PEŁNE WYJAŚNIENIE POZIOMU BEZPIECZEŃSTWA SYSTEMU PESEL

Sprawa wycieku danych PESEL pojawiła się pod koniec zeszłego miesiąca. Po wyjaśnieniach Ministerstwa Cyfryzacji okazało się, że nie doszło do żadnego wycieku, jedynie kancelarie komornicze korzystały z możliwości odciążenia sieci, pobierając dane osób, wobec których było prowadzone postępowanie, w godzinach nocnych. Poniżej Ministerstwo Cyfryzacji odpowiedziało na kilka pytań skierowanych drogą elektroniczną.

Czy system monitoringu obecnie działający w ramach struktur Ministerstwa Cyfryzacji oraz podległego mu NASK oraz ostatnio powołanego Narodowego Centrum Cyberbezpieczeństwa zdały swój pierwszy prawdziwy test (w odniesieniu do ostatniej afery PESEL)?

Dzięki systemowi, który zaczęło tworzyć i wdrażać Ministerstwo Cyfryzacji udało się wykryć niepokojące anomalie. Poinformowane o tym zostały stosowne organy. W związku z tym, że incydent dotyczył wewnętrznych procedur Systemu Rejestrów Państwowych, w przypadku których reagowanie na incydenty leży w kompetencji Agencji Bezpieczeństwa Wewnętrznego oraz dotyczył wydzielonej sieci, został powiadomiony o tym incydencie właściwy w tej sytuacji zespół reagowania – CERT.GOV.PL.

Co w przypadku kiedy taki atak mógłby mieć miejsce na systemy sieci odseparowane od globalnego internetu? Czy wyciek takich danych mógłby zaszkodzić obywatelom, zanim zadziałałby odpowiedni mechanizmy bezpieczeństwa?

Po stronie rejestrów nie stwierdzono żadnego nieuprawnionego poboru danych. Kancelarie komornicze są do tego uprawnione. Nie należy też mówić o „wycieku" danych. Prokuratura nie stwierdziła wycieku danych do osób nieuprawnionych. Nie mamy też do czynienia z tzw. włamaniem hakerskim, czyli z pokonaniem mechanizmów bezpieczeństwa.

Wiadomo dokładnie skąd pochodziły zapytania i kogo konkretnie dotyczyły. System jest monitorowany na bieżąco. Ministerstwo Cyfryzacji i podległy mu Centralny Ośrodek Informatyki robią to w ramach normalnych procedur.

Jak oceniają Państwo szybkość reagowania całego systemu zabezpieczeń na anomalie, jakim niewątpliwie było ściąganie przez kancelarie komornicze danych z systemu PESEL w godzinach nocnych?

System bezpieczeństwa Rejestrów Państwowych w Centralnym Ośrodku Informatyki jest dopiero tworzony. Z dniem 1 czerwca 2016 powstał w COI dedykowany Pion Bezpieczeństwa, w którego skład weszli pracownicy realizujący zadania związane z zapewnieniem bezpieczeństwa. Spowodowało to zwiększenie możliwości wykrywania zagrożeń (w tym monitorowania bezpieczeństwa SRP).

Czy przepustowość sieci w przypadku tego lub innych systemów wykorzystywanych przez administracje rządową jest odpowiednio przystosowanych do norm obecnych w innych krajach Europejskich. Czy przewidują Państwo usprawnienie oraz zwiększenie możliwości systemu w ramach pracy odpowiednich podmiotów odpowiedzialnych za samą infrastrukturę?

Przepustowość sieci dostępowej - jak i innych usług - jest w miarę możliwości na bieżąco dopasowywana do aktualnych potrzeb użytkowników oraz systematycznie modernizowana, by zapewnić adekwatny poziomu dostępu do usług.

Czy uważają Państwo, że cała nagonka na wyciek danych, który nie miał miejsca jest sterowana przez osoby z zewnątrz, czy po prostu w wyniku wakacyjnego braku tematów, informacja została rozdmuchana do dużych rozmiarów?

Ministerstwo od początku mówiło jedynie o anomaliach dotyczących poboru danych z rejestru, które należy wyjaśnić. Z tym zastrzeżeniem, że poboru dokonują podmioty posiadające do tego uprawnienia, a dostęp ten jest możliwy tylko w ramach określonych reguł i warunków dostępu.

Wzmożona aktywność komorników trwała od marca zeszłego roku, dlaczego Ministerstwo Cyfryzacji zareagowało dopiero teraz?

By stwierdzić wystąpienie anomalii - niezbędne jest prowadzenie obserwacji danych przez długi okres czasu.

Pracownicy ZUS mają dostęp do bazy PESEL z komputerów podłączonych do internetu? Czy to prawda? Czy to bezpieczne? Czy przechodzą jakieś specjalne przeszkolenie?

W chwili obecnej bezpośredni dostęp do rejestru PESEL za pomocą aplikacji ŹRÓDŁO posiada 4 pracowników Zakładu Ubezpieczeń Społecznych i jest to dostęp realizowany za pomocą wydzielonej sieci, wykorzystywanej przez ZUS do połączenia z Systemem Rejestrów Państwowych, nie posiadającej styku z siecią Internet.

Dodatkowo ZUS posiada możliwość pobierania z rejestru PESEL określonych danych osobowych, zgodnych z przepisami prawa, do swojego systemu. Proces zasilania systemu ZUS danymi z rejestru PESEL wykorzystuje również dedykowaną sieć, bez styku z siecią Internet. Od momentu pobrania danych osobowych z rejestru PESEL to ZUS jest ich dysponentem i odpowiada za ich należyte przetwarzanie oraz zabezpieczenie.

Reakcja Polaków na wyciek PESEL świadczy o niewielkim zaufaniu do rządowych organizacji? Pomimo oficjalnego komunikatu Ministerstwa Cyfryzacji, wciąż wiele osób uważa wyciek PESEL faktycznie nastąpił, czy Ministerstwo Cyfryzacji planuje wprowadzić działania ukierunkowane na zwiększenie zaufania i świadomości cyberbezpieczeństwa w Polsce?

Niezwykle ważnym elementem budowania sprawnego systemu cyberbezpieczeństwa jest świadomość społeczeństwa i użytkowników systemów informatycznych w zakresie bezpieczeństwa. Równie istotne jest zaangażowanie wszystkich podmiotów odpowiedzialnych za bezpieczeństwo i edukację w proces podnoszenia wiedzy na temat zagrożeń oraz budowania zaufania do usług publicznych. Ponadto uważamy, że w tym zakresie powinna być rozwijana współpraca sektora publicznego z sektorem prywatnym i organizacjami pozarządowymi oraz ośrodkami akademickimi i centrami naukowo-badawczymi.

Jak zabezpieczone są komputery obsługujące system PESEL?

Komputery obsługujące system PESEL są zabezpieczane zgodnie z Ustawą o Ochronie Danych Osobowych, zgodnie wytycznymi zawartymi w Polityce Bezpieczeństwa i Instrukcji zarządzania systemem teleinformatycznym oraz innymi regulacjami związanymi z bezpieczeństwem w danej jednostce, w szczególności z wytycznymi zawartymi w wymaganiach i zaleceniach dla podmiotów wnioskujących o dostęp do rejestrów państwowych poprzez aplikację Źródło, z wykorzystaniem sieci dedykowanej.

Czy istnieje świadomość, że komputery działające w ramach technologii Air-Gap również mogą stać się celem ataku.

Jesteśmy tego świadomi. W działaniach w zakresie cyberbezpieczeństwa brane są pod uwagę wszelkie aspekty.

Kto kontroluje że pracownik kancelarii nie wyniesie pobranych danych z systemu PESEL? W szczególności jak pracował w nocy.

Za przetwarzanie danych z rejestru odpowiedzialny jest kierownik jednostki organizacyjnej, której dane są udostępniane.

Czy przeprowadzane są specjalne szkolenia dla komorników z zakresu cyberbezpieczeństwa (szczególnie dla tych, którzy są odpowiedzialni za obsługę systemów PESEL)?

Nie są przeprowadzane specjalne szkolenia, natomiast każdy podmiot jest zapoznawany z Polityką Bezpieczeństwa. Fakt zapoznania z dokumentami jest dodatkowo potwierdzany podpisem.

Jaki system jest zabezpieczeń w kancelariach komorniczych?

Zgodnie z Ustawą o Ochronie Danych Osobowych, zgodnie wytycznymi zawartymi w Polityce Bezpieczeństwa i Instrukcji zarządzania systemem teleinformatycznym oraz innymi regulacjami związanymi z bezpieczeństwem w danej jednostce, w szczególności z wytycznymi zawartymi w wymaganiach i zaleceniach dla podmiotów wnioskujących o dostęp do rejestrów państwowych objętych projektem pl.ID, poprzez aplikację Źródło, z wykorzystaniem sieci dedykowanej.

Kto nadzoruje, że systemy są odpowiednio zabezpieczone?

Za nadzór nad systemami odpowiada kierownik jednostki organizacyjnej, w której one funkcjonują.

Czy przeprowadzane są coroczne audyty bezpieczeństwa? Jeśli tak kto je przeprowadza?

Do dziś nie były przeprowadzane dodatkowe audyty bezpieczeństwa w podmiotach posiadających dostęp do rejestru. Jednocześnie zgodnie z *Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (§ 20, pkt. 2 ust. 14.) - podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Kto jest odpowiedzialny za administrację systemu PESEL-NET?

Za administrację systemem PESEL-NET odpowiedzialny jest Minister Spraw Wewnętrznych i Administracji.

Dlaczego dopiero teraz Ministerstwo Cyfryzacji włącza się w audyt bezpieczeństwa systemów komputerowych w kancelariach komorniczych?

Sprawa została wykryta, gdy służby odpowiedzialne za bezpieczeństwo zauważyły niepokojąco wysokie ilości pobieranych danych (również nocą). Natychmiast zareagowaliśmy doniesieniem do organów ścigania.

Czytaj też: Nie ma ryzyka w obszarze bezpieczeństwa bankowości z powodu zamieszania wokół systemu PESEL