HartSOFT

Microsoft Solutions Partner
Modern Work

Kybernetická bezpečnost v kostce

Aktuální hrozby pohledem NÚKIB

Praktická opatření pro veřejnou správu

Klára Šašková, CCISO, CHFI, CEH, ISMS Certified Lead Auditor

Agenda

1. Co je kybernetická bezpečnost?
2. Legislativní rámec
3. Nejčastější útoky
4. Bezpečnost v Microsoft 365
5. Přehled minimálních KYBE opatření

Co je kybernetická bezpečnost?

Pro úřady, obce, kraje a příspěvkové organizace je kybernetická bezpečnost **zákonnou povinností i každodenní praxí**. Chrání osobní údaje občanů v agendových systémech (RPP, ISDS, CzechPOINT, spisová služba) a zajišťuje kontinuitu veřejných služeb.

Incident v úřadu dopadá přímo na občana > nemůže se dovolat na matriku, získat výpis z katastru, podat žádost o dávku…

Důvěrnost

Data jsou přístupná pouze oprávněným osobám a systémům.

Integrita

Data nejsou neoprávněně měněna, poškozena ani zfalšována.

Dostupnost

Systémy a data jsou přístupné vždy, když je uživatel legitimně potřebuje.

95 % útoků uspěje díky lidské chybě.

Nejúčinnější obranou je proškolený zaměstnanec, ne pouze nákladná technologie.

Legislativní rámec v České republice

Veřejná správa v ČR musí dodržovat závazné právní předpisy v oblasti KYBE. Nedodržení povinností může vést nejen k sankcím, ale hlavně k reálným bezpečnostním incidentům s dopadem na občany a chod úřadů.

Zákon č. 264/2025 Sb. (ZKB)

Původní zákon č. 181/2014 Sb. byl nahrazen novým zákonem č. 264/2025 Sb. o kybernetické bezpečnosti. Byl vyhlášen ve Sbírce zákonů dne 4. 8. 2025 a nabyl účinnosti 1. 11. 2025.

Sankce a související povinnosti

Pokuty za porušení v řádu milionů korun, dozor vykonává NÚKIB. Povinnost hlásit kybernetický bezpečnostní incident bezodkladně.
Vedle ZKB platí také GDPR: únik osobních údajů znamená dvojí ohlašovací povinnost.

Rozsah, režimy a prováděcí předpisy

Krajské úřady, nemocnice a větší příspěvkové org. zpravidla spadají do režimu vyšších povinností; menší obce a poskytovatelé do režimu nižších povinností. Vyhlášky č. 409/2025 Sb. a 410/2025 Sb. upravují bezpečnostní opatření.

Z praxe

Často se na nás obrací zákazníci, kteří pod zákon vůbec nespadají, ale řeší KYBE proaktivně, a jsou paradoxně mnohem dál než někteří povinní.

Kdo za co zodpovídá?

Kybernetická bezpečnost není výhradně věcí IT oddělení. Odpovědnost je sdílena napříč celou organizací. Jasné vymezení rolí je základním požadavkem zákona č. 264/2025 Sb. i vyhlášky NÚKIB.

Vedení / Ředitel

Odpovědnost za zavedení a financování ISMS. Schvaluje bezpečnostní politiku, jmenuje osobu pověřenou KB, rozhoduje o investicích do bezpečnosti a nese právní odpovědnost za plnění povinností plynoucích ze ZKB.

Bezpečnostní manažer

Zpracovává dokumentaci, řídí ISMS, koordinuje hlášení incidentů NÚKIB, zajišťuje soulad se ZKB (GDPR), provádí hodnocení rizik a komunikuje s auditory.

IT správce

Implementuje technická opatření: MFA, segmentace sítě, zálohy, antivirus/EDR, aktualizace systémů. Monitoruje logy a bezpečnostní události. Spolupracuje s BM na reakci na incidenty.

Každý zaměstnanec

Dodržuje bezpečnostní pravidla, nezveřejňuje přihlašovací údaje, rozpoznává podezřelé emaily a hlásí incidenty nadřízenému nebo IT oddělení. **Je první i poslední linií obrany.**

Phishing

Phishing je forma sociálního inženýrství, při níž se útočník vydává za důvěryhodnou instituci (banku, úřad nebo IT oddělení) a snaží se přimět oběť k prozrazení přihlašovacích údajů nebo kliknutí na škodlivý odkaz.
Veřejná správa je častým cílem cílených kampaní označovaných jako **spear phishing**.

Jak phishing poznat?

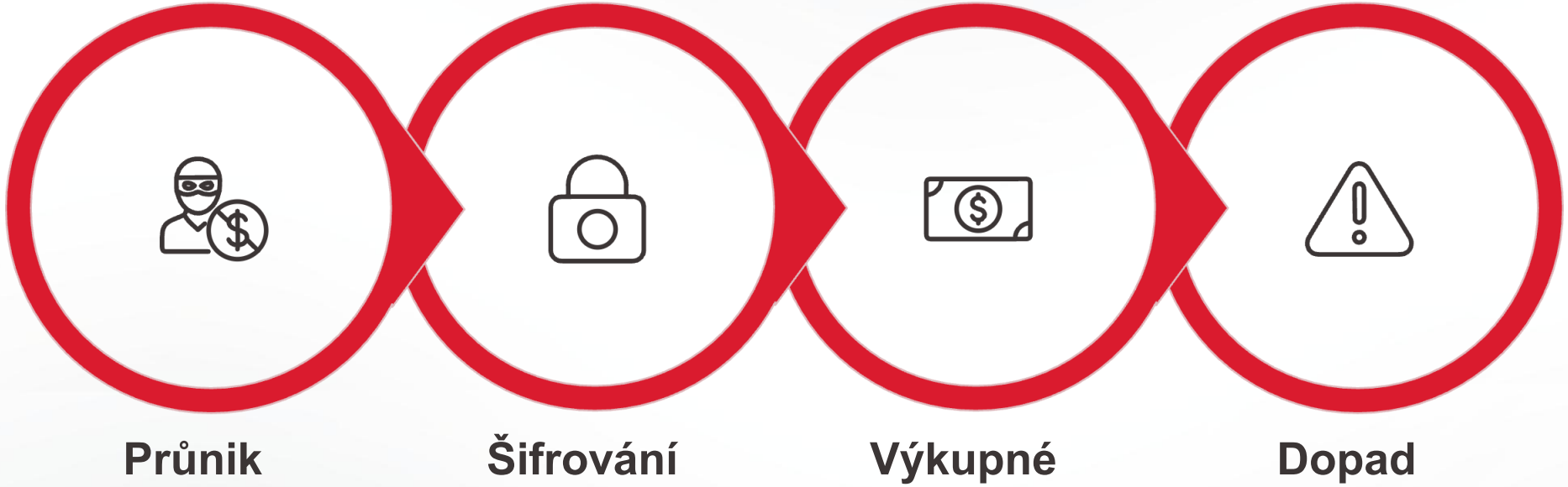
- Podvodný e-mail od „IT podpory" nebo „datové schránky”.
- Naléhavá výzva: „Váš účet bude zablokován do 24 hodin”.
- Odkaz vedoucí na falešnou přihlašovací stránku.
- Příloha s makry nebo spustitelným škodlivým kódem.
- Podezřelá emailová adresa odesílatele (doména nesedí).

Jak se bránit?

- Vícefaktorové ověřování (MFA) v Microsoft 365.
- Microsoft Defender pro Office 365 > filtrování příloh a odkazů.
- Pravidelná školení zaměstnanců včetně simulací phishingu.
- Ověření odesílatele před kliknutím na jakýkoliv odkaz.
- Nastavení DMARC/DKIM/SPF pro ochranu domény úřadu.

Ransomware

Ransomware zašifruje data oběti a za jejich obnovení požaduje výkupné, obvykle v kryptoměně. Pro veřejnou správu představuje zásadní hrozbu: může paralyzovat provoz úřadu a znemožnit přístup ke spisové službě, registrům i komunikaci s občany. **NÚKIB platbu nedoporučuje** > nezaručuje obnovu dat a financuje další útoky.



NÚKIB Q4 2025: Aktivní ransomware gangy Qilin, Inc. Ransom, Warlock, J Group a Obscura.
Cíle: zdravotnictví, vzdělávání a veřejný sektor.
Obranou jsou offline zálohy, pravidelné aktualizace, EDR a MFA.

Sociální inženýrství, BEC a insider threat

Útočníci zneužívají lidskou psychologii (strach, zvědavost nebo respekt k autoritě), aby získali přístup k systémům bez nutnosti technického hackingu. **Nejnebezpečnější útoky necílí na software, ale na lidi.**

Sociální inženýrství

- **Vishing:** útočník po telefonu vyláká hesla či kódy..
- **Pretexting:** předstíraná role (kolega, auditor, IT) získá přístup.
- **Baiting:** podstrčené USB nebo odkaz spustí škodlivý kód.

Business Email Compromise

- Útočník se vydává za starostu, tajemníka nebo ředitele.
- Naléhavá žádost o převod peněz nebo změnu účtu dodavatele.
- Škody v řádu statisíců až milionů korun.

Insider Threat

- Záměrné nebo neúmyslné vyzrazení dat vlastním zaměstnancem.
- Zneužití privilegovaného přístupu k systémům.
- Ochrana: Purview DLP, audit logů, PIM v Entra ID.

Z praxe: Nejúspěšnější útoky neprolomí firewall, proklouznou přes telefonát/mail „z IT". Pomáhá jednoduché pravidlo: „Když mě někdo pod tlakem nutí kliknout nebo nadiktovat kód, zavolám zpátky na ověřené číslo." Funguje to lépe než hodina školení.

Příklady z praxe v ČR

Uvedené příklady vycházejí z reportů NÚKIB, veřejně dostupných zdrojů a našich zkušeností z praxe.

Hasičský záchranný sbor ČR (2025): Ransomware

Ransomware útok na systémy Hasičského záchranného sboru ČR z března 2025 byl jedním z nejzávažnějších kybernetických incidentů ve veřejném sektoru v roce 2025.

Kdy a kde

Pondělí **24. 3. 2025**: HZS Královéhradeckého a Zlínského kraje. NÚKIB klasifikoval incident jako „velmi významný", tedy nejvyšší kategorii závažnosti.

Bezprostřední dopady

Napadená pracoviště byla okamžitě odpojena od společné sítě a byl zaveden náhradní způsob komunikace. Akceschopnost záchranných složek zůstala zachována jen díky rychlé reakci.

Širší kontext Q1/2025

Celkem **48 incidentů** v Q1/2025, z toho **10 ransomware** (6 pouze v březnu 2025). Zájem útočníků o kritickou infrastrukturu a záchranné složky výrazně roste.

Zdroj

NÚKIB Q1/2025

Ministerstvo vnitra ČR (2025): Kybernetický útok

V červenci 2025 ministerstvo vnitra ČR detekovalo kybernetický útok na jeden ze svých systémů, který byl následně odpojen od sítě. Tehdejší ministr vnitra Vít Rakušan incident potvrdil na tiskové konferenci 10. července 2025.

Co se stalo

10. 7. 2025 ministr Rakušan oznámil závažný incident. Útočník pronikl jedním kanálem, který byl okamžitě odpojen. Nešlo o ransomware.

Reakce a vyšetřování

Osobní data ani utajované informace neunikly.
Volební systémy ani kritická infrastruktura nezasaženy.
Jednou z variant je zapojení cizí státní moci.

Širší kontext

Druhý velký útok na české ministerstvo v roce 2025 > v květnu vláda atribuovala útok na MZV ČR čínské skupině APT31 (od 2022).

Zdroj

ČT24, 10. 7. 2025

Příklady z let 2024-2026: Ransomware na samosprávy

V letech 2024-2026 opakovaně zasáhly útoky ransomware českou veřejnou správu i kritickou infrastrukturu.
Největší rizika podstupují obce bez vlastního IT týmu a bezpečnostního oddělení.

Praha - Správa služeb (2024)

Gang Cicada3301 odcizil cca **200 GB dat**. Útok zasáhl příspěvkovou organizaci hlavního města. Ukázka rizika i pro velké organizace s IT zázemím.

Mapové portály samospráv (únor 2026)

NÚKIB evidoval **23 incidentů** (polovina kategorie Průnik) které cílily na mapové portály obcí a měst, slabě zabezpečené systémy vystavené do internetu.

Z praxe

Známe případ subjektu kritické infrastruktury, který má „super dodavatele“, který dodal kompletní portfolio nástrojů, většina z nich však reálně nechrání. Při ransomwarovém útoku organizace padne. **Bezpečnost nevzniká nákupem licencí ani množstvím nástrojů**, ale jejich správným nasazením, konfigurací a průběžnou kontrolou.

Zdroje

NÚKIB Q4/2025

NÚKIB Q1/2026

Olomouc - Magistrát města (duben 2021)

V dubnu 2021 zasáhl datovou síť olomouckého magistrátu masivní ransomwarový útok skupiny **Avaddon**. Útočníci požadovali výkupné 100 000 USD, město odmítlo zaplatit a obnovilo systémy vlastními silami.

Co se stalo

7.4. 2021 útočníci zašifrovali data magistrátu ransomwarem **Avaddon**. Pronikli přes zranitelný veřejně dostupný prvek sítě a získali administrátorské heslo. Požadovali výkupné ve výši 100 000 USD v kryptoměně.

Reakce a vyšetřování

Město **odmítlo zaplatit**, podalo trestní oznámení a informovalo NÚKIB. Jen IT obnova trvala několik týdnů a stála téměř 1 milion Kč. Případ vyšetřovala policie ve spolupráci s NÚKIB, VŠB-TU Ostrava a Europolem.

Širší kontext

Po odmítnutí výkupného následovala **odveta**, DDoS útok na web města a zveřejnění části dat na dark webu. Pachatel ze zahraničí nebyl identifikován, případ policie odložila v únoru 2022.

Zdroje

iROZHLAS, 22. 5. 2021

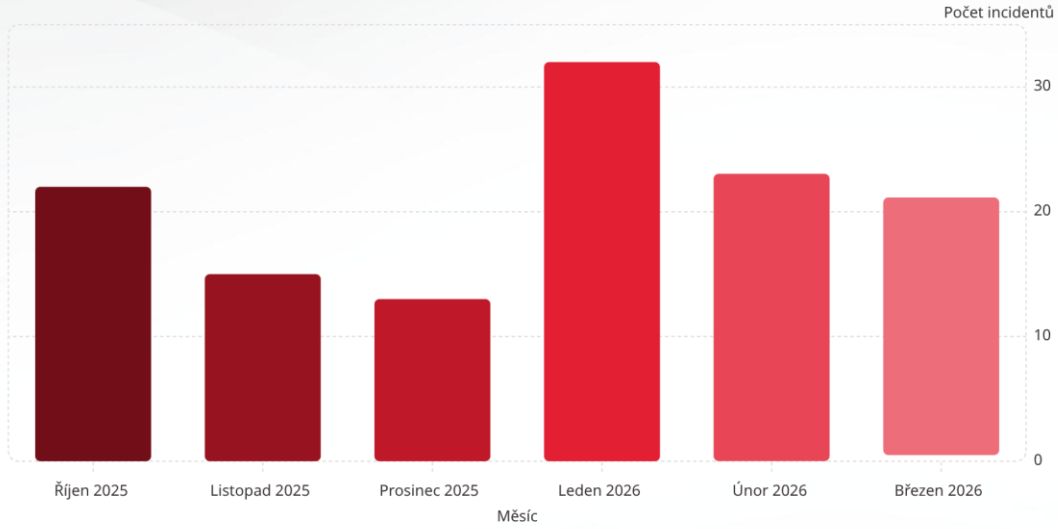
Novinky.cz, 17. 2. 2022

DataBreaches.net

Aktuální statistika NÚKIB (Q4 2025 - Q1 2026)

Q4 2025 přehled:

- 50 incidentů celkem (říjen 22, listopad 15, prosinec 13).
- Pokles DDoS na čtvrtinu oproti Q3 > pouze 5 útoků.
- Nejčastější: ransomware a provozní výpadky systémů.
- Aktivní gangy: Qilin, Inc. Ransom, Warlock, J Group, Obscura.
- Cíle: zdravotnictví, vzdělávání, veřejný sektor.



Q1/2026 přehled:

- Přes 70 incidentů (leden 32, únor 23, březen 20).
- 7 významných incidentů, primárně státní instituce.
- Leden: vlna DDoS proruských hacktivistů (NoName057, ServerKillers).
- Únor a březen: kategorie Průnik 48 % a 55 % všech útoků.

Trend: 3 měsíce v řadě bez ransomwaru u subjektů vyšších povinností. Útoky se přesouvají na samosprávy a poskytovatele v nižším režimu.

Bezpečnost v Microsoft 365

Nástroje a služby v ekosystému Microsoft 365, které organizacím pomáhají posílit kybernetickou bezpečnost.

Microsoft 365 jako bezpečnostní platforma

Microsoft 365 není jen kancelářský balík, ale komplexní bezpečnostní ekosystém. Nabízí nástroje, které pokrývají celý životní cyklus ochrany: od prevence přes detekci až po reakci na incidenty.

Microsoft Defender

Detekce a ochrana koncových bodů, emailů a identit v reálném čase pomocí AI.

Microsoft Entra ID

Správa identit a přístupů, MFA, podmíněný přístup a Privileged Identity Management.

Microsoft Purview

Klasifikace dat, DLP, šifrování a auditní záznamy pro plnění GDPR a ZKB požadavků.

Microsoft Sentinel

SIEM/SOAR sbírá logy a automatizuje řešení incidentů.

Vícefaktorové ověřování (MFA): první linie obrany

MFA je jedním z nejúčinnějších opatření proti neoprávněnému přístupu. Podle statistik Microsoft MFA blokuje více než **99,9 % automatizovaných útoků na účty**.

Jak MFA funguje v Microsoft 365?

- Heslo + ověřovací aplikace **Microsoft Authenticator**.
- Heslo + SMS kód (méně bezpečné, ale lepší než samotné heslo).
- Podmíněný přístup: MFA se vyžaduje při přihlášení z neznámého zařízení.
- Security Defaults: základní ochrana zdarma pro všechny plány M365.

Tři kroky k aktivaci MFA

1. **Nastavit Authenticator** > konfigurujte Microsoft Authenticator pro všechny uživatele.
2. **Povolit Security Defaults** > aktivujte je v portálu Entra ID.
3. **Otestovat a proškolit** > ověřte funkčnost a seznamte uživatele s novým postupem přihlášení.

Z praxe: Zákazníci, kteří MFA nasadili, jsou klidnější, eliminovali přístupy bez kontroly. Přihlášení trvá o 3 vteřiny déle. Incident může ochromit organizaci na měsíce.

Ochrana emailu a obrana proti phishingu

Email zůstává nejčastějším vstupním bodem kybernetických útoků. Microsoft 365 nabízí vícevrstvou ochranu.

1

Exchange Online Protection

Základní filtrace spamu, malwaru a podvodných emailů. Součást všech plánů Microsoft 365 bez příplatku.

2

Bezpečné přílohy

Každá příloha se před doručením do schránky otevírá v izolovaném prostředí (sandboxu) a kontroluje na přítomnost malwaru.

3

Bezpečné odkazy

Odkazy v emailech se přepisují a při každém kliknutí jsou v reálném čase znovu prověřeny vůči databázi hrozeb.

4

DMARC / DKIM / SPF

Ochrana proti spoofingu domény úřadu a ověřování identity odesílatelů. Zabraňuje zneužití vaší domény k phishingu.

Ochrana dat, dokumentů a spisová služba

Pro veřejnou správu je ochrana úředních dokumentů, osobních údajů i obsahu spisové služby klíčová. Atestovaný elektronický systém spisové služby (např. GINIS, e-spis) zajišťuje výkon spisové služby podle zákona č. 499/2004 Sb o archívnictví a spisové službě., zatímco nástroje Microsoft 365 a Microsoft Purview mohou doplňkově chránit pracovní dokumenty a osobní údaje v běžné kancelářské agendě před jejich vložením do eSSL.

Microsoft Purview - ochrana informací

- Automatická klasifikace dokumentů (Důvěrné, Interní, Veřejné).
- Šifrování dokumentů i při externím sdílení
- (DLP - prevence odeslání citlivých dat emailem nebo na USB).
- Audit trail - kdo, kdy a jak s dokumentem pracoval.

Propojení se spisovou službou

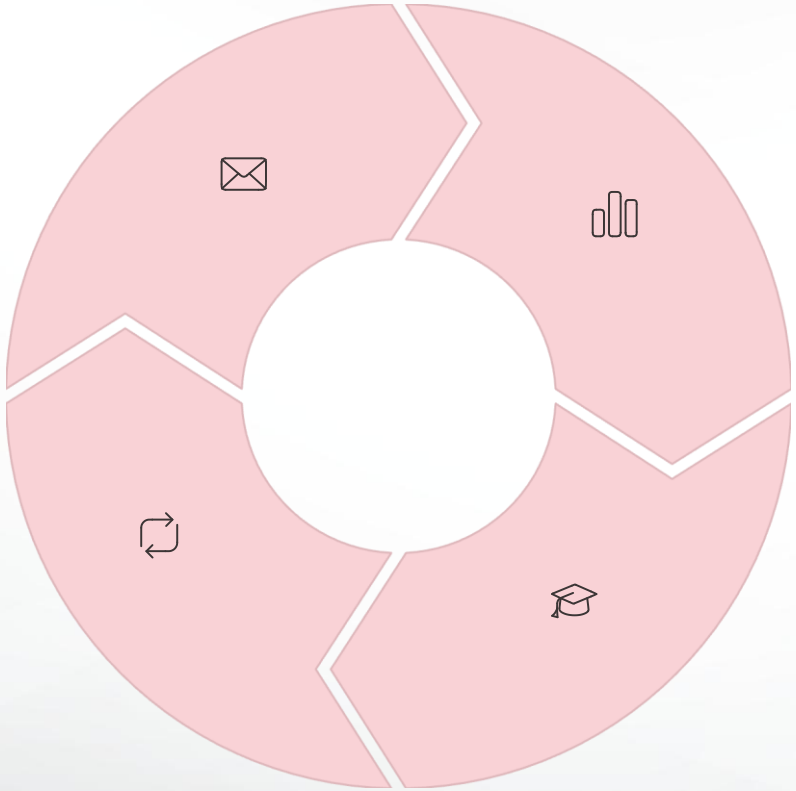
Microsoft Purview lze nasadit vedle atestované eSSL a doplnit tak požadavky zákona č. 499/2004 Sb., o archivnictví a spisové službě, o cloudovou ochranu dat a řízení jejich životního cyklu.

Vzdělávání a simulace phishingu

Technická opatření jsou nezbytná, ale sama o sobě nestačí. Zaměstnanci jsou první i poslední linií obrany. Nástroj **Attack Simulator** (součást Defenderu for Office 365 Plan 2), který umožňuje realisticky simulovat phishingové kampaně přímo ve vaší organizaci.

Simulace útoku

Rozesílání realistických phishingových emailů zaměstnancům.



Měření výsledků

Přehled o tom, kdo klikl, zadal údaje nebo naopak správně nahlásil pokus jako podezřelý.

Pravidelné opakování

Opakované kampaně průběžně měří a posilují odolnost celé organizace v čase.

Cílené školení

Automatické přiřazení e-learningového modulu zaměstnancům, kteří simulaci neodhalili.

Přehled minimálních KYBE opatření

Nemusíte mít všechno hned. Začněte třemi věcmi: MFA, zálohy off-line, plán co dělat když. To zvládne každá organizace, a díky tomuto minimu může pokrýt většinu reálných scénářů.
Prevence je vždy levnější než náprava.

1. Organizace a lidé

- Určit osobu pověřenou kybernetickou bezpečností.
- Vést dokument „Přehled bezpečnostních opatření".
- Proškolit vedení a všechny uživatele v KYBE.
- Ošetřit smlouvy s dodavateli (SLA, bezpečnostní požadavky).

2. Technika a přístupy

- Vícefaktorová autentizace (MFA) v definovaném rozsahu.
- Řízení privilegovaných účtů a princip nejmenších oprávnění.
- Segmentace sítě, aktualizace systémů, antivirus/EDR.
- Nikdy nevystavovat vzdálenou správu do internetu.

3. Kontinuita a incidenty

- Pravidelné offline zálohy a otestovaná obnova dat.
- Plán řešení incidentů a komunikační postupy.
- Hlášení incidentů přes Portál NÚKIB bezodkladně.
- Kryptografická ochrana komunikace a citlivých dat.

HartSOFT: Váš partner pro kybernetickou bezpečnost

HartSOFT poskytuje komplexní služby kybernetické bezpečnosti pro samosprávu a státní správu v prostředí Microsoft 365. Zajišťujeme technickou implementaci, školení, průběžný monitoring i správu bezpečnostního prostředí, vše v souladu s platnou legislativou.

Implementace M365 Security

Nasazení a konfigurace Defenderu, Entra ID, Purview a Sentinelu podle potřeb vaší organizace.

Školení a simulace

Phishingové kampaně, e-learning a workshopy pro zaměstnance i vedení organizace.

Průběžný monitoring

Správa bezpečnostních incidentů, aktualizací a pravidelný reporting pro vedení.

Soulad s legislativou

Poradenství a implementace ISMS, ZKB a GDPR pro veřejnoprávní subjekty.

Děkujeme za pozornost

info@hartsoft.cz