

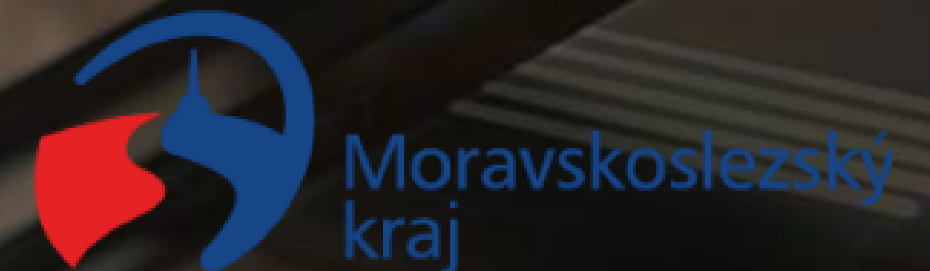
Konference IT4P 2024



Komplexní bezpečnostní ekosystém Microsoft: „Od ochrany po reakci“

2024-12-03 |
@marketingKPCS

Ostrava |



Obsah

- Fakta o KPCS
- Pohled na NIS2
- Další kroky
- Diskuze

Blahoslav Matějka
Key Account Manager KPCS CZ



matejka@kpcs.cz



+420 777 670 228



Fakta o KPCS

Microsoft Partner of the Year



Copilot for Microsoft 365 Jumpstart Partner



Strategické oblasti

kde umíme pomoci

Cloudová/Hybridní infrastruktura

Kybernetická bezpečnost

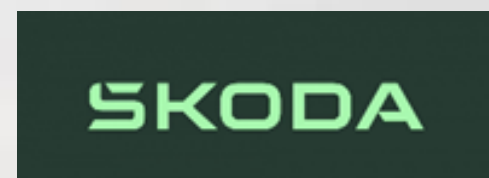
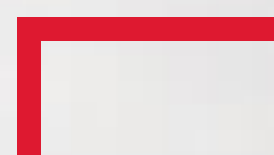
Umělá Inteligence

Automatizace / Služby „As a Service“

Moderní spolupráce

Vybrané reference

Certifikace ISO 9001 | ISO 27001



Draslovka



rockaway



Komplexní bezpečnostní ekosystém Microsoft: Od ochrany po reakci

Soulad a naplnění NIS2

kde pomohou řešení Microsoft

- Využijte co již máte, co používáte, co znáte.
- Komplexní sada řešení, které vám pomohou splnit požadavky služby NIS 2 a zlepšit stav kybernetického zabezpečení.

Řešení pokrývají tyto vybraná minimální opatření NIS2:

Vybraná řešení 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 **Entra ID 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 **Entra Multi-Factor Authentication** můžete přidat další vrstvu zabezpečení pro přihlášení uživatelů.

Vybraná řešení 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 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 společnostmi a přímým dodavatelem: čl. 21, odst. 2d)

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

Vybraná řešení pro soulad s NIS2

Posouzení rizik

NIS2: politika analýzy rizik a politika bezpečnosti informačních systémů

Microsoft Purview Compliance Manager

Microsoft Defender for Cloud



Průběžné posouzení rizik

Inteligentní skóre odráží vaši situaci souladu vzhledem k regulaci a standardům



Správa zranitelností

Průběžné monitorování zranitelností a chybných konfigurací, včetně prioritizace mitigace zranitelností



Akční pohledy

Doporučení akce pro zvýšení ochrany data



Multiplatformní podpora

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



Zjednodušený soulad

Jednoduché workflow napříč týmy a bohaté detailní reporty pro přípravu auditu

Vybraná řešení pro soulad s NIS2

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



Dvojitě 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.

Vybraná řešení pro soulad s NIS2

Plán pro řešení bezpečnostních 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 stávajících systémů a automatizace zpracování

NIS2: Oznamovací povinnosti a řešení incidentů

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

Jak vám může KPCS pomoci

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

Navrhovaná 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.

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

Tým odborníků KPCS 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 KPCS můžete zajistit vyšší míru souladu, protože víte, že vaše systémy a data jsou chráněny špičkovými řešeními zabezpečení.

Vybraná řešení pro soulad s NIS2

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





The Digital
Enablers

Touch the future. #DigitalOrganization



www.kpcs.cz

powered by  KPCS