Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.J. NEPŘIDĚLENO • BRNO • 15. ZÁŘÍ 2023

VERZE DOKUMENTU: 1.3

POŽADAVKY NA ZPRÁVY Z PENETRAČNÍCH TESTŮ V SOUVISLOSTI SE ZÁPISEM CLOUD COMPUTINGU DO KATALOGU CLOUD COMPUTINGU

VYSOKÁ A KRITICKÁ BEZPEČNOSTNÍ ÚROVEŇ

1 Úvod

Vzhledem ke změně a zvýšení požadavků na dokládání zpráv z penetračních testů od 1. září 2021 Národní úřad pro kybernetickou a informační bezpečnost přistoupil k vydání této metodiky, která má pomoci poskytovatelům správně doložit požadované skutečnosti. Kromě upozornění na zvýšené požadavky na dokládání zpráv z penetračních testů, tato metodika obsahuje také doporučení, která vycházejí z dosavadních zkušeností z posuzování nabídek cloud computingu. Tyto poznatky a z nich vycházející doporučení jsou proto souhrnně komunikovány veřejnosti v přehledném seznamu na straně 3 níže, aby bylo dosaženo efektivnějšího procesu zápisu nabídek cloud computingu do katalogu cloud computingu.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno – Žabovřesky

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

2 Požadavky na zprávu z penetračního testu

Národní úřad pro kybernetickou a informační bezpečnost je podle § 6u odst. 1 ve spojení s § 6n písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění účinném od 1. září 2021, příslušný k vydávání závazného stanoviska k posouzení splnění některých požadavků kladených na cloud computing v řízení o zápis nabídky cloud computingu do katalogu cloud computingu (dále jen „katalog“), vedeného Digitální a informační agenturou.

Některé požadavky kladené na cloud computing využívaný orgánem veřejné správy rozvádí vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška“).

Jedním z požadavků stanovených na řádcích 10.2 a 10.3 přílohy č. 2 vyhlášky pro vysokou a kritickou bezpečnostní úroveň je i provádění penetračních testů nezávislým subjektem, které mají prověřit zabezpečení poskytované služby cloud computingu. Cílem tohoto požadavku je pravidelně ověřovat podle uznávaných standardů, že nabízená služba cloud computingu nemá bezpečnostní nedostatky, které by znamenaly případné bezpečnostní riziko pro orgány veřejné správy.

Splnění tohoto požadavku má poskytovatel služby cloud computingu resp. žadatel o zápis do katalogu cloud computingu doložit zprávou z provedení penetračního testu. Není však nezbytné poskytovat konkrétní nálezy ve zprávě z provedení penetračního testu, odhalovat případné zranitelnosti. Není ani záměrem poskytovatele služby cloud computingu jakkoliv trestat, pokud byly zranitelnosti ve zprávě identifikovány. Klíčové je, že poskytovatel bezpečnost svých služeb pravidelně ověřuje a zjištěné chyby v zabezpečení je schopen reflektovat.

Ze samotného znění požadavku uvedeného na řádcích 10.2 a 10.3 přílohy č. 2 vyhlášky a způsobu doložení jeho splnění vyplývá, že je třeba, aby předkládaná zpráva z penetračního testu splňovala následující požadavky:

- **NEZÁVISLOST** – Zpráva byla vyhotovena třetím subjektem, který je nezávislý na poskytovateli.

- **DATUM** – Stáří zprávy z penetračním testu je maximálně 24 měsíců od podání žádosti o zápis do katalogu.

- **OBSAH** – Z obsahu zprávy z penetračního testu je patrné, že penetrační test proběhl v souladu s předepsanou metodikou OSSTMM nebo standardy NIST 800-115, OWASP Top 10 a tudíž:
    - zpráva obsahuje jednotlivé oblasti testování stanovené v metodice/standardech a
    - ve zprávě je uveden explicitní odkaz na metodiku/standardy, podle kterých byl penetrační test proveden nebo

- je provedení dle dané metodiky/standardu deklarováno alespoň v doložených dokumentech (např. čestné prohlášení subjektu provádějícího penetrační test).

- **ROZSAH** – Zpráva z penetračního testu zahrnuje výčet služeb cloud computingu, které byly:
  - zahrnuty do rozsahu penetračního testu nebo
  - zahrnuje takový popis rozsahu penetračního testu, ze kterého bude jednoznačně patrné, že služba cloud computingu, kterou poskytovatel žádá zapsat do katalogu cloud computingu, náleží do daného rozsahu penetračního testu cloud computingu nebo
  - poskytovatel služby cloud computingu připojuje čestné prohlášení s výčtem služeb, které byly v rozsahu daného penetračního testu.

3 Poznatky z proběhlých posouzení

V souladu s dřívější právní úpravou účinnou do 31. srpna 2021, byly zachovány druhy požadovaných standardů i metodik, a tudíž i požadavek na obsah zprávy. Zpřísněn však byl požadavek na stáří zprávy, které mohou být nově maximálně 24 měsíců staré. Již samotné snížení akceptovatelného stáří zprávy ze tří let na dva roky může pro některé poskytovatele znamenat potřebu zhotovení nového penetračního testu. V takovém případě zároveň upozorňujeme, že je nově výslovně požadováno, aby byl penetrační test zajištěn třetím subjektem, který je nezávislý na poskytovateli cloud computingu.

Zkušenosti z dosavadního posuzování nabídek cloud computingu ukázaly, že jedním z nejčastějších nedostatků při dokládání požadovaných dokumentů je absence vazby prokazovaných skutečností ke konkrétním nabízeným službám. Tento nedostatek se dosud projevil zejména u požadavků na doložení certifikace, kdy poskytovatelé dokládali aktuální certifikáty nikoliv pro konkrétní služby, ale pro určité skupiny služeb, aniž by doložili, jaké konkrétní služby byly zahrnuty do certifikovaných skupin služeb. Obdobný požadavek je nyní obsažený také v řádcích 10.2 a 10.3 přílohy č. 2 vyhlášky, a proto je vhodné na tuto skutečnost upozornit, aby nemuselo k podobným nesrovnalostem docházet i nadále.

V případě, že zpráva z penetračního testu neobsahuje konkrétní výčet testovaných služeb, pak je nezbytné doložit alespoň formou čestného prohlášení, jaké služby byly do rozsahu penetračního testu zahrnuty. Pokud tedy není prokázáno, zda nabízená služba byla v rozsahu penetračního testu dle specifikovaných kritérií, pak nejsou splněny podmínky vyhlášky, a tedy nelze takovou službu do katalogu zapsat.

V případě, že z doložené zprávy o provedení penetračního testu vyplývá, že penetrační test byl proveden podle jiné metodiky/standardu, než požaduje vyhláška, pak musí poskytovatel doložit, že tato jiná metodika/standard je v souladu s vyhláškou vyžadovanou metodikou/standardem. Poskytovatel může tuto skutečnost prokázat čestným prohlášením subjektu provádějícího

penetrační test nebo doložením této jiné metodiky/standardu, ze které bude patrné, že aplikuje vyhláškou požadovanou metodiku/standard.

Rovněž je nutné upozornit na to, že z čestného prohlášení musí jednoznačně vyplývat, že se vztahuje na poskytovatelem doloženou zprávu z provedení penetračního testu.

4 Metodika a standardy pro provádění penetračních testů

Zde uvádíme odkazy na metodiku OSSTMM a standardy NIST 800-115 i OWASP Top 10:

- The Open Source Security Testing Methodology Manual (OSSTMM): https://www.isecom.org/OSSTMM.3.pdf; https://www.isecom.org/research.html#content5-9d
- Technical Guide to Information Security Testing and Assessment, NIST SP 800-115: https://csrc.nist.gov/publications/detail/sp/800-115/final
- OWASP Top ten web application security risks: https://owasp.org/www-project-top-ten/

5 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (dostupná na webových stránkách Národní úřad pro kybernetickou a informační bezpečnost - Doporučení k používání protokolu TLP ke sdílení chráněných informací (nukib.cz). Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	**Podmínky použití**
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
1. prosince 2021	1.0	OREG - ORECC	Vytvoření dokumentu
22. prosince 2022	1.1	OREG	Změna kontaktních údajů
19. června 2023	1.2	OREG - ORECC	Změna odkazů z MV na DIA a aktualizace podmínek využití informací (TLP)
15. září 2023	1.3	OREG - ORDIT	Doplnění poznatků z proběhlých posouzení