მონაცემთა გაცვლის სააგენტოს თავმჯდომარის

ბრძანება №5

2013 წლის 4 თებერვალი

ქ. თბილისი

მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ

,,საჯარო სამართლის იურიდიული პირის - მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის $ბ^1$ ქვეპუნქტისა და ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-11 მუხლის მე-2 პუნქტის ,,ა“ ქვეპუნქტის თანახმად,

ვბრძანებ:

მუხლი 1

დამტკიცდეს ,,მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ წესები“.

მუხლი 2

ბრძანება ამოქმედდეს გამოქვეყნებისთანავე.

მონაცემთა გაცვლის სააგენტოს
თავმჯდომარე **ირაკლი გვენეტაძე**

მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის შესახებ წესები

მუხლი 1. ბრძანების მიზანი

ამ ბრძანების მიზანია მოახდინოს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის - CERT.GOV.GE (შემდგომში - დახმარების ჯგუფი) საქმიანობის რეგლამენტაცია, დახმარების ჯგუფის უფლებებისა და მოვალეობების დადგენა, მესამე პირებთან დახმარების ჯგუფის ურთიერთობის პრინციპების განსაზღვრა, დახმარების ჯგუფის მიერ გაწეული მომსახურების სახეებისა და პირობების დადგენა, ასევე სხვა ამოცანების განსაზღვრა, რომელიც ემსახურება საქართველოში კიბერსივრცის უსაფრთხოების დაცვას.

მუხლი 2. დახმარების ჯგუფის მანდატი და შემადგენლობა

1. დახმარების ჯგუფი CERT.GOV.GE წარმოადგენს ეროვნულ და სამთავრობო CERT–ს, რომლის სამოქმედო უფლებამოსილება მოიცავს სამთავრობო და კერძო სექტორის ობიექტების დაცვას კიბერ–შეტევებისა და სხვა სახის კომპიუტერული ინციდენტებისაგან.
2. დახმარების ჯგუფის უფლებამოსილება არ ვრცელდება საიდუმლო ინფორმაციის მართვისა, სისხლისსამართლებრივი გამოძიების ან სამხედრო ოპერაციების სფეროზე, გარდა იმ შემთხვევებისა, როდესაც ამ სფეროთა უფლებამოსილი წარმომადგენლები თანამშრომლობენ დახმარების ჯგუფთან ერთობლივი საფრთხეებისა და ამოცანების გადაჭრის მიზნით.
3. დახმარების ჯგუფის უფლებამოსილება არ ვრცელდება საიდუმლო ინფორმაციის მართვისა, სისხლისსამართლებრივი გამოძიების ან სამხედრო ოპერაციების სფეროზე, გარდა იმ შემთხვევებისა, როდესაც ამ სფეროთა უფლებამოსილი წარმომადგენლები თანამშრომლობენ დახმარების ჯგუფთან ერთობლივი საფრთხეებისა და ამოცანების გადაჭრის მიზნით.
4. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-9 მუხლის მე-5 პუნქტით გათვალისწინებულ შემთხვევაში, დახმარების ჯგუფის თანამშრომელი შეიძლება, მონაცემთა გაცვლის სააგენტოს თავმჯდომარის ბრძანებით, დაინიშნოს კომპიუტერული უსაფრთხოების სპეციალისტების საკოორდინაციო ჯგუფის ხელმძღვანელად, რათა ეფექტურად განხორციელდეს განსაკუთრებით სახიფათო ან/და მასშტაბური კიბერშეტევის თავიდან აცილება, მოგერიება ან/და მისი შედეგების აღმოფხვრა.
5. თუ სისხლის სამართლის საქმის ფარგლებში მიმდინარე გამოძიებისას დახმარების ჯგუფი ასრულებს კიბერ-შეტევის ანალიზს, დახმარების ჯგუფის წევრი უფლებამოსილია ჩვენება მისცეს სასამართლოში

როგორც მოწმემ, საქართველოს სისხლის სამართლის საპროცესო კოდექსით დადგენილი წესით.

მუხლი 3. დახმარების ჯგუფის უფლებები და მოვალეობები

1. დახმარების ჯგუფი უფლებამოსილია, განახორციელოს საქართველოს კიბერსივრცის მონიტორინგი კომპიუტერული ინციდენტების გამოვლენისა და მართვის მიზნით, განსაზღვროს და გაატაროს კიბერ უსაფრთხოების პოლიტიკა, წარმოადგინოს საქართველო ინფორმაციული და კიბერუსაფრთხოების საერთაშორისო ორგანიზაციებში და ღონისძიებებზე, ასევე განახორციელოს საქართველოს კანონმდებლობით მინიჭებული სხვა უფლებები.

2. დახმარების ჯგუფის მოვალეობებია:

ა) საქართველოს ერთიანი სამთავრობო ქსელის ფუნქციონირების მონიტორინგი კიბერუსაფრთხოების კუთხით;

ბ) კიბერუსაფრთხოების საკითხებში საზოგადოებრივი ცნობიერების ამაღლების პოლიტიკისა და მისი გატარების მეთოდების განსაზღვრა და განხორციელება;

გ) საქართველოს კიბერუსაფრთხოების ფორუმის კოორდინაცია და ორგანიზაციული მხარდაჭერა;

დ) ციფრული ხელმოწერის სერტიფიკატის (მოწმობის) გამცემის უსაფრთხოების საკითხების მონიტორინგი;

ე) სხვა მოვალეობები, რომელიც დადგენილია საქართველოს კანონით, საერთაშორისო შეთანხმებებით და ამ სფეროში მოღვაწე საერთაშორისო ორგანიზაციების წესებითა და რეკომენდაციებით.

3. თავისი საქმიანობის განხორციელებისას, დახმარების ჯგუფი ხელმძღვანელობს პრიორიტეტული საფრთხეებით, რომელიც დადგენილია „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე–8 მუხლის მე–2 პუნქტით და საქართველოს კიბერუსაფრთხოების სტრატეგიითა და სამოქმედო გეგმით.

მუხლი 4. დახმარების ჯგუფის მიერ გაწეული მომსახურებები

1. გარდა ამ წესების მე-3 მუხლით დადგენილი უფლებებისა და მოვალოებებისა, დახმარების ჯგუფი კრიტიკული ინფორმაციული სისტემის სუბიექტის და სხვა დაინტერესებული უწყებისა და ორგანიზაციისათვის ახორციელებს შემდეგ მომსახურებებს:

ა) კომპიუტერული ინციდენტის სრული ან ნაწილობრივი მართვა;

ბ) ინფორმაციული სისტემების სუსტი წერტილების მართვა;

გ) შეტყობინებების მიწოდება (როგორც პერიოდული, ისე კონკრეტული ინციდენტის პირობებში);

დ) შეღწევადობის (პენეტრაციის) ტესტის ჩატარება;

ე) შინაუწყებრივი ან ორგანიზაციის ქსელის მონიტორინგის განხორციელება;

ვ) ქსელური სენსორის კონფიგურაცია და მართვა;

ზ) მავნე კოდის ანალიზი (საექსპერტო საქმიანობა);

თ) პროგრამული კოდის ხარისხის ანალიზი;

ი) ინფორმაციული ტექნოლოგიების აუდიტის ჩატარება;

კ) ვებსაიტებისა და ვებსერვისების უსაფრთხოების სერტიფიკატის გაცემა;

ლ) სპეციალიზირებული სასწავლო კურსების ორგანიზება და შესაბამისი სერტიფიკატების გაცემა;

მ) სხვა მომსახურება, რომელიც დახმარების ჯგუფის უფლებამოსილებაში შედის და მოითხოვება დაინტერესებული უწყების ან ორგანიზაციის მიერ.

2. ამ მუხლით დადგენილი მომსახურების გაწევა ხორციელდება წინასწარ დადებული წერილობითი ხელშეკრულების საფუძველზე და ხელშეკრულების განსაზღვრულ ფარგლებში. გადაუდებელ შემთხვევებში, მომსახურების გაწევა შესაძლებელია ზეპირი შეთანხმების საფუძველზე, რომლის შედეგადაც შემდგომში უნდა დაიდოს წერილობითი ხელშეკრულება.

3. აუცილებლობის შემთხვევაში, ამ მუხლის ფარგლებში გაწეული მომსახურების პირობას წარმოადგენს მხარეებს შორის კონფიდენციალობისა და ინფორმაციის გაუმჟღავნებლობის შეთანხმება.

მუხლი 5. ურთიერთობა კრიტიკული ინფორმაციული სისტემის სუბიექტთან

1. „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის III თავის მოთხოვნათა დაცვით, კრიტიკული ინფორმაციული სისტემის სუბიექტთან დახმარების ჯგუფის ურთიერთობის სტანდარტულ ფორმატს წარმოადგენს კონტაქტი აღნიშნული სუბიქეტის კომპიუტერული უსაფრთხოების სპეციალისტთან.

2. თუ დახმარების ჯგუფი ან/და კრიტიკული ინფორმაციული სისტემის სუბიექტი საჭიროდ ჩათვლის, დახმარების ჯგუფისა და კომპიუტერული უსაფრთხოების სპეციალისტის ურთიერთობა ხორციელდება დაცული კავშირის, დაშიფრული გზავნილების ან/და ინფორმაციის დაცვის სხვა საშულებებით.

3. დახმარების ჯგუფის მოთხოვნა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული აქტივის, ინფორმაციული სისტემის ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალი საგნის წვდომაზე განსახილველად მიეწოდება სუბიექტის ინფორმაციული უსაფრთხოების მენეჯერს. დახმარების ჯგუფის მოთხოვნაზე პასუხის გაცემის (რეაგირების) ვადა განისაზღვრება მონაცემთა გაცვლის სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტის შეთანხმებით.

4. კომპიუტერული უსაფრთხოების სპეციალისტის ან ინფორმაციული უსაფრთხოების მენეჯერის

ხელმიუწვდომლობის შემთხვევაში, კრიტიკული ინფორმაციული სისტემის სუბიექტმა უნდა განსაზღვროს შემცვლელი თანამშრომელი (თანამშრომლები), რომელსაც მიეცემა გადაუდებელი ღონისძიებების განხორციელების უფლებამოსილება.
5. ამ მუხლით განსაზღვრული, ასევე სხვა დაკავშირებული საკითხების განსაზღვრის მიზნით, მონაცემთა გაცვლის სააგენტოსა და კრიტიკული ინფორმაციული სისტემის სუბიექტს შორის შესაძლებელია თანამშრომლობის მემორანდუმის შეთანხმება და დადება.

მუხლი 6. კომპიუტერული ინციდენტის მართვა

1. საქართველოს სამთავრობო ქსელის მონიტორინგის შედეგად გამოვლენილი, ქსელური სენსორების ქსელის მართვის დროს აღმოჩენილი, ქართული და უცხოეთის ორგანიზაციებიდან მიღებული ან სხვაგვარად დახმარების ჯგუფისათვის უშუალოდ მიწოდებული ინციდენტების მართვას ახორციელებს უშუალოდ დახმარების ჯგუფი.
2. კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციულ სისტემაში მომხდარი ან სავარაუდო ინციდენტის იდენტიფიცირებას ახოციელებს სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი. თუ კომპიუტერული უსაფრთხოების სპეციალისტი ინფორმაციულ სისტემაში არსებულ მოვლენას აიდეტენტიფიცრებს როგორც კომპიუტერულ ინციდენტს, ის ვალდებულია ამგვარი ინციდენტის შესახებ ინფორმაცია დაუყოვნებლივ მიაწოდოს დახმარების ჯგუფს.

მუხლი 7. დასკვნითი დებულებები

1. თუ კრიტიკული ინფორმაციული სისტემის სუბიქტი, სხვა სახელმწიფო ორგანო ან კერძო ორგანიზაცია ქმნის შინასამსახურებრივ CERT ჯგუფს, დახმარების ჯგუფის აღნიშნულ CERT ჯგუფთან ურთიერთობა რეგულირდება ამ წესების მე-5 მუხლით.
2. საქართველოს სამართალდამცავ ორგანოებთან უფლებამოსილების გამიჯვნის, გამოძიებაში დახმარების გაწევის, საექსპერტო დახმარების, ინციდენტების მართვისა და სხვა მნიშვნელოვანი საკითხები ფორმდება თანამშრომლობის მემორანდუმით.