ციფრული მმართველობის სააგენტოს თავმჯდომარის

ბრძანება №4

2021 წლის 14 დეკემბერი

ქ. თბილისი

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესების დადგენის შესახებ

„ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-10 მუხლის პირველი პუნქტის, „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“ საქართველოს კანონის მე-7 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტის, „ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის 25-ე მუხლისა და „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონში ცვლილების შეტანის თაობაზე“ 2021 წლის 10 ივნისის №632-IVმს-Xმპ საქართველოს კანონის მე-2 მუხლის მე-2 პუნქტის „დ“ ქვეპუნქტის შესაბამისად, **ვბრძანებ:**

1. დამტკიცდეს მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების თანდართული წესები.
2. ძალადაკარგულად გამოცხადდეს „ქსელური სენსორის კონფიგურაციის წესების დამტკიცების შესახებ“ ციფრული მმართველობის სააგენტოს თავმჯდომარის 2020 წლის 16 ოქტომბრის №3 ბრძანება.
3. ეს ბრძანება ამოქმედდეს 2021 წლის 30 დეკემბრიდან.

სსიპ ციფრული მმართველობის სააგენტოს თავმჯდომარე **დავით ნადირაშვილი**

მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესები

მუხლი 1. მოქმედების სფერო

1. ქსელური სენსორი არის აპარატული ან/და პროგრამული უზრუნველყოფის საშუალებების ერთობლიობა, რომელიც გამიზნულია ქსელური ნაკადის მონიტორინგისთვის, ინფორმაციული სისტემის წინააღმდეგ მიმართული კომპიუტერული ინციდენტის გამოსავლენად.

2. მესამე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტი (შემდგომ – მესამე კატეგორიის სუბიექტი) კომპიუტერული ინციდენტის იდენტიფიცირების მიზნით იყენებს ქსელურ სენსორს.

3. კომპიუტერული ინციდენტის იდენტიფიცირების ან/და მასზე რეაგირების მიზნით საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს (შემდგომ – სააგენტო) კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი (შემდგომ – დახმარების ჯგუფი) უფლებამოსილია მესამე კატეგორიის სუბიექტის თანხმობით ჰქონდეს წვდომა ამ სუბიექტის ქსელურ სენსორზე. ქსელური სენსორის კონფიგურირებასა და მართვას სააგენტო და მესამე კატეგორიის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტი ერთობლივად ახორციელებენ.

4. სუბიექტი უფლებამოსილია, შეარჩიოს მასთან განთავსებული ქსელური სენსორის მომსახურების სახე, კერძოდ, ქსელის ზედაპირული მონიტორინგი ან ქსელის პაკეტების ღრმა ანალიზის მონიტორინგი.

5. ინფორმაცია, რომელსაც შეიცავს ქსელური სენსორის მიერ გენერირებული მონაცემები,

მნიშვნელოვან დახმარებას უწევს როგორც დახმარების ჯგუფს, ისე მესამე კატეგორიის სუბიექტის კიბერუსაფრთხოების სპეციალისტს და სხვა ტექნიკურ პერსონალს ინციდენტის სწრაფად, დროულად და ეფექტიანად გამოვლენაში.

6. ამ წესში გამოყენებულ ტერმინებს აქვთ „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონით განსაზღვრული მნიშვნელობა.

მუხლი 2. ქსელური სენსორის კონფიგურაციის მიმართ განსაზღვრული მოთხოვნები

ქსელური სენსორის კონფიგურაციისას გათვალისწინებული უნდა იქნეს სულ მცირე შემდეგი მოთხოვნები:

ა) ჩანაწერების (ე.წ. „ლოგის“) შენახვის შესაძლებლობა, საჭიროებისამებრ, მესამე კატეგორიის სუბიექტის მიერ განსაზღვრული, მაგრამ არანაკლებ 3 თვის ვადით;

ბ) მესამე კატეგორიის სუბიექტის ინფრასტრუქტურის სერვერებზე წვდომის მონიტორინგის შესაძლებლობა;

გ) სხვადასხვა ქსელურ სეგმენტში არსებული ქსელური სენსორის სამართავი პანელის არსებობა;

დ) ქსელური სენსორის შეფერხებით ფუნქციონირების შემთხვევისთვის სათადარიგო მექანიზმების არსებობა;

ე) ქსელის მასშტაბის ზრდის შემთხვევაში, ახალი სენსორების დამატების შესაძლებლობა;

ვ) სენსორზე გარე ქსელიდან (ინტერნეტიდან) წვდომის შესაძლებლობის შეზღუდვა;

ზ) ქსელური სენსორისა და მისი სამართავი პანელის რთული და კომპლექსური პაროლით დაცვა;

თ) ინციდენტის გამოვლენის წესების მოდიფიკაციის, წაშლის და ახლის დამატების შესაძლებლობა.

მუხლი 3. ინფორმაციასთან წვდომა და კონფიდენციალურობის დაცვა

1. ქსელური სენსორის კონფიგურირებისას გამოირიცხება სააგენტოს მიერ მესამე კატეგორიის სუბიექტის კომუნიკაციის შინაარსობრივი მონაცემის ხელმისაწვდომობის შესაძლებლობა. სააგენტოს არ გააჩნია წვდომა ქსელის მონიტორინგის პაკეტების ღრმა ანალიზის საშუალებებზე. სააგენტოს, მესამე კატეგორიის სუბიექტთან შეთანხმებით, აქვს უფლება:

ა) მონიტორინგის მოწყობილობით მიიღოს ინფორმაცია ქსელში აღმოჩენილი ანომალიების შესახებ;

ბ) შეუფერხებლად მიიღოს სისტემის კონფიგურაციის შესახებ სრული ინფორმაცია;

გ) მოითხოვოს სისტემის კონფიგურაციის ცვლილება ან/და განახლება.

2. მესამე კატეგორიის სუბიექტი ვალდებულია, დაუყოვნებლივ აცნობოს მის მიერ ქსელის მონიტორინგის ინფრასტრუქტურაში დაგეგმილი ან გადაუდებელი პირობებით გამოწვეული ნებისმიერი ცვლილება.

3. სააგენტო ვალდებულია დაიცვას ინფორმაციის კონფიდენციალურობა, რომელიც შესაძლოა მისთვის ცნობილი გახდეს ამ წესით გათვალისწინებული უფლებამოსილების განხორციელებისას.