

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Table of Contents

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

Otevřený zdrojový kód

Otevřeným zdrojovým kódem eGovernmentu se rozumí zdrojový kód komponenty informačního systému určený pro další využití jiným orgánem veřejné správy, zkoumání kódu, rozhraní, algoritmů a postupů odbornou veřejností, přijímání návrhů na zlepšení její funkčnosti, kvality a bezpečnosti ze strany odborné veřejnosti, který je zveřejněný prostřednictvím jednotného úložiště.

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 licenci.

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	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	

Kategorie	Opatření	Popis
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	
	U dynamicky typovaných jazyků je využíváno striktní typování	
Použité knihovny	Aplikace a knihovny využívají udržované závislosti	
	Preferovány jsou knihovny s bezpečným API	
	Preferovány jsou knihovny, jejichž autoři „dbají na bezpečnost“	
	Pro aplikace: Aplikace při definování závislostí používají „lock file“	
	Závislosti jsou stahovány z důvěryhodných úložišť	
Kontinuální integrace	Pro aplikace: Jsou kontrolovány verze použitých závislostí	
	Nalezené zranitelnosti jsou testovány v rámci CI	
	Pro aplikace: Sestavení aplikace je plně automatizované	
	Je definován a vynucován standard pro zdrojový kód	
	Jsou prováděny jednotkové nebo integrační testy v oblastech s vlivem na bezpečnost	
	Jsou prováděny automatizované bezpečnostní testy	
	Je prováděna kontrola tajných identifikátorů ve zdrojovém kódu	
Kryptografické prostředky	Pro aplikace: Vydané verze jsou podepsány	
	Jsou využívány ověřené kryptografické knihovny	
	Jsou využívány odolné kryptografické prostředky	
	Při použití protokolu TLS je podporována alespoň verze 1.2	
	Je prováděno ověřování použitého certifikátu	
	Aplikace používá systémové úložiště důvěryhodných certifikátů	
	Porovnání hašů uložených hesel je odolné na časovou analýzu	
Záznamy o událostech	Ke generování náhodných tokenů jsou použity kryptograficky bezpečné pseudonáhodné generátory	
	Tajné identifikátory jsou odstraňovány z paměti	
	Pro knihovny: Knihovny využívají standardní rozhraní pro logování	
	Pro aplikace: Aplikace umožňuje logování důležitých akcí	
	Pro aplikace: Aplikace podporuje napojení na centrální log management	
Relační databáze	Nejsou zaznamenávány tajné identifikátory	
	Výjimky jsou řízeny	
	Jsou využívány primární klíče	
	Jsou používány cizí klíče při vazbě na číselníkové hodnoty anebo na jiné entity	
	V rámci databáze jsou kontrolovány hodnoty parametrů („constraints“)	
	Pokud databázový sloupec předpokládá unikátní hodnotu, je využit unikátní index	
	Při vkládání dat jsou využívány transakce	
	Databázové schéma je komentováno	

[open](#), [source](#), [zdrojovy](#), [kod](#)

From:

<https://archi.gov.cz/> - Architektura eGovernmentu ČR

Permanent link:

https://archi.gov.cz/znalostni_baze:otevreny_zdrojovy_kod

Last update: **2022/05/06 10:56**

