საქართველოს სახელმწიფო უსაფრთხოების სამსახური

სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის

ბრძანება №3

2024 წლის 5 ივნისი

ქ. თბილისი

„პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესების დადგენის შესახებ“ საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2022 წლის 11 მაისის №15 ბრძანებაში ცვლილების შეტანის თაობაზე

„ნორმატიული აქტების შესახებ“ საქართველოს ორგანული კანონის მე-20 მუხლის მე-4 პუნქტის, „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის მე-10 მუხლის პირველი პუნქტის, „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს დებულების დამტკიცების შესახებ“ საქართველოს მთავრობის 2017 წლის 29 მარტის №157 დადგენილებით დამტკიცებული დებულების მე-6 მუხლის „ა“ და „ბ“ ქვეპუნქტების საფუძველზე, **ვბრძანებ:**

მუხლი 1

შეტანილ იქნეს ცვლილება „პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესების დადგენის შესახებ“ საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსის 2022 წლის 11 მაისის №15 ბრძანებაში და ბრძანებით დამტკიცებული № 1 დანართის შემდეგ დაემატოს დანართი №2.

მუხლი 2

1. ეს ბრძანება, გარდა ამ ბრძანების დანართი № 2-ის მე-11-მე-17 პუნქტებისა, ამოქმედდეს 2025 წლის 1 იანვრიდან.
2. ამ ბრძანების დანართი № 2-ის მე-11-მე-17 პუნქტები ამოქმედდეს 2025 წლის 1 ივნისიდან.

საჯარო სამართლის იურიდიული პირის - საქართველოს ოპერატიულ-ტექნიკური სააგენტოს უფროსი — **კობა კობიძე**

დანართი №2

პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების ქსელური სენსორის ტექნიკური რეგლამენტი

თავი I

რეგულირების სფერო

1. რეგლამენტის გავრცელების სფერო

1.1. ამ რეგლამენტით დაწესებული მოთხოვნები სრულად ვრცელდება პირველი კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტზე.

1.2. ამ რეგლამენტის მოქმედება ვრცელდება მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტზე გარდა იმ ნორმებისა, რომელიც ითვალისწინებს სსიპ – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს (შემდგომში – სააგენტო) ქსელურ სენსორთან წვდომას და მის

ერთობლივ მართვას შესაბამისი კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული უსაფრთხოების სპეციალისტთან ერთად.

1.3. ამ რეგლამენტის მოქმედება სრულად გავრცელდება მეორე კატეგორიის სუბიექტთან მიმართებით, თუ ეს უკანასკნელი თანხმობას განაცხადებს სააგენტოს მიერ ქსელურ სენსორთან წვდომაზე და მის ერთობლივ მართვაზე;

1.4. ამ პუნქტის 1.3. ქვეპუნქტით გათვალისწინებული თანხმობა მეორე კატეგორიის სუბიექტს შეუძლია გაითხოვოს ნებისმიერ დროს საკუთარი შეხედულებისამებრ, სააგენტოს მინიმუმ 1 თვიანი წინასწარი ინფორმირებით.

1.5. ამ რეგლამენტის მოქმედება გარდა მე-4 პუნქტის 4.1.3., 4.1.6., 4.1.8. და 4.1.9 ქვეპუნქტებისა, ვრცელდება ასევე იმ სისტემებზე, რომელთაც არ აქვთ კავშირი გარე ქსელთან და გამოყენება კონფიდენციალური და შინასამსახურებრივი გამოყენების მონაცემების დამუშავების მიზნებისთვის.

2. რეგლამენტის მიზნები

2.1. პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების (შემდგომში – ორგანიზაცია) ქსელური სენსორის ტექნიკური რეგლამენტი (შემდგომში – რეგლამენტი) განსაზღვრავს მხოლოდ საბაზისო ტექნიკურ პარამეტრებს, რომელსაც უნდა აკმაყოფილებდეს ორგანიზაციის მიერ შერჩეული და საკუთარ საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურაში განთავსებული ქსელური სენსორები.

2.2. რეგლამენტი მიზნად ისახავს ორგანიზაციაში არსებული ინციდენტების მართვას ორ დონეზე: უშუალოდ ორგანიზაციის შიგნით თავად ორგანიზაციის მიერ და სააგენტოს დონეზე, ერთობლივად, ორგანიზაციისა და სააგენტოს მიერ.

2.3. ეს რეგლამენტი არ ზღუდავს ორგანიზაციას შეიძინოს ან შეიმუშაოს ისეთი ტიპის ტექნიკური გადაწყვეტები, რომელთაც აქვთ ამ რეგლამენტით განსაზღვრულ საბაზისო ტექნიკურ პარამეტრებზე მეტი ფუნქციონალი.

ქსელური სენსორი, მისი ძირითადი ფუნქციები და მასზე მონიტორინგი

3. ქსელური სენსორის ძირითადი ფუნქციონალი

3.1. ქსელური სენსორის ძირითადი ფუნქციონალი უნდა მოიცავდეს:

3.1.1. **მონაცემთა აგრეგაციას** – ორგანიზაციის ინფრასტრუქტურის შიგნით არსებული ძირითადი მოწყობილობებიდან აქტივობის ამსახველი ჩანაწერების (ლოგ ჩანაწერები) მონაცემების ცენტრალიზებული ფორმით შეგროვებისა და შენახვის საშუალება;

3.1.2. **მონაცემთა ნორმალიზაციას** – კონკრეტულ შემთხვევასთან დაკავშირებული სხვადასხვა წყაროებიდან მიღებული რელევანტური მონაცემების ურთიერთავსებადობის, კორელაციისა და დადარების შესაძლებლობა;

3.1.3. **მონაცემთა ანალიტიკას** – წინასწარ გაწერილი წესებისა და ინდიკატორების შესაბამისად მონაცემების დამუშავება და სავარაუდო შეტევის/საეჭვო შემთხვევების აღმოჩენა, მათ შორის მომხარებელთა ანომალიური ქცევის გამოვლენა (UBA – User Behavior Analytics);

3.1.4. **განგაშის გენერირებას** – შეტევის ან საეჭვო შემთხვევების აღმოჩენის შემთხვევაში შესაბამისი განგაშის რეალურ დროში გენერირების უნარი;

3.1.5. **მაკომპრომეტირებელი მონაცემების დამუშავებას** – შეტევის ან საეჭვო შემთხვევების დროს დაგენერირებული განგაშის შესაბამისი მონაცემების გამორჩევა და დეტალური დამუშავების შესაძლებლობა.

3.2. ქსელურ სენსორში მონაცემთა შეგროვებისა და დამუშავების პრინციპი ეფუძნება ინფორმაციული

უსაფრთხოების სტანდარტს – CIA (Confidentiality, Integrity, Availability) ტრიადას.

3.3. ქსელური სენსორი უნდა იძლეოდეს საეჭვო, ანომალიური ან/და მასში გაწერილი წესის შესაბამისად დადგენილ ინდიკატორზე მორეაგირე ქსელური ნაკადის ჩაწერის საშუალებას.

4. ქსელური სენსორის მიერ შესაგროვებელი მონაცემები

4.1. ქსელური სენსორი ორგანიზაციის ინფრასტრუქტურიდან აგროვებს შემდეგი ტიპის მონაცემებს:

4.1.1. სისტემური ლოგ ჩანაწერები;

4.1.2. სისტემური აპლიკაციებისა და სერვისების ლოგ ჩანაწერები;

4.1.3. ვირტუალური პლატფორმების და ვირტუალიზაციის წვდომისა და აქტივობის ლოგ ჩანაწერები;

4.1.4. DHCP სერვერის კავშირის (binding) ლოგ ჩანაწერები;

4.1.5. ფაერვოლის ლოგ ჩანაწერები;

4.1.6. მეილ სერვერზე წვდომისა და აქტივობის ლოგ ჩანაწერები;

4.1.7. ვებსერვერზე წვდომისა და აქტივობის ლოგ ჩანაწერები;

4.1.8. DNS ტრანზაქციის ლოგ ჩანაწერები;

4.1.9. ვებფილტრების წვდომისა და აქტივობის ლოგ ჩანაწერები;

4.1.10. მონაცემთა ბაზებზე წარმატებული და წარუმატებელი წვდომის ლოგ ჩანაწერები;

4.1.11. მონაცემთა ბაზებში მომხმარებელთა აქტივობის ლოგ ჩანაწერები;

4.1.12. მეტა ინფორმაცია ქსელური ნაკადის შესახებ (Flow);

4.1.13. ორგანიზაციის მიერ შემუშავებულ ან მართვაში გადაცემულ აპლიკაციებზე წვდომის ლოგ ჩანაწერები;

4.1.14. შესაბამისი აპარატული/პროგრამული გადაწყვეტილების შემთხვევაში, ქსელური ნაკადის ის ნაწილი, რომლის მეშვეობითაც გენერირდება განგაში, უშუალოდ ასეთი განგაშის გენერირების შემთხვევაში.

4.2. ამ პუნქტის 4.1.14. ქვეპუნქტით გათვალისწინებული შესაბამისი აპარატულ-პროგრამული გადაწყვეტილების არარსებობის შემთხვევაში, ორგანიზაცია ვალდებულია სააგენტოსთან შეთანხმდეს კონკრეტულ ვადაზე, რომლის განმავლობაშიც იგი ვალდებულია იქონიოს ასეთი აპარატული/პროგრამული გადაწყვეტილება.

4.3. ამ პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული ლოგ ჩანაწერები მოპოვებული უნდა იქნეს ლოგირების შემდეგი კატეგორიის/დონეების მიხედვით:

4.3.1. გაფრთხილების ლოგ ჩანაწერის კატეგორია/დონე (Warning Logging Level);

4.3.2. ინფორმაციული ლოგ ჩანაწერის კატეგორია/დონე (Informational Logging Level);

4.4. ამ პუნქტის 4.1.8. და 4.1.9. ქვეპუნქტებით გათვალისწინებული მონაცემები ორგანიზაციამ უნდა მოიპოვოს ფაერვოლის კონკრეტული პერიმეტრებით შეზღუდვის გარეშე.

4.5. ამ პუნქტის 4.1.14. ქვეპუნქტით გათვალისწინებული ნაკადის მონაცემის შენახვისას ორგანიზაცია, სათანადო ტექნიკური შესაძლებლობის შემთხვევაში, ვალდებულია ჩაწეროს უშუალოდ განგაშის

დამგენერირებელი ნაკადის პაკეტის წინ მდგომი პაკეტიდან მონაცემები ინციდენტის საბოლოო გამოკვლევამდე ან/და შესაბამისი საგამოძიებო მოქმედებების დასრულებამდე.

4.6. ორგანიზაცია ამ პუნქტის 4.1.8. ქვეპუნქტით გათვალისწინებული მონაცემების დასაგენერირებლად უნდა იყენებდეს საკუთარ ინფრასტრუქტურას.

4.7. ამ პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული ლოგ ჩანაწერები მოცემული უნდა იყოს გამჭვირვალე ლოგის (ე.წ. Transparent Logging) ფორმატში, რომლის ფარგლებშიც აღირიცხება მონაცემები კონკრეტული მოვლენის წარმომქმნელი რეალური წყაროს ან მიმართულებების შესახებ.

5. ქსელური სენსორის მიერ შეგროვებული მონაცემების შენახვის ფორმატები

5.1. ორგანიზაციას უფლება აქვს ქსელური სენსორის მიერ შეგროვებული მონაცემები შეინახოს მისთვის მისაღებ ნებისმიერ ფორმატში, თუმცა ორგანიზაციას უნდა გააჩნდეს მისი წაკითხვისა და ანალიტიკის დეტალური ინსტრუქცია.

5.2. ამ პუნქტის 5.1. ქვეპუნქტით გათვალისწინებული უფლების მიუხედავად, ორგანიზაცია ვალდებულია მის ინფრასტრუქტურაში განთავსებული ქსელური სენსორის მიერ შეგროვებული მონაცემები, გარდა ამ რეგლამენტის მე-4 პუნქტის 4.1.14. ქვეპუნქტისა, კონვერტირებადი იყოს .json, .cef და .csv სტრუქტურული სტანდარტის ფორმატებში.

5.3. ამ რეგლამენტის მე-4 პუნქტის 4.1.14. ქვეპუნქტით გათვალისწინებული მონაცემები კონვერიტირებადი უნდა იყოს .pcap ან/და .pcapng ფორმატში.

5.4. ამ რეგლამენტის მე-4 პუნქტის 4.1.12. ქვეპუნქტით გათვალისწინებული მონაცემები შესაძლოა ალტერნატიულად ინახებოდეს .pcap ან/და .pcapng ფორმატში.

6. ქსელური სენსორის მიერ შეგროვებული მონაცემების შენახვის ვადა

6.1. ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული ჩანაწერები ინახება მინიმუმ 90 დღის ვადით, გარდა ამავე პუნქტის 4.1.12 და 4.1.14 ქვეპუნქტებისა.

6.2. ამ რეგლამენტის მე-4 პუნქტით გათვალისწინებული ჩანაწერები, რომელიც უკავშირდება სააგენტოს ან ორგანიზაციის მიერ დადასტურებულ კომპიუტერულ უსაფრთხოების ინციდენტს ინახება მინიმუმ 5 წლის ვადით.

6.3. იმ შემთხვევაში, როდესაც ხორციელდება ინციდენტზე რეაგირება „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად, ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული მონაცემები ინახება ინციდენტის კვლევის დასრულებამდე, თუ კომპიუტერული უსაფრთხოების ინციდენტი საბოლოოდ გამოირიცხა. შეტევის დადასტურების შემთხვევაში გამოიყენება ამ პუნქტის 6.2. ქვეპუნქტით გათვალისწინებული ვადა.

6.4. ინციდენტის ფარგლებში, რომელზეც ხორციელდება სისხლის სამართლის გამოძიება, ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული მონაცემები ინახება სისხლის სამართლის საქმის შენახვის ვადით.

7. ქსელური სენსორის მიერ შეგროვებული მონაცემების შენახვის გარემო

7.1. ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული მონაცემები ინახება უშუალოდ ორგანიზაციის შიდა ინფრასტრუქტურაში, გარდა იმ შემთხვევისა, როდესაც ხორციელდება მათი გაზიარება სააგენტოსთან სავარაუდო ინციდენტის დადგენის ან მისი შემდგომი კვლევის გამოძიების მიზნით. მონაცემების გასაზიარებლად სააგენტო და ორგანიზაცია გამოიყენებს სპეციალურად საამისოდ შექმნილ ინფრასტრუქტურას, რომელიც მოიცავს სპეციალურ ოპტიკურ-ბოჭკოვან ქსელს, უსაფრთხო VPN კავშირებსა და აპლიკაციების პროგრამულ ინტერფეისებს.

7.2. იმ შემთხვევაში, როდესაც ორგანიზაციას გააჩნია სერვისები/ინფრასტრუქტურა ღრუბლოვან გარემოში, იგი ვალდებულია მოახდინოს ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით

გათვალისწინებული ლოგ ჩანაწერების სინქრონიზირებული შენახვა ლოკალურ გარემოში.

7.3. ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული მონაცემები უნდა ინახებოდეს ორგანიზაციის ძირითადი ქსელური ინფრასტრუქტურიდან ლოგიკურად და ფიზიკურად განცალკევებულ სერვერზე, რომელიც დაცული იქნება არავტორიზებული წვდომისგან და აღირიცხება მასზე განთავსებულ ინფორმაციაზე წვდომის კონტროლი.

7.4. სააგენტოსთან შეთანხმებით დროებით დასაშვებია ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული მონაცემების ღრუბლოვან გარემოში შენახვა იმ შემთხვევაში, თუ ორგანიზაციას აღნიშნული ვალდებულების დაკისრების კალენდარული წლისთვის არ გააჩნია შესაბამისი ფინანსური ხარჯები ან/და მოცემული ვალდებულების ჯეროვნად შესრულება უკავშირდება გარკვეულ დროსა და მნიშვნელოვან ძალისხმევას.

7.5. ამ პუნქტის 7.4. ქვეპუნქტით გათვალისწინებულ შემთხვევაში, ორგანიზაცია ვალდებულია შეუთანხმდეს სააგენტოს შემნახველი ღრუბლოვანი სისტემის კონკრეტულ უსაფრთხოების პირობებზე და ასევე ვადაზე, რა პერიოდშიც ორგანიზაცია ვალდებული იქნება დაასრულოს ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტში მოცემული მონაცემების მიგრაცია მისი ძირითადი ქსელური ინფრასტრუქტურიდან ლოგიკურად და ფიზიკურად იზოლირებულ სერვერზე.

8. ქსელური სენსორის და მასზე განთავსებულ ინფორმაციაზე წვდომის კონტროლი და მონიტორინგი

8.1. ქსელურ სენსორზე აუთენტიფიკაცია დასაშვებია მხოლოდ შიდა ქსელური გარემოდან (LAN) გარე ქსელში გაუსვლელად. გარე ქსელიდან კავშირი დასაშვებია იმ შემთხვევაში, თუ უფლებამოსილი პირი იყენებს დაცული და უსაფრთხო კავშირის ტექნოლოგიას, რომელიც უნდა ეფუძნებოდეს მათ შორის TLS შიფრაციის სტანდარტის საბოლოო ვერსიას.

8.2. ქსელურ სენსორსა და მასზე განთავსებულ ინფორმაციაზე წვდომის ყველა შემთხვევა უნდა აღირიცხებოდეს ფიზიკურად და ლოგიკურად განცალკევებულ სერვერზე, რომელზეც მონაცემების განთავსება და სინქრონიზაცია უნდა ხორციელდებოდეს არაუგვიანეს 24 საათისა. აღნიშნული ლოგ ჩანაწერი უნდა მოიცავდეს წვდომის დროსა და თარიღს, IP მისამართს, საიდანაც განხორციელდა წვდომა, წვდომის ხანგრძლივობას და სესიის დასრულების თარიღს.

8.3. ორგანიზაციის მიერ ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტში არსებული მონაცემების სააგენტოსთვის გადაცემის შემთხვევაში ამ პუნქტის 8.2. ქვეპუნქტით გათვალისწინებულ ლოგ ჩანაწერების დეტალებთან ერთად ასევე მიეთითება გადაცემული მონაცემის კონკრეტული ტიპი, მოცულობა, ფორმატი და ინციდენტის/განგაშის ნომერი, რომლის ფარგლებშიც მიეწოდა ეს მონაცემი.

8.4. სააგენტოს ამ მუხლის მოთხოვნათა შესრულების მონიტორინგის მიზნით შეუძლია როგორც გეგმიური, ისე არაგეგმიური საინფორმაციო ტექნოლოგიური შემოწმების განხორციელება და დარღვევის აღმოჩენის შემთხვევაში „ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონისა და მის საფუძველზე სააგენტოს უფროსის მიერ გამოცემული კანონქვემდებარე ნორმატიული აქტების შესაბამისად.

9. ქსელური სენსორის მიერ გენერირებული განგაშის ტიპები

9.1. სააგენტოს უფროსის 2022 წლის 11 მაისის №15 ბრძანებით დამტკიცებული პირველი ან მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელური სენსორის კონფიგურირების წესების 6.4.1 ქვეპუნქტით გათვალისწინებული მონაცემების გარდა, განგაშის სისტემას უნდა ჰქონდეს შესაძლებლობა დამატებით მიუთითოს სავარაუდო ინციდენტის კატეგორია, რომელიც შესაძლოა დაიყოს შემდეგ ტიპებად:

9.1.1. ადმინისტრატორის დონის (Root Level) კომპრომეტირება;

9.1.2. მოხმარებლის დონის კომპრომეტირება;

9.1.3. უკანონო წვდომის მცდელობა;

9.1.4. განაწილებული სერვისის მიუწვდომლობა (DDos);

9.1.5. სერვისის მიუწვდომლობა (Dos);

9.1.6. ღია პორტებისა და მოწყვლადობების მიზნობრივი სკანირება, თუ მას თან სდევს არასანქცირებული წვდომის მცდელობა;

9.1.7. ცნობილი მავნე კოდის გაშვება;

9.1.8. უცნობი კატეგორია (მაგ., ანომალია).

10. ქსელური სენსორის მიერ განგაშისა და მისი აქტივაციის შემდგომ რელევანტური მონაცემების მიწოდება სააგენტოსთვის

10.1. განგაშის გენერირების შემთხვევაში სააგენტოს ინციდენტების მართვის პლატფორმის მეშვეობით დაუყოვნებლივ მიეწოდება განგაშის ვერიფიცირებისთვის ან/და ინციდენტის გამოსაძიებლად საჭირო ლოგ ჩანაწერები ან/და გენერირებული ქსელური ნაკადის მონაცემი, რომლისთვისაც გამოიყენება ამ რეგლამენტის მე-7 პუნქტის 7.1. ქვეპუნქტით გათვალისწინებული ძალები და საშუალებები.

10.2. ამ რეგლამენტის მე-9 პუნქტის 9.1.1., 9.1.2. და 9.1.7. ქვეპუნქტებით გათვალისწინებული განგაშების შემთხვევაში, სააგენტოს პირველივე შესაძლებლობისთანავე მიეწოდება შესაბამისი ლოგ ჩანაწერები თავად განგაშის შეტყობინებასთან ერთად.

10.3. ამ რეგლამენტის მე-9 პუნქტის 9.1.3., 9.1.4., 9.1.5, 9.1.6 და 9.1.8. ქვეპუნქტებით გათვალისწინებული განგაშის შემთხვევაში სააგენტოს შესაბამისი ლოგირების ჩანაწერები მიეწოდება მხოლოდ მას შემდეგ, რაც ორგანიზაცია თავად გადაამოწმებს განგაშის სიგნალის რეალურობას და პირველადი კვლევით გამორიცხავს მის ცრუ დადებითობას.

10.4. ამ რეგლამენტის მე-9 პუნქტის 9.1.1., 9.1.2. და 9.1.7. ქვეპუნქტებით გათვალისწინებული განგაშების შემთხვევაში, სააგენტოს ქსელური ნაკადის ნაწილი, რომელმაც დააგენერირა მოცემული განგაში მიეწოდება მხოლოდ იმ შემთხვევაში, თუ მიწოდებული ლოგ მონაცემები გაანალიზდება და დადასტურდება განგაშის ნამდვილობა.

ქსელური სენსორის დამატებითი ფუნქციები

11. მომხმარებლის ანომალიური ქცევის ტიპები

11.1. ქსელური სენსორი ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული ინფორმაციის საფუძველზე ახორციელებს ორგანიზაციის ინფორმაციული უსაფრთხოების შესაბამისი პოლიტიკების მიხედვით, ქსელში არსებული თითოეული მომხმარებლის ქცევითი მოდელის შექმნას და რეაგირებს მისგან არსებითი გადახრის შემთხვევაში.

11.2. ამ პუნქტის 11.1. ქვეპუნქტით გათვალისწინებული მოდელიდან არსებით გადახრად ითვლება:

11.2.1. მაღალი პრივილეგიების არასაჭიროებისამებრ გამოყენება;

11.2.2. პრივილეგიების ამაღლება;

11.2.3. კონკრეტული მომხმარებლებიდან ორგანიზაციის ინფრასტრუქტურის გარეთ დიდი მოცულობის ან სხვაგვარად ანომალიური ქსელური ნაკადის მიმართვა;

11.2.4. მაავტორიზებელი მონაცემების მორგების მცდელობა;

11.2.5. ორგანიზაციის საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურის სენსიტიურ და შეზღუდულ ნაწილზე არაუფლებამოსილი წვდომა ან მისი მცდელობა;

11.2.6. სხვაგვარი ანომალიური ქცევა.

12. მაღალი პრივილეგიების არასაჭიროებისამებრ გამოყენება

12.1. დაუშვებელია ორგანიზაციის საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურის ადმინისტრატორების მიერ მათი პრივილეგიების გამოყენება საბაზისო უფლებების მქონე მომხმარებლების კუთვნილ საინფორმაციო აქტივებზე უნებართვო ან დაუსაბუთებელი წვდომისთვის.

12.2. ადმინისტრატორის პრივილეგიები განპიროვნებული უნდა იყოს მკაცრად განსაზღვრულ შესაბამისი ფუნქციური პროფილის თანამშრომლებზე, მისი გადაცემა დაუშვებელია სხვა პირზე. ადმინისტრატორის პრივილეგიების მქონე პირის მიერ დაუშვებელია მოცემული პრივილეგიის გამოყენება იმ რესურსებზე წვდომისთვის, რომლისთვისაც მოხმარებლის საბაზისო პრივილეგიები საკმარისია.

12.3. ორგანიზაციის ინფორმაციული უსაფრთხოების მენეჯერი ან/და კომპიუტერული უსაფრთხოების სპეციალისტი ვალდებულია შექმნას სპეციალური ლოგირების სისტემა მაღალი პრივილეგიების მქონე მომხმარებლებისთვის და რეგულარულად მოახდინოს მისი მონიტორინგი, ხოლო დაუსაბუთებელი ან უნებართვო წვდომის გამოვლენის შემთხვევაში მოახდინოს მისი მიზეზების კვლევა და ინციდენტის დადასტურების შემთხვევაში შეატყობინოს სააგენტოს და მიაწოდოს შესაბამისი ლოგ ჩანაწერები.

13. საბაზისო პრივილეგიების ამაღლება

13.1. ქსელურ სენსორს უნდა მიეწოდებოდეს ინფორმაცია ორგანიზაციის შიგნით მოხმარებელთა პრივილეგიების თაობაზე. ნებისმიერი ცვლილება იმ მოხმარებლებთან დაკავშირებით, რომლებიც სარგებლობენ საბაზისო პრივილეგიებით ცენტრალიზებული მართვის სისტემაში უნდა აგენერირებდეს სპეციალურ შეტყობინებას.

13.2. სპეციალური შეტყობინება საბაზისო პრივილეგიების მქონე მოხმარებლის უფლებებში ცვლილების თაობაზე, რომელიც არ არის დასაბუთებული და ადგილობრივი ადმინისტრატორის კონკრეტული გადაწყვეტილებით განხორციელებული, პირველივე შესაძლებლობისთანავე შესაბამისი განგაშის ფორმით უნდა მიეწოდოს სააგენტოს, ხოლო ასეთი შეტყობინება შესაბამის ლოგ ჩანაწერებთან ერთად დაუყოვნებლივ ეგზავნება ორგანიზაციის ინფორმაციული უსაფრთხოების მენეჯერსა და კომპიუტერული უსაფრთხოების სპეციალისტს.

14. კონკრეტული მომხმარებლებიდან ორგანიზაციის ინფრასტრუქტურის გარეთ დიდი მოცულობის ან სხვაგვარად ანომალიური ქსელური ნაკადის მიმართვა

14.1. ქსელურ სენსორს უნდა შეეძლოს განსაზღვროს ორგანიზაციის შიდა ქსელურ ინფრასტრუქტურაში არსებული მომხმარებლების მიერ ყოველდღიურად გენერირებული ქსელური ნაკადის მოცულობა და ასევე განსაზღვროს მისგან გადახრის დასაშვები ზღვარი. იმ შემთხვევაში, თუ დაფიქსირდება გადახრის დასაშვებ ზღვარზე მეტი რაოდენობით ქსელური ნაკადის გენერაცია გარკვეულ პერიოდში, ქსელური სენსორი სპეციალურ შეტყობინებას გაუგზანის ორგანიზაციის ინფორმაციული უსაფრთხოების მენეჯერსა და კომპიუტერული უსაფრთხოების სპეციალისტს.

14.2. ქსელური სენსორი ასევე უნდა განსაზღვრავდეს კონკრეტული მომხარებლის მიერ გენერირებული ქსელური ნაკადის მიმართულებას და ასევე ჰქონდეს გაწერილი იმ ქვეყნების სია, რომელშიც რეგისტრირებულ რესურსებზე მიმართვა წარმოადგენს ორგანიზაციისთვის მომეტებული საფრთხის წყაროს, თუმცა მიზანშეუწონელია მათი მასიური ბლანკეტური აკრძალვა.

14.3. ინფორმაციული უსაფრთხოების მენეჯერი და კომპიუტერული უსაფრთხოების სპეციალისტი ვალდებულნი არიან მოახდინონ ასეთი შემთხვევების მიზეზების კვლევა, ხოლო ინციდენტის დადასტურების შემთხვევა შეატყობინონ სააგენტოს და მიაწოდონ შესაბამისი ლოგ ჩანაწერები.

15. მაავტორიზებელი მონაცემების მორგების მცდელობა ან/და ანომალიურ პერიოდებში ან/და პერიოდით ორგანიზაციის შიგნით მომხმარებლის აქტივაცია

15.1. ქსელური სენსორი უნდა აფიქსირებდეს მაავტორიზებული მონაცემების მორგების მცდელობას და დასაშვები ზღვრის შემდგომ ავტომატურად ბლოკავდეს ავტორიზაციის დამატებით მცდელობებს,

რის შემდეგაც შესაბამის განგაშს უნდა აწვდიდეს ორგანიზაციის ინფორმაციული უსაფრთხოების მენეჯერსა და კომპიუტერული უსაფრთხოების სპეციალისტს.

15.2. ქსელურმა სენსორმა ასევე უნდა აღრიცხოს ორგანიზაციაში არსებული მომხარებლების აქტივაციის პერიოდები და ხანგრძლივობა, რის საფუძველზეც უნდა შეიმუშაოს თითოეული მომხმარებლის სათანადო ქცევითი მოდელი, რისგანაც არსებითი გადახრის შემთხვევაში უნდა დაგენერირდეს შესაბამისი შეტყობინება და მიეწოდოს ორგანიზაციის ინფორმაციული უსაფრთხოების მენეჯერსა და კომპიუტერული უსაფრთხოების სპეციალისტს.

15.3. ინფორმაციული უსაფრთხოების მენეჯერი და კომპიუტერული უსაფრთხოების სპეციალისტი ვალდებულნი არიან მოახდინონ ასეთი შემთხვევების მიზეზების კვლევა, ხოლო ინციდენტის დადასტურების შემთხვევა შეატყობინონ სააგენტოს და მიაწოდონ შესაბამისი ლოგ ჩანაწერები.

16. ორგანიზაციის საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურის სენსიტიურ და შეზღუდულ ნაწილზე არაუფლებამოსილი პირების წვდომა ან მისი მცდელობა

16.1. ქსელური სენსორის კონფიგურაციის დროს ინფორმაციული უსაფრთხოების მენეჯერი/კომპიუტერული უსაფრთხოების სპეციალისტი ვალდებულია განსაკუთრებით ღირებულ ან/და სენსიტიურ საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურის სეგმენტზე წვდომა უზრუნველყოს მხოლოდ ავტორიზებული პირებისა და მოწყობილობებისთვის, რომელთაც უნდა გააჩნდეს ასეთი წვდომის საჭიროება ყოველი კონკრეტული შემთხვევისთვის და იგი უნდა აღირიცხებოდეს შესაბამის ლოგ ჩანაწერებში, რომელზე დაყრდნობითაც უნდა შემუშავდეს უფლებამოსილი პირის ქცევითი მოდელის ნიმუში.

16.2. ორგანიზაციის საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურის სენსიტიურ და შეზღუდულ ნაწილზე არაუფლებამოსილი პირების წვდომის ან ანომალიურ პერიოდში (უფლებამოსილი პირის ქცევითი მოდელის ნიმუშიდან არსებითი გადახრა) წვდომის შემთხვევები აგენერირებს შესაბამის შეტყობინებას, რომელიც ინახება ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტით გათვალისწინებული მონაცემების ცენტრალიზებული შენახვისა და მართვის სისტემაში. აღნიშნული შეტყობინების გადამოწმების ვალდებულება გააჩნია ორგანიზაციის ინფორმაციული უსაფრთხოების მენეჯერს ან/და კომპიუტერული უსაფრთხოების სპეციალისტს.

16.3. ინფორმაციული უსაფრთხოების მენეჯერი და კომპიუტერული უსაფრთხოების სპეციალისტი ვალდებულნი არიან მოახდინონ ასეთი შემთხვევების მიზეზების კვლევა, ხოლო ინციდენტის დადასტურების შემთხვევა შეატყობინონ სააგენტოს და მიაწოდონ შესაბამისი ლოგ ჩანაწერები.

17. სხვაგვარი ანომალიური ქცევა

კრიტიკული ინფორმაციული სისტემის სუბიექტების ინფორმაციული უსაფრთხოების მენეჯერს ან/და კომპიუტერული უსაფრთხოების სპეციალისტს შეუძლიათ ქსელური სენსორი დააკონფიგურირონ იმდაგვარად, რომ იგი აიდენტიფიცირებდეს მომხმარებლის ანომალიური ქცევის ისეთ ტიპებს, რომელიც სახელდებით არ არის მოცემული ამ რეგლამენტში, თუმცა სრულად შეესაბამება მასში გათვალისწინებულ მიზნებს.

ქსელური სენსორის მართვა და დამატებითი კონტროლის ღონისძიებები

18. ქსელური სენსორის მართვა

18.1. ორგანიზაცია თავად განსაზღვრავს შესაბამისი წესებს და ტექნიკურ პოლიტიკებს, რომლის ინტეგრირებასაც ახდენს ქსელურ სენსორზე საკუთარ საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურაში არსებული ბიზნესპროცესების სპეციფიკის გათვალისწინებით.

18.2. ორგანიზაცია ვალდებულია უზრუნველყოს სააგენტოს მიერ ინფორმაციის შესაბამისი კლასიფიკაციით მიწოდებული კომპრომეტაციის ინდიკატორების (IP მისამართი, მავნე ფაილების ჰეშირებული მონაცემები, DNS ჩანაწერები, დომეინ სახელები, ქსელური კავშირები და დაკავშირებული მეტა მონაცემები) მეშვეობით საკუთარ საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურაში

მიმდინარე კომპრომეტირებული ან საეჭვო პროცესების ან/და ფაილების მოძიება და სააგენტოსთვის შეტყობინება არაუგვიანეს 72 საათისა გარდა იმ შემთხვევისა, როდესაც ორგანიზაციის აღნიშნული ინფრასტრუქტურა მოცულობითია და კონფიგურირებულია იმდაგვარად, რომ არ იძლევა საშუალებას მოცემული ინდიკატორებით კომპრომეტირებული/საეჭვო პროცესების სრულყოფილი ძებნა დასრულდეს 72 საათში. სააგენტო კომპრომეტაციის ინდიკატორებს ცენტრალიზებული ფორმით და თანადროულად უზიარებს ორგანიზაციას, რა მიზნითაც გამოიყენება ამ რეგლამენტის მე-7 პუნქტის 7.1. ქვეპუნქტით გათვალისწინებული საშუალებები.

18.3. ორგანიზაცია ვალდებულია უზრუნველყოს სააგენტოს მიერ მიწოდებული კომპრომეტაციის ინდიკატორების საკუთარ საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურაში იმპლემენტაცია (IP მისამართი, მავნე ფაილების ჰეშირებული მონაცემები, DNS ჩანაწერები, დომეინ სახელები, ქსელური კავშირები და მასთან დაკავშირებული მეტა მონაცემები) ამგვარი ინფორმაციის მიწოდებიდან არაუგვიანეს 72 საათისა, გარდა იმ შემთხვევისა, თუ ხსენებული დავალება მოცულობითია და მისი ავტომატური დამუშავება 72 საათში შეუძლებელია.

18.4. ქსელური სენსორის მართვის პროცესში ორგანიზაცია ვალდებულია მოახდინოს შესაბამისი განახლებების ინსტალაცია არაუგვიანეს 72 საათისა, გარდა იმ შემთხვევისა, თუ ეს განახლებები მოცულობითია და მისი სრულყოფილი იმპლემენტაცია საჭიროებს ორგანიზაციის საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურაში არსებით ცვლილებებს.

18.5. კრიტიკულ საინფორმაციო სისტემის სუბიექტს უფლება აქვს საკუთარი ქსელური სენსორი დააკონფიგურიროს ისე, რომ ამ რეგლამენტის მე-9 პუნქტში მითითებული ინციდენტები ავტომატურად დაიბლოკოს ან/და იმართოს.

18.6. სააგენტო უფლებამოსილია კრიტიკული საინფორმაციო სისტემის სუბიექტთან შეთანხმებით და მისი მონაწილეობით შემდგომი კვლევის მიზნით არ განახორციელოს ინციდენტის მყისიერი ბლოკირება მხოლოდ შემდეგი პირობების კუმულაციურად არსებობის შემთხვევაში:

18.6.1. ინციდენტის კვლევის ლეგიტიმური ინტერესი მაღალია ინციდენტის მხოლოდ ლოკალიზებისა და ნეიტრალიზაციის ინტერესთან მიმართებით;

18.6.2. ინციდენტის შედეგად ინფორმაციული აქტივი უკვე ხელყოფილია და არ არსებობს სხვა ინფორმაციული აქტივების ხელყოფის საფრთხე ან/და ასეთი საფრთხეები მინიმიზებულია ორგანიზაციისა და სააგენტოს ერთობლივი სამოქმედო გეგმით;

18.6.3. ინციდენტის სრულყოფილი მოკვლევა შეუძლებელია მის მიმდინარეობაზე რეალურ დროსა და გარემოში დაკვირვების გარეშე;

18.6.4. ინციდენტის რეალურ დროსა და გარემოში გამოძიება გრძელდება არაუმეტეს 6 თვისა.

18.7. იმ შემთხვევაში, თუ ინციდენტის შემდგომი კვლევის პროცესში დაირღვა ამ პუნქტის 18.5 ქვეპუნქტში მითითებული რომელიმე სავალდებულო პირობა, ინციდენტის რეალურ დროსა და სივრცეში გამოკვლევა წყდება და ხორციელდება კომპრომეტაციის პროცესის დაუყოვნებლივი აღკვეთა.

19. ქსელური სენსორის დამატებითი კონტროლის ღონისძიებები

19.1. ორგანიზაციის ქსელური სენსორიდან სააგენტოს ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტითა და მე-11 პუნქტის 11.2. ქვეპუნქტით გათვალისწინებული ინფორმაცია ეგზავნება დეპერსონალიზებული ფორმით და იგი ასევე არ უნდა მოიცავდეს მონაცემებს საბანკო გადარიცხვების შესახებ, გარდა იმ შემთხვევისა, როდესაც აღნიშნული მოთხოვნის შესრულება შეუძლებელია ორგანიზაციის შიდა ინფრასტრუქტურული მოწყობის ან/და დაკავშირებულია არაგონივრულ ძალისხმევასთან.

19.2. ამ პუნქტის 19.1 ქვეპუნქტის მიუხედავად, სააგენტოს შეუძლია ორგანიზაციას მოსთხოვოს ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტითა და მე-11 პუნქტის 11.2. ქვეპუნქტით გათვალისწინებული ინფორმაცია, რომელიც შეიცავს მათ შორის პერსონალურ ინფორმაციას იმ შემთხვევაში, თუ

სხვაგვარად შეუძლებელია ინციდენტის ყოველმხრივი და სრულყოფილი მოკვლევა.

19.3. ამ პუნქტის 19.2. ქვეპუნქტით გათვალისწინებული სიტუაციისას, სააგენტო შესაბამის შეტყობინებას უგზავნის პერსონალურ მონაცემთა დაცვის სამსახურს, რომელსაც უფლება აქვს შეამოწმოს აღნიშნული მონაცემების დამუშავების კანონიერება და „პერსონალური მონაცემების დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული სხვა მოთხოვნების შესრულება სააგენტოს მიერ.

19.4. სააგენტო ორგანიზაციიდან მიღებულ ამ რეგლამენტის გათვალისწინებულ მე-4 პუნქტის 4.1. ქვეპუნქტითა და მე-11 პუნქტის 11.2. ქვეპუნქტით გათვალისწინებული ინფორმაციის დამუშავებას აღრიცხავს შესაბამისი ლოგირების სისტემით, რომელშიც მიეთითება ორგანიზაციიდან მიღებული მონაცემის კონკრეტული ტიპი, მოცულობა, ფორმატი და ინციდენტის/განგაშის ნომერი, რომლის ფარგლებშიც მიეწოდა მას ეს მონაცემი.

19.5. ორგანიზაციიდან მიღებული ამ რეგლამენტის მე-4 პუნქტის 4.1. ქვეპუნქტითა და მე-11 პუნქტის 11.2. ქვეპუნქტით გათვალისწინებული ინფორმაციის არარელევანტურობის ან შენახვის ვადის გასვლის შემთხვევაში (სააგენტოს ან ორგანიზაციის მიერ დადასტურებულ შეტევასთან დაკავშირებულ ლოგ ჩანაწერები, ქსელური ნაკადი და მისი მეტა მონაცემები) სააგენტო ვალდებულია წაშალოს აღნიშნული ინფორმაცია და მისი ამსახველი ლოგირების მონაცემი ერთი კვირის ვადაში გადასცეს ამ ინფორმაციის მომწოდებელ ორგანიზაციას და ასევე პერსონალურ მონაცემთა დაცვის სამსახურს, თუ წაშლილი ინფორმაცია შეიცავს პერსონალურ მონაცემებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით დადგენილ ვადაში და წესით.

20. საპარლამენტო კონტროლი

სააგენტო ინციდენტის კვლევის ლეგიტიმური მიზნებისთვის ზიანის მიუყენებლად საქართველოს პარლამენტის თავდაცვისა და უშიშროების კომიტეტს წარუდგენს ყოველწლიურ მოხსენებას გამოვლენილი ინციდენტების თაობაზე მოქმედი კანონმდებლობით დადგენილი წესით.

გარდამავალი და დასკვნითი დებულებები

21. გარდამავალი დებულებები

ამ რეგლამენტის არცერთი ნორმა არ უნდა განიმარტოს იმდაგვარად, რომ იგი გულისხმობდეს ქსელური სენსორის მხოლოდ კომერციული მოდელების ინტეგრირებას პირველი და მეორე კატეგორიის კრიტიკული ინფორმაციული სისტემის სუბიექტების მხრიდან.