Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Brno 2. února 2020
Č.j.: 952/2021-NÚKIB-E/210

Věc: Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane  ,

Národní úřad pro kybernetickou a informační bezpečnost (dále jen jako „**NÚKIB**“) obdržel dne 19. 1. 2021 Vaši žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. V žádosti požadujete poskytnutí metodického materiálu, jak správně vyhovět požadavku, který je zformulován v ustanovení § 19 odst. 4 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen jako „**VKB**“). Konkrétně pak Váš dotaz směřuje na výklad pojmů „kryptografické klíče a obdobná úroveň bezpečnosti“.

K Vámi zaslané žádosti uvádím následující:

Ustanovení § 19 odst. 4 VKB v sobě zakotvuje úpravu postupu v případě, kdy povinné osoby prozatím nenaplňují požadavky pro zabezpečení ověřování identit podle ustanovení § 19 odst. 3 VKB. Úprava čtvrtého odstavce daného ustanovení stanovuje povinnost, aby nástroj pro ověřování identity uživatelů používal autentizaci kryptografických klíčů a zaručoval obdobnou úroveň bezpečnosti. Na tuto zákonnou dikci navazuje ustanovení § 26 VKB, kde jsou specifikovány kryptografické prostředky, mezi které jsou zařazeny i kryptografické klíče. Pojem kryptografické klíče je v tomto kontextu chápán jako klíčový pár asymetrické kryptografie, jenž je použit v rámci zabezpečení procesu autentizace uživatele vůči danému systému.

Konkrétní požadavky vyplývají z ustanovení § 26 VKB, kde je v písmenu d) stanoveno, že *„Povinná osoba pro ochranu aktiv informačního a komunikačního systému – d) zohledňuje doporučení v oblasti kryptografických prostředků vydaná Úřadem, zveřejněná na jeho internetových stránkách.“*

Ve smyslu výše citovaného tak NÚKIB vypracoval v oblasti kryptografických prostředků doporučující dokument, kde jsou v souladu s ustanovením § 26 VKB definovány bezpečné kryptografické prostředky, které jsou povinné osoby zavázány zohlednit, tzn. že by měly z tohoto dokumentu vycházet. Toto doporučení mimo jiné obsahuje souhrn schválených

algoritmů pro procesy dohod na klíči a šifrování klíčů. Zde je na místě uvést, že tyto kryptografické klíče, které se řídí ustanovením § 26 VKB a doporučením vydaným NÚKIB, řeší pouze doporučené algoritmy těchto klíčů.
Doporučující dokument v oblasti kryptografických prostředků je dostupný zde: Národní úřad pro kybernetickou a informační bezpečnost – Doporučení v oblasti kryptografických prostředků (nukib.cz).

Pojmem obdobná úroveň bezpečnosti se rozumí taková úroveň bezpečnosti, jakou poskytuje dvoufaktorová autentizace podle ustanovení § 19 odst. 3 VKB. Z praktického hlediska se jedná např. u unixových systémů o použití klíče při autentizaci na SSH server nebo použití X.509 certifikátů v případě Windows RDP (ať už v podobě smart karty nebo jako certifikát nainstalovaný na samotném zařízení). Zároveň však musí být dodrženy požadavky podle ustanovení § 26 VKB. Dále pak bezpečná správa a ověřování identit závisí na vnitřních politikách správce systému, které by měly vycházet z analýzy rizik.

Co se týče Vašeho dotazu, jakým způsobem je s těmito klíči nakládáno, je nutné uvést, že na tuto problematiku v současné době není ze strany NÚKIB zpracována žádná metodika ani doporučení. Obecně tak lze konstatovat, že na straně povinného subjektu je potřeba zpracovat analýzu rizik a na základě této analýzy rizik nastavit dobu platnosti certifikátu, možnost revokace a způsob, jakým bude systém s certifikátem nakládat.
K této problematice se dále vztahuje dokument „Minimální bezpečností standard“, který je dostupný zde: Národní úřad pro kybernetickou a informační bezpečnost – Minimální bezpečností standard (nukib.cz).

S pozdravem a přáním pěkného dne

Mgr. Pavel Král
Ředitel odboru právního

Obdrží:
 datovou schránkou

Vypraveno dne:
viz časový údaj na obálce datové zprávy