PAŃSTWOWA KOMISJA BADANIA WYPADKÓW LOTNICZYCH

Informacja o zdarzeniu [raport]

Numer ewidencyjny zdarzenia:	***1112/15***			
Rodzaj zdarzenia:	***INCYDENT***			
Data zdarzenia:	***21 czerwca 2015 r.***			
Miejsce zdarzenia:	***EPWA***			
Rodzaj, typ statku powietrznego:	***ND***			
Dowódca SP:	***ND***			
Liczba ofiar / rodzaj obrażeń:	***Śmiertelne***	***Poważne***	***Lekkie***	***Bez obrażeń***
	-	-	-	-
Nadzorujący badanie:	***Edward Łojek***			
Podmiot badający:	***Użytkownik***			
Skład zespołu badawczego:	***nie wyznaczano***			
Forma dokumentu zawierającego wyniki:	***INFORMACJA O ZDARZENIU [RAPORT]***			
Zalecenia:	***NIE***			
Adresat zaleceń:	***NIE DOTYCZY***			
Data zakończenia badania:	***9 września 2016 r.***			

Przebieg i okoliczności zdarzenia:

W dniu 21 czerwca 2015 roku nastąpiło znaczące obciążenie przepustowości łącza internetowego operatora. W wyniku tego, działanie systemów, które wykorzystują to łącze, zostało spowolnione, co z kolei przełożyło się na brak możliwości ich efektywnego wykorzystania do przygotowania dokumentacji na rejs oraz odprawy pasażerów. Zagrożenie dla bezpieczeństwa lotniczego zostało zminimalizowane poprzez wstrzymanie uruchomienia rejsów, na które nie było możliwe przygotowanie wymaganej dokumentacji i odprawienie pasażerów. Zaistniałe zdarzenie miało istotny wpływ na ciągłość działalności przewozowej. W związku z tym został powołany sztab kryzysowy, którego zadaniem było zarządzanie dostępnymi zasobami w celu przywrócenia działalności przewozowej i minimalizacji konsekwencji operacyjnych zaistniałej sytuacji.
Działania podjęte przez operatora pozwoliły na przywrócenie normalnej przepustowości łącza internetowego. W rezultacie, szybkość działania systemów służących do przygotowywania

dokumentacji na rejs i odprawiania pasażerów umożliwiła ich wykorzystanie przez służby operacyjne.
Po analizie systemów wspomagania operacji lotniczych stwierdzono że nie doszło do ingerencji w systemy planowania, wyważania, obliczania osiągów i zarządzania ciągłą zdatnością do lotu. Incydent był incydentem informatycznym. Bezpośrednia przyczyna wyczerpania pasma łącza było długotrwałe wykorzystanie sieci operatora do ataku DDoS (Distributed Denial of Service).
Atak DDoS polega na działaniu prowadzącym do wyczerpania zasobów sieciowych lub obliczeniowych atakowanego serwisu tak, by uniemożliwić mu realizacje normalnych czynności. Ataki Reflected Amplification DDoS polegają na wysłaniu do wielu otwartych serwerów zapytań, dla których rozmiary odpowiedzi są znacznie większe od samego zapytania. Zapytania wysyłane są protokołem UDP ze sfałszowanym adresem źródłowym IP, pod który serwery wysyłają odpowiedzi. W ten sposób przy pomocy niewielkiego nakładu środków można bardzo efektywnie (bo z pomocą wielu serwerów) wygenerować olbrzymi ruch w sieci.
Po wystąpieniu ataku zwołano Sztab Kryzysowy oraz poinformowano CERT - rządowy zespół reagowania na incydenty, które w toku badania zwróciło uwagę na niedociągnięcia wymagające poprawy zabezpieczeń w funkcjonowaniu sieci IT operatora. W celu otrzymania głębszej analizy zwrócono się do zespołu CERT Polska działającego w strukturach Naukowej i Akademickiej Sieci Komputerowej (NASK) o dokonanie pełnej analizy. Zgodnie z analizą przeprowadzoną przez NASK atak nie był wymierzony w infrastrukturę sieci operatora.

Przyczyny zdarzenia lotniczego:

1. Zidentyfikowano pośrednie przyczyny incydentu których wybrane elementy to:
    - nieprawidłowa reguła w zaporze sieciowej Fortunatek (zastępującej wcześniejszą zaporę Checkpoint) otwierająca dostęp do wewnętrznego serwera DNS dla całego ruchu sieciowego, także spoza sieci użytkownika. Wprowadzenie tej reguły było wynikiem błędnego przeniesienia reguł z poprzedniej zapory;
    - nieskuteczność procedury dotyczącej działania podczas ataków DDoS. Przewidziane procedura działania operatorów nie wystąpiły lub były nieadekwatne. Plan działań nie przewidywał wewnętrznych czynności prowadzących do rozpoznania i zniesienia ataku;
    - brak wykwalifikowanego wsparcia dla zapory FortiGate w trakcie przełączenia. Zdalne wsparcie zapewniane przez firmę Trecom okazało się niewystarczające;
    - brak procedur dotyczących zapewnienia łączności dla krytycznych systemów (np. zapasowe, niezależne łącza w innym systemie autonomicznym).
2. Monitoring ruchu sieciowego w wewnętrznych systemach, w szczególności testów przełączeniowych jak i właściwego przełączenia był nieskuteczny.
3. Nieskuteczne monitorowanie zdarzeń bezpieczeństwa dotyczących systemów wewnętrznych, takich jak nieuprawnione próby logowania, nadmierne obciążenie, błędna konfiguracja.

Zastosowane środki profilaktyczne:

1. Zapoznano członków Zarządu z Raportem i rekomendacją odnośnie rozważenia systemowego wprowadzenia Bussiness Continuity Management. BCM powinien obejmować zarówno obszary IT, infrastrukturę, korporacyjne jak również operacyjne, ponieważ w przypadku braku zasobów IT obecnie istnieją nieliczne procesy pozwalające na realizację operacji (np. obliczenia Mass & Balance).

2. Rekomendacje dla obszaru IT zostały zdefiniowane w raporcie NASK.
3. Zdarzenie zostało zarejestrowane w bazie SMS operatora. Dokonano klasyfikacji zgodnie z przyjętymi kryteriami. W związku z tym, zdarzenie zostanie ujęte we wskaźnikach bezpieczeństwa lotniczego, które są monitorowane zgodnie z zasadami opisanymi w Podręczniku Zarządzania Bezpieczeństwem Lotniczym.

Zalecenia dotyczące bezpieczeństwa:

Komisja nie formułowała zaleceń dotyczących bezpieczeństwa.

Koniec

	Imię i nazwisko	Podpis
Nadzorujący badanie:	Edward Łojek	*podpis na oryginale*