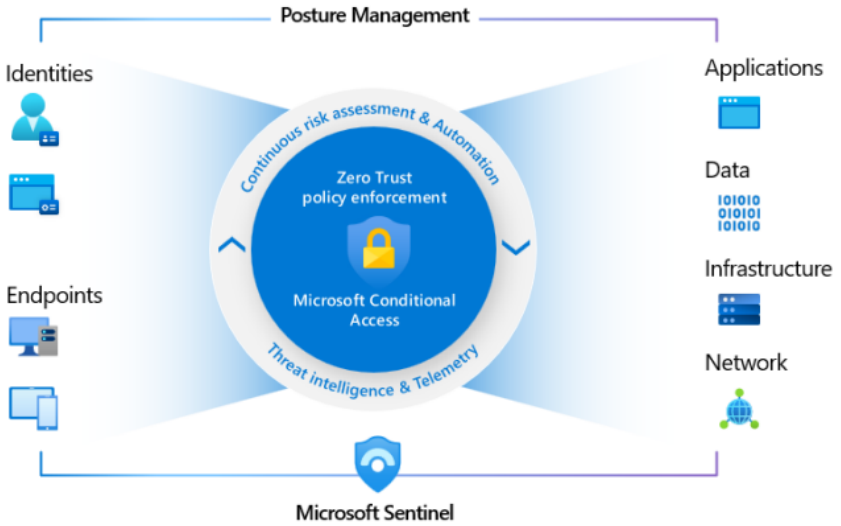
Policies on risk analysis and information system security

Explanation

Effective security policies must be implemented consistently across the organization to protect information systems and customers. Security policies must also account for variations in business functions and information systems to be universally applicable.

Zero Trust Framework

Zero Trust architecture recommends continuous risk assessment in the digital world where attacks happen at cloud speed. Each request shall be intercepted and verified explicitly by analyzing signals on user, location, device compliance, data sensitivity, and application type.



Incidenty: Detekce a reakce

B

NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Incident handling

Security incident handling is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. It seeks to give a robust and comprehensive view of any security issues within an IT infrastructure.

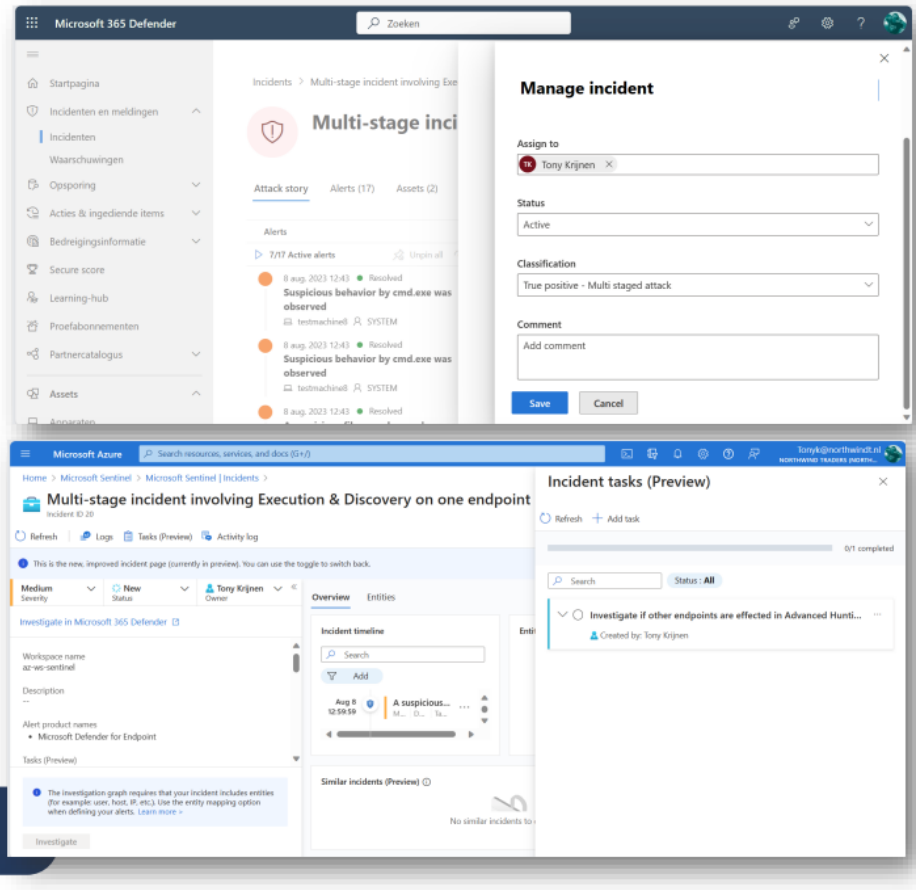
Incident handling with Microsoft Defender

The standard Microsoft Defender security incident homepage allows staff to assign, label, classify and comment on the incidents.

Incident handling with Microsoft Sentinel

Microsoft Sentinel is the Microsoft SIEM (Security Information and Event Management) solution. Sentinel analyzes the signals from all different sources in the organization and allows for full incident and event management, creating and assigning tasks, activity logs, etc.

More information on Sentinel Incident handling



Kontinuita: Zálohování

C NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Business continuity – Backup management (1)

Business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyberattacks and communication failures. Aspects of business continuity are Backup management, Disaster recovery and Crisis management. We will cover each topic in a separate slide, this is the slide on Microsoft 365 backup management.

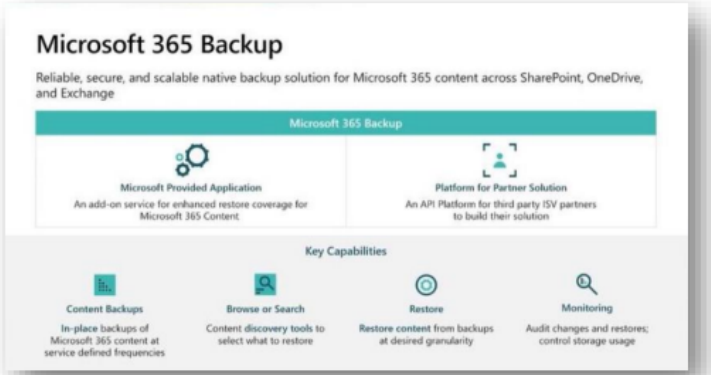
Microsoft 365 Backup

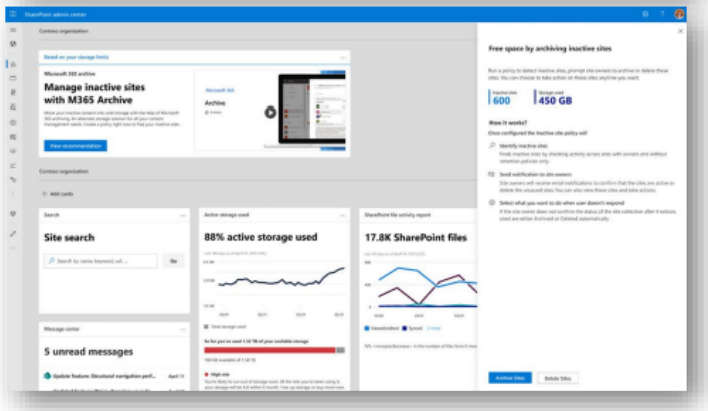
Microsoft 365 backup is a feature that allows you to recover your OneDrive, SharePoint, and Exchange data in case of data loss or corruption. You can backup all or select sites, accounts, and mailboxes in your tenant, and restore them to a prior point-in-time. You can access Microsoft 365 backup directly in the Microsoft 365 admin center or through a partner's application built on top of the Backup APIs1.

Microsoft 365 Archiving

Microsoft 365 Archive gives you a cold data storage tier that enables you to keep inactive or aging data within SharePoint at a cost-effective price point matching the value of that data's lifecycle stage. Because the content is archived in place, it retains Microsoft 365's valuable security, compliance, search, and rich metadata.

More information on
Microsoft 365 Backup & Archive





Kontinuita: Zálohování

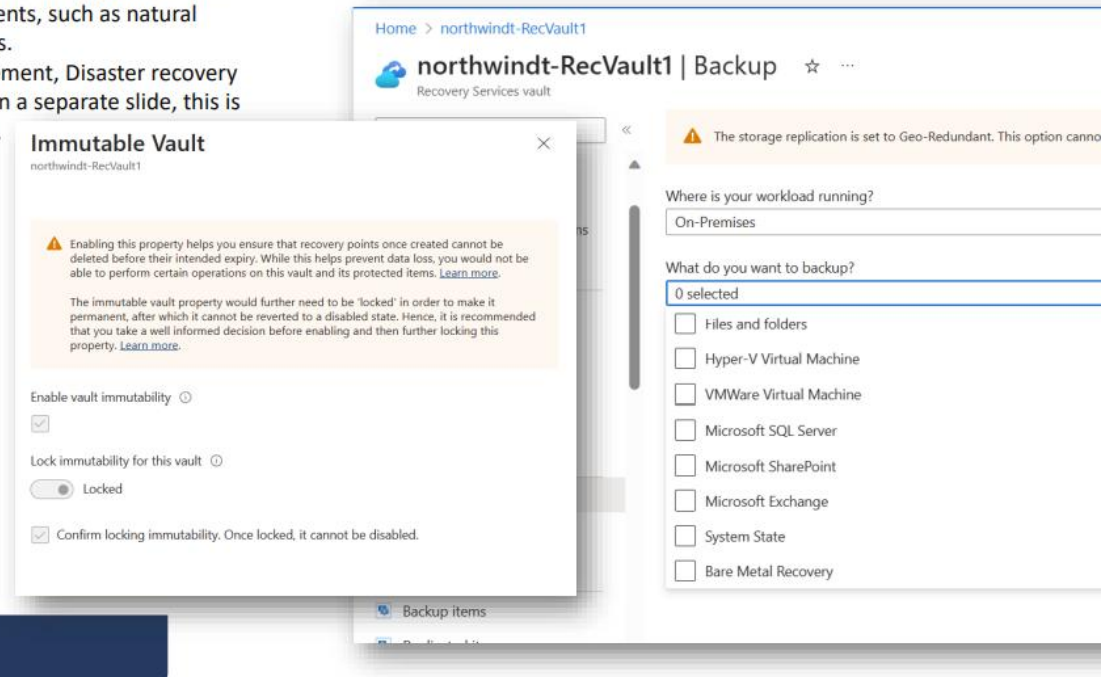
C NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Business continuity – Backup management (2)

Business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyberattacks and communication failures.
Aspects of business continuity are Backup management, Disaster recovery and Crisis management. We will cover each topic in a separate slide, this is the slide on Microsoft Azure backup management.

Microsoft Azure Backup

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.
Azure Backup helps protect your critical business systems and backup data against a ransomware attack by implementing preventive measures and providing tools that protect your organization from every step that attackers take to infiltrate your systems. It provides security to your backup environment, both when your data is in transit and at rest.



What is Microsoft Azure Backup ?

Kontinuita: Zotavení

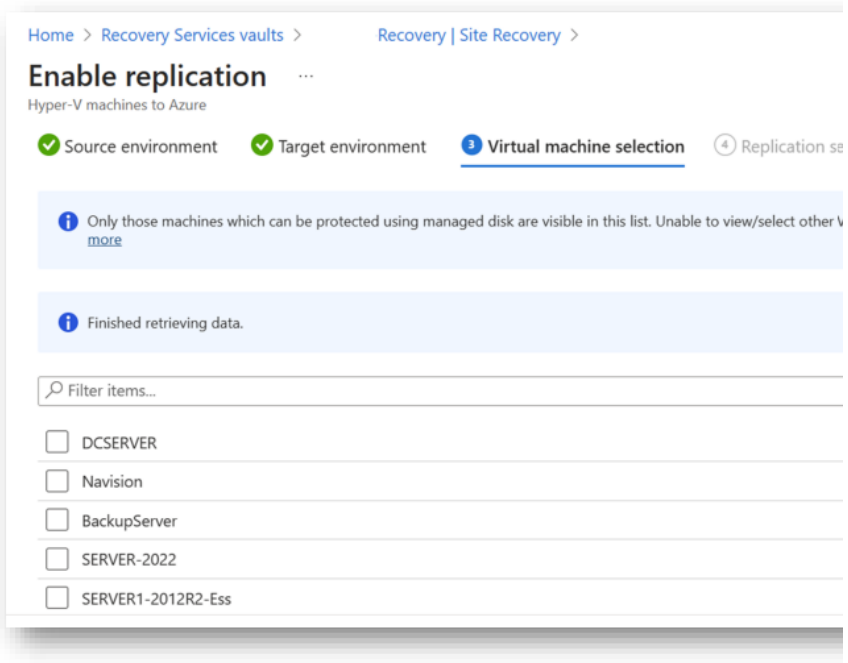
C NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Business continuity – Disaster Recovery

Business continuity is the capability of your enterprise to stay online and deliver products and services during disruptive events, such as natural disasters, cyberattacks and communication failures. Aspects of business continuity are Backup management, Disaster recovery and Crisis management. We will cover each topic in a separate slide, this is the slide on Microsoft Disaster Recovery.

Microsoft Azure Site Recovery

Azure Site Recovery is a service that helps you keep your business running during IT outages. It allows you to replicate your workloads to Azure or another location, and fail over and recover them when needed. You can use it to protect Azure VMs, on-premises VMs, physical servers, and databases. Azure Site Recovery offers simple deployment and management, cost savings, reliable recovery, and security features



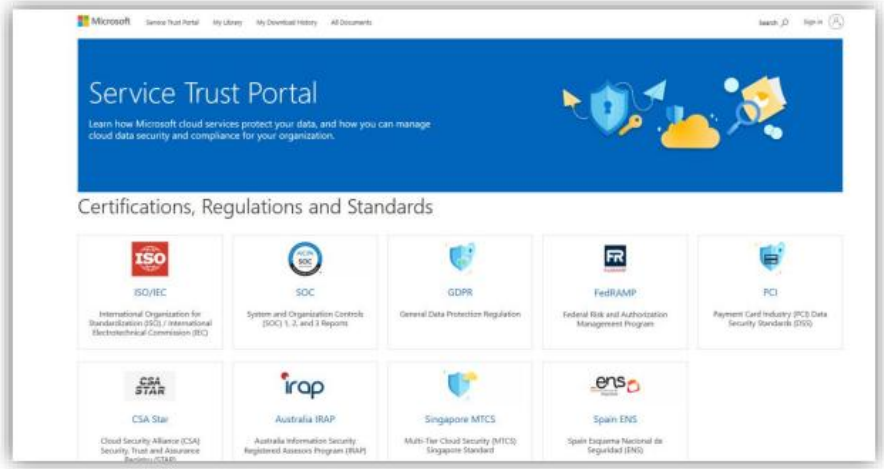
More information on Microsoft Disaster Recovery

Bezpečnost dodavatelů: Microsoft

D NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Supply chain security

Digital supply chains are becoming more complex, more digital, and more interdependent, which means that any vulnerability or attack in one part of the supply chain can have a ripple effect on the entire chain. One example of this is how Microsoft is showcasing their compliance.



Compliance (3rd party assurance/SOC verklaring)

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

External Access (technology)

Entra ID Connect is an on-premises Microsoft application that's designed to meet and accomplish your hybrid identity goals. Use Entra ID Connect to benefit from a modernized Active Directory and benefit from security features such as single sign on and conditional access policies.

Get started with **Entra ID**

Bezpečnost informačních systémů

E

NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Security in network and information systems acquisition, development and maintenance

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.

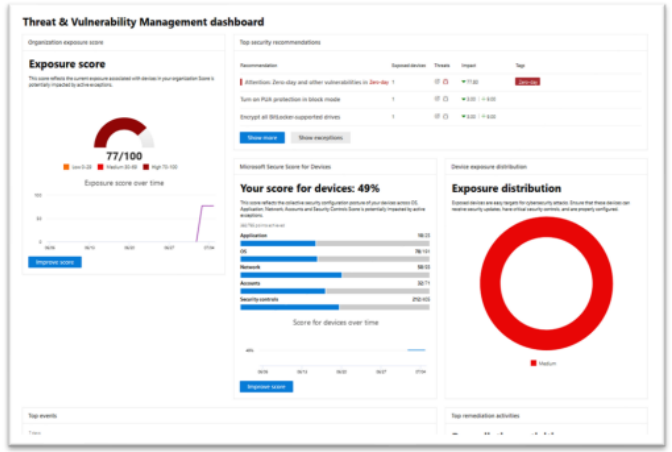
Defender Vulnerability Management

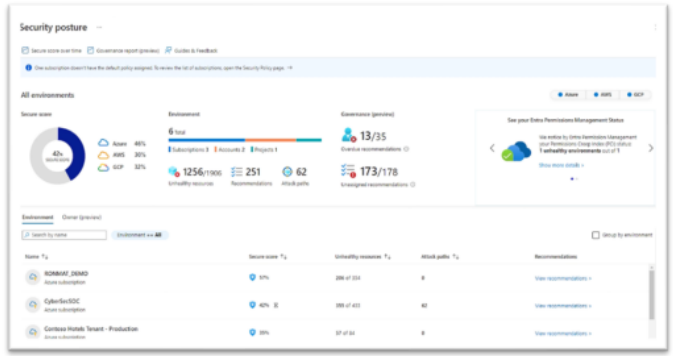
Defender Vulnerability Management (DVM) delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Leveraging Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

Cloud Security Posture Management

Cloud Security Posture Management (CSPM) provides you with hardening guidance that helps you efficiently and effectively improve your security. CSPM also gives you visibility into your current security situation.

Get started with DVM and CSPM





Bezpečnost provozních technologií

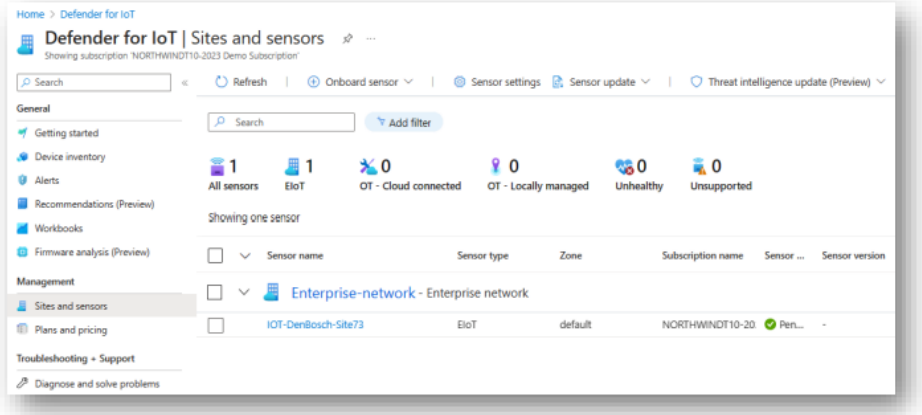
E NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Security in network and information systems acquisition, development and maintenance

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.

Defender for IOT

Defender for IoT is a security solution that protects IoT and OT devices from physical and cyber threats. It provides asset discovery, vulnerability management, and threat detection for complex, digital, and interdependent environments. It also integrates with other security tools such as Sentinel, Splunk, and Defender for Endpoint



Get started with Defender for IoT

Bezpečný vývoj a akvizice

NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

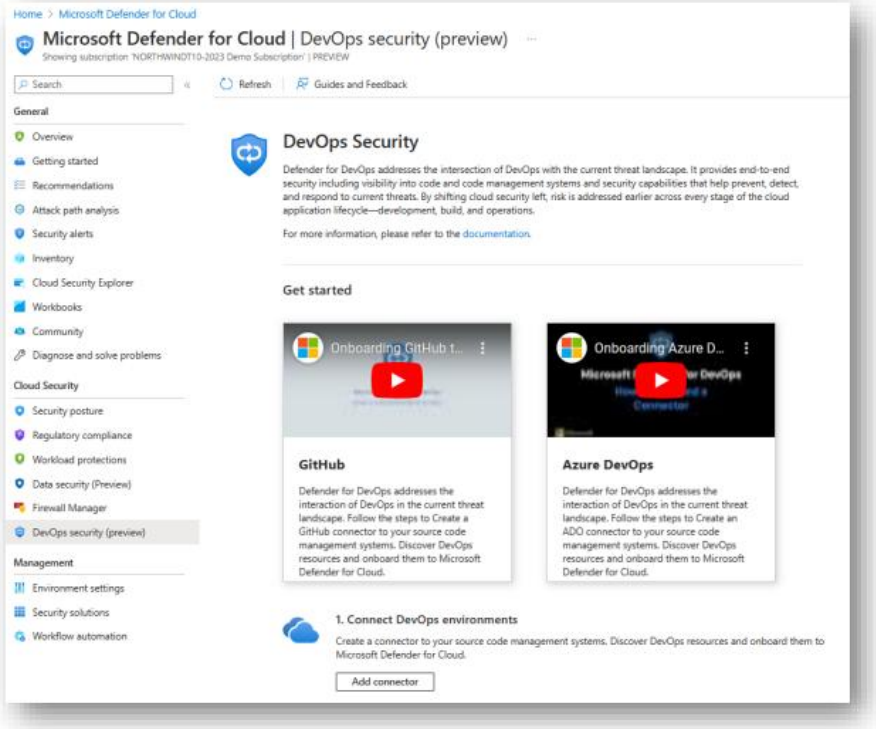
Security in network and information systems acquisition, development and maintenance

From acquisition to maintenance, ensuring network and information systems security is paramount. Ongoing maintenance demands constant monitoring, timely patches, and regular security assessments to safeguard data integrity and operational stability.

Defender for DevOps

Defender for DevOps uses a central console to empower security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, such as GitHub and Azure DevOps. Findings from Defender for DevOps can then be correlated with other contextual cloud security insights to prioritize remediation in code.

Get started with Defender for DevOps



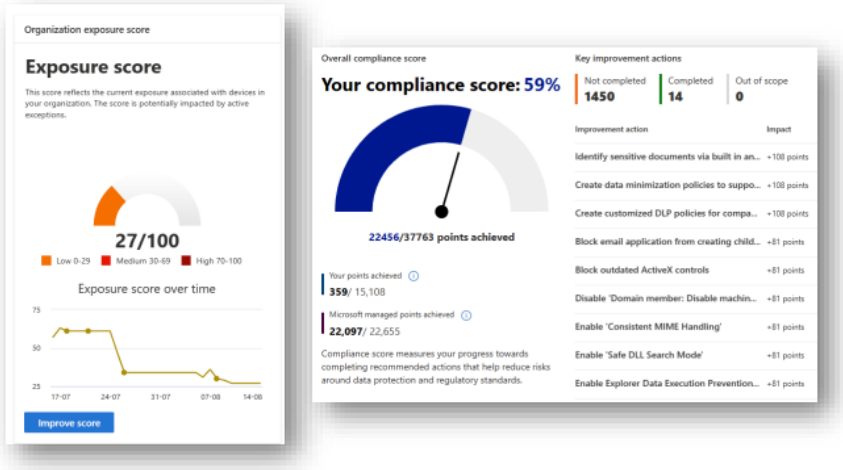
Řízení kybernetických rizik

F NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (1)

Although there are many methods and frameworks for policies, procedures and assessing the effectiveness of cybersecurity risk-management measures, common steps are:

- Understand the security landscape of your organization, including its assets, systems, vendors, and regulations
- Identify gaps in your current cybersecurity controls, such as outdated software, weak passwords, or phishing vulnerabilities
- Create a team of qualified and experienced cybersecurity professionals who can monitor, respond, and improve your security posture
- Determine the informational value of your assets and prioritize them based on their importance and sensitivity
- Analyze and address the risks that pose the most threat to your assets, using tools such as penetration testing, risk scoring, and mitigation strategies



More information on Zero Trust

Řízení kybernetických rizik

F NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (2)

This slide focusses on how you can understand the security landscape of your organization. Microsoft Secure Score helps organizations by reporting on the current state of the organization's security posture; Improve security posture by providing discoverability, visibility, guidance, and control and compare with benchmarks and establish key performance indicators (KPIs).

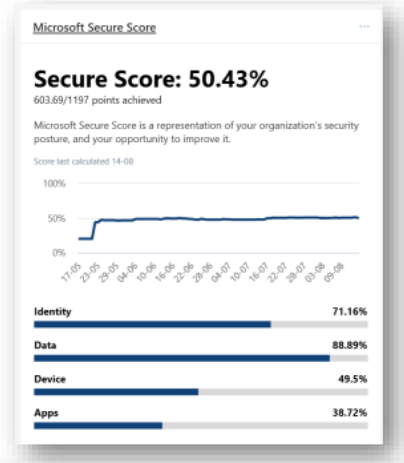
Microsoft Defender Secure Score

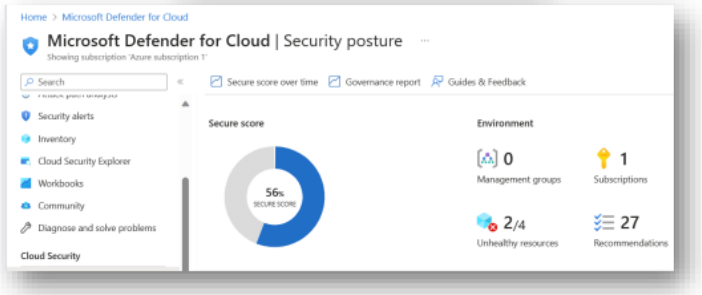
The Microsoft Defender Secure Score is applicable for Microsoft SaaS workloads, such as Microsoft 365, Identity, Devices and Apps. It evaluates your configuration settings and behaviors and gives you a score based on the alignment with security standards.

Microsoft Defender for Cloud Secure Score

The Microsoft Defender for Cloud Secure Score applies to PaaS, IaaS, hybrid and multi-cloud workloads. It assesses your cross-cloud resources for security issues and gives you a score based on the implementation of best practices. Defender for Cloud can provide recommendations for Microsoft Azure, Amazon Web Services, Google Cloud Suite, etc.

More information on Secure Score





Řízení kybernetických rizik

F

NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Policies and procedures to assess the effectiveness of cybersecurity risk-management measures (3)

This slide focusses on how you can identify gaps in your current cybersecurity controls, such as outdated software, weak passwords, or phishing vulnerabilities.

Microsoft Defender Exposure Score

Microsoft Defender exposure score is a metric that reflects how vulnerable your organization is to cybersecurity threats. Your exposure score is influenced by factors such as weaknesses, threats and security alerts on your devices.

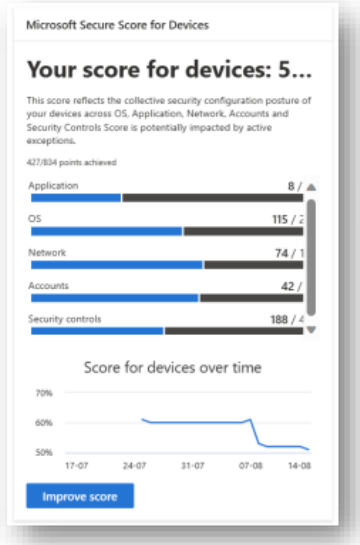
Microsoft Defender for Identity

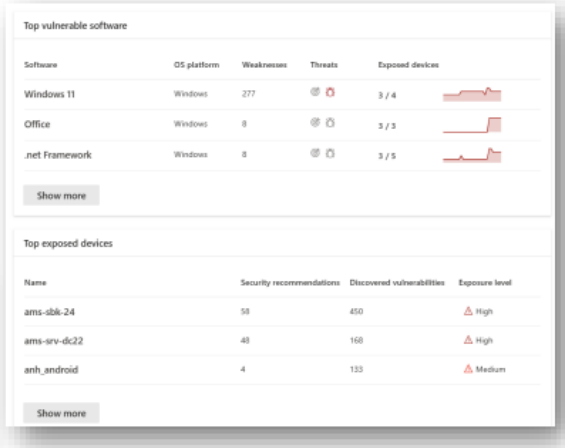
Defender for Identity can detect accounts with unsecure attributes that expose a security risk, such as PasswordNotRequired. It can also detect weak cipher usage on devices and accounts, such as RC4 or DES2. Additionally, it can alert you of credential access attempts by malicious actors.

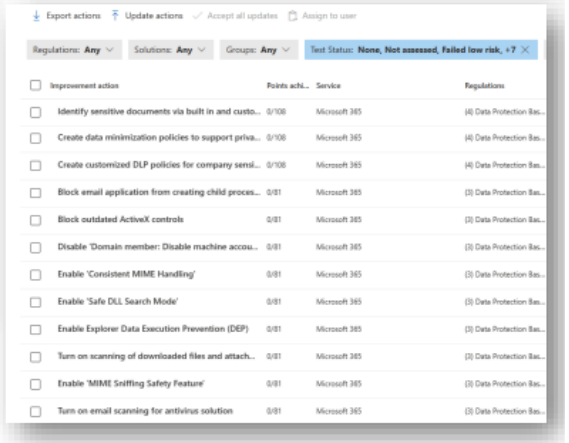
Compliance manager

Compliance score measures progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

More information on Compliance Score







Vzdělávání uživatelů a bezpečnostní hygiena

G NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Basic cyber hygiene practices and cybersecurity training (1)

Cybersecurity training is the process of educating yourself and others about the risks and best practices of cyber hygiene. Training can help you develop the skills and knowledge to protect yourself and your organization from cyber threats.

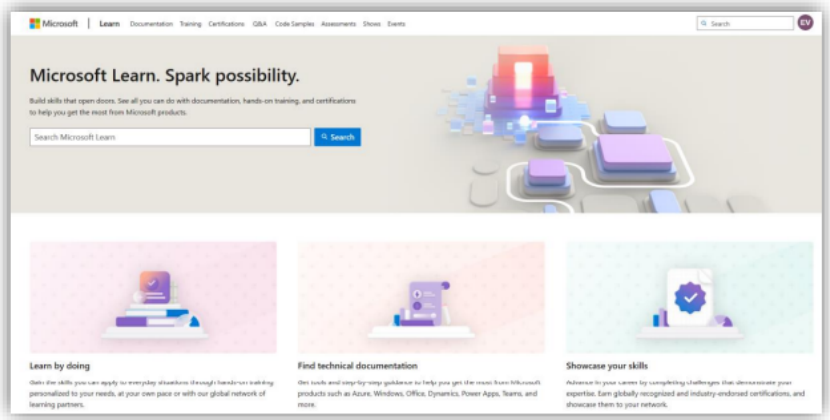
Microsoft 365 Learn

Microsoft Learn offers learning paths for Microsoft 365 , Security and Microsoft Teams, as well as virtual training days and a community to connect with other learners and professionals. Microsoft Support provides video training, templates, quick starts, cheat sheets, infographics, and more for Microsoft 365.

Defender for Office 365

On of the key features of Defender for Office 365 is the Attack simulation training, which allows you to run realistic attack scenarios in your organization and identify vulnerable users. By using Attack simulation training, you can educate your users on how to recognize and report phishing, malware, and ransomware attacks, and improve their security awareness and behavior.

Get started with Microsoft Learn



Vzdělávání uživatelů a bezpečnostní hygiena

G NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

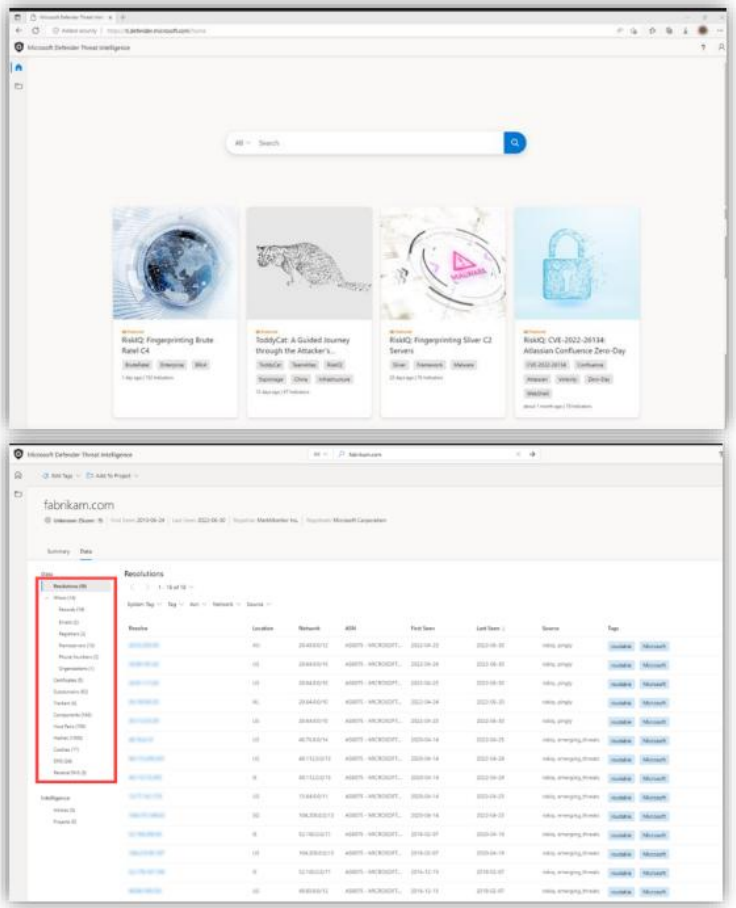
Basic cyber hygiene practices and cybersecurity training (2)

Cybersecurity training is the process of educating yourself and others about the risks and best practices of cyber hygiene. Training can help you develop the skills and knowledge to protect yourself and your organization from cyber threats.

Your cybersecurity weather forecast
Defender Threat Intelligence

Microsoft Defender Threat Intelligence (Defender TI) is a platform that streamlines triage, incident response, threat hunting, vulnerability management, and cyber threat intelligence analyst workflows when conducting threat infrastructure analysis and gathering threat intelligence. Analysts spend a significant amount of time on data discovery, collection, and parsing, instead of focusing on what actually helps their organization defend themselves--deriving insights about the actors through analysis and correlation.

Get started with Defender TI



Kryptografie

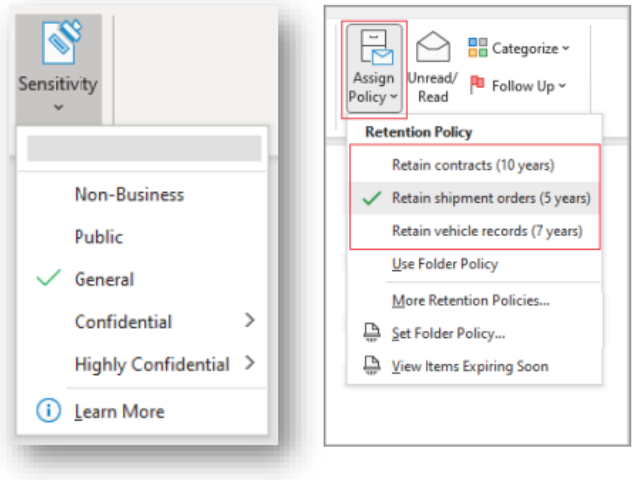
H NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Policies and procedures regarding the use of cryptography and, where appropriate, encryption

Encryption is an important part of your file protection and information protection strategy. Encryption by itself doesn't prevent content interception. Encryption is part of a larger information protection strategy for your organization. By using encryption, you help ensure that only authorized parties can use the encrypted data.

Purview Information Protection Sensitivity Labels
Microsoft Purview Information Protection to help you discover, classify, and protect with the use of encryption the sensitive information wherever it lives or travels. Sensitivity labels let you classify and protect your organization's data in-rest and in-motion, while making sure that user productivity and their ability to collaborate isn't hindered.

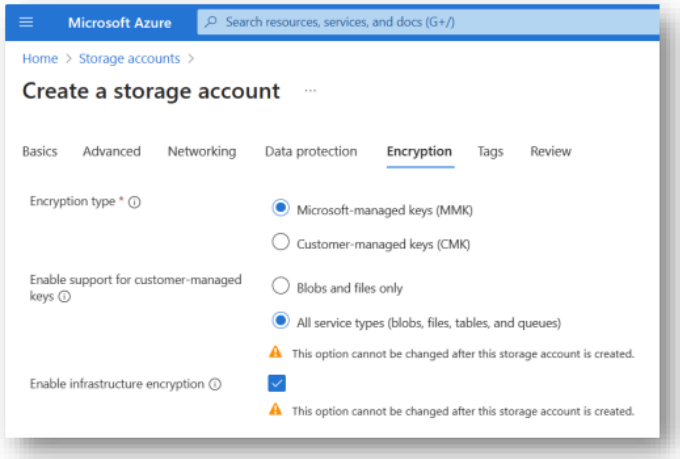
Data Lifecycle Management
Microsoft Purview Data Lifecycle Management provides you with tools and capabilities to retain the content that you need to keep and delete the content that you don't. Retaining and deleting content is often needed for compliance and regulatory requirement, but deleting content that no longer has business value also helps you manage risk and liability



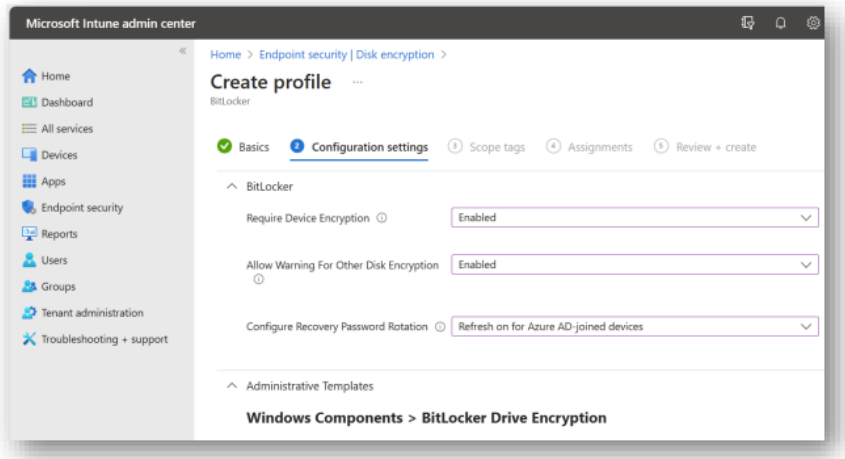
Kryptografie

H NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Policies and procedures regarding the use of cryptography and, where appropriate, encryption



ENCRYPTION SETTINGS IN A MICROSOFT AZURE STORAGE ACCOUNT



ENFORCING HARDDISK DRIVE ENCRYPTION THROUGH DEVICE POLICIES

Řízení přístupu a lidských zdrojů

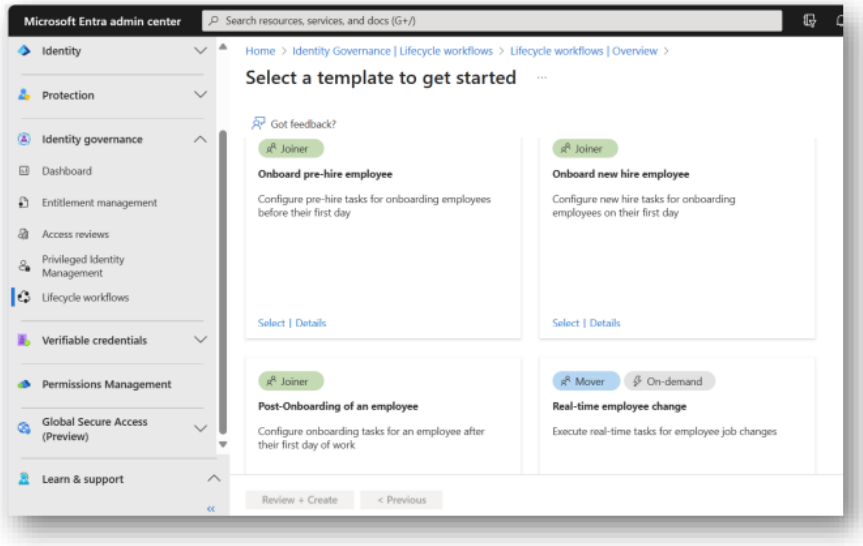
NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Human resources security, access control policies and asset management (1)

Microsoft Entra ID Governance allows you to balance your organization's need for security and employee productivity with the right processes and visibility. It provides you with capabilities to ensure that the right people have the right access to the right resources.

Microsoft Entra Lifecycle Management

Entra lifecycle management is a feature of Microsoft Entra ID Governance that helps you manage users by automating their joiner, mover, and leaver processes.
You can create and manage workflows that consist of tasks and execution conditions to perform actions on users based on their attributes, group memberships, or status changes.
Lifecycle workflows can even integrate with the ability of Microsoft logic apps tasks to extend workflows for more complex scenarios that require integration with existing systems and procedures.



What are Microsoft Entra lifecycle workflows?

Řízení přístupu a lidských zdrojů

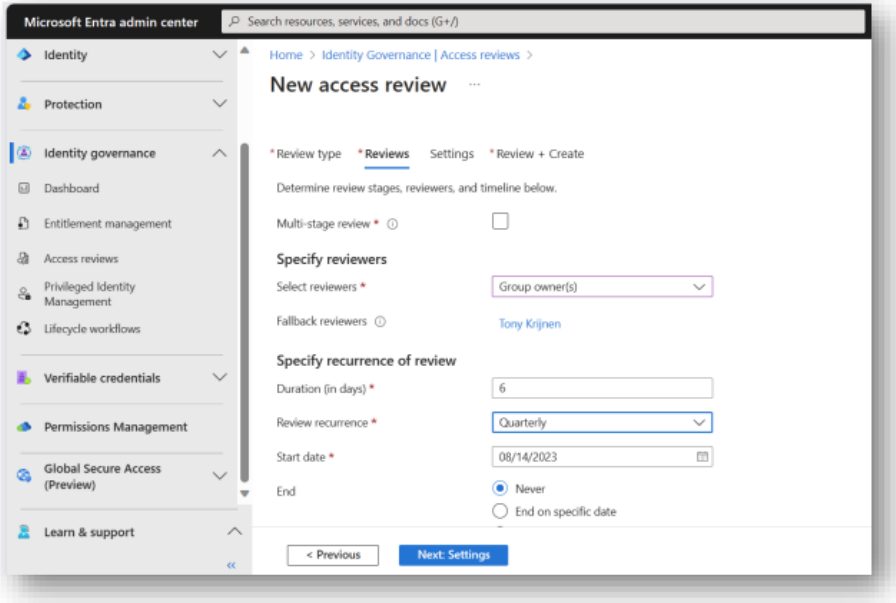
NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Human resources security, access control policies and asset management (2)

With the new Entra ID (Azure Active Directory) Governance features organizations have more control over standard procedures as well as timed access reviews.

Microsoft Entra Access Reviews

Also a feature of the Microsoft Entra ID Governance, Microsoft Entra access reviews helps you manage the access to your resources, such as groups and applications, by reviewing them regularly. You can create and perform access reviews for users or guests, and ask them or a decision maker to confirm or revoke their access based on their needs. You can also use access reviews to comply with policies, audit requirements, or security best practices.



What are Microsoft Entra Access Reviews?

Řízení přístupu a lidských zdrojů

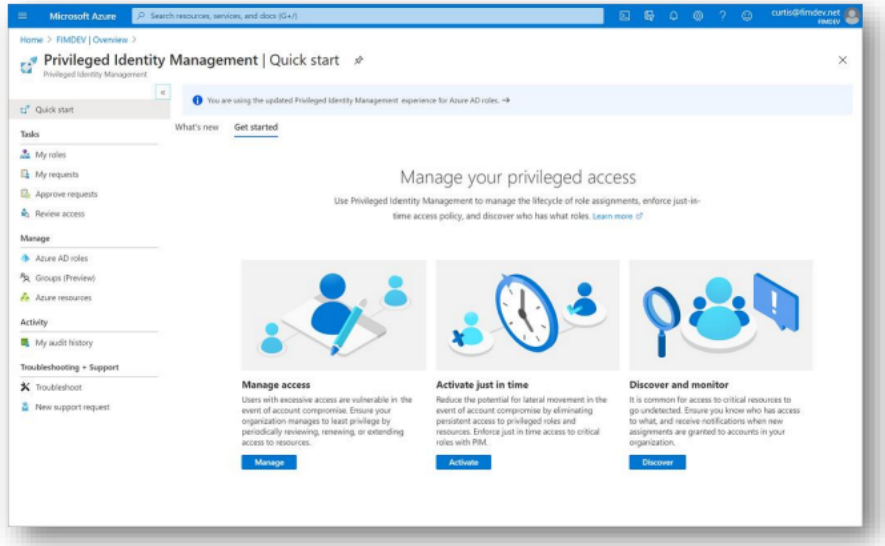
NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

Human resources security, access control policies and asset management

Microsoft Conditional access and Microsoft Privileged Identity Management help organizations to limit access to administrative roles until that access is needed and only when conditions are met.

Privileged Identity Management

Privileged Identity Management (PIM) is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization (Microsoft Entra ID, Azure, Microsoft 365 and other Microsoft Online Services).|
It provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.



https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Bezpečná komunikace a druhý faktor

J NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity

Explanation
The modern security perimeter extends beyond an organization's network perimeter to include user and device identity. Organizations now use identity-driven signals as part of their access control decisions.

Zero Trust Mapping
Zero Trust requires that every transaction between systems (user identity, device, network, and applications) be validated and proven trustworthy before the transaction can occur.

Conditional Access
Azure AD Conditional Access brings signals together, to make decisions, and enforce organizational policies. Conditional Access is Microsoft's Zero Trust policy engine taking signals from various sources into account when enforcing policy decisions. This feature helps organizations to align their identities with the three guiding principles of a Zero Trust architecture: verify explicitly, use least privilege and assume breach.

Risk based Conditional Access
Most users have a normal behavior that can be tracked, when they fall outside of this norm it could be risky to allow them to just sign in. You may want to block that user or maybe just ask them to perform multifactor authentication to prove that they're really who they say they are. A sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner.

Bezpečná komunikace a druhý faktor

J NIS2 COMPLIANCE IS A ZERO TRUST JOURNEY

The use of multi-factor authentication or continuous authentication solutions

Token interception through an Adversary-in-the-middle attacks is the most common way to bypass MFA and allow attacks to leverage a token replay to gain full access. Microsoft Entra Authentication Strengths can help to mitigate these attacks.

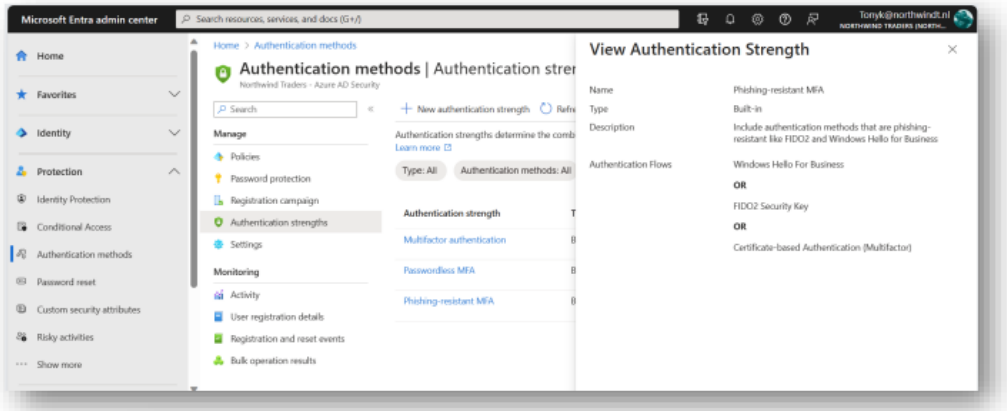
Microsoft Entra Authentication Strengths

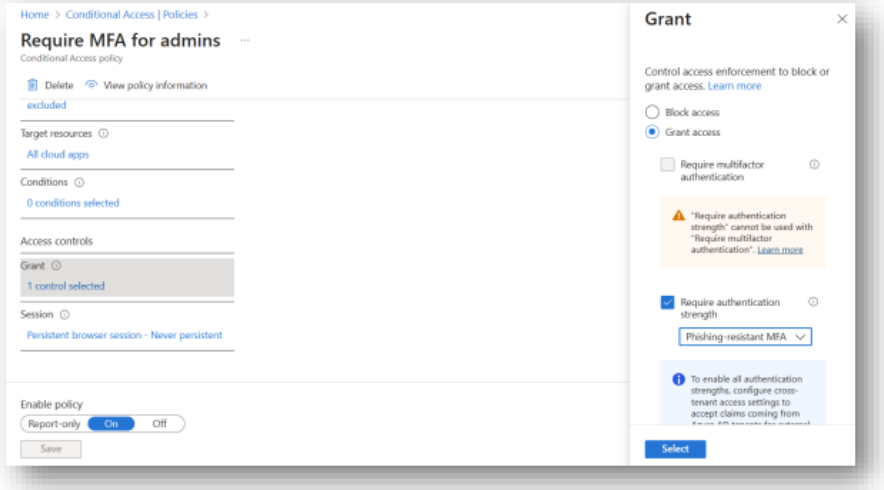
The new Entra Authentication Strengths (a feature of Microsoft Entra ID) allows you to specify which combination of authentication methods can be used to access a resource. For example, you can require phishing-resistant methods (FIDO2 keys, Windows Hello, Smartcards for sensitive resources.

Enforce Authentication Strengths through CA

You can use authentication strengths in conditional access policies to define a minimum level of authentication strength required for access, based on factors such as the user's sign-in risk level, the sensitivity of the resource being accessed, the user's location, and more

Get started with **Entra ID**





Organizační opatření

- Povinné role v organizaci (manažer, architekt, garant, …)
- Povinnost vrcholového managementu a jeho zapojení do kybernetické bezpečnosti a jeho vzdělávání
- Vedení a řízení aktualizované dokumentace
- Řízení aktiv a rizik
- Řízení dodavatelů
- Řízení kontinuity činností
- Přijetí povinných bezpečnostních opatření
- Hlášení incidentů

Organizační opatření v detailu

- Systém řízení bezpečnosti informací (ISMS, neustálé zlepšování, …)
- Povinnosti vrcholového vedení, zajištění zdrojů, vzdělávání se
- Bezpečnostní role a jejich zajištění
- Řízení bezpečnostní politiky a bezpečnostní dokumentace
- Řízení aktiv (primární a podpůrná)
- Řízení rizik (hrozby, zranitelnosti, dopad, …)
- Řízení dodavatelů
- Bezpečnost lidských zdrojů a jejich vzdělávání
- Řízení změn
- Akvizice, vývoj a údržba
- Řízení přístupu a privilegovaného přístupu
- Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- Řízení kontinuity činností, zálohování, plán obnovy
- Audit kybernetické bezpečnosti
- …

Bezpečnostní politiky a technická opatření

- Politika systému řízení bezpečnosti informací
- Politika organizační bezpečnosti
- Politika řízení aktiv
- Politika řízení rizik
- Politika zvládání kybernetických bezpečnostních událostí a incidentů
- Politika fyzické bezpečnosti
- Politika detekce kybernetických bezpečnostních událostí
- Politika pro sběr a vyhodnocování kybernetických bezpečnostních událostí
- Politika bezpečnosti komunikační sítě
- Politika bezpečného používání mobilních zařízení
- Politika bezpečnosti lidských zdrojů
- Politika řízení přístupu
- Politika bezpečného chování uživatelů, administrátorů a osob zastávajících bezpečnostní role·
- Politika řízení dodavatelů
- Politika pro zaznamenávání událostí
- Politika řízení zranitelností a aktualizací aplikačního vybavení
- Politika akvizice, vývoje a údržby
- Politika řízení změn
- Politika používání kryptografie
- Politika řízení kontinuity činností
- Politika dlouhodobého ukládání, zálohování a obnovy
- …

NÚKIB a první kroky…

- Registrace?
- Doporučení, Varování, Reaktivní Opatření, Ochranné opatření

- Audit nebo plán zajištění souladu
  - Podpora vedení při procesu sebe/určení
- Kontrola aktiv, dokumentace, směrnic, procesů, technologií
  - Zranitelnosti, aktualizace, správa identit a MFA
  - Segmentace sítí, VPN, zálohování a obnova, logování, incidenty
  - Šifrování, školení uživatelů a vedení, krizové postupy a kontinuita
  - Podpora partnera při konzultacích, analýze souladu nebo nasazení

Kam dál?

- NÚKIB
  - https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti
  - Základní a první místo pro další studium
- Cybrela
  - https://cybrela.com/
  - Potřebujete se nachytřit organizačně
- KPCS CZ
  - https://www.kpcs.cz/
  - Potřebujete se nachytřit technologicky

Že už používáte a platíte za služby Microsoft 365? Využijte jejich benefitů na maximum!

Definujte priority bezpečnosti: Zero Trust Workshop by KPCS

Ověřte si realitu IT prostředí: Security Risk Assessment by KPCS

Dotazy a diskuse

Petr Vlk
Microsoft MVP
Microsoft 365 Enterprise Security Architect @ KPCS CZ
vlk@kpcs.cz


KPCS