ყოველკვირეული დაიჯესტი კიბერუსაფრთხოებასა და ინფორმაციულ ტექნოლოგიებში

24-30 ივლისი, 2023

CRC კიბერმედეგობის ცენტრი
CYBER RESILIENCE CENTER

ნორვეგიის მთავრობის წინააღმდეგ განხორციელებული კიბერშეტევა

24 ივლისის ოფიციალური განცხადების თანახმად, განხორციელებულმა კიბერშეტევამ, ნორვეგიის მთავრობის 12 სამინისტო დააზარალა. ნორვეგიის ეროვნული უსაფრთხოების ორგანომ ოფიციალურად დაადასტურა, რომ თავდამსხმელთა ჯგუფმა გამოიყენა ე.წ. ნულოვანი დღის დაუცველობა (zero-day vulnerability), რის შედეგადაც წარმატებით შეაღწია პროგრამულ პლატფორმაში, რომელსაც ქვეყნის 12 სამინისტრო იყენებს. მიუხედავად იმისა, რომ თავდასხმა "უკიდურესად დამაზარარებლად" ჩაითვალა, ყოველდღიური ციფრული ოპერაციები მაინც ჩვეულ რეჟიმში გაგრძელდა. ნორვეგიის ეროვნული უსაფრთხოების ორგანომ განაცხადა ისიც, რომ უკვე შეკრებილია კრიზისული შტაბი სიტუაციის მოსაგვარებლად და, საბედნიეროდ, კრიტიკულად მნიშვნელოვანი ინსტიტუტები, ერთ-ერთი როგორიცაა - პრემიერის ოფისი, არ დაზარალდნენ. კიბერუსაფრთხოების ექსპერტები ხაზს უსვამენ მიწოდების ჯაჭვების მონიტორინგისა და უსაფრთხოების მკაცრი ზომების გატარების მნიშვნელობას, რაც მსგავსი თავდასხმების პრევენციას შეუწყობს ხელს.

24.07.2023

ChatGPT ახლა უკვე ხელმისაწვდომია Android-ის მომხმარებლებისათვის რამდენიმე ქვეყანაში

ChatGPT-ის აპლიკაცია 2023 წლის 25 ივლისიდან უკვე ხელმისაწვდომი გახდა Google Play Store-ზე Android-ის მომხმარებლებისთვის აშშ-ში, ინდოეთში, ბანგლადეშსა და ბრაზილიაში. კომპანია მომავალ კვირაში ასევე გეგმავს დამატებით სხვა ქვეყნებში აპლიკაციის ჩაშვებას. თავდაპირველად არსებული ხარვეზების მიუხედავად, მათ შორის, გამოყენების სიმცირის, გარკვეული ფუნქციების შეფერხების ან შეჩერების შემთხვევებისა, OpenAI მიზნად ისახავს ახალი მომხმარებლის მოზიდვას და წვდომის გაფართოებას აპლიკაციის Android-ზე ხელმისაწვდომობით.

25.07.2023

Worldcoin-ს, OpenAI-ის კრიპტო პლატფორმას, უკვე 2 მილიონზე მეტი მომხმარებელი ჰყავს

Worldcoin-მა, ახალმა კრიპტო პლატფორმამ, რომელიც OpenAI-ის აღმასრულებელმა დირექტორმა, სემ ალტმანმა, 24 ივლისს, მსოფლიო ბაზარზე ჩაუშვა, უკვე ორ მილიონზე მეტი მომხმარებელი შეიძინა. პლატფორმის უნიკალურმა შეთავაზებამ ციფრული იდენტურობისა და ფინანსური ქსელის შესახებ არაერთი ადამიანი მოხიბლა. ყველაზე ინოვაციური ფუნქციით, სახელწოდებით WorldID, კონფიდენციალურობის შენარჩუნებით,

ციფრული პასპორტის დანერგვითა და ბიომეტრიული ირისის ამოცნობის გამოყენებით, Worldcoin მიზნად ისახავს შეცვალოს ადამიანების დამოკიდებულება და ურთიერთქმედება ხელოვნური ინტელექტის მიმართ. პროექტს ასევე აქვს პოტენციალი, ებრძოლოს შემოსავლების უთანასწორობას AI ტექნოლოგიების წინსვლის პირობებში.

24.07.2023

გადახდა ხელის გულის სკანირებით: Amazon One-ის ახალი გადახდის მეთოდი ბიომეტრიული ტექნოლოგიების გაფართოების ფონზე

Amazon წლის ბოლომდე გეგმავს ხელის გულის სკანირების დანერგვას, რომლის მეშვეობით მომხმარებელებს შეეძლებათ გადახდა Amazon One ტექნოლოგიის გამოყენებით Whole Foods-ის ყველა მაღაზიაში. ბიომეტრიული ტექნოლოგია მომხმარებლებს საშუალებას აძლევს განახორციელონ შესყიდვები სალაროში არსებულ ხელსაწყოზე ხელის გულის სკანირებით, რომელიც თავის მხრივ დაკავშირებულია მომხარებლების საკრედიტო ბარათებთან. მიუხედავად იმისა, რომ Amazon-ის მტკიცებით, მსგავსი მეთოდი გადახდებისთვის უსაფრთხო, ხოლო დუბლირება კი შეუძლებელი, კრიტიკოსები შეშფოთებას გამოთქვამენ ბიომეტრიული მონაცემების ბოროტად გამოყენებისა და მისი დაუცველობის შესახებ.

25.07.2023

TETRA-ის რადიო სისტემის ბაგები: რისკები და მათი პრევენცია

TETRA , რადიო სისტემა, რომელსაც სამართალდამცავი ორგანოები, სამხედროები, სამრეწველო კომპანიები და კრიტიკული ინფრასტრუქტურა იყენებს, მინიმუმ 5 ბაგის (პროგრამული შეცდომის) გამო ხშირად ხდება კიბერშეტევების ობიექტი. ხარვეზები იდენტიფიცირებულ იქნა კიბერუსაფრთხოების ფირმის Midnight Blue-ის მიერ, რომლის ცნობითაც, პოტენციურ კიბერ კრიმინალს მარტივად შეუძლია მავნე მონაცემების სისტემაში შეყვანით სისტემის გატეხვა და არაავტორიზირებული წვდომის მოპოვებით ისეთი ქმედებების განხორციელება როგორიცაა - უნებართვო წვდომის მოპოვება კერძო რადიოკავშირებზე, სამრეწველო აღჭურვილობის ან სარკინიგზო სიგნალების კონტროლი და ა.შ. Midnight Blue-ის ანგარიშში აღნიშნულია, რომ, საბედნიეროდ, კონკრეტული ხარვეზები უკვე აღმოფხვრილია და შესაძლო შეტევის შანსი TETRA-ზე, ფაქტობრივად, ნულის ტოლია.

25.07.2023

HRM Enterprises-ზე კიბერშეტევისას 40 ათასზე მეტი მომხმარებელი დაზარალდა

HRM Enterprises, აშშ-ის უმსხვილესი ტექნიკის მაღაზია, კიბერშეტევის შედეგად, 40 000-ზე მეტი მომხმარებლის საკრედიტო ბარათზე არსებული ინფორმაციის მოპარვას ადასტურებს. მათი განცხადებით, 26 ივლისს კიბერშეტევა განხორციელდა HRM-ის ელექტრონული კომერციის პლატფორმის პროვაიდერის, Commerce V3-ის მეშვეობით, რომელზეც ჰაკერებს წვდომა უკვე ერთ წელზე მეტია რაც აქვთ. მოპარული მონაცემები მოიცავს კლიენტების სახელებს, გადახდის ბარათის დეტალებს, CVV კოდებს, ვადის გასვლის თარიღსა და ელ-ფოსტებს. HRM დაზარალებულ კლიენტებს ურჩევს თვალყური ადევნონ საგადახდო ბარათების თაღლითობას და ნებისმიერი საეჭვო აქტივობის შემთხვევაში, დაუყონებლივ ფინანსურ ინსტიტუტებს ან სამართალდამცავ ორგანოებს მიმართონ.

27.07.2023