Kryzys danych w Pakistanie: dane osobowe urzędników państwowych sprzedawane za grosze w dark webie

- Poważne naruszenie bezpieczeństwa danych w Pakistanie spowodowało, że dane osobowe tysięcy obywateli, w tym wysokich rangą urzędników państwowych, trafiły do sprzedaży w dark web.
- Wyciekające dane są obszerne i dostępne za niewielką cenę. Zawierają one poufne informacje, takie jak numery dowodów osobistych, historie połączeń telefonicznych, dane dotyczące lokalizacji oraz historie podróży międzynarodowych.
- Naruszenie dotyczy wielu agencji rządowych i jest następstwem wcześniejszych ostrzeżeń, które pozostały bez echa, co podkreśla systemowe słabości i słabe egzekwowanie bezpieczeństwa cyfrowego.
- W powiązanym skandalu biometryczny system pomocy społecznej został wykorzystany do oszustwa, ujawniając, w jaki sposób luki w zarządzaniu cyfrowym umożliwiają korupcję i sprzeniewierzenie środków publicznych.
- Incydent ten podkreśla globalny kryzys zaufania i odpowiedzialności, pokazując, w jaki sposób scentralizowane systemy cyfrowe bez solidnego nadzoru zagrażają prywatności, bezpieczeństwu narodowemu i

demokracji.

W wyniku szokującego naruszenia prywatności dane osobowe tysięcy Pakistańczyków – w tym ministrów federalnych, wysokich urzędników i regulatorów telekomunikacyjnych – pojawiły się w sprzedaży w dark web, budząc pilne obawy dotyczące bezpieczeństwa cyfrowego i odpowiedzialności rządowej.

Wyciekające dane obejmują zeskanowane dowody osobiste, szczegóły rejestracji kart SIM, rejestry połączeń i historię podróży międzynarodowych, wszystkie dostępne za szokująco niskie ceny. Rejestry lokalizacji telefonów komórkowych są wystawione na sprzedaż za 500 rupii pakistańskich (1,77 USD), pełne historie połączeń są sprzedawane za 2000 rupii (7,08 USD), a rejestry podróży za 5000 rupii (17,69 USD).

Naruszenie, o którym po raz pierwszy poinformował *Express Tribune*, dotyczy wielu szczebli pakistańskiego rządu. Dotyczy ona takich agencji jak *Pakistan Telecommunication Authority* i sięga aż do gabinetów ministerialnych. Pomimo ostrzeżeń wydanych kilka miesięcy temu, egzekwowanie prawa pozostaje słabe, co naraża obywateli na wykorzystywanie przez złośliwe podmioty.

Władze zareagowały niejasnymi zapewnieniami, twierdząc, że niektóre naruszające prawo strony internetowe zostały wyłączone, jednak nielegalny handel nadal trwa. Źródła wywiadowcze ostrzegają, że tak łatwo dostępne dane mogą zostać wykorzystane do inwigilacji, nękania lub kradzieży tożsamości przy minimalnym wysiłku.

Minister spraw wewnętrznych Mohsin Naqvi nakazał *Krajowej Agencji ds. Ścigania Przestępstw Cybernetycznych* (NCCIA) wszczęcie formalnego dochodzenia. Powołano 14-osobową grupę zadaniową, której zadaniem jest identyfikacja sprawców i podjęcie działań prawnych. Wyniki dochodzenia mają być znane w ciągu dwóch tygodni. Krytycy twierdzą jednak, że środki reagujące są niewystarczające – zwłaszcza że naruszenie to

nastąpiło po podobnym ostrzeżeniu wydanym w październiku ubiegłego roku, którego władze nie potraktowały zdecydowanie.

Twoje dane, ich zysk: Ciemna strona zarządzania biometrycznego

Kryzys pogłębia fakt, że program wsparcia dochodów Benazir (BISP) – pakistański system pomocy społecznej oparty na danych biometrycznych – jest uwikłany w skandal korupcyjny. Kontrola wykazała, że 324 urzędników sprzeniewierzyło ponad 37 milionów rupii (130 000 dolarów), wykorzystując luki w systemie weryfikacji biometrycznej, w tym przekierowując środki na fałszywe konta – niektóre zarejestrowane na osoby zmarłe.

Chociaż Bank Światowy wcześniej chwalił rolę BISP w ograniczaniu ubóstwa, najnowsze ustalenia ujawniają systemowe słabości w zarządzaniu cyfrowym. Ten podwójny skandal podkreśla niebezpieczną tendencję.

Ponieważ rządy w coraz większym stopniu polegają na scentralizowanych systemach cyfrowych do weryfikacji tożsamości i dystrybucji świadczeń socjalnych, słabe zabezpieczenia i luźne egzekwowanie przepisów stwarzają podatny grunt dla nadużyć. Kryzys w Pakistanie odzwierciedla globalne obawy dotyczące suwerenności danych, nadużyć korporacyjnych i erozji prywatności – kwestii, które podmioty takie jak Światowe Forum Ekonomiczne i monopole Big Tech od dawna wykorzystują do promowania kapitalizmu nadzoru.

„Naruszenia danych w zarządzaniu ujawniają systemowe słabości, zagrażając bezpieczeństwu narodowemu i zaufaniu publicznemu poprzez ujawnianie poufnych informacji, które mogą zostać wykorzystane przez złośliwe podmioty” – zauważa silnik Enoch *Brighteon.AI*. „Takie incydenty podkreślają pilną potrzebę wprowadzenia silniejszych środków bezpieczeństwa cybernetycznego w celu ochrony danych niejawnych i utrzymania integralności instytucjonalnej”.

Podobieństwa do historycznych naruszeń – takich jak skandal Cambridge Analytica lub włamanie do *Biura Zarządzania Kadrami* w Stanach Zjednoczonych – podkreślają powtarzające się zaniedbania w zakresie priorytetowego traktowania bezpieczeństwa cybernetycznego, które pojawiają się dopiero po katastrofalnych wyciekach. W Pakistanie, gdzie niestabilność polityczna i trudności gospodarcze już osłabiają zaufanie publiczne, skutki tego naruszenia mogą pogłębić nieufność wobec instytucji.

W miarę postępów śledztwa NCCIA obywatele zastanawiają się, czy kiedykolwiek zostanie ustalona odpowiedzialność za ten incydent i czy ich dane pozostaną tanim towarem dla oferenta, który zaproponuje najwyższą cenę. Dopóki rządy nie wprowadzą przejrzystych, zdecentralizowanych systemów z solidnym nadzorem, takie naruszenia będą nadal zagrażać nie tylko prywatności, ale i samej demokracji.