Naša št.: 283-44/4-2024
Datum: 12. 11. 2024

TEHNIČNE SPECIFIKACIJE IN ZAHTEVE NAROČNIKA

Storitve kibernetskega inženiringa operativnih sistemov, št. 283-44

© 2024 Slovenia Control. All rights reserved. No part of this document may be reproduced, transmitted, stored in a retrieval system or translated into any language, in any form, or by any means, without the prior written consent of Slovenia Control.

KAZALO

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA.....3
2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE.....3
2.1 Splošno.....3
2.2 Storitve kibernetskega inženiringa.....3
2.2.1 Obseg storitev in režim izvajanja.....3
2.2.2 Dokumentacija.....4
2.3 Usposobljenost ponudnika.....4
3 Varnostne in druge zahteve.....5
3.1 Zagotavljanje skladnosti z Izvedbeno Uredbo Komisije EU/2017/373.....5

1 PREDMET IN TEHNIČNE ZAHTEVE JAVNEGA NAROČILA

Predmet tega naročila so Storitve kibernetskega inženiringa za obdobje dveh (2) let.

Izbrani ponudnik bo moral za naročnika zagotavljati storitve opisane v nadaljevanju v dogovorjenem obsegu in roku.

2 TEHNIČNE SPECIFIKACIJE IN ZAHTEVE

2.1 Splošno

Naročnik na področju zagotavljanja kibernetske varnosti načrtuje operativno delovanje s sodelovanjem strokovnjakov ponudnika v ekipi za kibernetsko varnost naročnika. Naloge ponudnika so opisane v nadaljevanju.

2.2 Storitve kibernetskega inženiringa

Storitve kibernetskega inženiringa se izvajajo v sodelovanju z osebjem naročnika in vključujejo predvsem:

a)
- redne preglede, analizo delovanja sistemov z ugotovitvami/poročili in predlogi izboljšav;
- reševanje dogodkov in incidentov;
- izvajanje storitev in sprememb nastavitev rešitev za kibernetsko varnost na zahtevo naročnika;
- optimizacijo, svetovanje in uvedba novih funkcionalnosti;
- spremljanje delovanja in posredovanje na daljavo;
- telefonsko pomoč pri opravilih na vzdrževanem sistemu;
- koordinacijo del s principalom pri morebitnem odpravljanju napak na kibernetski opremi.

b)
- kibernetsko obveščevalno dejavnost (Cyber Threat Intelligence), zbiranje, analizo in diseminacijo kibernetskih groženj, s pomočjo uporabe zasebnih virov, honeypotov in na podlagi analiz, posledično priprava poročil, predlogov izboljšave nivoja kibernetske varnosti, priprava predloga sprememb nastavitev opreme in / ali implementacija procesov ali opreme vezane na grožnje. Ponudnik vzpostavi vsaj 6 različnih tipov »honeypotov« in jih prilagodi, da lahko odražajo naročnikovo okolje (različne segmente).

Za uspešno opravljanje zgoraj naštetih storitev bo moral ponudnik zagotoviti strokovnjake s specialističnimi znanji na področju oziroma orodjih:
- Požarne pregrade Palo Alto Networks,
- Požarne pregrade Fortinet,
- Darktrace,
- Microsoft Defender for IoT – Cyber X,
- EDR/XDR rešitve, MS Defender P2 in Palo Alto Cortex Pro
- Omrežni agregator Garland Technology.

Za storitve kibernetsko obveščevalne dejavnosti mora ponudnik zagotoviti lastno rešitev in njeno implementacijo/integracijo v okolje naročnika oziroma s predstavljanem okolja naročnika.

2.2.1 Obseg storitev in režim izvajanja

Izbrani ponudnik bo moral zagotavljati do 35 ur mesečno oz. 420 ur letno storitev kibernetskega inženiringa v rednem delovnem času naročnika (8-16) z odzivnim časom naslednji delovni dan oz. NBD.

Ponudnik bo storitve kibernetskega inženiringa opravljal v dogovoru in po naročilu naročnika.

Storitve kibernetsko obveščevalne dejavnosti ponudnik zagotavlja z lastno rešitvijo in njeno implementacijo/integracijo v okolje naročnika oziroma s predstavljanem okolja naročnika. Zagotoviti mora vsaj 6 različnih tipov honeypotov. Zagotavljanje in uporaba rešitve se obračunava mesečno.

Storitve ponudnik opravlja na lokaciji naročnika oz. po dogovoru z naročnikom na daljavo.

2.2.2 Dokumentacija

Izbrani ponudnik bo ob izvajanju sprememb na sistemih naročnika le-te ustrezno dokumentiral v naročnikovo dokumentacijo in jo sproti tudi dopolnjeval. V primeru implementacije novih rešitev ali večjih sprememb mora izbrani ponudnik pripraviti ustrezno novo dokumentacijo za izveden projekt ali poseg.

Za izvajanje kibernetske obveščevalne dejavnosti (Cyber Threat Intelligence) bo izvajalec pripravljal mesečna poročila. V primeru zaznave dejavnosti, ki bi lahko neposredno vplivala na odpornost naročnikovega okolja ali imela bistven vpliv na CIA triado, bo izvajalec naročnika obvestil takoj ob zaznavi oziroma.

2.3 Usposobljenost ponudnika

Ponudnik mora naročniku zagotoviti in izkazati, da ima, za namene opravljanja storitev kibernetskega inženiringa, usposobljeno osebje, s spodaj podanimi specialističnimi znanji in njihovo ustrezno število..

Ponudnik mora razpolagati z zadostnim številom strokovno usposobljenih kadrov, in sicer z najmanj dvema (2) usposobljenima inženirjema z naslednjimi kompetencami, ki se jih izkaže z veljavnimi certifikati in/ali licencami navedenimi v spodnji tabeli:

Orodje	**Licenca (ponudnik priloži kopijo licence)**	**Število tehničnih strokovnjakov**
Požarne pregrade Palo Alto Networks	Palo Alto Networks Certified Network Security Engineer	2
Požarne pregrade Fortinet	Fortinet Certified Professional Network Security	1
	Fortinet Certified Solution Specialist Network Security	1
Darktrace,	Certified Darktrace Cyber Engineer	2
Microsoft Defender for IoT – Cyber X,	Technical Certificate	2
Omrežni agregator Garland Technology	Certificate for Garland Technology Technical Training	2

Kader, ki ga bo ponudnik imenoval za izvajanje tega javnega naročila, mora imeti najmanj 3 leta delovnih izkušenj s področja kibernetskega inženiringa, kar ponudnik izkaže z navedbo referenc in izkušenj posameznega kadra.

Ponudnik lahko z isto osebo izkazuje zahteve iz zgornje tabele. Kar pomeni, če ima ponudnik na voljo dva kadra, od katerih ima vsak več licenc/certifikatov (hkrati), lahko v ponudbi navede le ta dva kadra. Vsi certifikati morajo biti veljavni na dan oddaje ponudbe. Veljavnost licenc/certifikatov se izkazuje z izpisom trajanje veljavnosti. Izbrani ponudnik mora ves čas trajanja predmetnega naročila razpolagati z ustrezno usposobljenimi strokovnjaki z veljavnimi licencami in / ali certifikati.

3 Varnostne in druge zahteve

Objekti, v katerih deluje naročnik, so namenjeni izvajanju storitev navigacijskih služb zračnega prometa in spadajo med objekte posebnega pomena, za katere veljajo posebni varnostni režimi na podlagi predpisov s področja varovanja civilnega letalstva. Izvajalec, ki bo izpolnjeval pogodbene obveznosti, je dolžen slediti naročnikovim navodilom, glede vstopa ter gibanja po naročnikovih prostorih oz. območjih.

Izvajalec je seznanjen s tem, da so lokacije kjer deluje naročnik na območjih, za katere velja poseben režim varovanja. Zaradi tega bo izvajalec, zagotovil, naslednje podatke: registrske številke vseh vozil, s katerimi se bodo opravile dostave in osebne podatke vseh delavcev ter ostalih prisotnih, ki bodo opravili dostavo in/ali testiranje.

3.1 Zagotavljanje skladnosti z Izvedbeno Uredbo Komisije EU/2017/373

Naročnik je na podlagi veljavne zakonodaje:

- Izvedbena uredba Komisije (EU) 2017/373 z dne 1. 3. 2017 o skupnih zahtevah za izvajalce storitev upravljanja zračnega prometa/izvajanja navigacijskih služb zračnega prometa in drugih funkcij omrežja za upravljanje zračnega prometa ter njihov nadzor, razveljavitvi Uredbe (ES) št. 482/2008, izvedbenih uredb (EU) št. 1034/2011, (EU) št. 1035/2011 in (EU) 2016/1377 ter spremembi Uredbe (EU) št. 677/2011 (UL L št. 62, z dne 8. 3. 2017, str. 1), na zadnje spremenjene z Izvedbeno uredbo Komisije (EU) 2021/1338 z dne 11. avgusta 2021 o spremembi Izvedbene uredbe (EU) 2017/373 v zvezi z zahtevami glede poročanja in kanalih za poročanje med organizacijami ter zahtevami za meteorološke službe (UL L št. 289, z dne 12. 8. 2021, str. 12) (v nadaljevanju: Izvedbena uredba Komisije 2017/373/EU);
- Izvedbena uredba Komisije (EU) 2019/317 z dne 11. februarja 2019 o določitvi načrta izvedbe in ureditve pristojbin na enotnem evropskem nebu ter razveljavitvi izvedbenih uredb (EU) št. 390/2013 in (EU) št. 391/2013 (UL L št. 56, z dne 25. 2. 2019, str. 1), (v nadaljevanju: Izvedbena uredba Komisije 2019/317/EU);
- Uredba Komisije (EU) št. 73/2010 z dne 26. januarja 2010 o zahtevah glede kakovosti letalskih podatkov in letalskih informacij za enotno evropsko nebo (UL L št. 23, z dne 27. 1. 2010, str. 6), nazadnje spremenjena z Izvedbeno uredbo Komisije (EU) št. 1029/2014 z dne 26. septembra 2014 o spremembi Uredbe (EU), št. 73/2010 o zahtevah glede kakovosti letalskih podatkov in letalskih informacij za enotno evropsko nebo (UL L št. 284, z dne 30. 9. 2014, str. 9), (v nadaljevanju: Uredba Komisije 73/2010/EU)
- Priloga 17 (Varovanje) h Konvenciji o mednarodnem civilnem letalstvu (Annex 17 – Security to the Convention on International Civil Aviation),

dolžan izvajati ukrepe za zaščito sistemov kritičnih letalskih informacij.

Naročnik zagotavlja, da se ukrepi varovanja oz. informacijske varnosti upoštevajo pri načrtovanju, izvedbi, delovanju sistemov. Prav tako je naročnik določen kot element kritične infrastrukture Republike Slovenije in zaradi dejavnost, ki jo opravlja, je posebnega pomena za obrambo, in sicer na podlagi Sklepa o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji.

Ponudniki / izvajalci so seznanjeni z dejstvom, da naročnik deluje v letalskem prometu, kjer so vsi posegi v tehnologijo podvrženi predhodni najavi in odobritvi s strani naročnika, kakor tudi vsi posegi, ki so predmet tega javnega naročila. **Ponudniki oz. izbrani izvajalec se mora zavedati, da lahko pri izvajanju storitev, ki so predmet tega naročila, z nekompetentnim poseganjem in ravnanjem neposredno ogroža in vpliva na varnost v zračnem prometu!**

Ker je naročnik zavezan k izpolnjevanju zahtev iz Izvedbena uredba Komisije (EU) 2017/373[1], bo moral ponudnik oz. izbrani izvajalec zagotavljati izpolnjevanje zahteve ATM/ANS.OR.B.015 Contracted activities, kot izhajajo iz predmetne uredbe za, t.i. naročnikove zunanje storitve ter omogočiti pregled nadzornemu organu s področja varnosti in varovanja v civilnem letalstvu - Javna agencija za civilno letalstvo Republike Slovenije, ker so storitve, ki so predmet tega javnega naročila, identificirane kot varnostno pomembne za zagotavljanje naročnikovih storitev.

..... konec dokumenta .....

[1] Izvedbena uredba Komisije (EU) 2017/373 z dne 1. marca 2017 o skupnih zahtevah za izvajalce storitev upravljanja zračnega prometa/izvajanja navigacijskih služb zračnega prometa in drugih funkcij omrežja za upravljanje zračnega prometa ter njihov nadzor, razveljavitvi Uredbe (ES) št. 482/2008, izvedbenih uredb (EU) št. 1034/2011, (EU) št. 1035/2011 in (EU) 2016/1377 ter spremembi Uredbe (EU) št. 677/2011 (UL L št. 62, z dne 8. 3. 2017, str. 1), na zadnje spremenjena z Izvedbeno uredbo Komisije (EU) 2022/938 z dne 26. julija 2022 o spremembi Izvedbene uredbe (EU) 2017/373 v zvezi z zahtevami za katalog letalskih podatkov in zbornik letalskih informacij (UL L št. 209, z dne 10. 8. 2022, str. 1).