LOTNISKA CORAZ CZĘŚCIEJ OBIEKTEM ZAINTERESOWANIA CYBERPRZESTĘPCÓW

Sektor lotniczy cieszy się coraz większym zainteresowaniem cyberprzestępców – ostrzegają eksperci Stormshield. Infrastruktura portów i linii lotniczych czy wrażliwe dane pasażerów narażone są na skutki ataków hakerów. Konsekwencją ich działalności mogą być utrudnienia w funkcjonowaniu lotnisk, których efektem są nie tylko mające wymierny finansowo charakter opóźnienia czy wysokie grzywny, którymi obciążani są operatorzy.

W ostatnich latach wrażliwe dane milionów pasażerów, w tym dotyczące bankowości, trafiły w niepowołane ręce. Na liście ofiar cyberprzestępców nie brakuje lotnisk działających w Polsce, a także krajach sąsiednich, z których usług korzystają polscy pasażerowie.

Miliony pasażerów to miliony danych

W lipcu bieżącego roku z usług krakowskiego lotniska Balice skorzystało ponad 383 tys. pasażerów, co jest liczbą o połowę mniejszą niż w czasach przed pandemią, ale jednocześnie stanowi wzrost o 86 proc. w stosunku do lipca 2020 roku.

Natomiast warszawskie lotnisko im. Fryderyka Chopina w pierwszym półroczu br. obsłużyło niemal 1,9 mln podróżujących. Z kolei przez katowickie Pyrzowice w czerwcu przewinęło się 226 tys. pasażerów, co stanowiło wzrost o 2656 proc., w porównaniu do analogicznego miesiąca ubiegłego roku.

Tegoroczne wzrosty są wynikiem obowiązujących w 2020 roku lockdownów, w tym także obostrzeń w podróżach. Nie mniej jednak statystyki potwierdzają, że po miesiącach zamknięcia Polacy ruszyli w świat, a branża lotnicza zaczyna odrabiać straty.

"Miliony pasażerów oznacza de facto miliony akordów danych osobowych, także tych obejmujących informacje umożliwiające dostęp do bankowości. To niewątpliwie łakomy kąsek dla cyberprzestępców. Niestety pasażer korzystający z usług linii lotniczej czy portu lotniczego ma ograniczone możliwości ochrony swoich danych, powierza je bowiem podmiotowi zewnętrznemu. Branża lotnicza stosuje najnowocześniejsze rozwiązania, które jak się okazuje nie zawsze są skuteczną zaporą. Jak pokazują przykłady z San Francisco czy British Airways, warto być czujnym i sprawdzać czy kanały, którymi komunikujemy się z lotniskiem czy linią lotniczą są autentyczne" – komentuje Piotr Zielaskiewicz, manager produktu w Stormshield.

10 przykładów cyberataków dotyczących branży lotniczej

Atak DDoS na linię lotniczą uziemia pasażerów na lotnisku w Warszawie

W czerwcu 2015 roku Polskie Linie Lotnicze LOT stały się celem cyberataku, w efekcie którego na kilka godzin sparaliżowano część floty przewoźnika na warszawskim lotnisku. Dziesięć lotów zostało

odwołanych, a piętnaście innych opóźnionych, co przyczyniło się do uziemienia co najmniej 1,4 tys. pasażerów.

Zdaniem ekspertów, ten powietrzny chaos był spowodowany atakiem DDoS, który wpłynął na systemy informatyczne przewoźnika, uniemożliwiając mu wykonywanie lotów według normalnych planów.

Port lotniczy w Kijowie dwukrotnie ofiarą ataków

W 2016 roku Ukraina doświadczyła fali cyberataków, które uderzyły w infrastrukturę krytyczną kraju, a źródłem tych sabotaży była Rosja. Międzynarodowy port lotniczy Kijów-Boryspol był jedną z zaatakowanych struktur i - jak oceniają specjaliści - został zainfekowany szkodliwym oprogramowaniem BlackEnergy.

Według ukraińskiego CERT-u (CERT-UA) szkodliwe oprogramowanie zostało w porę zneutralizowane, zapobiegając w ten sposób jego rozprzestrzenieniu w systemach informatycznych lotniska.

W 2017 roku Ukraina ponownie stała się ofiarą fali cyberataków, które jednocześnie dotknęły wiele podmiotów, w krajach takich jak Rosja, Hiszpania, Wielka Brytania i Francja. Tym razem jako wektor ataku zidentyfikowano ransomware GoldenEye, który spowodował niedostępność części sprzętu IT na lotnisku w Kijowie.

Heathrow ujawnia poufne dane

Natomiast w 2017 roku brytyjskie lotnisko Heathrow zostało skrytykowane za zaniedbania w ochronie informacji poufnych. W wyniku niedbałości jednego z pracowników lotniska, stracono klucz USB zawierający 76 folderów i ponad 1 tys. poufnych plików dotyczących tożsamości pasażerów, tras pokonywanych przez członków rządu brytyjskiego oraz informacje dotyczące kamer nadzoru i pasów startowych na lotnisku.

Wszystkie te poufne dane były łatwo dostępne, ponieważ klucz USB nie zawierał hasła ani systemu szyfrowania. Osoba, która znalazła klucz zaalarmowała prasę i zwróciła urządzenie służbom lotniska. Port Heathrow został ukarany grzywną w wysokości 140 tys. euro za nieprzestrzeganie przepisów o ochronie danych poufnych.

Usterka w aplikacji mobilnej Air Canada naraziła tysiące klientów

W sierpniu 2018 roku linia lotnicza Air Canada wykryła nietypową aktywność w przeznaczonej dla klientów firmy aplikacji mobilnej. Po trzech dniach analiz zespoły IT potwierdziły, że aplikacja została zhakowana, ujawniając dane 20 tys. klientów.

Według firmy, informacje dotyczące podróży i tożsamości pasażerów – adresy, numery paszportów, daty urodzenia itp. – zostały ujawnione, ale żadne dane bankowe nie zostały naruszone. Po wykryciu usterki Air Canada jako środek bezpieczeństwa, przeprowadziła reset 1,7 miliona kont użytkowników aplikacji.

British Airways i ogromny wyciek danych

We wrześniu 2018 roku British Airways padło ofiarą masowego naruszenia bezpieczeństwa danych, które dotknęło jej klientów i pracowników. Według Biura Komisarza ds. Informacji (The Information Commissioner's Office - ICO) osoby atakujące przejęły ruch tysięcy klientów, którzy wierzyli, że łączą się z oficjalną stroną British Airways, podczas gdy w rzeczywistości byli przekierowywani na fałszywą stronę.

W ciągu dwóch miesięcy cyberprzestępcy byli w stanie zebrać dane osobowe, w tym bankowe 400 tys. osób. Wycieku informacji można było uniknąć, gdyby British Airways podjęło niezbędne środki bezpieczeństwa cybernetycznego. Linia została ukarana grzywną w wysokości 26 milionów dolarów.

Luki bezpieczeństwa Cathay Airways

Kilka luk w zabezpieczeniach systemów informatycznych Cathay Airways istniejących w okresie od marca do października 2018 roku, doprowadziło do ujawnienia danych należących do 9,4 mln klientów firmy.

To największy jak dotąd wyciek informacji w branży lotniczej. Według ICO, osoby atakujące były w stanie kilkakrotnie przeniknąć do systemów Cathay Airways, wgrywając złośliwe narzędzie w celu przechwycenia danych klientów. Cathay Airways została zmuszona do zapłaty grzywny w wysokości prawie 700 tys. dolarów za naruszenie ochrony danych swoich klientów.

EasyJet – wyciek informacji o 9 milionach klientów

Linie lotnicze EasyJet padły ofiarą poważnego naruszenia bezpieczeństwa danych. Ujawniono dane osobowe 9 milionów klientów, w tym dane bankowe ponad 2 milionów z nich.

Według niektórych ekspertów, atak w szczytowym momencie kryzysu pandemicznego związany był z większym zainteresowaniem cyberprzestępców danymi osobowymi, które są następnie ponownie wykorzystywane do innych celów.

Włamanie na strony internetowe lotniska w San Francisco

Dwa portale logowania – jeden zarezerwowany dla pracowników portu oraz drugi przeznaczony dla partnerów i usługodawców – na międzynarodowym lotnisku w San Francisco zostały zhakowane w marcu 2020 roku.

Do obu witryn wstrzyknięto złośliwy kod w celu przechwycenia nazw użytkowników i haseł używanych w czasie logowania. Liczba ujawnionych kont nie jest jeszcze znana, ale lotnisko podjęło natychmiastowe działania zapobiegawcze i zresetowało wszystkie hasła swoich pracowników i klientów.

Próby zamachów udaremnione przez lotnisko w Pradze

Lotnisko Vaclava Havla w Pradze potwierdziło, że było celem wielu prób cyberataków na jego systemy, co miało miejsce w kwietniu 2020 roku.

Według czeskiego, krajowego organu ds. bezpieczeństwa systemów informatycznych – cyberprzestępcy próbowali wstrzykiwać złośliwe oprogramowanie zaprojektowane w celu uszkadzania lub niszczenia zainfekowanych stacji roboczych. W przypadku lotniska Vaclava Havla zespoły IT wykryły atak na wystarczająco wczesnym etapie, w fazie eksploracyjnej, co umożliwiło szybką i skuteczną reakcję.

Dostawca IT w branży lotniskowej ofiarą cyberataku

W marcu br., ofiarą cyberataku padła firma SITA, opracowująca oprogramowanie i rozwiązania wykorzystywane przez tysiące podmiotów z branży lotniczej.

Wczesne wyniki trwającego wciąż śledztwa sugerują, że celem cyberprzestępców były serwery przechowujące dane klientów linii lotniczych. Firma nie skomentowała dotychczas oficjalnie skali

ataku, ale reperkusje dla jej klientów mogą być znaczące. Wydane w maju oświadczenie linie lotniczej Air India wskazywało, że atak na SITA doprowadził do kradzież danych 4,5 mln pasażerów indyjskiej firmy.

Branża musi zachowywać czujność

"Jak widać, sposoby działania przestępców mogą być różne, ale to co zwraca uwagę to nasilająca się w ostatnim czasie tendencja do atakowania dostawców cyberbezpieczeństwa i ich rozwiązań. Opisany przykład potwierdza to, co sygnalizuje wielu ekspertów. Hakerzy decydują się na takie działania, ponieważ to najkrótsza droga do zdobycia cennych i pożądanych z ich punktu widzenia zasobów. Dostawcy oprogramowania, ale oczywiście również firmy działające w branży lotniczej muszą zachowywać czujność i odpowiednio dostosowywać swoje strategie obronne" – podsumowuje Piotr Zielaskiewicz, manager produktu w Stormshield.

Na podst. informacji prasowej

Chcemy być także bliżej Państwa – czytelników. Dlatego, jeśli są sprawy, które Was nurtują; pytania, na które nie znacie odpowiedzi; tematy, o których trzeba napisać – zapraszamy do kontaktu. Piszcie do nas na: redakcja@cyberdefence24.pl. Przyszłość przynosi zmiany. Wprowadzamy je pod hasłem #CyberIsFuture.

Fot. Reklama