NIE WYSTARCZY DOBRY SYSTEM IT

Zarządzanie bezpieczeństwem cyfrowym w samorządach

Samorządy terytorialne to skomplikowane organizmy. Administracja samorządowa, wykonując swoje ustawowe zadania, gromadzi i przetwarza ogromne ilości danych. Są to dane osobowe obywateli (w tym dane wrażliwe), dane dotyczące gospodarki, administracji itd. Dane związane z Inteligentnymi Systemami Transportowymi oraz innymi rozwiązaniami Smart City. Samorządy gospodarują również znacznym majątkiem i dysponują znacznymi sumami pieniędzy. Bezpieczeństwo informacyjne administracji samorządowej przekłada się na bezpieczeństwo obywateli, którzy z mocy prawa przekazują wiele swoich danych urzędom[1]. Przede wszystkim jednak organy samorządu terytorialnego sprawują powierzoną im ustawami władzę i odpowiadają za funkcjonowanie społeczeństwa i państwa.

Tymczasem dane i pieniądze stanowią główny cel cyberprzestępców motywowanych ekonomicznie. Władza i administracja (a raczej ich destabilizacja) to główny cel cyberprzestępców sponsorowanych przez państwa, grupy terrorystyczne itp.

Dlatego też w sposób oczywisty jednostki samorządu terytorialnego stają się przedmiotem ataków hakerskich. Potwierdzają to zresztą różnorakie statystki[2] „(…) analiza posiadanych przez Zespół CERT. GOV.PL danych potwierdza, że najwięcej prób infekcji oprogramowaniem złośliwym typu botnet dotyczy głównie sektorów: służby – 30,72%, kluczowe przedsiębiorstwa – 21,62% oraz administracja terenowa – 7,22%". Nie ulega najmniejszym wątpliwościom, że administracja samorządowa jest zagrożona atakami informatycznymi. Przytoczmy kilka powszechnie wskazywanych ataków z ostatnich lat:

- na stronie internetowej Urzędu Miasta Poznania dostępne były informacje potrzebne do logowania do wersji szkoleniowej i testowej systemu Wsparcia Organów Wyborczych,
- dane osobowe inicjatorów referendum wyciekły z Urzędu Miasta w Piotrkowie Trybunalskim,
- w Urzędzie Miejskim w Toruniu atakującym udało się dokonać zmiany zawartości (ang. defacement) strony internetowej,
- taka sama sytuacja miała miejsce z witryną internetową należącą do Wielkopolskiego Urzędu Wojewódzkiego w Poznaniu,
- kielecka policja zatrzymała osobę, która zgłosiła się do urzędu wojewódzkiego i powiadomiła, że udało mu się włamać na jeden z należących do urzędu serwerów,
- strona internetowa Urzędu Miasta Łodzi wraz z niektórymi serwisami (np. zapisanie się na wizytę w Wydziale Praw Jazdy i Rejestracji Pojazdów) została zablokowana na kilka dni przez hakerów. Urząd Miasta Łodzi zapłacił aż 43 tys. zł brutto firmie, która „czyściła" system po ataku oraz za ponowne „postawienie" strony,
- poprzez przekierowanie na fałszywe konta przelewów w pięciu urzędach gmin (Błażowa, Belsk Duży, Gidle, Rząśnia, Jaworzno) atakującym udało się ukraść ponad 2 miliony złotych[3].

Wymusza to podejmowanie działań zabezpieczających systemy teleinformatyczne, którymi posługują się samorządy.

Część podstawowych zasad bezpieczeństwa wynika wprost z obowiązujących przepisów prawa. Wiele nowych, powszechnie obowiązujących regulacji wejdzie w życie niebawem, w szczególności bardziej zaawansowane środki określone są w publikowanych

przez stronę publiczną lub organizacje branżowe zaleceniach, rekomendacjach, kodeksach postępowania lub zbiorach dobrych praktyk.

Należy pamiętać również, że administracja samorządowa – pośrednio lub bezpośrednio – zarządza infrastrukturą krytyczną, a wszelkie incydenty w tym obszarze mogą mieć bardzo duży wpływ na społeczeństwo. Nietrudno wyobrazić sobie również, że celem ataku mogą stać się krytyczne dla zdrowia i życia ludzkiego, a zarządzane przez samorządy, transport i komunikacja, szpitale czy zaopatrzenie w wodę pitną.

Jednostki samorządu terytorialnego muszą dostosować się nie tylko do norm prawnych wyznaczających standardy ochrony, ale także do realiów szybko zmieniającej się rzeczywistości cyberprzestrzennej. Powinny także, wzorem innych podmiotów publicznych i prywatnych, wprowadzać skuteczne strategie zarządzania ryzykiem w oparciu o dogłębną analizę możliwości lepszego przygotowania do obrony. W tym celu powinny włączyć się aktywnie w realizację państwowej strategii cyberbezpieczeństwa, wdrażać obowiązujące przepisy oraz międzynarodowe standardy ISO.

PAŃSTWOWA STRATEGIA CYBERBEZPIECZEŃSTWA

9 maja 2017 r. została przyjęta przez rząd strategia cyberbezpieczeństwa, której oficjalny tytuł to „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022". W dokumencie dostrzeżona została poważna rola samorządu terytorialnego. Zgodnie z Krajowymi Ramami Polityki Cyberbezpieczeństwa „rząd w ramach współpracy administracji rządowej z administracją samorządową będzie rekomendował i działał na rzecz jednostek samorządu terytorialnego w zakresie tworzenia klastrów bezpieczeństwa dla tej administracji".

Należy zatem spodziewać się zwiększenia aktywności rządu w zakresie współpracy z samorządami, ale także nałożenia w drodze regulacji ustawowych dodatkowych obowiązków i standardów w tym zakresie. Jednostki samorządu terytorialnego powinny być aktywne we współpracy z administracją rządową w zakresie budowy cyberbezpieczeństwa.

KRAJOWE RAMY INTEROPERACYJNOŚCI

Zagadnienia cyberbezpieczeństwa, pojmowanego z jednej strony jako bezpieczeństwo systemów teleinformatycznych, a z drugiej jako bezpieczeństwo informacji przetwarzanych w tych systemach, regulowane są w różnych aktach prawnych. Jednym z ważniejszych jest ustawa o informatyzacji[4], a w szczególności akt wykonawczy do tej ustawy – Krajowe Ramy Interoperacyjności[5]. Zgodnie ze wspomnianą ustawą samorządy zobowiązane są używać do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów.

Mimo obowiązujących przepisów stan zabezpieczeń w administracji samorządowej nie jest zadowalający:

- 33 proc. urzędów samorządowych nie ma na wyposażeniu urządzenia typu firewall[6],
- 24% urzędów samorządowych ma opracowaną analizę ryzyka[7],
- 12% urzędów samorządowych nie posiada polityki bezpieczeństwa informacji[8].

OCHRONA DANYCH OSOBOWYCH

W kontekście cyberbezpieczeństwa należy również rozważać kwestie ochrony danych osobowych. Na ten temat, zarówno w odniesieniu do obowiązującej jeszcze ustawy o ochronie danych osobowych[9] jak i w odniesieniu do RODO[10], wylano morze atramentu. W tym miejscu należy jedynie wspomnieć, że RODO, które weszło w życie 25 maja 2018 r., wyznacza wyższy standard ochrony danych dotyczących osób fizycznych. Rozporządzenie nie wymaga implementacji, jednakże nie oznacza to, że nie zmienią się ustawy krajowe. Wraz z wejściem w życie RODO znacznie zwiększą się możliwości prawnego dochodzenia odszkodowań z tytułu naruszenia danych osobowych na drodze cywilnej. Tak więc nawet jeżeli samorządy terytorialne nie będą narażone na dotkliwe finansowe sankcje administracyjne, to będą ponosiły odpowiedzialność cywilnoprawną.

DYREKTYWA NIS I USTAWA O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Bardzo ważnym krokiem w rozwoju standardów prawnych dotyczących budowy cyberbezpieczeństwa będzie wejście w życie ustawy o krajowym systemie cyberbezpieczeństwa, implementującej dyrektywę NIS[11]. Dotyczyć ona będzie w szczególności tzw. operatorów usług kluczowych, którzy w pewnej mie-

rze pokrywają się z podmiotami odpowiedzialnymi za infrastrukturę krytyczną. W konsekwencji może dotyczyć samorządów lub części przedsiębiorstw komunalnych. Ustawa implementująca dyrektywę NIS ustanowi m.in. procedury i obowiązki zgłaszania incydentów dotyczących cyberbezpieczeństwa oraz wyznaczy szczególne wymogi dotyczące zapewniania bezpieczeństwa przez operatorów usług kluczowych. Ustawa implementująca dyrektywę NIS powinna wkrótce zostać przyjęta przez rząd, przesłana do parlamentu i niezwłocznie wejść w życie.

Jednostki samorządu terytorialnego powinny podjąć pilne i kompleksowe działania na rzecz budowy cyberbezpieczeństwa. Powinny zostać opracowane standardy zarządzania dotyczące cyberbezpieczeństwa określające zachowania mające chronić przed incydentami, jak i przewidujące plany działań po atakach. Włodarze samorządowi muszą pamiętać, że nie wystarczy kupić dobry system IT, ale konieczne jest również przygotowanie organizacyjne urzędu, szkolenia i budowa świadomości zagrożeń. Konieczne jest również przygotowanie (i przećwiczenie) procedur na wypadek zaistnienia incydentu. Obowiązuje bowiem niestety zasada, aby nie pytać, czy tylko kiedy zostaniemy skutecznie zaatakowani.

Wojciech Dziomdziora
radca prawny, Counsel w kancelarii
Domański Zakrzewski Palinka sp.k.

PRZYPISY / PODSTAWA PRAWNA:

1. *D. Lisiak-Felicka, M. Szmit „Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia", European Association for Security, Kraków 2016, s. 68*
2. *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2015 roku; Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL; Warszawa, kwiecień 2016*
3. *D. Lisiak-Felicka, M. Szmit „Cyberbezpieczeństwo ...." op.cit. str. 11 i nast*
4. *Ustawa z 17 lutego 2015 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. jedn. Dz.U. z 2017 r. poz. 570 ze zm.)*
5. *Rozporządzenie 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 (t.j. Dz.U. z 2016 r. poz. 113 ze zm.)*
6. *Badanie Fortinet, za http://www.polskaszerokopasmowa.pl/artykuly/jak-to-jest-z-cyberbezpieczenstwem-w-samorzadach.html*
7. *ibid.*
8. *P. Jatkiewicz, „Raport z badań: Wdrożenie wybranych wymagań dotyczących systemów informatycznych oraz Krajowych Ram Interoperacyjności w jednostkach samorządu terytorialnego, PTI, Warszawa 2016 r.*
9. *Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2016 r. poz. 922 ze zm.)*
10. *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*
11. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*