**Experti apelují na posílení kybernetické bezpečnosti jaderných provozů včetně malých reaktorů. Do Česka míří směrnice NIS2**

***Na konci ledna vláda prostřednictvím Podvýboru pro energetiku vyjádřila podporu rozvoji české jaderné energetiky. Nejen nové projekty, jako jsou dostavba jaderných bloků v Dukovanech a Temelíně nebo tak zvané malé modulární reaktory, ale i ty stávající budou muset zohlednit přísnější legislativu upravující zabezpečení provozů z pohledu kybernetické bezpečnosti. Českou republiku totiž v rámci eurounijní legislativy čeká implementace směrnice NIS2.***

**Regulaci a zvýšení úrovně kybernetické bezpečnosti v České republice nastolí účinnost nového zákona o kybernetické bezpečnosti; zhruba ve druhé polovině roku 2024. Nový zákon s sebou ponese i změny dané směrnicí NIS2. Ta rozděluje subjekty na dvě skupiny, a to na zásadní entity a na důležité entity. Právě energetika patří k těm zásadním.**

**Kybernetická bezpečnost jaderných projektů je pro jejich provoz prioritní oblastí, a to nejen v České republice. V poslední letech po celém světě narůstá počet kybernetických útoků, jejichž cílem je narušování kritické infrastruktury – nemocnice, vodárny či elektrárny se stávají pro hackery jasnými cíli.**

**„*Již v loňském roce americký prezident Joe Biden na základě zprávy FBI o internetové kriminalitě důrazně varoval celý svět před narůstajícími ruskými hackerskými útoky, které jsou odvetou za sankce uvalené na Rusko kvůli válce s Ukrajinou,“* připomíná Pavel Duchan, konzultant kybernetické bezpečnosti ze společnosti DoxoLogic, která se problematikou kyberbezpečnosti dlouhodobě zabývá.**

**Celosvětové statistiky ukazují významný nárůst narušení dat a hackingu.**

**V České republice mají povinnost hlásit Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB) kybernetické incidenty jen ty subjekty, které reguluje zákon o kybernetické bezpečnosti. Těch je nyní přibližně 400. „*Co se týče počtu kybernetických incidentů, ten byl u těchto subjektů v minulém roce obdobný jako v roce 2021,“* uvedl Marek Vala, vedoucí oddělení komunikace NÚKIB. Podle Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2021 bylo NÚKIB hlášeno 476 kybernetických incidentů.**

**Data, kterými NÚKIB disponuje, jsou tak pouze špičkou ledovce a lze z nich odvodit celkový obraz stavu kybernetické bezpečnosti především u kritické infrastruktury státu. V oblasti kybernetické kriminality je však evidován dlouhodobý nárůst. Například za rok 2022 policie evidovala meziročně dvojnásobek těchto trestných činů (v roce 2021 9 518, v roce 2022 18 554).**

**Díky novému zákonu, do nějž bude implementována i zmiňovaná eurounijní směrnice NIS2, stoupne počet subjektů povinných hlásit kybernetické incidenty NÚKIB z původních cirka 400 na více než 6 000.**

***„Pokud chceme ochránit naši republiku před hrozbami 21. století, pak je posilování kybernetické bezpečnosti zejména v oblasti krizové infrastruktury přímo nutností. Narušení, byť jen jediného článku řetězce například v energetice, může mít zásadní dopad na chod celé společnosti. Tomu musíme aktivně čelit a rozšiřovat možnosti, jak se proti takovým útokům nejen bránit, ale také jak jim předcházet,“* konstatuje Róbert Teleky (KDU-ČSL), předseda sněmovního podvýboru pro energetiku.**

**Je třeba si navíc uvědomit, že kyberprostor již dávno není jen pro kriminální živly. „*Online ekvivalentem protestujících, kteří bojují za určitou věc, jsou kyberaktivisté. Jejich hlavním cílem bývá narušení chodu dané společnosti a šíření povědomí o své činnosti,*“ vysvětluje Duchan z DoxoLogic.**

**Očekává se, že kyberaktivismus v nadcházejících letech poroste. I proto se stává kybernetická bezpečnost čím dál tím palčivější otázkou bezpečnosti jaderných projektů. Petr Pávek, který stojí za projektem Teplator, inovativního konceptu nepřetržité výroby tepla pro vytápění, uvedl, že právě kyberbezpečnost je něco, co v žádném projektu nemůže být nikdy hotovo. „*Zabezpečení veškerých IT systémů je pro nás absolutní prioritou. Jak v projektové fázi, tak v ostrém provozu je bezpečnost naprosto zásadním aspektem, jemuž věnujeme nejvyšší pozornost*.“ Otázky kybernetické bezpečnosti považují za zásadní i autoři dalších alternativních jaderných projektů, jako je plynem chlazený rychlý reaktor IV. generace Napoleon HR-4F s potenciálem výroby vodíku od skupiny FABA CAPITAL nebo malý jaderný reaktor David od strojírenské skupiny Witkowitz.**

**Podle**[**odhadů Statista Cybersecurity Outlook**](https://www.statista.com/outlook/tmo/cybersecurity/worldwide#cost)**se očekává, že globální náklady na boj s počítačovou kriminalitu v příštích pěti letech vzrostou z 8,44 bilionu dolarů (rok 2022) na 23,84 bilionu dolarů do roku 2027.**