Kraków, 19.12.2018r.

Czy sektor bankowy zabezpiecza swoje domeny?

Zaledwie 23% domen transakcyjnych polskich banków zabezpieczonych jest przez protokół DNSSEC chroniący użytkowników przed najczęstszym przestępstwem w sieci, czyli phishingiem. Wagę tego zabezpieczenia już w 2009 roku docenił amerykański rząd federalny, obligując wszystkie agencje rządowe, np. FBI, CIA, a także Bank Rezerw Federalnych, do ochrony swoich domen przy pomocy protokołu DNSSEC[i]. Polska na tle Europy plasuje się na czwartym miejscu rejestrów zabezpieczonych tym protokołem, za Holandią, Szwecją i Czechami[ii].

Według najnowszych badań poziomu zabezpieczeń domen instytucji finansowych polegających na sprawdzeniu obecności certyfikatu SSL i protokołu DNSSEC w danej domenie wynika, że polskie domeny związane z branżą finansową nie są kompleksowo zabezpieczone. Sprawdzeniu poddano 89 instytucji finansowych, w tym 29 banków, 37 firm pożyczkowych, tzw. parabanków, i 23 kantory internetowe. Analizą objęto zarówno strony główne danej instytucji, jak i strony transakcyjne oraz serwisy marketingowe.

Obraz rynku

Ochrona klientów instytucji finansowych poprzez certyfikat SSL jest powszechna na stronach głównych i stronach transakcyjnych. Wyjątkiem na dzień badania był jeden e-kantor, który nie posiadał stosownego certyfikatu chroniącego swoich klientów przed przechwyceniem danych. Nieco słabiej wygląda poziom zabezpieczeń witryn o przeznaczeniu marketingowym, gdzie najlepiej wypadają banki, zabezpieczając certyfikatem SSL 89% swoich witryn.

Sytuacja wygląda zupełnie inaczej w kontekście ochrony przed phishingiem. Ogólny odsetek stron internetowych instytucji finansowych zabezpieczonych przy pomocy protokołu DNSSEC waha się w zależności od rodzaju witryn od 11 do 30% - *wynik ten jest dość niepokojący w szczególności w kontekście stron transakcyjnych oraz marketingowych, bo te są najczęściej wykorzystywane przez cyberprzestępców do wyłudzania danych lub co gorsza pieniędzy klientów* – mówi Krzysztof Cebrat, prezes zarządu nazwa.pl, firmy, która zabezpiecza 91% domen chronionych protokołem DNSSEC w Polsce.

Gdzie znaleźć bezpieczne domeny?

Duży wpływ na globalny poziom bezpieczeństwa domen internetowych miała ostatnia decyzja Google i Mozilla. Firmy te w swoich przeglądarkach automatycznie oznaczają strony nieposiadające certyfikatu SSL jako niebezpiecznie. W ten sposób użytkownik, który chce wejść na stronę nieposiadającą tego zabezpieczenia zostanie o tym ostrzeżony. Na polskim rynku w czerwcu tego roku nazwa.pl, wyprzedzając ruch światowych gigantów, nadała certyfikat SSL dla 600 tys. domen swoich klientów, chroniąc w ten sposób ponad 25% polskich

stron WWW. Nieco trudniej jest sprawdzić, czy właściciel danej strony WWW chroni swoich klientów przed atakami phishingowymi. Do tego służy protokół DNSSEC, który na razie nie jest oznaczany w przeglądarkach. – *Nazwa.pl uruchomiła ostatnio narzędzie pozwalające każdemu zweryfikować poziom zabezpieczeń danej witryny WWW. Wystarczy wejść na stronę szybkość i bezpieczeństwo i sprawdzić, czy strona posiada niezbędne zabezpieczenia. Jeżeli użytkownik nie wie, czy jego bank lub ulubiony sklep internetowy w pełni chroni go przed atakami cyberprzestępców, to może to właśnie w tym miejscu sprawdzić* – tłumaczy Krzysztof Cebrat, prezes zarządu nazwa.pl.

Odpowiedzialność przedsiębiorcy

Problem zabezpieczeń związanych z ochroną transakcji internetowych jest znacznie szerszy niż sam sektor bankowy, który można by sądzić, że jest najlepiej zabezpieczony pod tym względem. Wartość rynku e-commerce to ponad 40 mld złotych rocznie i skoro w sektorze finansowym zdarzają się witryny, które nie są kompleksowo chronione, to warto zadać pytanie, jak wygląda sytuacja w całej branży handlu internetowego? – *Odpowiedzialność za bezpieczeństwo transakcji leży po stronie właściciela domeny. Posiadanie bezpiecznej domeny to dziś wręcz obowiązek dla sklepu online czy banku i sam certyfikat SSL to znacznie za mało. Technologie związane z bezpieczeństwem domeny powinny być zatem priorytetem, a ich powszechność stosowania to wyraz odpowiedzialności, jaką biorą za swoich klientów przedsiębiorcy. Z punktu widzenia właściciela sklepu internetowego bezpieczna domena nie tylko chroni jego klientów przed przestępcami, ale i pozytywnie wpływa na poziom jego wyników w wyszukiwarce Google* – mówi Krzysztof Cebrat, prezes zarządu nazwa.pl.

Świadomość zagrożeń

Państwowy instytut badawczy NASK, nadzorowany przez Ministerstwo Cyfryzacji, prowadzi intensywne działania edukacyjne w zakresie popularyzacji usług internetowych. – *Jednym z najistotniejszych zadań realizowanych przez rejestr domeny krajowej jest dbałość o bezpieczeństwo. Rosnąca liczba nazw zabezpieczonych protokołem DNSSEC poprawia bezpieczeństwo i zwiększa zaufanie abonentów oraz użytkowników do usług internetowych* – mówi Roman Malinowski, kierujący krajowym rejestrem domeny .pl w NASK. Rola edukacji jest niezwykle ważnym elementem w procesie dbania o wzrost poziomu zabezpieczeń internetowych. - *Warto podkreślić, że jeżeli sami użytkownicy będą oczekiwali od właścicieli stron WWW odpowiednich technologii chroniących ich interesy, to naturalną rzeczą w konsekwencji będzie zainteresowanie firm z branży e-commerce i sektora finansowego stosowaniem tych zabezpieczeń* – dodaje Krzysztof Cebrat.

[i] https://web.archive.org/web/20080916034802/http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf

[ii] https://www.dns.pl/sites/default/files/2018-06/NASK_Q1_2018_RAPORT.pdf