ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №9

2021 წლის 14 დეკემბერი

ქ. თბილისი

„მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების წესისა და პერიოდულობის დადგენის შესახებ“

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-12 პუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტისა და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2021 წლის 10 ივნისის №632-IVმს-Xმპ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „ი“ ქვეპუნქტის შესაბამისად,

ვბრძანებ:

1. დამტკიცდეს „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების წესი და პერიოდულობა“.
2. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის
სააგენტოს თავმჯდომარე — დავით ნადირაშვილი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების წესი და პერიოდულობა

მუხლი 1. გავრცელების სფერო

1. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის (შემდგომ – მესამე კატეგორიის სუბიექტი) შეღწევადობის (პენეტრაციის) ტესტს (შემდგომ – პენეტრაციის ტესტი), კრიტიკული ინფორმაციული სისტემის სუბიექტის შერჩევით, ატარებს საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირი – ციფრული მმართველობის სააგენტო (შემდგომ – სააგენტო) ან მის მიერ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის 6^1 მუხლის შესაბამისად ავტორიზებული ორგანიზაცია (შემდგომ – ავტორიზებული ორგანიზაცია).

2. მესამე კატეგორიის სუბიექტი ვალდებულია უზრუნველყოს ინფორმაციული უსაფრთხოების მართვის სისტემის (შემდგომ – იუმს) გავრცელების სფეროში შემავალ ყველა კრიტიკულ ინფორმაციულ სისტემაში პენეტრაციის ტესტის ჩატარება წინასწარ დაგეგმილი და დოკუმენტირებული ამოცანის მიხედვით. იუმს-ის გავრცელების სფეროში შემავალი კრიტიკული სისტემები განისაზღვრება „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანების შესაბამისად. დოკუმენტირებულ ამოცანაში აღნიშნული უნდა იყოს იმ ინფორმაციული სისტემების შესახებ, რომლებისთვისაც ტარდება პენეტრაციის ტესტი, აგრეთვე ინფორმაცია მისი ჩატარების მეთოდოლოგიის შესახებ.

3. მესამე კატეგორიის სუბიექტსა და სააგენტოს/სააგენტოს მიერ ავტორიზებულ პირს შორის ფორმდება წერილობითი ხელშეკრულება, რომლითაც განსაზღვრულია პენეტრაციის ტესტის ფარგლები, მეთოდოლოგია, ვადები, საფასური და სხვა საკითხები.

4. მესამე კატეგორიის სუბიექტ კომერციულ ბანკებში ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის ჩატარებისთვის ავტორიზებული ორგანიზაციების პენეტრაციის ტესტის

ჩატარების უფლებამოსილების მქონე თანამშრომლების „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის 6^1 მუხლის მე-2 პუნქტით დადგენილი წესის შესაბამისად უსაფრთხოებაზე შემოწმების მიზნით შემოწმების პროცესის ინიციირებას მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის ინფორმაციული უსაფრთხოების აუდიტის ან/და პენეტრაციის ტესტის დაწყებამდე აღნიშნული კომერციული ბანკის შეტყობინების საფუძველზე უზრუნველყოფს საქართველოს ეროვნული ბანკი. საქართველოს ეროვნული ბანკი უზრუნველყოფს აგრეთვე ამ კომერციული ბანკისთვის უსაფრთხოებაზე შემოწმების შედეგების შესახებ ინფორმაციის მიწოდებას.

5. ამ ბრძანებაში გამოყენებულ ტერმინებს აქვთ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

მუხლი 2. პენეტრაციის ტესტის ჩატარება

1. პენეტრაციის ტესტის ჩატარება მიზნად ისახავს ინფორმაციულ სისტემაში არსებული არასწორი კონფიგურაციის/სისუსტეების გამოვლენას, რაც გულისხმობს შესაბამისი ხელსაწყოების გამოყენებით ინფორმაციული სისტემის სკანირებას.

2. მესამე კატეგორიის სუბიექტი უზრუნველყოფს სააგენტოს/ავტორიზებული ორგანიზაციების უფლებამოსილ წარმომადგენელთა დაშვებას მის კუთვნილ ინფორმაციულ სისტემაში, აგრეთვე ყველა იმ ინფორმაციის მიწოდებას, რაც აუცილებელია პენეტრაციის ტესტის განსახორციელებლად.

3. პენეტრაციის ტესტის ჩატარებისას გამოიყენება სხვადასხვა კომერციული და არაკომერციული ხელსაწყოები:

ა) OWASP;

ბ) OSSTMM;

გ) NIST;

დ) PTES;

ე) ISSAF.

4. გარდა ამ მუხლის მე-3 პუნქტში მითითებული ხელსაწყოებისა, აგრეთვე შესაძლებელია გამოყენებულ იქნეს სხვა, კიბერუსაფრთხოების სფეროში ცნობილი და აღიარებული ორგანიზაციის მიერ შექმნილი ხელსაწყოები. ავტორიზებული ორგანიზაციის მიერ პენეტრაციის ტესტის ჩატარებისას განსხვავებული ხელსაწყოების გამოყენების თაობაზე წინასწარ ეცნობება სააგენტოს.

5. მესამე კატეგორიის სუბიექტი ვალდებულია პენეტრაციის ტესტის ჩატარებამდე სააგენტოს წარუდგინოს პენეტრაციის ტესტის შესახებ შემდეგი ინფორმაცია:

ა) ინფორმაცია იმ ინფორმაციული სისტემების შესახებ, რომლებისთვისაც ტარდება პენეტრაციის ტესტი;

ბ) პენეტრაციის ტესტის ჩატარების მეთოდოლოგიის შესახებ;

გ) პენეტრაციის ტესტის განმახორციელებელი ორგანიზაციის შესახებ;

დ) პენეტრაციის ტესტი ჩატარების ვადების შესახებ.

6. მესამე კატეგორიის სუბიექტი ვალდებულია პენეტრაციის ტესტის ჩატარებამდე დარწმუნდეს, რომ ტესტის განმახორციელებელი შეყვანილია სააგენტოს მიერ წარმოებულ, ავტორიზებული ორგანიზაციებისა და აუდიტორების/ტესტის განმახორციელებელი პირების სიაში.

7. ამ მუხლის მე-4 პუნქტით გათვალისწინებულ შემთხვევაში პენეტრაციის ტესტის ჩატარება

დასაშვებია მხოლოდ სააგენტოს წერილობითი თანხმობის შემდეგ. სააგენტოს მიერ ამ პუნქტით გათვალისწინებული თანხმობა/უარი ეცნობება მესამე კატეგორიის სუბიექტს წერილობით მომართვიდან 30 დღის ვადაში. თანხმობა გაცემულად ითვლება იმ შემთხვევაშიც, თუ აღნიშნულ ვადაში პასუხი არ იქნება გაცემული.

მუხლი 3. პენეტრაციის ტესტის დასკვნა

1. პენეტრაციის ტესტის ჩატარების შემდეგ სააგენტოს ან ავტორიზებული ორგანიზაციის მიერ დგება დასკვნა, რომელშიც მოცემულია შესასრულებლად სავალდებულო მითითებები და აგრეთვე, რეკომენდაციები. პენეტრაციის ტესტი სრულდება პენეტრაციის ტესტის დასკვნის შედგენით. პენეტრაციის ტესტის დასკვნაში ასახული უნდა იყოს ტესტის შედეგად გამოვლენილი არასწორი კონფიგურაციის/სისუსტეების ჩამონათვალი, უსაფრთხოების თვალსაზრისით არსებული პრობლემები (ასეთის არსებობის შემთხვევაში) და მათი გადაწყვეტის გზები (რეკომენდაციები).

2. ავტორიზებული ორგანიზაციის მიერ პენეტრაციის ტესტის მესამე კატეგორიის სუბიექტში ჩატარების შემთხვევაში, პენეტრაციის ტესტის დასრულებისთანავე დასკვნის 1 ეგზემპლარი მესამე კატეგორიის სუბიექტის მიერ ეგზავნება სააგენტოს. სააგენტოს ან ავტორიზებული ორგანიზაციის (მათ შორის, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის 6^1 მუხლის მე-4 პუნქტის შესაბამისად ავტორიზებული ორგანიზაციის) მიერ პენეტრაციის ტესტის მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტ კომერციულ ბანკში ჩატარების შემთხვევაში დასკვნის 1 ეგზემპლარი ეგზავნება ეროვნულ ბანკს.

3. თუ პენეტრაციის ტესტის ჩატარების შედეგად აღმოჩენილ იქნა ინფორმაციული სისტემის სისუსტეები, მესამე კატეგორიის სუბიექტი აანალიზებს მათ და აღნიშნულის აღმოსაფხვრელად განსაზღვრავს სამოქმედო გეგმას. სამოქმედო გეგმა უნდა შეიცავდეს მისი შესრულების გრაფიკს და პენეტრაციის ტესტის დასრულებიდან 1 თვის ვადაში მესამე კატეგორიის სუბიექტის (გარდა მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკისა) მიერ წარედგინება სააგენტოს, ხოლო მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი კომერციული ბანკის შემთხვევაში – საქართველოს ეროვნულ ბანკს. ავტორიზებული ორგანიზაციის მიერ პენეტრაციის ტესტის ჩატარების შემთხვევაში ამ პუნქტით გათვალისწინებული სამოქმედო გეგმის გარდა სააგენტოს ასევე ეგზავნება ინფორმაცია აღმოჩენილი ინფორმაციული სისტემის სისუსტეების შესახებ.

4. სააგენტო საკუთარი კომპეტენციის ფარგლებში უზრუნველყოფს წარდგენილი სამოქმედო გეგმის შეფასებას, შესაბამისი რეკომენდაციების ან/და შესასრულებლად სავალდებულო მითითებების შემუშავებას და შეთანხმებული სამოქმედო გეგმის შესრულების მონიტორინგს.

მუხლი 4. კონფიდენციალურობა

1. პენეტრაციის ტესტის ჩატარებისას სააგენტოს/სააგენტოს მიერ ავტორიზებულ პირს ხელი არ მიუწვდება იმ ინფორმაციაზე, რომელიც სცილდება პენეტრაციის ტესტის ჩატარების მიზნებს. ამასთან, სააგენტო/სააგენტოს მიერ ავტორიზებული პირი ვალდებულია დაიცვას ინფორმაციის კონფიდენციალურობა, რომელიც შესაძლოა მისთვის ცნობილი გახდეს პენეტრაციის ტესტის ჩატარების შედეგად.

2. პენეტრაციის ტესტის ჩატარების შემდეგ მომზადებული დასკვნა არ შეიძლება ხელმისაწვდომი გახდეს სხვა პირებისათვის, გარდა კანონით გათვალისწინებული შემთხვევებისა.

მუხლი 5. პასუხისმგებლობა

სააგენტო/სააგენტოს მიერ ავტორიზებული პირი თავისუფლდება პასუხისმგებლობისაგან ყველა იმ ზიანის ან დაბრკოლების შექმნისთვის, რაც შესაძლოა დადგეს პენეტრაციის ტესტის ჩატარებისას, თუკი მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი არ შექმნის სატესტო გარემოს. პენეტრაციის ტესტის ჩატარებისას, მესამე პირისთვის მიყენებული ნებისმიერი ზიანისთვის პასუხისმგებლობა სრულად ეკისრება მესამე კატეგორიის სუბიექტს.

მუხლი 6. პერიოდულობა

1. მესამე კატეგორიის სუბიექტი ვალდებულია ამ წესით გათვალისწინებული პენეტრაციის ტესტი თითოეულ ინფორმაციულ სისტემაზე ჩაიტაროს, სულ მცირე, წელიწადში ერთხელ.

2. ამ ბრძანებით გათვალისწინებული პენეტრაციის ტესტის ჩატარების ვალდებულება მესამე კატეგორიის სუბიექტს წარმოეშობა „მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტისთვის ინფორმაციული უსაფრთხოების მინიმალური მოთხოვნების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის ბრძანებით გათვალისწინებული იუმს-ის გავრცელების სფეროს განსაზღვრისთვის გათვალისწინებული ვადის გასვლიდან 1 წლის განმავლობაში.