Cyberdefence 24

aut. Łukasz Boguszewski 12.06.2018

AWARIA SYSTEMÓW REJESTRÓW PAŃSTWOWYCH. LEKCJA NA PRZYSZŁOŚĆ [KOMENTARZ]

Ministerstwo Cyfryzacji poinformowało o awarii systemów informatycznych w urzędach w Polsce. Problemy dotyczyły działania między innymi Systemu Rejestrów Państwowych. Awarię udało się usunąć, ale warto przy tej okazji zadać kilka ważnych pytań.

System Rejestrów Państwowych (SRP) to wdrożony za ponad 100 mln PLN, opracowany przez Ministerstwo Spraw Wewnętrznych i Centralny Ośrodek Informatyki „system systemów" integrujący dane o obywatelach, rozproszone wcześniej w innych systemach. Lokalne systemy urzędów miast i gmin zastąpiono ogólnokrajowym systemem elektronicznym. Najważniejsze ewidencje państwa jak rejestr PESEL, Rejestr Dowodów Osobistych, baza CEPIK czy ePUAP zintegrowane są aplikacją ŹRÓDŁO - dedykowanym programem do przetwarzania danych w Systemie Rejestrów Państwowych.

Sprawność systemu była wielokrotnie podważana przez różne instytucje państwa. Najwyższa Izba Kontroli (NIK) wskazywała w marcu 2017 roku na szereg nieprawidłowości w funkcjonowaniu programu ŻRÓDŁO. Jedną z kluczowych uwag było niewłaściwe zorganizowanie zarządzania bezpieczeństwem systemu. Także Generalny Inspektor Ochrony Danych Osobowych (GIODO) wydał decyzję nakazującą Ministerstwu Cyfryzacji poprawę bezpieczeństwa danych zawartych w rejestrze PESEL, będącym jednym ze składowych SRP.

W dniu 12 czerwca br. Ministerstwo Cyfryzacji poinformowało o wystąpieniu dużej awarii Systemu Rejestrów Państwowych, a co za tym idzie wstrzymaniu działania podstawowych serwisów obsługujących dane obywateli: OBYWATEL, CEPIK, ePUAP, SRP. Większość urzędów opustoszała, a funkcjonalności systemów informatycznych zostały zawieszone.

Były Szef Agencji Wywiadu, Grzegorz Małecki w rozmowie z CyberDefence24.pl zauważa, ze można wskazać kilka powodów awarii, przy czym najbardziej prawdopodobnym wydaje się być błąd techniczny. Nie można także wykluczyć błędu ludzkiego spowodowanego niewłaściwą obsługą.

G. Małecki nie wyklucza także działania celowego, czyli operacji grup hakerskich, których celem mogło być testowanie i sparaliżowanie systemu, oraz sprawdzenie mechanizmów reagowania w celu udoskonalania oprogramowań typu malware. Możliwe jest także, ale bardzo mało prawdopodobne, działanie celowe podmiotów zewnętrznych. Niemniej jednak służby specjalne, odpowiedzialne za bezpieczeństwo cyberprzestrzeni, w ocenie G. Małeckiego, powinny zająć się szczegółową analizą tego przypadku.

> *Potrzebna jest ocena sytuacji i wyciągnięcie wniosków. Kolejny etap to poprawa systemu. Nawet jeśli jest to kosztowne, to dane osobowe obywateli powinny być chronione pod każdym względem. Dane osobowe obywateli to zasób strategiczny. Państwo ma obowiązek ochrony danych. Przykład niewłaściwego użycia mieliśmy za pośrednictwem np. Cambridge Analitics*
>
> *Grzegorz Małecki - były szef Agencji Wywiadu*

Sama reakcja Ministerstwa Cyfryzacji, które za pośrednictwem mediów podało, że naprawa będzie długotrwała wskazywać może, że w sprawie jest znacznie więcej znaków zapytania niż odpowiedzi. Wydaje się także, że SRP nie posiada odpowiedniej architektury zapewniając redundancje, wysoką dostępność (high availability) i skalowalność, a także że w systemie występują tzw. single point of failure (SPOF). Pojawia się także pytanie, czy tak kluczowe systemy informatyczne państwa nie powinny mieć architektury rozproszonej w oparciu o łatwo skalowalne, bezstanowe kontenery aplikacyjne lub niezależne środowiska uruchomieniowe. Być może przyszłością są systemy oparte na nowoczesnych technologiach jak blockchain, przy jednoczesnym unikaniu SPOF.

Grzegorz Małecki podkreśla, że niezależnie od powodów awarii należy dokonać starannej i sumiennej analizy tego co się wydarzyło. Następnie warto wyciągnąć wnioski i zaimplementować rozwiązania, służące poprawie bezpieczeństwa. To czego nie wolno zrobić, to zbagatelizować takie wydarzenie i nic się z niego nie nauczyć.