

## Česko v digitální Evropě

Ve dvacátém druhém vydání newsletteru se dozvíte o evropském programu CEF2, vyhlášení výzvy ke cloudové infrastruktuře, online průzkumu k Aktu o datech anebo o Akčním plánu ke strategii kybernetické bezpečnosti. Dále také o iniciativách v online bezpečnosti a chystaných akcích v digitální oblasti.

Pěkné čtení Vám přeje Oddělení evropské digitální agentury

### **CZ.NIC a Policie ČR proti nezákonnému obsahu na internetu**

Mezi CZ.NIC a Policií ČR byla v rámci projektu Safer Internet Centrum (SIC) uzavřena deklarace o spolupráci při provozu linky [STOPonline.cz](https://stoponline.cz), jejímž záměrem je ochrana dětí a mládeže před trestnou činností tak, aby se minimalizoval výskyt dětské pornografie, kybergroomingu či nepatřičné dětské nahoty na internetu. Více informací [zde](#).

### **Test ověřující bezpečné chování v online prostředí**

Česká bankovní asociace (ČBA), která každoročně sestavuje [Index Kyberbezpečnosti](#), uskutečnila ve spolupráci se společností ESET a agenturou SC&C tzv. Kybertest, který simuloval rizikové situace a hrozby. Češi v něm dosáhli pouze 43% úspěšnosti. Nyní je tento test k dispozici veřejnosti na [webu projektu](#).

### **Zpráva o stavu kybernetické bezpečnosti (ZSKB) za rok 2020**

ZSKB, jejímž hlavním autorem je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), je hlavní dokument, který shrnuje dění v oblasti kybernetické bezpečnosti v ČR v uplynulém roce. Zpráva stojí na datech získaných od více než 200 subjektů a její celé znění je k dispozici na [webu NÚKIB](#).

### **Nová podoba evropského programu CEF2**

Dne 7. července 2021 Evropský parlament odsouhlasil novou podobu programu The Connecting Europe Facility (CEF2) v hodnotě 30 mld. EUR, který poskytne v období mezi roky 2021 a 2027 finanční zdroje na projekty zaměřené na oblast digitalizace, dopravy a energetiky. V rámci pilíře CEF2 Digital je cílem podpořit vývoj projektů celoevropského zájmu, mezi něž se řadí např. rozvoj zabezpečených velmi vysokokapacitních digitálních sítí a systémů 5G, cloudová řešení, tzv. superpočítače (HPC), kvantová komunikační infrastruktura či podmořské kabely. V rámci Evropy by měl program CEF2 také usnadnit zavádění gigabitových sítí a digitální transformaci podniků a vzdělávání lidí. Více informací o programu [zde](#).

### **IPCEI: Vyhlášení výzvy v oblasti cloudové infrastruktury**

Ministerstvo průmyslu a obchodu (MPO) společně s CzechInvest připravuje prostředí pro rozvoj a využití cloudové infrastruktury a služeb nové generace prostřednictvím mezinárodní spolupráce v rámci tzv. Významných projektů společného evropského zájmu (IPCEI). V souvislosti s tím MPO vyhlásilo výzvu k vyjádření zájmu o účast v takovýchto inovačních projektech. Koncept IPCEI umožňuje podpořit spolupráci mezi malými i velkými podniky na projektech od aplikovaného výzkumu, přes vývoj a inovace až po první průmyslové nasazení v rámci celé Evropské unie. Cílem aktuální výzvy je identifikovat vhodné podniky a jejich projekty, které se zabývají cloudovou infrastrukturou a službami a které jsou škálovatelné, interoperabilní, udržitelné, důvěryhodné a energeticky účinné. **Projektové přihlášky je možné zasílat do 15. srpna 2021.** Více o podmínkách výzvy na [webu MPO](#).

3. 8. 2021



## MPO: Online průzkum k Aktu o datech

V souvislosti s chystaným Aktem o datech (Data Act), legislativním návrhem, který má za cíl upravovat pravidla pro sdílení dat mezi podniky a státní správou a podniky navzájem, spustila Evropská komise [veřejnou konzultaci](#). V návaznosti na tuto konzultaci zahájilo Ministerstvo průmyslu a obchodu (MPO) vlastní online průzkum vycházející ze stejných dotazů a který poslouží pro vytvoření národní pozice k návrhu tohoto nařízení. **Neváhejte se zapojit do vyplnění tohoto [dotazníku](#) v anglickém jazyce do 12. srpna 2021.**

## OECD: Veřejná konzultace k pokynům pro odpovědné inovace blockchainu a DLT

Organizace pro hospodářskou spolupráci a rozvoj (OECD) v současné době vypracovává [návrh doporučení](#) pro blockchain a další technologie distribuované účetní knihy (DLT). Snahou OECD je poskytnout obecné, jasné a ucelené pokyny, jak dosáhnout odpovědných inovací a jak přijímat tyto technologie do praxe všemi aktéry a zájmovými skupinami, kteří jsou zapojeni do jejich vývoje a využívání. V souvislosti s tím byla zahájena veřejná konzultace, které je možné se zúčastnit do 31. srpna 2021 na [webu OECD](#).

### **Konference Otevřená data 2021**

Šestý ročník konference k otevřeným datům proběhne sice až 5. listopadu 2021, avšak již nyní je možné se přihlásit k aktivní účasti formou příspěvku a představit zajímavé příklady využití otevřených dat. [Přihlašování](#) je možné do 29. srpna 2021.

### **Konference womENCourage 2021**

Czechitas ve spolupráci s ACM-W Europe pořádá od 22. do 24. září 2021 třídní virtuální konferenci womENCourage, jejímž záměrem je propojit ženy z různých technických oborů a povzbudit je, aby pokračovaly ve svém vzdělávání a v profesi v ICT oboru. První kolo [registrací](#) je otevřeno do 10. srpna 2021.

## Veřejná soutěž na podporu centra digitálního vzdělávání

Evropská komise vyhlásila veřejnou soutěž na založení a rozvoj centra digitálního vzdělávání (tzv. Digital Education Hub), které vytvoří prostředí pro spolupráci mezi odborníky na digitální vzdělávání. Centrum cílí na pomoc při sdílení rad a zkušeností, spoluvytváření kooperativních aktivit napříč sektory, navazování kontaktů mezi národními experty a regionálními vzdělávacími iniciativami. Projekt digitálního centra je spjatý s [Akčním plánem digitálního vzdělávání](#) (2021–2027) a vizí Evropské unie o budoucnosti systémů vzdělávání a odborné přípravy pro digitální věk. Termín podávání přihlášek je do 23. srpna 2021. Více informace [zde](#).

## Akční plán ke strategii kybernetické bezpečnosti

Vláda ČR na svém jednání 26. července 2021 schválila Akční plán k Národní strategii kybernetické bezpečnosti, jehož vznik koordinoval Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Tematicky se akční plán zaměřuje např. na posílení kybernetické bezpečnosti ve zdravotnictví, posuzování rizikového profilu dodavatelů či na vytvoření metodiky pro efektivní strategickou komunikaci zaměřenou na zvládání velkých kybernetických bezpečnostních incidentů. Loni schválená národní strategie je založená na 3 principech: Sebevědomě v kyberprostoru, Silná a spolehlivá spojení a Odolná společnost. Nově schválený akční plán nastiňuje konkrétní kroky, jimiž lze dosáhnout cílů vytyčených v této strategii. Více informací a celé znění akčního plánu najdete na [webu NÚKIB](#).

Pro odběr newsletteru nás kontaktujte na [digiczech@vlada.cz](mailto:digiczech@vlada.cz)

@digiczech   
[www.digitalnicesko.cz](http://www.digitalnicesko.cz)