Kategoria: Aktualności
Opublikowano: poniedziałek, 19, wrzesień 2022 13:26
Alicja Cisowska

Cyberprzestępcy zagrażają nie tylko branży komercyjnej, ale również sektorowi publicznemu, który jest odpowiedzialny za infrastrukturę krytyczną dla funkcjonowania państwa oraz przetwarzanie danych mieszkańców i obywateli.

W ubiegłym roku aż 80% organizacji nadzorujących infrastrukturę krytyczną doświadczyło ataku ransomware, a w następstwie aktualnej sytuacji geopolitycznej, w Polsce do 30 listopada br. obowiązuje trzeci stopień alarmowy CRP, sygnalizujący zagrożenia dla państwowej infrastruktury. Nic więc dziwnego, że coraz częściej przetargi w sektorze publicznym wymagają od wykonawców certyfikatów poświadczających posiadanie kompetencji z zakresu przetwarzania danych oraz zapewnienia ich bezpieczeństwa.

W najnowszym zestawieniu najbezpieczniejszych cyfrowo krajów Polska uplasowała się w pierwszej dwudziestce rankingu – to wyżej niż takie kraje Europy Zachodniej jak Niemcy, Francja czy Hiszpania. W rankingu autorstwa firmy Comparitech uwzględniono również ocenę poziomu zabezpieczeń państwowych.

Infrastruktura pod cybernetycznym ostrzałem

Zagrożenie dotyczy nie tylko infrastruktury centralnej, ale również lokalnej. W Polsce już w pierwszych miesiącach pandemii wzrosła liczba ataków hakerskich na serwery jednostek samorządu terytorialnego. Aktualnie globalnie nawet 4 na 10 naruszeń bezpieczeństwa informacji za pośrednictwem ransomware dotyczy władz lokalnych. Mając na uwadze, że nawet 94% ataków tego typu wiąże się z próbą zniszczenia kopii zapasowych, wyzwanie jest realne – w ostatnich latach samorządy straciły średnio od 20 do 60 tys. złotych w wyniku udanych naruszeń bezpieczeństwa. Koszt obejmuje m.in. ukradzione pieniądze, ale również opłaty dla firm przywracających system do działania po incydencie bezpieczeństwa.

W przetargach stawia się na bezpieczeństwo

W kontekście powyższych danych instytucje sektora publicznego – zarówno na szczeblu centralnym, jak i lokalnym – przy ogłaszaniu zamówień na elementy infrastruktury informatycznej szczególnie uważnie sprawdzają kompetencje wykonawców związane z przetwarzaniem i zabezpieczaniem danych. Tom II rekomendacji dotyczących zamówień publicznych na systemy informatyczne opublikowany w grudniu 2021 r. przez Urząd Zamówień Publicznych uwzględnia m.in. wymóg określenia przez zamawiającego wymagań w zakresie cyberbezpieczeństwa systemu informatycznego. Rekomendacje wskazują wprost, że można to zrobić na podstawie powszechnie uznawanych norm i certyfikacji z zakresu bezpieczeństwa cybernetycznego, takich jak ISO, Narodowe Standardy Cyberbezpieczeństwa czy standardy określone przez amerykański Narodowy Instytut Standaryzacji i Technologii. Co więcej, wymagania dotyczą nie tylko zabezpieczenia infrastruktury, ale również odpowiedniego zarządzania dostępem i przetwarzaniem danych przez personel wykonujący zadania w ramach projektu.

W efekcie w zamówieniach publicznych często wprost jest określony wymóg zaprezentowania przez wykonawcę dokumentu potwierdzającego te kompetencje. Przykładem jest ISO 27001 – jeden z najbardziej renomowanych i rozpoznawalnych certyfikatów, który zaświadcza o przestrzeganiu międzynarodowych standardów w zakresie bezpieczeństwa informacji. Szacuje się, że tylko do 2020 roku spełnianiem norm ISO 27001 mogło poszczycić się ok. 45 000 firm na całym świecie, z czego 710 w Polsce. To certyfikat szczególnie pożądany w branży IT – około 25% certyfikowanych globalnie

podmiotów działa właśnie w tym sektorze gospodarki.

Rosnąca świadomość dotycząca zagrożeń w przestrzeni cybernetycznej i wyzwań związanych z utrzymaniem infrastruktury krytycznej przekłada się na coraz wyższe wymagania wobec dostawców systemów. Trend jest szczególnie widoczny w przypadku postępowań dotyczących aplikacji dedykowanych, które należy opracować od podstaw na zamówienie danego podmiotu. W tym kontekście regularne audyty i certyfikacje dawno przestały już być „mile widzianym dodatkiem" – to konieczność, przed którą stają firmy IT, które chcą wygrywać i realizować zamówienia dla sektora publicznego.

Źródło: IP