საქართველოს თავდაცვის მინისტრის
ბრძანება

ქ. თბილისი

MOD 8 15 00000693

30/09/2015

კომპიუტერული უსაფრთხოების ინციდენტების შესახებ შეტყობინების პროცედურის თაობაზე

,,საქართველოს თავდაცვის სამინისტროს დებულების დამტკიცების შესახებ" საქართველოს მთავრობის 2013 წლის 22 ნოემბრის №297 დადგენილებით დამტკიცებული დებულების მე-3 მუხლის მე-3 პუნქტის „ე" ქვეპუნქტის საფუძველზე,

ვ ბ რ ძ ა ნ ე ბ:

1. დამტკიცდეს ,,კომპიუტერული უსაფრთხოების ინციდენტების შეტყობინების პროცედურა" დანართი №1-ის შესაბამისად.
2. დამტკიცდეს ,,ინციდენტების კრიტიკულობის შკალა" დანართი №2-ის შესაბამისად.
3. ბრძანების შესრულებაზე კონტროლი დაევალოს საქართველოს თავდაცვის მინისტრის პირველ მოადგილეს ბატონ დავით ებრალიძეს.
4. ბრძანება ძალაშია ხელმოწერის დღიდან.

მინისტრის მოვალეობის შემსრულებელი
დავით ებრალიძე

დანართი №1

კომპიუტერული უსაფრთხოების ინციდენტების შეტყობინების პროცედურა

1. ,,თავდაცვის სფეროში კრიტიკული ინფორმაციული სისტემის სუბიექტების ნუსხის დამტკიცების შესახებ" საქართველოს მთავრობის 2014 წლის 29 სექტემბრის №567 დადგენილებით განსაზღვრული სუბიექტის მიერ კომპიუტერული უსაფრთხოების ინციდენტის შესახებ შეტყობინება სსიპ - კიბერუსაფრთხოების ბიუროს (შემდგომში - ბიურო) კომპიუტერულ ინციდენტებზე დახმარების ჯგუფის (cert.mod.gov.ge) (შემდგომში - cert.mod.gov.ge) მორიგეს შესაძლებელია გაეგზავნოს შემდეგი მეთოდებით:

ა) ბიუროს ინფორმაციული და კომუნიკაციების ტექნოლოგიების დეპარტამენტის კომპიუტერულ უსაფრთხოების ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილების (შემდგომში - განყოფილება) მიერ წინასწარ განსაზღვრულ შიდა, ქალაქის და მობილური ტელეფონის ნომრებზე;

ბ) ელექტრონული კითხვარის, სამინისტროს შიდა ქსელში არსებული ბიუროს კომპიუტერულ ინციდენტებზე შეტყობინების ელექტრონული კითხვარის მეშვეობით (csb.mil.ge);

გ) ელექტრონული ფოსტის საშუალებით, განყოფილების წინასწარ განსაზღვრულ ელექტრონული ფოსტის მისამართზე.

2. სამუშაო საათებში cert.mod.gov.ge -ის მორიგის მიერ კომპიუტერული უსაფრთხოების ინციდენტის შესახებ მიღებული შეტყობინება დაუყოვნებლივ მიეწოდება cert.mod.gov.ge -ის რეაგირების მორიგე ჯგუფს.

3. არასამუშაო საათებში და უქმე დღეებში კომპიუტერული უსაფრთხოების ინციდენტის შესახებ მიღებული შეტყობინება დაუყოვნებლივ მიეწოდება cert.mod.gov.ge -ის მძღოლს და რეაგირების მორიგე ჯგუფს. მძღოლი, თავის მხრივ, დაუყოვნებლივ უზრუნველყოფს რეაგირების მორიგე ჯგუფის, წინასწარ დადგენილი გამოძახების სქემის მიხედვით, დანიშნულების ადგილზე მიყვანას.

4. ინციდენტების კრიტიკულობის შკალის (დანართი №2) პირველი დონის კომპიუტერული უსაფრთხოების ინციდენტის შესახებ ინფორმაცია, დაუყოვნებლივ მიეწოდება საქართველოს შეიარაღებული ძალების გენერალური შტაბის J-3 ოპერატიული დაგეგმვის დეპარტამენტის სამხედრო მართვის ცენტრს, ბიუროს დირექტორს, დირექტორის მოადგილეებს და ბიუროს სამართლებრივი უზრუნველყოფის სამმრთველოს.

5. ინციდენტების კრიტიკულობის შკალის (დანართი №2) მეორე დონის კომპიუტერული უსაფრთხოების ინციდენტის შესახებ ინფორმაცია, დაუყოვნებლივ მიეწოდება საქართველოს შეიარაღებული ძალების გენერალური შტაბის J-3 ოპერატიული დაგეგმვის დეპარტამენტის სამხედრო მართვის ცენტრს, ბიუროს დირექტორს და დირექტორის პირველ მოადგილეს;

6. ინციდენტების კრიტიკულობის შკალის (დანართი №2) მესამე დონის კომპიუტერული უსაფრთხოების ინციდენტის შესახებ ინფორმაცია სამუშაო რეჟიმში მიეწოდება cert.mod.gov.ge -ს;

7. ინციდენტების კრიტიკულობის შკალის (დანართი №2) მეოთხე დონის კომპიუტერული უსაფრთხოების ინციდენტის შესახებ ინფორმაცია ცრუ შეტყობინებების საეჭვოდ მაღალი სიხშირის და არამიზნობრივი შეტყობინებების დროს მხოლოდ ფიქსირდება შესაბამის ჟურნალში და მონაცემთა ბაზაში და რჩება რეაგირების გარეშე.

დანართი №2

ინციდენტების კრიტიკულობის შკალა

კრიტიკულობის დონე	ინციდენტის განმარტება	ინციდენტის კატეგორია	რეაგირების დრო	რეაგირება (კრიტიკული ფაზა)	რეაგირება (არაკრიტიკული ფაზა)	კომუნიკაცია
1	ინციდენტი ზეგავლენას ახდენს კრიტიკულ სისტემაზე ან/და ინფორმაციაზე	- DDoS/DoS შეტევა - კომპრომეტირებული აქტივი - შიდა ჰაკინგი (აქტიური) - გარე ჰაკინგი (აქტიური) - მავნე პროგრამები - ჰოსტის კონფიგურაციის შეცვლა	1 საათი	CSIRT-ი რეაგირებას ახდენს 24/7-ზე	CSIRT-ი რეაგირებას ახდენს სამუშაო საათებში	**კრიტიკულ ფაზაში**: CSIRT-ი ახორციელებს აქტიურ ქმედებებს ინფორმაციის განახლება უნდა მოხდეს მინიმუმ 2 საათში ერთხელ. **არაკრიტიკულ ფაზაში**: ინფორმაციის განახლება უნდა მოხდეს ყოველდღიურად
2	ინციდენტი ზეგავლენას ახდენს არაკრიტიკულ სისტემაზე ან/და ინფორმაციაზე.	- შიდა ჰაკინგი (არა აქტიური) - გარე ჰაკინგი (არა აქტიური) - არაავტორიზებული წვდომა - კანონსაწინააღმდეგო აქტივობა - სკანირება, სნიფინგი - უსაფრთხოების ნორმების დარღვევა	4 საათი	CSIRT-ი რეაგირებას ახდენს 24/7-ზე	CSIRT-ი რეაგირებას ახდენს სამუშაო საათებში	**კრიტიკული ფაზაში**: ინფორმაციის განახლება უნდა მოხდეს ყოველდღიურად **არაკრიტიკულ ფაზაში:** ინფორმაციის განახლება უნდა მოხდეს კვირაში ერთხელ
3	შესაძლო ინციდენტები პოტენციური საფრთხეები	- ელ. ფოსტა - სისტემის არასათანადო გამოყენება	48 საათი	CSIRT-ი რეაგირებას ახდენს პრიორიტეტების გათვალისწინებით	CSIRT-ი რეაგირებას ახდენს პრიორიტეტების გათვალისწინებით	ინფორმაციის განახლება უნდა მოხდეს კვირაში ერთხელ

4	შეტყობინება რეაგირების გარეშე	- შეტყობინება ინციდენტზე რომელზე რეაგირებაც სცდება ბიუროს კომპეტენციას - ცრუ შეტყობინება	-			

შენიშვნა: დანართ №2-ში გამოყენებულ ტერმინთა განმარტებები:

1. **კანონსაწინააღმდეგო აქტივობა** - თაღლითობა, პორნოგრაფიის გავრცელება, რასობრივი, რელიგიური ან/და სხვა სახის შუღლის გავრცელება, სხვა არაკანონიერი ქმედება.
2. **უსაფრთხოების ნორმების დარღვევა** - კონფიდენციალური ან/და შიდა სამსახურებრივი ინფორმაციის გავრცელება, ინფორმაციული უსაფრთხოების ნორმების მიზანმიმართული დარღვევა, კომპიუტერის, ქსელის ან/და აპლიკაციის არასათანადო გამოყენება, უფლებამოსილების არასანქცირებულად გაზრდა ან მიზანმიმართული ქმედება წვდომის კონტროლის მართვის ხელში ჩასაგდებად.
3. **ელ.ფოსტა** - სპამი, ფიშინგი და სხვა საფრთხის შემცველი ქმედება.
4. **შიდა ჰაკინგი** - შპიონაჟი ან სხვა საეჭვო ქმედება, რომელიც ხორციელდება დაწესებულების ქსელიდან.
5. **გარე ჰაკინგი** - შპიონაჟი ან სხვა საეჭვო ქმედება, რომელიც ხორციელდება დაწესებულების ქსელზე გლობალური ქსელიდან.
6. **კვლევა** - ნებისმიერი კვლევითი სამუშაო რომელიც უნდა ჩატარდეს CSIRT-ის მიერ.
7. **კომპრომეტირებული აქტივი** - ინტელექტუალური საკუთრების ან/და სენსიტიური ინფორმაციის განადგურება ან განადგურების მცდელობა, გამჟღავნება, მთლიანობის დარღვევა.
8. **მავნე პროგრამები** - ვირუსი, ტროიანი, ვორმი და სხვა სახის პროგრამები, რომელთაც ზეგავლენის მოხდენა შეუძლიათ ელექტრონულ ინფორმაციაზე კომპიუტერზე ან მის კონფიგურაციაზე.
9. **DDoS/DoS შეტევა** - შეტევა, რომელიც ხორციელდება სერვერის პარალიზების მიზნით.
10. **არაავტორიზებული წვდომა** - ქმედება რომლის დროსაც პიროვნება ან/და სისტემა იღებს არასანქცირებულ წვდომას ქსელზე, სისტემაზე, პროგრამულ უზრუნველყოფაზე ან სხვა IT რესურსზე.
11. **კრიტიკული ფაზა** - დროის ის მონაკვეთი როდესაც ინციდენტი არ არის დასრულებული და აუცილებელია აქტიური რეაგირება. ეს მოიცავს სისტემის ან/და სერვისის მუშაობის შეფერხებას, მტკიცებულებების გამოვლენას, შეგროვებას, შენახვას, შეფასებას, სორტირებას, პირველადი აღდგენითი სამუშაოების ჩატარებას.
12. **არაკრიტიკული ფაზა** - დროის ის მონაკვეთი როცა ინციდენტზე არ არის საჭირო გადაუდებელი რეაგირება, მტკიცებულებების შეგროვება, კვლევა, ანალიზი და სრული აღდგენა.