Přísnější pravidla pro kyberbezpečnost zasáhnou tisíce firem. Připravte se, radí odborník

22.5.2025 - | HAVEL & PARTNERS

Česko má za sebou zásadní krok v oblasti kybernetické bezpečnosti. Poslanecká sněmovna na konci dubna schválila nový zákon, který zavádí evropskou směrnici NIS2 a rozšiřuje okruh firem pro které budou platit vyšší nároky na řízení rizik a odpovědnost managementu. Společnosti si také budou muset více hlídat spolupráci s dodavateli.

„Předpokládáme, že by regulace mohla být účinná nejdřív od září či října tohoto roku,“ říká právník HAVEL & PARTNERS Dalibor Kovář. Finální datum účinnosti nových pravidel kyberbezpečnosti se bude totiž odvíjet od rychlosti zbývající části legislativního procesu, tedy schválení Senátem a podepsání prezidentem. *„Spolu s roční zákonnou lhůtou k naplnění povinností se to sice může jevit jako dostatek času, ale splnění podmínek vyžaduje celkem pečlivou a dlouhodobější přípravu. Se změnami ve firmě bych tak rozhodně neotálel,“* dodává Kovář.

Nový zákon rozšiřuje působnost na tisíce podniků a organizací napříč 22 odvětvími – od energetiky, zdravotnictví, potravinářství až po digitální služby. Povinnosti se ale mohou dotknout i dalších subjektů mimo vyjmenovaná odvětví, a to zejména v případě, že jsou dodavateli firem a společností, kterých se regulace týká. Některé subjekty navíc mezi regulované může zařadit i sám Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), když vyhodnotí, že jejich činnost může mít dopad na kybernetickou bezpečnost v zemi.

Pokuty v milionech EUR

Zákon nově klade důraz na osobní odpovědnost vedení firem za řízení kybernetických rizik. Management musí například schvalovat bezpečnostní politiku firmy, zajistit školení zaměstnanců v oblasti kyberbezpečnosti a pravidelně vyhodnocovat bezpečnostní opatření. Za porušení povinností hrozí pokuty až 10 milionů eur nebo dvě procenta celosvětového obratu. Dalibor Kovář proto doporučuje firmám, aby s co nejdříve prověřily, zda a v jakém rozsahu na ně nová regulace dopadá. *„Zejména pak jaká jsou jejich primární aktiva, například klíčové systémy, data, infrastruktura„* přiblížil.

Nezbytná je pode něj i revize smluv. *„Je nutné aktualizovat smlouvy s dodavateli, interní postupy i bezpečnostní dokumentaci. Klíčové je zároveň proškolit zaměstnance i vedení v nových povinnostech a kybernetických rizicích. Určitě se vyplatí využít konzultace a odborné audity, zejména v oblasti řízení rizik a incidentů*,“ vyjmenoval.

Čeká se na prováděcí předpisy

Mnoho detailů bude jasných ale až po vydání prováděcích vyhlášek. Například přesné vymezení regulovaných služeb. Vyhlášky se v polovině tohoto května objevily v meziresortním připomínkovém řízení, ale dokud nebudou účinné, podniky nebudou mít jistotu, zda se na ně zákon opravdu vztahuje. *„A to přirozeně komplikuje přípravu. Vyhlášky se teoreticky mohou objevit ve Sbírce zákonů až po účinnosti samotného zákona,“* potvrzuje Kovář.

Na Slovensku už obdobná legislativa platí od 1. ledna 2025. Učinná už je i v Belgii, Chorvatsku, Řecku, Maďarsku, Itálii, Lotyšsku, Litvě, na Maltě a v Rumunsku. Zkušenosti v těchto zemích ukazují, že včasná příprava je klíčová – společnosti, které začaly s implementací v předstihu, zvládají přechod na nová pravidla snadněji. „*Prokazatelný postup zavádění nových povinností do praxe organizací bude bezesporu hrát roli i v rámci případných kontrol a jejich závěrů*," dodává právník.

https://www.havelpartners.cz/prisnejsi-pravidla-pro-kyberbezpecnost-zasahnou-tisice-firem-pripravte-se-radi-odbornik