

Září 2026 - číslo 09



ZPRAVODAJ

Asociace škol kritické infrastruktury

Září 2026

VZDĚLÁVEJTE BEZPEČNOST, CHRAŇTE BUDOUCNOST!
EDUCARE SECURITATEM, CUSTODIRE FUTURUM!



ISSN 3029-6749

Vítejte v našem světě © ASKI...



Vydavatel:

Asociace škol kritické infrastruktury

Revoluční 981, 661 01 Tišnov

Číslo ročníku: 9 (září)

Rok vydání: 2026

Počet stran: 67

Zpravodaj ASKI © 2025 by **Asociace škol kritické infrastruktury, z.s.** is licensed under **Creative Commons Attribution-ShareAlike 4.0 International**

Všechna práva vyhrazena

E-mail: info@aski.cz

www.aski.cz

Redakční rada

PhDr. Mgr. Dušan Kalášek, MBA, LL.M.

Ing. František Vlach, Ph.D., MBA, LL.M.

Bc. Radka Slavíková, MBA, LL.M.

Webarchivováno
Národní knihovnou
ČR

ISSN 3029-6749



OBSAH

Září 2026 jako měsíc vzdělávání, odpovědnosti a české státnosti	5
<i>PhDr. Mgr. Dušan Kalášek, MBA, LL.M.</i>	
Ochrana obyvatelstva a efektivní řízení dobrovolnických zdrojů	12
<i>Pavel Štyndl, CEVRO Univerzita</i>	
Dodavatelský řetězec kritické infrastruktury podle nového zákona o kybernetické bezpečnosti: co musí obsahovat smlouva a jak to doložit	16
<i>Lukáš Medovič, MBA, RAGUARD.CZ</i>	
Úvod k sérii řešerší vystoupení z konference ASKI	19
<i>PhDr. Mgr. Dušan Kalášek, MBA, LL.M., president ASKI</i>	
Legislativní změny v oblasti krizového řízení, kritické infrastruktury a kybernetické bezpečnosti v kontextu školství a vzdělávání	22
<i>PhDr. Mgr. Dušan Kalášek, MBA, LL.M., prezident ASKI</i>	
Školy jako součást kritické infrastruktury: řízení rizik a ochrana osobních údajů v praxi	27
<i>PhDr. Jaroslav Hora, LL.M., ČSÚ</i>	
Krajské vojenské velitelství jako partner škol při implementaci bezpečnostních témat do výuky	31
<i>plk. gšt. Ing. Alois Matýzka, Krajské vojenské velitelství Brno</i>	
Potenciál Národní soustavy kvalifikací pro oblast kritické infrastruktury	34
<i>Mgr. Richard Veleta, Ph.D., NPI ČR, správce Národní soustavy kvalifikací</i>	
Témata ochrany obyvatelstva jako součást RVP	38
<i>Ing. Josef Myslín, Ph.D., Ed.D., MSc., MPA, CEVRO Univerzita</i>	
Kde stojí člověk a kde AI	41
<i>Mgr. Vojtěch Kašpárek MBA</i>	
Umělá inteligence na hranici mezi pomocí a závislostí	43
<i>Dr. Ing. Evžen Šanc</i>	
Budoucnost bezpečnosti začíná v systematické přípravě odborníků	46
<i>Bc. Jaroslav Kocián</i>	





Když se ve škole něco stane	49
<i>Hana Sobotková, BAKALÁŘI software</i>	
VOŠ Kybernetická bezpečnost pro kritickou infrastrukturu.....	52
<i>Ing. Olga Hölzlová, ředitelka SŠIF Brno</i>	
Bezpečná digitální distribuce výukových materiálů	55
<i>PaedDr. Pavel Hanousek, Publi.cz</i>	
Kam kráčí bezpečnost na základních a mateřských školách	58
<i>Mgr. Monika Bendová, LL.M., Asociace pověřenců ČR</i>	
Metodická podpora bezpečnosti a ochrany zdraví ve školách	61
<i>Ing. Ilona Vaculová, MŠMT</i>	
Shrnutí připravených řešerší z konference ASKI.....	64





Září 2026 jako měsíc vzdělávání, odpovědnosti a české státnosti

PhDr. Mgr. Dušan Kalášek, MBA, LL.M.

Vážení členové ASKI, kolegyně a kolegové, partneři,

zářijové číslo ASKI Zpravodaje vychází s mírným zpožděním. Nešlo však o zpoždění náhodné. Chtěli jsme jeho vydání symbolicky propojit s obdobím, které má pro Českou republiku hluboký historický i společenský význam díky významnému svátku svatého Václava a s touto událostí spojeným Dnem české státnosti.

Den české státnosti připadá na 28. září a připomíná odkaz knížete Václava, patrona české země a jednu z nejvýznamnějších osobností českých dějin. Tento den je od roku 2000 státním svátkem České republiky a bývá spojován nejen s historickou pamětí, ale také s vědomím odpovědnosti za stát, jeho kontinuitu, kulturu, bezpečnost a budoucnost.

Pro ASKI má tento symbolický rámec mimořádný význam. Česká státnost není pouze historická vzpomínka. Je to závazek. Závazek chránit to, na čem stát stojí. Závazek vzdělávat nové generace. Závazek posilovat bezpečnost, odolnost, schopnost spolupráce a připravenost společnosti na situace, které mohou ohrozit její běžné fungování.

Když dnes mluvíme o kritické infrastruktuře, kybernetické bezpečnosti, krizovém řízení, ochraně obyvatelstva, zdravotnictví, vzdělávání nebo společenské odolnosti, nemluvíme o úzkých technických tématech. Mluvíme o praktické podobě odpovědnosti za stát. Mluvíme o tom, aby Česká republika dokázala fungovat i v době narušení, hrozeb, krizí a nejistoty.

A právě proto je pro nás zářijové číslo ASKI Zpravodaje důležité.

Období od 25. srpna do 28. září 2026 bylo pro ASKI mimořádně intenzivní. Velkou část času jsme věnovali přípravě a realizaci odborné konference, která se uskutečnila dne 22. září 2026 v Brně, a zároveň zahájení dvou významných postgraduálních programů **MBA Manažer kritické infrastruktury** a **MBA Manažer kybernetické bezpečnosti**.

Tyto dvě linie, odborná konference pro školy a zahájení specializovaného manažerského vzdělávání, velmi dobře vystihují směr, kterým se ASKI dlouhodobě ubírá. Na jedné straně přenášíme témata kritické infrastruktury, kybernetické bezpečnosti a odolnosti do prostředí škol. Na straně druhé připravujeme odborníky, kteří budou schopni tato témata řídit na manažerské úrovni v organizacích, institucích a systémech, na nichž závisí fungování společnosti.



Září jako měsíc příprav a zahájení postgraduálního vzdělávání

Jedním ze stěžejních organizačních bodů září bylo zahájení dvou postgraduálních programů MBA ASKI v Brně na Čichnově v našem Centru pro postgraduální MBA a LL.M. studium, v areálu Střední školy a vyšší odborné školy informatiky a financí Brno, příspěvkové organizace.

Dne 19. září 2026 jsme zahájili běhy programů **MBA Manažer kritické infrastruktury** a **MBA Manažer kybernetické bezpečnosti**. Oba programy reagují na rostoucí potřebu odborného a zároveň prakticky orientovaného vzdělávání v oblasti bezpečnostního managementu, krizového řízení, kybernetické bezpečnosti, ochrany organizací, řízení rizik a odolnosti.

Program **MBA Manažer kritické infrastruktury** je zaměřen na problematiku kritické infrastruktury, krizového managementu, krizové komunikace, složek záchranného systému, identifikace rizik a hrozeb a ochrany osob a majetku ve firmách a organizacích. Program je prezentován jako mezinárodně certifikované studium.

Program **MBA Manažer kybernetické bezpečnosti** se zaměřuje na oblast kybernetické bezpečnosti jako jednu z klíčových oblastí současného bezpečnostního managementu. Také tento program je uváděn jako mezinárodně certifikované studium.

Zahájení těchto programů považuji za velmi důležité. Kritická infrastruktura ani kybernetická bezpečnost nemohou být řízeny pouze izolovanými technickými znalostmi. Vyžadují lidi, kteří rozumí organizaci, rizikům, provozu, komunikaci, právním souvislostem, krizovým postupům, dodavatelským vazbám a odpovědnosti managementu.

Právě proto má smysl rozvíjet vzdělávání na úrovni MBA. Ne jako formální titul, ale jako prostor pro odbornou přípravu lidí, kteří budou schopni propojovat jednotlivé oblasti bezpečnostní praxe do jednoho funkčního celku.

Velmi si vážíme také toho, že význam takto zaměřeného vzdělávání dlouhodobě potvrzuje řada odborníků působících v oblasti bezpečnostního managementu, krizového řízení, kybernetické bezpečnosti, ochrany dat, kritické infrastruktury i vzdělávání. Je zřejmé, že poptávka po lidech, kteří dokážou tato témata chápat systémově a manažersky, bude v příštích letech dále růst.

Konference ASKI v Brně a odpovědnost ředitelů škol v nové bezpečnostní realitě

Nejvýznamnější událostí sledovaného období byla odborná konference ASKI „**Odpovědnost ředitelů škol v oblasti kritické infrastruktury a kybernetické bezpečnosti podle nové legislativy**“, která se uskutečnila dne **22. září 2026** ve Střední škole informatiky, poštovníctví a finančnictví Brno na ulici Čichnova.



Konference se konala pod záštitou hejtmána Jihomoravského kraje pana **Mgr. Jana Grolicha** a byla zaměřena na propojení nové legislativy, kybernetické bezpečnosti, kritické infrastruktury, krizového řízení a vzdělávání v prostředí škol.

Přestože se pan hejtmán z pracovních důvodů nemohl osobně zúčastnit, velmi si vážíme jeho záštity. Pro ASKI i pro účastníky konference je to významné potvrzení, že téma bezpečnosti škol, kybernetické bezpečnosti, kritické infrastruktury a odolnosti vzdělávacího systému má v Jihomoravském kraji své místo a důležitost.

Tímto bych chtěl panu hejtmánovi **Mgr. Janu Grolichovi** za udělení záštity upřímně poděkovat. Při této příležitosti bych chtěl také vyzdvihnout klíčový podíl spolupráce na organizaci naší konference ze strany vedoucího odboru školství Krajského úřadu Jihomoravského kraje, pana Mgr. Hynka Nespěšného.

Konference byla původně plánována od 9:00 do 14:30 hodin. Zájem účastníků, intenzita diskuse a praktický význam jednotlivých témat však způsobily, že se program nakonec protáhl až přibližně do 16:15 hodin. V sále s kapacitou okolo 200 osob byla většina míst obsazena, což jasně ukázalo, že téma odpovědnosti ředitelů škol v oblasti bezpečnosti, kybernetické ochrany a nové legislativy není okrajové.

Naopak. Je to téma, které vedení škol, odborníci i partneři z praxe vnímají jako velmi aktuální.

Program, který propojil legislativu, vzdělávání, praxi a technologie

Program konference byl koncipován do čtyř hlavních odborných bloků. Dopolední část zahrnovala blok **Legislativní, resortní a strategický rámec odolnosti škol**, následovaný blokem **Vzdělávací systém, kvalifikace a digitální kompetence**. Odpolední část byla věnována tématům **Praktická implementace ve školách a příprava odborníků** a **Technologická podpora, distribuce obsahu a krizové nástroje**.

Tato struktura nebyla zvolena náhodně. Odpovídá tomu, jak ASKI dlouhodobě chápe bezpečnost škol. Nejde pouze o jednu legislativní povinnost, jeden metodický dokument nebo jednu technologii. Jde o celek, ve kterém se potkávají zákony, školní realita, odpovědnost vedení, práce s daty, ochrana osobních údajů, kybernetická bezpečnost, krizová komunikace, bezpečnostní vzdělávání a příprava budoucích odborníků.

První blok se věnoval legislativnímu, resortnímu a strategickému rámci odolnosti. Vystoupili zde odborníci z oblasti ASKI, školství, vojenského prostředí, ochrany osobních údajů a kybernetické bezpečnosti. Mezi vystupujícími byli mimo jiné také zástupci ASKI, MŠMT, Krajského vojenského velitelství Brno, Asociace pověřenců ČR a odborníci na ochranu osobních údajů a kybernetickou bezpečnost.



Druhý blok otevřel otázku vzdělávacího systému, kvalifikací a digitálních kompetencí. Zazněla témata Národní soustavy kvalifikací, ochrany obyvatelstva v kontextu vzdělávání, umělé inteligence a digitálních kompetencí pedagogů.

Třetí blok byl věnován praktické implementaci ve školách a přípravě odborníků. Zaměřil se na bezpečnostní přípravu, BOZP, požární ochranu, ochranu měkkých cílů, školní informační systémy, krizové nástroje, vyšší odborné vzdělávání v oblasti kybernetické bezpečnosti a Junior centrum excelence informační bezpečnosti.

Čtvrtý blok se věnoval technologické podpoře, distribuci obsahu a krizovým nástrojům. V této části se ukázalo, že pokud chceme bezpečnostní témata dostat do škol skutečně udržitelně, nestačí jednorázová konference. Je potřeba vytvářet obsah, metodiku, digitální nástroje a komunikační kanály, které budou školy schopny využívat dlouhodobě.

Také omluvené absence potvrdily, že téma je živé

Je fér zmínit, že někteří plánovaní a avizovaní vystupující se z různých důvodů nemohli osobně zúčastnit. Předem byli omluveni **Ing. Jaroslav Vítek, MBA, Ing. Ilona Vaculová, des. Ing. Radek Doubrava a Dominik Piták.**

Program však díky tomu neztratil kontinuitu. Čas vymezený pro některá vystoupení využili ostatní řečníci a diskuse se mohla více rozvinout. Právě skutečnost, že se konference protáhla až do odpoledních hodin nad původní rámec, potvrzuje, že účastníci neměli zájem pouze „odsedět si program“, ale skutečně diskutovat, ptát se a hledat praktické souvislosti.

To je podle mého názoru jeden z nejdůležitějších výstupů celé akce.

Konference nebyla pouze prezentací. Byla pracovním setkáním.

Školy jako místo, kde začíná budoucí odolnost státu

Jeden z hlavních motivů konference vyjadřoval už samotný úvodní rámec prezentace, ve kterém zazněla myšlenka připisovaná Dógenovi ze Sinópe: **„Základem každého státu je vzdělání jeho mládeže.“** Tato myšlenka byla součástí úvodních podkladů konference a velmi přesně vystihuje důvod, proč se ASKI zaměřuje právě na školství.

Pokud chceme mít v budoucnu odborníky pro kritickou infrastrukturu, kybernetickou bezpečnost, krizové řízení, ochranu obyvatelstva, zdravotnictví, energetiku, dopravu, veřejnou správu a další strategické oblasti, musíme začít vzděláváním.



A nejde pouze o odborné střední a vysoké školy. Bezpečnostní povědomí, schopnost orientovat se v rizicích, rozumět technologiím, chránit data, chápat odpovědnost a spolupracovat v krizových situacích se musí rozvíjet postupně.

Školy jsou jedním z nejdůležitějších míst, kde se formuje budoucí odolnost společnosti.

Proto je důležité, aby ředitelé škol, zástupci vedení, pedagogové, zřizovatelé a odborní partneři měli možnost tato témata sdílet v jednom prostoru. Ne odděleně. Ne izolovaně. Ale jako součást jedné bezpečnostní reality.

Návaznost na předchozí práci ASKI

Brněnská konference nebyla samostatnou akcí bez návaznosti. Navázala na odborný kulatý stůl, který ASKI pořádala dne 24. března 2026 v Poslanecké sněmovně Parlamentu České republiky pod záštitou paní poslankyně **Mgr. Jany Berkovcové**. Tam jsme otevřeli celostátní diskusi o odolnosti kritické infrastruktury a kybernetické bezpečnosti ve školství.

Záměrem ASKI bylo od počátku přenášet tato témata dále, z parlamentní a expertní debaty do konkrétních regionů, škol a odborných komunit. Jihomoravský kraj byl v tomto směru prvním významným regionálním krokem.

Konference ukázala, že tento směr má smysl. Školy potřebují srozumitelný výklad. Potřebují praktické příklady. Potřebují odborné partnery. A potřebují prostor, kde se mohou ptát bez obav, že budou okamžitě zahlceny složitou právní nebo technickou terminologií.

Výstupy z konference v tomto čísle Zpravodaje

Součástí aktuálního vydání ASKI Zpravodaje jsou také stručné výstupy z jednotlivých prezentací. Na základě podkladových materiálů, které byly v rámci konference prezentovány, jsme si dovoluili vybrat z každého vystoupení základní charakteristiku, hlavní odborné sdělení a praktický význam pro školy.

Tyto rešerše nejsou doslovným přepisem vystoupení. Jsou zpracovány jako stručné odborné shrnutí pro čtenáře, kteří se konference nemohli zúčastnit, nebo se chtějí k hlavním myšlenkám vrátit.

Naším cílem je zachovat kontinuitu odborné práce. Konference nemá skončit odchodem posledního účastníka ze sálu. Pokud má mít skutečný dopad, musí její obsah dále žít v metodických materiálech, článcích, diskusích, vzdělávacích programech a dalších navazujících aktivitách.



Každodenní práce, která drží asociaci pohromadě

Vedle dvou hlavních zářijových událostí — zahájení MBA programů a realizace konference — probíhala také každodenní práce, která je méně viditelná, ale naprosto nezbytná.

Byly to telefonáty se členy, komunikace s kolegy z vedení ASKI, jednání s partnery, příprava podkladů, doladování organizačních záležitostí, komunikace s vystupujícími, členy, příznivci a sledujícími.

Velká část této práce není vidět v programu konference ani v hotovém čísle Zpravodaje. Přesto právě ona rozhoduje o tom, zda se odborná činnost asociace rozvíjí stabilně, důvěryhodně a dlouhodobě.

ASKI není jednorázový projekt. Je to odborná platforma, která vzniká každodenní prací lidí, kteří věří, že školství, kritická infrastruktura, kybernetická bezpečnost, krizové řízení a společenská odolnost spolu souvisejí více, než se na první pohled může zdát.

Co nám září 2026 ukázalo

Září 2026 nám ukázalo několik důležitých věcí:

- 1) Zájem škol a odborné veřejnosti o témata kritické infrastruktury a kybernetické bezpečnosti je skutečný. Konference v Brně ukázala, že ředitelé škol, zástupci vedení, odborníci a partneři chtějí těmto tématům rozumět a hledat praktické způsoby, jak s nimi pracovat.
- 2) Vzdělávání manažerů kritické infrastruktury a kybernetické bezpečnosti je nezbytné. Zahájení dvou postgraduálních programů MBA potvrdilo, že bezpečnostní management potřebuje odborníky s mezioborovým přesahem.
- 3) Školství je přirozeným místem, kde se musí začít budovat dlouhodobá odolnost společnosti. Nejen prostřednictvím bezpečnostních opatření, ale také prostřednictvím vzdělávání, kultury odpovědnosti a přípravy budoucích odborníků.
- 4) Regionální spolupráce má velký význam. Záštitu hejtmána Jihomoravského kraje, spolupráce se SŠIPF Brno, zapojení odborných partnerů a vysoká účast ukázaly, že bezpečnostní témata nelze řešit pouze centrálně. Musí se přenášet do regionů, škol a konkrétních komunit.
- 5) Česká státnost není jen historický pojem. V dnešní době se projevuje také tím, jak chráníme své základní služby, jak vzděláváme mladou generaci, jak připravujeme odborníky, jak chráníme data, jak posilujeme bezpečnost institucí a jak dokážeme spolupracovat napříč veřejným, soukromým a vzdělávacím sektorem.



Záříjové číslo ASKI Zpravodaje vydáváme v období Dne české státnosti.

Vnímám to jako důležitý symbol.

Jsme hrdí na českou státnost. Jsme hrdí na tradici, která připomíná, že stát není samozřejmost. A jsme si vědomi toho, že skutečná odpovědnost za stát se dnes neprojevuje pouze slavnostními slovy, ale konkrétní prací.

- Prací na ochraně kritické infrastruktury.
- Prací na zvyšování kybernetické bezpečnosti.
- Prací na vzdělávání odborníků.
- Prací na podpoře škol.
- Prací na krizové připravenosti.
- Prací na společenské odolnosti.

Kritická infrastruktura České republiky není abstraktní pojem. Je to voda, energie, zdravotnictví, doprava, data, komunikace, veřejná správa, bezpečnostní systém, školy a lidé, kteří tyto oblasti každý den drží v chodu.

Pokud chceme zachovat bezpečnou, funkční a odolnou Českou republiku, musíme začít u vzdělávání, odpovědného řízení a schopnosti spolupráce.

Děkuji všem členům ASKI, kolegům z vedení asociace, partnerům, vystupujícím, organizátorům, účastníkům zářijové konference i studentům našich postgraduálních programů.

Září 2026 ukázalo, že cesta, kterou jsme zvolili společně s našimi členy a příznivci, má smysl.

Pokud máte jakékoliv dotazy, připomínky nebo návrhy, neváhejte nás kontaktovat na e-mailové adrese info@aski.cz. Těšíme se na vaše nápady a rady, které nám pomohou dále rozvíjet a zlepšovat naši práci.



S pozdravem a přáním všeho bezpečného,

PhDr. Mgr. Dušan Kalášek, MBA, LL.M.
prezident Asociace škol kritické infrastruktury



Ochrana obyvatelstva a efektivní řízení dobrovolnických zdrojů

Analýza výzev a návrhy na zlepšení v rámci České republiky

Pavel Štyndl, CEVRO Univerzita

Abstrakt

Tento článek se zabývá problematikou moderního systému ochrany obyvatelstva v České republice s důrazem na strategické řízení a integraci dobrovolnických zdrojů. Současné hrozby, ať už v podobě přírodních katastrof, technologických havárií nebo globálních krizí (pandemie COVID-19, uprchlické vlny), jasně ukazují, že tradiční model spoléhající se výhradně na profesionální složky již není plně dostačující. Článek představuje koncept Skupin dobrovolníků ochrany obyvatelstva (SDOO) jako organizovaného a systematicky řízeného partnera Integrovaného záchranného systému (IZS), analyzuje legislativní a ekonomické výzvy a přináší konkrétní doporučení pro zvýšení celospolečenské odolnosti.

Klíčová slova: Ochrana obyvatelstva, dobrovolnictví, krizové řízení, SDOO, Integrovaný záchranný systém, odolnost komunity.

Úvod

Dobrovolníci dnes v České republice představují nepostradatelný pilíř mnoha typů klíčových služeb zajišťovaných státem, kraji nebo obcemi. Tradičně nacházejí uplatnění v sociální sféře, při práci s dětmi, seniory či zdravotně postiženými, kde jejich činnost tvoří neocenitelný doplněk k profesionální péči. Zkušenosti z posledních let však ukazují, že význam dobrovolnictví dramaticky roste také v oblastech bezpečnosti a krizového řízení. Mimořádné události, jako bylo ničivé tornádo na Moravě, rozsáhlé povodně, globální pandemie COVID-19 či bezprecedentní uprchlická vlna vyvolaná konfliktem na Ukrajině, jasně demonstrovaly, že dobrovolníci často stojí v první linii pomoci.

Bez jejich okamžitého zapojení a obětavosti by zvládnutí těchto krizí bylo pro státní aparát nejen organizačně daleko složitější, ale také ekonomicky neúnosné. Prostředky a úsilí vložené do podpory dobrovolnictví se společností násobně vrací. Přestože je laická podpora lidského kontaktu a materiální pomoci klíčová, naráží současná praxe na limity v oblasti koordinace, legislativního ukotvení a systematické přípravy. Investovat do dobrovolnictví na všech úrovních se prokazatelně vyplatí, je však nutné



přejít od reaktivního využívání spontánní pomoci k proaktivnímu, systematickému řízení těchto cenných lidských zdrojů.

Nové pojetí bezpečnosti a role občana

V rámci moderních bezpečnostních studií dochází k zásadnímu posunu vnímání role veřejnosti při zajišťování bezpečnosti. Tradiční paternalistická představa, že za zvládnutí krizové situace odpovídají výhradně státní instituce a profesionální záchranné složky, je v podmínkách současných komplexních hrozeb již neudržitelná. Kapacity profesionálních sborů jsou limitované a při rozsáhlých mimořádných událostech dochází k jejich okamžitému vytížení. Moderní pojetí ochrany obyvatelstva proto vyžaduje aktivní zapojení občanů a budování tzv. komunitní odolnosti (resilience).

Každý občan by měl být schopen alespoň v počáteční fázi mimořádné události samostatně reagovat, chránit život a zdraví své i svého okolí a poskytnout základní součinnost. Tento přístup vyžaduje systematické zvyšování bezpečnostní gramotnosti veřejnosti, posilování individuální odpovědnosti a vzdělávání již od školního věku. Dobrovolnictví v tomto kontextu funguje jako přirozený most mezi státem a občanskou společností, kdy se organizovaní občané aktivně podílejí na preventivních opatřeních, edukaci komunity a bezprostřední likvidaci následků krizí.

Skupiny dobrovolníků ochrany obyvatelstva (SDOO)

Jako efektivní řešení současných koordinačních nedostatků se navrhuje institucionalizace a rozvoj **Skupin dobrovolníků ochrany obyvatelstva (SDOO)**. Tyto skupiny nejsou zamýšleny jako náhrada profesionálních složek Integrovaného záchranného systému (IZS) či zavedených jednotek sborů dobrovolných hasičů (JSDH), nýbrž jako jejich specializovaný, organizovaný a odborně připravený partner na úrovni obcí.

Hlavním přínosem SDOO je jejich hluboká znalost místního prostředí, obyvatelstva a specifických rizik daného území. Mezi základní úkoly těchto skupin patří:

- Podpora obcí při organizaci a provádění evakuace a nouzového přežití obyvatel.
- Distribuce humanitární pomoci, materiálu, pitné vody a potravin v postižených oblastech.
- Zajišťování informační podpory pro občany a asistence při varování obyvatelstva.
- Poskytování první laické psychosociální pomoci zasaženým osobám.



- Spolupráce na preventivních a vzdělávacích aktivitách v oblasti krizové připravenosti na komunitní úrovni.

Zahraniční zkušenosti z vyspělých evropských států potvrzují, že existence takto strukturovaných dobrovolnických útvarů radikálně zvyšuje rychlost a efektivitu lokální reakce na krize a výrazně snižuje celkové materiální i lidské ztráty.

Klíčový princip SDOO

Skupiny dobrovolníků ochrany obyvatelstva představují chybějící článek mezi operativní činností profesionálních záchranářů a potřebami civilního obyvatelstva v místě krize. Nenahrazují odborné profese, ale multiplikují akceschopnost samospráv.

Podmínky pro efektivní řízení a udržitelnost

Aby mohly skupiny SDOO dlouhodobě a spolehlivě fungovat, je nezbytné pro ně vytvořit odpovídající organizační, personální, zdravotní a materiální zázemí. Současná analýza odhaluje dva hlavní pilíře, na kterých úspěšná integrace dobrovolníků stojí: preventivní péče spolu s pojištěním a stabilní systém financování.

Zdravotní péče a právní ochrana: Výkon dobrovolnické činnosti v oblasti ochrany obyvatelstva s sebou nese specifická rizika. Pro zajištění bezpečnosti samotných dobrovolníků je nutné implementovat doporučený systém preventivního očkování (např. proti hepatitidě či tetanu) a garantovat komplexní úrazové a odpovědnostní pojištění. Dobrovolník musí mít právní jistotu, že v případě zranění či neúmyslného způsobení škody při výkonu služby nezůstane bez systémové podpory.

Více zdroje financování: Bez finančního zajištění nelze realizovat pravidelnou odbornou přípravu, pořizovat ochranné pracovní pomůcky, zdravotnický materiál ani moderní spojovací prostředky. Jako nejvhodnější se jeví transparentní vícezdrojový model, který rozkládá rizika a zajišťuje stabilitu:

- **Komunální úroveň:** Základní příspěvky obcí a měst, které mají přímý zájem na bezpečnosti svého území.
- **Státní a krajská úroveň:** Cílené dotační programy zaměřené na ochranu obyvatelstva a požární ochranu.
- **Externí zdroje:** Evropské fondy, granty nadací a programy společenské odpovědnosti firem (CSR).



Legislativní rámec a společenské uznání

Významným krokem vpřed je rozvoj legislativního prostředí, které dobrovolníkům přizná jasný oficiální status, přesně vymezí jejich práva a povinnosti a zjednoduší administrativní zátěž spojenou s jejich registrací a nasazováním. Nová právní úprava by měla reflektovat ekonomickou a společenskou hodnotu dobrovolnické práce a umožnit její vyčíslení, což usnadní například uznávání této činnosti jako spolufinancování u dotačních projektů.

Zároveň je klíčové zavést standardizovaná osvědčení (certifikáty) o vykonaném dobrovolnictví a získaných kompetencích. Takové osvědčení má prokazatelný potenciál zvýšit uplatnitelnost dobrovolníků na trhu práce a poskytnout jim hmatatelné benefity v rámci profesního rozvoje či studia. Společenské uznání se tak transformuje z morálního ocenění do praktické hodnoty oceňované zaměstnavateli i vzdělávacími institucemi.

Závěr a doporučení

Účinná ochrana obyvatelstva v 21. století není a nemůže být pouze úkolem státu a profesionálních složek IZS. Vyžaduje aktivní spoluodpovědnost a kooperaci celé společnosti. Systematická integrace Skupin dobrovolníků ochrany obyvatelstva (SDOO) do struktur krizového řízení představuje vysoce perspektivní nástroj pro rozvoj komunitní odolnosti v České republice.

Pro úspěšnou realizaci tohoto konceptu je doporučeno zaměřit se na následující prioritní oblasti:

- 1) Vytvoření jednotných metodických pravidel a standardů odborné přípravy pod záštitou MV-GŘ HZS ČR.
- 2) Zakotvení specifického statusu krizového dobrovolníka do národní legislativy s odpovídajícími garancemi pojištění a zdravotní prevence.
- 3) Zavedení stabilního vícezdrojového financování s fixní podporou ze strany krajů a obcí.
- 4) Implementace systému certifikace získaných dovedností pro zvýšení prestiže a reálné hodnoty dobrovolnictví na trhu práce.
- 5) Posílení výuky ochrany obyvatelstva a krizové připravenosti v rámci vzdělávacího systému a realizace celonárodních informačních kampaní.

Pouze harmonické propojení špičkově připravených profesionálních složek, moderních technologií a organizovaných, motivovaných občanů dokáže zajistit, že Česká republika bude schopna úspěšně čelit budoucím krizovým výzvám a minimalizovat jejich dopady na lidské životy a celou společnost.



Dodavatelský řetězec kritické infrastruktury podle nového zákona o kybernetické bezpečnosti: co musí obsahovat smlouva a jak to doložit

Lukáš Medovič, MBA, RAGUARD.CZ

Ochrana kritické infrastruktury se tradičně řeší na úrovni vlastních systémů, sítí a fyzického perimetru. Zákon č. 264/2025 Sb. o kybernetické bezpečnosti, účinný od listopadu 2025, ale klade stejný důraz na článek řetězce, který provozovatelé kritické infrastruktury často řídí nejméně přímo, na dodavatele. Firmám v sektorech energetiky, dopravy, zdravotnictví, ICT, vodního hospodářství a financí, které pod zákon spadají, běží dvanáctiměsíční lhůta na splnění většiny povinností, počítaná od doručení rozhodnutí o registraci, ne od podání žádosti. Řada firem už tuto lhůtu má, aniž by si to plně uvědomovala.

Co zákon konkrétně vyžaduje

Vyhláška č. 409/2025 Sb. pro firmy ve vyšším režimu a vyhláška č. 410/2025 Sb. pro nižší režim stanoví přesný obsah smluv s dodavateli. U vyššího režimu jde o osmnáct konkrétních ustanovení v příloze č. 5, u nižšího o čtrnáct v příloze č. 2. Nejde o doporučení. Jde o taxativní výčet toho, co smlouva musí obsahovat, od ustanovení o mlčenlivosti a auditu dodavatele přes exit strategii až po povinnost dodavatele hlásit změnu vlastnické struktury.

Firma navíc musí své významné dodavatele identifikovat, evidovat a písemně informovat o jejich statusu. Musí sledovat, zda smlouva danou povinnost skutečně obsahuje, a pokud ne, musí to napravit s termínem a odpovědnou osobou. V praxi to znamená projít desítky až stovky dodavatelských smluv a u každé ověřit čtrnáct nebo osmnáct bodů zvlášť.

Zákon k tomu přidává povinnost hlásit kybernetické bezpečnostní incidenty v pevných lhůtách: do 24 hodin prvotní hlášení, do 72 hodin oznámení s prvotním posouzením a do 30 dnů závěrečnou zprávu. Dále vyžaduje vedení dokumentace organizačních a technických opatření podle § 14 zákona, včetně registru aktiv navázaných na poskytování regulované služby, registru rizik a bezpečnostních politik schválených vedením. Pro provozovatele kritické infrastruktury, kde je fyzická i kybernetická bezpečnost dlouhodobě řízenou disciplínou, jde o rozšíření existující praxe o novou, právně přesně definovanou vrstvu. Pro jejich dodavatele, kteří takovou praxi často nemají, jde o zásadní změnu.



Kde tento proces reálně naráží

V praxi se opakují dva vzorce. Buď to řeší jeden interní člověk v Excelu vedle svých ostatních povinností, a výsledek neodpovídá tomu, co vyhláška skutečně žádá, protože přílohu vyhlášky nečte právník. Nebo se najme konzultant, který dokumentaci připraví jednorázově, a o rok později neodpovídá realitě, protože dodavatelé se mění a smlouvy se obnovují.

Co jsem postavil

RAGUARD je platforma, která tento proces řeší softwarově. Firma zaeviduje dodavatele podle IČO, dodavatel dostane odkaz na dotazník bez nutnosti zakládat účet, a otázky v dotazníku odpovídají bod po bodu obsahu příloh 5 a 2. Když dodavatel odpoví, systém porovná odpověď s textem vyhlášky a navrhne konkrétní znění chybějícího ustanovení, vždy s citací, ze které části vyhlášky návrh vychází.

Návrh nikdy nejde do dokumentace automaticky. O každém rozhoduje člověk. To není marketingové gesto, je to podmínka, za které má produkt smysl používat v prostředí, kde odpovědnost za právní úkony nese statutární orgán, ne algoritmus.

Text zákona a obou vyhlášek, ze kterého systém cituje, jsem porovnal slovo od slova s aktuálním zněním ve Sbírce zákonů. Platforma běží v produkci na evropské infrastruktuře, s izolací dat mezi zákazníky na úrovni databáze a neměnným auditním záznamem každé schválené změny. Export pro kontrolu NÚKIB je deterministický, což znamená, že vygenerovaný dvakrát dá stejný výsledek, a má tak plnou důkazní hodnotu.

Kolem dodavatelského jádra jsem postavil zbytek toho, co zákon vyžaduje: registr aktiv, registr rizik s vlastníkem a stavem řešení, šablony bezpečnostních politik se schvalovacím workflow, evidenci školení a modul hlášení incidentů, který hlídá zákonné lhůty.

Projekt se letos umístil mezi pěti nejlépe hodnocenými v rámci univerzitního programu VUT BoosterChallenge 2026. Na závěrečné přehlídce hodnotilo 36 studentských projektů třináct odborníků z akademické i firemní sféry ([článek VUT](#)), a univerzita projekt dál podporuje v dalším rozvoji.

Hledám pilotní partnery

Platforma běží v produkčním provozu. Chybí mi ověření na reálném dodavatelském řetězci střední nebo velké firmy, ideálně ve vyšším režimu podle zákona, s desítkami až stovkami dodavatelů.



Pilotní implementaci (proof of concept) nabízíme bez nákladů a závazků výměnou za zpětnou vazbu. Pilot znamená reálné nasazení na části dodavatelského řetězce, ne demo na uměle vytvořených datech. Zajímá mě především pohled člověka, který má compliance na starosti, ať už jde o manažera kybernetické bezpečnosti, IT ředitele, nebo osobu odpovědnou za dodavatelské vztahy.

Pokud vaše organizace provozuje nebo dodává do kritické infrastruktury, spadá pod zákon a řešíte, jak dostat pod kontrolu desítky nebo stovky dodavatelských smluv, ozvěte se. V pátek 25. 9. budu na Innovation Week na stánku JIC v Brně, kde si o tom můžeme promluvit osobně. Rád přijedu i jinam a ukážu, jak systém v praxi funguje.

Lukáš Medovič

lukas.medovic@raguard.cz · raguard.cz

The screenshot shows the Raguard website with a dark theme. The top navigation bar includes links for 'FUNKCE', 'JAK TO FUNGUJE', 'SOULAD', 'ČASTE OTÁZKY', 'BEZPEČNOST', and 'PRŮVODCE', along with 'Přihlásit' and 'Spustit pilot' buttons. The main content area features the heading '6 BEZPEČNOST' and a large, bold title: 'Chránit dodavatelský řetězec začíná tím, že chráníme vaše vlastní data.' Below this, a paragraph states: 'Tohle jsou konkrétní opatření, která běží v produkci — ne prohlášení o záměru. Kde to má smysl, je uvedeno i to, co jsme si sami ověřili, ne jen navrhli.'



Úvod k sérii rešerší vystoupení z konference ASKI

PhDr. Mgr. Dušan Kalášek, MBA, LL.M., president ASKI, z. s.

Redakční uvedení odborných výstupů z konference „Odpovědnost ředitelů škol v oblasti kritické infrastruktury a kybernetické bezpečnosti podle nové legislativy“.

V aktuálním čísle ASKI Zpravodaje zahajujeme sérii stručných rešerší vybraných vystoupení, která zazněla na odborné konferenci ASKI konané dne 22. září 2026 v Brně. Konference byla věnována odpovědnosti ředitelů škol v oblasti kritické infrastruktury, kybernetické bezpečnosti, krizového řízení a odolnosti podle nové legislativy.

Cílem této série není nahradit samotné prezentace ani vytvořit doslovný přepis vystoupení. Smyslem je zpřístupnit hlavní odborné myšlenky také těm čtenářům, kteří se konference nemohli zúčastnit, a současně uchovat základní obsah jednotlivých příspěvků v podobě, která je čitelná pro vedení škol, zřizovatele, odborníky i širší profesní veřejnost.

Jak budou rešerše zpracovány

Každý rešeršní článek bude vycházet z podkladových materiálů prezentovaných příslušným autorem na konferenci. U každého výstupu se pokusíme zachytit základní charakteristiku tématu, hlavní odborné sdělení, praktický význam pro školy a širší souvislosti s oblastí kritické infrastruktury, kybernetické bezpečnosti, krizového řízení, ochrany osobních údajů, digitálních kompetencí nebo bezpečnostního vzdělávání.

Jednotlivé články budou pojaty jako redakční výtah z prezentovaných podkladů. Každý článek bude zároveň graficky doplněn obrázkem úvodního snímku prezentace autora, aby bylo zřejmé, ke kterému konferenčnímu vystoupení se daná rešerše vztahuje.

Rozsah rešerší se bude lišit podle délky, povahy a odborné šíře jednotlivých prezentací. U kratších vystoupení půjde o stručnější shrnutí, u rozsáhlejších a koncepčnějších prezentací bude text přirozeně širší.

Poznámka k rešerším vystoupení z konference ASKI

Redakční a právní vymezení

V tomto čísle ASKI Zpravodaje si dovoluujeme přinést stručné rešerše vybraných vystoupení z odborné konference „Odpovědnost ředitelů škol v oblasti kritické infrastruktury a kybernetické bezpečnosti podle nové legislativy“, která se uskutečnila dne 22. září 2026 ve Střední škole a vyšší odborné škole informatiky a financí Brno.



V rámci konference byli vystupující veřejně požádáni o možnost využít jejich prezentované podklady pro následné odborné shrnutí ve Zpravodaji ASKI. Níže uvedené rešerše proto nepředstavují autorizovaný přepis vystoupení ani právní, metodické nebo oficiální stanovisko autora, pořadatele či zastoupených institucí. Jde o redakční rešerši a volnou interpretaci informací obsažených v podkladových prezentacích, zpracovanou pro potřeby čtenářů ASKI Zpravodaje.

Rešerše nebyly samostatně konzultovány ani autorizovány autory prezentací, pokud není u konkrétního článku výslovně uvedeno jinak. V případě první prezentace je autorem vystoupení i odborného rámce prezident ASKI PhDr. Mgr. Dušan Kalášek, MBA, LL.M., a proto je souhlas se zpracováním tohoto textu dán automaticky.

Smyslem těchto rešerší není nahrazovat původní prezentace ani rozšiřovat odpovědnost autorů za následný výklad. Cílem je zachytit základní myšlenky, odborné souvislosti a praktické podněty, které na konferenci zazněly, a zpřístupnit je také těm čtenářům, kteří se akce nemohli osobně zúčastnit.

Proč rešerše zveřejňujeme

Konference ASKI nebyla koncipována jako jednorázová akce, která skončí posledním vystoupením v programu. Jejím cílem bylo otevřít praktickou odbornou diskusi o tom, jak se nová bezpečnostní a legislativní témata promítají do prostředí škol, jejich řízení, vzdělávacích programů a přípravy budoucích odborníků.

Právě proto považujeme za důležité, aby výstupy z konference měly pokračování také v publikační podobě. Rešerše umožňují zachovat základní obsah jednotlivých příspěvků, vrátit se k hlavním myšlenkám a nabídnout je širšímu okruhu čtenářů ASKI Zpravodaje.

Témata kritické infrastruktury, kybernetické bezpečnosti, ochrany osobních údajů, krizové komunikace, bezpečnosti škol, umělé inteligence, digitálních kompetencí a vzdělávání odborníků nelze řešit izolovaně. Právě jejich propojení bylo hlavní hodnotou celé konference a tuto hodnotu chceme promítnout i do následujících textů.

Společný rámec celé série

Série rešerší bude sledovat společnou linku, která dokazuje, že školy dnes nejsou pouze místem výuky, ale také organizacemi, které pracují s daty, technologiemi, lidmi, provozem, bezpečností a odpovědností vůči žákům, rodičům, zaměstnancům i zřizovatelům.

Nová legislativa v oblasti kritické infrastruktury a kybernetické bezpečnosti zároveň mění prostředí, do kterého školy připravují své absolventy. Proto má smysl, aby vedení škol rozumělo základním souvislostem, umělo rozlišit reálné povinnosti od širších odborných doporučení a dokázalo bezpečnostní témata přiměřeně začlenit do řízení školy i vzdělávání.



ASKI chce v tomto procesu vystupovat jako odborná platforma, která propojuje školství, veřejnou správu, bezpečnostní instituce, technologické partnery, odborníky z praxe a vzdělávací systém.

Následující řešerše jsou jedním z kroků, jak tuto roli naplňovat i po skončení samotné konference.





Legislativní změny v oblasti krizového řízení, kritické infrastruktury a kybernetické bezpečnosti v kontextu školství a vzdělávání

PhDr. Mgr. Dušan Kalášek, MBA, LL.M., prezident ASKI

Zkrácený autorský článek podle úvodní prezentace z konference ASKI dne 22. září 2026 v Brně.



**Asociace škol kritické
infrastruktury, z. s.**
Revoluční 981
666 01 Tišnov
www.aski.cz
info@aski.cz

Legislativní změny v oblasti krizového řízení, kritické infrastruktury a kybernetické bezpečnosti v kontextu školství a vzdělávání

PhDr. Mgr. Dušan Kalášek, MBA, LL.M.

prezident
Asociace škol kritické infrastruktury, z.s. - ASKI

22. září 2026

Střední škola a vyšší odborná škola
informatiky a financí Brno, příspěvková organizace

Úvodní snímek prezentace autora z konference ASKI, 22. 9. 2026.

Ve svém úvodním vystoupení jsem se zaměřil na propojení tří oblastí, které se v praxi často řeší odděleně:

- 1) krizového řízení,
- 2) kritické infrastruktury
- 3) a kybernetické bezpečnosti.

V prostředí školství však tyto oblasti stále více tvoří jeden společný rámec. Škola už dnes není pouze místem výuky, ale také organizací, která pracuje s daty, technologiemi, lidmi, provozem, komunikací, bezpečností a odpovědností vůči žákům, rodičům, zaměstnancům i zřizovatelům.

Mým cílem nebylo tvrdit, že školy jsou automaticky subjekty kritické infrastruktury. Takové zjednodušení by nebylo správné. Naopak jsem chtěl ukázat, že školy mají zásadní vzdělávací, systémovou a společenskou roli. Přípravují budoucí občany





a odborníky pro svět, ve kterém bude schopnost chránit základní služby, data, technologie a organizace stále důležitější.

Vzdělávání jako základ budoucí odolnosti

Prezentaci jsem uvedl myšlenkou Jana Amose Komenského: „*Takový je příští věk, jak jsou vychováni příští jeho občané.*“ Právě tato věta podle mého názoru vystihuje vztah mezi školstvím a bezpečností státu. Pokud chceme odolnější společnost, nemůžeme začít až u dospělých odborníků ve chvíli, kdy nastane problém. Musíme začít u vzdělávání, návyků, kompetencí a schopnosti mladých lidí chápat svět kolem sebe.

Bezpečnostní gramotnost, digitální hygiena, schopnost pracovat s informacemi, porozumění rizikům, odpovědnost a schopnost spolupráce nejsou témata, která by měla stát mimo vzdělávací systém. Naopak. Jsou to kompetence, které budou rozhodovat o tom, jak budou budoucí absolventi schopni fungovat v osobním, občanském i profesním životě.

Legislativní rámec a důvod, proč se školy musí zajímat

Ve vystoupení jsem vycházel z několika základních právních a strategických rámců. Prvním byl krizový zákon, tedy zákon č. 240/2000 Sb., který dlouhodobě tvoří základ krizového řízení v České republice. Už v koncepčních materiálech ochrany obyvatelstva se přitom objevuje problém nedostatku odborně vyškoleného a zkušeného personálu. Jedním z řešení je větší důraz na vzdělávání, propojení teorie s praxí a využití výsledků bezpečnostního výzkumu.

Druhým důležitým rámcem je školský zákon. Ten neřeší pouze organizaci školství, ale také cíle vzdělávání, rozvoj osobnosti člověka, přípravu pro občanský a profesní život a zdokonalování vzdělávacího procesu podle výsledků vědy, výzkumu a vývoje. Právě zde se bezpečnostní témata mohou přirozeně potkávat s posláním škol.

Třetím rámcem je Strategie vzdělávací politiky ČR do roku 2030+, která pracuje s tím, že vzdělávání má připravovat člověka pro dynamicky se měnící svět. A právě tento svět se dnes mění velmi rychle: technologicky, bezpečnostně, legislativně i společensky.

Proč vznikla ASKI

Jedním z důležitých momentů mé prezentace bylo připomenutí roku 2022. Napadení Ukrajiny velmi konkrétně ukázalo, že kritická infrastruktura není abstraktní pojem. Útoky a dopady konfliktu se netýkaly pouze vojenských cílů, ale také civilní infrastruktury, energetiky, vodních děl, nemocnic, dopravy a dalších služeb, na kterých stojí každodenní život společnosti.

ASKI vznikla v listopadu 2022 právě v této bezpečnostní a společenské atmosféře. Její výchozí myšlenka byla jednoduchá: kritická infrastruktura není pouze technika



a objekty. Je to především schopnost lidí chápat služby, rizika, data, dodavatele a krizové situace. A tato schopnost začíná ve školách.

Proto ASKI dlouhodobě působí jako odborná, profesní a nepolitická platforma zaměřená na podporu vzdělávání v oblasti kritické infrastruktury, informační bezpečnosti a souvisejících procesů. Postupně jsme od osvěty a podpory škol přešli k odborným akcím, konferencím, publikační činnosti, mezinárodní certifikaci a postgraduálnímu vzdělávání.

Školy a bezpečnostní realita

Ve vystoupení jsem připomněl také tragickou událost z prosince 2023 na Filozofické fakultě Univerzity Karlovy. Nešlo o to tuto událost jakkoli zjednodušovat nebo využívat. Šlo o připomenutí skutečnosti, že školy a školská zařízení jsou součástí bezpečnostní reality a že ochrana měkkých cílů, krizová komunikace a schopnost vedení školy reagovat na mimořádné situace musí být součástí odpovědného řízení.

Školy samozřejmě nemohou a nemají nahrazovat bezpečnostní složky. Musí však vědět, jaká rizika se jich mohou týkat, s kým spolupracovat, jak nastavit základní procesy, jak komunikovat a jak vytvářet prostředí, které je bezpečnější a připravenější.

Kritická infrastruktura jako průřezové téma

Důležitou částí prezentace bylo ukázat, že kritická infrastruktura může být ve školství chápána jako průřezové téma. Netýká se pouze technických oborů, kybernetické bezpečnosti nebo specializovaných vzdělávacích programů. Může se promítat do občanského vzdělávání, informatiky, ekonomiky, zdravotnických oborů, technických předmětů, environmentálních témat i tělesné výchovy.

V tomto smyslu nejde o to vytvářet další izolovanou agendu. Jde o to ukazovat souvislosti. Voda, energie, doprava, zdravotnictví, data, veřejná správa, bezpečnost a komunikace nejsou oddělené světy. Jsou to základní služby a systémy, jejichž vzájemná závislost je pro dnešní společnost určující.

Rok 2025 změnil pravidla

V prezentaci jsem zdůraznil, že rok 2025 přinesl zásadní legislativní změnu. Nový zákon o kybernetické bezpečnosti a nový zákon o odolnosti subjektů kritické infrastruktury mění způsob, jakým přemýšlíme o bezpečnosti organizací. **Přecházíme od ochrany jednotlivých prvků ke schopnosti řídit odolnost základních služeb.**

To má význam i pro školy. Ne proto, že by se každá škola automaticky stala regulovaným subjektem, ale proto, že se mění prostředí, do kterého školy připravují děti, žáky a studenty. Absolventi budou vstupovat do světa, kde budou stále důležitější pojmy jako odolnost, kontinuita, řízení rizik, kybernetická bezpečnost, dodavatelské řetězce, ochrana dat a krizová komunikace.



Budoucnost v pohybu: AI, digitalizace a lidský faktor

Další část vystoupení se věnovala technologickým a společenským změnám. Umělá inteligence, digitalizace, botizace a automatizace výrazně ovlivní pracovní trh i fungování organizací. Některé činnosti budou automatizovány, vzniknou nové profese a většina pracovních pozic bude vyžadovat alespoň základní digitální dovednosti.

Digitalizace přináší velké příležitosti: monitoring a analýzu dat v reálném čase, využití umělé inteligence v kybernetické bezpečnosti, digitální dvojčata nebo simulace krizových situací. Současně ale přináší nové zranitelnosti, kybernetické útoky, potřebu ochrany dat a riziko přílišné závislosti na technologiích.

Proto jsem v závěru této části zdůraznil, že největší výzvou nemusí být pouze technologická krize, ale krize lidského faktoru. Budeme mít dostatek znalostí a dovedností? Dostatek etiky, odpovědnosti, sebereflexe a schopnosti jednat ve prospěch věcí budoucích? To jsou otázky, na které musí vzdělávání reagovat.

Proč školy zapojovat do tématu KI

V závěru jsem uvedl tři hlavní důvody, proč je důležité zapojovat školy do tématu kritické infrastruktury. Za prvé: školy nejsou automaticky subjekty kritické infrastruktury a jejich případné zařazení by záviselo na poskytování základní služby a splnění kritérií významnosti. To je nutné říkat přesně a bez zbytečného strašení.

Za druhé: skutečný přínos škol je vzdělávací a systémový. Školy mohou rozvíjet bezpečnostní gramotnost, digitální hygienu, krizovou komunikaci, cvičení a personální pipeline pro bezpečnostní obory.

Za třetí: školy mohou spolupracovat s veřejnou správou, HZS, policií, NÚKIB, odbornými školami a provozovateli infrastruktury. Cílem jsou připravenější občané, kompetentnější absolventi a lepší pochopení závislostí základních služeb.

Tři věty, které si má vedení školy odnést

Nová legislativa není jen právní změna. Je to změna prostředí, do kterého posíláme děti, žáky a studenty.

Bezpečnostní a odolnostní kompetence se musí začít budovat od mateřských a základních škol a systematicky pokračovat až k odborné praxi a řízení kritické infrastruktury.

Kdo chce udržet kvalitu školy i relevanci absolventů, musí jednat nyní a spolupracovat se zřizovateli, odbornou praxí a ASKI.



Moje vystoupení nebylo pouze legislativním přehledem. Bylo především výzvou ke změně pohledu. Pokud chceme bezpečnější a odolnější Českou republiku, musíme začít u vzdělávání. Musíme rozvíjet kompetence lidí, kteří budou jednou řídit organizace, chránit data, provozovat základní služby, reagovat na krizové situace a rozhodovat v prostředí nejistoty.

Školy v tomto procesu nejsou okrajovým hráčem. Jsou místem, kde se formují občané, odborníci i budoucí manažeři kritické infrastruktury. Právě proto má smysl, aby témata kritické infrastruktury, kybernetické bezpečnosti, krizového řízení a společenské odolnosti byla do školství přenášena srozumitelně, odborně a prakticky.

To je také dlouhodobý směr ASKI: propojovat školství, bezpečnostní praxi, veřejnou správu, technologie a vzdělávání tak, aby složité změny nebyly jen textem v zákonech, ale aby se proměnily ve skutečnou schopnost lidí a organizací jednat odpovědně a včas.



Školy jako součást kritické infrastruktury: řízení rizik a ochrana osobních údajů v praxi

PhDr. Jaroslav Hora, LL.M., ČSÚ

Rešerše vystoupení z konference ASKI dne 22. září 2026 v Brně.



Poznámka k rešerši: Následující text je redakčním výtahem z podkladové prezentace autora. Rešerše není autorizovaným přepisem vystoupení ani oficiálním stanoviskem autora či zastoupených institucí. Formulace vycházejí pouze z informací uvedených v prezentaci a jsou zpracovány jako stručná charakteristika hlavních sdělení pro čtenáře ASKI Zpravodaje.

Východisko prezentace

Autor prezentoval školy jako významný uzel propojující současnou odolnost společnosti s její budoucností. V prezentaci uvádí, že škola není okrajovým sektorem, ale prostředím, které se dotýká energetiky, zdravotnictví, veřejné správy i přípravy budoucích odborníků kritické infrastruktury. Vzdělávání autor označuje za základní službu státu a školu současně popisuje jako datový uzel, který propojuje rodiny, obce, kraje i stát a zpracovává údaje téměř každého dítěte a rodiče.

V této souvislosti autor zdůrazňuje, že bezpečnostní povědomí a digitální kompetence, které se dnes ve škole nevytvoří, mohou později chybět v energetice, zdravotnictví i veřejné správě. Slabé zabezpečení škol podle prezentace neohrožuje pouze žáky, ale také dodavatelský řetězec, s nímž je škola propojena.



Proč jsou školy atraktivním cílem

Autor uvádí několik důvodů, proč mohou být školy atraktivním cílem útočníků. Na prvním místě stojí koncentrace citlivých dat, mezi která prezentace řadí zdravotní záznamy, posudky pedagogicko-psychologických poraden, informace o sociálních poměrech a osobní údaje tisíců nezletilých. Dalším faktorem je nízká úroveň zabezpečení IT, omezené rozpočty, chybějící IT specialisté, zastaralé systémy a nejednotná správa přístupů.

Podstatným motivem prezentace je také vynucená digitální stopa. Autor upozorňuje, že žák ani rodič nemají v rámci povinné školní docházky skutečnou volbu, komu svá data svěří. Riziko je podle prezentace zesíleno i možností vydírání formou double extortion, tedy kombinací šifrování dat a hrozby zveřejněním citlivých záznamů. Školní informační systémy, cloudové platformy a elektronické žákovské knížky autor v této souvislosti popisuje jako sdílené riziko pro větší počet institucí.

Paradox digitální školy

Výraznou část vystoupení autor staví na kontrastu mezi chráněným fyzickým světem a nedostatečně hlídaným digitálním prostorem. Na straně fyzické bezpečnosti prezentace uvádí čipové karty u vstupu, turnikety, videotelefony, návštěvní knihy, doprovod cizích osob po budově, kamerové systémy a investice do mechanického zabezpečení.

Proti tomu autor staví digitální realitu, v níž si učitel může volně zaregistrovat bezplatnou cloudovou utilitu, nahrát celé jmenné seznamy tříd na neproverené servery, neřešit jurisdikci provozovatele ani smluvní podmínky a využívat spotřebitelské účty pro školní agendu. Autor prezentuje příklad, v němž učitelka nahrála docházku a posudky žáků se speciálními vzdělávacími potřebami do online nástroje na tvorbu rozvrhů se sídlem mimo EU. Klíčovým závěrem tohoto bloku je, že škola nemůže hlídat fyzický práh a současně ignorovat digitální tok dat.

Právní rámec a ochrana dat

Autor prezentoval provázanost nového zákona o kybernetické bezpečnosti, zákona o odolnosti subjektů kritické infrastruktury a GDPR. U zákona č. 264/2025 Sb. zmiňuje povinnou samoidentifikaci subjektů, řízení rizik dodavatelského řetězce, hlášení kybernetických bezpečnostních incidentů vůči NÚKIB a odpovědnost vedení organizace za zavedení bezpečnostních opatření.

U zákona č. 266/2025 Sb. autor uvádí přechod od ochrany „prvků“ k poskytovatelům základních služeb, vzdělávací soustavu jako páteř fungování moderní společnosti, důraz na kontinuitu provozu při krizových stavech a výpadech a propojení s krizovými plány obcí, ORP a krajských úřadů. GDPR autor označuje za základní stavební kámen ochrany soukromí. Zpracování dat dětí je podle prezentace legální pouze při splnění



zásad GDPR, přičemž integrita a důvěrnost znamenají technické zabezpečení dat v kyberprostoru. Autor rovněž uvádí DPIA jako povinnost před nasazením plošných školních technologií.

Dodavatelé, datové hromadění a minimalizace

Samostatné místo v prezentaci má téma dodavatelských rizik. Autor popisuje iluzi jednotného balíčku, kdy školy uzavřou smlouvu na hlavní informační systém, ale následně k němu připojují neprověřené doplňky. Zpracovatelské smlouvy podle prezentace často chybí nebo mají podobu jednostranných formulářů velkých technologických firem. Autor zde výslovně varuje, že dodavatel školního softwaru bez přesné zpracovatelské smlouvy a prověrky bezpečnosti není partner, ale nekontrolované riziko.

Dalším tématem je takzvané digitální hromadění. Autor uvádí, že školy mohou ukládat data stylem „pro jistotu to nemažte“, ponechávat roky neudržované e-mailové schránky bývalých zaměstnanců, staré posudky PPP, zdravotní omluvenky či záznamy o rodinných sporech na síťových discích bez řízeného přístupu. Ve scénáři ransomwaru dvojího vydírání podle prezentace školu nemusí nejvíce ohrozit rozvrhy či známky, ale zveřejnění citlivých zpráv z výchovného poradenství. Řešením má být důsledná hygiena dat, dodržování retenčních a skartačních lhůt, segmentace a šifrování zvláštních kategorií údajů. Autor shrnuje, že data, která škola nemá, nemohou uniknout.

Systémová governance a řízení rizik

Autor dále upozorňuje na neudržitelný model, v němž má být ředitel školy současně pedagogickým lídrem, personalistou, krizovým manažerem, správcem budovy a navíc expertem na kybernetickou bezpečnost a GDPR. Jako funkční řešení prezentace uvádí model sdílených kapacit, v němž ORP nebo kraj zaměstnává profesionální bezpečnostní a datový tým. Sdílený DPO a architekt bezpečnosti pak mohou školám poskytovat metodické vedení, společnou DPIA na školní informační systémy, centrální audit dodavatelů a synergie při nákupu licencí.

V řízení rizik autor představil cyklus šesti kroků: identifikaci hrozeb, identifikaci zranitelností, ohodnocení rizika, výpočet rizikového skóre, návrh opatření a akceptaci zbytkového rizika vedením školy. Tento cyklus se má opakovat ročně, po incidentu nebo při změně. Za častou chybu autor označuje obrácené pořadí kroků, kdy škola nejprve nakupuje kamery a firewall, technika přichází bez znalosti rizik, školení je až poslední a analýza rizik chybí. Doporučené pořadí naopak začíná auditem a analýzou rizik, pokračuje organizačními opatřeními a pravidly, školením a nácviky a teprve poté technickými opatřeními.



Závěr prezentace

V závěru autor formuluje čtyři kroky pro reálnou odolnost školství: metodickou unifikaci od MŠMT a NÚKIB, závazný minimální standard dat a bezpečnosti, podporu modelu sdílených pověřenců DPO a CISO a pojetí lidského faktoru jako skutečné první linie obrany. Prezentace uzavírá, že škola jako kritická infrastruktura nechrání pouze kabely a servery, ale především digitální identitu a soukromí dětí.

Závěrečný snímek shrnuje, že praxe posledních let potvrzuje útoky na malé i velké instituce, univerzity i venkovské školy. Podle autora je nejlevnější obranou minimalizace dat, proškolení lidí a funkční, nikoli formální DPO. Odolnost školství má být podle prezentace postavena na systémové správě rizik, nikoli pouze na technických řešeních.





Krajské vojenské velitelství jako partner škol při implementaci bezpečnostních témat do výuky

plk. gšt. Ing. Alois Matýzka, Krajské vojenské velitelství Brno

Rešerše vystoupení



Úvodní slide prezentace použitý jako obrazové uvedení rešerše.

Zaměření prezentace

Plukovník gšt. Ing. Alois Matýzka, ředitel KVV Brno, ve své prezentaci představil Krajské vojenské velitelství Brno jako partnera škol při implementaci bezpečnostních témat do výuky. Autor prezentace vymezil tři hlavní obsahové okruhy:

- brannou povinnost,
- dobrovolné vojenské cvičení pro studenty středních škol
- a přípravu občanů k obraně státu, tedy POKOS.

Prezentace je zpracována jako stručný a věcný přehled. Ppracuje s vybranými body, které mají ředitelům škol a vedení škol přiblížit základní rámec spolupráce s Krajským vojenským velitelstvím Brno a ukázat, jak mohou být témata obrany státu a krizové připravenosti promítána do školního prostředí.

Branná povinnost

V první části pan plukovník Matýzka uvádí právní základ branné povinnosti. Odkazuje na zákon č. 585/2004 Sb., o branné povinnosti a jejím zajišťování, tedy na branný



zákon. Podle prezentace vzniká všem občanům České republiky po dovršení 18 let věku branná povinnost.

Autor dále prezentoval roli krajských vojenských velitelství při informování občanů, kteří dosáhli věku 18 let. Krajská vojenská velitelství těmto občanům sdělují vznik branné povinnosti a informují je o jejím obsahu a možnostech převzetí.

V prezentaci je zároveň rozlišeno, že občan plní brannou povinnost za stavu ohrožení státu nebo za válečného stavu. V době míru je podle uvedených podkladů branná povinnost založena na dobrovolnosti.

Autor v této souvislosti jmenuje několik možností zapojení:

- vojáka z povolání,
- aktivní zálohu,
- dobrovolné vojenské cvičení
- a dobrovolné předurčení.

Dobrovolné vojenské cvičení pro studenty středních škol

Druhá část prezentace se věnuje dobrovolnému vojenskému cvičení pro studenty středních škol. Jak autor uvádí, podle § 5a zákona č. 585/2004 Sb. může občan, který dovršil 18 let věku, v době míru dobrovolně převzít brannou povinnost a požádat o účast na vojenském cvičení.

Plukovník Matýzka dále připomíná, že v roce 2025 vznikl projekt dobrovolného vojenského cvičení pro studenty středních škol, který probíhá v červenci daného roku. Prezentace uvádí i konkrétní podmínky účasti. Patří mezi ně podání žádosti v termínu listopad až březen, dosažení věku 18 let, zdravotní způsobilost k výkonu služby a studium ve 2. až 4. ročníku střední školy, včetně 1. až 2. ročníku nástavbového studia.

Autor zároveň prezentoval údaje o účasti studentů na dobrovolném vojenském cvičení v roce 2026. Celorepublikově podle prezentace nastoupilo 1 132 studentů. V Jihomoravském kraji bylo podáno 150 žádostí, z toho 91 studentů nastoupilo a 81 výcvik dokončilo.

Příprava občanů k obraně státu - POKOS

Třetím tematickým okruhem byla příprava občanů k obraně státu, označovaná zkratkou POKOS. Podle prezentace POKOS umožňuje občanům České republiky rozvíjet znalosti, dovednosti a návyky potřebné k účinnému zvládnutí vojenských i nevojenských krizových situací.

Autor zde odkazuje na § 52 zákona č. 222/1999 Sb., o zajišťování obrany České republiky. Jak je v prezentaci uvedeno, POKOS má charakter vzdělávání a provádí se



na základních a středních školách ve spolupráci Ministerstva obrany s Ministerstvem školství, mládeže a tělovýchovy, a to v rámci rámcově vzdělávacího programu.

Součástí prezentace je také zmínka o Koncepti POKOS 2025-2030. Příprava podle autora probíhá formou vzdělávacích a osvětových aktivit. Prezentace uvádí projektové dny ve spolupráci s Českým červeným křížem, plánovanou spolupráci s Policií České republiky v oblasti prevence a kritického myšlení, dále přednášky, besedy a školení pedagogů. Školení pedagogů je v prezentaci doplněno o instrukčně metodické zaměstnání Policie České republiky k tématu „Aktivní střelec“. Výhledově autor zmiňuje také aktivitu pro stávající a budoucí pedagogy s názvem „V kůži vojáka“.

Význam pro školy

Z podkladové prezentace vyplývá, že Krajské vojenské velitelství Brno nabízí školám partnerství zejména v oblasti přenosu bezpečnostních a obranných témat do výuky. Plukovník gšt. Ing. Alois Matýzka prezentoval tuto spolupráci na třech rovinách:

- právní informovanost o branné povinnosti,
- možnost dobrovolného vojenského cvičení pro plnoleté studenty středních škol
- a vzdělávací a osvětové aktivity v rámci POKOS.

Ve vztahu ke školám je podstatné, že prezentace pracuje se vzdělávacím charakterem těchto témat. Nejde pouze o informaci o armádě nebo branné povinnosti, ale o možnost rozvíjet znalosti, dovednosti a návyky potřebné pro zvládání krizových situací. Právě tento vzdělávací rozměr propojuje obsah prezentace s širším zaměřením konference ASKI na bezpečnost, odolnost a praktickou připravenost školního prostředí.

Shrnutí

Prezentace plukovníka gšt. Ing. Aloise Matýzky byla zaměřena stručně, prakticky a7 informačně. Autor představil základní rámec branné povinnosti, vysvětlil možnost dobrovolného vojenského cvičení pro studenty středních škol a popsal POKOS jako vzdělávací nástroj pro rozvoj znalostí, dovedností a návyků potřebných ke zvládání vojenských i nevojenských krizových situací.

Hlavní sdělení prezentace lze shrnout tak, že Krajské vojenské velitelství Brno může být pro školy partnerem při implementaci bezpečnostních témat do výuky, a to zejména prostřednictvím informování, vzdělávacích a osvětových aktivit, projektových dnů, přednášek, besed a školení pedagogů.



Potenciál Národní soustavy kvalifikací pro oblast kritické infrastruktury

Mgr. Richard Veleta, Ph.D., NPI ČR, správce Národní soustavy kvalifikací

Rešerše vystoupení



Text je zpracován jako stručná redakční rešerše prezentace. Vychází pouze z informací uvedených v podkladové prezentaci autora a nepřidává další externí obsah.

Zaměření prezentace

Mgr. Richard Veleta, Ph.D. ve své prezentaci představil téma „Potenciál Národní soustavy kvalifikací (NSK) pro oblast kritické infrastruktury“. Vystoupení bylo zařazeno do programu konference ASKI „Odpovědnost ředitelů škol v oblasti kritické infrastruktury a kybernetické bezpečnosti podle nové legislativy“, která se konala dne 22. září 2026 ve Střední škole informatiky, poštovníctví a finančnictví Brno. Autor v úvodním slidu vystupuje za Národní pedagogický institut jako správce Národní soustavy kvalifikací.

Autor nejprve představil Národní soustavu kvalifikací jako systém dostupný prostřednictvím portálu www.narodnikvalifikace.cz. K datu 22. září 2026 prezentace uvádí 1448 profesních kvalifikací, 1257 autorizovaných osob a 444 417 vydaných osvědčení. Tím byl vytvořen základní rámec pro další část vystoupení, která se věnovala tomu, jak lze existující profesní kvalifikace vztáhnout k bezpečnosti škol, kritické infrastruktury a kybernetické bezpečnosti.



Odpovědnost škol, zřizovatelů a MŠMT

Richard Veleta si v prezentaci dovilil parafrázovat název konference. Vedle odpovědnosti ředitelů škol výslovně doplnil také odpovědnost zřizovatelů škol a MŠMT v oblasti kritické infrastruktury a kybernetické bezpečnosti. Tím autor rozšířil pohled z jedné řídicí funkce školy na širší systém odpovědnosti, ve kterém mají své místo škola, její zřizovatel i ministerská úroveň.

V prezentaci následně připomněl citaci Dušana Kaláška ze Zpravodaje ASKI, podle níž směr zůstává stejný: **propojovat vzdělávání, bezpečnost, kritickou infrastrukturu, kybernetickou bezpečnost, krizové řízení a praktickou připravenost organizací**. Autor tím zasadil téma NSK do širšího rámce odborných aktivit ASKI a nové legislativní reality.

Možnosti využívání profesních kvalifikací školami

Jak autor uvádí, profesní kvalifikace NSK spojené s oblastí kritické infrastruktury a kybernetické bezpečnosti mohou školy využívat dvěma základními způsoby. První možností je zaměstnávat profesionály, kteří jsou držiteli osvědčení NSK, případně využívat jejich služeb. Druhou možností je aktivní využití profesních kvalifikací samotnými školami.

V tomto druhém směru prezentace rozlišuje několik rolí:

- škola může působit jako autorizovaná osoba, tedy zkoušet podle zákona č. 179/2006 Sb.;
- může vystupovat jako vzdělavatel dospělých a nabízet přípravné kurzy;
- a může využívat profesní kvalifikace také ve výuce vlastních oborů.

Autor tak prezentoval NSK nejen jako databázi kvalifikací, ale jako praktický nástroj, který může vstupovat do personální, vzdělávací i odborné činnosti školy.

Pět oblastí kvalifikací pro bezpečnost škol

Mgr. Veleta dále uvádí, že v Národní soustavě kvalifikací neexistuje jedna úzce specializovaná profesní kvalifikace určená výhradně pro „bezpečnost škol“. Současně však prezentace zdůrazňuje, že bezpečnost a ochranu infrastruktury ve vzdělávacích zařízeních pokrývá několik klíčových profesních kvalifikací rozdělených do pěti oblastí.

- Fyzická ostraha, režimová opatření a kontrola vstupu.
- Strategické řízení bezpečnosti a ochrana měkkých cílů.
- Bezpečnost provozu a prevence rizik, tedy BOZP a požární ochrana.
- Technická správa budov a areálů.
- Kybernetická bezpečnost.



Autor poté jednotlivé oblasti konkretizoval prostřednictvím vybraných profesních kvalifikací a jejich významu pro školské prostředí.

Vybrané kvalifikace a jejich význam pro školy

V oblasti fyzické ostrahy, režimových opatření a kontroly vstupu prezentace uvádí kvalifikace Strážný / strážná, Bezpečnostní referent / referentka a Pracovník / pracovnice ostrahy veřejných akcí. U kvalifikace Strážný autor zmiňuje kontrolu vstupu osob a vjezdu vozidel, odbavení návštěv, prevenci vnesení nebezpečných předmětů a látek, pochůzkovou činnost a obsluhu základních mechanických a elektronických zábranných systémů. Bezpečnostní referent je v prezentaci spojen s vedoucí ostrahy na univerzitních kampusech nebo velkých školních areálech. Pracovník ostrahy veřejných akcí je podle autora klíčový při pořádání hromadných školních akcí.

V oblasti strategického řízení bezpečnosti a ochrany měkkých cílů autor prezentoval kvalifikaci Bezpečnostní manažer / manažerka v obchodě a službách. Přestože název směřuje k obchodu a službám, standard podle prezentace definuje komplexní řízení security i safety, zahrnuje analýzu rizik, tvorbu provozních a traumatologických řádů, krizových směrnic a výběr bezpečnostních technologií. Autor tuto kvalifikaci označil jako nejbližší kvalifikační ekvivalent pro pozici bezpečnostního manažera školy nebo univerzity.

V oblasti BOZP a požární ochrany autor uvádí kvalifikace Technik / technička BOZP a Manažer / manažerka BOZP. Technik BOZP je v prezentaci spojen s identifikací a vyhodnocováním rizik v odborných učebnách, dílnách, laboratořích i tělocvičnách, se stanovováním preventivních opatření, tvorbou interní bezpečnostní dokumentace a školením personálu. Manažer BOZP je podle autora vhodný pro velké školské správy, univerzitní rektoráty nebo zřizovatele více školních zařízení.

Technickou správu budov a areálů prezentace spojuje s kvalifikacemi Domovník / domovnice, Správce / správkyň nemovitostí a Facility manažer / manažerka. U domovníka autor uvádí kontrolu technického stavu budovy, uzamykacích mechanismů, únikových cest, osvětlení a odhalování technických havárií. Správce nemovitostí je v prezentaci spojen s technickým dohledem nad infrastrukturou, revizemi a protipožárními systémy. Facility manažer podle prezentace odpovídá za strategickou integraci lidí, prostorů, procesů a technologií v celém areálu.

Samostatnou oblast tvoří profesní kvalifikace z oblasti kybernetické bezpečnosti. Autor v prezentaci uvádí kvalifikace Analytik/analytická kybernetické bezpečnosti, Manažer/manažerka kybernetické bezpečnosti, Architekt/architektka kybernetické bezpečnosti, Auditor/auditorka kybernetické bezpečnosti, Technik/technička kybernetické bezpečnosti a Pracovník/pracovnice bezpečnostního dohledového centra informačních systémů.



Navržené kvalifikace a další rozvoj NSK

V závěrečné části prezentace autor upozornil také na kvalifikace, které byly do NSK navrženy, ale zatím nebyla zadána jejich příprava. Prezentace mezi nimi uvádí Manažera kritické infrastruktury navrženého ASKI, krizového intervenanta a koordinátora bezpečnosti veřejného prostoru.

Mgr. Richard Veleta, Ph.D. zároveň ukázal, že profesní kvalifikaci je možné navrhnout prostřednictvím formuláře „*Návrh na tvorbu nové profesní kvalifikace NSK*“.

Shrnutí řešerše

Prezentace Mgr. Richarda Velety, Ph.D. ukázala Národní soustavu kvalifikací jako nástroj, který může být využitelný pro oblast kritické infrastruktury, bezpečnosti škol a kybernetické bezpečnosti. Autor nepředstavil jednu hotovou kvalifikaci pro bezpečnost školy, ale poukázal na soubor existujících profesních kvalifikací, které mohou společně pokrýt různé části bezpečnostní reality školského prostředí.

Hlavním sdělením prezentace je, že bezpečnost školy může být nahlížena přes více profesních oblastí: od fyzické ostrahy a režimových opatření přes strategické řízení bezpečnosti, BOZP, technickou správu areálu až po kybernetickou bezpečnost. Národní soustava kvalifikací tak podle prezentace nabízí rámec, který mohou školy, zřizovatelé i další aktéři využívat při zaměstnávání odborníků, přípravě kurzů, autorizovaném zkoušení i rozvoji výuky.



Témata ochrany obyvatelstva jako součást RVP

Ing. Josef Myslín, Ph.D., Ed.D., MSc., MPA, CEVRO Univerzita

Rešerše vystoupení



Poznámka: Tento text je stručnou redakční rešerší zpracovanou výhradně z přiložené prezentace autora. Nejde o autorizovaný přepis vystoupení ani o doplnění obsahu mimo podklady uvedené v prezentaci.

Zaměření prezentace

Autor prezentace, Ing. Josef Myslín, Ph.D., Ed.D., MSc., MPA z Katedry bezpečnostních studií CEVRO Univerzity, představil téma ochrany obyvatelstva jako součásti rámcových vzdělávacích programů. V úvodním vymezení se jeho příspěvek soustředil na otázku, proč má být ochrana obyvatelstva přítomna ve školách a jaké místo může mít ve vzdělávání.

Jak autor uvádí, důvodem pro zařazení tématu ochrany obyvatelstva do školního prostředí je rostoucí počet mimořádných událostí. Prezentace jako příklady uvádí povodně, požáry, výpadky infrastruktury a hrozbu válečného konfliktu. Dr. Ing. Josef Myslín zároveň upozorňuje na nízkou připravenost obyvatelstva, kdy lidé často nevědí, jak správně reagovat, rizika bagatelizují nebo je dokonce popírají.

Ochrana obyvatelstva a role školy

Autor ochranu obyvatelstva vymezuje jako soubor opatření, který zahrnuje ochranu života, zdraví a majetku při mimořádných událostech. V prezentaci je ochrana obyvatelstva popsána jako oblast, která zahrnuje prevenci, represi i řešení následků. Prevence je spojena s předcházením mimořádným událostem, přípravou na jejich zvládnutí a opatřeními k minimalizaci jejich následků. Represe znamená zvládnutí



samotné mimořádné události, pokud nastane, a řešení následků je popsáno jako činnost směřující k obnově stavu před mimořádnou událostí.

V této souvislosti autor používá také pojem resilience. V prezentaci ji vysvětluje jako schopnost zvládnout mimořádnou událost a vyjít z ní pokud možno nezraněn či posílen. Zároveň zdůrazňuje, že na ochraně obyvatelstva se musí podílet státní složky, složky integrovaného záchranného systému, ale také samotní občané, a to aktivně i pasivně.

Škole Ing. Myslín přisuzuje výchovnou funkci. Podle prezentace škola formuje návyky a odpovědnost, poskytuje informace a měla by učit kritickému myšlení a informační gramotnosti. Právě tato výchovná role je v prezentaci spojena s potřebou zahrnout témata ochrany obyvatelstva do vzdělávání.

Legislativní a kurikulární rámec

V části věnované legislativnímu rámci autor uvádí několik důležitých dokumentů. Jmenuje krizový zákon a ústavní zákon o bezpečnosti České republiky, které podle prezentace řeší řízení státu při krizích, definují krizové stavy a opatření pro krizové stavy. Dále zmiňuje zákon o integrovaném záchranném systému, který vymezuje spolupráci záchranných složek.

Autor dále uvádí koncepci ochrany obyvatelstva, která stanovuje dlouhodobé cíle a principy fungování ochrany obyvatelstva. V návaznosti na školy prezentace pracuje také s RVP, tedy rámcovými vzdělávacími programy, které podle autora řeší základní parametry vzdělávacího programu školy a na něž následně navazují školní vzdělávací programy.

Ochranu obyvatelstva v RVP autor označuje za průřezové téma. Výslovně uvádí, že nejde a nemá jít o samostatný předmět. Příslušná témata by se podle prezentace měla objevit v mnoha předmětech a měla by tvořit ucelený rámec. Autor zde zmiňuje vzdělávací oblasti jako Člověk a zdraví a Člověk a společnost a upozorňuje také na mezipředmětové vazby.

Cíle výuky a tematické okruhy

V části zaměřené na cíle výuky autor uvádí tři hlavní směry: rozpoznání rizik, správnou reakci a odpovědnost. Žáci by podle prezentace měli identifikovat nebezpečné situace a chápat, že žijeme ve světě, ve kterém existuje riziko mimořádných událostí. Současně se mají učit, jak na nebezpečí správně reagovat, a mají chápat legislativní a procesní aspekty řešení mimořádných událostí.

Ing. Josef Myslín dále uvádí, že žáci mají znát, mít a umět obsluhovat potřebné základní vybavení pro osobní potřeby. V oblasti odpovědnosti prezentace zdůrazňuje, že žáci mají chápat sdílenou odpovědnost za bezpečnost mezi státem, jeho složkami



a občany. Autor zároveň uvádí, že žáci mají akceptovat, že součástí pojmu vlastnictví je také minimální objem zapojení se.

Mezi možné tematické okruhy prezentace řadí fundamentální principy, tedy základy legislativy a základy koncepce ochrany obyvatelstva, dále požární ochranu, první pomoc, evakuaci, nouzové přežití a varovné signály. U evakuace autor zmiňuje bezpečné opuštění prostoru a evakuační zavazadlo, u varovných signálů pak znalost varovných signálů a reakci na výstrahy.

Formy výuky, spolupráce s IZS a výzvy

Autor prezentoval také možné formy a metody výuky. Teoretickou přípravu označuje navzdory její neoblíbenosti za nutnou, protože bez základní teorie nelze postoupit k praxi. Současně uvádí, že i teorie se dá učit zajímavým a přijatelným způsobem. Další formou jsou simulace, tedy modelové situace pro pochopení evakuace, zajištění nouzového přežití, reakce na varovný signál nebo využití prostředků ochrany obyvatelstva.

Jako další metodu prezentace uvádí projektové dny, které mají propojovat teorii a praxi a umožňovat řešení konkrétních problémů. V návaznosti na to autor zdůrazňuje spolupráci s IZS. U hasičů uvádí praktické ukázky a zkušenosti, u zdravotníků výuku první pomoci a u Policie ČR nebo městské policie bezpečnost a prevenci. Společné akce podle prezentace zvyšují realističnost výuky a učí žáky, že spolupráce se složkami IZS je normální chování vyspělého občana.

V závěrečné části autor pojmenovává výzvy ve výuce. Uvádí nedostatek času, omezený prostor v kurikulu a souboj předmětů o hodinovou dotaci. Dále upozorňuje na nedostatek materiálů, chybějící metodickou podporu, chybějící studijní materiály a chybějící koncepci. Téma ochrany obyvatelstva je podle prezentace často podceňováno a snahy o jeho řešení jsou označovány jako strašení nebo válečné štvání.

Závěr prezentace

Závěrem autor zdůrazňuje potřebu systematického postupu. Podle prezentace je nutné identifikovat potřeby a oblasti, určit vhodná místa v RVP, kam tato témata zařadit, vytvořit kvalitní materiály ve spolupráci s příslušnými odborníky a institucemi a vyškolit učitele. Ing. Josef Myslín zároveň uvádí, že zásadní je politická podpora.

Autorovo závěrečné sdělení lze shrnout tak, že nejde o strašení ani bagatelizaci, ale o reálné pojmenování rizik. Prezentace zdůrazňuje, že je třeba do oblasti investovat, přičemž autor výslovně dodává, že nejde jen o peníze. Téma ochrany obyvatelstva tak v jeho pojetí patří do vzdělávání jako průřezová, praktická a odpovědnostní oblast, která má žáky připravovat na zvládání mimořádných událostí a na vědomé zapojení do bezpečnosti společnosti.



Kde stojí člověk a kde AI

Mgr. Vojtěch Kašpárek MBA

Rešerše vystoupení Konference ASKI, 2026



Redakční rešerše prezentace

Mgr. Vojtěch Kašpárek, MBA ve své prezentaci s názvem „Kde stojí člověk a kde AI“ otevřel otázku postavení člověka a umělé inteligence v prostředí českého školství. V úvodu autor zařadil téma do rámce konference ASKI 2026 a navázal na motiv TeacherOS, u něhož položil otázku, zda je v českém školním prostředí možná symbióza s AI.

Autor prezentoval opakující se formulaci „*Hodnocení vytvořeno ve spolupráci s AI*“. Tato věta v prezentaci tvoří jednu z hlavních os vystoupení.

Postupně je doplňována o jednotlivé pojmy, které autor uvádí jako součást práce s AI: kontext, agenty, ústavu, druhý mozek, validaci a anonymizaci. Z prezentace vyplývá, že samotné využití AI není oddělené od pravidel, vstupních podkladů, ověřování a ochrany informací.

V dalších snímcích Mgr. Vojtěch Kašpárek, MBA pracoval s principem „*Human in the loop*“. Ten je v prezentaci opakován jako zásadní rámec pro spolupráci člověka a AI. Autor tím ukazuje, že člověk nemá z procesu mizet, ale má zůstat jeho aktivní součástí. V prezentaci se tento princip objevuje společně s formulací „Hodnocení bylo vytvořeno ve spolupráci s AI“ a s pojmy ústava, kontext, guardrails a agent.



Autor dále odkazuje na koncept „*Meaningful human control*“ podle Santoni de Sio a van den Hoven z roku 2018. V prezentaci jsou k tomuto konceptu uvedeny tři prvky: tracking, tracing a reagování na lidský úsudek. Současně je zde zdůrazněna dohledatelnost rozhodnutí. V návaznosti na to prezentace pracuje s tím, že při využívání AI musí být možné sledovat postup, dohledat rozhodnutí a zároveň zachovat prostor pro lidský úsudek.

Vojtěch Kašpárek v prezentaci upozornil také na riziko návyku na AI. Uvádí citaci podle Bansal et al. z roku 2021: „Nebezpečí není strach z AI. Nebezpečí je, že si na ni zvyknete a přestanete se dívat.“ Tato část vystoupení působí jako varování před nekontrolovaným spoléháním se na výstupy umělé inteligence. V logice prezentace je proto důležitá validace a průběžná lidská kontrola.

Ve střední části prezentace autor rozvíjel souvislost mezi Human in the loop a nástroji, které mají činnost AI usměrňovat. Objevují se zde pojmy ústava, kontext, guardrails a agent. Prezentace tyto pojmy nerozvádí do rozsáhlých definic, ale pracuje s nimi jako s prvky systému, v němž má být spolupráce člověka a AI řízena a ohraničena.

Důležitou součástí je přitom anonymizace a validace.

Na samostatném snímku autor shrnul vazbu mezi tracking, tracing a learning. Tracking je v prezentaci spojen s reagováním na lidský úsudek, tracing s dohledatelnými rozhodnutími a learning s tím, že pedagog ladí vlastní systém. Z této části vyplývá, že autor nevnímá AI pouze jako jednorázový nástroj, ale jako systém, který se má používat způsobem umožňujícím dohled, kontrolu a postupné nastavování ze strany pedagoga.

V závěru prezentace Mgr. Vojtěch Kašpárek, MBA uvedl citaci F. Dřímalky z roku 2026: „*Technologické firmy začínají vyžadovat systémy, které jsou napojené na AI.*“ Autor poté uzavírá prezentaci otázkou, zda je princip „Human in the loop“ odpovědí na dnešní compliance pravidla. Závěr tedy nesměřuje k jednoznačnému technickému návodu, ale k formulaci otázky po odpovědném, kontrolovaném a pravidly ohraničeném využívání AI ve školním prostředí.

Celkově prezentace pracuje s umělou inteligencí nikoli jako s izolovanou technologií, ale jako s tématem, u něhož je nutné řešit roli člověka, pravidla, kontext, validaci, anonymizaci, dohledatelnost a schopnost reagovat na lidský úsudek. Autorovo vystoupení tak podle podkladových materiálů směřovalo k otázce, kde má stát člověk v prostředí, v němž AI začíná vstupovat do práce školy a pedagogického rozhodování.

Umělá inteligence na hranici mezi pomocí a závislostí

Dr. Ing. Evžen Šanc

Rešerše vystoupení



Základní rámec vystoupení

Dr. Ing. Evžen Šanc ve své prezentaci „*Umělá inteligence na hranici mezi pomocí a závislostí*“ představil téma umělé inteligence v prostředí škol především jako oblast, která má současně bezpečnostní, technologický i psychologický rozměr. Autor se na úvod představil jako systémový analytik v oblasti IT s více než 35 lety zkušeností v informačních technologiích. Uvedl také specializaci na vývoj v .NET, integraci systémů a aktivní využívání umělé inteligence v praxi, včetně certifikací společnosti Microsoft, mimo jiné AI Fundamentals (AI-900).

Autor prezentoval téma útoků na školy v souvislosti s AI jako dvě odlišné, ale vzájemně propojené skupiny rizik. První skupinou je kybernetické ohrožení školy, které může přicházet zvenčí i zevnitř, přičemž AI podle prezentace výrazně mění možnosti útočníků. Druhou skupinou je fyzické a psychologické ohrožení školy zevnitř, tedy násilné nebo vysoce rizikové chování žáků a krizové situace.

Kybernetické ohrožení školy

V části věnované kybernetickému ohrožení školy Dr. Ing. Šanc uvádí, že online svět je součástí každodenního života studentů. Osobní údaje, fotografie a chování žáků vytvářejí digitální stopu a internet může podle autora ovlivnit psychiku, vztahy i reputaci. Kybernetické útoky autor členil na útoky zvenčí, útoky zevnitř, využití AI jako nástroje útočníka a současně také AI jako nástroje obrany.



Autor dále prezentoval konkrétní přehled kybernetických útoků ve spojení s AI. U phishingu uvádí možnost AI generovaných věrohodných e-mailů směřovaných na učitele, vedení školy nebo rodiče. U sociálního inženýrství upozorňuje, že AI umožňuje personalizovat útok podle informací o škole. V prezentaci jsou dále uvedeny deepfake hlasu nebo videa učitele, ředitele či jiné autority, krádeže účtů, ransomware, DDoS útoky, malware, insider threat a AI jako pomocník útočníka při generování textů, překladu, průzkumu nebo automatizaci sociálního inženýrství.

V oblasti obrany proti kybernetickým útokům autor představil základní technická opatření. Patří mezi ně aktualizace softwaru a používání antivirových programů, používání silných hesel a dvoufaktorového ověření a pravidelné zálohování důležitých dat. Ve vztahu k AI v obraně prezentace uvádí detekci anomálií, phishingu a podporu incident response.

Dr. Ing. Evžen Šanc v prezentaci zároveň uvádí, že většina běžných základních a středních škol nespadá pod nový zákon, přesto jim NÚKIB doporučuje zavést alespoň základní bezpečnostní opatření. Autor také připomíná, že NÚKIB má samostatný obsah zaměřený na střední školy, mimo jiné na kyberšikanu, sexting, sextortion a další specifická rizika středoškoláků.

Fyzické a psychologické ohrožení školy zevnitř

Druhá tematická část prezentace se věnovala fyzickému a psychologickému ohrožení školy zevnitř. Autor zde jako fyzické incidenty uvádí násilí mezi studenty, útok na učitele, závažné krizové situace a incidenty s včasnými varovnými signály. V této souvislosti Dr. Ing. Šanc přesouvá pozornost od čistě technického pojetí AI ke školnímu prostředí, v němž mohou digitální nástroje souviset i s psychickou zátěží, rizikovým chováním nebo krizovou komunikací mladého člověka.

Ve vztahu ke středoškolákům autor prezentoval tři specifika: samostatné používání ICT při nízkém povědomí o rizicích, skutečnost, že méně než polovina studentů chrání mobilní zařízení antivirem, a také to, že anonymita podporuje rizikové chování a sexting. Tyto body autor v prezentaci řadí mezi faktory, které je nutné při práci se středoškolskou populací zohlednit.

AI jako psychologické prostředí a nástroj rizikového jednání

V části věnované jednotlivým fenoménům a důkazům autor rozlišil několik tvrzení podle míry doložení. Chatbot jako emoční podpora je v prezentaci označen jako dobře doložený fenomén. Souvislost s osamělostí je označena jako asociace, problematické používání jako oblast s rostoucí evidencí a posilování bludných interpretací jako oblast klinických případů. Naopak tvrzení, že AI způsobuje psychózu, agresivitu nebo školní útoky, autor v prezentaci označuje jako neprokázaná. Možnost, že AI může být použita při přípravě násilí, je v prezentaci uvedena jako oblast jednotlivých případů.



Autor následně pracuje s otázkou, co když škola vůbec neví, že student prochází krizí, protože jeho hlavním „konzultantem“ není člověk, ale AI chatbot. Prezentace rozlišuje dvě linie. První označuje jako AI jako psychologické prostředí. V této linii se objevuje psychická zátěž, sociální izolace, AI jako důvěrník, rostoucí závislost na AI, potvrzování určitých interpretací reality, zhoršování psychického stavu u zranitelného jedince a následná krize nebo rizikové chování.

Druhou linii autor označuje jako AI jako nástroj rizikového jednání. Zde prezentace popisuje rizikového jedince, AI jako nástroj, hledání, simulaci nebo plánování a následné konkrétní rizikové jednání. V obou liniích tak autor zůstává u rozlišení mezi prostředím, které může působit na zranitelného jedince, a nástrojem, který může být použit při rizikovém jednání.

Digitální závislost a závislost na chatbotech

Samostatná část prezentace se věnovala digitální závislosti. Dr. Ing. Šanc ji v podkladech spojuje s nadměrným používáním sociálních sítí, her nebo sázení. Jako projevy prezentace uvádí zhoršení prospěchu, poruchy spánku a izolaci. Jako možná řešení jsou uvedeny nastavení limitů, offline aktivity a rovnováha.

Autor dále samostatně upozorňuje na závislost na chatbotech a AI. Podle prezentace mohou AI chatboti vyvolat pocit porozumění a přátelství. Současně však autor uvádí riziko úniku z reality a oslabení skutečných vztahů. Závěr této části je formulován jako doporučení užívat AI jako nástroj, nikoli jako náhradu mezilidského kontaktu.

Závěry pro školy

V závěru prezentace autor shrnul několik bodů určených školám. Jak Dr. Ing. Evžen Šanc uvádí, část krizové komunikace mladého člověka může probíhat mimo lidské vztahy, tedy v AI. Současně ale prezentace výslovně uvádí, že nejde o sledování soukromých konverzací studentů. Jde o schopnost rozpoznat změny v chování a další varovné signály.

Autor dále zdůraznil potřebu jasného postupu školy. Tento postup má podle prezentace určit, kdo signál zachytí, kdo situaci vyhodnotí, kdo zapojí rodiče a odborníky a kdy se aktivuje krizový plán. Posledním bodem závěru je důraz na prevenci zaměřenou na konkrétní chování a rizikové signály, nikoli na nálepkování studentů s duševními obtížemi.

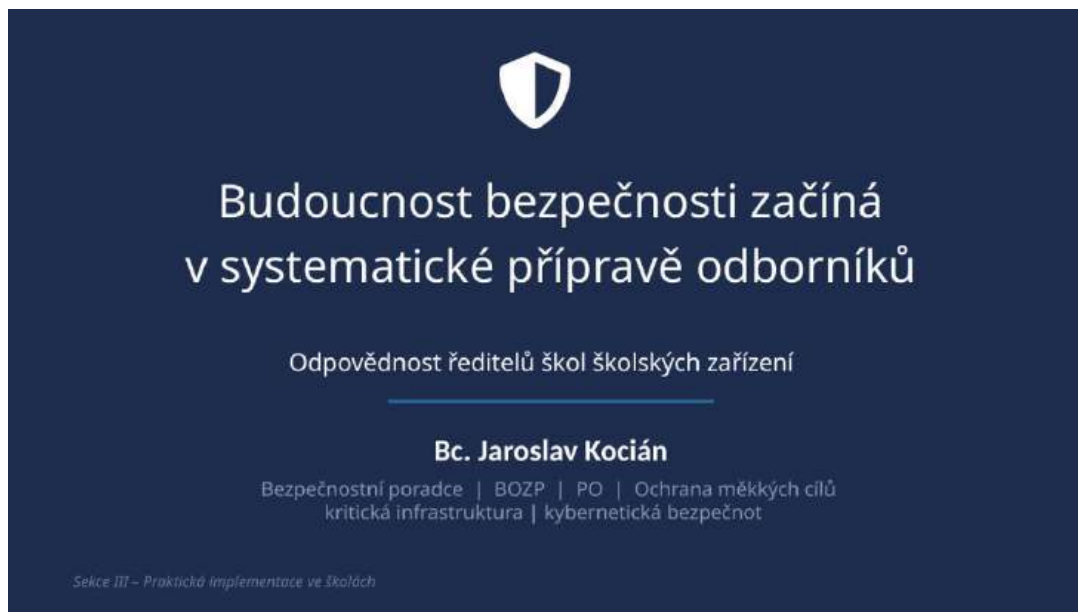
Celkově prezentace představuje umělou inteligenci nikoli pouze jako technický nástroj, ale jako fenomén, který se ve školním prostředí může dotýkat kybernetické bezpečnosti, psychologické zranitelnosti, rizikového chování, digitální stopy i krizové připravenosti. Rešerše vychází pouze z informací uvedených v prezentaci autora a nepřidává k nim další externí výklad.



Budoucnost bezpečnosti začíná v systematické přípravě odborníků

Bc. Jaroslav Kocián

Rešerše prezentace



Zaměření prezentace

Bc. Jaroslav Kocián ve své prezentaci vystoupil s tématem „*Budoucnost bezpečnosti začíná v systematické přípravě odborníků*“. V úvodním slidu autor vymezuje svůj odborný rámec oblastmi bezpečnostního poradenství, BOZP, požární ochrany, ochrany měkkých cílů, kritické infrastruktury a kybernetické bezpečnosti. Prezentace byla zařazena do části věnované praktické implementaci ve školách.

Jak autor uvádí, bezpečnostní prostředí se dramaticky proměnilo. Mezi hlavní důvody, proč je třeba se tématu věnovat právě nyní, řadí hybridní hrozby, kybernetické útoky a fyzické hrozby na školy i ve školách. Současně upozorňuje na legislativní rámec, zejména NIS2, nový zákon o kybernetické bezpečnosti a zákon o krizovém řízení, které podle prezentace vyžadují nové kompetence. Školy označuje za měkké cíle se specifickou zranitelností, kterou dosavadní systém podle autora nedostatečně vnímá.

Diagnóza současného stavu

Bc. Kocián prezentoval jako klíčovou tezi větu, že „systém je tak silný, jak jsou silní lidé, kteří ho obsluhují“. Na tuto myšlenku navazuje jeho popis toho, co ve školním prostředí chybí. Autor zmiňuje roztříštěnost rolí, kdy se BOZP, požární ochrana, kybernetická bezpečnost nebo agenda DPO řeší izolovaně. Podle prezentace chybí



bezpečnostní pracovník nebo manažer a zároveň neexistuje komplexní profil odborníka se zaměřením na školství.

Autor dále uvádí, že školy jako měkké cíle vyžadují komplexní přístup. Za problematické považuje také nedostatečnou dokumentaci, protože podle prezentace řada škol a školských zařízení nemá ani základní bezpečnostní dokumentaci v požadované úrovni. V části věnované školám jako měkkým cílům Kocián poukazuje na otevřené budovy, snadný přístup, minimální kontrolu vstupů, velké počty dětí a nízkou bezpečnostní kulturu, kdy personál nemusí mít bezpečnostní školení.

Nový rozměr bezpečnosti škol

Autor prezentoval svoje tvrzení, že geopolitická situace, válka na Ukrajině a hybridní válka zásadně mění bezpečnostní rámec. Ve školách podle něj nestačí uvažovat pouze evakuační plány pro případ požáru. Prezentace výslovně uvádí potřebu zohlednit také útok na měkký cíl, blackout, chemickou nebo technickou havárii a další situace. Školy jsou zde popsány také jako potenciální krizová centra a úkryty v komunitě, přičemž autor zmiňuje zpracovávání plánů krizové připravenosti.

Ve vztahu k pedagogům Bc. Jaroslav Kocián uvádí, že v krizové situaci mohou být právě pedagogové těmi, kdo rozhodují o bezpečnosti desítek dětí. Prezentace proto pracuje s pojmem „první respondenti“ a zdůrazňuje psychologickou připravenost, zvládání stresu, základy první pomoci a komunikaci s dětmi v krizi. Odborník ve školství podle autora nemá znát jen BOZP, BOZ a požární ochranu, ale také krizové řízení, ochranu měkkých cílů a ochranu osobních údajů.

Kompetenční rámec a fragmentace vzdělávání

Autor představil šest pilířů systematické přípravy bezpečnostního odborníka ve školství.

Patří mezi ně:

- 1) bezpečnost a ochrana zdraví,
- 2) krizové řízení a evakuace,
- 3) základy kybernetické bezpečnosti,
- 4) ochrana měkkých cílů a minimální standard bezpečnosti,
- 5) právní minimum včetně GDPR, zákoníku práce a školského zákona
- 6) a také komunikace v krizi a mediální gramotnost.

Jako problém Bc. Kocián popsal fragmentaci vzdělávání. Jednotlivé oblasti, například BOZP, požární ochrana, kybernetická bezpečnost a ochrana měkkých cílů, se podle jeho prezentace školí zvlášť, bez propojení, a „žijí vlastním životem“. Chybějícím dílem



skládačky má být ucelený program pro bezpečnostního manažera školy, tedy komplexní role, která by propojila všechny oblasti do jednoho funkčního celku. Autor zároveň uvádí, že nemusí jít o samostatného člověka, ale může jít o pracovníka, který vedle svého zaměření projde základním vzděláváním.

Doporučení pro školy a součinnost s IZS

V doporučeních autor uvádí potřebu vzdělávacího programu pro bezpečnostní manažery škol, povinnou roli bezpečnostního manažera s jasně definovanou odpovědností a kompetencemi, propojení s IZS, tedy Policií ČR, HZS a ZZS, a pojetí bezpečnosti jako průřezové kompetence celého pedagogického sboru, nikoli pouze jednoho pověřeného pracovníka.

Významná část prezentace byla věnována praktickým informacím pro spolupráci s Policií ČR a dalšími složkami IZS při incidentu nebo zásahu. Autor zmiňuje informace k měkkému cíli, zejména informace o objektu, obvyklý a okamžitý počet osob, odpovědnou kontaktní osobu, počet vstupů do objektu, generální klíč nebo vstupní kartu, systém vyrozumění, fyzickou ostrahu a pojmy evakuace, invakuace a lock-down. U kamerového systému prezentace upozorňuje na záznam, osoby s přístupem k záznamům, rychlost dohledání konkrétní smyčky, možnost dálkového přístupu a dostupnost 24/7.

Další praktická doporučení se týkají stanovení evakuačních míst, ideálně alespoň ve dvou variantách. Autor uvádí, že shromaždiště pro bezpečnostní evakuaci by mělo být mimo přímý dohled na budovu, mělo by mít dostatečnou kapacitu a záložní shromaždiště v jiném směru. V části k přípravě na mimořádnou událost prezentace uvádí nutnost určit odpovědnou osobu s rozhodovacími pravomocemi, mít kartu pro součinnost s IZS, seznam kontaktů, označení pater a místností, předem připravená hlášení, klíče nebo karty pro pohyb po budově a dostupný zdravotnický materiál.

Závěrečné sdělení

Závěr prezentace shrnuje autorovu hlavní myšlenku: „*Systém komplexní ochrany škol a školských zařízení je tak odolný, jak jsou připraveni lidé, kteří ho chrání. A ti lidé se nepřipraví sami.*“ Podle prezentace je proto zapotřebí systém, který tyto lidi připraví. Celé vystoupení tak směřuje k požadavku systematické, propojené a prakticky orientované přípravy osob odpovědných za bezpečnost škol a školských zařízení.



Když se ve škole něco stane

Hana Sobotková, BAKALÁŘI software

Rešerše prezentace



Zaměření prezentace

Hana Sobotková ve své prezentaci představila téma „Když se ve škole něco stane“ s podtitulem „Krizová komunikace a připravenost školy s Emergency modulem“. Prezentace byla připravena pro konferenci ASKI v Brně dne 22. září 2026 a vychází z prostředí Bakaláři software.

Jak autorka uvádí hned v úvodním modelovém rámci, krizová situace může nastat i ve chvíli, kdy je vedení mimo školu. Prezentace pracuje s příkladem požáru v jedné z budov a klade tři praktické otázky: kdo převezme řízení, jak se dostane pokyn do tříd a jak škola zjistí, kdo je v bezpečí. Právě na tyto otázky navazuje ukázka práce s Emergency modulem.

Příprava předem v Emergency modulu

Hana Sobotková prezentovala, že podstatná část krizové připravenosti se odehrává ještě před samotnou mimořádnou událostí. V Emergency modulu je podle prezentace možné předem připravit krizový tým, tedy určit, kdo může vyhlásit poplach. Dále se připravují scénáře a postupy pro situace ve škole, příjemci a zprávy, tedy komu a co se má odeslat, a také cvičný režim, který slouží k ověření při nácviku.

V prezentaci jsou jako příklady scénářů uvedeny cvičná evakuace, cvičný lockdown, ozbrojený útočník, podezřelý předmět a požár. Na snímcích z administrátorského prostředí je vidět, že scénář lze zařadit jako cvičení nebo poplach a že u vybraného



scénáře lze pracovat s nastavením incidentu, ikonou, skupinou informovaných osob, textem zprávy i náhledem varování.

Autorka dále ukazuje, že připravené scénáře mohou obsahovat i praktické postupové kroky. Na snímku k požáru jsou v systému uvedeny kroky krizového managementu a priority, například výběr krizového centra v bezpečné vzdálenosti, zajištění potřebného vybavení krizového centra, svolání krizového týmu, zvažování bezpečnostních opatření, aktualizace přehledu zraněných osob, navázání kontaktu s IZS a monitoring informací o situaci.

Vyhlášení poplachu v mobilní aplikaci

V další části Hana Sobotková prezentovala postup vyhlášení poplachu z pohledu oprávněného uživatele. Prvním krokem je otevření Emergency modulu v mobilní aplikaci Bakaláři. Druhým krokem je výběr typu události. V ukázce autorka pracuje s režimem Poplach a připraveným scénářem Požár. Prezentace uvádí, že scénář obsahuje předem nastavené příjemce a text varování.

Třetím krokem je kontrola a samotné vyhlášení poplachu. Podle prezentace uživatel ověří příjemce a text varování a následně zvolí možnost „Vyhlásit poplach“. V ukázce je zároveň požadováno potvrzení bezpečí od účastníků. Prezentace tím ukazuje, že vyhlášení poplachu není jen rozesláním zprávy, ale součástí řízeného postupu, ve kterém se pracuje s připraveným scénářem, adresáty, textem upozornění a následnou zpětnou vazbou.

Varování a potvrzení bezpečí

Autorka následně představila administrátorský pohled na varování a potvrzení bezpečí. Jak prezentace uvádí, jakmile je účastník v bezpečí, může to potvrdit volbou „Jsem mimo nebezpečí“. Přes volbu „Nová zpráva“ může administrátor posílat další pokyny.

V části věnované sledování potvrzení bezpečí Hana Sobotková ukazuje, že v sekci Účastníci je možné najít přehled zaměstnanců, tříd a žáků. Seznam lze podle prezentace filtrovat podle skupiny a podle stavu účastníků. Další snímky ukazují detail konkrétního žáka, kde může každý zaměstnanec potvrdit bezpečí žáka i jiného zaměstnance. Telefonní kontakty jsou dostupné, pokud je škola vyplnila v Kartě žáka.

Prezentace dále uvádí, že u žáka se může zobrazit informace „Je mimo nebezpečí“ a jméno zaměstnance, který bezpečí potvrdil. Potvrzení vidí i ostatní zaměstnanci školy. Součástí modulu je také přehled podle stavu účastníků, kde lze vybírat například stavy „Mimo nebezpečí“ nebo „Neodpověděl“. Autorka přitom výslovně upozorňuje, že chybějící odpověď sama o sobě neznamená, že je člověk v nebezpečí.



Checklist, ukončení poplachu a cvičný režim

Významnou část prezentace tvoří ukázka checklistu. Podle Hany Sobotkové checklist připomíná kroky okamžité reakce i úkoly, které přijdou na řadu později. Předem připravené postupy jsou podle prezentace dostupné přímo v mobilní aplikaci. Snímek ukazuje, že checklist může obsahovat konkrétní kroky reakce v době, než kontrolu na místě převezme IZS.

Autorka dále prezentovala ukončení poplachu. Účastníkům se podle prezentace automaticky odešle notifikace o ukončení poplachu a záznam události je možné najít ve webové aplikaci pro zpětné vyhodnocení. Tato část ukazuje, že modul v prezentaci nepokrývá pouze okamžik vyhlášení, ale i následné ukončení a evidenci události.

Samostatně byl představen také cvičný režim. Jak Hana Sobotková uvádí, v Emergency modulu lze při výběru typu události přepnout z režimu „Poplach“ na „Cvičení“. V ukázce lze zvolit cvičnou evakuaci nebo lockdown a pokračovat tlačítkem „Další krok“. Prezentace tím zdůrazňuje, že připravenost nezačíná až v reálné krizové situaci, ale také nácvikem a pravidelným ověřováním postupů.

Hlavní sdělení prezentace

Závěrečná část prezentace shrnuje myšlenku, že připravenost začíná nácvikem.

Autorka uvádí tři jednoduché body:

- 1) vědět, co mám udělat,
- 2) připravit se i v hlavě
- 3) a vracet se k přípravě pravidelně.

Podle prezentace si mají účastníci vyzkoušet postupy, ujasnit si svou roli a seznámit se s ovládáním Emergency modulu. Současně si mají v klidu představit možnou krizovou situaci, promyslet vlastní reakci a opakováním upevňovat postupy i zapojovat do přípravy nové kolegy a žáky.

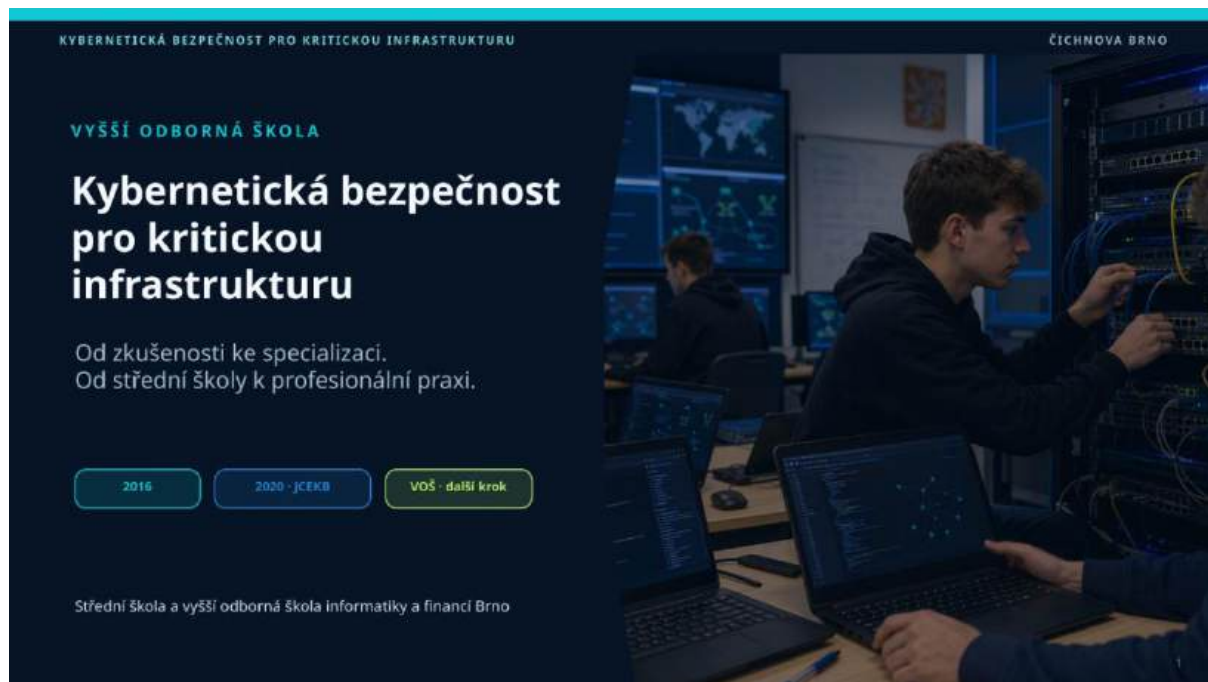
Závěrečný snímek se vrací k otázkám modelové situace: kdo převezme řízení, jak se dostane pokyn do tříd a jak zjistit, kdo je v bezpečí. Prezentace tak ukazuje Emergency modul jako nástroj pro krizovou komunikaci, připravené scénáře, rychlé varování, potvrzení bezpečí, checklisty, ukončení poplachu a nácvik krizových postupů ve škole.



VOŠ Kybernetická bezpečnost pro kritickou infrastrukturu

Ing. Olga Hölzlová, ředitelka SŠIF Brno

Rešerše prezentace



Základní rámec prezentace

Jak autorka uvádí v úvodním slidu, prezentace představuje vyšší odbornou školu zaměřenou na kybernetickou bezpečnost pro kritickou infrastrukturu. Základní sdělení je vystavěno na návaznosti „od zkušenosti ke specializaci“ a „od střední školy k profesionální praxi“. Prezentace tak nepopisuje izolovaný projekt, ale další krok ve vývoji vzdělávací koncepce Střední školy a vyšší odborné školy informatiky a financí Brno.

Ing. Olga Hölzlová prezentovala kybernetickou bezpečnost jako oblast, která se na škole rozvíjí dlouhodobě. V jejím podání je vyšší odborné vzdělávání přirozeným pokračováním dosavadních zkušeností, vybudovaného odborného zázemí a práce se žáky v oblasti kybernetické bezpečnosti.

Deset let systematického rozvoje

Autorka popisuje vývoj školy jako deset let systematického rozvoje. Kybernetická bezpečnost je zde podle prezentace rozvíjena jako dlouhodobá vzdělávací koncepce, nikoli jako jednorázový projekt. V roce 2016 škola začala s výukou a postupně budovala odborné kompetence, tým a partnerství. Rok 2020 je v prezentaci spojen se vznikem JCEKB, tedy Junior centra excellence kybernetické bezpečnosti, které propojuje výuku s praxí.



Prezentace dále zdůrazňuje, že obsah není statický. Metodika i témata se průběžně aktualizují podle vývoje oboru. Na tuto dosavadní cestu navazuje další krok v podobě vyššího odborného vzdělávání, které podle autorek přirozeně rozvíjí středoškolský základ.

Proč právě vyšší odborná škola

V části věnované otázce „Proč VOŠ“ autorka uvádí, že vyšší odborná škola propojuje kontinuitu, specializaci a rychlý přechod do odborné praxe. Kontinuita spočívá v návaznosti na znalosti a dovednosti ze středního vzdělávání. Specializace podle prezentace prohlubuje technické, procesní i právní kompetence.

Důležitým prvkem je také praxe. Prezentace výslovně uvádí laboratorní výuku, projekty a spolupráci s odborníky. Vedle toho autorka zdůrazňuje odpovědnost, tedy přípravu absolventů na ochranu dat, systémů a kritických služeb. Celý směr je znázorněn jako postup od střední školy přes vyšší odbornou školu k odborné praxi.

Náplň studia a způsob výuky

Jak autorka prezentovala, náplň studia je pojata jako rozvoj kompetencí pro celý životní cyklus bezpečnosti. Studium podle prezentace kombinuje technologii, řízení, právo a schopnost reagovat na reálné incidenty. Mezi hlavní oblasti patří sítě a infrastruktura, operační systémy a cloud, hrozby a incidenty, řízení rizik a ISMS, právo a normy a také kritická infrastruktura.

U sítí a infrastruktury prezentace uvádí architekturu, segmentaci, bezpečné služby a monitoring. U operačních systémů a cloudu se zaměřuje na správu, hardening, identity a přístupová oprávnění. Oblast hrozeb a incidentů je popsána prostřednictvím detekce, analýzy, reakce a obnovy provozu. Řízení rizik a ISMS je spojeno s aktivy, zranitelnostmi, opatřeními a kontinuitou činností. Právo a normy zahrnují legislativu, ochranu dat, odpovědnost a compliance. Kritická infrastruktura je v prezentaci vymezena přes specifika průmyslových a veřejných systémů.

Způsob výuky popisuje jako cestu od principu k praktickému zvládnutí. Student má nejprve pochopit principy, rizika a souvislosti, následně si vyzkoušet laboratorní úlohy a scénáře, poté vyhodnotit důkazy, dopady a priority a nakonec obhájit řešení, týmovou práci a dokumentaci. Metodika se podle prezentace průběžně aktualizuje podle vývoje hrozeb, technologií a potřeb praxe.

Ekosystém školy a návaznost na praxi

Ing. Hölzlová dále představila školní ekosystém, který přesahuje jednu třídu. Zkušenosti jsou podle prezentace sdíleny se žáky, pedagogy a partnerskými školami. V centru tohoto ekosystému stojí JCEKB a VOŠ. Na jedné straně jsou žáci školy, výuka, maturita a projekty. Na další straně jiné školy, workshopy a sdílení praxe.



Důležitou součástí jsou také pedagogové, metodika a další vzdělávání, stejně jako partneři, odborníci, firmy a instituce.

Prezentace uvádí, že koncepce získala uznání a škola ji proměnila ve vzdělávací realitu. Tento posun je popsán čtyřmi prvky: koncepcí jako jasnou odbornou vizí, realizací prostřednictvím lidí, vybavení a metodiky, dopadem v podobě výuky, workshopů a sdílení a oceněním jako potvrzením kvality a významu. Další formou vzdělávání je právě program kybernetické bezpečnosti pro kritickou infrastrukturu, který má přímou návaznost na zkušenosti, infrastrukturu a odborné zázemí školy.

Uplatnění absolventů a ambice programu

V závěru prezentace autorka ukazuje možné uplatnění absolventů. Uvádí pozice bezpečnostního analytika nebo pracovníka SOC, správce sítí a systémů, specialisty řízení rizik, koordinátora informační bezpečnosti, specialisty ochrany kritické infrastruktury a bezpečnostního konzultanta. Prezentace současně připomíná také možnost dalšího studia, certifikací a specializací podle zvolené profesní dráhy.

Závěrečná ambice prezentace je formulována jako snaha vychovat odborníky, kteří dokážou chránit digitální svět. Vyšší odborná škola je zde představena jako další krok v dlouhodobé cestě školy. Podle ing. Hölzlové stojí tento směr na třech pilířích: odbornosti, tedy porozumění technologiím i rizikům; praxi, tedy schopnosti navrhnout a obhájit řešení; a spolupráci, tedy učení se s odborníky a od odborníků.

Stručné shrnutí

Prezentace představuje VOŠ Kybernetická bezpečnost pro kritickou infrastrukturu jako navazující a logický krok dlouhodobé vzdělávací koncepce školy. Její hlavní sdělení stojí na kontinuitě od roku 2016, zkušenosti JCEKB od roku 2020, pravidelné aktualizaci obsahu a orientaci na praxi. Autorka zdůrazňuje, že cílem není pouze předat technické znalosti, ale připravit absolventy na ochranu dat, systémů a kritických služeb v prostředí, které vyžaduje technologickou, procesní, právní i praktickou připravenost.



Bezpečná digitální distribuce výukových materiálů

PaedDr. Pavel Hanousek, [Publi.cz](https://publi.cz)

Rešerše vystoupení – Konference ASKI 22. 9. 2026 Brno



Redakční poznámka k podkladu

K tomuto vystoupení nebyla dodána samostatná prezentace ve formátu slidů. Následující text je proto zpracován jako rešerše z doplňujícího podkladového dokumentu „ASKI a Publi“, který byl poskytnut dodatečně. Článek zachovává stejný formát jako rešerše ostatních vystoupení a vychází pouze z informací uvedených v tomto podkladu. Nejde o doslovný přepis vystoupení, ale o redakční shrnutí hlavních sdělení a souvislostí, které podklad k tématu bezpečné digitální distribuce výukových materiálů obsahuje.

Publi jako digitální jistota pro odolnou infrastrukturu

Jak autor v podkladovém materiálu uvádí, systém Publi vznikl ve světě, kde na dokumentech závisí vzdělávání, bezpečnost, provoz i klíčová rozhodnutí. V takovém prostředí podle autora není prostor pro kompromisy. Právě proto byl v roce 2012 vytvořen informační systém Publi, jehož cílem je poskytovat organizacím plnou kontrolu nad dokumenty, procesy a znalostmi. Podklad shrnuje základní charakter systému slovy: spolehlivě, bezpečně a přehledně.



PaedDr. Pavel Hanousek ve svém vystoupení podle dodaných podkladů navazoval na původní filozofii Publi. Systém vznikl původně pro školství, a to s cílem modernizovat výuku a tvorbu materiálů. Autor uvádí, že díky jednoduchému vytváření a sdílení interaktivních dokumentů jej dnes využívá čtrnáct největších univerzit a desítky středních škol. Postupně byl systém rozšířen také pro firemní a státní sektor, kde byly doplněny pokročilé prvky zabezpečení a řízení distribuce. Výsledkem má být nástroj, který pokrývá celý životní cyklus dokumentů – od jejich tvorby až po sledování čtenosti a aktualizací.

Autor dále prezentoval, že systém Publi se podle podkladového dokumentu nachází také u Armády České republiky a Ministerstva zahraničních věcí. V kontextu konference ASKI je tento údaj významný zejména proto, že téma vystoupení nebylo pojato pouze jako obecné digitální vzdělávání, ale jako otázka řízené, bezpečné a přehledné práce s dokumenty v prostředí, kde může mít dostupnost a správnost informací zásadní provozní význam.

Jak podklad uvádí, Publi umožňuje tvorbu, správu a distribuci dokumentů od interních směrnic a manuálů až po školení, výukové materiály a testy. Součástí řešení je přehledná online knihovna a mobilní aplikace, která umožňuje také offline přístup. Důležité informace tak mohou být dostupné kdykoli a kdekoli. Vystoupení tedy podle obsahu podkladu zdůrazňovalo nejen elektronickou podobu dokumentů, ale především jejich použitelnost v různých provozních situacích.

Jedním z klíčových prvků systému je podle autora vlastní interaktivní formát mKniha, založený na HTML. Podklad uvádí, že tento formát podporuje videa, 3D modely, formuláře, checklisty a další nástroje pro efektivní práci s obsahem. Online editor má umožňovat rychlou tvorbu: autor doplní obsah a vizuální podoba se vytváří automaticky podle potřeby zákazníka. V tomto směru PaedDr. Hanousek prezentoval Publi jako nástroj, který nemá sloužit pouze k ukládání dokumentů, ale také k jejich modernímu, interaktivnímu a prakticky využitelnému zpracování.

V další části podkladu autor popisuje technologii, která má držet krok s provozem. Základem systému Publi je na míru postavená e-knihovna dokumentů a mobilní aplikace pro práci v jakémkoli prostředí. Každý materiál může mít podobu interaktivní mKnihy podporující multimediální obsah. Podle autora tato forma usnadňuje uživatelům porozumění dokumentaci i práci s ní – ve výuce, v kanceláři i v terénu. Podklad výslovně uvádí, že mKniha výrazně zjednodušuje tvorbu dokumentace a šetří čas.

Významná část podkladu je věnována vztahu Publi ke kritické infrastruktuře. Autor uvádí, že členové ASKI potřebují systém, který obstojí v krizových situacích a zároveň zjednoduší každodenní provoz. Stejně tak má takový systém podle podkladu sloužit ke vzdělávání veřejnosti a ke zvyšování povědomí o asociaci a vědeckých výstupech. Publi se v těchto podmínkách podle autora dlouhodobě osvědčuje jako nástroj pro



řízení životního cyklu dokumentů a směrnic, ověřování připravenosti pomocí interaktivních testů a checklistů, kontrolu souladu s interními i bezpečnostními požadavky, bezpečný provoz bez závislosti na stálém připojení a atraktivní prostředí pro efektivní předání informací.

PaedDr. Hanousek v této souvislosti podle podkladů zdůraznil, že Publi pomáhá organizacím udržovat pořádek v informacích, snižovat riziko lidských chyb a posilovat provozní jistotu. Tyto hodnoty jsou v materiálu označeny jako zásadní pro odolnou infrastrukturu. Pro školy, instituce a organizace zapojené do témat kritické infrastruktury je tak podstatné, že systém není popisován pouze jako digitální knihovna, ale jako nástroj pro řízení informací, dokumentace a připravenosti.

Závěrečná část podkladu představuje Publi jako české řešení s mezinárodní důvěrou. Za systémem podle autora stojí brněnská společnost Code Creator, s.r.o., která úzce spolupracuje se společností AURA, s.r.o. Podklad uvádí, že AURA je známá obrannými a logistickými systémy využívanými i v rámci projektů NATO. Obě firmy podle textu sdílejí důraz na bezpečnost, spolehlivost a dlouhodobou udržitelnost.

Výsledkem má být podle autora nástroj, který propojuje vzdělávání, řízenou dokumentaci a distribuci informací do jednoho bezpečného celku – s českým původem a světovou kvalitou. V závěru podkladu je zdůrazněna myšlenka, že stabilita začíná u informací. V době rostoucích nároků na efektivní správu dat a bezpečnost provozu představuje Publi jistotu, že dokumentace je vždy pod kontrolou. Pomáhá přeměňovat data ve spolehlivé, ověřené a vždy aktuální informace, které jsou v podkladu označeny jako základ každé skutečně odolné infrastruktury.

Shrnutí řešerše

Vystoupení PaedDr. Pavla Hanouska lze na základě dodaného podkladového materiálu shrnout jako představení systému Publi jako nástroje pro bezpečnou digitální distribuci dokumentů, výukových materiálů, směrnic, školení a testů. Podklad akcentuje zejména kontrolu nad dokumenty, práci s interaktivním formátem mKniha, dostupnost obsahu on-line i off-line, řízení životního cyklu dokumentů, možnost ověřování připravenosti pomocí testů a checklistů a význam aktuálních informací pro odolnost organizací. V kontextu konference ASKI tak příspěvek ukazoval technologickou podporu pro školy, instituce i další subjekty, které potřebují pracovat s informacemi bezpečně, přehledně a provozně použitelně.

Kam kráčí bezpečnost na základních a mateřských školách

Mgr. Monika Bendová, LL.M., Asociace pověřenců ČR

Rešerše vystoupení Konference ASKI, 22. 9. 2026 Brno



Poznámka redakce: Následující text je stručnou redakční rešerší vystoupení zpracovanou výhradně na základě obsahu poskytnuté prezentace autorky. Nejde o doslovný přepis přednášky ani o autorizované stanovisko autorky; text zachycuje hlavní témata, souvislosti a formulace vyplývající z prezentovaných podkladů.

Jak autorka uvádí již v názvu své prezentace, vystoupení bylo zaměřeno na otázku, kam směřuje bezpečnost na základních a mateřských školách. Úvodní snímek propojuje téma školy s pojmy prevence, ochrana, spolupráce, důvěra a vzdělávání. Mgr. Monika Bendová, LL.M., vystoupila na konferenci v Brně dne 22. září 2026 za Asociaci pověřenců ČR a rámovala bezpečnost škol jako oblast, která se netýká pouze jednoho technického nebo právního opatření, ale celého prostředí, ve kterém se pohybují děti, zaměstnanci školy i další osoby.

Autorka v prezentaci nejprve pojmenovala výzvy současného školství. Mezi hlavní témata zařadila časté změny legislativy dopadající na činnost škol, digitalizaci, rozšiřování možností systémů elektronických matrik a správné využití umělé inteligence ve výuce. Dále upozornila na požadavky ze strany státu, zejména na rozšiřující se požadavky na zadávání a odesílání osobních údajů o žácích, JMHZ ve



vztahu k zaměstnancům, systematické sledování školní docházky, chystané nové registry žákovský a pedagogický a obecně vyšší rozsah zpracovávaných údajů.

Mgr. Bendová zároveň zdůraznila bezpečnost osob nacházejících se ve školském zařízení. V prezentaci uvádí rostoucí počet incidentů ze strany žáků, prevenci psychického stavu žáků a well-being, psychickou odolnost pedagogů, edukaci k tomu, co dělat v případě incidentů, bezpečnostní opatření a kamerové systémy. Z podkladů vyplývá, že autorka chápe školní bezpečnost jako téma, které je současně organizační, lidské, technologické i právní.

Další část prezentace zdůrazňuje, že se má „**začínat s lidmi a u lidí**“. Autorka prezentovala potřebu propojit nové výzvy s ochranou osobních údajů, zavádět nové technologie s respektem k ochraně soukromí a osobních údajů všech osob a nestavět bezpečnost a ochranu soukromí do vzájemné opozice. Tento motiv je jedním z hlavních sdělení celé prezentace: bezpečnost školy nemá být budována proti soukromí, ale společně s ním. Na jednom ze snímků je tento princip vyjádřen také obrazovým sdělením „Osobní údaje + bezpečnost = důvěra ve škole“.

Autorka poté otevírá praktickou otázku přístupu osob do školy prostřednictvím jednoduché, ale výstižné otázky: „Koho pustím dál?“ Prezentace tím přechází od obecných výzev ke konkrétní každodenní situaci školy. Otázka vstupu do budovy, kontroly osob a přístupového režimu je v prezentaci zasazena do širšího rámce jedné bezpečnosti, která zahrnuje fyzickou i kybernetickou rovinu.

V části nazvané „Jedna bezpečnost“ Mgr. Monika Bendová, LL.M., rozlišila fyzickou bezpečnost a kybernetickou bezpečnost. U fyzické bezpečnosti upozornila na vysoký počet, různorodost a výměnu osob, nízký stupeň zabezpečení, zranitelnost dětí a také na předchozí zkušenosti a analýzy útoků ve školách, které podle prezentace potvrzují atraktivitu škol pro útočníky různých typů. U kybernetické bezpečnosti autorka uvádí, že základní a mateřské školy nespadají do režimu vyšších ani nižších povinností podle ZoKB, současně však hojně využívají externí dodavatele IT systémů. Výslovně zmiňuje systémy školní matriky, objednávky jídel, čipy do družiny, sdílená prostředí, preventivní programy v online prostředí, účetnictví a personalistiku. Jako slabé místo jsou v prezentaci označeny smlouvy a doložky o zpracování osobních údajů.

Prezentace dále pracuje s příklady bezpečnostních a datových rizik, která se mohou škol dotýkat. Tyto příklady v kontextu prezentace ilustrují, že bezpečnost škol se dnes neodehrává pouze u vstupních dveří nebo v režimových opatřeních, ale také v digitálních systémech, v práci s účty, v předávání údajů a v nových formách evidence a monitoringu.



Samostatnou část autorka věnovala kamerám. V prezentaci klade sérii otázek: zda kamery zvýší bezpečnost uvnitř školy, zda mají preventivní účinek, co posouzení vlivu nebo balanční test před instalací, jaké funkce dnes kamery mají a zda nejsou dostačující jiné způsoby zabezpečení, například řízení a kontrola přístupů do budovy, bezpečnostní režim a plán budovy, videotelefony nebo čipy. Mgr. Bendová zároveň upozorňuje na praktickou otázku, zda bude mít škola vůbec někoho, kdo bude kameru pravidelně sledovat tak, aby v reálném čase zachytil problém.

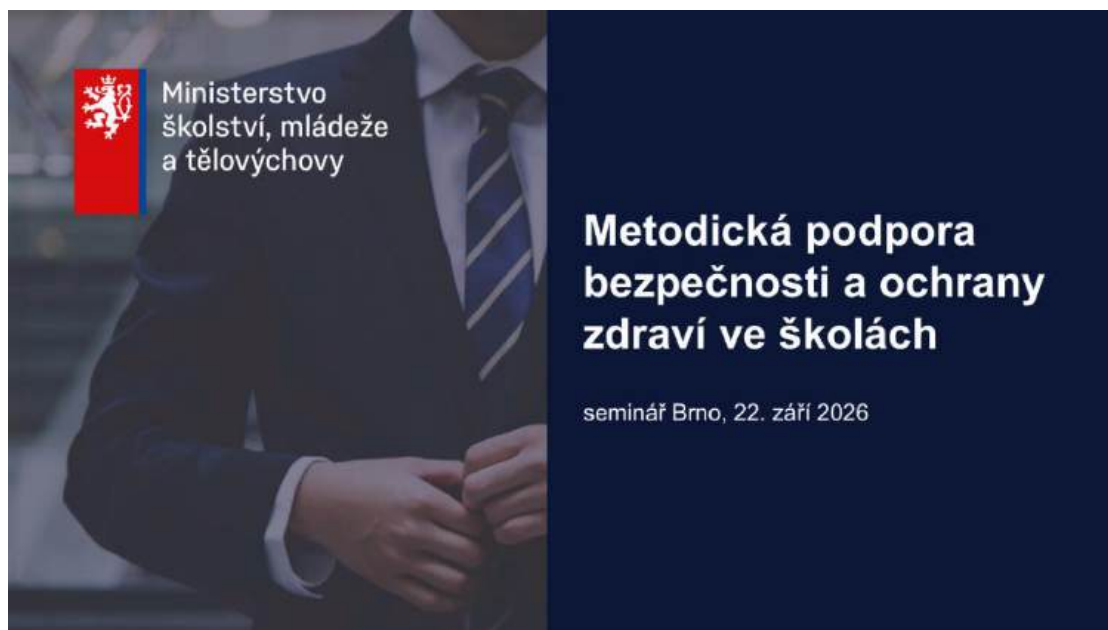
K řešení kamerového systému autorka v prezentaci uvádí několik konkrétních bodů: proškolení osob, přístup dodavatele, cloud a mobilní aplikace, provozní dobu záznamu a retenční dobu záznamu. Tyto body jsou v prezentaci zakončeny odkazem na balanční test. Rešeršně lze shrnout, že autorka nepředstavuje kamery jako samospásné řešení, ale jako opatření, které musí být promyšlené, organizačně zvládnuté, právně posouzené a prakticky provozovatelné.

Závěr prezentace se vrací k prevenci a lidskému faktoru. Autorka uvádí potřebu informovanosti, připravenosti a prevence, zejména předcházení a včasného odhalení rizik, simulace situací, školení a informací k novým technologiím a přednášek pro děti, rodiče i veřejnost. Poslední tematický snímek shrnuje, že bezpečnost začíná a končí u lidí. V tomto rámci prezentace uvádí zabezpečení objektu, stálé informování zaměstnanců o bezpečnosti ve škole, přístupy osob, informace pro rodiče a žáky a cvičení. Hlavní sdělení vystoupení tak směřuje k tomu, že bezpečnost základních a mateřských škol není jen otázkou technického vybavení, ale především průběžné práce s lidmi, informacemi, pravidly, odpovědností a důvěrou.

Metodická podpora bezpečnosti a ochrany zdraví ve školách

Ing. Ilona Vaculová, MŠMT

Rešerše prezentace



Poznámka k zařazení prezentace: Ing. Ilona Vaculová se z vážných pracovních důvodů několik dnů před konáním konference řádně omluvila z osobní účasti. Současně poskytla pořadatelům svoji prezentaci a požádala prezidenta ASKI, aby její podkladový materiál v rámci konference zpřístupnil. Tuto rešerši proto uvádíme jako redakční shrnutí obsahu prezentace, kterou na konferenci za autorku představil prezident ASKI. Za důvěru, vstřícnost a spolupráci patří Ing. Vaculové poděkování. Text níže není autorizovaným přepisem vystoupení ani oficiálním stanoviskem autorky či zastoupené instituce. Jde o volnou rešerši vycházející výhradně z informací uvedených v poskytnuté prezentaci.

Jak autorka uvádí již v úvodu prezentace, tématem podkladového materiálu je metodická podpora bezpečnosti a ochrany zdraví ve školách. Prezentace byla připravena pro seminář v Brně dne 22. září 2026 a je zpracována v rámci Ministerstva školství, mládeže a tělovýchovy. Ing. Ilona Vaculová ve svém materiálu vymezuje bezpečnost jako schopnost vytvářet a udržovat bezpečné prostředí pro vzdělávání, systematicky identifikovat a řídit rizika a zajišťovat ochranu osob, hodnot i vzdělávacího procesu v každodenním provozu i při mimořádných událostech. Zároveň zdůrazňuje, že bezpečnost je proces, nikoli jednorázové opatření.



Autorka prezentovala bezpečnost jako širší soubor oblastí. V prezentaci jsou uvedeny ochrana informací, fyzická bezpečnost, BOZ(P), ochrana majetku, požární ochrana, ochrana hodnot, kyberbezpečnost, připravenost a zvládání mimořádných událostí, psychická bezpečnost a PPRCH. Tím je bezpečnost školy představena jako komplexní rámec, nikoli jako jedna izolovaná agenda. V tomto pojetí se vedle tradičních provozních oblastí objevují také témata informací, kyberprostoru, psychické bezpečnosti a prevence rizikového chování.

Ing. Vaculová dále upozorňuje na rozdíl mezi fyzickou bezpečností a „klasickou“ BOZ(P). V prezentaci je fyzická bezpečnost spojena s pojmem security, tedy s ochranou před protiprávními činy a úmyslným jednáním. Naproti tomu BOZ(P) je spojeno s pojmem safety, tedy s prevencí nehod a neúmyslných událostí. Toto rozlišení je pro školy důležité, protože ukazuje, že bezpečnostní opatření nemají být zaměřována pouze za běžnou prevenci úrazů. Součástí širší bezpečnosti školy je také příprava na úmyslné činy, mimořádné události a situace, které mohou narušit bezpečné prostředí pro vzdělávání.

V části věnované základům legislativy autorka uvádí několik právních předpisů v platném znění. Mezi nimi zmiňuje školský zákon, trestní zákoník, zákon o požární ochraně, zákon o integrovaném záchranném systému, vyhlášku o požární prevenci a nařízení GDPR. Prezentace tím ukazuje, že metodická podpora bezpečnosti a ochrany zdraví ve školách se neopírá o jediný izolovaný předpis, ale stojí na souběhu školské, trestněprávní, požární, krizové a datové regulace.

Samostatná část prezentace je věnována dokumentaci. Autorka rozlišuje základní povinnou dokumentaci a dokumentaci doporučující. Mezi povinné základní dokumenty zařazuje školní nebo vnitřní řád, vnitřní směrnice k podmínkám dohledu nad nezletilými žáky, požární poplachové směrnice, požární evakuační plán, informační povinnost o evidenci osobních údajů a způsob zpracování a evidence osobních údajů. Jako doporučující dokumenty prezentace uvádí evidenci bezpečnostních incidentů, bezpečnostní analýzu včetně vyhodnocení ohroženosti, bezpečnostní plán, koordinační plán, kartu školy pro součinnost s IZS a plán sekundární a terciální intervence.

V další části Ing. Vaculová připomíná Metodický pokyn BOZ z roku 2005. V prezentaci je uvedena otázka, zda tento metodický pokyn stále platí, a odpověď zní: „ANO, ale...“. Materiál tím naznačuje, že starší metodická opora zůstává relevantní, ale současně je nutné vnímat ji v kontextu novějších bezpečnostních požadavků a metodických materiálů, které reagují na dnešní podobu rizik ve školách.

Významnou část prezentace tvoří Minimální standard bezpečnosti v regionálním školství z roku 2024. Autorka uvádí, že metodika podává komplexní informace a přehled doporučených opatření k zajištění fyzické bezpečnosti osob v prostorách školy a školského zařízení a při vzdělávání a s ním souvisejících činnostech.



Dokument je podle prezentace primárně zaměřen na bezpečnostní incidenty a mimořádné události zapříčiněné úmyslným působením člověka. Současně klade velký důraz na prevenci, minimalizaci bezpečnostních rizik a organizační i režimová opatření školy.

Autorka dále uvádí, že Minimální standard bezpečnosti v regionálním školství respektuje postupy a interní směrnice složek integrovaného záchranného systému. Věcný obsah byl podle prezentace konzultován s dotčenými subjekty, konkrétně s Ministerstvem vnitra, Policejním prezidiem, Ministerstvem vnitra - Generálním ředitelstvím Hasičského záchranného sboru, školskými asociacemi a Českou školní inspekcí. Prezentace tento materiál označuje za ucelený a komplexní systém zajištění fyzické bezpečnosti ve školách.

V návaznosti na tento dokument Ing. Vaculová prezentuje také očekávané přínosy jeho dodržování. Podle prezentace mohou školy díky postupům uvedeným v metodice docílit minimalizace bezpečnostních rizik, větší akceschopnosti při reakci na bezpečnostní incident nebo mimořádnou událost a také efektivnějšího zásahu složek IZS. Prezentace současně uvádí, že Minimální standard bezpečnosti v regionálním školství z roku 2024 nahrazuje dřívější Metodické doporučení k bezpečnosti dětí, žáků a studentů ve školách a školských zařízeních - Minimální standard bezpečnosti, č. j. MSMT-1981/2015-1.

Závěrečná část prezentace je věnována vzdělávání. Jak autorka uvádí, vzdělávání a pravidelná edukace jsou důležitým preventivním prvkem. Materiál rozlišuje specializované teoretické vzdělávání zaměstnanců, specializované praktické vzdělávání zaměstnanců a vzdělávání žáků. Součástí prezentace je také citace § 14 odst. 5 vyhlášky č. 317/2005 Sb., podle níž právnická osoba vykonávající činnost školy nebo školského zařízení zajistí zaměstnancům zpravidla jednou za tři roky školení v oblasti fyzické bezpečnosti, zejména o postupech a opatřeních v případě mimořádných a krizových událostí na pracovišti nebo při činnostech souvisejících se vzděláváním mimo místo, kde se uskutečňuje vzdělávání.

V závěru prezentace jsou uvedeny další informační zdroje, konkrétně záložka k bezpečnosti na edu.gov.cz a e-mailová adresa bezpecnost.na.skolach@msmt.gov.cz. Prezentace je zakončena poděkováním a kontaktem na Ing. Ilonu Vaculovou z Oddělení organizace předškolního, základního a základního uměleckého vzdělávání. Celkově lze z prezentace vyčíst důraz na bezpečnost jako dlouhodobý proces, který propojuje fyzickou bezpečnost, BOZ(P), požární ochranu, dokumentaci, metodickou podporu, spolupráci se složkami IZS a pravidelné vzdělávání zaměstnanců i žáků.



Shrnutí připravených řešerší z konference ASKI

ASKI Zpravodaj 09/2026 | Přehled souborů 000–013

Tento shrnující článek přináší stručný přehled souborů připravených pro sérii řešerší vystoupení z odborné konference ASKI „Odpovědnost ředitelů škol v oblasti kritické infrastruktury a kybernetické bezpečnosti podle nové legislativy“, která se uskutečnila dne 22. září 2026 v Brně.

Přehled je řazen podle číslování pořadí zveřejněných autorských řešerší od 000–013 a zachycuje, jaké téma bylo v každém dokumentu zpracováno a jaký byl hlavní obsah příslušné řešerše. Smyslem není opakovat celé články, ale vytvořit rychlou orientaci v tom, co jednotlivé výstupy obsahují.

Přehled zpracovaných řešerší

000 – Úvod k sérii řešerší vystoupení z konference ASKI

Dokument uvádí celou sérii řešerší, vysvětluje jejich redakční a právní rámec a vymezuje, že nejde o autorizované přepisy vystoupení, ale o redakční shrnutí podkladových prezentací. Současně zdůrazňuje návaznost na konferenci ASKI a význam zpřístupnění odborných výstupů širšímu okruhu čtenářů.

001 – PhDr. Mgr. Dušan Kalášek, MBA, LL.M. – legislativní změny v kontextu školství

Autorský článek shrnuje úvodní vystoupení prezidenta ASKI k propojení krizového řízení, kritické infrastruktury a kybernetické bezpečnosti se školstvím. Text zdůrazňuje, že školy nejsou automaticky subjekty kritické infrastruktury, ale mají zásadní vzdělávací, systémovou a společenskou roli při přípravě budoucích občanů a odborníků.

002 – PhDr. Jaroslav Hora, LL.M. – školy jako součást kritické infrastruktury

Řešerše se věnuje škole jako významnému datovému a rizikovému uzlu. Autor řešil řízení rizik, ochranu osobních údajů, dodavatelské vztahy, GDPR, kybernetickou bezpečnost, minimalizaci dat a potřebu systémové governance škol včetně sdílených odborných kapacit.

003 – plk. gšt. Ing. Alois Matýzka – Krajské vojenské velitelství jako partner škol

Dokument představuje Krajské vojenské velitelství Brno jako partnera škol při implementaci bezpečnostních témat do výuky. Řešerše shrnuje brannou povinnost, dobrovolné vojenské cvičení pro studenty středních škol a přípravu občanů k obraně státu v rámci POKOS.



004 – Mgr. Richard Veleta, Ph.D. – potenciál Národní soustavy kvalifikací

Rešerše představuje Národní soustavu kvalifikací jako nástroj využitelný pro oblast kritické infrastruktury, bezpečnosti škol a kybernetické bezpečnosti. Autor ukázal, jak lze různé profesní kvalifikace vztáhnout k fyzické ostraze, BOZP, technické správě, strategickému řízení bezpečnosti i kybernetické bezpečnosti.

005 – Ing. Josef Myslín, Ph.D., Ed.D., MSc., MPA – ochrana obyvatelstva jako součást RVP

Text shrnuje vystoupení zaměřené na začlenění témat ochrany obyvatelstva do rámcových vzdělávacích programů. Autor řešil mimořádné události, roli školy při rozvoji odpovědnosti žáků, prevenci, spolupráci s IZS, tematické okruhy výuky a potřebu systematického postupu.

006 – Mgr. Vojtěch Kašpárek, MBA – kde stojí člověk a kde AI

Rešerše se věnuje postavení člověka a umělé inteligence ve školním prostředí. Autor pracoval s principem Human in the loop, validací, anonymizací, dohledatelností rozhodnutí a otázkou odpovědného využívání AI v pedagogickém rozhodování.

007 – Dr. Ing. Evžen Šanc – umělá inteligence na hranici mezi pomocí a závislostí

Dokument shrnuje pohled na AI jako technologický, bezpečnostní i psychologický fenomén. Autor propojil AI s kybernetickým ohrožením škol, phishingem, deepfake, digitální stopou, chatboty, závislostí, psychologickými riziky a potřebou jasných školních postupů při rozpoznávání varovných signálů.

008 – Bc. Jaroslav Kocián – systematická příprava odborníků

Rešerše se zaměřuje na bezpečnost škol jako měkkých cílů a na potřebu systematické přípravy osob odpovědných za bezpečnost. Autor řešil fragmentaci bezpečnostních rolí, potřebu bezpečnostního manažera školy, spolupráci s IZS, praktickou krizovou připravenost a kompetenční rámec odborníka.

009 – Hana Sobotková / Bakaláři software – Emergency modul

Text shrnuje prezentaci krizové komunikace a připravenosti školy s Emergency modulem. Rešerše popisuje přípravu scénářů, vyhlášení poplachu, potvrzení bezpečí osob, práci s účastníky, checklisty, ukončení poplachu, evidenci události a cvičný režim.

010 – Ing. Olga Hözllová / Ing. Marie Potůčková – VOŠ Kybernetická bezpečnost pro kritickou infrastrukturu

Dokument představuje vyšší odborné vzdělávání v oblasti kybernetické bezpečnosti pro kritickou infrastrukturu. Rešerše shrnuje dlouhodobý rozvoj školy, návaznost na



JCEKB, laboratorní a projektovou výuku, propojení s praxí a přípravu absolventů na ochranu dat, systémů a kritických služeb.

011 – PaedDr. Pavel Hanousek / PUBLI – bezpečná digitální distribuce výukových materiálů

Rešerše představuje systém Publi jako nástroj pro řízenou distribuci dokumentů, výukových materiálů, směrnic, školení a testů. Text popisuje interaktivní formát mKniha, online i offline přístup, řízení životního cyklu dokumentů, checklisty a význam aktuálních informací pro odolnost organizací.

012 – Mgr. Monika Bendová, LL.M. – bezpečnost na základních a mateřských školách

Dokument shrnuje současné výzvy bezpečnosti na základních a mateřských školách. Autorka řešila ochranu osobních údajů, digitalizaci, fyzickou a kybernetickou bezpečnost, přístupy osob, kamerové systémy, balanční test, informovanost, prevenci a důvěru ve škole.

013 – Ing. Ilona Vaculová / MŠMT – metodická podpora bezpečnosti a ochrany zdraví ve školách

Rešerše vychází z prezentace poskytnuté Ing. Vaculovou a shrnuje bezpečnost jako dlouhodobý proces. Text rozlišuje fyzickou bezpečnost a BOZ(P), uvádí základní legislativní rámec, školní dokumentaci, Minimální standard bezpečnosti v regionálním školství 2024 a význam pravidelného vzdělávání zaměstnanců i žáků.

Společný rámec celé série

Připravené rešerše dohromady vytvářejí ucelený obraz konference ASKI. Ukazují, že bezpečnost škol nelze chápat pouze jako jednu izolovanou oblast, ale jako propojení legislativy, řízení rizik, ochrany osobních údajů, krizové komunikace, fyzické a kybernetické bezpečnosti, ochrany obyvatelstva, umělé inteligence, digitální distribuce obsahu, odborné přípravy a metodické podpory.

Série současně ukazuje, že školy dnes nejsou pouze místem výuky. Jsou organizacemi, které pracují s lidmi, daty, technologiemi, provozem, odpovědností a důvěrou. Právě proto má smysl, aby výstupy z konference byly uchovány v podobě stručných, čitelných a tematicky navazujících rešerší.



Našim aktivitám jsou příznivě nakloněny tyto fyzické a právnické osoby a organizace:

