

TECHNINĖ SPECIFIKACIJA

Lietuvos Respublikos užsienio reikalų ministerija (toliau – Perkančioji organizacija), siekdama užtikrinti Lietuvos Respublikos diplomatinės tarnybos institucijoms interesantų pateikiamos informacijos saugumą, diplomatinės tarnybos institucijų teikiamų paslaugų ir veiklos tęstinumą, perka Perkančiosios organizacijos **elektroninių ryšių tinklo infrastruktūros (toliau – tinklas) atsparumo raudonos komandos (angl. Red Team) išilaužimams patikrinimo (toliau – Patikrinimas) paslaugas**. Viešojo pirkimo–pardavimo sutarties galiojimo laikotarpiu perkančioji organizacija įsipareigoja įsigyti ne mažiau kaip 540 val. ir ne daugiau kaip 2700 val. Patikrinimo paslaugų.

I. PIRKIMO OBJEKTAS, JO KIEKIAI (APIMTYS)

1. Pirkimo objektą sudarančios Patikrinimo paslaugos (toliau – Paslaugos) ir jų apimtis (kiekis):

Paslaugos		Mato vnt.	Preliminarus 12 mėn. kiekis
1.1.	Tikslinių atakų simuliacijos paslaugos iš išorės tinklo:	val.	40
1.1.1.	Tikslinės atakos iš viešojo interneto	val.	24
1.1.2.	Bevielio tinklo taško dvynio (angl. rogue ap) atakos scenarijus pasirinktoje lokacijoje	val.	16
1.2.	Tikslinės atakos iš pasirinkto vidinio tinklo segmento	val.	500
Iš viso:		val.	540

II. BENDRIEJI REIKALAVIMAI PASLAUGOMS IR PROJEKTO (PASLAUGŲ TEIKIMO) VALDYMUI

2. Paslaugos Sutarties galiojimo laikotarpiu bus užsakomos, jų rezultatai bus priimami ir už jas bus atsiskaitoma atskirai. Sudaromoje Sutartyje nustatomas Paslaugų teikimo terminas negali būti ilgesnis kaip 60 (šešiasdešimt) mėnesių nuo Sutarties įsigaliojimo dienos.
3. Konkretaus užsakymo Paslaugos turi būti įvykdytos ne vėliau kaip per 2 (du) mėnesius nuo šio užsakymo suderinimo (patvirtinimo) dienos. Šiame punkte nurodytas Paslaugų teikimo terminas gali būti pratęstas rašytiniu Perkančiosios organizacijos ir Paslaugų teikėjo susitarimu, kai Paslaugų teikėjas Paslaugas vėluoja suteikti dėl trečiųjų asmenų kaltės ar Perkančiajai organizacijai vėluojant vykdyti sutartinius įsipareigojimus. Paslaugų teikimo terminas pratęsiamas tiek laiko, kiek trečiųjų asmenų ar Perkančiosios organizacijos veiksmai įtakojo vėlavimą. Nesutarimo atveju sprendimo teisė priklauso Perkančiajai organizacijai.
4. Paslaugų teikėjas teikdamas Paslaugas privalo:

- 4.1. parengti ir su Perkančiąja organizacija suderinti Paslaugų teikimo (kiekvieno užsakymo) planą, grafiką, prieš kiekvieną šios techninės specifikacijos 13 punkte nustatytą veiksmą, Perkančiosios organizacijos įgaliotiems atstovams pateikti detalią informaciją apie numatomus veiksmus;
- 4.2. suteikti Paslaugų teikimo plane ir grafike nustatytais sąlygomis ir terminais Paslaugas, atitinkančias šios techninės specifikacijos reikalavimus;
- 4.3. suderinti su Perkančiąja organizacija Paslaugų rezultatų dokumentaciją, jų formą ir turinį;
- 4.4. perduoti Perkančiajai organizacijai Paslaugų rezultatą ir suderintą dokumentaciją.
5. Patikrinimas turi būti atliktas pagal viešai žinomą ir pripažintą atvirą ar komercinę Raudonos komandos išsilaužimų įvertinimo metodiką (angl. [*Red Teaming Methodology*](#)). **Pasiūlyme būtina nurodyti metodikos (-ų) pavadinimą (-us) bei pateikti aktyvią (-as) interneto svetainės (-ių) nuorodą (-as) į jos (jų) aprašymą arba patį metodikos (-ų) aprašą.**
6. Paslaugų teikėjas atsakingas už projekto (Paslaugų teikimo) administravimą, projekto veiklų organizavimą bei informacijos pateikimo ar sąlygų jai gauti užtikrinimo klausimus. Taip pat Paslaugų teikėjas atsakingas už projekto komunikaciją, projekto rizikų valdymą, dokumentų formą ir turinį, suderinimą ir Paslaugų perdavimą.
7. Sėkmingo įsiskverbimo metu bet kokie veiksmai turi būti detalieai dokumentuoti bei prieš tai suderinti su Perkančiosios organizacijos atsakingais darbuotojais. Įsiskverbimo metu pasiekta Perkančiosios organizacijos vidinė informacija negali būti kopijuojama jokiais formomis ir jokiais metodais į išorinius tinklus ar laikmenas.
8. Paslaugų teikėjas, atlikęs Paslaugas (kiekvieną užsakytą jų dalį), turi pateikti suteiktų paslaugų ataskaitą (-as).
9. Projekto dokumentacija turi būti rengiama ir derinama vadovaujantis šiais reikalavimais:
 - 9.1. Paslaugų teikėjas privalo suderinti visų pateikiamų projekto rezultatų (dokumentų) formą ir turinį prieš juos pateikdamas Perkančiajai organizacijai;
 - 9.2. esant reikalui, Paslaugų teikėjas turi atlikti papildomus projekto rezultatų (dokumentų) pakeitimus iki jų pateikimo Perkančiajai organizacijai;
 - 9.3. pateiktų dokumentų projektus Perkančioji organizacija įvertina per 15 (penkiolika) darbo dienų nuo pateikimo dienos.
10. Visa Paslaugų dokumentacija turi būti parengta bendrine lietuvių kalba ir pateikiama atviru standartiniu elektroniniu formatu (PDF, OpenXML arba lygiaverčiu).
11. Atsparumo raudonosios komandos patikrinimo paslaugos baigiamos, kai Paslaugų teikėjas saugos vertinimo ataskaitą pateikia ir ją pristato Perkančiosios organizacijos atstovams.
12. Tiekėjas turi būti įdiegęs informacijos saugumo vadybos sistemą, atitinkančią ISO/IEC 27001:2022 (toliau – ISO 27001) arba lygiaverčio standarto reikalavimus. **Kartu su pasiūlymu Paslaugu teikėjas privalo pateikti akredituotos sertifikavimo įstaigos išduotą sertifikatą ar kitus lygiaverčius įrodymus, patvirtinantį, kad Paslaugų**

tiekėjas yra įdiegęs informacijos saugumo vadybos sistemą, atitinkančią ISO 27001 arba lygiaverčio standarto reikalavimus. Lygiaverčiu standartu laikomas toks standartas, kurio reikalavimai visiškai atitinka arba viršija ISO 27001 standarto reikalavimus. Tokio standarto reikalavimų atitikimą ISO 27001 standarto reikalavimams turi patvirtinti akredituota sertifikavimo įstaiga.

III. RAUDONOSIOS KOMANDOS ATAKŲ SAUGUMO VERTINIMAS

13. Tikslinių atakų bei raudonosios komandos įsilaužimo testavimo simuliacija susideda iš šių dalių:
 - 13.1. Žvalgyba (angl. *Reconnaissance*) – pirmasis testo žingsnis apima žvalgybos žingsnį, kurio tikslas yra surinkti kiek įmanoma daugiau informacijos apie būsimą testo objektą. Žingsnio metu surenkama informacija apie atakos objektą, susijusias technologijas, aplinką, įrankius, atsakingus asmenis ir pan.
 - 13.2. Įsilaužimo priemonių parengimas (angl. *Weaponisation*) – surinkta informacija apie infrastruktūrą, technologijas ir naudojamas saugumo priemones yra analizuojama atakos scenarijui suformuoti konkrečiam taikiniui.
 - 13.3. Vykdymas (angl. *Delivery*) – kritinis tikslinės atakos simuliacijos paslaugos žingsnis, kurio metu atliekama reali atakos simuliacija. Raudonoji komanda atlieka veiksmus prieš numatytus taikinius, tam, kad pasiektų atakai suformuotus tikslus.
 - 13.4. Pažeidžiamumų išnaudojimas (angl. *Exploitation*) – pažeidžiamumų išnaudojimo žingsnyje, raudonosios komandos tikslas yra „įsilaužti“, t. y. sukompromituoti serverių, taikomosios programinės įrangos, tinklų saugumą išnaudojant egzistuojančius pažeidžiamumus.
 - 13.5. Kontrolė ir nematomas judėjimas (angl. *Control and movement*) – sėkmingai sukompromitavus kažkurio iš tinklo ar taikomosios programinės įrangos komponentų saugumą, raudonoji komanda atlieka judėjimą (angl. *lateral movement*) iš vieno pažeidžiamo Tinklo resurso į kitus aukštesnės vertės resursus.
 - 13.6. Veiksmai prieš taikinius (angl. *Actions on target*) – šis žingsnis apima tolimesnės prieigos prie testo metu sukompromituotų Tinklų resursų informacijos ir duomenų. Šio žingsnio metu raudonoji komanda siekia užbaigti testą ir pasiekti numatytus tikslus planavimo fazėje.
14. Paslaugų teikėjas atlikdamas Paslaugas turi vadovautis MITRE ATT&CK standarto gairėmis – simuliacijai atlikti naudoja 14 įsilaužimo taktikų bei atsižvelgiant į konkretaus testo situaciją bei eigą pritaiko kombinaciją iš 202 apibrėžtų įsilaužimo technikų.
15. Paslaugos metu turi būti atlikti bent jau šie scenarijai:
 - 15.1. Informacijos surinkimas apie Perkančiąją organizaciją, darbuotojus, saugos politikas ir kt. pasinaudojant OSINT programiniais įrankiais ir viešai prieinama informacija;
 - 15.2. Galimai nutekintų Perkančiosios organizacijos kredencialų paieška viešai prieinamose duomenų bazėse ir „tamsiajame internete“ (angl. *Dark Web*);

- 15.3. Slaptažodžių purškimo (angl. *Password Spraying*), slaptažodžių kimšimo (angl. *Password Stuffing*) atakų testavimas;
- 15.4. Žmogiškųjų pažeidžiamumų paieška ir išnaudojimas (angl. *Social Engineering*);
- 15.5. Horizontalus privilegijų eskalavimo galimybės testavimas;
- 15.6. Vertikalus privilegijų eskalavimo galimybės testavimas;
- 15.7. Įsilaužimo testavimas laisvai pasirinktais, bet suderintais su Perkančiąja organizacija vektoriais ir atakų tipais, užtikrinant nematomą judėjimą ir slaptumą tinkle bei saugos sprendimų apėjimą;
- 15.8. Bevielių tinklų-dvynių (angl. *rouge access point*) įrengimą Perkančiosios organizacijos lokacijose;
- 15.9. Ypatingas dėmesys turi būti skirtas atakų, susijusių su Windows Domenu bei Active Directory saugumo spragomis patikrinimui, apimant, bet neapsiribojant:
 - 15.9.1. Žvalgyba: nustatoma domeno kontrolių bei kitų svarbių Active directory komponentų (pvz., KDC, DNS ir kt.) lokacija atliekant standartinių vardų paieškos, tinklo skanavimo ar siunčiant LDAP užklausas. Domeno vardo suradimui naudojamos LDAP užklausos, MS-RPC interfeisai ir multicast bei broadcast užklausų analizė.
 - 15.9.2. Kontrolė ir Nematomas Judėjimas atliekami šie atakų scenarijai:
 - 15.9.2.1. NTLM bei Kerberos protokolų atakos (DCOM, NTLM MITM and relay, NTLM capture, ASREP Roasting, Timeroasting, Kerberoasting, Golden-Ticket, OverPass-the-Hash, Pass-the-Hash, Unconstrained Delegation, Constrained Delegation ir kt.);
 - 15.9.2.2. Tikrinamas Domenu kontrolių ir susijusių paslaugų atsparumas tipinėms atakoms (ZeroLogon, ProxyShell, PrintNightmare ir pan.);
 - 15.9.2.3. Tikrinamos atakos bei pažeidžiamumai susiję su Microsoft Endpoint Configuration Manager (MECM) bei WSUS (SCCM Site Takeover, PXETHief, Retrieve credentials via PXE boot media, Request a policy containing credentials, Extract currently deployed credentials stored as DPAPI blobs, Extract legacy credentials stored as DPAPI blobs, Extract the SC_UserAccount table from the site database, SCCM Persistence, SCCM Relay);
 - 15.9.3. Veiksmai prieš taikinius (angl. *Actions on target*) atliekami šie atakų scenarijai (angl. *peristence*):
 - 15.9.3.1. DC Shadow, SID History, Skeleton key, GoldenGMSA, AdminSDHolder, tikrinami Certificate Services (AD-CS) pažeidžiamumai bei kt.
- 15.10. Simuliacijos metu atliekami veiksmai apimantys naudotojų prisijungimo duomenų saugumo vertinimą:
 - 15.10.1. tikrinama, ar visų tipų (įskaitant nutolusius naudotojus) nurodytų Perkančiosios organizacijos naudotojai negali plėsti savo teisių Organizacijos tinkle, atlikti veiksmų ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu;
 - 15.10.2. pažeidžiamumų paieška išorinio bei vidinio tinklo segmentuose, taikomojoje programinėje įrangoje bei susijusiose paslaugose;

- 15.10.3. vartotojų prisijungimo duomenų rinkimui naudojamos technikos apima Cached Credentials, Local Security Authority (LSA) Secrets, NTDS from Domain Controller, Group Policy Preference (GPP), LAPS, Shadow Credentials ir pan.
16. Turi būti pateiktos ekspertinės saugumo konsultantų išvados ir rekomendacijos;
 17. Turi būti parengta apibendrinta atsparumo Raudonosios komandos atsparumo įsilaužimams ataskaita, nesigilinant į konkrečius pažeidžiamumus ar technines detales. Šioje ataskaitoje turi atsispindėti statistika, tendencijos, bendra saugumo būklė, pavojingiausi pažeidžiamumai, saugumo trūkumai ir prioretizuotos saugumo gerinimo kryptys.
 18. Turi būti parengtos detalios visų patikrinimo sudedamųjų dalių ataskaitos detaliai nurodant tikrinimo tikslus, tikrintus objektus, tikrinimo eigą, tikrinimo rezultatus, aptiktas saugumo spragas jas klasifikuojant pagal svarbą, rekomendacijas dėl spragų pašalinimo bei kitą naudingą informaciją.
 19. Ataskaitose turi būti pateikiami visi galimi pažeidžiamumų bei atakų išnaudojimo scenarijai – detaliai aprašyta veiksmų seka, kaip išnaudoti vieną ar kitą saugumo trūkumą.
 20. Ataskaitos turi leisti iš karto identifikuoti labiausiai pažeidžiamas Tinklo vietas ir didžiausius trūkumus, o atlikus pakartotinius pažeidžiamumų įvertinimus ateityje, leisti palyginti gautus rezultatus ir įvertinti pokyčius.
-