

ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №2

2024 წლის 10 ივნისი

ქ. თბილისი

„კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესისა და ავტორიზაციის პროცედურების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №8 ბრძანებაში ცვლილების შეტანის თაობაზე

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის 6¹ მუხლის პირველი პუნქტისა და „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის მე-20 მუხლის მე-4 პუნქტის საფუძველზე, ვბრძანებ:

მუხლი 1

„კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესისა და ავტორიზაციის პროცედურების დადგენის შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2021 წლის 14 დეკემბრის №8 ბრძანებით (საქართველოს საკანონმდებლო მაცნე (www.matsne.gov.ge), 15/12/2021, სარეგისტრაციო კოდი: 010320000.59.071.016024) დამტკიცებულ „კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული უსაფრთხოების აუდიტის ან/და ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილების მქონე ორგანიზაციათა მიერ ავტორიზაციის გავლის წესისა და ავტორიზაციის პროცედურებში“ შეტანილ იქნეს შემდეგი ცვლილება:

1. მე-6 მუხლის:

ა) მე-2 პუნქტის „ბ“ ქვეპუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„ბ) ორგანიზაციაში დასაქმებული ინფორმაციული უსაფრთხოების აუდიტორის/ტესტის განმახორციელებელი პირის კომპეტენციის დამადასტურებელი დოკუმენტ(ებ)ის ასლ(ებ)ი. ამასთანავე:

ბ.ა) სავალდებულოა ასლის დედანთან სისწორე დამოწმებული იყოს სანოტარო წესით, თუ წარმოდგენილია ამ წესის მე-9 მუხლის პირველი პუნქტით გათვალისწინებული რომელიმე სერტიფიკატი, რომლის ვალიდურობაც არ არის გადამოწმებადი შემდეგ ვებსაიტზე: Credly (<https://www.credly.com>);

ბ.ბ) თუ წარმოდგენილია ამ წესის მე-10 მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით გათვალისწინებული ერთ-ერთი სერტიფიკატის ასლი, სავალდებულოა სააგენტოს აგრეთვე წარედგინოს აღნიშნული სერტიფიკატის ორიგინალი (ელექტრონული) ეგზემპლარი, რომელზეც შესრულებულია Council of Registered Ethical Security Testers (CREST)-ის ელექტრონული ხელმოწერა/ელექტრონული შტამპი;“.

ბ) მე-3 პუნქტი ამოღებულ იქნეს.

2. მე-9 მუხლის მე-2 პუნქტი ამოღებულ იქნეს.

3. მე-10 მუხლი ჩამოყალიბდეს შემდეგი რედაქციით:

მუხლი 10. მოთხოვნები ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის განხორციელების მსურველი ორგანიზაციის მიმართ



„1. განცხადებაში მითითებულ, განმცხადებელთან დასაქმებულ ტესტის განმახორციელებელ პირს უნდა ჰქონდეს ქვემოთ მოცემული ერთ-ერთი ორგანიზაციის მიერ გაცემული კომპეტენციის დამადასტურებელი ერთ-ერთი მოქმედი სერტიფიკატი:

ა) ორგანიზაცია: Offensive Security (OffSec). სერტიფიკატი:

ა.ა) OffSec Certified Professional (OSCP);

ა.ბ) OffSec Certified Expert (OSCE);

ა.გ) OffSec Web Expert (OSWE);

ა.დ) OffSec Exploitation Expert (OSEE);

ა.ე) OffSec Experienced Pentester (OSEP);

ა.ვ) OffSec Exploit Developer (OSED);

ბ) ორგანიზაცია: International Council of E-Commerce Consultants (EC-Council). სერტიფიკატი:

ბ.ა) Certified Ethical Hacker (CEH);

ბ.ბ) Certified Penetration Testing Professional (CPENT);

ბ.გ) Licensed Penetration Tester (LPT);

გ) ორგანიზაცია: The Computing Technology Industry Association (CompTIA). სერტიფიკატი: PenTest+;

დ) ორგანიზაცია: The Global Information Assurance Certification (GIAC). სერტიფიკატი:

დ.ა) GIAC Penetration Tester (GPEN);

დ.ბ) GIAC Web Application Penetration Tester (GWAPT);

დ.გ) GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);

დ.დ) GIAC Certified Incident Handler (GCIH);

ე) ორგანიზაცია: INE Security. სერტიფიკატი:

ე.ა) eLearnSecurity Junior Penetration Tester (eJPT);

ე.ბ) eLearnSecurity Certified Professional Penetration Tester (eCPPT);

ე.გ) eLearnSecurity Web Application Penetration Tester (eWPT);

ე.დ) eLearnSecurity Web application Penetration Tester eXtreme (eWPTX);

ვ) ორგანიზაცია: Hack The Box Ltd (HackTheBox). სერტიფიკატი:

ვ.ა) Certified Penetration Testing Specialist (HTB CPTS);

ვ.ბ) Certified Web Exploitation Expert (HTB CWEE);

ზ) ორგანიზაცია: Zero-Point Security. სერტიფიკატი:



ზ.ა) Certified Red Team Operator (CRTO);

ზ.ბ) Certified Red Team Lead (CRTL);

თ) ორგანიზაცია: Altered Security. სერტიფიკატი:

თ.ა) Certified Red Team Professional (CRTP);

თ.ბ) Certified Red Team Expert (CRTE);

თ.გ) Certified Red Team Master (CRTM);

ო) ორგანიზაცია: Council of Registered Ethical Security Testers (CREST). სერტიფიკატი:

ო.ა) CREST Certified Tester - Infrastructure (CCT INF);

ო.ბ) CREST Certified Tester - Application (CCT APP);

ო.გ) CREST Certified Simulated Attack Specialist (CCSAS).

2. ამ მუხლის პირველი პუნქტის „ა“-„თ“ ქვეპუნქტებით გათვალისწინებული შესაბამისი სერტიფიკატის ვალიდურობა გადამოწმებადი უნდა იყოს ერთ-ერთ შემდეგ ვებსაიტზე: Credly (<https://www.credly.com>), Accredible (<https://www.credential.net>), ASPEN (<https://aspen.eccouncil.org>), INE (<https://certs.ine.com>), HackTheBox (<https://www.hackthebox.com>), Canvas Badges (<https://eu.badgr.com>). ამ მუხლის პირველი პუნქტის „ი“ ქვეპუნქტით გათვალისწინებული შესაბამისი სერტიფიკატის ვალიდურობა მოწმდება ამ წესის მე-6 მუხლის მე-2 პუნქტის „ბ.ბ“ ქვეპუნქტის შესაბამისად.“.

4. მე-12 მუხლის მე-2 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„2. ამ მუხლის პირველი პუნქტით გათვალისწინებული, საქართველოს სახელმწიფო უსაფრთხოების სამსახურის უფროსის ნორმატიული აქტით განსაზღვრულ უსაფრთხოების მოთხოვნებთან შესაბამისობის თაობაზე ინფორმაციის მიღების მიზნით, სააგენტო უფლებამოსილ სახელმწიფო ორგანოს მიმართავს ამ წესის მე-8 მუხლის პირველი პუნქტის მიხედვით განცხადებისა და მასზე თანდართული დოკუმენტების ამ წესის მოთხოვნებთან შესაბამისობის დადგენიდან 5 დღის ვადაში.“.

5. მე-13 მუხლის:

ა) პირველი პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„1. ავტორიზაციის შესახებ განცხადებისა და მასზე თანდართული დოკუმენტების/ინფორმაციის კანონთან და ამ წესთან სრულად შესაბამისობის დადგენის შემთხვევაში, სააგენტო იღებს გადაწყვეტილებას ავტორიზაციის მინიჭების შესახებ. გადაწყვეტილებაში მიეთითება ავტორიზებულ ორგანიზაციაში დასაქმებული ის აუდიტორი/ტესტის განმახორციელებელი პირი, რომლის მეშვეობითაც ავტორიზებულ ორგანიზაციას ენიჭება ინფორმაციული უსაფრთხოების აუდიტის/ინფორმაციულ სისტემაში შეღწევადობის (პენეტრაციის) ტესტის ჩატარების უფლებამოსილება ამ წესის მე-9 ან მე-10 მუხლით გათვალისწინებული შესაბამისი სერტიფიკატის მოქმედების ვადის განმავლობაში, ხოლო თუ სერტიფიკატი გაცემულია განუსაზღვრელი ვადით – სააგენტოს მიერ ავტორიზაციის მინიჭების თარიღიდან სამი წლის განმავლობაში.“;

ბ) მე-2 პუნქტი ამოღებულ იქნეს;

გ) მე-4 პუნქტი ჩამოყალიბდეს შემდეგი რედაქციით:

„4. ავტორიზაციის ვადის ათვლა იწყება სააგენტოს მიერ ამ მუხლის მე-3 პუნქტით გათვალისწინებული სერტიფიკატის გაცემის მომენტიდან.“.

მუხლი 2

ბრძანება გავრცელდეს მხოლოდ მისი ამოქმედების შემდეგ წარდგენილი ავტორიზაციის შესახებ



განცხადებების განხილვაზე.

მუხლი 3

ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

სსიპ ციფრული მმართველობის
სააგენტოს თავმჯდომარე

დავით ნადირაშვილი

