Warszawa, 24.01.2019r.

2018 rok upłynął pod hasłem poprawy bezpieczeństwa w sieci

Polski rynek hostingu ma ogromny potencjał rozwoju. Jest to efekt transformacji cyfrowej, szczególnie na dwóch płaszczyznach: szeroko rozumianego bezpieczeństwa oraz konieczności rozwoju infrastruktury. Obecnie zaledwie 50% firm w naszym kraju posiada stronę WWW czy adres e-mail we własnej domenie. Społeczeństwo coraz częściej korzysta z nowych technologii, a z tym trendem zwiększa się także ryzyko związane z ochroną danych osobowych.

Obecnie dane osobowe stanowią realną wartość, a co za tym idzie wchodzą w obszar zainteresowania cyberprzestępców. Również sama infrastruktura IT firm jest narażona na różnego typu zagrożenia, takie jak ataki ransomware czy DDoS, co wymusza nieustanne podnoszenie poziomu zabezpieczeń. Potwierdzają to wyniki badania EY Global Information Security Survey 2018–19[i], według którego już 76% firm w następstwie naruszenia ich danych zwiększyło swój budżet na bezpieczeństwo. Coraz większą odpowiedzialnością są obarczani operatorzy i usługodawcy, którzy powinni działać z wyprzedzeniem, przystosowując swoją infrastrukturę i wyprzedzając oczekiwania swoich klientów, nie zawsze świadomych istniejących zagrożeń i wymogów związanych ze standardami bezpieczeństwa.

Cyberbezpieczeństwo coraz ważniejsze

Coraz więcej przedsiębiorców dostrzega oczywisty fakt, że wraz z udanym cyberatakiem może dojść do realnych strat finansowych oraz utraty wiarygodności firmy. Według badań 37% respondentów twierdzi, że atak DDoS zaszkodził reputacji ich działalności, całkowicie podważając zaufanie klientów do przedsiębiorstwa. Co ważne, skala tego zjawiska rośnie z roku na rok. W związku z tym ochrona przeciwko zagrożeniom związanym z atakami typu DDoS stała się dla firm niezwykle ważna, szczególnie po serii incydentów, które miały miejsce wśród polskich dostawców usług hostingowych. – *Nazwa.pl w obliczu rosnącego zagrożenia tego typu atakami już od początku ubiegłego roku intensywnie pracowała nad rozwiązaniami chroniącymi dane Klientów* – podkreśla Krzysztof Cebrat, prezes zarządu nazwa.pl. - *W przeciągu roku wydaliśmy miliony złotych, przygotowując naszą infrastrukturę na różnego typu zagrożenia. Uruchomienie Scrubbing Center, chroniącego w szczególności przed atakami DDoS, przeskalowanie do globalnego zasięgu w zakresie uczestnictwa w wielu punktach Internet Exchange w Polsce i za granicą, wykorzystanie technologii DNS Anycast z serwerami zlokalizowanymi na wszystkich kontynentach, pozwala nam stwierdzić, że jesteśmy firmą hostingową, która najlepiej w Polsce chroni swoich Klientów przed zagrożeniami związanymi z naruszeniem danych i utratą ciągłości działania* – dodaje Cebrat.

Trzeba pamiętać, że cyberprzestępcy nieustannie zmieniają swoje metody i schematy działania, dlatego to po stronie firm hostingowych leży odpowiedzialność za wdrożenie stosownych zabezpieczeń, które ograniczają ryzyko udanego ataku do minimum. – *Jednym z wprowadzonych przez nas rozwiązań jest wspomniane Scrubbing Center, czyli specjalna infrastruktura, przy pomocy której dokonywana jest analiza ruchu IP w celu wykrycia w nim wszelkich zagrożeń, począwszy od ataków DDoS, poprzez wykrywanie ataków na serwisy internetowe, kończąc na zagrożeniach związanych ze szkodliwym oprogramowaniem* – tłumaczy Rafał Lorenc, dyrektor IT w nazwa.pl.

Samo wykrycie zagrożenia może jednak nie wystarczyć. - *Istnieje kilka innych sposobów obrony przed atakami DDoS. Jednym z nich jest przekierowanie wzmożonego ruchu. Nazwa.pl poprzez globalnie rozlokowane serwery DNS Anycast jest w stanie rozłożyć ruch na serwerach, obsługując od kilku do kilkudziesięciu milionów zapytań do DNS na sekundę* – wyjaśnia Lorenc. – *Technologia DNS Anycast zapewnia jeszcze jedną przewagę. Pozwala ona*

na błyskawiczne rozwiązanie nazwy domeny z dowolnego miejsca na Ziemi, co stanowi ogromną przewagę konkurencyjną dla segmentu e-commerce – wyjaśnia Cebrat. Technologia ta, poza poprawą bezpieczeństwa, podnosi komfort użytkowania stron WWW oraz usług dostępnych w Internecie.

Certyfikaty i protokoły bezpieczeństwa

Na początku 2018 roku Google ogłosiło, że poczynając od wersji Chrome 68 przeglądarka będzie oznaczać strony nieposiadające certyfikatu SSL jako niebezpieczne. Nazwa.pl jako największy dostawca usług hostingowych w Polsce, wyprzedzając ruch giganta z Mountain View, jeszcze przed wprowadzeniem zmian w przeglądarce zabezpieczyła ponad 600 tys. domen swoich klientów, udostępniając im w ramach opłaty za domenę certyfikat SSL. – *Planując to wdrożenie, wiedzieliśmy, że to śmiałe i niespotykane na rynku posunięcie. Dotychczas firmy hostingowe dodatkowo zarabiały na sprzedaży certyfikatów. Nazwa.pl jednak wyznacza standardy dla całej branży i nie boi się nieszablonowych rozwiązań. Takie działanie zaowocowało tym, że po zakończeniu procesu generowania certyfikatów nazwa.pl chroniła co czwartą polską domenę internetową* – z dumą przyznaje Krzysztof Cebrat, prezes zarządu nazwa.pl. Jednak sam SSL to nie wszystko, pełną ochronę zapewnia połączenie certyfikatów SSL i DNSSEC.

Zabezpieczenie w postaci protokołu DNSSEC to globalny trend, czego przykładem jest wymóg jego stosowania przez administrację federalną w USA. Jak wygląda Polska na tle innych krajów? Obecnie według raportu NASK Polska jest na czwartym miejscu wśród krajów europejskich pod względem ilości domen zabezpieczonych protokołem DNSSEC. Co ciekawe, ponad 91% domen zabezpieczonych tym rozwiązaniem znajduje się w domenie zarejestrowanej za pośrednictwem nazwa.pl. – *Jako największy rejestrator domen w Polsce naszym priorytetem jest bezpieczeństwo, dlatego wprowadziliśmy szereg rozwiązań chroniących naszych Klientów i użytkowników ich serwisów. Nazwa.pl nie tylko rejestruje domeny, ale w ramach Pakietu Bezpieczna Domena dostarcza bez dodatkowych opłat certyfikat SSL, zabezpiecza domeny przed atakami cyberprzestępców protokołem kryptograficznym DNSSEC, a serwery DNS nazwa.pl obsługujące domeny zabezpiecza za pomocą technologii Anycast oraz DNS over TLS. Te rozwiązania czynią domenę zarejestrowaną w nazwa.pl najbezpieczniejszą domeną w Polsce* – tłumaczy Krzysztof Cebrat, prezes zarządu nazwa.pl. - *W dodatku jako jedyna polska firma wsparliśmy międzynarodową organizację tworzącą certyfikat bezpieczeństwa Let's Encrypt, znajdując się w towarzystwie takich gigantów jak Google czy Facebook* – dodaje Cebrat.

Dalszy wzrost w zakresie poziomu zabezpieczeń to trend, który będzie narastał w wyniku zmian dyktowanych przez liderów rynku oraz samych użytkowników. To właśnie użytkownicy są coraz bardziej świadomi i oczekują, że ich dane będą chronione. Każda firma, której zależy na wiarygodności w sieci i bezpieczeństwie swoich klientów, powinna zwrócić na ten aspekt szczególną uwagę. Ruchy światowych gigantów takich jak Google czy Facebook oraz rodzimi liderzy technologiczni jasno wskazują priorytety na nadchodzące lata.

[i] EY Global Information Security Survey 2018–19 https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf