Národní bezpečnostní úřad, P. O. BOX 49, CZ 150 00 Praha 56

Národní
bezpečnostní
úřad

Č. j.: 2770/2016-NBÚ/80
Sp. zn.: 80 - 29736/2016

Ministerstvo vnitra
Odbor veřejné správy, dozoru a kontroly
Praha

Praha 8. duben 2016

Odmítnutí přístupu člena zastupitelstva hlavního města Prahy do informačních systémů hlavního města Prahy s odkazem na zákon o kybernetické bezpečnosti – odpověď

V návaznosti na Váš dopis sp. zn. MV-44141-2/ODK-2016 uvádím, že zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) stanovuje v § 4 odst. 2 povinnost pro správce významného informačního systému v rozsahu nezbytném pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření pro významný informační systém. Dále pak podle § 5 odst. 2 písm. i) zákona o kybernetické bezpečnosti patří mezi bezpečnostní opatření i řízení přístupu osob k významnému informačnímu systému a podle § 6 písm. a) a c) zákona o kybernetické bezpečnosti stanoví prováděcí právní předpis obsah bezpečnostních opatření a rozsah bezpečnostní opatření pro orgány a osoby uvedené v § 3 písm. c) až e) – tedy i pro správce významného informačního systému. Tímto prováděcích právním předpisem je vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), která řízení přístupu osob k významnému informačnímu systému upravuje v § 11 odst. 1 a 2, kde v odstavci 1 je uvedeno, že „orgán a osoba uvedená v § 3 písm. c) až e) zákona na základě provozních a bezpečnostních potřeb řídí přístup k…významnému informačnímu systému“.

Obecně lze tedy vyvodit, že zákon o kybernetické bezpečnosti a na něj navazující vyhláška o kybernetické bezpečnosti stanovují povinnost správců významných informačních systémů řídit přístupy uživatelů do systémů na základě jejich oprávnění přístupu k jednotlivým datům. Ani jeden z těchto předpisů však materiálně rozsah oprávnění přístupů jednotlivých uživatelů neurčuje. O povolení přístupu konkrétního uživatele k významnému informačnímu systému nebo jeho části rozhoduje správce systému např. prostřednictvím garanta aktiv. Ten je pak samozřejmě vázán analýzou rizik či jinými předpisy, jako je zákon č. 131/2000 Sb., o hlavním městě Praze, ve znění pozdějších předpisů, interními předpisy organizace aj.

Problém oprávněnosti přístupu konkrétního uživatele k předmětnému informačnímu systému není tedy primárně otázkou zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů, ale otázkou rozsahu oprávnění přístupu zastupitele k informačním systémům hlavního města Prahy.

Mgr. Jiří Malý
ředitel odboru právního a legislativního
elektronicky podepsáno