



Energie, infrastruktura a kybernetická bezpečnost ve střední Evropě

20. 5. 2026 | 14:00–16:00

Konferenční centrum Krocínova (Krocínova 1050/1, 110 00 Praha 1)

Ochrana kritické infrastruktury se stala jednou z klíčových otázek evropské bezpečnostní politiky. Energetické sítě, ropovody, jaderné elektrárny, dopravní uzly i digitální infrastruktura čelí rostoucímu riziku sabotáží, kybernetických útoků a hybridních operací. S incidenty mají zkušenosti země napříč Evropou, včetně Česka a Německa.

Do tohoto prostředí vstupuje evropská směrnice NIS2, která výrazně zpřísnila požadavky na kybernetickou bezpečnost v klíčových sektorech. Nová pravidla ukládají provozovatelům přísnější standardy řízení rizik, bezpečnosti dodavatelských řetězců, hlášení incidentů a osobní odpovědnosti vedoucích pracovníků. Otázka přitom nezní pouze „jak splnit směrnici“. Jde o to, jak zajistit, aby energetická transformace a digitalizace nezakládaly nové zranitelnosti.

Řečníci:

LUKÁŠ KINTR

ředitel Národního úřadu pro kybernetickou a informační bezpečnost
(případně zastoupen náměstkem)

zástupce Asociace kritické infrastruktury ČR
(tbc)

KATEŘINA HŮTOVÁ

jednatelka, CEO a ISMS manažerka
společnosti Cybrela

VÁCLAV STUPKA

Deputy Director v CyberSecurityHub, z.ú.

a další

Moderace:

JAN VITÁSEK

vydavatel portálu Update EU

Program:

13:40	příchod hostů, registrace
14:00	zahájení, úvodní komentáře řečníků
14:20	moderovaná diskuze s aktivním zapojením všech hostů
15:20	shrnutí diskuse, ukončení formální části
15:30	neformální diskuse, networking, občerstvení

-
- Jaká jsou nejzávažnější rizika pro kritickou infrastrukturu ve střední Evropě? Které části kritické infrastruktury jsou nejzranitelnější?
 - Jak Česko a Německo přistoupily k transpozici NIS2? Je aktuální legislativní nastavení dostatečné, vzhledem k závažnosti hrozeb? Kde jsou případné mezery a jak je řešit?
 - Kde je prostor pro hlubší česko-německou spolupráci právě v oblasti posilování odolnosti infrastruktury?
-