SAMORZĄDY CORAZ ATRAKCYJNIEJSZYM CELEM DLA CYBERPRZESTĘPCÓW. EKSPERCI ZNAJĄ ROZWIĄZANIE PROBLEMU

Rozwijające kolejne cyfrowe usługi samorządy stają się coraz atrakcyjniejszym celem dla cyberprzestępców. Eksperci ostrzegają że dzieje się tak z uwagi na ograniczone środki finansowe, jakie mogą przeznaczyć na sprzęt i specjalistów.

Wiele urzędów oferuje obecnie usługi za pośrednictwem aplikacji mobilnych lub internetowych, wykorzystując do tego środowiska chmurowe. To oznacza, że jednostki samorządowe zbierają, przechowują i przetwarzają coraz więcej wrażliwych danych obywateli, które w przypadku naruszenia bezpieczeństwa IT w urzędach mogą zostać wykradzione.

Dostarczająca rozwiązania z zakresu cyberbezpieczeństwa firma Fortinet zwraca uwagę, że infrastruktury IT są coraz bardziej rozproszone i niejednorodne, a zakres możliwego ataku coraz większy, podczas gdy możliwości władz lokalnych w zakresie obrony i reagowania nie zawsze są wystarczające. Samorządy m.in. stają się łatwym celem dla oprogramowania typu ransomware, które najpierw szyfruje dane na zainfekowanym urządzeniu, a następnie żąda wpłacenia okupu w zamian za ich odblokowanie. Widoczny jest już trend: hakerzy odchodzą od masowych ataków na wszystkich, w zamian przeprowadzając celowane, poprzedzone odpowiednim rozpoznaniem ataki na konkretne instytucje, które uznają za gotowe do zapłacenia okupu.

Z problemem tym zetknęło się już wiele miast USA, które zdecydowały się zapłacić po kilkaset tysięcy USD, by uruchomić miejskie systemy teleinformatyczne.

Według dyrektor firmy Fortinet w Polsce Jolanty Malak, warto stosować zintegrowane rozwiązania ochronne, które są bardziej efektywne kosztowo oraz łatwiejsze do wdrażania i administrowania niż zatrudnienie grona ekspertów odpowiedzialnych za ochronę środowiska IT. "Jeśli wszystkimi elementami infrastruktury można zarządzać za pomocą centralnego interfejsu, liczba godzin pracy przeznaczonych na zabezpieczanie znacząco spada, a koszty mogą być znacznie niższe" – podkreśliła.