CONPET S.A., România
Str. Anul 1848 nr. 1-3, Ploieşti, 100559, Prahova
Tel: +40 - 244 - 401360; fax: + 40 – 244 – 516451
CIF: RO 1350020; Cod CAEN 4950; J29/6/22.01.1991
Capital social subscris şi vărsat 28 569 842,40 lei

Departamentul Comercial
Serviciul Achiziţii
Nr. inreg.: 42440/15.11.2022

Referinţă: Procedura simplificata organizată de CONPET SA în vederea atribuirii contractului de achiziţie ce are ca obiect servicii de audit securitate pentru rețelele şi sistemele informatice CONPET S.A.

Urmare a clarificărilor solicitate de către operatorii economici interesați cu privire la documentația publicată pentru procedura de achiziție mai sus menţionată, vă comunicăm următoarele:

Întrebare 1: CONPET S.A. dorește realizarea unui audit de securitate integral, în conformitate cu prevederile Legii 362/2018, sau doar un audit de securitate cibernetică care se rezumă la scanări de vulnerabilități, teste de penetrare la nivelul sistemelor informatice cuprinse în infrastructura IT a CONPET S.A.?

Pentru a clarifica diferența dintre cele 2 activități de audit, facem precizarea că atât în Legea 362/2018 (Legea NIS), cât și în celelalte normative conexe (Ordinul 599/2019, Ordinul 1323/2020, Decizia 88/2020 etc.) se prevede obligativitatea Operatorilor de Servicii Esentiale (OSE) de a realiza audituri de securitate cibernetică care trebuie să acopere 5 paliere: Guvernanță, Protecție, Apărare, Reziliență, Teste de penetrare.
Aceste 5 paliere prevăzute de legislatia aplicabilă operatorilor de servicii esentiale (OSE) reprezintă auditarea întregului sistem de management al securității informațiilor, respectiv auditarea:

- Managementului securității informației (analiza si evaluarea riscurilor, planuri de tratare a riscurilor, acreditarea de securitate, indicatori de securitate, auditul de securitate, testarea si evaluarea securitătii rețelelor și sistemelor informatice, asigurarea securității din punct de vedere al personalului, constientizarea si instruirea utilizatorilor, managementul resurselor informationale etc.)
- Managementul ecosistemului informațional (cartografierea sistemului, relatiile ecosistemului informational)
- Managementul arhitecturii (managementul configuratiei rețelelor si sistemelor informatice, managementul mediilor de stocare, segregarea si segmentarea rețelelor și sistemelor, filtrarea traficului, protecția serviciilor de rețea, protecția antimalware)
- Managementul administrării (administrarea conturilor, administrarea rețelelor și sistemelor, managementul accesului de la distanță)
- Managementul identității și accesului (managementul identificării și autentificării utilizatorilor, managementul drepturilor de acces)
- Managementul mentenanței (mentenanța rețelelor și sistemelor, sisteme de control industrial SCADA, monitorizare, control și achiziții de date)
- Managementul securității fizice (asigurarea protecției fizice a rețelelor și sistemelor informatice)
- Managementul detecției (managementul vulnerabilităților și alertelor de securitate, înregistrarea evenimentelor, jurnalizarea și asigurarea trasabilității activităților din cadrul rețelelor și sistemelor informatice)

- Managementul incidentelor de securitate (răspunsul la incidente, raportarea incidentelor, comunicarea cu DNSC/CSIRT)
- Managementul continuității (asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice, managementul recuperării datelor)
- Managementul crizelor (organizarea gestionării crizelor, procesul de gestionare a crizelor)
- Identificarea și evaluarea vulnerabilităților de securitate a sistemelor informatice și a infrastructurii (scanarea si identificarea tuturor componentelor infrastructurii, scanarea de vulnerabilități la nivel de sisteme și aplicații, identificarea SPOF – Single Point Of Failure)
- Teste de penetrare/exploatare a vulnerabilităților cum ar fi: Broken Access Control, Cryptographic Failures, Insecure Design, Security Misconfiguration, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Server-side Request Forgery, Out-of-bounds Write, Cross-site Scripting, SQL Injection, Improper Input Validation, Out-of-bounds Read, OS Command Injection, Path Traversal, Cross-site Request Forgery, Integer Overflow or Wraparound, Improper Authentification, Use of Hard-coded Credentials, Missing Authorization, Command Injection, Incorrect Default Permissions, Server-side Request Forgery, Concurrent Execution using Shared Resource with Improper Synchronization (Race Condition), Uncontrolled Resource Consumption, Improper Restriction of XML External Entity Reference, Code Injection etc.

Ca o concluzie, auditul de securitate cibernetică în conformitate cu Legea 362/2018 presupune realizarea analizei și evaluării tuturor aspectelor prezentate succint mai sus pentru ca societatea Dvs., CONPET S.A., să poată demonstra printr-un Raport de audit complet că respectă în totalitate prevederile legale în domeniul securității cibernetice.

Din acest punct de vedere, ținând cont de numărul de locații, servere, echipamente, infrastructura CONPET S.A. și de clarificările pe care le-am obținut prin intermediul Anexei la Caietul de sarcini în cadrul căreia la pct. 4 ați menționat că nu aveți implementat și funcțional un sistem de management al securității informațiilor și nici de management al riscurilor, apare neclaritatea dacă se dorește auditarea conform Legii 362/2018 sau doar un audit de securitate IT. Un Raport de audit care nu cuprinde toate domeniile enumerate mai sus nu reprezintă un raport valabil pentru Directoratul National pentru Securitate Cibernetică (DNSC). Or, în acest sens, termenul de execuție de 30 zile prevăzut în Caietul de sarcini este insuficient iar CONPET S.A. va obține o serie de neconformități referitoare la managementul securității informatiilor pe care va trebui să le rezolve în cel mai scurt timp.

Răspuns 1: Chiar dacă nu avem implementat un sistem de management al securității informațiilor, activitatea se desfășoară în baza unor proceduri interne care reglementează activitatea utilizatorilor de sisteme informatice precum și pe cea a entităților organizatorice care administrează infrastructura informatică a CONPET SA.

Ca urmare, CONPET S.A. dorește realizarea unui audit de securitate în conformitate cu prevederile Legii 362/2018, pentru a confirma către DNSC măsurile de securitate pe care le avem implementate. In același timp, suntem conștienți de faptul că întotdeauna se pot imbunătăți măsurile existente și suntem deschisi pentru punerea în practică a recomandarilor care vor fi făcute de auditor în raportul de audit care atestă îndeplinirea cerințelor minime de securitate, respectând principiul

CONPET S.A., România
Str. Anul 1848 nr. 1-3, Ploieşti, 100559, Prahova
Tel: +40 - 244 - 401360; fax: + 40 – 244 – 516451
CIF: RO 1350020; Cod CAEN 4950; J29/6/22.01.1991
Capital social subscris şi vărsat 28 569 842,40 lei

proporționalității – asigurarea unui echilibru între riscurile la care rețelele și sistemele informatice sunt supuse și cerințele de securitate implementate.

În ceea ce privește termenul de execuție, pentru a nu îngrădi participarea tuturor ofertanților și având în vedere faptul că perioada de desfășurare a contractului se va suprapune cu perioada sărbătorilor de iarnă, când vor apărea mai multe zile nelucrătoare, se va prelungi termenul de execuție de la 30 la 60 de zile.

Menționăm că oferta va fi elaborată ținând cont de indicațiile precizate mai sus și că restul cerințelor rămân neschimbate,

ȘEF DEPARTAMENT COMERCIAL
Jr. Dan MANOLACHE

Dan Manolache
Digitally signed by Dan Manolache
Date: 2022.11.16 08:52:07 +02'00'

ȘEF SERVICIU ACHIZIȚII
Ing. Florina POPESCU

Florina Popescu
Digitally signed by Florina Popescu
Date: 2022.11.15 14:46:05 +02'00'

SERVICIUL ACHIZIȚII
Coord. Achiz. Laura MIHAIL

Camelia-Mihaela Barbuceanu
Digitally signed by Camelia-Mihaela Barbuceanu
Date: 2022.11.15 14:43:05 +02'00'