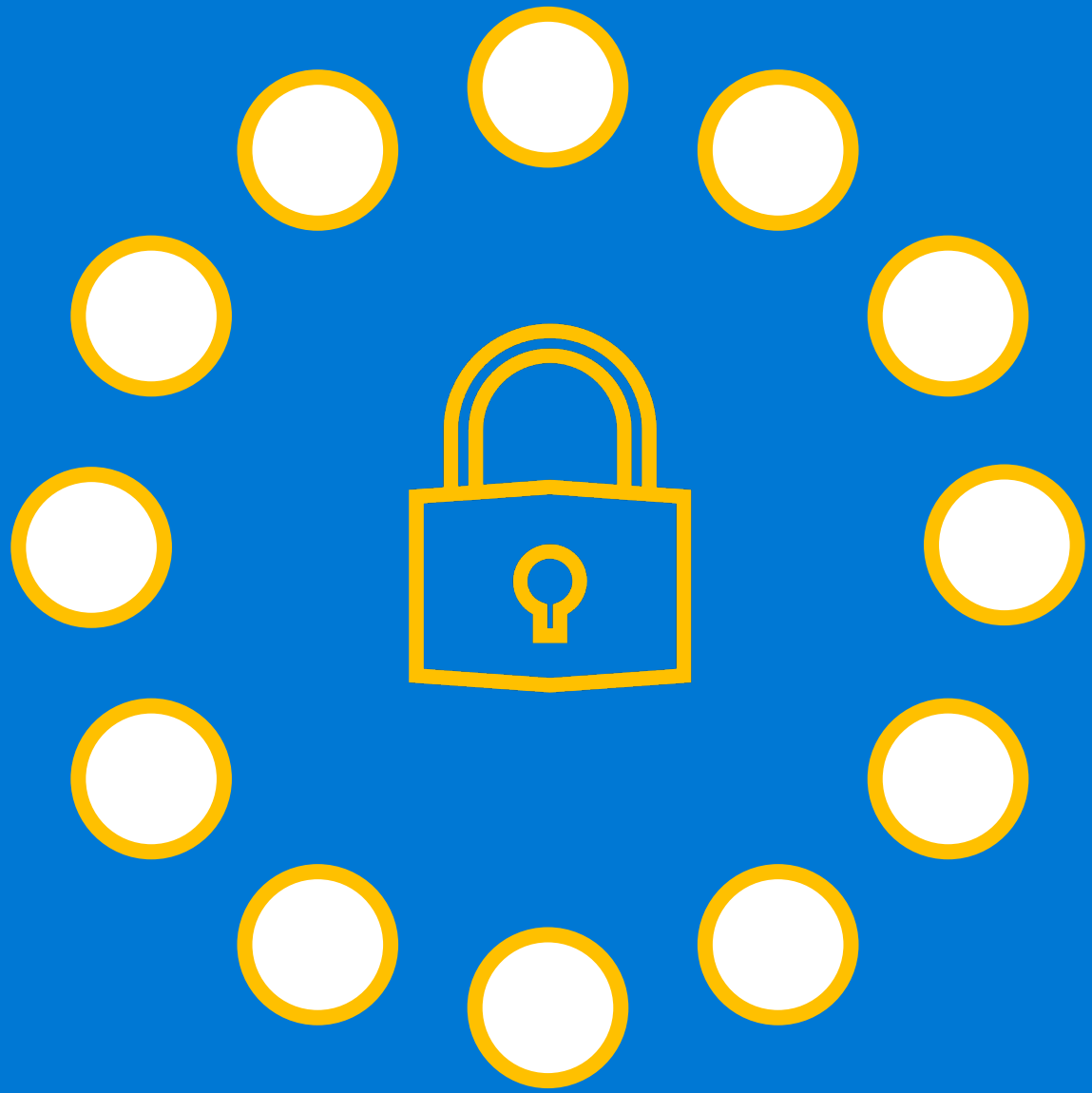
Microsoft

NIS2: vybrané technologie pro zajištění souladu

Dalibor Kačmář

Technologický ředitel

Microsoft



Klíčové vlastnosti NIS2

Komplexní evropská směrnice o kybernetické bezpečnosti

Zdůrazňuje potřebu kybernetické bezpečnosti v dodavatelských řetězcích a vztah mezi společnostmi a přímými dodavateli

Týká se více než 160 000 společností

Stanoví referenční "minimální opatření", včetně posouzení rizik, zásad a postupů pro kryptografii, bezpečnostních postupů pro zaměstnance s přístupem k citlivým datům, vícefaktorové autentizace a školení v oblasti kybernetické bezpečnosti.

Obsahuje pokyny k hlášení incidentů zabezpečení a potenciálních zranitelností

Cílem je harmonizovat požadavky na kybernetickou bezpečnost a prosazování ve všech členských státech

Zahrnuje 15 odvětví, včetně: Energetika, finance, zdravotnictví, doprava a výroba

Dává společnostem pokyn k vytvoření plánu pro řešení bezpečnostních incidentů a řízení obchodních operací během a po bezpečnostním incidentu

Microsoft

Jaké zákonné požadavky zakládá NIS2 pro Microsoft a zákazníky?

Opatření pro řízení rizik kybernetické bezpečnosti

NIS 2 uplatňuje přístup založený na rizicích a zaměřený na výsledky opatření týkající se:

- **(a) analýzy rizik** a **bezpečnostní politiky informačních systémů;**
- (b) řešení **incidentů;**
- **(c) kontinuita činnosti** a řešení krizí**;**
- **(d) bezpečnost dodavatelského řetězce;**
- (e) bezpečnost při **pořizování, vývoji a údržbě** sítí a informačních systémů, včetně řešení **zranitelností** a jejich zveřejňování;
- (f) politiky a postupy pro **posuzování účinnosti** opatření k řízení kybernetických bezpečnostních rizik**;**
- (g) základní **hygienu** a odbornou přípravu v oblasti **kybernetické bezpečnosti;**
- (h) zásady a postupy týkající se kryptografie a **šifrování;**
- **(i) bezpečnost lidských zdrojů**, včetně politik kontroly přístupu a správy aktiv; a
- (j) používání **řešení MFA** nebo průběžného ověřování **(Nulová důvěra)** a dalších technických kontrol

Hlášení incidentů

hlášení "**incidentů, které mají významný dopad na poskytování jejich služeb**" = způsobující **závážné narušení provozu služby** nebo **finanční ztráty; postihující jiné osoby formou značných hmotných nebo nehmotných škod**.

1. **do 24 hodin** předloží příslušnému orgánu "**včasné varování**"
2. **neprodleně** předložit informace o zmírnění a prevenci
3. **do 72 hodin** předložit "**oznámení o incidentu**" (posouzení, závažnost, ukazatele ohrožení)
4. **na žádost** regulační agentury předkládat **průběžné zprávy**
5. **do jednoho měsíce** od počátečního zjištění informací předložit buď **závěrečnou zprávu, nebo zprávu o pokroku**, po níž budou následovat další měsíční zprávy o pokroku až do závěrečné zprávy

Jsme v tom s vámi

Microsoft

Řešení společnosti Microsoft pro soulad s NIS2

Nabízíme komplexní sadu řešení, která vám pomohou splnit požadavky služby NIS 2 a zlepšit stav kybernetického zabezpečení.

Naše řešení pokrývají následující minimální opatření NIS2:

Řešení společnosti Microsoft pro soulad s NIS2

Posouzení rizik: čl. 21, odst. 2a)

Pomocí **Microsoft 365 Compliance Manager a Microsoft Defender for Cloud** můžete vyhodnocovat rizika a dodržovat předpisy. Microsoft 365 Compliance Manager už poskytuje šablony hodnocení s podrobnými doporučeními pro NIS. Šablony hodnocení souladu s NIS2 také brzy poskytneme.

Použití kryptografie: čl. 21, odst. 2h)

Využijte **Microsoft Azure Key Vault a Microsoft Purview** pro bezpečnou správu klíčů a šifrování.

Bezpečnost při pořizování systémů čl. 21, odst. 2e)

Využijte **Microsoft Intune a Endpoint Manager** ke správě zařízení a zajištění nasazení bezpečnostních politik.

Bezpečnostní politiky zaměstnanců čl. 21, odst. 2i)

s přístupem k citlivým nebo důležitým datům: implementujte řešení pro správu identit a přístupu, jako jsou **Azure Active Directory a Privileged Identity Management**, pro řízení přístupu k citlivým datům.

Microsoft Information Protection včetně **Data Loss Prevention** může pomoci chránit data a omezit způsob jejich použití. Kromě toho může **Microsoft Insider Risk Management** pomoci detekovat rizikové chování insiderů a sledovat jejich chování.

Více-faktorové ověřování: čl. 21, odst. 2j)

Pomocí **Azure Active Directory Multi-Factor Authentication** můžete přidat další vrstvu zabezpečení pro přihlášení uživatelů.

Řešení společnosti Microsoft pro soulad s NIS2

Zásady a postupy: čl. 21, odst. 2f)

pro vyhodnocení efektivity bezpečnostních opatření: **Microsoft Defender** a **Azure Sentinel** vám pomůžou monitorovat a detekovat bezpečnostní hrozby v reálném čase.

Plán pro řešení bezpečnostních incidentů: čl. 21, odst. 2b); čl. 23

Service Health, Microsoft Information Protection, včetně **Data Loss Prevention** a **Microsoft Insider Risk Management** poskytuje vlastní zobrazení pro správu výstrah a incidentů.

Školení kybez a praxe pro základní počítačovou hygienu: čl. 20, odst. 2); čl. 21, odst. g)

Využijte **Microsoft Learn** a **Microsoft Defender for Office 365** ke vzdělávání zaměstnanců o osvědčených postupech v oblasti kybernetické bezpečnosti.

Plán řízení obchodních operací během a po bezpečnostním incidentu: čl. 21, odst. 2c)

Pomocí služby **Microsoft Azure Site Recovery** and **Backup** můžete zajistit kontinuitu podnikových procesů v případě bezpečnostního incidentu.

Bezpečnost dodavatelských řetězců a vztah mezi společností a přímým dodavatelem: čl. 21, odst. 2d)

Pomocí **Microsoft Defender 365** můžete zabezpečit svá zařízení a síť před útoky dodavatelského řetězce.

Posouzení rizik

NIS2: politika analýzy rizik a politika bezpečnosti informačních systémů

Compliance Manager

Průběžné posouzení rizik
Inteligentní skóre odráží vaši situaci souladu vzhledem k regulaci a standardům

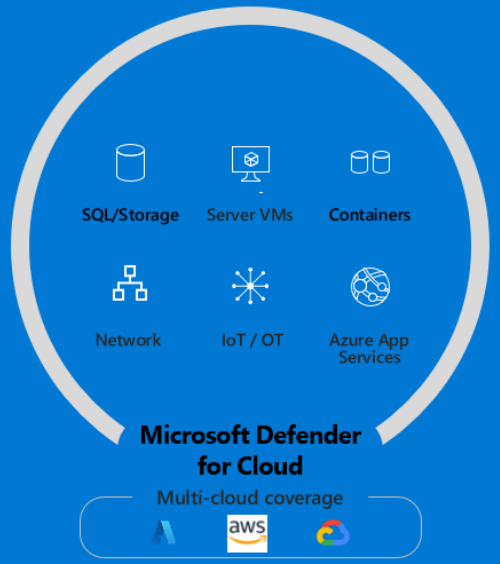
Akční pohledy
Doporučení akce pro zvýšení ochrany data

Zjednodušený soulad
Jednoduché workflow napříč týmy a bohaté detailní reporty pro přípravu auditu

Microsoft Defender for Cloud

Správa zranitelností
Průběžné monitorování zranitelností a chybných konfigurací, včetně prioritizace mitigace zranitelností

Multiplatformní podpora
Není omezeno pouze na Microsoft cloud (Azure), ale integruje se i prostředím Google (GCP) a Amazon (AWS)



Použití kryptografie

NIS2: politiky a postupy týkající se používání kryptografie a případně šifrování

Azure Key Vault

Bezpečné uložení a správa šifrovacích klíčů
Možnost uložení klíčů a provádění kryptografických operací v hardwarových šifrovacích modulech (HSM)

Podpora bezpečných šifrovacích algoritmů
Soulad s doporučeními pro šifrovací algoritmy vydávané NÚKIB

Integrace s on-premise HSM moduly
Pro naplnění nejvyšších požadavků na klíčové hospodářství je možnost integrace s on-premise HSM a implementace BYOK.

Microsoft Purview

Štítkování a šifrování v SaaS službách
Štítkování informací a jejich šifrování v SaaS službách podle organizačních politik

Dvojité šifrování pro vyšší bezpečnost
Víceúrovňové šifrování pro nejvyšší úroveň ochrany informací s kontrolou mimo prostředí cloudu

Šifrování informací a videokonferencí
Šifrování informací, nikoli úložišť zajistí ochranu nezávisle na jejich uložení. Podpora E2EE šifrování videokonferencí.

Šifrování v úložišti	Šifrování při přenosu	Šifrování při použití

Plán pro řešení bezpečnostních incidentů

NIS2: Oznamovací povinnosti a řešení incidentů

Service Health

Jednotné místo pro notifikace & reporty
Jedno místo pro oznámení o kybernetických incidentech ve všech typech služeb (IaaS, PaaS, SaaS). Uveřejňování Post Incident Reportů

Bezpečnostní incidenty i notifikace o změnách
Notifikace o technických změnách nebo údržbě, které by mohly mít vliv na dostupnost nebo funkčnost služby

Role a integrace s externími systémy
Rozdělení odpovědností za zpracování notifikací
Integrace do stávající systémů a automatizace zpracování

DLP a Insider Risk Management

Identifikace interních rizik
Identifikace a hodnocení signálů z Office, Windows a Azure – soubory, komunikace a abnormální chování

Ošetření častých scénářů
Krádeže IP, narušení důvěrnosti, potenciální porušení bezpečnosti

Ochrana proti úniku citlivých dat
Dobře nastavené DLP politiky brání úniku citlivých dat (incident) a působí i jako vzdělávací nástroj pro koncové uživatele

Školení kybernetické bezpečnosti a praxe pro základní počítačovou hygienu

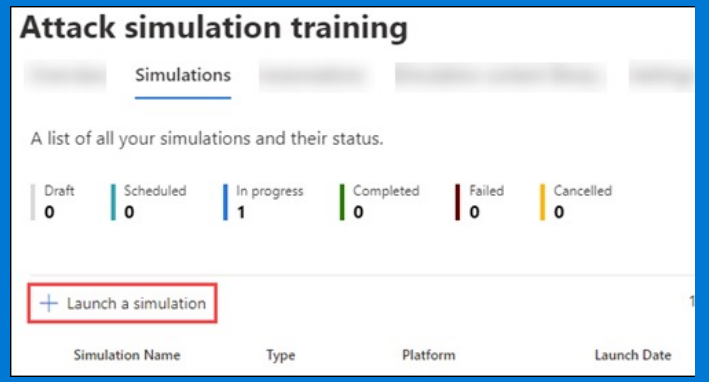
NIS2: - členové řídících orgánů základních a důležitých subjektů musí absolvovat školení
- základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti

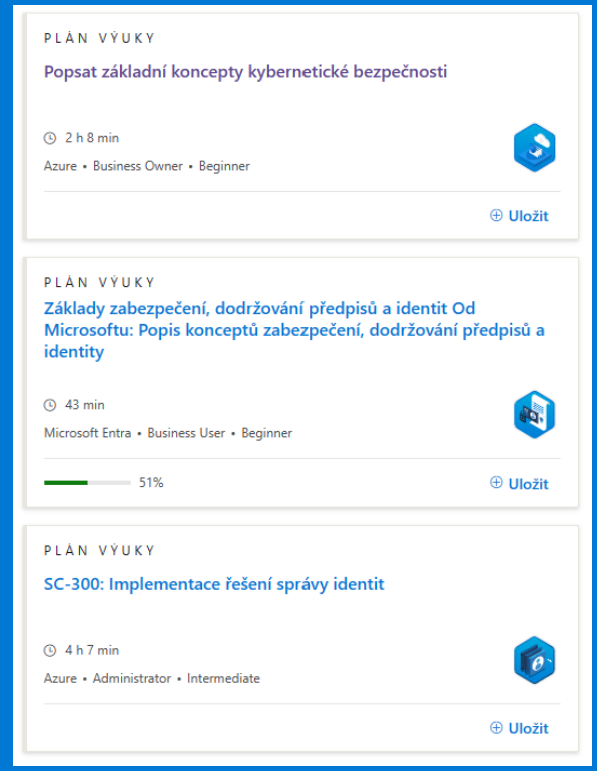
Microsoft Learn & Microsoft 365 Learning Paths

Online vzdělávací kurzy
Dostupné zdarma a jako součást Microsoft 365 Defender. Kurzy dostupné i českém jazyce od naprostých základů až pro profesionály a administrátory

Simulace útoků a phishingových kampaní
Nejlepší znalosti lze získat z reálných (simulovaných) situací, včetně vyhodnocení chování uživatelů.

Příprava na získání certifikací
Slouží k naplnění interních požadavků na pravidelná školení a reakce na simulovaná cvičení až po přípravu na získání certifikací





Zásady a postupy pro vyhodnocování efektivity bezpečnostních opatření

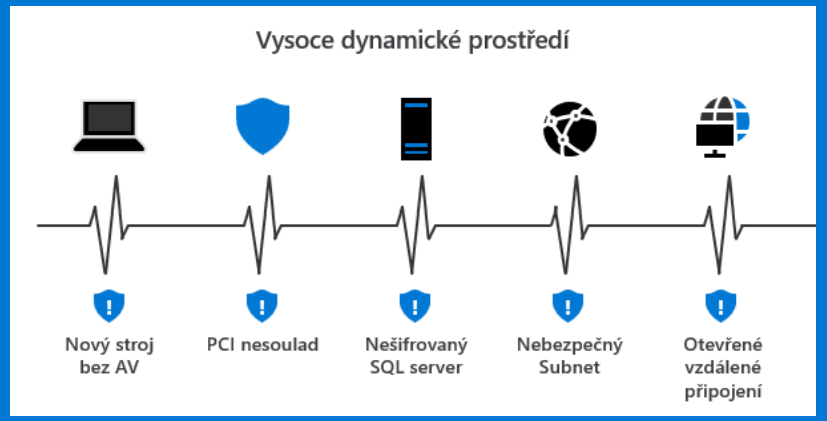
NIS2: politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik

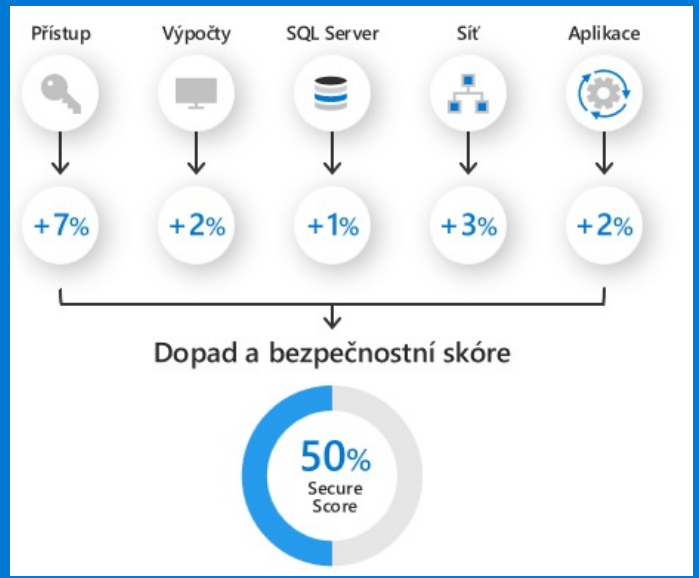
Bezpečnostní skóre

Průběžný pohled na stav bezpečnosti služeb
Inteligentní skóre odráží vaši situaci souladu vzhledem k regulaci a standardům

Řešení zranitelností s prioritizací
Doporučení akce pro zvýšení ochrany data

Vyhodnocení bezpečnostního skóre pro naplnění regulatorních povinností
Jednoduché workflow napříč týmy a bohaté detailní reporty pro přípravu auditu





Jak vám může Microsoft pomoci

V Microsoftu chápeme důležitost kybernetické bezpečnosti a potřebu dodržovat regulační rámce, jako je NIS2

Naše cloudová řešení poskytují bezpečnou a spolehlivou platformu pro správu a zabezpečení vašich dat a systémů

Díky pokročilým funkcím ochrany před internetovými útoky můžete detekovat hrozby a reagovat na ně dříve, než způsobí škodu

Řešení pro správu identit a přístupu zajišťují, že k vašim citlivým datům a systémům mají přístup pouze oprávnění pracovníci

Poskytujeme nástroje a pokyny, které vám pomohou splnit minimální opatření vyžadovaná NIS2, jako jsou posouzení rizik, bezpečnostní postupy a plány reakce na incidenty

Náš tým odborníků na kybernetickou bezpečnost s vámi může spolupracovat na posouzení vašeho současného stavu zabezpečení a vývoji přizpůsobeného plánu zabezpečení, který vyhovuje vašim specifickým potřebám

S nabídkou Microsoftu můžete zajistit vyšší míru souladu, protože víte, že vaše systémy a data jsou chráněny špičkovými řešeními zabezpečení

Microsoft

Další kroky

01 Pokud máte jakékoli dotazy nebo obavy týkající se služby NIS2, neváhejte se obrátit na zástupce společnosti Microsoft.

02 Společnost Microsoft se zavazuje pomáhat svým zákazníkům dosáhnout shody se službou NIS2 tím, že poskytuje pokyny k tomu, jak mohou naše řešení pomoci splnit minimální opatření.

03 Přijměte proaktivní opatření a začněte se připravovat na dodržování NIS2 před termínem 17. října 2024.

04 Využijte služby kybernetického zabezpečení společnosti Microsoft, vyhodnoťte aktuální stav zabezpečení vaší organizace a identifikujte oblasti pro zlepšení.

05 Pokračujte v monitorování aktualizací o transpozici NIS2 a odpovídajícím způsobem upravte strategii kybernetické bezpečnosti vaší organizace.

06 Nezapomeňte, že NIS2 je příležitostí ke zlepšení kybernetické bezpečnosti vaší organizace a ochraně před potenciálními kybernetickými hrozbami. Umožněte Microsoftu, aby byl vaším důvěryhodným partnerem na této cestě k dosažení dodržování předpisů.

Microsoft

dalibor.kacmar@microsoft.com