# sovak_bar_dopl_text

# Vás zve na seminář:

**Klíčová opatření v oblasti kybernetické bezpečnosti,**

který se uskuteční

**5. 10. 2023 od 10:00 hod.**

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

Na tomto semináři se v návaznosti na předchozí seminář s názvem „Kybernetická bezpečnost ve vodárenství   
v kontextu směrnice NIS2“, který se konal 23. 2. 2023, a probíhající implementaci směrnice NIS2 do naší zákonné úpravy kybernetické bezpečnosti, zaměříme na diskusi doporučených klíčových opatření kybernetické bezpečnosti, na které by se měla každá větší i menší vodárna zaměřit nebo by se alespoň měla s těmito klíčovými opatřeními seznámit a zahájit úvodní kroky. Představíme Vám také vhodné postupy a nástroje při realizaci těchto opatření. Účastníci, kteří diskutovaná témata již řeší, budou mít možnost náhledu na řešení z dalšího pohledu a prostor pro diskusi jejich otázek.

Seminář zahájíme **představením aktuálního stavu implementace NIS2** **v České republice** přímo zástupcem NÚKIB, tedy osobou v této oblasti nejpovolanější. Následovat bude prezentace možností řešení osobní odpovědnosti statutárních zástupců organizací za implementaci opatření kybernetické bezpečnosti a za důsledky kybernetických incidentů v případě nedostatečného řešení bezpečnosti.

V další části naváže **jeden z** **předních etických hackerů v naší republice a přímo v přednáškové síti na živo demonstruje kybernetický útok na vodárenský systém v připraveném laboratorním prostředí, tedy ukáže, jak může být vodárenská infrastruktura zranitelná, pokud nejsou svědomitě aplikována řádná bezpečnostní opatření**. Připravené laboratorní prostředí pak využije ve druhé části své přednášky pro osvětlení, jak lze bezpečnostní technologie soutěžit na kvalitu, a nikoli jen na cenu.

Po přestávce Vás seznámíme s velmi diskutovaným tématem v souvislosti s implementací NIS2, a to s otázkou **zajištění bezpečnosti dodavatelského řetězce**, resp. jak úroveň bezpečnosti dodavatelů poznat a jaká opatření je vhodné následně aplikovat. Seminář pak zakončíme **praktickým představením bezpečnostních technologií**, které je vhodné zvážit při přípravě a implementaci technických opatření pro zajištění potřebné úrovně bezpečnosti,   
a zároveň pro zajištění souladu s požadavky připravované novelizace kybernetického zákona v návaznosti na NIS2.

**Duchem semináře bude jeho účastníkům představit doporučení a možností jejich řešení v rámci vodárenských společností praktickou formou,** nikoli strašení o formálních dopadech nové směrnice NIS2 a doporučení formalizovaných opatření.

***Přednášet budou:***

**Petr Hrachy** je referent bezpečnosti státu ze společnosti NÚKIB a řeší aktuální stav implementace NIS2 v České republice.

**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 softwaru, cloudových služeb a e-commerce)   
a duševního vlastnictví. Působí jako zapsaný mediátor se specializací na spory z vývoje a implementace softwaru   
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 zástupcem 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.

**Robin Bay** je zástupem společnosti FORTINET. Robin Bay pracuje jako technik v oblasti bezpečnosti od roku 2000. Řešil audity sítí, bezpečnostní incidenty u zákazníků v rámci incident response nebo školil etický hacking a bezpečnostní produkty v největších firmách Evropy.

**Program:**

***9:30 Registrace***

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

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

**10:10**  **Struktura bezpečnostních opatření s ohledem na NIS 2 a nejčastější zjištění z kontrol**

* Petr Hrachy, NÚKIB

**10:50** **Možnosti částečného přenesení odpovědnosti (pojištění) a opatření v rámci interních organizačních norem**

* Jindřich Kalíšek, advokát

**11:30**  **Jak soutěžit bezpečnostní technologie na kvalitu a nikoli na cenu, bonus: Skutečný kybernetický útok na „vodárenský systém“ pohledem hackera/penetračního testera**

* Daniel Hejda, Cyber Rangers s.r.o.

***12:30 Přestávka***

**12:45** **Opatření a nástroje v oblasti bezpečnosti dodavatelského řetězce**

* Michal Beneš, system boost a.s.

**13:20** **Technologie pro řešení technických opatření v návaznosti na bezpečnostní požadavky v souvislosti s implementací NIS2**

* Robin Bay, FORTINET

***14:00*** ***Diskuse a závěr***

*Změna programu vyhrazena*

V případě zájmu o účast vyplňte, prosím, následující přihlášku a zašlete ji nejpozději do **27. 9. 2023** na některý z níže uvedených kontaktů:

* e-mail: [doudova@sovak.cz](mailto: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.**