Czy samorządy są atrakcyjnym celem ataku dla hakerów?

Kategoria: Aktualności
Opublikowano: wtorek, 21, grudzień 2021 15:11
Joanna Gryboś-Chechelska

Co najmniej 14% samorządów zostało zaatakowanych przez hakerów. Choć najczęstszą formą ataku są phishing i ransomware, to z racji na swoje podatności JST powinny być również wyczulone na DDoS. Jak samorządy mogą skutecznie przeciwstawić się przestępcom? Podstawą jest diagnoza cyberbezpieczeństwa i wprowadzenie w życie jej wyników, aktualizacja oprogramowania i szkolenie pracowników.

Ryzyko cyberataku rośnie z roku na rok i obecnie trzeba już myśleć o tym „kiedy" on nastąpi zamiast zastanawiać się „czy w ogóle". Jak pokazują dane gromadzone przez CERT NASK, zajmujący się koordynacją obsługi incydentów zgłaszanych m.in. przez samorządy, liczba incydentów wzrosła o 60,7% w zeszłym roku. Choć nie ma jeszcze informacji o tym, jak wyglądał krajobraz w 2021 r., to patrząc na trendy światowe, gdzie statystyki rosną w tempie kilkukrotnym (np. liczba ataków phishingowych wzrosła 7-krotnie), zauważymy zapewne dalszy wzrost – i to pewnie niemały.

14% samorządów ofiarą hakerów

Jak to wygląda w przypadku polskich JST? Z jednej strony można powiedzieć, że nie jest aż tak źle. Według danych NASK tylko 3,72% incydentów dotyczyło samorządów, ale to nadal 388 ataków, czyli średnio 1 dziennie. Patrząc z kolei na liczbę jednostek administracyjnych, oznacza to, że zaatakowano 14% polskich samorządów. A to tylko zgłoszone w 2020 r. incydenty – wykrycie obecności hakerów od momentu złamania przez nich zabezpieczeń, może zająć nawet kilka miesięcy. Dodatkowo, potrafią oni sparaliżować pracę administracji lokalnej na wiele dni. W skrajnym do tej pory przypadku, powrót urzędu do pełnej sprawności po zainfekowaniu ransomware, trwał ponad miesiąc.

– Zagrożenie jest realne i nie można go bagatelizować. Zwłaszcza patrząc na trendy światowe, które powoli widać też w Polsce. Według Barracuda Networks ofiarami ponad 44% ataków ransomware są właśnie władze lokalne. Niestety administracja gminna, miejska czy powiatowa jest bardzo atrakcyjnym celem ataku dla hakerów. Z wielu powodów, ale przede wszystkim dlatego, że mogą być furtką do zainfekowania złośliwym oprogramowaniem wielu innych instytucji, a także firm. Przykładowo poprzez masową wysyłkę „złych" linków ze zhakowanej skrzynki urzędniczej. Poza tym w bazach samorządowych przechowywane są praktycznie wszystkie dane osobowe obywateli, które przestępcy mogą wykorzystać do kradzieży tożsamości – zauważa Patrycja Tatara, ekspert ds. cyberbezpieczeństwa w Sprint S.A.

Najważniejsze przyczyny zainteresowania hakerów samorządami:

- JST mogą być „punktem wyjścia" do dalszych ataków.
- Samorządy gromadzą wiele cennych danych – zwłaszcza osobowych.
- Zabezpieczenia JST postrzegane są jako słabsze niż w przypadku firm.
- Samorządy nie posiadają zazwyczaj rozbudowanych zespołów IT.

Na co narażone są JST?

Choć wspomniane już ataki ransomware i phishingowe są obecnie największym zagrożeniami, to niestety nie koniec listy ataków, na które trzeba się przygotować. Trzeba pamiętać jeszcze o:

- malware – czyli różnej maści złośliwe oprogramowanie, które może powodować m.in. zaszyfrowanie danych, blokadę dostępu do systemów IT czy jego poszczególnych części, kradzieży danych i plików oraz wielu innych niepożądanych zdarzeń.

- ransomware – to podtyp malware, najpopularniejszy, którego zadaniem jest zaszyfrowanie kluczowych danych, co skutkuje zazwyczaj paraliżem całego systemu. Następnie przestępcy żądają okupu za odblokowanie, najczęściej w bitcoinach. Częstą formą rozprzestrzeniania tego oprogramowania jest phishing.
- phishing – masowa próba ataku, najczęściej w formie wysyłki wiadomości e-mail czy sms zawierających hiperłącze do złośliwego oprogramowania lub mających zachęcić do interakcji, której finałem będzie zachęcenie do kliknięcia w „zły" link lub wyłudzenie informacji wrażliwych. Kto z nas nie otrzymał maila od nigeryjskiego biznesmena czy prawnika oferującego nam pieniądze czy spadek?
- spear-phishing – to szczególnie groźna forma ataku, choć co do zasady podobna do powyższej. Podstawową różnicą jest fakt, że jak nazwa wskazuje, jest to atak wycelowany w konkretną osobę, instytucję, wykorzystujący np. informacje osobiste – przestępcy podszywają się pod znajomego/przełożonego. Może mu towarzyszyć też połączenie telefoniczne, zwiększające wiarygodność przestępców.
- DoS i DDoS – ataki generujące wzmożony ruch w stronę ofiary. Ich celem są serwery czy strony internetowe, a efektem ich „padnięcie", ponieważ nie mogą obsłużyć dodatkowego ruchu.

– Choć najbardziej popularne obecnie są phishing i ransomware, to samorządy muszą być również wyczulone na te ostatnie – DoS i DDoS, którym także może towarzyszyć żądanie okupu w zamian za zwolnienie łączy. Liczba tych ataków może wzrosnąć w najbliższym czasie, patrząc na wnioski z badania zabezpieczeń JST zrealizowane przez CERT NASK. Dostępność baz danych bezpośrednio z Internetu czy otwarte panele logowanie do CMS stron internetowych samorządów to furtki, które trzeba jak najszybciej zamknąć – dodaje Patrycja Tatara.

Samorządy mogą walczyć z hakerami

Podstawą sukcesu jest przede wszystkim dokładana analiza podatności i sprawdzenie luk, co między innymi ma zapewnić diagnoza cyberbezpieczeństwa obowiązkowa dla każdego JST, które otrzyma rządowe wsparcie. To jednak początek. Wśród działań, które warto rozważyć, ponieważ mogą radykalnie zmniejszyć ryzyko skutecznego ataku, są także:

- dokładnie opracowane i przestrzegane polityki bezpieczeństwa, w tym zasad zarządzania hasłami czy podłączania urządzeń zewnętrznych do systemów,
- przetestowany plan reakcji na atak i ciągłości działania w razie złamania zabezpieczeń,
- regularne szkolenia informujące o nowych zagrożeniach,
- cykliczne aktualizacje oprogramowania,
- współpraca z zewnętrznymi ekspertami ds. cyberbezpieczeństwa, outsourcing części zadań,
- partnerstwo z innymi jednostkami celem zoptymalizowania kosztów ochrony, np. powiatowy system bezpieczeństwa z którego korzysta wiele gmin.

Źródło: ip