

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Otevřený zdrojový kód	3
<i>Doporučení NÚKIB a MVČR</i>	3

Otevřený zdrojový kód

Doporučení NÚKIB a MVČR

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) ve spolupráci s Ministerstvem vnitra (MV) připravil [bezpečnostní doporučení pro vývoj otevřeného softwaru](#). Doporučení je určeno vývojářům a osobám zabývajícím se kybernetickou bezpečností nebo společností dodávajícím software. Nenahrazuje požadavky zákona o kybernetické bezpečnosti a není pevně závazné. Je tak na konkrétních organizacích, které části a v jaké míře budou u svých projektů případně využívat.

[Tento materiál](#) může pomoci k rozšíření open-source řešení v rámci veřejné správy nebo ho mohou využít i subjekty soukromého sektoru, pakliže se rozhodnou zveřejnit vyvíjený software pod open source licencí.

Uvedená bezpečnostní doporučení mohou být důležitou inspirací při vývoji otevřených řešení ve veřejné správě, která jsou trendem například v oblasti eGovernmentu některých evropských států již několik posledních let. Navíc vzhledem k narůstajícímu počtu kybernetických hrozeb je dodržování bezpečnostních zásad při rozvoji eGovernmentu naprosto klíčové a jinak tomu není ani při budování otevřených řešení. Na vytvořený materiál Ministerstvo vnitra odkáže i v chystané metodice k projektu s názvem Portál otevřeného kódu.

Zmíněný software s otevřeným kódem přináší určité bezpečnostní výhody, lze v něm jednodušeji najít záměrně vytvořená „zadní vrátka“, a tak odhalit i méně zjevné zranitelnosti. Na druhou stranu je otevřen i případným útočníkům, což jim zjednodušuje práci ve zneužití bezpečnostních mezer softwaru. Proto by organizace při zveřejňování zdrojového kódu měla zvážit možné přínosy a taktéž rizika s tím spojená. Cílem vydaného doporučení je snížit množství potenciálních zranitelností („secure by design“) a podpořit co možná nejrychlejší nápravu v případě, že se v kódu nějaká zranitelnost objeví.

V doporučení jsou popsány organizační opatření pro zacházení s kódem, jeho správa a tvorba, dále použité knihovny třetích stran a to, jak s nimi nakládat, kryptografické prostředky v komunikaci, záznamy o událostech pro aplikace a knihovny, relační databáze pro ukládání dat a v neposlední řadě kontinuální integrace jakožto automatizované spouštění definovaných procesů při změnách kódu.

Stručný přehled pravidel

Kategorie	Opatření	Popis
Organizační opatření	Před začátkem vývoje je zváženo výběr použitého jazyka a frameworku z hlediska bezpečnosti	
	Zdrojový kód je zveřejněn co nejdříve	
	Součástí repozitáře je soubor SECURITY	
	Je určena osoba zodpovědná za nahlášené zranitelnosti	
	Nahlášené zranitelnosti jsou opraveny do 90 dnů	
	Všechny opravené zranitelnosti jsou uvedeny v souboru se změnami	
	Účty vývojářů při autentizaci používají vícefaktorovou autentizaci	
	Účty vývojářů jsou svázány s pracovní e-mailovou adresou	
	Dokumentace je součástí repozitáře	
	Pro knihovny: Zranitelné verze knihoven jsou označeny	
	Neudržované aplikace a knihovny jsou označeny	
	Pro aplikace: Výchozí konfigurace je restriktivní	
	Správa a tvorba kódu	
	Zdrojový kód je verzován (VCS) a zveřejněn v otevřeném repozitáři	
	Pro vývoj se používají oddělené větve, které se následně slučují do hlavní vývojové větve	
	Je prováděna kontrola změn kódu	
	Repozitář neobsahuje binární spustitelné soubory nebo kompilované kódy	

[illegible]

Last update: **2022/05/06 09:51**

