Jak cyberprzestępcy atakują urzędy?

Kategoria: Aktualności
Opublikowano: środa, 16, kwiecień 2025 11:04
Alicja Cisowska

Coraz częstsze incydenty cybernetyczne w Polsce i na świecie uwidaczniają poważne braki w zabezpieczeniach cyfrowych struktur samorządowych. Cyberprzestępcy bez skrupułów wykorzystują słabe ogniwa lokalnych urzędów, kradnąc dane, środki finansowe i blokując dostęp do kluczowych usług publicznych. Mimo rosnącej skali zagrożeń, kwestie cyberbezpieczeństwa niemal nie zaistniały w debacie publicznej kończącej się kampanii samorządowej. Tymczasem skutki takich ataków mogą bezpośrednio zagrozić bezpieczeństwu obywateli i stabilności lokalnych instytucji.

Cyberataki to coraz poważniejsze zagrożenie

W ostatnich latach doszło do szeregu poważnych incydentów: ataku na urząd w Nowej Sarzynie, ataku na jednostkę w Jędrzejowie, kampanii phishingowych zakończonych wyłudzeniem milionów złotych z kont samorządów oraz masowych ataków DDoS. Dane CERT Polska wskazują, że liczba tego typu zdarzeń systematycznie rośnie. Przykłady z zagranicy pokazują, że skutki mogą być jeszcze poważniejsze – obejmujące nawet zakłócenia w funkcjonowaniu służby zdrowia, infrastruktury krytycznej czy kradzież danych osobowych pracowników urzędów i mieszkańców.

W Polsce działa ponad 2,8 tys. jednostek samorządowych, z których każda przetwarza ogromne zbiory informacji – od danych adresowych po informacje finansowe i zdrowotne. To atrakcyjny cel dla cyberprzestępców, którzy doskonale zdają sobie sprawę z często niewystarczających zabezpieczeń, braku wyspecjalizowanej kadry IT oraz ograniczonych budżetów lokalnych urzędów.

Różne motywacje atakujących

Celem cyberprzestępców może być nie tylko kradzież tożsamości czy środków finansowych – niektóre ataki mają charakter destabilizujący, inne mają na celu ujawnienie luk w systemach bezpieczeństwa, jeszcze inne są inspirowane działaniami geopolitycznymi. W kontekście trwającej wojny za wschodnią granicą, eksperci zwracają szczególną uwagę na aktywność rosyjskich grup hakerskich, które wielokrotnie wykorzystywały kryzysy do przeprowadzania zmasowanych ataków.

Jednostki samorządowe i urzędy są dla cyberprzestępców wyjątkowo atrakcyjnym celem. Zawierają wrażliwe dane i zarządzają lokalną infrastrukturą. Niestety ich poziom zabezpieczeń bywa niewystarczający, co grozi nie tylko potencjalnymi stratami finansowymi, lecz także wizerunkowymi.

Nowe środki, nowe obowiązki

Temat cyberbezpieczeństwa wraca dzięki programowi „Cyberbezpieczny Samorząd", który umożliwia pozyskanie nawet 850 tys. zł na rozwój infrastruktury IT, wdrażanie zabezpieczeń oraz szkolenia kadry urzędniczej. Do 2026 roku samorządy mają czas na realizację projektów, na które przeznaczono łącznie 1,5 mld zł.

Równolegle do wsparcia finansowego, w życie wchodzą nowe regulacje prawne. Dyrektywa NIS2, której implementacja jest już w toku, wymusi na wielu jednostkach samorządowych i podległych im instytucjach obowiązek wdrożenia konkretnych rozwiązań zabezpieczających i raportowania incydentów.

Człowiek najsłabszym ogniwem

Specjaliści zwracają uwagę, że nawet najbardziej zaawansowane rozwiązania technologiczne nie są w

stanie zastąpić świadomych i dobrze przeszkolonych pracowników. To właśnie czynnik ludzki najczęściej staje się przyczyną naruszeń bezpieczeństwa. Osoby zatrudnione w administracji powinny dysponować odpowiednią wiedzą, znać procedury ochrony danych i umieć właściwie reagować na potencjalne zagrożenia. Równie ważne jest systematyczne aktualizowanie oprogramowania – to prosty krok, który w wielu sytuacjach może skutecznie zapobiec atakom.

Pięć kluczowych zasad dla bezpiecznego samorządu

- Kopie zapasowe danych – najlepiej zarówno w chmurze, jak i na odłączonych dyskach zewnętrznych.
- Oprogramowanie antywirusowe – od zaufanych dostawców, z automatycznymi aktualizacjami.
- Systematyczne aktualizacje – nie tylko systemów operacyjnych, ale także aplikacji i urządzeń peryferyjnych.
- Zabezpieczenie kont użytkowników – silne hasła, menedżery haseł i uwierzytelnianie dwuskładnikowe.
- Bezpieczeństwo urządzeń mobilnych – aktualizacje, blokady biometryczne, możliwość zdalnego wyczyszczenia danych.

- Zadbanie o bezpieczeństwo urzędów i samorządów jest obecnie priorytetowym zadaniem dla wielu zespołów bezpieczeństwa. Nowe dyrektywy oraz ciągły rozwój cyberzagrożeń sprawia, że każda jednostka powinna sprawdzić aktualny poziom swoich zabezpieczeń i dostosować je do nowych realiów – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: bitdefender.pl