SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Připomínky Svazu průmyslu a dopravy České republiky k návrhu vyhlášky o informační bezpečnosti
Č. J.	101/2024
DATUM ZPRACOVÁNÍ	21. 10. 2024
KONTAKTNÍ OSOBA	Kateřina Kalužová
E-MAIL	kkaluzova@spcr.cz

ZÁSADNÍ KONKRÉTNÍ PŘIPOMÍNKY

1) **Zohlednění NATO certifikace dodavatelů v rámci procesu certifikace informačního systému a v rámci podmínek pro jeho provozování (obecné připomínky k materiálu):**

Doporučujeme, aby Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) v rámci návrhu vyhlášky o informační bezpečnosti (dále jen „vyhláška o informační bezpečnosti“) zohlednil v rámci podmínek provozování systémů a v rámci procesu certifikace informačního systému skutečnost, kdy **dodavatelé komponent systémů (např. operačních systémů či cloudových řešení) disponují certifikací pro nakládání s utajovanými informacemi příslušného stupně utajení (např. NATO Restricted) vydávané dle příslušných předpisů Organizace Severoatlantické smlouvy (NATO).**

Právě dodavatelé disponující výše uvedenou certifikací osvědčují, že splňují nejpřísnější bezpečnostní požadavky na ochranu utajovaných informací. Tato skutečnost by se měla pozitivně promítnout do rozsahu povinností provozovatelů systémů, kteří na takové dodavatele spoléhají, a měli by tak na ně být kladeny nižší nároky z hlediska rozsahu bezpečnostních povinností, které musí provozovatelé systémů plnit. Ačkoliv dle vyhlášky o informační bezpečnosti není při provádění certifikace informačního systému přímo hodnoceno plnění bezpečnostních požadavků ze strany dodavatelů, doporučujeme tuto provazbu ve vyhláškách zohlednit například doplněním nového ustanovení k § 31 týkajícího se povinností ve vztahu k dodavatelům (nebo doplněním zcela nového paragrafu) v následujícím znění:

§ 31
(1) *Pokud se na provozu, rozvoji nebo zajištění informační bezpečnosti podílí dodavatel, pak bezpečnostní dokumentace pro účely analýzy rizik stanoví*

a. *zásady hodnocení rizik dodavatele,*
b. *náležitosti smlouvy s dodavatelem, kterými jsou smluvní ujednání o úrovni dodávaných služeb, o realizaci bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti, a*
c. *pravidla pro ověření bezpečnostních opatření zavedených dodavatelem.*

(2) Dodavatelé disponující certifikací pro nakládání s utajovanými informacemi daného stupně utajení, vydávané dle předpisů Organizace Severoatlantické smlouvy, se považují za vyhovující bezpečnostním požadavkům kladeným na systémy. (pozn.: lze doplnit také jako zcela nový paragraf vyhlášky).