სამფაქტორიანი აუტენტიფიკაცია - ნდობის დონის ამაღლება

დავით გომელაური, კორნელი ოდიშარია, თინათინ კაიშაური
საქართველოს ტექნიკური უნივერსიტეტი

რ ე ზ უ მ ე

თანამედროვე საქმიანობა წარმოუდგენელია საინფორმაციო სისტემების გამოყენების გარეშე. ასეთი სისტემების ინფორმაციული უსაფრთხოება ორგანიზაციის საქმეთა წარმოების ერთ-ერთ გადამწყვეტ ფაქტორს წარმოადგენს. ორგანიზაციის განვითარებასთან ერთად რთულდება მისი საინფორმაციო სისტემა და ინფორმაციის მთლიანობის დარღვევამ შეიძლება გამოიწვიოს კატასტროფული შედეგები. ნაშრომში განხილულია ინფორმაციის დაცვის კონკრეტული მექანიზმი- სამფაქტორიანი აუტენტიფიკაცია ნდობის დონის და ინფორმაციის დაცვის დონის ამაღლების მიზნით.

1. შესავალი

ჩვენ ვცხოვრობთ ტოტალური ციფრული ტექნოლოგიების საუკუნეში. ინფორმაციული სისტემები განიცდიან უწყვეტ სრულყოფა - გართულებას, მათში სულ უფრო მეტი კრიტიკულად მნიშვნელოვანი, კონფიდენციალური ინფორმაცია ბრუნავს და ყოველგვარი ძალდატანების გარეშე შეიძლება ითქვას, რომ დღეს ნებისმიერი კომპანიისათვის ამ ინფორმაციის მოპოვება, დაკარგვა ან დამახინჯება - ძალზე სერიოზული დარტყმაა, რაც შეიძლება საწარმოომ ვერც კი გადაიტანოს.

ხატოვნად რომ ვთქვათ, თანამედროვე ბიზნესი - 80% ინფორმაციაა, რომელიც ცირკულირებს მის ყველა შესაძლო კომპიუტერული და ტელესაკომუნიკაციო სისტემებში. ბუნებრივია, მომხმარებელთა იდენტიფიკაცია და აუდენტიფიკაცია დგას ყველაზე უფრო აქტუალურ საკითხების რიგში. ბოროტგანმზრახველი, რომელმაც შეძლო თავის გასაღება ლეგიტიმურ მომხმარელად, ღებულოს დაშვებას ინფორმაციული სიმდიდრეებთან, ძვირადღირებული ინფორმაციული უსაფრთხოების (იუ) სისტემის გვერდის ავლით. აქედან გამომდინარე, განხილული იქნება უმნიშვნელოვანესი პრობლემები და ძირითადი მოქმედებათა მიმართულებები მოცემულ სფეროში.

2. ძირითადი ნაწილი

თუ გავიხსენებთ თუ რა იყო 15 წლის წინ, მაშინ ჩვენ ვნახავთ, რისგან დაიწყო თანამედროვე აუტენტიფიკაციის სისტემები. ყველა ისინი ეფუძნებოდა ისეთ მარტივ და გასაგებ მექანიზმს, როგორიცაა ლოგინი და პაროლი (Login- სისტემაში შესვლა). წყვილი ლოგინს + პაროლი იყო ის ძირითადი რამ, რომელსაც ეფუძნებოდა იდენტიფიკაცია და აუტენტიფიკაცია ყველა ინფორმაიცლ სისტემაში. დროთა განმავლობაში რისკი იზრდებოდა და მიჩვეული მიდგომა იქცა არადამაკმაყოფილებლად. ასე გაჩნდა ცნება ორფაქტორიანი აუტენტიფიკაციისა, და პრინციპის „მე ვიცი საიდუმლო პაროლი), ამიტომ მე ვარ ის ვისად თავს ვასაღებ“ სანაცვლოდ მოვიდა ახალი: „მე ვიცი საიდუმლო (პაროლი ან პინკოდი) და ამასთან ერთად მე გამაჩნია უნიკალური ფიზიკური იდენტიფიკატორი (ტოკენი, სმარტ - ბარათი და ა. შ.), ამიტომ მე ვარ ის ვისად თავს ვასაღებ“, თავის დროზე სწორედ მეორე ფაქტორის გამოჩენა იქცა სერიოზულ ნაბიჯად წინ გაგადგმული. რამაც შესაძლებელი გახადა აუტენტიფიკაციის სანდოობის საჭირო დონეზე აწევა - იუ - ს რისკების თვალსაზრისით.

დღეს ჩვენ მოწმე ვართ იმისა, რომ ხდება ტოტალური გადასვლა 0 აუტენტიფიკაციის ორ ფაქტორიან მოდელზე. შეიძლება ისიც ითქვას, რომ ჩვენ მივუახლოვდის მობრუნების პუნქტს: ორფაქტორიანი აუტენტიფიკაციის იდეასთან მივიდნენ მსოფლიო გიგანტი - კომპანიები. ცოტა ხნის წინანდელი განცხადება Google - ის უსაფრთხოების დარგში ვიცე - პრეზიდენტის ერიკ

გროსი (Eric Grosse) ლაპარაკობს იმაზე, რომ აუტენტიფიკაციის მომქმედი მეთოდები, რომლებიც დაფუძნებულია წყვილზე ლოგინი/პაროლი იქცნენ სრულიად დისკრედიტირებულად - ამის დადასტურებაა. სწორედ ოოგლე სერვისების ფარგლებში ორფაქტორიანი აუტენტიფიკაციის დანერგვა შეიძლება იქცეს გარდამტეხ მომენტად, რომლის შემდეგაც ჩვენ ვნახავთ მომხმარებლების მასობრივ გადასვლას აუტენტიფიკაციის ორფაქტორიან მოდელზე - ტოკენების გამოყენებით.

ამასთან ერთად აღწერილი პროცესის პარალელურად წარმოშობიან აუდენტიფიკაციის სფეროში კიდევ უფრო საინტერესო ტენდენციები. ზოგიერთი ექსპერტი იუ - ს სფეროში და მთელი რიგი კომპანიებისაც კი ალაპარაკდნენ მრავალფაქტორიან აუდენტიფიკაციაზე. გავეცნოთ ამ ტენდენციებს უფრო დეტალურად. ზოგადად რომ ვთქვათ, აუტენტიფიკაციის საკითხი - ესაა ნდობის საკითხთა მრავალფაქტორიანი აუტენტიფიკაციის იდეა გულისხმობს პროცესში დამატებითი ფაქტორების შემოღება შემოწმებისათვის, რითაც მაღლდება ნდობის დონე. პაროლისა და უნიკალური გასაღების მატარებლის გარდა, აუტენტიფიკაციის პროცესს ერთვება ისეთი მონაცემები როგორიცაა, მაგალითად, გეოლოკაციური მონაცემები, რომლებიც აფიქსირებენ მომხმარებლის ადგილსამყოფელს, დღე - ღამის დრო, ბიომეტრიული მონაცემები, ყოფაქცევითი ალგორითმები და ა. შ. ყველაფერი ეს საშუალებას იძლევა ამაღლდეს ნდობა მომხმარებლის მიმართ, ამაღლდეს ალბათობა იმისა, რომ ის ვინც ითხოვს დაშვებას, არა შენიღბული ბოროტგანმზრახველია, არამედ ლეგიტიმური მომხმარებელია.

ასეთი ღონისძიებების აქტუალობს მომდინარეობს იქიდან, რომ ზოგიერთი ინფორმაციული სისტემები იქცნენ ძალზე მნიშვნელოვან და ღირებულ სისტემებად, ხოლო ფინანსური შედეგები ასეთი სისტემების დაშვების კომპრომეტაციისა შეიძლება იყოს ძალზე მტკივნეული.მეორეს მხრივ მრავალფაქტორიან აუტენტიფიკაციას შეუძლია უზრუნველყოს არსებითი პლუსები დაშვების მართვის თვალსაზრისით, გადაწყვეტის იდეა ეფუძნება აუტენტიფიკაციის პროცესში დამატებითი მონაცემების ჩართვას, მაგალითად მომხმარელის ადგილსამყოფელი კომპანიის ოფისში.

განვიხილოთ რეულური ინციდენტი, რომელიც გამოიხატა კომპანიის ანგარიშიდან თანხის მოხსნაში - მოპარვაში. მას შემდეგ რაც ფაქტი იქნა აღმოჩენილი, დაიწყო შიდა გამოძიება, რომელმც ანახა, რომ კომპანიამ ფაქტიურად ფული დაკარგა ფულად გადახდაში რომელიღაც დაუდგენელ ფირმაზე. სისტემა „ბანკი - კლიენტი“ ურყევად ამტკიცებდა, რომ ამ ფულად გადასახადს ხელი პირადად მთავარმა ბუღალტერმა მოაწერა - თავისი ტოკენის წარმდგენით ე. ხელისმოწერით. ბუღალტერი იფიცებოდა, რომ მას ეს არ გაუკეთებია, და უფრო მეტიც, ამ დრომ იმყოფებოდა სასადილოში, თანაც ბევრმა კოლეგამ ეს დაადასტურა. გამოირკვა, ბუღალტერი მიდიოდა რა სადილზე, თავის ტოკენი ელ. ხელმოწერით დატოვა მიერთებულ ჩართულ კომპიუტერზე და პოტენციური ბოროტგანმზრახველისათვის არავითარ სირთულეს არ წარმოდგენდა მისთვის საჭირო ოპერაციის ჩატარება. ვიდეოთვალთვალის კამერები ბუღალტერის ოთახში არ იყო დაყენებული, ამიტომ შემოწმება ქურდული მოქმედებებისა ვერ მოხერხდა. მიუხედავად ამისა დაშვების კონტროლისა და მართვის სისტემის (დკმს) მიერ მოგროვილი მონაცემებით, ასევე ჩანაწერებით კამერებიდან შესაძლებელი გახდა დადგენილიყო წრე იმ ადამიანებისა, რომლებიც ამ დროს შესაძლებელი იყო ყოფილიყვნენ ბუღალტრის კაბინეტში.

ეს მაგალითი გახდა ბიძგი ახალი იდეისა, მომხდარიყო აუტენტიფიკაციის სისტემის ინტეგრაცია დკმს - თან. უნდა გაკეთებულიყო ისე, რომ ბუღალტერს არ შეეძლოს გამოსვლა კაბინეტიდან თუ არ გამორთავდა თავის ტოკენს კომპიუტერიდან და თან არ წაიღებდა და ვერ იმუშავებდა ბანკ - კლიენტთან, თუ არ გაივლიდა დკმს - ის გადამწოდებს ბუღალტრის კაბინეტის კარების გავლით.

სამ ფაქტორიანი აუტენტიფიკაციის სქემის რეალიზაციამ მოითხოვა შეთავსება ფუნქციონალისა IDM - სისტემის (სააღრიცხვო ჩანაწერები) მართვა საინფორმაციო სისტემებში). PKI მართვის სისტემის (ღია გასაღებების ინფრასტრუქტურის) და ნაგებობაში დაშვების ფიზიკური კონტროლის სისტემის დკმს. შესაძლებელი გახდა წარმატებული შეთავსება ადრე დამოუკიდებელი პროცესებისა დაშვების ლოგიკური და ფიზიკური კონტროლისა, რისთვისაც გამოყენებული იქნა უნივერსალური მატარებელი (ტოკენები და სმარტ - ბარათები RFID ნიშნულებით), რომელიც რეაგირებს თანამშრომლის შესვლაზე ოფისში დკმს - ის გავლით, ასევე მომხმარებლების მიერ საკუთარი კომპიუტერების ჩასართავად და ინფორმაციულ სისტემებში შესასვლელად. აღნიშნული სისტემა დაშვების მართვისა აღმოჩნდა საკმაოდ მოქნილი და მარტივი დასანერგად. მოხერხებულობა სახეზეა, მაგრამ პრობლემა პერსონალის გულგრილი დამოკიდებულებისა ინფორმაციული უსაფრთხოების პოლიტიკისადმი თავისთავად წყდება - თუ არ ამოიღებს კონკრეტული პირი თავის ტოკენს კომპიუტერიდან ის ვერ გავა კაბინეტიდან და შესაბამისად, თუ ის არ შევა დკმს - ის გავლით საკუთარ კაბინეტში, ვერ მიიღებს დაშვებას ინფორმაციულ სისტემებთან, ვინაიდან ისინი იქნებიან მისთვის დაბლოკილები. იდეა ინტერესით იქნა მიღებული მომხმარებლების მიერ დკმს რომ პრაქტიკულად არის კომპანიის ყველა ოფისში და ეს სისტემა ყოველგვარი გლობალური გადაკეთების გარეშე შეიძლება იქცეს დამატებით წყაროდ ინფორმაციის უსაფრთხოების საკითხის გადასაჭრელად. უფრო მეტიც, იდეამ წარმოაჩინა დამატებითი შესაძლებლობები, ასე მაგალითად, აუტენტიფიკაციისადმი ასეთი მიდგომა საშუალებას იძლევა მოხდეს დაცვის უპასუხისმგებლო თანამშრომლებისაგან, რომლებიც შორიდან ერთვებიან კორპორაციულ ინფორმაციულ სისტემებში, საყოველთაოდ ხელმისაწვდომი ქსელებიდან (ღია WiFi- ი კაფეებში და აეროპორტებში). მათი დაშვება არ განხორციელდება, თუ იუ - ს პოლიტიკა მოითხოვს კრიტიკულ სისტემებთან მუშაობას მხოლოდ ოფისის შიგნიდან.

აქვე უნდა აღინიშნოს, რომ დაშვების მართვის ეფექტური სისტემის აგება ყოველთვის დაკავშირებულია მოვლენებთან, რომლებიც მიმდინარეობენ საკადრო სამსახურში. სწორედ კადრების სამსახურმა იცის ნათლად, რომელი თანამშრომელი სად და რა თანამდებობაზე მუშაობს, რომელი მათგანია მივლინებაში, შვებულებაში, რომელია დათხოვნილი და ა. შ. აღნიშნული ინფორმაციის გათვალისწინება კიდევ უფრო გაზრდის ნდობის აუტენტიფიკაციის პროცესისადმი.

3. დასკვნა

იდენტიფიკაცია, აუტენტიფიკაციის სისტემები თანამედროვე პირობებში განიცდიან ტრანსფორმაციას და რთულდებიან, ხდება მათი მორგება ცვლად პირობებთან. მოყვანილი მაგალითები მიგვანიშნებს, რომ დაშვების მართვის თანამედროვე სისტემებს შეუძლიათ უზრუნველყონ არა მარტო მაღალი დონე ინფორმაციული უსაფრთხოების, არამედ არსებითად აამაღლონ მომხმარებლისათვის ეფექტურობა და მოხერხებულობა.

ლიტერატურა:

1. Анин Б.Ю. Защита компьютерной информации. СПБ. Петербург. 2010. ISBN 5-8206-0104-1
2. Multifactor authentication - http://en.wikipedia.org/wiki/Multi-factor_authentication
3. Stang D.J., Moon S. Network Security Secrets. IDG Books Worldwide 2009

THREE FACTOR AUTHENTICATION - INCREASE CONFIDENCE LEVEL

Gomelauri David, Odisharia Korneli, Kaishauri Tinatin
Georgian Technical University

Summary

In the modern business environment information systems are actively applied. Therefore information security becomes one of key factors in organization's business processes. In development process of an organization its information system becomes complicated and destruction of integrity of information may cause catastrophic consequences for the business activity. In the article is described a specific mechanism of protection of information-such as three factor authentication for increasing confidence and information security levels.

ТРЁХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ- УВЕЛИЧЕНИЕ УРОВНЯ ДОВЕРИЯ

Гомелаури Д., Одишария К., Каишаури Т.
Грузинский Технический Университет

Резюме

В современном деловом мире активно используются информационные системы. В связи с этим информационная безопасность становится одним из решающих факторов делопроизводство организации. По мере развития организации усложняется её информационная система и разрушение целостности информации может привести катастрофическим последствиям для организации. В статье описывается конкретный механизм защиты информации - трёхфакторная аутентификация для повышения уровня доверия и информационные безопасности.