poslední aktualizace:

2. 10. 2025

Národní strategie kybernetické bezpečnosti 2026

Česká republika vstupuje do roku 2026 s novou Národní strategií kybernetické bezpečnosti (NSKB), která určuje směr rozvoje do roku 2030. Vláda dokument připravený Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) schválila v září 2025. Strategie vytyčuje **dlouhodobé priority státu v oblasti kybernetické bezpečnosti** a nahrazuje předchozí verzi platnou od roku 2021. Strategii bude provázet akční plán s konkrétními úkoly pro odpovědné instituce, jehož plnění má být každoročně vyhodnocováno a výsledky předkládány vládě. Například válka na Ukrajině jasně ukázala, že **kyberprostor se stal pevnou součástí moderních konfliktů** a standardním bojištěm. Kybernetické operace již nejsou jen doplňkovou aktivitou, ale integrální součástí vedení války. NSKB je proto koncipována tak, aby Česko dokázalo včas reagovat na nové hrozby i využít příležitostí spojených s digitalizací.

Strategie je **vrcholným národním strategickým dokumentem** pro kybernetickou bezpečnost a nedílnou součástí bezpečnostního rámce státu. Vytváří jednotný, koordinovaný rámec zaměřený na ochranu a odolnost informačních a komunikačních systémů, kybernetickou obranu, kybernetickou diplomacii, boj s kyberkriminalitou a zvyšování odolnosti společnosti vůči hrozbám v kyberprostoru. Jinými slovy, pokrývá technická opatření, vojenskou i zahraničněpolitickou dimenzi kyberprostoru, policejní potírání kriminality i celkovou připravenost občanů čelit digitálním rizikům. Dokument je rozdělen na analytickou část, popisující aktuální hrozby a stav zabezpečení, a navazující část strategickou, která formuluje vizi a strategické cíle. Podle NÚKIB se na přípravě strategie podílely **desítky organizací z veřejného i soukromého sektoru a proběhly veřejné konzultace.** NÚKIB je gestorem realizace strategie. Koordinuje plnění akčního plánu napříč subjekty a každoročně vyhodnocuje dosažený pokrok.

NSKB staví na třech hlavních strategických oblastech:

1. **Bezpečná strategická infrastruktura:** posílení odolnosti kritických systémů a schopnosti státu včas odhalovat hrozby v kyberprostoru a čelit jim;

2. **Celospolečenská připravenost a rozvoj:** budování digitálních dovedností občanů, zvyšování počtu a motivace kyberbezpečnostních odborníků a podpora inovací;

3. **Mezinárodní spolupráce a prosazování zájmů:** aktivní role Česka v EU, NATO a dalších organizacích při obraně i ochraně otevřeného a svobodného digitálního prostoru.

Strategie zároveň **stanovuje konkrétní priority pro nadcházející roky.** Česká republika bude muset intenzivněji využívat nové technologie k ochraně svých organizací, připravit se na možné kybernetické krize, výrazně zlepšit pracovní podmínky pro experty na kyberbezpečnost ve veřejné správě a rozšiřovat vzdělávání v kybernetické bezpečnosti. Zároveň by měly vznikat alternativní (bezpečnější) varianty k rizikovým technologiím, nové platformy pro sdílení varovných informací a koordinovaný mezinárodní postup k odstrašení škodlivých státních aktérů.

Tyto záměry odrážejí **tři klíčové výzvy,** na které strategie reaguje: rostoucí počet a sofistikovanost kybernetických hrozeb, technologickou závislost na nedůvěryhodných dodavatelích a nedostatek kvalifikovaných odborníků. Zásadní posun představuje **důraz na proaktivní přístup** k zajištění bezpečnosti. Místo pouhého reagování na incidenty strategie prosazuje aktivní vyhledávání skrytých hrozeb, kontinuální monitoring a preventivní opatření. NÚKIB výslovně uvádí, že **Česko nemůže „pasivně čekat" na další útoky a že je nutné hrozby a zranitelná místa včas odhalovat a předcházet jim.** Platí to jak pro zabezpečení informačních systémů, tak pro obranu proti škodlivým aktérům spojeným s nepřátelskými státy.

Strategie otevřeně identifikuje **hlavní protivníky v kyberprostoru.** Vůbec poprvé jsou v oficiálním dokumentu přímo jmenováni největší kybernetičtí nepřátelé Česka, totiž Rusko a Čína (dále pak Severní Korea nebo Írán). Tento adresný přístup navazuje na trend posledních let, kdy české úřady začaly veřejně připisovat odpovědnost za kybernetické útoky konkrétním státům (v květnu 2024 NÚKIB označil za viníka útoku skupinu napojenou na Rusko, v květnu 2025 zase čínskou kyberšpionážní skupinu APT31). Hrozby spojované s **Ruskem a Čínou** jsou dnes považovány za nejvážnější. Ruské aktivity zahrnují kybernetickou špionáž, sabotáže i vlivové operace proti Česku a jeho spojencům, zatímco Čína se snaží pronikat do strategických systémů s cílem je ovládnout či zneužít ve svůj prospěch.

NÚKIB varuje, že intenzita kybernetických útoků prudce roste v souvislosti mimo jiné i s rychlým vývojem technologií, který na jedné straně přináší nové možnosti, na té druhé však i hrozby. V roce 2024 zaznamenal úřad dosud nejvyšší počet závažných kybernetických incidentů, celkem 268. Tyto útoky míří jak na vládní instituce, tak na soukromé firmy či jednotlivce, kteří se staví proti zájmům agresorských režimů. Typickým příkladem jsou DDoS kampaně proruských hackerských skupin v odvetě za kroky české vlády. **„Kyberprostor je zrcadlem reálného světa. Co probíhá v reálném světě, probíhá i v kyberprostoru,"** uvedl trefně v televizním rozhovoru náměstek ředitele NÚKIB Tomáš Krejčí. Kybernetické hrozby tedy bezprostředně odrážejí geopolitické konflikty a napětí.

NSKB 2026–2030 si klade za cíl připravit Česko na tuto realitu a zvýšit jeho odolnost. **Klíčová je spolupráce napříč veřejným, soukromým i akademickým sektorem.** „Je proto třeba více než kdy dříve klást důraz na posilování obranných kapacit, využívání moderních bezpečnostních technologií a na prohlubování spolupráce mezi veřejným, soukromým a akademickým sektorem," zdůraznil ředitel NÚKIB Lukáš Kintr v úvodním slovu ke strategii. Společná bezpečnost totiž **není pouze úlohou státu,** ale vyžaduje důvěru a aktivní zapojení expertů, firem i běžných uživatelů. Nová strategie proto vznikla konsenzem napříč institucemi a obory. NÚKIB spojil síly **s orgány odpovědnými za kybernetickou obranu, diplomacii i boj proti kyberkriminalitě.** Všechny tyto složky nyní sdílejí jednotný pohled na největší hrozby, slabiny a potřebná opatření.

Tento jednotný přístup se odráží v celé strategii a má zajistit, že Česko dokáže účinně reagovat na kybernetické incidenty i dlouhodobě budovat bezpečné digitální prostředí. Důraz je kladen také na **lidské zdroje.** Stát plánuje **investovat do rozvoje kyberbezpečnostních talentů a zlepšit podmínky pro specialisty ve veřejné správě,** aby si udržel špičkové odborníky. Neméně důležité je zvyšování povědomí veřejnosti – od školní výuky až po osvětové kampaně – tak, aby se základní pravidla digitální bezpečnosti stala běžnou součástí života občanů.

Strategie je postavena na principech **realističnosti a měřitelnosti.** Opatření budou naplňována prostřednictvím akčních plánů, které určí konkrétní úkoly, odpovědné instituce, termíny a ukazatele plnění. Financování bude zajištěno z národních i evropských zdrojů, s důrazem na efektivní využití prostředků a koordinaci mezi institucemi. Stát má zároveň usilovat o dlouhodobou udržitelnost systému a o snižování závislosti na externích financích.

Nová strategie přináší Česku ucelenou vizi digitálně vyspělé a bezpečné země. V cílovém stavu má být Česko státem s **odolnou informační infrastrukturou, vzdělanou, kriticky myslící a inovativní společností a silnými mezinárodními i domácími partnerstvími,** které společně zajistí efektivní ochranu a prosazování českých zájmů v kyberprostoru.

Investice do kybernetické bezpečnosti a zejména do lidí, kteří ji zajišťují, jsou vnímány nejen jako nutnost, ale i jako konkurenční výhoda podporující ekonomický růst země. Představitelé NÚKIB zdůrazňují, že kybernetická bezpečnost je **investicí do budoucnosti a konkurenceschopnosti** České republiky a že nová strategie ukazuje, jak zajistit bezpečnější a prosperující kyberprostor pro všechny. Úspěch však bude záviset na důsledné realizaci navržených opatření a na pokračující spolupráci státu, expertů i soukromé sféry. Jedině společným úsilím lze dosáhnout toho, že se Česká republika stane **odolnější vůči kybernetickým hrozbám a připravená na digitální budoucnost.**