

საინფორმაციო ტექნოლოგიების ინფრასტრუქტურის შედარება ტესტირება

1. შედარების ტესტირების განხორციელების მეთოდები და სტანდარტები
 - 1.1. მომწოდებელმა უნდა განხორციელოს ვებ და მობილური აპლიკაციების და ქსელური ინფრასტრუქტურის შედარების ტესტირება, როგორც ავტომატური ხელსაწყოების გამოყენებით, ასევე უშუალოდ პროექტზე მომუშავე სპეციალისტის მონაწილეობით მანუალური მეთოდით.
 - 1.2. უნდა განხორციელდეს Black და Grey Box ტიპის ტესტირება.
 - 1.3. მომწოდებელმა შედარების ტესტირება უნდა განხორციელოს ფართოდ გავრცელებული და საერთაშორისოდ აღიარებული მეთოდოლოგიებისა და სტანდარტების შესაბამისად, როგორცაა:
 - 1.3.1. Information Systems Security Assessment Framework (ISSAF);
 - 1.3.2. Open Source Security Testing Methodology Manual (OSSTMM);
 - 1.3.3. National Institute of Standards and Technology (NIST) Guideline on Network Security Testing;
 - 1.3.4. Open Web Application Security Project (OWASP);
 - 1.3.5. BSI Penetration Testing Model;
 - 1.3.6. Cybersecurity Vulnerability Assessment Methodologies (Cybersecurity VAMs);
 - 1.3.7. Penetration Testing Execution Standard (PTES);
 - 1.4. შეფასების დროს უნდა მოხდეს:
 - 1.4.1. არსებული დაუცველობების იდენტიფიცირება და მათი გამოყენების შესაძლებლობის ანალიზი;
 - 1.4.2. დაუცველობის გამოყენების შესაძლებლობის დასაბუთება;
 - 1.4.3. რისკების შეფასება ტესტირებად აპლიკაციებთან მიმართებაში;
 - 1.4.4. ექსპერტული შეფასება და კონსულტაცია ინფრასტრუქტურის დიზაინის და მისი კომპონენტების უსაფრთხოებაზე.
 - 1.5. სერვისების მიწოდებას ტესტირების თითოეული ეტაპის განმავლობაში კოორდინაციას უწევს დამკვეთის წარმომადგენლები. თუ არსებობს სამიზნე სისტემების გაუმართაობის დიდი ალბათობა, ან თუ შემსრულებელი მიაღწევს მომხმარებლის კონფიდენციალურ ინფორმაციასთან წვდომას, შემსრულებელი შეაჩერებს ტესტირების შემდგომ შესრულებას მანამ, სანამ მომსახურების შესრულების გაგრძელების ოფიციალური ნებართვა არ იქნა მიღებული დამკვეთისგან.
 - 1.6. ტესტირების პროცესში შემსრულებელმა არ უნდა ჩაატაროს ე.წ. DDoS ტიპის შეტევები, ე.წ. brute force attacks ტიპის შეტევები და ასევე რაიმე სახის ტესტირება, რომელიც მოახდენს ღრუბლოვანი სერვერის (Cloud Server) ჰიპერვიზორის ექსპლოიტირების მცდელობას.
 - 1.7. ტესტირების დასრულებისთანავე მომწოდებელმა უნდა განხორციელოს გარემოს გასუფთავება (clean up) და ტესტირების დასრულებიდან 10 სამუშაო დღის ვადაში პროექტის ფარგლებში მიღებული/მოპოვებული ინფორმაციის განადგურება.
2. პრეტენდენტმა კომპანიამ უნდა წარმოადგინოს:
 - 2.1. ვებ-აპლიკაციაზე შედარების ტესტირების განხორციელებამდე, წარმოადგინოს მეთოდოლოგია/მიდგომა, გეგმა, წინასწარ განსაზღვრული მიდგომა ინციდენტების მართვისა და მათი შემდგომ ესკალაციასთან დაკავშირებით, იმისათვის, რომ დროულად და მარტივად მოხდეს ტესტირების დროს წარმოშობილ პრობლემებთან გამკლავება.
 - 2.2. ციფრული მმართველობის სააგენტოს მიერ ინფორმაციულ სისტემაში შედარების (პენეტრაციის) ტესტის ჩატარების ავტორიზაციის დამადასტურებელი დოკუმენტი;

- 2.3. შედწევადობის ტესტირების მომსახურების განხორციელების 5 წლიანი გამოცდილება და მინიმუმ 1 სარეკომენდაციო წერილი.
- 2.4. პრეტენდენტმა პროექტში უნდა ჩართოს სულ მცირე 2 ტესტირების უშუალოდ განმახორციელებელი ქართულენოვანი პირი და ყველა ჩართულ პირს უნდა ქონდეს ჩამოთვლილი სერთიფიკატებიდან სულ მცირე ერთი:
 - 2.4.1.OSCP
 - 2.4.2.OSEP
 - 2.4.3.GCIH
 - 2.4.4.CRTP

3. ფარგლები და განხორციელების დრო:

- 3.1. 50 გარე IP მისამართი
- 3.2. 3 ვებ აპლიკაცია
- 3.3. 2 მობილური აპლიკაცია (Android & IOS)
- 3.4. 5 შიდა სერვისი

მომწოდებელმა შედწევადობის ტესტირება უნდა განახორციელოს ხელშეკრულების გაფორმებიდან არაუმეტეს 15 დღის ვადაში.

4. ანგარიშგება - შედწევადობის ტესტირება

შედწევადობის ტესტირების დასრულების შემდეგ, მომწოდებელმა დამკვეთს უნდა მიაწოდოს ორი განსხვავებული რეპორტი:

- 4.1. ტოპ მენეჯმენტისთვის, რომელიც უნდა მოიცავდეს:
 - 4.1.1.ჩატარებული ტესტირების შეჯამებას - შესრულებული სამუშაოს მოცულობა, ტესტირების მეთოდოლოგია და გამოყენებული სტანდარტები, აღმოჩენილი ხარვეზები და რეკომენდაციები. ასევე, ვიზუალიზაციის მიზნით, ანგარიში უნდა მომზადდეს გრაფიკის ან დიაგრამის გამოყენებით.
- 4.2. ინფორმაციული უსაფრთხოების და ტექნიკური მიმართულებებისათვის, რომელიც უნდა მოიცავდეს მინიმუმ ქვემოთ ჩამოთვლილ ინფორმაციას:
 - 4.2.1.შესრულებული მომსახურების შეჯამება (Executive Summary);
 - 4.2.2.სამუშაოს მოცულობა;
 - 4.2.3.კრიტიკული კომპონენტების იდენტიფიცირება;
 - 4.2.4.ტესტირების მეთოდოლოგია და გამოყენებული საშუალებები (Tool);
 - 4.2.5.შეზღუდვების აღწერა, რომელმაც ზეგავლენა მოახდინა ტესტირების ჩატარებაზე.
 - 4.2.6.ტესტირების მიმდინარეობის აღწერა;
 - 4.2.7.ტესტირებისას აღმოჩენილი ტექნიკური სისუსტეების შესახებ დეტალური ინფორმაცია (მათი სიმძიმე; დაკავშირებული რისკები და ა.შ.)
 - 4.2.8.გამოყენებული და კომპრომიტირებული სისუსტეების დეტალური აღწერა, შესაბამისი დამადასტურებელი მტკიცებულებით (Screenshot);
 - 4.2.9.სისუსტეებისთვის რისკის რეიტინგის განსაზღვრა .
 - 4.2.10. გამოვლენილ ხარვეზებისა და სისუსტეების გამოსწორების მიზნით შესაბამისი რეკომენდაციები და კონკრეტული რეაგირების ნაბიჯები.