# sovak_bar_dopl_text

# Vás zve na seminář:

**Kybernetická bezpečnost ve vodárenství**

**v kontextu směrnice NIS2,**

který se uskuteční

 **23. 2. 2023 od 10:00 hod.**

**v zasedací místnosti č. 217, Novotného lávka 200/5, Praha 1**

Na semináři se v návaznosti na probíhající implementaci směrnice NIS2 do naší zákonné úpravy kybernetické bezpečnosti zaměříme na představení aktuální stavu procesu novelizace zákona o kybernetické bezpečnosti, harmonogram zavádění novely do praxe, rozsah změn a jejich dopad na společnosti v České republice. Zhodnotíme aktuální situaci v oblasti kybernetické bezpečnosti v odvětví vodárenství a řekneme si praktické dopady nové legislativy na tento segment. V dalších přednáškách se zaměříme na praktická doporučení v klíčových oblastech kybernetické bezpečnosti, na které nová legislativa klade důraz, a to kybernetické bezpečnosti v rámci dodavatelského řetězce, systému osvěty a vzdělávání napříč organizací a zabezpečení kontinuity činnosti organizace po haváriích a útocích.

Duchem semináře je představení nových povinností a doporučení pro jejich adopci v rámci vodárenských společností praktickou formou, nikoli strašení o formálních dopadech nové směrnice NIS2 a doporučení formalizovaných opatření.

***Přednášet budou:***

**Martin Švéda** v roce 2017 nastoupil na Národní bezpečnostní úřad, do jeho tehdejšího Národního centra kybernetické bezpečnosti; byl tak u vzniku Národního úřadu pro kybernetickou a informační bezpečnost, kde působí jako právník zaměřující se na regulaci kybernetické bezpečnosti. Od roku 2021 zde vede oddělení regulace soukromého sektoru. Zaměřuje se především na problematiku výkladu zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů a podílí se na návrzích jejich změn – aktuálně také koordinuje přípravné práce na novelizaci zákona o kybernetické bezpečnosti v souvislosti s přijetím směrnice NIS2.

**Daniel Hejda** je spolumajitelem firmy Cyber Rangers s.r.o., která se zabývá kontrolou bezpečnosti v IT a OT prostředí. Daniel je red teamer, výzkumník, sociální inženýr a bezpečnostní konzultant s více jak 15 lety praxe
v oblasti IT technologií a 5 let v oblasti technologií OT. V rámci své činnosti se zabývá nejen audity, poradenstvím a testováním, ale také přednášením na předních českých konferencích. Mezi hlavní činnosti v oblasti bezpečnosti patří penetrační testování, sociální inženýrství, zpravodajská činnost a výzkum kybernetických útoků nejen státem sponzorovaných skupin (APT). Daniel je držitelem certifikací CEHv10, eWPTv1, COMPTIA Pentest+, PECB ISO27001 Lead Auditor, C|OSINT, MCSE, MCSA, MCSD a je také držitelem prestižního ocenění Microsoft MVP pro Cloud and Datacenter Management a přispěvatelem komunity CIS Security Benchmarks.

**Jindřich Kalíšek** je advokátem specializujícím se na kybernetickou bezpečnost a ochranu osobních údajů a soukromí na internetu, právo nových technologií (především na problematiku software, cloudových služeb a e-commerce)
a duševního vlastnictví. Působí jako zapsaný mediátor se specializací na spory z vývoje a implementace software
a spory z práv duševního vlastnictví a také jako pověřenec pro ochranu osobních údajů. Jindřich poskytuje právní poradenství komerčním i neziskovým organizacím (herním společnostem, dodavatelům energií, poskytovatelům služeb v e-commerce a dalším) v oblasti ochrany informací (osobních údajů, obchodních tajemství a důvěrných informací), kybernetické bezpečnosti, elektronické identifikace a služeb vytvářejících důvěru a s vymáháním práv
z duševního vlastnictví. Je členem Sekce České advokátní komory pro IT a GDPR, Spolku pro ochranu osobních údajů, ČIMIB a Pověřencem roku v soukromém sektoru za rok 2019.

**Michal Beneš** je společníkem a ředitelem společnosti system boost a.s. V oblasti IT a kybernetické bezpečnosti se pohybuje již více jak 19 let. V rámci své poradenské praxe se zaměřoval na implementaci informačních systémů, digitalizaci, audity IT a kybernetické bezpečnosti a Business Continuity Management. Michal je soudním znalcem v oborech Kybernetika a Ekonomika.

**Program:**

**9:30 Registrace**

**10:00**  **Zahájení a úvod do tématu**

* Ing. Vilém Žák, ředitel a člen představenstva SOVAK ČR

**10:10**  **Kybernetická bezpečnosti ve vodním hospodářství směrnice NIS2 v České republice a praktické dopady**

* *Tématem přednášky bude představení problematiky v souvislosti s přijetím směrnice NIS2 v České republice z pohledu legislativy a legislativního procesu. Zároveň také budou představeny praktické dopady a výsledky kontaktu a jednání s firmami z oboru VaK v uplynulém období.*
* Martin Švéda, NÚKIB

**11:05** **Implementace požadavků kybernetické bezpečnostní legislativy do organizace v praxi**

* *Přestože směrnice NIS2 bude vyžadovat transpozici do právního řádu České republiky (novelou zákona
o kybernetické bezpečnosti a novými vyhláškami), již nyní jsou zřejmé některé povinnosti a požadavky, které budou muset její adresáti naplnit. Mezi tyto oblasti patří zavedení konkrétních organizačních
a technických opatření k zajištění kybernetické bezpečnosti (v příslušném režimu), zajištění průběžného vzdělávání zaměstnanců a managementu v otázkách kybernetické bezpečnosti, pravidelné vyhodnocování bezpečnostní situace a reporting řídícím orgánům, reakce na bezpečnostní incidenty, řízení dodavatelských řetězců a personální bezpečnosti. V přednášce shrneme nejvýznamnější oblasti, ve kterých bude nutné provést v organizaci změny a navrhneme, jak k nim přistoupit, aby byla implementace efektivní, smysluplná a přínosná.*
* Jindřich Kalíšek, advokát

**11:45 Přestávka**

**12:00**  **Problémy v rámci dodavatelského řetězce a školení (nejen) vrcholového managementu**

* *Během přednášky vám v první části povíme o problémech, které můžete identifikovat v rámci dodavatelského řetězce. Povíme si, jak je možné kontrolovat dodavatele a na co byste při kontrole neměli zapomenout. Ve druhé části přednášky se zaměříme na top 10 kybernetických hrozeb, o kterých by měl vrcholový management organizace vědět. V rámci přednášky se dozvíte, jak často školení realizovat a zda je vhodnější použití e-learningu nebo prezenčního školení.*
* Daniel Hejda, Cyber Rangers s.r.o.

**12:40** **Zajištění kontinuity činností organizace je úkolem všech zaměstnanců a spolupracovníků**

* *V rámci přednášky se zaměříme na důležitost konceptu řízení kontinuity činností, jakožto přístupu
k zachování fungování společnosti a podnikání i v případě rozsáhlých havárií nebo kybernetických útoků. Tento koncept v sobě zahrnuje jak rychlou reakci na krizovou událost, alespoň základní stabilizaci společnosti a aktivaci předem nastavených náhradních procesů a procesů obnovy standardních procesů
a infrastruktury po krizové události, tak racionální přípravu a zavedení preventivních mechanismů
a technologií pro zmírnění rozsahu a následků budoucích negativních událostí.*
* Michal Beneš, system boost a.s.

**13:15**  **Diskuse a závěr**

V případě zájmu o účast vyplňte, prosím, následující přihlášku a zašlete ji nejpozději do **17. 2. 2023** na některý z níže uvedených kontaktů:

* e-mail: doudova@sovak.cz
* adresa: SOVAK ČR, Novotného lávka 200/5, 110 00 Praha 1

**Poplatek za účast na semináři je pro řádné členy SOVAK ČR 1 210,- Kč (včetně 21 % DPH), pro přidružené členy a ostatní účastníky 1 815,- Kč (včetně 21 % DPH), v případě platby na místě konání semináře je účtován příplatek za administrativu 605,- Kč (včetně 21 % DPH) každému účastníkovi semináře. V ceně vložného je sborník v elektronické podobě a drobné občerstvení.**

**Storno účasti je možné provést nejpozději 5 kalendářních dnů před konáním akce, v případě neúčasti se vložné nevrací.**