Kybernetický zákon teď dopadá na více než 6000 organizací, říká Dalibor Kovář

19.11.2025 - IT a technologie | HAVEL & PARTNERS

Legalweb otevírá novou sérii textů věnovanou kyberbezpečnosti a nedávným změnám zákona o kybernetické bezpečnosti, účinným od začátku listopadu. „Nová regulace dopadá na více než 6000 organizací v České republice napříč 22 odvětvími. Rozhodující je typ služby a velikost – regulace se typicky aplikuje na subjekty s více než 50 zaměstnanci nebo obratem přes 10 milionů eur," upozorňuje na rozsah dopadů nových pravidel Dalibor Kovář, partner kanceláře HAVEL & PARTNERS.

Pokud byste měl vybrat z nového zákona o kybernetické bezpečnosti tři základní informace, které by měl každý znát, o co by šlo?

Nová regulace dopadá na více než 6000 organizací v České republice napříč 22 odvětvími. Rozhodující je typ služby a velikost – regulace se typicky aplikuje na subjekty s více než 50 zaměstnanci nebo obratem přes 10 milionů eur.

Organizace musí hlásit incidenty bez zbytečného odkladu: do 24 hodin prvotní hlášení, do 72 hodin aktualizace a do 30 dnů závěrečnou zprávu. Velcí poskytovatelé regulovaných služeb hlásí NÚKIB, menší subjekty Národnímu CERT.

Zvyšují se požadavky na bezpečnostní opatření podle režimu povinností. Vyšší režim zahrnuje například pokročilou detekci hrozeb, kryptografii a řízení dodavatelů. Všechny subjekty mají na implementaci jeden rok od registrace.

Nicméně regulace nepředpokládá, že budou v této lhůtě zavedena všechna bezpečnostní opatření.

Co byznys v nové úpravě kyberbezpečnosti z vašich dosavadních zkušeností nejvíce podceňuje?

Firmy vnímají compliance jako jednorázový projekt, nikoli jako kontinuální řízení rizik, školení a audity. Realita je taková, že hodně firem za rok teprve začne.

Druhý aspekt je osobní odpovědnost vedení. NÚKIB může uložit dočasný zákaz výkonu funkce minimálně na šest měsíců za opakované nebo závažné porušení povinnosti při výkonu funkce. To není pokuta pro firmu – je to silný donucovací prostředek na úrovni člena vedení.

Třetím faktorem je řízení dodavatelů. Organizace musí smluvně přenášet konkrétní povinnosti na všechny dodavatele a subdodavatele, což vytváří exponenciální administrativní zátěž.

Většina útoků využívá lidské chyby. Zákon proto vyžaduje prokazatelné školení všech zaměstnanců včetně vedení – bez toho jsou všechny systémy prakticky zbytečné.

Jak celkově hodnotíte současnou regulaci kyberbezpečnosti? Je odpovídající?

Regulace jde správným směrem. NÚKIB zaznamenává průměrně kolem dvou desítek incidentů měsíčně, rok 2024 přinesl 268 hlášení. Harmonizace díky NIS2 je nezbytná pro jednotný přístup v EU.

Existují však obavy o proporcionálnost. Malí poskytovatelé ve zdravotnictví a střední firmy budou zatíženi neúměrně. NÚKIB má omezené kapacity na dohled nad tisíci subjekty a hrozí riziko politizace při hodnocení dodavatelů.

Pozitivem je technologická neutralita a dva režimy povinností reflektující realitu různých organizací. Klíčový bude test v příštích dvou letech – zda NÚKIB bude provádět konzistentní a inteligentní dohled bez zbytečné administrativní zátěže.

https://www.havelpartners.cz/kyberneticky-zakon-ted-dopada-na-vice-nez-6000-organizaci-rika-dalibor-kovar