Scientific and Practical Cyber Security Journal (SPCSJ) 7(1): 31-37 ISSN 2587- 4667 Scientific Cyber Security Association (SCSA)

ორწერტილოვანი დაშიფვრის საჭიროება ფინანსურ ტრანზაქციებში

დიანა პოპოვა, სამეცნიერო კიბერ უსაფრთხოების ასოციაცია
ოქსანა კოვალჩუკ, სახუმის უნივერსიტეტი

THE NEED OF POINT-TO-POINT ENCRYPTION IN FINANCIAL TRANSACTIONS

Diana Popova, Scientific Cyber Security Association

Oksana Kovalchuk Sokhumi State University

აბსტრაქტი: დღეს, როგორც არასდროს, მომხმარებლებს სურთ ისარგებლონ სწრაფი და უსაფრთხო გადახდის საშუალებებით. ამავდროულად, ბიზნესმა უნდა დაიცვას მომხმარებლის მონაცემები. მაგრამ მუდმივად ცვალებადმა მოთხოვნამ და გადახდის ტექნოლოგიამ გაზარდა ბიზნესის ოპერაციული და ტექნიკური სირთულე.

ფედერალური ფინანსური ინსტიტუტების ექსპერტიზის საბჭოს მიერ გამოქვეყნებული IT Examination Handbook-ს სახელმძღვანელოს მიხედვით, ფინანსურმა ინსტიტუტებმა ინფორმაციის შენახვისა და ტრანზიტის დროს მგრძნობიარე ინფორმაციის გამჟღავნების ან ცვლილების რისკის შესამცირებლად უნდა გამოიყენონ დაშიფვრა.

ორწერტილოვანი დაშიფვრა (P2PE) იცავს ბარათის მფლობელთა მონაცემებს, უადვილებს ორგანიზაციებს გადახდის მონაცემების უსაფრთხოდ შენახვას და ეხმარება მათ PCI SSC (Payment Card Inductry Security Standards Council) შესაბამისობის მოთხოვნების და უსაფრთხოების უახლესი სტანდარტების დაცვაში, რაც ამცირებს თაღლითობის რისკს.

P2PE სტანდარტების გამოყენება ცალკეული კომპანიების პასუხისმგებლობაა, რომლებიც სთავაზობენ პროდუქტებსა და სერვისებს ამ სტანდარტების გამოყენებით, და არა თავად PCI SSC მმართველი საბჭოსი. გადახდის სისტემების მოთხოვნების დამსახურებით PCI SSC სტანდარტები ხორციელდება უამრავ ორგანიზაციაში, მაგრამ ისინი არ არის გათვალისწინებული სახელმწიფო დონეზე, როგორც სავალდებულო. რიგი ფაქტორების გაანალიზების შემდეგ შეგვიძლია ვთქვათ, თარლითობის რისკის მინიმუმამდე დასაწევად, საჭიროა მიღებული სტანდარტები გავხადოთ სავალდებულო ყველა ორგანიზაციისთვის. სტატიაში ასევე მოცემულია რეკომენდაციები მომხმარებლისათვის თაღლითური სქემის თავიდან ასარიდებლად.

საკვანძო სიტყვები: *დაშიფვრა, მონაცემები, უსაფრთხოება, ფინანსური*

ABSTRACT: Today, more than ever, consumers need fast and secure payment options. At the same time, businesses must protect customer data. But ever-changing demand and payment technology have increased the operational and technical complexity of business.

According to the IT Examination Handbook published by the Federal Financial Institutions Examination Board, financial institutions must use encryption in storage and transit to reduce the risk of exposure or alteration of sensitive information.

Point-to-point encryption (P2PE) protects cardholder data, makes it easier for organizations to secure payment data, and helps them meet PCI SSC (Payment Card Industry Security Standards Council) compliance requirements and the latest security standards, reducing the risk of fraud.

The use of P2PE standards is the responsibility of the individual companies that offer products and services using those standards, not the PCI SSC Governing Board itself. Thanks to the requirements of payment systems, PCI SSC standards are implemented in many organizations, but they are not considered mandatory at the state level. After analyzing a number of factors, we can say that in order to minimize the risk of fraud, we need to make the accepted standards mandatory for all organizations. The article also provides recommendations for consumers to avoid fraudulent schemes.

KEYWORDS: *encryption, data, security, financial*

შესავალი

დღეისათვის რადიკალური ცვლილებები ხდება ფინანსური ტექნოლოგიების სფეროში, რაც გავლენას ახდენს სექტორის მთელ ინფრასტრუქტურაზე და ასოცირდება ავტომატიზაციის, ღიაობისა და მომხმარებელზე ფოკუსირების დონის მატებასთან. ხელოვნური ინტელექტის ტექნოლოგიების განვითარება, დიდ მონაცემთა დამუშავება, ახალი ანალიტიკური ინსტრუმენტები და ღრუბლოვანი სერვისები ხელს უწყობს მომხმარებლის მომსახურების ხარისხის ახალ დონეზე გადასვლას. პრაქტიკულად შესაძლებელია ნებისმიერი ფინანსური ტრანზაქცის განხორციელება მობილური მოწყობილობის გამოყენებით, რომელიც უზრუნველყოფს პირადი ფინანსური მენეჯმენტის, ბიომეტრიული გადახდების, სოციალური გადახდების და ა.შ. შესაძლებლობებს.

ონლაინ პლატფორმების ფარგლებში პროდუქტების გაცვლაზე ან ალტერნატიული ვალუტების გამოყენებაზე აგებული ტრანზაქციების რაოდენობა აქტიურად იზრდება; ფართო გავრცელება ჰპოვა სრულიად ახალი ტიპის ფინანსურმა ტრანზაქციებმა მოწყობილობებს შორის, რომელსაც არ ესაჭიროება ადამიანის ჩარევა. იზრდება კიბერუსაფრთხოების, პერსონალური მონაცემების დაცვის, ტრანზაქციების განხორციელებისას პირის საინფორმაციო სივრცეში იდენტიფიცირების პრობლემების მნიშვნელობა.

ფინანსური მონაცემების დაშიფვრა

გრემის-ლიჩის-ბლაილის კანონი (GLBA) კონკრეტულად მოითხოვს, რომ ინსტიტუციებმა, რომლებიც აწარმოებენ ბიზნესს აშშ-ში, დააწესონ შესაბამისი სტანდარტები მომხმარებელთა არა-საჯარო პერსონალური ინფორმაციის უსაფრთხოებისა და კონფიდენციალურობის დასაცავად [1].

მიზნები არის შემდეგი:

- მომხმარებლის ჩანაწერებისა და ინფორმაციის უსაფრთხოების და კონფიდენციალურობის უზრუნველყოფა.

- ასეთი ჩანაწერების უსაფრთხოებასა და მთლიანობაზე მოსალოდნელი საფრთხეებისგან დაცვა.
- დაცვა ინფორმაციაზე არაავტორიზებული წვდომისგან, რამაც შეიძლება გამოიწვიოს მნიშვნელოვანი ზიანი ან დისკომფორტი ნებისმიერი კლიენტისთვის.

გარდა ამისა, ფედერალური ფინანსური ინსტიტუტების ექსპერტიზის საბჭო (FFIEC), რომელიც „უფლებამოსილია განსაზღვროს ერთიანი პრინციპები, სტანდარტები და ანგარიშგების ფორმები ფინანსური ინსტიტუტების ზედამხედველობის ერთგვაროვნების ხელშეწყობის მიზნით“, დასძენს:

„ფინანსურმა ინსტიტუტებმა მგრძნობიარე ინფორმაციის გამჟღავნების ან შეცვლის რისკის შესამცირებლად უნდა გამოიყენონ დაშიფვრა ინფორმაციის შენახვისა და ტრანზიტის დროს“.

FFIEC-სა და GLBA-ს თანახმად ბანკებმა და ფინანსურმა ინსტიტუტებმა უნდა დაშიფრონ:

- ნებისმიერი სენსიტიური ინფორმაცია, რომელსაც ინდივიდი გასცემს ფინანსური პროდუქტის ან სერვისის მისაღებად (როგორიცაა სახელი, მისამართი, შემოსავალი, სოციალური დაცვის ნომერი ან სხვა ინფორმაცია განაცხადის შესახებ);
- ნებისმიერი ინფორმაცია, რომელსაც ისინი იღებენ ინდივიდის შესახებ ტრანზაქციისგან, რომელიც მოიცავს ფინანსურ პროდუქტებს ან მომსახურებას (მაგალითად, ის ფაქტი, რომ ფიზიკური პირი არის ფინანსური ორგანიზაციის მომხმარებელი, ანგარიშის ნომრები, გადახდის ისტორია, სესხის ან დეპოზიტის ნაშთები და საკრედიტო ან სადებეტო ბარათით შესყიდვები);
- ნებისმიერი ინფორმაცია, რომელსაც ისინი იღებენ ფიზიკური პირის შესახებ ფინანსური პროდუქტის ან მომსახურების მიწოდებასთან დაკავშირებით (მაგალითად, ინფორმაცია სასამართლოს ჩანაწერებიდან ან მომხმარებლის ანგარიშიდან).

გასაღების გენერირება და მართვა

დაშიფვრა ხშირად განიხილება პირადი მონაცემების დაცვის ურთულეს ნაწილად. პირველი ნაბიჯი, რომლის გადადგმაც ბანკებს და ფინანსურ სერვისებს შეუძლიათ, არის დაშიფვრის დანერგვა ინდუსტრიაში გამოცდილი და მიღებული ალგორითმების საფუძველზე, გასაღების საიმედო სიგრძესთან ერთად [2,3].

დაშიფვრა - სპეციფიკური მოთხოვნაა, რადგან დაშიფვრისა და გაშიფვრის ოპერაციები უნდა განხორციელდეს ადგილობრივად, არა დისტანციური სერვისით, რადგან გასაღებებიც და მონაცემებიც უნდა დარჩეს მონაცემთა მფლობელის უფლებამოსილებაში თუ რა თქმა უნდა კონფიდენციალურობის მიღწევა დგას დღის წესრიგში. ამის პრაქტიკაში მისაღწევად, ორგანიზაციები სავარაუდოდ განიხილავენ ფსევდონიმიზაციის ტექნიკის გამოყენების გაზრდას.

დაშიფვრა ისეთივე უსაფრთხოა, როგორც თქვენი დაშიფვრის გასაღები. გასაღებების მართვის გადაწყვეტის არსებითი ფუნქციები მოიცავს დაშიფვრის გასაღებების

განცალკევებით შენახვას იმ მონაცემებისგან, რომლებსაც ისინი იცავენ, ასევე დაშიფვრის გასაღებების მართვას მთელი სასიცოცხლო ციკლის განმავლობაში, მათ შორის:

• გასაღებების გენერირება სხვადასხვა კრიპტოგრაფიული სისტემებისთვის და სხვადასხვა აპლიკაციებისთვის;

• საჯარო გასაღებების გენერირება და მიღება;

• გასაღებების განაწილება შესაბამის მომხმარებლებს შორის, გაქტიურების ინსტრუქციის ჩათვლით;

• გასაღებების შენახვა, მათ შორის, ავტორიზებული მომხმარებლების გასაღებებზე წვდომის წესები;

• გასაღებების შეცვლა ან განახლება, მათ შორის წესები, როდის და როგორ უნდა შეიცვალოს გასაღებები;

• კომპრომეტირებული გასაღებების ადრესაცია;

• დაარქივება, უკუკავშირი და გასაღებების ამოღების ან დეაქტივაციის მითითებები;

• დაკარგული ან დაზიანებული გასაღებების აღდგენა, როგორც ბიზნესის უწყვეტობის მენეჯმენტის ფარგლებში;

• გასაღებების მართვასთან დაკავშირებული ძირითადი აქტივობების აუდიტი;

• განსაზღვრული აქტივაციისა და დეაქტივაციის თარიღების დაწესება და გასაღებების გამოყენების პერიოდის შეზღუდვა.

დაშიფვრის განხორციელება

FFIEC უზრუნველყოფს GLBA-ს ხელმძღვანელობასა და ზედამხედველობას ბანკებისა და ფინანსური ორგანიზაციებისთვის. ისინი აქვეყნებენ IT Examination Handbook-ს, რომელიც გამოსცემს მითითებებს IT უსაფრთხოების კონტროლისთვის, რომელიც შეიძლება ან უნდა იქნას გამოყენებული პერსონალური ინფორმაციის დასაცავად GLBA-ს ფარგლებში [4,5]. სახელმძღვანელოს მიხედვით, ფინანსურმა ინსტიტუტებმა უნდა გამოიყენონ დაშიფვრა ინფორმაციის შენახვისა და ტრანზიტის დროს მგრძნობიარე ინფორმაციის გამჟღავნების ან ცვლილების რისკის შესამცირებლად. დაშიფვრის განხორციელება უნდა შეიცავდეს:

- საკმარის დაშიფვრის სიძლიერეს ინფორმაციის გამჟღავნებისგან დასაცავად მანამ, სანამ გამჟღავნება არ წარმოადგენს მატერიალურ რისკს;
- გასაღების მართვის ეფექტურ პრაქტიკას;
- მაღალ საიმედოობას.

ორწერტილოვანი დაშიფვრა (P2PE)

P2PE არის ტექნოლოგიური სტანდარტი, რომელიც შემუშავებულია ელექტრონული ფინანსური ტრანზაქციების უსაფრთხოების დასაცავად.

იგი შექმნილია გადახდების დამმუშავებელი მსხვილი კომპანიების კონსორციუმის მიერ.

ახალი ტექნოლოგიების გაჩენისთანავე P2PE სტანდარტები განაგრძობს განვითარებას.

P2PE სტანდარტების შესაბამისად, ტრანზაქციის მონაცემები სრულად არის დაშიფრული იმ მომენტიდან, როდესაც კლიენტი შეიყვანს თავის მონაცემებს ამ ინფორმაციის გადახდის პროცესორზე გადაცემის მომენტამდე. მიღებისთანავე, გადახდის პროცესორი ახდენს მონაცემების გაშიფვრას და ამტკიცებს ან უარყოფს ტრანზაქციას.

რადგან მთელი პროცესის განმავლობაში ტრანზაქციის მონაცემები სრულად არის დაშიფრული, ის არის დაცული არაავტორიზებული მესამე პირის მიერ მოპოვებისა და ბოროტად გამოყენებისგან. იმ შემთხვევაშიც კი, თუ ჰაკერი კონკრეტულ ტრანზაქციას ხელში ჩაიგდებს, მიღებული ინფორმაცია გაუგებარი იქნება, რადგან ის მაინც დაშიფრულია. ინფორმაციის გაშიფვრისთვის მომხმარებელს უნდა ჰქონდეს დაშიფვრის გასაღები, რომელიც ხელმისაწვდომია მხოლოდ ავტორიზებული მხარისთვის.

ცალკეულ კომპანიებს შეუძლიათ თავისუფლად განავითარონ ახალი პროდუქტები და სერვისები, რომლებიც ურთიერთქმედებენ ელექტრონული გადახდების ეკოსისტემასთან. თუმცა, იმისათვის, რომ ამ კომპანიებმა მიაღწიონ P2PE შესაბამისობას, მათ უნდა აჩვენონ, რომ მათი ახალი შეთავაზება აკმაყოფილებს ან აღემატება P2PE სტანდარტებს. პრაქტიკაში, ეს ნიშნავს, რომ მათ უნდა უზრუნველყონ ყველა ტრანზაქციის ინფორმაციის სრულად დაშიფვრა და შეთავაზებაში ჩართული ნებისმიერი აპარატურის უსაფრთხოდ მართვა. ასევე პროცესში გამოყენებული ნებისმიერი კრიპტოგრაფიული გასაღები უნდა იყოს უსაფრთხოდ გენერირებული, გადაცემული და შენახული.

PCI SSC უსაფრთხოების სტანდარტების საბჭო ატარებს რეგულარულ ღონისძიებებს და ხელს უწყობს ინფორმაციის გაცვლას ამ სტანდარტების ცვლილებებთან დაკავშირებით ფინანსური ტრანზაქციების ინდუსტრიაში ჩართული ორგანიზაციების დასახმარებლად. ისტორიულად, ეს მმართველი ორგანო დაარსდა მსხვილი გადახდის ბრენდების მიერ, მათ შორის American Express (AXP), Discover Financial Services (DFS), MasterCard (MA) და Visa (V). ამასთან, P2PE სტანდარტების გამოყენება ცალკეული კომპანიების პასუხისმგებლობაა, რომლებიც სთავაზობენ პროდუქტებსა და სერვისებს ამ სტანდარტების გამოყენებით, და არა თავად მმართველი საბჭოსი.

დასკვნა

PCI SSC სტანდარტები არ არის გათვალისწინებული სახელმწიფო დონეზე, როგორც სავალდებულო, უფრო ზუსტად რომ ვთქვათ, მხოლოდ აშშ-ის ზოგიერთმა შტატმა მიიღო ისინი საკანონმდებლო დონეზე. მაგრამ, გადახდის სისტემების მოთხოვნების წყალობით,

ისინი ხორციელდება უამრავ ორგანიზაციაში. Cisco-ს 2011 წელს აშშ-ს შესაბამისობის კვლევამ დაადგინა შემდეგი:

- საცალო ვაჭრობა სრული სერიოზულობით მოეკიდა PCI DSS სტანდარტის დანერგვას და რეალიზებას. (Payment Card Industry Data Security Standard ერთ-ერთი ძირითადი სტანდარტია).
- გამოკითხულთა 85% თვლის, რომ მათ ორგანიზაციებს ამჟამად შეუძლიათ წარმატებით გაიარონ PCI DSS აუდიტი.
- სამთავრობო ორგანიზაციების 85%-მა წარმატებით გაიარა PCI DSS აუდიტი პირველივე ცდიდან. ყველაზე ცუდად ეს აუდიტი გავლილი აქვთ სამედიცინო ორგანიზაციებს (72%).
- გამოკითხული აღმასრულებელი დირექტორიებისა და საბჭოს წევრების 67% ამბობს, რომ PCI DSS ძალიან მნიშვნელოვანი ინიციატივაა.

ჩემი აზრით, გასათვალისწინებელია ის, რომ თაღლითობის რისკის შესამცირებლად საჭიროა მიღებული სტანდარტები გავხადოთ სავალდებულო ყველა ორგანიზაციისთვის, სასურველია, რომ ეს მოხდეს სახელმწიფოს დონეზე.

რეკომენდაციები

ამჟამად, გადახდის ინდუსტრიაში ყველაზე დიდი საფრთხე არის სოციალური ინჟინერიის თაღლითობა. აქედან გამომდინარე, მნიშვნელოვანია საბანკო სერვისების მომხმარებლებში ტექნოლოგიური წიგნიერების განვითარება.

ციფრული ჰიგიენის ზომები რომლებიც რეკომენდირებულია გადახდის სისტემების მომხმარებლისთვის:

- ნუ შეინახავთ გადახდის მონაცემებს საეჭვო სერვისებზე, შეადარეთ რისკები და გადახდის მონაცემების შეყვანის აუცილებლობა რესურსებზე, რომლებიც არ უჭერენ მხარს 3D Secure სტანდარტს (PCI Three-Domain Secure Core Security Standard» (3DS), ის არის PCI SSC სტანდარტული პაკეტის ნაწილი და მოითხოვს მხარდაჭერას არა მხოლოდ გადახდის სისტემისა და ფინანსური ორგანიზაციის, არამედ თავად სავაჭრო კომპანიის);
- არ შეინახოთ კოდი ბარათის უკანა მხარეს განთავსებული (CVV კოდი) და არავის გაუმზილოთ შემდეგი კოდები: CVV კოდი, SMS კოდი, Push შეტყობინებები, ბარათის PIN კოდი;
- მოერიდეთ თაღლითობებს: იყავით ფხიზლად, ნუ ენდობით სატელეფონო ზარებს. არ გაამჟღავნოთ თქვენი პირადი მონაცემები: სრული სახელი, დაბადების ადგილი და წელი, პასპორტის მონაცემები.
- დააწესეთ ბარათის ლიმიტები წარმატებული თაღლითობის შემთხვევაში დიდი თანხების დაკარგვის თავიდან ასაცილებლად.

ბიბლიოგრაფია:

1. H. DeYoung, D. Garg, L. Jia, D. Kaynar and A. Datta, "Experiences in the logical specification of the hipaa and glba privacy laws", Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society ser. WPES '10, pp. 73-82, 2010.
2. Avtandil Gagnidze, Maksim Iavich, Giorgi Iashvili, SOME ASPECTS OF POST-QUANTUM CRYPTOSYSTEMS, Eurasian Journal of Business and Management, 5(1), 2017, 16-20 DOI: 10.15604/ejbm.2017.05.01.002
3. Iavich, M., Gnatyuk, S., Fesenko, G.: Cyber security European standards in business. Scientific and Practical Cyber Security Journal. J. 3, 36–39 (2019)
4. H. Qin, Z. Li, P. Hu, Y. Zhang and Y. Dai, "Research on Point-To-Point Encryption Method of Power System Communication Data Based on Block Chain Technology," 2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA), Xiangtan, China, 2019, pp. 328-332, doi: 10.1109/ICICTA49267.2019.00076.
5. S. Jahan, M. S. Rahman and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," 2017 International Conference on Networking, Systems and Security (NSysS), Dhaka, Bangladesh, 2017, pp. 39-44, doi: 10.1109/NSysS.2017.7885799.