**Atak DDoS na rządowy serwis – czas na kolejny stopień alarmowy?**

* **W poniedziałek atak DDoS sparaliżował eZamówienia.**
* **Niespełna tydzień wcześniej hakerzy zaatakowali Centrum Zdrowia Matki Polki w Łodzi, a 27 października przeprowadzono atak DDoS na serwery Senatu RP.**
* **Instytucje publiczne były już atakowane przez hakerów od początku roku. W Polsce nadal obowiązuje trzeci stopień alarmowy CHARLIE-CRP. Czy powód do zmartwień mają także firmy?**

Do cyberataku na Platformę eZamówienia doszło w poniedziałek, 7 listopada, chwilę po godzinie 9:00. W oficjalnym komunikacie na stronie gov.pl czytamy, że od 9:07 trwał atak DDoS na infrastrukturę Platformy eZamówienia. Podjęto wówczas działania mające na celu przywrócenie działania platformy. Rzecznik Urzędu Zamówień Publicznych (UZP) przekazał, że atak przeprowadzono z serwerów znajdujących się poza granicami kraju. Strona ezamowienia.pl nie działała jeszcze o godzinie 17:45.

– *Ataki hakerskie na instytucje publiczne już od paru lat przybierają na sile. Do tej pory miały one w zdecydowanej większości wyłącznie typowo przestępczy wymiar – kradzież danych, wyłudzenie okupu. Ostatnie z kolei są niezaprzeczalnie związane z rosnącym napięciem politycznym na linii Ukraina-Rosja. Niestety, jak widać, polskie instytucje także są zagrożone. Uważam, że także przedsiębiorcy nie mogą spać zupełnie spokojnie. Atakujący systemy rządowe mogą wykorzystać je jako furtkę do dalszych działań i zainfekowania biznesu* – mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

**Ataki na Senat i Centrum Zdrowia Matki Polki w Łodzi**

Platforma eZamówienia to nie jedyny państwowy serwis, który został zaatakowany w ostatnim czasie. W ubiegły czwartek, 3 listopada, ofiarą hakerów padło Centrum Zdrowia Matki Polki w Łodzi. Był to atak ransomware, w ramach którego hakerzy blokują dostęp do danych i oferują ofierze odblokowanie dostępu do informacji w zamian za okup. Na szczęście na incydent szybko zareagowali specjaliści z NASK, którzy podjęli działania mające na celu minimalizację skutków ataku. Dane medyczne nie zostały wówczas zaszyfrowane. Atak dotyczył danych aplikacji, na których podstawie pracował szpital. Z kolei nieco wcześniej, 27 października, przeprowadzono atak DDoS na serwery Senatu RP. Paraliż senackiego serwisu nie trwał jednak długo, bo zaledwie 40 minut. Atak miał charakter wielokierunkowy i był przeprowadzany m.in. z Rosji. Marszałek Tomasz Grodzki stwierdził na konferencji prasowej, że atak mógł mieć związek z uznaniem władz rosyjskich przez polski Senat za reżim terrorystyczny i publikacją stosownej uchwały.

**Czy to czas na kolejny alarm?**

Warto podkreślić, że w Polsce nadal obowiązuje trzeci stopień alarmowy CHARLIE-CRP oznaczający wezwanie instytucji publicznych do zachowania szczególnej czujności, intensywniejszego niż dotychczas monitorowania bezpieczeństwa systemów IT. Skala ma cztery stopnie, co już mówi o stopniu zagrożenia cyberatakami na instytucje publiczne. O cyberzagrożeniach instytucji publicznych mówi się od początku 2022 roku – już w lutym premier ogłosił pierwszy stopień ALFA-CRP. W związku z trwającą wojną w Ukrainie wszyscy powinni być przygotowani na ataki hakerów i każda organizacja powinna zadbać o wzmocnienie zabezpieczeń infrastruktury IT. W takiej sytuacji powinniśmy zadać sobie pytanie, kiedy zostaniemy zaatakowani, a nie czy w ogóle to nastąpi.

**Czym jest atak DDoS?**

Metoda DDoS ma za zadanie zablokować działanie systemów, stron internetowych, aplikacji. W tym celu przestępcy kierują sztuczny, nadmiarowy ruch w stronę swoich celów powodując przeciążenie łączy, skutkujące zatrzymaniem działania systemów. DDoS to pochodna ataku DoS, a różnica polega na tym, że w pierwszym przypadku cyberprzestępcy wykorzystują botnet. Istnieją jednak różne formy ataków DoS i DDoS i nie wszystkie są do siebie podobne. Niektóre z nich wiążą się przykładowo, tylko z zawieszeniem działania usługi. Z kolei inne tylko z pobieraniem plików i zawieszeniem. Warto jeszcze dodać, że chodzi nie tylko o pakiety, ale atak może też bazować na zmasowanej liczbie zapytań do aplikacji, które mogą powodować jej paralić. Przy zmasowanym ataku DDoS lub DoS ofiarą może paść wiele instytucji, także komercyjnych.

– *Owszem najbardziej zagrożone, w przypadku ataku na instytucje publiczne, są największe organizacje i firmy, ale nie można zapominać, że coraz częściej hakerzy liczą na ilość, a nie jakość ofiar. Dlatego i sektor MŚP jest w obszarze ich zainteresowania. To, co przedsiębiorcy mogą zrobić, to zadbać przede wszystkim o infrastrukturę cybersecurity i procedury bezpieczeństwa. Nie wystarczą już rozwiązania takie jak szyfrowanie łączy czy stosowanie zewnętrznych firewalli. Aby móc skutecznie się bronić należy doposażać się w rozwiązania klasy SIEM, WAF czy też EDR. Często hakerzy rezygnują z ataku, jak w trakcie prób uzyskania dostępu do infrastruktury powstrzymują ich od tego silne zabezpieczenia* – dodaje Patrycja Tatara ze Sprint S.A.

Źródło: Sprint S.A.