

Průvodce řízením aktiv a rizik podle vyhlášky o kybernetické bezpečnosti

Autor: Národní úřad pro kybernetickou a informační bezpečnost (srpen 2022)

Zdroj: [Tisková zpráva](#), [Vyhláška](#) a [Průvodce](#)

Souhrn

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) ve spolupráci s Ministerstvem vnitra, Státní pokladnou Centrem sdílených služeb, Ministerstvem průmyslu a obchodu, Ministerstvem zemědělství, Ministerstvem školství, mládeže a tělovýchovy a Fakultní nemocnicí Plzeň připravil obsáhlý podpůrný materiál k problematice řízení aktiv a rizik dle § 4 a § 5 vyhlášky o kybernetické bezpečnosti.

Tato vyhláška zapracovává Směrnici NIS a pro informační systémy kritické informační infrastruktury, komunikační systémy kritické informační infrastruktury, významné informační systémy, informační systémy základní služby anebo informační systémy nebo sítě elektronických komunikací, které využívá poskytovatel digitálních služeb, upravuje:

- obsah a strukturu bezpečnostní dokumentace,
- obsah a rozsah bezpečnostních opatření,
- typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů,
- náležitosti a způsob hlášení kybernetického bezpečnostního incidentu,
- náležitosti oznámení o provedení reaktivního opatření a jeho výsledku,
- vzor oznámení kontaktních údajů a jeho formu,
- způsob likvidace dat, provozních údajů, informací a jejich kopií.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB) a vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VKB) stojí především na přístupu založeném na posuzování rizik. Proto NÚKIB ve spolupráci s dalšími subjekty vytvořil Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti. Materiál přibližuje problematiku řízení aktiv a rizik především těm, kteří s ní mají minimální zkušenosti nebo nemají zkušenosti žádné. Zkušenější osoby zodpovědné za řízení aktiv a rizik mohou dokument využít jako zdroj inspirace pro vylepšení již zavedených postupů.

Nově zveřejněný podpůrný materiál představuje jeden z možných správných postupů řízení aktiv a rizik v souladu s VKB. Jedná se o doporučení a je nutné uvedené základní principy přizpůsobit prostředí konkrétní organizace. Dokument obsahuje teoretické i praktické části a modelové příklady. V teoretické části jsou rozebírána jednotlivá ustanovení VKB, praktická

část obecně popisuje, jak požadavky plynoucí z těchto ustanovení naplnit. Modelové příklady obsahují konkrétní ukázky obecných postupů, které jsou aplikovány v prostředí fiktivního Ministerstva pro certifikaci senzorů. Podpůrný materiál vychází z VKB, ale je doplněn o řadu zkušeností z praxe.

