Achizitie comuna/ Joint Procurement: Teste de penetrare infrastructura informatica / Supply of IT Security Assessment Services: Penetration Testing / IT Security Assessment Services according to the TIBER-EU framework

I.D.: 64079160

Data publicarii	12.12.21	Coduri CPV	72820000-4
Pretul estimativ:	200.000,00 EUR - 200.000,00 EUR		

Descriere: 2. Targeted Threat Intelligence Services, The IT infrastructure of the NBR (as well as that of the other participating institutions), as it is implemented at the time of the tests, available to both internal and external customers is within the purpose of these tests. The IT infrastructure contains the components required to operate and manage the IT environments.These components include hardware, software, networking components, an operating system (OS), and data storage, all of which are used to deliver IT services and solutions.The main objective is to identify the Participating Institution's cybersecurity risks and to take appropriate technical and organizational measures to minimize/mitigate those risks. More granular objectives are defined as follows:-Identify the external exposure in terms of surface attack and determine if the implemented security controls ensure appropriate protection against malicious actors;-Measure the level of responsiveness and capability to identify and react against a cyber-attack targeted to the weakness points;-Determine if the security policy and controls implemented within the internal IT infrastructure are strong enough to be able to identify an ongoing cyber-attack and to take measures to stop it;-Measure the effectiveness of the security awareness program by testing the user’s reaction to a social engineering cyber-attack;-Determine if the sensitive data is well protected against bad actors;-Being compliant with the regulatory requirements in terms of ensuring that the IT infrastructure offers a certain level of security protection.From the point of view of the TIBER - EU methodology:The tests will provide an overview of the existing vulnerabilities in employees, business processes, associated technology (applications and infrastructure) and will provide a detailed threat assessment that can be used to raise awareness of the current situation and the measures to be taken to address it, improve the situation and reduce the associated risks. These tests performed on the basis of the "Red / Blue / White Team" concept are an extended form of the classic concept of penetration testing which usually provides a detailed and useful assessment of technical and configuration vulnerabilities. In the end, the tests will follow a complete scenario for a targeted attack against the entire entity.. 3. Red team IT Security Services, The IT infrastructure of the NBR (as well as that of the other participating institutions), as it is implemented at the time of the tests, available to both internal and external customers is within the purpose of these tests. The IT infrastructure contains the components required to operate and manage the IT environments.These components include hardware, software, networking components, an operating system (OS), and data storage, all of which are used to deliver IT services and solutions.The main objective is to identify the Participating Institution's cybersecurity risks and to take appropriate technical and organizational measures to minimize/mitigate those risks. More granular objectives are defined as follows:-Identify the external exposure in terms of surface attack and determine if the implemented security controls ensure appropriate protection against malicious actors;-Measure the level of responsiveness and capability to identify and react against a cyber-attack targeted to the weakness points;-Determine if the security policy and controls implemented within the internal IT infrastructure are strong enough to be able to identify an ongoing cyber-attack and to take measures to stop it;-Measure the effectiveness of the security awareness program by testing the user’s reaction to a social engineering cyber-attack;-Determine if the sensitive data is well protected against bad actors;-Being compliant with the regulatory requirements in terms of ensuring that the IT infrastructure offers a certain level of security

protection.From the point of view of the TIBER - EU methodology:The tests will provide an overview of the existing vulnerabilities in employees, business processes, associated technology (applications and infrastructure) and will provide a detailed threat assessment that can be used to raise awareness of the current situation and the measures to be taken to address it, improve the situation and reduce the associated risks. These tests performed on the basis of the "Red / Blue / White Team" concept are an extended form of the classic concept of penetration testing which usually provides a detailed and useful assessment of technical and configuration vulnerabilities. In the end, the tests will follow a complete scenario for a targeted attack against the entire entity.. 1. IT Security Assessment Services in line with the latest Regular Penetration Testing Execution Standards, The IT infrastructure of the NBR (as well as that of the other participating institutions), as it is implemented at the time of the tests, available to both internal and external customers is within the purpose of these tests. The IT infrastructure contains the components required to operate and manage the IT environments.These components include hardware, software, networking components, an operating system (OS), and data storage, all of which are used to deliver IT services and solutions.The main objective is to identify the Participating Institution's cybersecurity risks and to take appropriate technical and organizational measures to minimize/mitigate those risks. More granular objectives are defined as follows:-Identify the external exposure in terms of surface attack and determine if the implemented security controls ensure appropriate protection against malicious actors;-Measure the level of responsiveness and capability to identify and react against a cyber-attack targeted to the weakness points;-Determine if the security policy and controls implemented within the internal IT infrastructure are strong enough to be able to identify an ongoing cyber-attack and to take measures to stop it;-Measure the effectiveness of the security awareness program by testing the user’s reaction to a social engineering cyber-attack;-Determine if the sensitive data is well protected against bad actors;-Being compliant with the regulatory requirements in terms of ensuring that the IT infrastructure offers a certain level of security protection.Penetration tests are performed usually by following the stages defined below:•Pre-engagement Interactions;•Intelligence Gathering and Threat Modelling;•Vulnerability Identification and Analysis;•Exploitation;•Post Exploitation;•Reporting..