კომპიუტერულ ინციდენტზე შეტყობინების წესი

ტერმინთა განმარტება

ა) **სამინისტრო** - საქართველოს თავდაცვის სამინისტროს სტრუქტურული ქვედანაყოფები და მის სისტემაში შემავალი საჯარო სამართლის იურიდიული პირები.
ბ) **თანამშრომელი** - თავდაცვის სამინისტროს და მისი სტრუქტურული ერთეულების მოსამსახურეები/თანამშრომლები.
გ) **მარშრუტიზატორი** -მინიმუმ ერთი ქსელური ინტერფეისის მქონე სპეციალური ქსელური კომპიუტერი, რომელიც უზრუნველყოფს სხვადასხვა არქიტექტურის ქსელებსა და ქსელის სხვა და სხვა სეგმენტებს შორის მონაცემთა პაკეტების გადაგზავნაზე გადაწყვეტილების მიღებას, ქსელის ტოპოლოგიის და წინასწარ დადგენილი წესების მიხედვით.
დ) **სოციალური ინჟინერია** - გამოყენებითი სოციოლოგიის მიდგომათა ერთობლიობა, რომელიც ორიენტირებულია ადამიანის ქცევის, განწყობისა და მათზე კონტროლის მიზანდასახულ წარმართვაზე.
ე) **გამოთვლითი მანქანა** - თანამშრომლის პერსონალური კომპიუტერი.
ვ) **ლოკალური გამოთვლითი ქსელი** - წარმოადგენს სხვა და სხვა მოწყობილობების ერთობლიობას, რომლებიც დაკავშირებულია ერთმანეთთან და რომლის გავრცელების არეალს წარმოადგენს ერთი ან ერთმანეთთან ახლოს მდებარე რამდენიმე შენობა (სათავსო).
ზ) **კომპიუტერული ინციდენტი** - ინფორმაციული უსაფრთხოების პოლიტიკის რეალური ან პოტენციური დარღვევა, რომელიც ხორციელდება ინფორმაციული ტექნოლოგიის გამოყენებით და იწვევს ინფორმაციის უნებართვო წვდომას, გამჟღავნებას, დაზიანებას, შეფერხებას ან ინფორმაციული რესურსის მიტაცებას.
თ) **კონფიდენციალური ინფორმაცია** – ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას, სავარაუდოდ მოჰყვება კრიტიკული ინფორმაციული სისტემის სუბიექტის ფუნქციებისათვის მნიშვნელოვანი ზიანი და რომლის კონფიდენციალურ ინფორმაციად კლასიფიცირების მიზანია, ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას.
ი) **შინასამსახურებრივი გამოყენების ინფორმაცია** – ინფორმაცია, რომელიც განკუთვნილია მხოლოდ კრიტიკული ინფორმაციული სისტემის სუბიექტის თანამშრომლისათვის, ან/და მასთან სახელშეკრულებო ურთიერთობის მქონე პირისათვის, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფა, სავარაუდოდ, გამოიწვევს კრიტიკული ინფორმაციული სისტემის სუბიექტის მიერ თავისი ფუნქციების შესრულების მნიშვნელოვან შეფერხებას, ან ზიანს მიაყენებს სახელმწიფო ხელისუფლების ორგანოს უსაფრთხოებას, სახელმწიფო ინტერესს, ან კერძო პირის საქმიან რეპუტაციას და რომლის შინასამსახურებრივი გამოყენების ინფორმაციად კლასიფიცირების მიზანია, ინფორმაციული აქტივების მართვის წესების უზრუნველყოფა, გარდა იმ წესებისა, რომლებითაც საქართველოს ზოგადი ადმინისტრაციული კოდექსი განსაზღვრავს საჯარო ინფორმაციის ხელმისაწვდომობას.
კ) **მავნებელი პროგრამული უზრუნველყოფა (Virus, Malware)** - კრებითი სახელწოდება, ყველა ტიპის მავნე ფუნქციის მქონე თვითგამრავლებადი პროგრამისთვის, რომელიც თანამშრომლის სურვილის გარეშე ფუნქციონირებს სისტემაში, იწვევს ინფორმაციაზე

უნებართვო წვდომას, გამჟღავნებას, დაზიანებას, შეფერხებას ან ინფორმაციული რესურსის მიტაცებას.
ლ) ციფრული მოწყობილობა - მოწყობილობა, რომლის დანიშნულებაცაა ციფრულ ფორმატში ინფორმაციის მიღება, დამუშავება შენახვა ციფრული ტექნოლოგიების გამოყენებით.

კომპიუტერულ ინციდენტზე შეტყობინება

1. სსიპ - კიბერუსაფრთხოების ბიუროსთვის (შემდგომში - კიბერუსაფრთხოების ბიურო) კომპიუტერულ ინციდენტზე შეტყობინება შესაძლებელია შემდეგი მეთოდებით:

ა) სატელეფონო შეტყობინება, კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილების წინასწარ განსაზღვრულ ტელეფონის ნომრებზე;
ბ) ელექტრონული კითხვარის, სამინისტროს შიდა ქსელში არსებული კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე შეტყობინების ელექტრონული კითხვარის მეშვეობით;
გ) ელექტრონული ფოსტის საშუალებით, კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილების წინასწარ განსაზღვრულ ელექტრონული ფოსტის მისამართზე.

2. თანამშრომელი ვალდებულია შეატყობინოს კომპიუტერული ინციდენტის შესახებ კიბერუსაფრთხოების ბიუროს კომპიუტერულ ინციდენტებზე რეაგირების საკომუნიკაციო მომსახურების განყოფილებას შემდეგ შემთხვევებში:

ა) მის დაუკითხავად და სურვილის გარეშე ელექტრონულ ფოსტაზე იღებს არასასურველ სარეკლამო ან სხვა შინაარსის მატარებელ წერილებს;
ბ) გამოთვლით მანქანაზე აღმოჩენილია მავნებელი პროგრამული უზრუნველყოფა (Virus, Malware);
გ) სოციალური ინჟინერიის გამოყენებით პაროლების ან/და სხვა კონფიდენციალური ინფორმაციის მოპოვების მცდელობა. ტელეფონის, ელ-ფოსტის ან სხვა კომუნიკაციის საშუალებით, პაროლებთან, სისტემებთან ან/და ქსელთან დაკავშირებული ინფორმაციის შესახებ მონაცემების მიღების მცდელობა;
დ) გამოთვლითი მანქანიდან კონფიდენციალური ან/და შინასამსახურებრივი ინფორმაციის დაკარგვა, დაზიანება, ცვლილება;
ე) ციფრული მოწყობილობის დაკარგვა;
ვ) სისტემაში არასანქცირებული აქტივობის აღმოჩენა;
ზ) სისტემაზე არასანქცირებული დისტანციური წვდომის მცდელობა;
თ) პაროლი კომპრომეტირებულია;
ი) პროგრამებისა და აპლიკაციების ანომალიური აქტივობა (მაგ: აპლიკაციები ეშვება და იხურება ავტომატურად);
კ) წარუმატებელი აუტენტიფიკაციის მცდელობის გამო, სისტემის მიერ ანგარიშის დაბლოკვა, როდესაც ავტორიზებული თანამშრომელი არ ცდილობდა აუტენტიფიკაციის გავლას;

ლ) სისტემაში ისეთი ფუნქციების აქტივობა, რომლებიც ტიპიურად არ გამოიყენება თანამშრომელის მიერ;
მ) სისტემური შეცდომების დიდი რაოდენობა;
ნ) სისტემის ანომალურად შემცირებული წარმადობა;
ო) ოპერაციულ სისტემაში „მოციმციმე“ სარეკლამო ფანჯრები (Pop-Ups);
პ) კორპორატიული ლოკალური გამოთვლითი ქსელის სერვისების მასიური შეფერხება;
ჟ) ვებ-გვერდების იერსახის არასანქცირებული ცვლილება (Defacing);
რ) ქსელური დაცვის ეკრანის (Firewall) წესების დარღვევა;
ს) შემოჭრის აღმოჩენის და პრევენციის სისტემების (IDS/IPS) განგაში;
ტ) DoS ან DDoS შეტევა ვებ-გვერდზე ან ქსელურ მოწყობილობაზე;
უ) მარშრუტიზატორის სისტემურ ჟურნალში დაფიქსირებული არაავტორიზებული წვდომის მცდელობა ან/და არაავტორიზებული წვდომა;
ფ) პორტების ინტენსიური, გახშირებული სკანირება შიდა ან გარე ქსელიდან;
ქ) ქსელში არაავტორიზებული უსადენო მოწყობილობის აღმოჩენა;
ღ) სისტემაში დაფიქსირებული თანამშრომლის ანგარიშები, რომლებიც არ არის უფლებამოსილი პირის მიერ შექმნილი;
ყ) ფაილების უფლებების ცვლილება;
შ) არაავტორიზებული წვდომა სისტემურ ფაილებზე, სისტემური ფაილების ცვლილების მცდელობა.

კომპიუტერულ ინციდენტზე შეტყობინებისას დაუშვებელია:

ა) ერთი და იმავე შინაარსის რამდენიმე შეტყობინების გაგზავნა;
ბ) ცრუ ან/და არამიზნობრივი შეტყობინების გაგზავნა.

კომპიუტერული ინციდენტის აღმოჩენა:

1. კომპიუტერული ინციდენტის აღმოჩენისას:
ა) არ შეეცადოთ სისტემაში ცვლილებების შეტანას;
ბ) არ შეეცადოთ დამოუკიდებლად ინციდენტის აღმოფხვრას;
გ) ჩაიწეროთ, ჩაინიშნეთ ინფორმაცია მომხდარი ინციდენტის ან/და მიმდინარე პროცესების შესახებ.
დ) არ გათიშოთ კომპიუტერი, გამოაერთეთ ქსელის კაბელი კომპიუტერიდან, გათიშეთ უსადენო (Wireless) კავშირი.

2. იმ შემთხვევაში, თუ ვერ ხერხდება ინციდენტის მიკუთვნება ზემოთ ჩამოთვლილ ერთ-ერთ პუნქტთან, თანამშრომელი ვალდებულია, მომხდარის შესახებ შეატყობინოს საქართველოს შეიარაღებული ძალების გენერალური შტაბის სახმელეთო ჯარების კავშირგაბმულობის ცენტრის ინფორმაციული ტექნოლოგიების უზრუნველყოფის სამმართველოს ტექნიკური დახმარების განყოფილებას, ან შესაბამის პასუხისმგებელ სტრუქტურულ ერთეულს.