Metodika dokládání provádění skenů zranitelností a penetračního testování pro zápis do katalogu cloud computingu

TLP:CLEAR

18. prosince 2025

Verze 1.0

Národní úřad
pro kybernetickou
a informační bezpečnost

Obsah

1 Úvod

Účelem tohoto dokumentu je stanovit minimální požadavky pro dokládání provádění skenů zranitelností a penetračního testování v rámci požadavků řádků 8 příloh č. 1 až 4 (dále jen „požadavky“) vyhlášky č. 505/2025 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „vyhláška“).

Požadavkem stanoveným vyhláškou je provádění **skenů zranitelností a penetračních testů**, které mají prověřit zabezpečení poskytované služby cloud computingu. Cílem tohoto požadavku je zajistit, že poskytovatel cloud computingu (dále jen „poskytovatel“) bude pravidelně prověřovat, že nabízená služba cloud computingu nemá nedostatky, které by znamenaly bezpečnostní riziko pro orgány veřejné správy.

Splnění tohoto požadavku má poskytovatel doložit záznamem o provedení skenu zranitelností nebo zprávou z penetračního testu dle dané bezpečnostní úrovně. Není nezbytné ve zprávě poskytovat konkrétní nálezy a odhalovat případné zranitelnosti.

> Poskytovatel nebude jakkoli postihován za odhalené a popsané zranitelnosti. Klíčové je, že poskytovatel bezpečnost svých služeb pravidelně prověřuje a aktivně reaguje na zjištěné chyby v zabezpečení (opravou, vytvořením plánu oprav nebo analýzou rizik).

Splnění požadavků *FedRAMP Penetration Test Guidance* pro penetrační testy, případně *FedRAMP Vulnerability Scanning Requirements* pro skenování zranitelností (dále jen „FedRAMP“) je za dodržení podmínek určujících rozsah a požadavky na bezpečnostní úroveň bráno jako **splnění této metodiky**. Není rozhodné, zda bude požadavek vyhlášky prokázán podle této metodiky, nebo proběhne doložením dokumentu prokazujícím soulad s metodikou FedRAMP.

Pokud máte jakékoliv další otázky, napište nám na regulace@nukib.gov.cz.

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 Určení rozsahu

Popis rozsahu pro jednotlivé bezpečnostní úrovně nabízeného cloud computingu

Nízká

Minimálně provést sken zranitelností bez autentizace (je možné doložit i penetračním testem).

Střední

Sken zranitelností s autentizací tam, kde je to možné (je možné doložit i penetračním testem s autentizací).

Vysoká

Sken zranitelností s autentizací tam, kde je to možné.

Penetrační test s autentizací na všechny odlišné úrovně uživatelských oprávnění (s plnou autentizací i autorizací) tam, kde je to možné.

Kritická

Sken zranitelností s autentizací tam, kde je to možné.

Penetrační test s autentizací na všechny odlišné úrovně uživatelských oprávnění (s plnou autentizací i autorizací) tam, kde je to možné.

Ve finálním rozsahu penetračního testu či skenu zranitelností musí být zahrnuty a posouzeny všechny komponenty, související služby a přístupové cesty (interní/externí) v rámci definované testovací hranice systému poskytovatele a toto testování je nutné provádět buď na všech aktivech nebo na jejich smysluplném vzorku. Pravidla a omezení pro zapojení do testování[1] musí umožňovat a definovat vhodné testovací metody a techniky spojené se zneužitím příslušných zařízení nebo služeb tam, kde je to možné.

V případě, že je poskytování cloud computingu závislé na jiném cloud computingu dle § 6t odst. 7 písm. e) zákona o informačních systémech veřejné správy, musí poskytovatel podpůrného cloud computingu splňovat stejnou nebo vyšší bezpečnostní úroveň a musí dojít k jeho otestování. Pro splnění požadavku musí poskytovatel dodat zprávu z provedení penetračního testu služby podpůrného cloud computingu. Lze uznat i penetrační test provedený z pokynu poskytovatele podpůrného cloud computingu, který bude splňovat požadavky této metodiky.

[1] Rules of Engagement (ROE)

3 Požadavky na skenování zranitelností

Skenu musí být podrobena **všechna aktiva, která jsou dostupná uživateli** (dle dané úrovně). Sken zranitelností musí ověřit zranitelnosti operačních systémů, webového rozhraní, síťových služeb. Nálezy objevené při skenování zranitelností musí být přiřazené k označení zranitelnosti CVE z National Vulnerability Database (NVD), pokud je to možné.

K tomu musí být přidáno také označení Common Vulnerability Scoring System (dále jen „CVSS“), aby bylo snazší určit vážnost nálezu. Pokud není CVSS přiřazeno, lze použít interní hodnocení nástroje pro skenování zranitelností, avšak je nutné doložit kritéria hodnocení.

Pro každé skenování musí být využit takový nástroj, který bude mít k dispozici aktualizovaný seznam zranitelností k datu testování.

Pro úroveň zabezpečení střední a vyšší musí být skenovací nástroj schopný ověřit zranitelnosti služeb s autentizovaným přístupem tam, kde je to možné.

Skenovací nástroj musím mít povolené všechny nedestruktivní detekce na všech síťových portech nebo na všech otevřených portech.

3.1 Záznam ze skenu zranitelností

Náležitosti záznamu o provedení skenu zranitelností:

- **DATUM**
    - Požadovány jsou minimálně **3 záznamy o provedení skenu zranitelnosti**, kdy nejstarší záznam byl pořízen maximálně 12 měsíců a nejnovější byl proveden maximálně 3 měsíce před podáním žádosti o zápis služby cloud. Mezi jednotlivými skeny zranitelností musí být časový odstup alespoň jeden měsíc, aby bylo patrné, že se skeny zranitelností provádějí pravidelně.
- **OBSAH**
    - Z obsahu záznamu je patrné, že sken proběhl v souladu s touto metodikou nebo dle pokynu FedRAMP, což bude i explicitně uvedeno v záznamu nebo v jiném předkládaném dokumentu nebo v rámci čestného prohlášení.
    - Z obsahu záznamu musí být patrná zlepšující se tendence zabezpečení nebo způsob vypořádání se se zranitelnostmi ze záznamu předchozího skenu zranitelností (opravou, vytvořením plánu oprav, analýzou rizik, false positive).
- **ROZSAH**
    - Výčet služeb cloud computingu, které byly zahrnuty do rozsahu skenu a souhrn dohodnuté autentizace a autorizace (v případě, že sken probíhá pouze na části aktiv, např. formou vzorkování, je nutné uvést jaká aktiva byla v rozsahu testů a která nebyla), nebo

- takový popis rozsahu skenu, ze kterého bude jednoznačně patrné, že služba cloud computingu, kterou poskytovatel žádá zapsat do katalogu náleží do daného rozsahu skenu cloud computingu, nebo
- připojenou smluvní dokumentaci uzavřenou mezi poskytovatelem a subjektem provádějící skeny zranitelností obsahující výčet služeb cloud computingu, které byly určeny do rozsahu skenů zranitelností, nebo
- v případě, že je testován soubor služeb, který nese komerční/společný název produktu je nutné doložit popis produktu a separátní čestné prohlášení s výčtem zahrnutých služeb.

4 Požadavky pro penetrační testování

Penetračnímu testu musí být, pokud je to možné, podrobeny všechny funkcionality, které jsou dostupné autentizovanému uživateli. Zároveň musí být test proveden z pohledu všech autorizovaných uživatelských rolí. Otestován musí být i systém správy poskytovatele sloužící k administraci poskytované služby pracovníkům poskytovatele a dalším oprávněným osobám.

4.1 Povinné vektory útoku

Techniky testování jednotlivých systémů se mohou lišit v závislosti na nabídce služeb (IaaS, PaaS, SaaS a hybridní). Vzhledem ke společným rysům systému jsou následující techniky povinnými vektory útoku pro všechny služby určené k zápisu do katalogu cloud computingu (dále jen „katalog“). Jakékoli odchylky od povinných vektorů útoku musí být odůvodněné v předkládané zprávě z testování (např. služba nezahrnuje mobilní aplikaci).

- Z externího pohledu vůči systému správy poskytovatele
- Z externího pohledu vůči cílovému systému poskytovatele
- Z tenanta do systému správy poskytovatele
- Z tenanta na tenanta
- Z mobilní aplikace do cílového systému
- Z aplikace na straně klienta a/nebo agenta do cílového systému

4.2 Obecné kroky/techniky penetračního testování

V závislosti na architektuře autorizované služby (IaaS, PaaS, SaaS, hybridní) je možné uplatnit velké množství technik/kroků penetračního testování. Ačkoli se nejedná o úplný seznam, cílem penetračního testování by mělo být dosažení otestování smysluplných bodů podle znalostní báze MITRE ATT&CK[2]. Testeři musí využít nalezené zranitelnosti nebo ověřit možnost zneužití, pokud předchozí není možné. Penetrační test by se neměl striktně omezovat na techniky automatického skenování, ale měl by zahrnovat i manuální techniky. Pro jednodušší kontrolu je vhodné do zprávy pro poskytovatele uvést konkrétní popisy průběhu jednotlivých útoků a technický popis verifikace

[2] https://attack.mitre.org/matrices/enterprise/cloud/

a validace zranitelností identifikovaných během testování, aby bylo zajištěno, že jednotlivé útoky/kroky byly řádně splněny.

4.3 Správné určení metodiky

V závislosti na zapisovaných službách je nutné vhodně zvolit metodiku pro penetrační test. Zjednodušeně je pro webové služby nutné zvolit *OWASP ASVS v1*, případně *OWASP Top 10*. Pro ostatní služby zvolit *NIST 800-115* nebo *OSSTMM*. V případě kombinovaných služeb je logicky nutné být v souladu *OWASP ASVS v1* (případně *OWASP Top 10*) a zároveň *NIST 800-115* nebo *OSSTMM*.

Kromě klasických webových služeb je možné *OWASP ASVS v1*, případně *OWASP Top 10* částečně využívat i u služeb jako jsou různé formy API rozhraní, desktopové aplikace, mobilní aplikace komunikující s backendem. Pro testování validace vstupů, autentizace, správy chyb nebo šifrování a bezpečné komunikace.

Testování podle *OWASP Top 10* představuje možné riziko provedení v různé kvalitě. Proto je nutné, aby doložený test obsahoval i popis kroků, které byly prováděny v rámci testování dle *OWASP Top 10*. Za nedostatečné se považuje uvedení pouze aktuálního výčtu *OWASP Top 10*.

4.4 Zpráva z penetračního testování

Náležitosti zprávy z penetračního testu:

- **NEZÁVISLOST**
    - Zpráva byla vyhotovena subjektem nezávislým na poskytovateli.
- **DATUM**
    - Stáří zprávy z penetračním testu je maximálně 24 měsíců k datu podání žádosti o zápis do katalogu.
- **OBSAH**
    - Z obsahu zprávy je patrné, že penetrační test proběhl v souladu s Metodikou nebo dle pokynu FedRAMP, což bude i explicitně uvedeno ve zprávě nebo v jiném předkládaném dokumentu nebo v rámci čestného prohlášení vyhotoveného subjektem provádějícím penetrační test.
    - V případě, že penetrační test neproběhl v souladu s pokynem FedRAMP, v závislosti na rozsahu bude ve zprávě uveden explicitní odkaz na metodiku/standardy, s nimiž je penetrační test v souladu (NIST 800-115, OSSTMM) nebo pro webové služby v souladu se standardem *OWASP ASVS Level 1*, či *OWASP Top 10* u bezpečnostní úrovně “Vysoká” a *OWASP ASVS Level 1* u bezpečnostní úrovně “Kritická” nebo je provedení dle dané metodiky/standardu deklarováno alespoň v doložených dokumentech (např. čestné prohlášení subjektu provádějícího penetrační test).
- **ROZSAH**

- Výčet služeb cloud computingu, které byly zahrnuty do rozsahu penetračního testu a souhrn dohodnuté autentizace a autorizace (v případě, že testování probíhá pouze na části aktiv, např. formou vzorkování, je nutné uvést jaká aktiva byla v rozsahu testů a která nebyla), nebo
- takový popis rozsahu penetračního testu, ze kterého bude jednoznačně patrné, že služba cloud computingu, kterou poskytovatel žádá zapsat do katalogu, náleží do daného rozsahu penetračního testu cloud computingu, nebo
- připojenou smluvní dokumentaci mezi poskytovatelem a subjektem provádějící penetrační testování obsahující výčet služeb cloud computingu, které byly dohodnuty do rozsahu penetračního testu, nebo
- v případě, že je testován soubor služeb, který nese komerční/společný název produktu je nutné doložit popis produktu a separátní čestné prohlášení s výčtem zahrnutých služeb v době provádění penetračního testování, nebo
- čestné prohlášení subjektu provádějící penetrační testování obsahující výčet služeb cloud computingu, které byly zahrnuty do rozsahu penetračního testu.

- **VEKTORY**
  - Seznam testovaných vektorů, případně odůvodnění jejich neotestování.

5 Slovník pojmů

Poskytovatel – pojem poskytovatel cloud computingu vychází ze zákona o informačních systémech veřejné správy. Dle zákona o informačních systémech veřejné správy jím může být jak prodejce, tak i ten, kdo službu fakticky poskytuje. V kontextu vyhlášky jím bude zejména subjekt odpovědný za nasazení, údržbu a zabezpečení systému pro zápis do katalogu.

Systém správy poskytovatele – backendové aplikace, systémy, služby, hardware, infrastruktura nebo vzdálená správa, která usnadňuje administrativní přístup ke cloudové službě. Systém správy je podpůrná infrastruktura přístupná pouze pracovníkům poskytovatele a oprávněným osobám.

Cílový systém poskytovatele – služba zapisovaná do katalogu

Tenant – zákaznická instance cloudové služby

Závěrečná zpráva z penetračního testu – zpráva kterou předložila nezávislá autorita provádějící penetrační test

Předkládaná zpráva z testování pro zápis do katalogu – poskytovatel pro zápis může dokládat přímo závěrečnou zprávu z penetračního nebo upravenou zprávu, která splňuje požadavky bodu 4.4. této metodiky

Testování formou vzorkování – testování může probíhat formou vzorkování, ale všechny funkcionality by měly být otestovány, aby se zajistila celková kvalita systému. Tedy příkladem formy vzorkování může být situace, kdy stejná funkcionalita je nasazena v rámci několika zařízení/kontejnerů, ale otestována bude pouze jedna instance. Zároveň je pochopitelné, že každá zákaznická instance může vyžadovat jinou množinu funkcí a není možné otestovat všechny kombinace, ale měly by být testovány všechny funkce.

6 Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí 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**
18. prosince 2025	1.0	CERT/OREG	Vytvoření dokumentu