ორგანოები

შვეიცარიაში კიბერუსაფრთხოება ეროვნულ დონეზე უზრუნველყოფილია და კოორდინირებულია რამდენიმე სუბიექტის მიერ, მათ შორის: ეროვნული ეკონომიკური მიწოდების ფედერალური ოფისი (FONES): FONES პასუხისმგებელია შვეიცარიის კრიტიკული ინფრასტრუქტურის უსაფრთხოებისა და გამძლეობის უზრუნველყოფაზე, მათ შორის ენერგეტიკის, წყლისა და ტრანსპორტის სექტორებში. FONES მჭიდროდ თანამშრომლობს კრიტიკული ინფრასტრუქტურის ოპერატორებთან კიბერ საფრთხეების იდენტიფიცირებისა და შერბილების მიზნით და კოორდინაციას უწევს ეროვნულ რეაგირებას კიბერშეტევის შემთხვევაში. შვეიცარიის მოხსენებისა და ანალიზის ცენტრი ინფორმაციის უზრუნველყოფის მიზნით (MELANI): MELANI პასუხისმგებელია შვეიცარიაში კიბერ საფრთხეებისა და ინციდენტების შესახებ ინფორმაციის შეგროვებასა და ანალიზზე. MELANI აწვდის რჩევებსა და მხარდაჭერას კრიტიკული ინფრასტრუქტურის ოპერატორებს და სხვა დაინტერესებულ მხარეებს, თუ როგორ აღკვეთონ და უპასუხონ კიბერშეტევებს. MELANI ასევე ემსახურება როგორც ეროვნული საკონტაქტო პუნქტი კიბერ ინციდენტების მოხსენებისა და კოორდინაციისთვის. ფედერალური სადაზვერვო სამსახური (FIS): FIS პასუხისმგებელია შვეიცარიის ეროვნული უსაფრთხოების კიბერ საფრთხეების შესახებ ინფორმაციის შეგროვებაზე და სტრატეგიული რჩევების მიწოდებაზე სამთავრობო უწყებებსა და კრიტიკული ინფრასტრუქტურის ოპერატორებისთვის. კიბერუსაფრთხოების ფედერალური დელეგაცია (FCSD): FCSD პასუხისმგებელია ეროვნული კიბერუსაფრთხოების სტრატეგიებისა და პოლიტიკის შემუშავებასა და განხორციელებაზე. FCSD ასევე კოორდინაციას უწევს ეროვნულ ძალისხმევას კიბერშეტევების პრევენციისა და რეაგირებისთვის და მჭიდროდ თანამშრომლობს სხვა სამთავრობო უწყებებთან და კრიტიკული ინფრასტრუქტურის ოპერატორებთან, რათა უზრუნველყოს შვეიცარიის კიბერ ინფრასტრუქტურის უსაფრთხოება და გამძლეობა. ამ ერთეულების გარდა, შვეიცარიამ ასევე დაამყარა პარტნიორობა სხვა ქვეყნებთან და საერთაშორისო ორგანიზაციებთან, რათა ხელი შეუწყოს გლობალური კიბერუსაფრთხოების თანამშრომლობას და ინფორმაციის გაზიარებას. მაგალითად, შვეიცარია არის ევროკავშირის კიბერუსაფრთხოების სააგენტოს (ENISA) წევრი და მონაწილეობს სხვადასხვა საერთაშორისო კიბერუსაფრთხოების ფორუმებსა და ინიციატივებში.

კრიტიკული ინფრასტრუქტურის კრიტერიუმები

შვეიცარიაში კრიტერიუმები, რომლებიც განსაზღვრავს, ითვლება თუ არა კომპანია კრიტიკულ ინფრასტრუქტურად კიბერუსაფრთხოებაში, განსაზღვრულია ფედერალური აქტით კრიტიკული ინფრასტრუქტურის დაცვის შესახებ (PCI აქტი). PCI აქტის თანახმად, კრიტიკული ინფრასტრუქტურა განისაზღვრება, როგორც „ძირითადი ობიექტები, სერვისები და დანადგარები, რომლებიც ეროვნული მნიშვნელობისაა და რომელთა უკმარისობა ან გაუფასურება გამოიწვევს მნიშვნელოვან შედეგებს შვეიცარიის მოსახლეობის, ეკონომიკისა თუ უსაფრთხოებისთვის“.

იმის დასადგენად, განიხილება თუ არა კომპანია PCI აქტის მიხედვით კრიტიკულ ინფრასტრუქტურაში, შეიძლება განიხილებოდეს შემდეგი კრიტერიუმები:

არსებითობა: კომპანია გთავაზობთ სერვისებს ან ობიექტებს, რომლებიც აუცილებელია საზოგადოების ფუნქციონირებისთვის, როგორიცაა ელექტროენერგია, წყალი ან ტრანსპორტი.

ურთიერთდამოკიდებულება: კომპანიის სერვისები ან ობიექტები მჭიდროდ არის 0დაკავშირებული სხვა კრიტიკულ ინფრასტრუქტურულ სექტორებთან ან სერვისებთან, როგორიცაა ფინანსური სექტორი.

სირთულე: კომპანიის სერვისები ან დაწესებულებები ძალიან რთული და ძნელად ჩანაცვლებაა, როგორიცაა მოწინავე სამედიცინო დაწესებულებები ან კვლევითი დაწესებულებები.

შედეგები: კომპანიის მომსახურების ან ობიექტების წარუმატებლობა ან გაუფასურება მნიშვნელოვანი შედეგები მოჰყვება შვეიცარიის მოსახლეობას, ეკონომიკას ან უსაფრთხოებას.

მნიშვნელოვანია აღინიშნოს, რომ გადაწყვეტილება იმის შესახებ, განიხილება თუ არა კომპანია კრიტიკულ ინფრასტრუქტურად, მიიღება თითოეულ შემთხვევაში და საბოლოოდ განისაზღვრება შვეიცარიის კომპეტენტური ორგანოების მიერ. თუ კომპანია დადგინდა, რომ არის კრიტიკული ინფრასტრუქტურა, ის დაექვემდებარება დამატებით კიბერუსაფრთხოების მოთხოვნებს და ვალდებულებებს PCI აქტით.

კრიტიკული ინფრასტრუქტურა

შვეიცარიაში კიბერუსაფრთხოების კრიტიკული სექტორები განისაზღვრება ფედერალური აქტით კრიტიკული ინფრასტრუქტურის დაცვის შესახებ (PCI Act), რომელიც კრიტიკულ ინფრასტრუქტურას სამ კატეგორიად ყოფს: სექტორის სპეციფიკურ კრიტიკულ ინფრასტრუქტურას, სექტორთაშორისი კრიტიკული ინფრასტრუქტურა და ფედერალური კრიტიკული ინფრასტრუქტურა.

სექტორის სპეციფიკური კრიტიკული ინფრასტრუქტურის კატეგორია მოიცავს შემდეგ სექტორებს, რომლებიც კრიტიკულად ითვლება შვეიცარიაში კიბერუსაფრთხოებისთვის:

ენერგეტიკა: ეს სექტორი მოიცავს ელექტროენერგიის და გაზის წარმოებას, გადაცემას და განაწილებას.

წყალი: ეს სექტორი მოიცავს სასმელი და სანიტარული წყლის მიწოდებას, დამუშავებას და განაწილებას.

ტელეკომუნიკაციები: ეს სექტორი მოიცავს ინფორმაციის გადაცემას და გაცვლას სატელეკომუნიკაციო ქსელების მეშვეობით, როგორიცაა ინტერნეტი და მობილური ქსელები.

საბანკო და ფინანსები: ეს სექტორი მოიცავს ფინანსურ ინსტიტუტებსა და სისტემებს, რომლებიც მხარს უჭერენ შვეიცარიის ეკონომიკას, როგორიცაა ბანკები და საფონდო ბირჟები.

ჯანდაცვა: ეს სექტორი მოიცავს ჯანდაცვის დაწესებულებებს და სერვისებს, როგორიცაა საავადმყოფოები და სასწრაფო სამედიცინო მომსახურება.

ტრანსპორტი: ეს სექტორი მოიცავს ადამიანებისა და საქონლის გადაადგილებას საჰაერო, სახმელეთო და საზღვაო გზით, ასევე დაკავშირებულ ინფრასტრუქტურას, როგორიცაა აეროპორტები, პორტები და სარკინიგზო სისტემები.

საჯარო ადმინისტრირება: ეს სექტორი მოიცავს სამთავრობო უწყებებს და სისტემებს, რომლებიც უზრუნველყოფენ აუცილებელ სერვისებს მოქალაქეებისთვის, როგორიცაა პოლიცია, სასწრაფო დახმარების სამსახურები და კომუნალური მომსახურება.

განათლება და კვლევა: ეს სექტორი მოიცავს საგანმანათლებლო დაწესებულებებს და კვლევით ცენტრებს, რომლებიც მხარს უჭერენ შვეიცარიის ეკონომიკისა და საზოგადოების განვითარებას.

მედია: ეს სექტორი მოიცავს საკომუნიკაციო და საინფორმაციო სერვისებს, რომლებიც აწვდიან სიახლეებს და გართობას შვეიცარიის საზოგადოებისთვის.

აღსანიშნავია, რომ კიბერუსაფრთხოების კრიტიკული სექტორების კლასიფიკაცია შეიძლება შეიცვალოს ახალი საფრთხეების გაჩენის და ქვეყნის კიბერუსაფრთხოების საჭიროებების დროთა განმავლობაში განვითარებასთან ერთად.

ვალდებულებები

შვეიცარიაში კრიტიკული ინფრასტრუქტურის კომპანიების პასუხისმგებლობა კიბერუსაფრთხოების მიმართ განისაზღვრება ფედერალური აქტით კრიტიკული ინფრასტრუქტურის დაცვის შესახებ (PCI Act), რომელიც მოითხოვს კრიტიკული ინფრასტრუქტურის ოპერატორებს მიიღონ შესაბამისი ზომები, რათა უზრუნველყონ მათი სისტემებისა და მონაცემების დაცვა კიბერ საფრთხეებისგან.

კერძოდ, შვეიცარიაში კრიტიკული ინფრასტრუქტურის კომპანიებს მოეთხოვებათ:

ჩაატაროს რისკების შეფასება: კომპანიებმა უნდა შეაფასონ რისკები მათი სისტემებისა და მონაცემებისთვის და განახორციელონ შესაბამისი კიბერუსაფრთხოების ზომები მათი რისკის პროფილიდან გამომდინარე.

კიბერუსაფრთხოების შესაბამისი ზომების განხორციელება: კომპანიებმა უნდა განახორციელონ შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რათა დაიცვან თავიანთი სისტემები და მონაცემები კიბერ საფრთხეებისგან. ეს მოიცავს ზომებს, როგორიცაა წვდომის კონტროლი, დაშიფვრა და რეგულარული სარეზერვო ასლები.

შეატყობინეთ კიბერუსაფრთხოების ინციდენტების შესახებ: კომპანიებმა უნდა შეატყობინონ კიბერუსაფრთხოების ნებისმიერ ინციდენტს, რამაც შეიძლება გავლენა მოახდინოს მათი კრიტიკული ინფრასტრუქტურის ხელმისაწვდომობაზე ან მთლიანობაზე ინფორმაციის უზრუნველყოფის შვეიცარიის საანგარიშო და ანალიზის ცენტრს (MELANI).

თანამშრომლობა ხელისუფლებასთან: კომპანიებმა უნდა ითანამშრომლონ შვეიცარიის შესაბამის ორგანოებთან კრიტიკული ინფრასტრუქტურის დაცვის უზრუნველსაყოფად და კიბერუსაფრთხოების ნებისმიერ ინციდენტზე რეაგირებისთვის.

რეგულარულად გადახედონ და განაახლონ თავიანთი კიბერუსაფრთხოების ზომები: კომპანიებმა რეგულარულად უნდა განიხილონ და განაახლონ კიბერუსაფრთხოების ზომები, რათა უზრუნველყონ, რომ ისინი ეფექტური დარჩნენ განვითარებადი კიბერ საფრთხეების წინაშე.

ამ პასუხისმგებლობების შეუსრულებლობამ შეიძლება გამოიწვიოს სანქციები, ჯარიმები და სხვა სამართლებრივი შედეგები PCI აქტის მიხედვით.

მნიშვნელოვანია აღინიშნოს, რომ ეს პასუხისმგებლობები შეიძლება განსხვავდებოდეს კონკრეტული სექტორისა და კრიტიკული ინფრასტრუქტურის ხასიათის მიხედვით. კომპანიებმა უნდა გაიარონ კონსულტაცია შვეიცარიის შესაბამის ორგანოებთან, რათა დარწმუნდნენ, რომ ისინი ასრულებენ კიბერუსაფრთხოების შესახებ კანონით ნაკისრ ვალდებულებებს.

თავდასხმების კლასიფიკაცია

შვეიცარიაში კიბერშეტევის სიმძიმე კატეგორიზებულია ზემოქმედების დონის მიხედვით, რომელიც მას აქვს დაზარალებულ ორგანიზაციაზე, მის მომხმარებლებზე და ფართო საზოგადოებაზე. შვეიცარიის მოხსენებისა და ანალიზის ცენტრმა ინფორმაციის უზრუნველყოფის ცენტრმა (MELANI) დაადგინა კიბერშეტევების სიმძიმის ოთხი კატეგორია:

დონე 1 (დაბალი სიმძიმე): კიბერშეტევები, რომლებსაც აქვთ მცირე გავლენა დაზარალებულ ორგანიზაციაზე, როგორიცაა არაავტორიზებული წვდომის ცალკეული ინციდენტები ან მცირე მონაცემების დარღვევა. ამ შეტევებს, როგორც წესი, შეუძლია მიმართოს ორგანიზაციის შიდა IT გუნდს.

დონე 2 (საშუალო სიმძიმის): კიბერშეტევები, რომლებსაც აქვთ ზომიერი გავლენა დაზარალებულ ორგანიზაციაზე, როგორიცაა მონაცემთა მნიშვნელოვანი დარღვევა ან კრიტიკული სისტემების შეფერხებები. ამ შეტევებმა შეიძლება მოითხოვოს კიბერუსაფრთხოების ექსპერტების გარე მხარდაჭერა და შეიძლება გამოიწვიოს ბიზნეს ოპერაციების მცირე შეფერხება.

დონე 3 (მაღალი სიმძიმე): კიბერშეტევები, რომლებიც მნიშვნელოვან გავლენას ახდენენ დაზარალებულ ორგანიზაციაზე, როგორიცაა მონაცემთა ფართოდ გარღვევა, კრიტიკული სისტემების მნიშვნელოვანი შეფერხებები ან მგრძნობიარე ინფორმაციის ქურდობა. ეს თავდასხმები, როგორც წესი, მოითხოვს დაუყოვნებლივ მოქმედებას კიბერუსაფრთხოების ექსპერტებისგან და შეიძლება გამოიწვიოს ბიზნეს ოპერაციების მნიშვნელოვანი შეფერხება.

დონე 4 (ძალიან მაღალი სიმძიმე): კიბერშეტევები, რომლებიც სერიოზულ გავლენას ახდენენ დაზარალებულ ორგანიზაციაზე და მნიშვნელოვან საფრთხეს უქმნიან ეროვნულ უსაფრთხოებას, საზოგადოებრივ უსაფრთხოებას ან კრიტიკული ინფრასტრუქტურის ფუნქციონირებას. ეს თავდასხმები შეიძლება მოიცავდეს კრიტიკული მონაცემების ან სისტემების ქურდობას ან განადგურებას და შეიძლება მოითხოვოს სამართალდამცავი და ეროვნული უსაფრთხოების სააგენტოების ჩართვა.

მნიშვნელოვანია აღინიშნოს, რომ კიბერშეტევის სიმძიმე შეიძლება განსხვავდებოდეს კონკრეტული გარემოებებისა და ორგანიზაციის რისკის პროფილის მიხედვით. თუმცა, ეს კატეგორიები იძლევა ჩარჩოს კიბერშეტევის გავლენის შესაფასებლად და შესაბამისი რეაგირების განსაზღვრისთვის.

სანქციები

შვეიცარიაში, კრიტიკული ინფრასტრუქტურის კომპანიებს, რომლებიც ვერ ასრულებენ კიბერუსაფრთხოების მოთხოვნებს, შეიძლება დაეკისრონ რამდენიმე სანქცია, მათ შორის:

ჯარიმები: კომპანიებს, რომლებიც არ ასრულებენ კიბერუსაფრთხოების მოთხოვნებს, შესაძლოა დაჯარიმდნენ. ჯარიმის ოდენობა შეიძლება დამოკიდებული იყოს დარღვევის სიმძიმეზე და კომპანიის ზომასა და შემოსავალზე.

ოპერაციული შეზღუდვები: ზოგიერთ შემთხვევაში, შვეიცარიის ხელისუფლებამ შეიძლება დააწესოს ოპერაციული შეზღუდვები კრიტიკული ინფრასტრუქტურის კომპანიებზე, რომლებიც არ ასრულებენ კიბერუსაფრთხოების მოთხოვნებს. ეს შეიძლება მოიცავდეს კომპანიის წვდომის შეზღუდვას გარკვეულ სისტემებსა თუ ქსელებზე ან კომპანიისგან უსაფრთხოების კონკრეტული ზომების განხორციელების მოთხოვნას.

ლიცენზიების შეჩერება ან გაუქმება: კრიტიკულ ინფრასტრუქტურულ კომპანიებს, რომლებიც ვერ ასრულებენ კიბერუსაფრთხოების მოთხოვნებს, შეიძლება ლიცენზია შეუჩერონ ან გაუქმდნენ. ამან შეიძლება ხელი შეუშალოს კომპანიას გარკვეულ სექტორებში ოპერირებაში ან გარკვეული ტექნოლოგიების გამოყენებაში.

სისხლისსამართლებრივი დევნა: იმ შემთხვევებში, როდესაც კიბერშეტევა კრიტიკულ ინფრასტრუქტურაზე მნიშვნელოვან ზიანს აყენებს საზოგადოებას ან ეროვნულ უსაფრთხოებას, დამნაშავე შეიძლება დაექვემდებაროს სისხლისსამართლებრივ დევნას.

მნიშვნელოვანია აღინიშნოს, რომ კონკრეტული სანქციები, რომლებიც შეიძლება დაწესდეს კრიტიკული ინფრასტრუქტურის კომპანიებს კიბერუსაფრთხოების დარღვევისთვის, შეიძლება განსხვავდებოდეს გარემოებებისა და დარღვევის სიმძიმის მიხედვით. შვეიცარიის ხელისუფლებამ შესაძლოა გაითვალისწინოს კომპანიის ძალისხმევა კიბერუსაფრთხოების მოთხოვნებისა და კიბერუსაფრთხოების ზოგადი მდგომარეობის შესასრულებლად შესაბამისი სანქციების დადგენისას.