BRK-05-2016-05, př. 1
počet stran: 2

Informace o průběhu implementace procesního rámce pro řízení informační bezpečnosti u Zdravotnické záchranné služby Kraje Vysočina, Hasičského záchranného sboru Kraje Vysočina a u Krajského ředitelství Policie Kraje Vysočina.

1. Zdravotnická záchranná služba Kraje Vysočina

Na základě požadavků zákona 181/2014 Sb. o kybernetické bezpečnosti, došlo v roce 2015 k úspěšné implementaci procesního rámce systému řízení bezpečnosti informací u ZZS KV. ZZS KV je v současné době držitelem certifikátu ISO/IEC 27001, který je potvrzením úspěšného nastavení procesního rámce této normy. Dne 23.11. - 25.11.2016 úspěšně proběhl dozorový externí audit integrovaného systému řízení ISO 9001 – systém řízení kvality, ISO 14001 – environmentální management, OHSAS 18001 – ochrana a bezpečnost při práci a ISO/IEC 27001 – systém managementu bezpečnosti informací.

V současné době dochází k dalšímu rozvoji a zkvalitňování systému tím, že jsou dále podrobněji definována pravidla ISO 27001 pro jednotlivé dílčí činnosti ZZS KV. Například se jedná o zvýšení uživatelské bezpečnosti osobních PC – politika hesel, zvýšení bezpečnosti informací na firemních informačních systémech spravujících zdravotnickou dokumentaci – logování záznamů, zvýšení výkonnosti a zabezpečení serveru, detailní popis procesů systému řízení informací v oblasti IT, nákup technologie na sledování incidentů pro bezpečnost vnitřního systému. Vzhledem k tomu, že ZZS KV je již od roku 2008 držitelem certifikátu kvality dle ISO 9001, je v organizaci zavedena široká míra opatření vztahující se k ochraně bezpečnosti informací, především v oblasti ochrany osobních údajů, jak zaměstnanců, tak pacientů. Z tohoto důvodu bylo pro ZZS KV zavedení systému řízení bezpečnosti informací logickým a návazným krokem k rozvoji integrovaného systému řízení kvality.

2. Hasičský záchranný sbor Kraje Vysočina

Implementace ISMS u HZS Kraje Vysočina vychází ze závazných pravidel a pokynů, které v rámci rezortu Ministerstva vnitra ČR vydává odbor kybernetické bezpečnosti a koordinace ICT. K těmto pravidlům patří řízení přístupu do kybernetického prostoru MV, využívání služebních prostředků ICT pro pracovní účely, zabezpečení proti neoprávněnému použití nebo zcizení, ochrana před škodlivým SW, zálohování dat, zabezpečení elektronické komunikace, řízení přístupu k systémům rezortu MV přes veřejnou síť Internet, použití legálního SW, apod.
Jedním z preventivních opatření proti kybernetickým rizikům bylo zřízení e-mailové adresy kyberinfo@grh.izscr.cz na jaře roku 2016, ze které jsou jednotlivým HZS krajů zasílány informace o kybernetických hrozbách a na kterou HZS krajů zasílají informace o případných incidentech.
V současné době je připravován SIAŘ Generálního ředitele HZS ČR, který stanovuje povinnost všem uživatelům komunikačních a informačních systémů v rámci HZS ČR absolvovat školení v oblasti kybernetické bezpečnosti – seznámení se základními materiály o dopadech zákona č. 181/2014 Sb. o kybernetické bezpečnosti na resort MV. Uvedený předpis stanovuje i zásady bezpečného chování v rámci kybernetického prostoru.

3. Krajské ředitelství Policie Kraje Vysočina.

V souvislosti s přípravou na implementaci požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“), do prostředí policie byl vydán rozkaz policejního prezidenta č. 188/2014 ze dne 1. září 2014, kterým se zavádí u Policie České republiky organizační opatření pro systém řízení kybernetické bezpečnosti. Současně byl zahájen proces pro ustanovení a implementaci systému řízení informační bezpečnosti v rámci Odboru informatiky a provozu informačních technologií Policejního prezidia České republiky (dále jen „odbor informatiky“), neboť odbor informatiky je provozovatelem centrálních informačních systémů

policie, tj. většiny těch, které byly do dnešního dne určeny podle ZoKB významným informačním systémem nebo informačním systémem kritické informační infrastruktury. Přesah systému řízení bezpečnosti informací oboru informatiky je definován směrem k uživatelům těchto informačních systémů. Tento systém řízení byl následně certifikován podle mezinárodní normy ISO/IEC 27001.
V rámci databázového centra odboru informatiky je provozováno dohledové pracoviště v režimu 24x7, které je současně jednotným kontaktním bodem pro hlášení bezpečnostních incidentů v rámci policie. Toto dohledové centrum zajišťuje hlášení bezpečnostních incidentů směrem k resortnímu Dohledovému centru eGovernmentu, které zajišťuje komunikaci směrem k NCKB/NBÚ.
Na území Krajského ředitelství policie kraje Vysočina je provozován jediný informační systém určený podle ZoKB, jako informační systém kritické informační infrastruktury, kterým je příjem linky tísňového volání, potažmo IS Jitka.
Ministerstvem vnitra bylo rozhodnuto o zavedení systému řízení bezpečnosti informací s platností pro celý resort ministerstva, tj. včetně krajských ředitelství policie, dále ZoKB požadované bezpečnostní role, tj. manažer kybernetické bezpečnosti, auditor kybernetické bezpečnosti, architekt kybernetické bezpečnosti, byly ustanoveny v rámci struktury ministerstva. Zavedený systém řízení byl následně certifikován podle mezinárodní normy ISO/IEC 27001.
Bezpečnost informací v rámci policie není vázána pouze na systémy určené podle ZoKB. Bezpečnost informací je řešena napříč všemi informačními systémy policie. Proto jsou některé informační systémy, provozované v rámci krajských ředitelství policie napojeny na centrální nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, tzv. SIEM.
Pro komunikaci s dalšími orgány veřejné správy se využívá výhradně prostupů prostřednictvím centralizované komunikační infrastruktury veřejné správy, tzv. Centrální místo služeb, které zajišťuje garantované, bezpečné a auditovatelné propojení jednotlivých orgánů mezi sebou.