Kyberbezpečnost? NIS2? Jak se týká NIS2 přístupových sítí FTTx. Jak si s tím poradí ISP a provozovatelé sítí? Kyberbezpečnost komunikačních technologií od přenosového média po aplikační vrstvu.

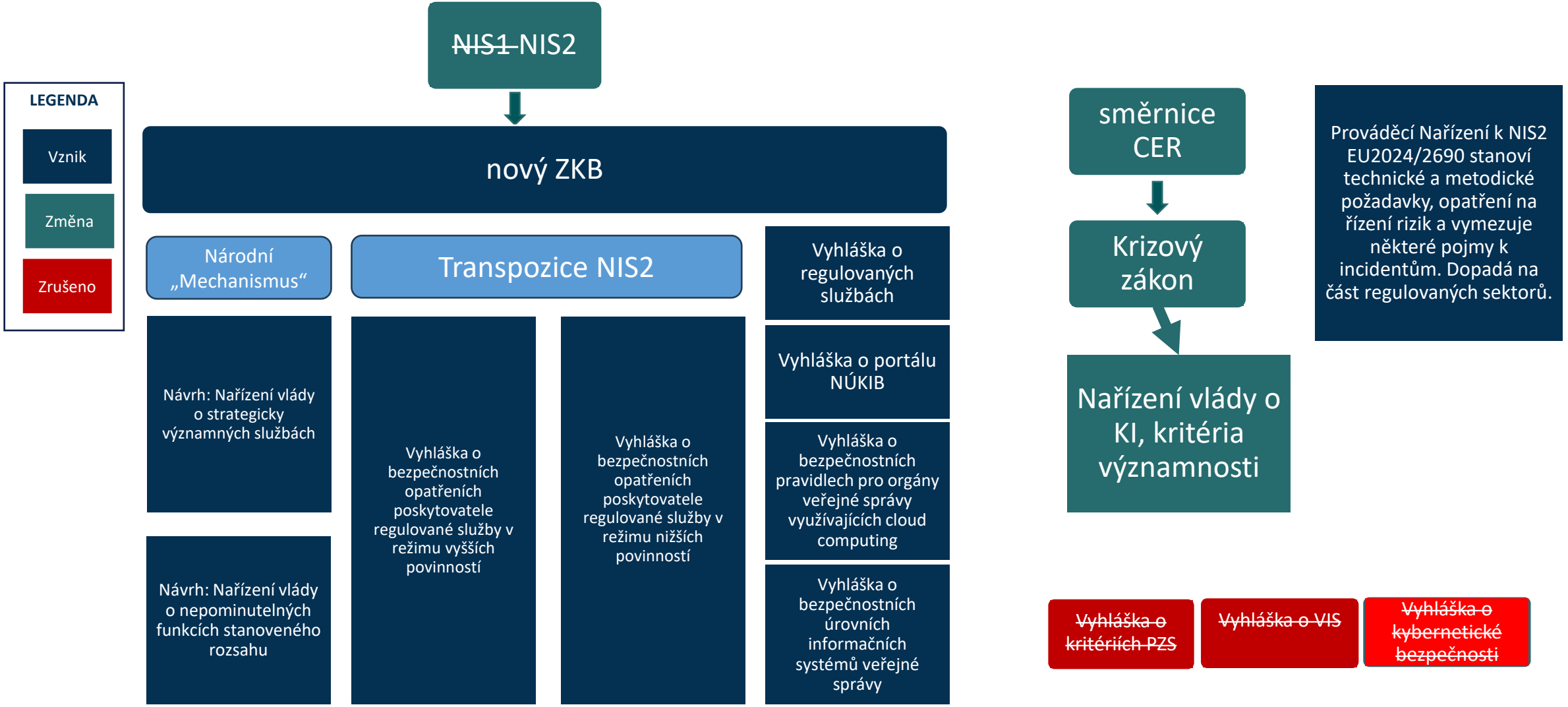
Mgr. Jakub Rejzek, MBA, LL.M.

Výbor Nezávislého ICT průmyslu

Nový Zákon o kybernetické bezpečnosti

Od 1. listopadu 2025 platí nový Zákon o kybernetické bezpečnosti, 264/2025 Sb.

Aktuální stav legislativy + co bylo zrušeno:



Výbor Nezávislého ICT průmyslu

Koho se nové povinnosti týkají dle směrnice NIS 2

Regulované služby uvedeny v přílohách směrnice NIS 2 rozšířené ve Vyhlášce o regulovaných službách z 18 na 22 sektorů.

Kybernetickou bezpečnost má být zajištěna např.

- při výrobě elektřiny,
- poskytování zdravotní péče,
- poskytování služeb elektronických komunikací,
- u dalších více než **60 služeb zařazených do ~~18~~ 22 odvětví**

Směrnice NIS2 nepředpokládá ukládání povinností každému subjektu, který danou službu poskytuje (viz čl. 2 směrnice NIS2 – zejm. s ohledem na kritérium velikosti podniku).

Mechanismus prověřování bezpečnosti dodavatelského řetězce podle (Díl 5 nZKB) se týká Digitální infrastruktury, dopravy, energetiky a veřejné správy.

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

NIS2 a Mechanismus

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

Základním kritériem pro posouzení velikosti podnikatele je počet zaměstnanců, velikost ročního obratu a bilanční suma roční rozvahy (velikost aktiv). Údaje, které se mají použít pro stanovení počtu zaměstnanců a finančních veličin, jsou údaje vztahující se k poslednímu uzavřenému zdaňovacímu období vypočtené za období jednoho kalendářního roku.

- Za **drobného, malého a středního podnikatele** se považuje podnikatel, který zaměstnává méně než 250 zaměstnanců a jeho roční obrat nepřesahuje 50 milionů EUR nebo jeho bilanční suma roční rozvahy nepřesahuje 43 milionů EUR.
- V rámci kategorie malých a středních podniků jsou **malé podniky** vymezeny jako podniky, které zaměstnávají méně než 50 osob a jejichž roční obrat nebo bilanční suma roční rozvahy nepřesahuje 10 milionů EUR.
- V rámci kategorie malých a středních podniků jsou **drobní podnikatelé** vymezeni jako podnikatelé, kteří zaměstnávají méně než 10 osob a jejichž roční obrat nebo bilanční suma roční rozvahy nepřesahuje 2 miliony EUR.

Nový Zákon o kybernetické bezpečnosti

Stručný návod – jak na regulovanou službu.

Odkaz na můj drive

- **Jak zjistíte, jestli jste regulovanou osobou podle ZKB?** Vyhláškou o regulovaných službách nás provede Ing. Luděk Nezmar v přednášce *Požadavky směrnice NIS2 a ZKB – jak zjistit, zda se vaše firma stane regulovaným subjektem a pokud ano, jak na vás regulace dopadne?*

- **Kyberbezpečnostní minimum:** pro regulované osoby vycházíme z *Vyhlášky 410/2025Sb. o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.*

Nový Zákon o kybernetické bezpečnosti

§ 3

Systém zajišťování minimální kybernetické bezpečnosti

(1) Povinná osoba při zajišťování kybernetické bezpečnosti

a) zavede a provádí bezpečnostní opatření, která jsou přiměřená bezpečnostním potřebám, a

b) zavede a provádí alespoň bezpečnostní opatření podle odstavců 2 až 6, § 4 až 6 a § 10.

Nový Zákon o kybernetické bezpečnosti

(2) Povinná osoba

a) stanoví přehled bezpečnostních opatření podle přílohy č. 1 k této vyhlášce, který obsahuje přehled všech bezpečnostních opatření, která

1. byla povinnou osobou zavedena, včetně popisu jejich zavedení,
2. budou povinnou osobou zavedena, včetně termínů pro jejich zavedení, priority jejich zavedení a určení osoby odpovědné za jejich zavedení, a
3. nebyla zavedena, včetně odůvodnění jejich nezavedení,

b) provede a dokumentuje alespoň jednou ročně aktualizaci přehledu bezpečnostních opatření, včetně vyhodnocení účinnosti zavedených bezpečnostních opatření,

c) uchovává jednotlivé přehledy bezpečnostních opatření a jejich aktualizace alespoň po dobu 4 let.

Výbor Nezávislého ICT průmyslu

Nový Zákon o kybernetické bezpečnosti

(3) Povinná osoba v rámci řízení bezpečnostní politiky a bezpečnostní dokumentace

a) stanoví bezpečnostní politiku a bezpečnostní dokumentaci k bezpečnostním opatřením požadovaným touto vyhláškou,

b) pravidelně přezkoumává a aktualizuje pravidla a postupy stanovené v bezpečnostní politice a bezpečnostní dokumentaci a

c) vynucuje dodržování pravidel a postupů stanovených v bezpečnostní politice a bezpečnostní dokumentaci.

(4) Povinná osoba v rámci řízení aktiv stanoví pravidla pro používání a manipulaci technických aktiv.

Nový Zákon o kybernetické bezpečnosti

(5) Povinná osoba při uzavírání smlouvy s dodavatelem do stanoveného rozsahu podle § 12 zákona zohlední hrozby a zranitelnosti spojené s tímto dodavatelem, celkovou kvalitu produktů a postupů v oblasti kybernetické bezpečnosti tohoto dodavatele, včetně postupů bezpečného vývoje a na základě toho zajistí, aby smlouvy s tímto dodavatelem obsahovaly relevantní požadavky na smluvní ujednaní uvedené v příloze č. 2 k této vyhlášce.

(6) Povinná osoba v souvislosti s plánovanou akvizicí, vývojem a údržbou technických aktiv stanoví bezpečnostní požadavky v oblasti kybernetické bezpečnosti a vymáhá jejich dodržování, přičemž vychází z požadavků na bezpečnostní opatření podle této vyhlášky.

Nový Zákon o kybernetické bezpečnosti

§ 4

Požadavky na vrcholné vedení

Statutární orgán povinné osoby nebo jiná osoba anebo skupina osob v obdobném řídícím postavení povinné osoby (dále jen „vrcholné vedení“) s ohledem na zajišťování minimální kybernetické bezpečnosti

a) určí osobu pověřenou kybernetickou bezpečností, které svěří pravomoci potřebné k řízení a rozvoji kybernetické bezpečnosti, dohledu nad stavem kybernetické bezpečnosti a komunikaci s vrcholným vedením, přičemž pro výkon této činnosti
    1. absolvuje bez zbytečného odkladu odborné školení podle § 5 odst. 2 písm. d), nebo
    2. prokáže odbornou znalost v kybernetické bezpečnosti,
b) absolvuje prokazatelně školení podle § 5 odst. 2 písm. a),
c) zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření,
d) se prokazatelně seznamuje se stavem plnění bezpečnostních opatření uvedeným v přehledu bezpečnostních opatření podle § 3 odst. 2 písm. a),
e) prosazuje neustálé zlepšování zajišťování kybernetické bezpečnosti a za tímto účelem podporuje osobu pověřenou kybernetickou bezpečností a jiné relevantní osoby a
f) stanoví prioritu obnovy primárních aktiv.

Nový Zákon o kybernetické bezpečnosti

§ 5

Bezpečnost lidských zdrojů

(1) Povinná osoba v rámci bezpečnosti lidských zdrojů

a) stanoví politiku bezpečného chování uživatelů, v jejímž rámci zohledňuje relevantní témata uvedená v příloze č. 3 k této vyhlášce,

b) stanoví pravidla rozvoje bezpečnostního povědomí vrcholného vedení, uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností, včetně pravidel pro tvorbu hesel,

c) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osoby pověřené kybernetickou bezpečností a

d) stanoví pravidla a postupy pro řešení případů porušení bezpečnostní politiky.

(2) Povinná osoba v souladu s pravidly rozvoje bezpečnostního povědomí zajistí

a) poučení vrcholného vedení o jeho povinnostech a o bezpečnostní politice, zejména v oblasti zajišťování kybernetické bezpečnosti, formou vstupních a pravidelných školení,

b) vstupní školení v oblasti kybernetické bezpečnosti,

c) pravidelná školení v oblasti kybernetické bezpečnosti a

d) potřebná odborná teoretická i praktická školení administrátorů a osoby pověřené kybernetickou bezpečností v souladu s jejich pracovní náplní.

(3) Povinná osoba vede přehledy o provedených školeních a seznamy školených osob podle odstavce 2.

Nový Zákon o kybernetické bezpečnosti

§ 6

Řízení kontinuity činností

Povinná osoba v rámci řízení kontinuity činností

a) stanoví prioritu technických aktiv, pořadí a postupy jejich obnovy a zohlední přitom stanovenou prioritu relevantního primárního aktiva podle § 4 písm. f),

b) stanoví povinnosti a odpovědnost konkrétních osob za jednotlivé činnosti pro zajištění kontinuity činností a k obnově podle písmene a) a

c) vytváří pravidelné zálohy informací, dat, konfigurací a nastavení technických aktiv nezbytných zejména pro účely obnovy regulované služby pro případ kybernetického bezpečnostního incidentu.

Jak si s tím poradí ISP a provozovatelé sítí?

§14 odst. (2) Pro poskytovatele regulované služby v režimu nižších povinností jsou organizačními a technickými opatřeními

a) systém zajišťování minimální kybernetické bezpečnosti,
b) požadavky na vrcholné vedení,
c) řízení aktiv,
d) řízení rizik,
e) bezpečnost lidských zdrojů,
f) řízení kontinuity činností,
g) řízení přístupu,
h) řízení identit a jejich oprávnění,
i) detekce a zaznamenávání kybernetických bezpečnostních událostí,
j) řešení kybernetických bezpečnostních incidentů,
k) bezpečnost komunikačních sítí,
l) aplikační bezpečnost a
m) kryptografické algoritmy.

Jak se týká NIS2 přístupových sítí FTTx?

- ochrana **aktivních prvků sítě** (OLT, switche, routery)
- zabezpečení **řízení sítě a NMS systémů**
- řízení přístupů administrátorů
- monitoring a detekce incidentů
- řízení dodavatelského řetězce
- řízení akvizic
- Fyzická bezpečnost

Školení k ZKB pro ISP

Nadcházející události

KAM KRÁČÍ DIGITÁLNÍ SÍTĚ MIKULOV 2026

31. 03. 2026

AKTUÁLNÍ TÉMATA, INOVATIVNÍ PŘÍSTUP, PRAKTICKÉ POHLEDY, BUDOUCNOST TRHU. Chceme být o krok napřed, reagujeme na potřeby trhu a dáváme prostor tomu, co odborná veřejnost skutečně chce slyšet a zažít.

Galant Mikulov****

REGISTROVAT

Certifikační školení k Zákonu o kybernetické bezpečnosti pro ISP

30. 03. 2026

Certifikační školení k Zákonu o kybernetické bezpečnosti proběhne v pondělí 30. března - odpoledne před konferencí KKDS Mikulov. Obdržíte potvrzení o proškolení statutárních zástupců o povinnostech podle ZKB. Registrovat se můžete na webu KKDS Mikulov 2026.

Hotel Galant Mikulov

REGISTROVAT

Děkuji Vám za pozornost.

Mgr. Jakub Rejzek, MBA, LL.M

Výbor nezávislého ICT průmyslu, z.s
jakub.rejzek@vnictp.cz