Irlandia Północna zawiesza system paszportów szczepionkowych po incydencie wycieku danych

Departament Zdrowia Irlandii Północnej (DoH) tymczasowo wstrzymał swoją internetową usługę certyfikacji szczepionek przeciw COVID-19 po incydencie związanym z ujawnieniem danych, podkreślając ryzyko powierzenia danych dotyczących zdrowia rządowi.

Według DoH niektórym użytkownikom usługi COVIDCert NI przedstawiono w pewnych okolicznościach dane innych użytkowników. Stwierdzono, że ograniczona liczba użytkowników była potencjalnie narażona na dane innych użytkowników.

COVIDCert umożliwia w pełni zaszczepionym osobom z Irlandii Północnej uzyskanie cyfrowego zaświadczenia potwierdzającego status szczepienia przeciw COVID-19. Jest to system odrębny od przepustki COVID *National Health Service* (NHS) stosowanej w Anglii i Walii oraz podobnej usługi w stylu paszportu szczepień stosowanej przez *Public Health Scotland*.

Witryna COVIDCert i aplikacja mobilna nie działają

Usługa Irlandii Północnej jest dostępna za pośrednictwem strony internetowej covidcertni.nidirect.gov.uk lub aplikacji mobilnej dla użytkowników systemów Android i iOS. Zarówno witryna COVIDCert, jak i punkty końcowe aplikacji mobilnej nie

działały podczas testów przeprowadzanych przez *BleepingComputer*, witrynę zajmującą się nowościami technologicznymi.

„Nasze usługi nie są obecnie dostępne. Pracujemy nad jak najszybszym przywróceniem wszystkich usług. Sprawdź ponownie wkrótce" – czytamy w jednym z komunikatów o błędach generowanych przez usługę na swojej stronie internetowej.

W międzyczasie komunikat „zasób… usunięto" jest wyświetlany użytkownikom aplikacji mobilnej, którzy próbują się zalogować.

DoH natychmiast zgłosił problem do *Biura Komisarza ds. Informacji* w Wielkiej Brytanii (ICO). „DoH bardzo poważnie traktuje prywatność danych obywateli i nawiązano kontakt z ICO w ramach należytej staranności w zakresie ochrony danych obywateli", powiedział departament w ogłoszeniu opublikowanym we wtorek, 27 lipca.

„Podjęto również natychmiastowe działanie w celu tymczasowego usunięcia części usługi zarządzającej tożsamością".

Lista stron, na które incydent nie miał wpływu

DoH opublikowała również listę stron, na które incydent nie miał wpływu, w tym wnioskodawców, którzy już posiadają certyfikat (ich aplikacje lub papierowe kopie nadal działają); wnioskodawców, którzy złożyli wniosek za pośrednictwem portalu internetowego o plik PDF do pobrania, którzy jeszcze go nie otrzymali (ich plik PDF zostanie dostarczony); oraz wnioskodawcy, którzy złożyli wniosek za pomocą aplikacji COVIDCert NI o wydanie certyfikatu elektronicznego, którzy go jeszcze nie otrzymali (otrzymają plik PDF jako etap pośredni).

Incydent nie będzie miał wpływu na niektóre osoby, które już złożyły wniosek o certyfikat cyfrowy lub oczekują na

weryfikację tożsamości. Mogą nadal normalnie korzystać z usług po przywróceniu operacji.

Wnioskodawcy, którzy złożyli wniosek o wydanie certyfikatu elektronicznego, ale zamiast tego otrzymali kopię PDF, będą mogli się zalogować i pobrać wersję elektroniczną po rozwiązaniu problemu. Wnioskodawcy, którzy obecnie przechodzą weryfikację tożsamości w przepływie pracy NIDirect, mogą kontynuować. Po pomyślnym zweryfikowaniu będą musieli się wstrzymać, aż problem zostanie rozwiązany.

Niektórzy użytkownicy mogą nie być w stanie zalogować się przez swoje konto NIDirect, ponieważ zostali zablokowani z powodu problemów technicznych.

Liczba naruszeń danych w służbie zdrowia rośnie z roku na rok

Incydent z danymi miał miejsce w czasie, gdy wśród społeczeństwa jest wiele kontroli i obaw dotyczących paszportów szczepionkowych przeciwko COVID-19. Naruszenia danych w służbie zdrowia rosną wykładniczo z roku na rok i nie wydaje się, aby w najbliższym czasie spowolniły.

Ważne jest, aby specjaliści IT z opieki zdrowotnej podejmowali kroki w celu zabezpieczenia swoich systemów, niezależnie od tego, czy oznacza to ochronę przed zewnętrznymi zagrożeniami stwarzanymi przez hakerów i cyberprzestępców, czy zabezpieczenie wewnętrznych zagrożeń wynikających z nadużyć dostępu ze strony użytkowników wewnętrznych.

Dane dotyczące opieki zdrowotnej są cenne na czarnym rynku, ponieważ często zawierają wszystkie informacje umożliwiające identyfikację danej osoby, a nie pojedynczą informację, która może zostać znaleziona w przypadku naruszenia finansowego.

Rekord danych medycznych jest wart na czarnym rynku do 250 USD

Według raportu Trustwave, rekord danych medycznych może być wyceniany na 250 USDna czarnym rynku, w porównaniu do 5,40 USD za kolejny rekord o najwyższej wartości – karty płatnicze.

Większość z tych naruszeń można przypisać przestępcom wewnętrznym i hakerom, którzy uzyskują dostęp za pośrednictwem zewnętrznych dostawców. Instytut Ponemon ustalił, że koszty związane z naprawą naruszenia szacuje się na 740 000 USD. Jeśli osoba trzecia spowoduje naruszenie danych, koszt ataku wzrasta o ponad 370 000 USD.

Eksperci branżowi twierdzą, że wektorami ataków są najprawdopodobniej ataki typu ransomware lub SQL injection, które mogą wystąpić, gdy złośliwa poczta e-mail, witryna internetowa lub oprogramowanie jest zainstalowane lub uzyskuje dostęp w sieci, często przez niczego niepodejrzewającego użytkownika.

Opieka zdrowotna podatna na ataki ransomware

Branża opieki zdrowotnej jest szczególnie podatna na ataki złośliwego oprogramowania ransomware. W styczniu 2018 r. atak zmusił informatyków w Hancock Health do zamknięcia swoich systemów, podczas gdy informacje umożliwiające identyfikację pacjentów były zakładnikami.

Naruszenie przypisano hakerowi, który korzystał z portalu zdalnego dostępu i danych uwierzytelniających innej firmy, które są głównymi przyczynami cyberataków. Szpital został później zmuszony przez atakującego do zapłacenia 55 000 USD za pomocą bitcoinów.

Prawdziwe niebezpieczeństwo ataków hakerów na placówki opieki zdrowotnej polega na tym, że personel medyczny pilnie potrzebuje dostępu do akt pacjentów na miejscu. W niektórych przypadkach może to być dosłownie kwestia życia i śmierci.

Hakerzy atakujący placówki opieki zdrowotnej wiedzą, że po uzyskaniu dostępu za pośrednictwem sieci VPN, danych uwierzytelniających lub phishingu nie ma możliwości ograniczenia dostępu do napotkanych informacji. Otwarcie tych drzwi oznacza nieograniczony dostęp do dziesiątek, setek, a nawet tysięcy akt pacjentów.

Źródła obejmują:

BleepingComputer.com

SecureLink.com

USA oskarża 6 rosyjskich oficerów GRU o globalną operację hakerską

Departament Sprawiedliwości oskarżył sześciu rosyjskich hakerów wojskowych o angażowanie się w serię ataków na infrastrukturę, wybory czy biznesy innych krajów, co zostało opisane jako „najbardziej uciążliwa i destrukcyjna serii ataków komputerowych przypisana do jednej grupy.”

Oskarżeni, będący agentami rosyjskiej agencji wywiadu wojskowego, znanej jako GRU, rzekomo stosowali różne taktyki cybernetyczne, w tym rozmieszczanie destrukcyjnego szkodliwego

oprogramowania w celu wspierania interesów rządu rosyjskiego w destabilizacji i ingerowaniu w systemy polityczne i gospodarcze innych krajów, powiedział Departament Sprawiedliwości (DOJ).

GRU to ta sama agencja, która rzekomo była zaangażowana w próby włamania się, aby ingerować w wybory prezydenckie w USA w 2016 roku.

Wśród celów znajduje się ukraińska sieć elektroenergetyczna, Ministerstwo Finansów i Służba Skarbu Państwa; Partia polityczna prezydenta Francji Emmanuela Macrona i francuscy politycy; gospodarze, uczestnicy, partnerzy, uczestnicy i systemy informatyczne Zimowych Igrzysk Olimpijskich w PyeongChang 2018; organizacje i podmioty badające zatrucie środkiem nerwowym Siergieja Skripala; Gruzińskie firmy i jednostki rządowe; oraz firmy i placówki medyczne w Stanach Zjednoczonych.

„Żaden kraj nie wykorzystał swoich zdolności cybernetycznych tak złośliwie i nieodpowiedzialnie jak Rosja, bezmyślnie powodując bezprecedensowe szkody w celu osiągnięcia niewielkiej przewagi taktycznej i zaspokojenia napadów złośliwości" – powiedział zastępca prokuratora generalnego ds. Bezpieczeństwa narodowego John C. Demers podczas konferencji prasowej 19 października ogłaszając zarzuty.

Zgodnie z aktem oskarżenia hakerzy wdrożyli „jedne z najbardziej destrukcyjnych dotychczas szkodliwych programów na świecie" – takie jak KillDisk, Industroyer i NotPetya – które spowodowały rozległe szkody, w tym przerwy w dostawie energii na Ukrainie i zakłócenia pracy tysięcy komputerów używanych do obsługi programu Winter 2018 Igrzyska Olimpijskie.

Mężczyźni zostali oskarżeni o spisek mający na celu dokonywanie oszustw i nadużyć komputerowych, spisek w celu popełnienia oszustwa elektronicznego, oszustwa elektronicznego, niszczenia chronionych komputerów i kradzieży

tożsamości. Każdy jest oskarżony w każdym przypadku w akcie oskarżenia zwróconym przez federalne trybunały sądowe w Pittsburghu.

Plakat przedstawiający sześciu poszukiwanych oficerów rosyjskiego wywiadu wojskowego.

(Departament sprawiedliwości)
Departament powiedział, że kilku mężczyzn zostało wcześniej oskarżonych o ich role w rzekomym ingerowaniu w wybory w USA w 2016 roku.

Demers powiedział, że zarzuty powinny być dowodem na to, że Stany Zjednoczone nie powinny zaakceptować oferty prezydenta Władimira Putina dotyczącej cyber „resetu" między dwoma krajami. Porozumienie wymagałoby od obu zapewnienia gwarancji, że nie będą angażować się w „cyberwtrącanie się" do swoich wyborów.

> *„Rosja z pewnością ma rację, że zaawansowane technologicznie narody, które aspirują do przywództwa, mają szczególną odpowiedzialność za zabezpieczenie światowego porządku i przyczynianie się do powszechnie akceptowanych norm, pokoju i stabilności. To właśnie robimy tutaj dzisiaj"- powiedział Demers.*

> *„Ale ten akt oskarżenia obnaża wykorzystanie przez Rosję jej zdolności cybernetycznych do destabilizacji i ingerowania w wewnętrzne systemy polityczne i gospodarcze innych krajów, stanowiąc w ten sposób zimne przypomnienie, dlaczego jej propozycja jest niczym innym jak nieuczciwą retoryką oraz cyniczną i tanią propagandą".*

Departament Sprawiedliwości powiedział, że ataki spowodowały prawie miliard dolarów strat trzech ofiar w USA, w tym Heritage Valley Health System w Pensylwanii. Mężczyźni rzekomo wdrożyli złośliwe oprogramowanie NotPetya, które spowodowało „niedostępność list pacjentów, historii pacjentów, plików badań i danych laboratoryjnych".

„Heritage Valley utraciło dostęp do swoich krytycznych systemów komputerowych (takich jak te związane z kardiologią, medycyną nuklearną, radiologią i chirurgią) na około tydzień, a administracyjne systemy komputerowe na prawie miesiąc,

powodując tym samym zagrożenie dla zdrowia i bezpieczeństwa publicznego," zgodnie z oświadczeniem wydziału.

Inne cele w USA to TNT Express BV, spółka zależna FedEx Corp., oraz duży producent farmaceutyczny.

Źródło:

theepochtimes.com