საქართველოს იუსტიციის სამინისტრო

საქართველოს იუსტიციის სამინისტრო
პერსონალურ მონაცემთა დაცვის სააგენტო

დანართი №3

საჯარო ინფორმაციის პროაქტიულად გამოქვეყნება

საშუალოვადიანი სამოქმედო გეგმა (2013-2016 წ.წ.)

პრიორიტეტის დასახელება: **საქართველოს ინფორმაციული უსაფრთხოების განვითარება**

განხორციელების სავარაუდო ვადები:

1. ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი ამოქმედება საჯარო სექტორში და კრიტიკულ ინფრასტრუქტურაში.
2. კომპიუტერული ინციდენტების სწრაფი რეაგირების ჯგუფის ამოქმედება.

პრიორიტეტის დასაბუთება, არსებული სიტუაციიდან გამომდინარე

დღეისთვის ქვეყნის ერთ–ერთ მნიშვნელოვან პრიორიტეტულ მიმართულებას წარმოადგენს სახელმწიფო ხელისუფლების განხორციელებისას ელექტრონული მმართველობის პრინციპებზე დაფუძნებული ერთიანი სისტემის შექმნა, ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი განხორციელების ხელშეწყობა.

ელექტრონული სერვისები წარმოადგენს სახელმწიფოს მიერ განხორციელებული მომსახურების ყველაზე უფრო იაფ, მოსახერხებელ და სწრაფ მომსახურებას. ელექტრონული მომსახურების განვითარებასთან ერთად კრიტიკულ მნიშვნელობას იძენს ინფორმაციული უსაფრთხოების საკითხები, რაც სახელმწიფო უსაფრთხოების საკითხებს განეკუთვნება.

ქვეყნის ინფორმაციული ინფრასტრუქტურის მუდმივი და სწრაფი განვითარების პირობებში, სახელმწიფო მმართველობის პროცესები სულ უფრო მეტად ხდება დამოკიდებული საინფორმაციო სისტემებზე, მეორე მხრივ, ბიზნეს-პროცესების ავტომატიზებული მართვა იწვევს დამატებით რისკ ფაქტორებს, რომლებიც უკავშირდება საჯარო, სამსახურებრივი, პირადი საიდუმლო და სხვა სახის ინფორმაციის გამიჯვნას, მათი გაცვლის და მათზე წვდომის მოწესრიგებას და მონაცემებზე არასანქცირებული წვდომის გამორიცხვას. ინფორმაციული უსაფრთხოების პროგრამული და აპარატურული უზრუნველყოფის სწორად და მიზანმიმართულად დანერგვასთან ერთად აუცილებელია ინფორმაციის გაცვლასთან დაკავშირებული ადმინისტრაციული საკითხების მოგვარება, ყველა ბიზნეს-პროცესის ერთიან სტანდარტში და პროცედურებში მოქცევა, რაც გულისხმობს როგორც ნორმატიული ბაზის მომზადებას და დამტკიცებას, ასევე, ინფორმაციული უსაფრთხოების პოლიტიკის ჩარჩო დოკუმენტის და სტანდარტების, დეტალური ინსტრუქციების და სახელმძღვანელოების შემუშავებას სახელმწიფო ადმინისტრირების ყველა სფეროსთვის და პრაქტიკაში მათი დანერგვის უზრუნველყოფას.

დამატებითი ინფორმაციისთვის დაუკავშირდით:
ნატა გოდერძიშვილი - მონაცემთა გაცვლის სააგენტოს იურიდიული სამმართველოს უფროსი
ტელ: (+995 32) 291 51 40 (116); ელ.ფოსტა: foi@dea.gov.ge

საქართველოს იუსტიციის სამინისტრო

საქართველოს იუსტიციის სამინისტრო
მონაცემთა გაცვლის სააგენტო

დანართი №3

საჯარო ინფორმაციის პროაქტიულად გამოქვეყნება

ქვეყნის უსაფრთხოების განვითარების ერთ–ერთ უმთავრეს მიმართულებას წარმოადგენს ინფორმაციული უსაფრთხოების ინციდენტების მართვის და პრევენციის სისტემის შექმნა.
ამ მიმართულებით არსებობს საერთაშორისო გამოცდილება, როდესაც სახელმწიფო სტრუქტურებში იქმნება ინციდენტებზე სწრაფი რეაგირების ჯგუფები, რომელთა მიზანსაც წარმოადგენს ინციდენტებზე რეაგირების სქემების შემუშავება, კონსულტაცია და ტრენინგი,
აგრეთვე სამთავრობო ქსელის მონიტორინგი.

პრიორიტეტის მოკლე აღწერა:

ინფორმაციული უსაფრთხოების პოლიტიკის შემუშავება და მისი ამოქმედება გულისხმობს საკანონმდებლო ინიციატივის მომზადებას, რომლებიც დაარეგულირებს ყველა საჯარო სამსახურის და კრიტიკული ინფრასტრუქტურის ერთიან ნორმატიულ სივრცეში მოქცევას ინფორმაციული უსაფრთხოების კუთხით. ამ მიზნით 2012 წლის ივნისში პარლამენტმა მიიღო მონაცემთა გაცვლის სააგენტოს მიერ ინიცირებული კანონი „ინფორმაციული უსაფრთხოების შესახებ“, 2012 წლის ბოლომდე დაგეგმილია კანონქვემდებარე ნორმატიული აქტების მომზადება, რომლითაც განისაზღვრება ინფორმაციული უსაფრთხოების პოლიტიკა და სტანდარტები, რომელებიც უკავშირდება, როგორც პერსონალის მართვას, ასევე მონაცემთა აქტივების უსაფრთხოებას. დამატებით შეიქმნება დეტალური ინსტრუქციები და განმარტებითი სახელმძღვანელოები ყველა იმ პირისთვის, რომლებიც ჩართული იქნებიან ინფორმაციული უსაფრთხოების პროცესში. პრიორიტეტის ფარგლებში მონაცემთა გაცვლის სააგენტომ სახელმწიფო უწყებების და კრიტიკული ინფრასტრუქტურის წამომადგენლებისთვის მომზადა ტრენინგები ინფორმაციული უსაფრთხოების პოლიტიკის და კომპიუტერული ინციდენტების თემებზე. ტრენინგები ინტენსიურად მიმდინარეობს და გაგრძელდება შემდეგ წლებში, რადგან კანონი ინფორმაციული უსაფრთხოების შესახებ“ სახელმწიფო სექტორის და კრიტიკული უსაფრთოხების კერძო სუბიექტებს ავალდებულებს შესაბამისად მომზადებული ინფორმაციული უსაფრთხოების ოფიცრის შტატის შემოღებას. ამავე კანონისა და კანონქვემდებარე აქტებზე დაყრდნობით მონაცემთა გაცვლის სააგენტო განახორციელებს კრიტიკულ ინფრასტრუქტურაში ინფორმაციული უსაფრთოხების პოლიტიკის დანერგვის მონიტორინგს და აუდიტს.

2012 წელს დაიწყო საბიუჯეტო ორგანიზაციებში ინფორმაციული უსაფრთხოების მდგომარეობის შეფასება. ამ პროექტის მიზნებს წარმოადგენს ინფორმაციული უსაფრთხოების კუთხით საბიუჯეტო ორგანიზაციებში არსებული მდგომარეობის ზოგადი სურათის შექმნა, ინფორმაციული უსაფრთხოების მართვის სისტემის ძირითადი ტენდენციების, ძლიერი და სუსტი მხარეების გამოვლენა. აგრეთვე, ყველაზე უფრო ხშირად განმეორებადი ძირითად სისუსტეების იდენტიფიცირება, მათი აღმოფხვრის და რისკების შემცირების სტრატეგიების შემუშავების ხელშეწყობა. აღნიშნული შეფასებები

დამატებითი ინფორმაციისთვის დაუკავშირდით:
ნატა გოდერძიშვილი - მონაცემთა გაცვლის სააგენტოს იურიდიული სამმართველოს უფროსი
ტელ: (+995 32) 291 51 40 (116); ელ.ფოსტა: foi@dea.gov.ge

საჯარო ინფორმაციის პროაქტიულად გამოქვეყნება

ორგანიზაციებში განხორციელდება წელიწადში ერთხელ, რათა შემოწმდეს, რამდენად მოხდეს წინა შეფასების დროს მიცემული რეკომენდაციების გათვალისწინება.

ინციდენტებზე სწრაფი რეაგირების ჯგუფი შეიქმნა მონაცემთა გაცვლის სააგენტოს ფარგლებში, რომელიც გაწევრიანდა ინციდენტებზე რეაგირების საერთაშორისო ორგანიზაციაში -Tristed Introducer, 2013 დაგეგმილია მისი გაწევრიანება შემდეგ ორგანიზაციაში-First.org საიდანაც მიიღებს როგორც საკონსულტაციო მომსახურებას, ასევე, საჭიროების შემთხვევაში ინციდენტებზე რეაგირებისას უშუალო დახმარებას. ინციდენტების რეაგირების ჯგუფი ჩამოყალიბდა სააგენტოს სტრუქტურული ქვედანაყოფის სახით, მოხდა თანამშრომელთა პირველადი ტრენინგი და ამუშავდა ინციდენტების ანგარიშგების სისტემა. სამომავლოდ ეს ჯგუფი დაამყარებს ქსელური კავშირის მონიტორინგს ყველა სახელმწიფო სტრუქტურასთან. პირველ ეტაპზე ინფორმაციული ინციდენტების დამუშავება და ანალიზი მთლიანად ცენტრალიზებულად ხორციელდება. შემდეგ ეტაპზე (2013–2015 წლები) შეიქმნება ინციდენტების მართვის ადგილობრივი ჯგუფები მსხვილ სახელმწიფო და კრიტიკული ინფრასტრუქტურის ორგანიზაციებში. ქსელური ტრაფიკის მონიტორინგისთვის 2012 წელს დაიწყო სახელმწიფო დაწესებულებებში სპეციალური სენსორების დაყენება, რომელთა მიზანია ინციდენტების პრევენცია, მათი დროულად გამოვლენა და სწრაფი რეაგირების განხორციელება. 2013 წელს გაგრძელდება კრიტიკულ ინფრასტრუქტურაში სენსორების დაყენება. CERT.GOV.GE მომხმარებლებს სთავაზობს სერვისების მრავალფეროვან სპექტრს, როგორიცაა შეღწევადობის ტექსტი, ორგანიზაციების საინფორმაციო სისტემების და აპლიკაციების პროგრამული კოდის შემოწმების სერვისი და ა.შ. 2012 წელს ასევე გაეშვა IP მისამართების მონიტორინგის სერვისი, რაც გულისხმობს იმ IP მისამართების ბაზის შექმნას, რომლებიც მოხვდნენ კომპიუტერულ ინციდენტებზე რეაგირების საერთაშირისო ორგანიზაციების მიერ წარმოებულ დაინფიცირებული მისამართების ბაზაში და განლაგებული არიან საქართველოს ტერიტორიაზე. ეს მონაცემები სპეციალური სისტემის საშუალებით შედარდება სახელმწიფო ორგანიზაციების IP მისამართების მასივებს და საჭიროების შემთხვევაში ხდება შესაბამისი რეაგირება. 2013 წლისთვის იგეგმება სერვისში ჩართული ორგანიზაციების რაოდენობა.

კრიზისულ სიტუაციაში ქვეყანაში არსებული IT და ინფორმაციულ უსაფრთხოებასთან დაკავშირებული რესურსები მიმოფანტულია, გართულებულია მათი კონსოლიდაცია და კოორდინაცია, რაც დაკავშირებულია კრიტიკულ რისკებთან. საჭიროა შეიქმნას რესურსების სწრაფი და ეფექტური მობილიზაციის სქემა და მექანიზმი, ამასთან მნიშვნელოვანია, რომ ღირებული საკადრო რესურსებს ჰქონდეთ კომუნიკაციის და ერთობლივი მუშაობის მოსახერხებელი გარემო. ამ მიზნით 2012 წელს მონაცემთა სააგენტოს ინიციატივით შეიქმნა კიბერ-უსაფრთხოების გაერთიანება, რომელშიც მონაწილეობას იღებს სახელმწიფო და კერძო ორგანიზაციების 50-მდე ექსპერტი.

დამატებითი ინფორმაციისთვის დაუკავშირდით:
ნატა გოდერძიშვილი - მონაცემთა გაცვლის სააგენტოს იურიდიული სამმართველოს უფროსი
ტელ: (+995 32) 291 51 40 (116); ელ.ფოსტა: foi@dea.gov.ge

საქართველოს იუსტიციის სამინისტრო

საქართველოს იუსტიციის სამინისტრო
მონაცემთა გაცვლის სააგენტო

დანართი №3

საჯარო ინფორმაციის პროაქტიულად გამოქვეყნება

2013-2016 წლებისთვის დაგეგმილია გაერთიანების, სტრუქტურის, სამუშაო სპეციფიკის და ინფრასტრუქტურის დაგეგმვა და მომზადება, კრიზისულ სიტუაციებში მოქმედების გეგმის შედგენა, ამ გეგმის გამოცდა სიმულაციურ გარემოში.

მოსალოდნელი შედეგები:

შუალედური შედეგი 2013 წლის ბოლოსთვის: შექმნილია ინფორმაციული უსაფრთხოების პოლიტიკის დოკუმენტების ყოველწლიური რევიზიის და დანერგვის მექანიზმები, განსაზღვრულია ინფორმაციული უსაფრთხოების კუთხით კრიტიკული ინფრასტრუქტურის სუბიექტები, დაწყებულია პოლიტიკის დანერგვა კრიტიკულ ინფრასტრუქტურაში, შემუშავებულია და აქტიურად გამოიყენება კრიტიკულ ინფრასტრუქტურაში ინფორმაციული უსაფრთხოების დანერგვის მონიტორინგის და ანგარიშგების ინსტრუმენტები, მომზადებული არიან სერტიფიცირებული სპეციალისტები ინფორმაციული უსაფრთხოების სფეროში, შემუშავებულია მესამე პირების მიერ კრიტიკულ ინფრასტრუქტურაში ინფორმაციული უსაფრთხოების დანერგვის და აუდიტის ავტორიზაციის მექანიზმები, მონაცემთა გაცვლის სააგენტო ახორციელებს ინფორმაციული უსაფრთხოების არსებული მდგომარეობის პერიოდულ შეფასებას (რევიზიას) კრიტიკული ინფრასტრუქტურის სუბიექტებში. აგებულია ინფრასტრუქტურა CERT.GOV.GE-ისთვის, ამუშავებულია კომპიუტერულ ინციდენტებზე რეაგირების სისტემა და სქემა, CERT.GOV.GE გაწევრიანებულია საერთაშირისო ორგანიზაციაში First.org, დაწესებულია მონიტორინგი ინფორმაციის გაცვლის ინფრასტრუქტურაზე, აქტიურად მუშაობს კიბერ-უსაფრთხოების გაერთიანება, მომზადებულია კრიზისულ სიტუაციებში მოქმედების გეგმა .

საბოლოო შედეგი: ინფორმაციული უსაფრთხოების პოლიტიკა დანერგილია კრიტიკულ ინფრასტრუქტურაში. შექმნილი და დატრენინგებულია ინციდენტების მართვის ადგილობრივი ჯგუფები მსხვილ სახელმწიფო და კრიტიკული ინფრასტრუქტურის ორგანიზაციებში, შექმნილია ციფრული ხელმოწერის სერტიფიკატის (მოწმობის) გამცემის უსაფრთხოების საკითხების მონიტორინგის მექანიზმები, დაწესებულია მონიტორინგი სამთავრობო ქსელზე.

შედეგების შეფასების კრიტერიუმები:

2013 წლის ბოლომდე კრიტიკული ინფრასტრუქტურის 50% ჩართულია პოლიტიკის აქტიურ დანერგვაში, რაც აისახება მათ მიერ მოწოდებულ პერიოდულ ანგარიშებში. მათგან 60%-ში ჩატარდა ინფორმაციული უსაფრთხოების მდგომარეობის მეორადი შეფასება, და 50%-ზე მეტ შემთხვევაში

დამატებითი ინფორმაციისთვის დაუკავშირდით:
ნატა გოდერძიშვილი - მონაცემთა გაცვლის სააგენტოს იურიდიული სამმართველოს უფროსი
ტელ: (+995 32) 291 51 40 (116); ელ.ფოსტა: foi@dea.gov.ge

დანართი №3

საჯარო ინფორმაციის პროაქტიულად გამოქვეყნება

პირველადი შეფასებისას მიცემული რეკომენდაციები გათვალისწინებულია. 2016 წლის ბოლომდე კრიტიკული ინფრასტრუქტურის სუბიექტების 90% ჩართულია პოლიტიკის აქტიურ დანერგვაში, მათგან 80% აკმაყოფილებს სტანდარტით განსაზღვრულ მოთხოვნებს.

2013 წლის ბოლომდე კრიტიკულ ინფრასტრუქტურაში დაყენებულია 15-მდე ქსელური სენსორი. მათ მიერ გამოვლენილ ყველა ინციდენტზე მოხდენილია დროული და სათანადო რეაგირება.

კიბერ-უსარფთხოების გაერთიანების წევრების რაოდენობა 2012 წელთან შედარებით გაზრდილია 20%-ით და ფარავს კრიტიკული ინფრასტრუქტურის დიდ ნაწილს. გაერთიანება 2013 წლის ბოლომდე იკრიბება არანაკლებ 6-ჯერ.

IP მისამართების მონიტორინგის სერვისში ჩართულია არანაკლებ 25 ორგანიზაციისა.

კომპიუტერულ ინციდენტებზე რეაგირების სისტემაში წლის ბოლომდე დარეგისტრირებული და ბოლომდე გაანალიზებულია ყველა მაღალი დონის ინფორმაციული ინციდენტი (150-ზე მეტი), რომელიც შემოვა ქსელში ჩართული საჯარო და კერძო კრიტიკული ინფრასტრუქტურიდან.
შემუშავებულია არანაკლებ 30 რეკომენდაცია ყველაზე უფრო ტიპიური ინფორმაციული ინციდენტის შემდგომი პრევენციისთვის.

2016 წლამდე კრიტიკული ინფრასტრუქტურის ყველა სუბიექტში დაკომპლექტებული და დატრენინგებულია ინციდენტებზე რეაგირების ადგილობრივი ჯგუფები. შექმნილია სატრენინგო და საკონსულტაციო ინფრასტრუქტურა. ტრენინგების მონაწილეთა 80%-ზე მეტი ტრენინგს წარმატებულად აფასებს და პრაქტიკაში იყენებს მიღებულ ცოდნას და უნარ-ჩვევებს.

დამატებითი ინფორმაციისთვის დაუკავშირდით:
ნატა გოდერძიშვილი - მონაცემთა გაცვლის სააგენტოს იურიდიული სამმართველოს უფროსი
ტელ: (+995 32) 291 51 40 (116); ელ.ფოსტა: foi@dea.gov.ge