Z pamiętnika admina: Zosia Samosia robi migracje.

Wszyscy znamy wierszyk Juliana Tuwima „Zosia Samosia”. Morał zawarty w tej rymowance poucza nas, żeby nie uważać się za najmądrzejszą osobę i korzystać z pomocy innych. Jednakże moje ostatnie doświadczenia mówią coś zupełnie innego. Początkowo może się Wam wydawać, że niniejszy artykuł nie ma nic wspólnego z bezpieczeństwem IT, ale wszystko wyjaśni się w dalszej części artykułu.

Jakiś czas temu pisaliśmy na naszych profilach społecznościowych o migracji, w wyniku której możemy być chwilowo niedostępni. Zamieściliśmy tę informację by uniknąć późniejszych plotek, że padł nam serwer, zostaliśmy zhackowani, czy też zamknęli nas za obrażanie Prezydenta

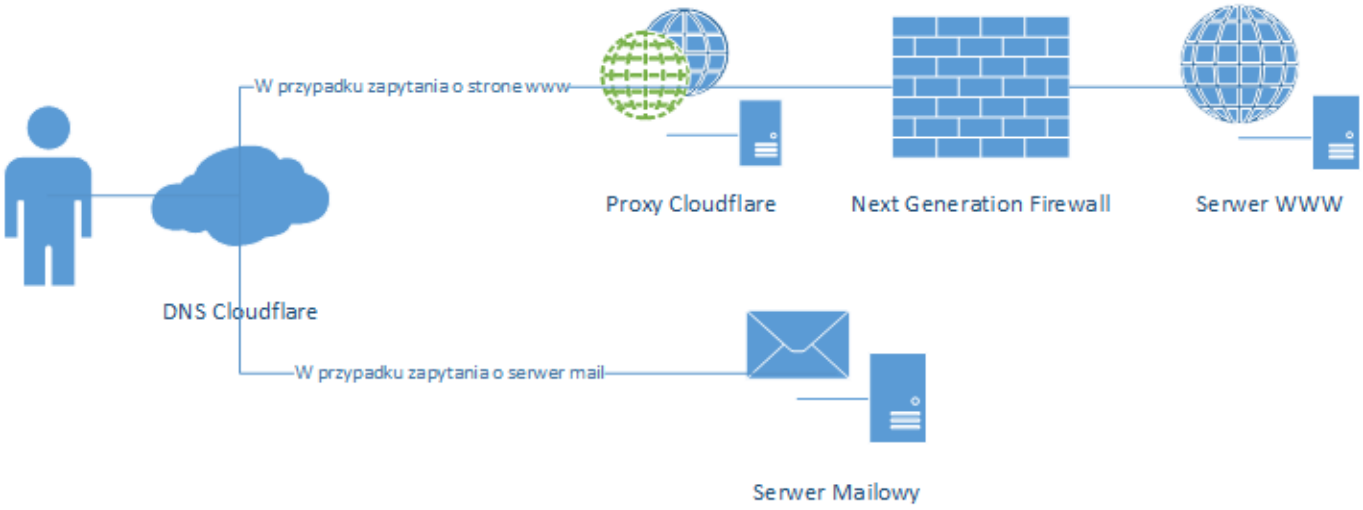
Przeprowadzenia migracji, jak zawsze zresztą, podjąłem się ja – PHT. Bo akurat miałem czas, bo tak, bo jestem w SMS odpowiedzialny za infrastrukturę, bo chciałem. Powodów było wiele. Wydawało mi się, że to co muszę zrobić będzie łatwe jak bułka z masłem. Co musiałem zrobić, zapytacie? Ot, przenieść konta mailowe na nowy serwer. Pomyślicie sobie, że to kilka kliknięć, zmiana w DNS i maksymalnie godzina czekania? NIE.

Niniejszy tekst postanowiłem podzielić na części – akty, niczym Szekspir dzielący swoje dramaty.

Akt I – szukanie nowego dostawcy usługi.

Dotychczas korzystaliśmy w zakresie hostingu serwera mail z usług zacnej, aczkolwiek upośledzonej komunikacyjnie firmy AZ Spółka z o.o. (naprawdę mieli ograniczoną odpowiedzialność). Postanowiliśmy odejść z AZ z kilku powodów – głównie ceny i częstych wywrotów serwera. Z tym drugim poradziliśmy sobie przenosząc WWW na osobny serwer w siedzibie SMS, a maile, z którymi nie było problemu, pozostawiliśmy na hoście od AZ. Do tego doszedł Cloudflare i wszystko było super. Do czasu. Gdy przyszedł okres rozliczeń okazało się, że odnowienie naszej usługi (a trzeba tu wspomnieć, że był to hosting „Business (bez limitu transferu)") wynosi (tylko albo i aż) 552.27 zł brutto. To nas zabolało. Ktoś

mógłby pomyśleć, że to zwykłe cebulactwo, ale tak szczerze – płacić tyle za serwer mailowy? Przypomnę że za te cenę można mieć całkiem fajnego dedyka.



(Dotychczasowa konfiguracja)

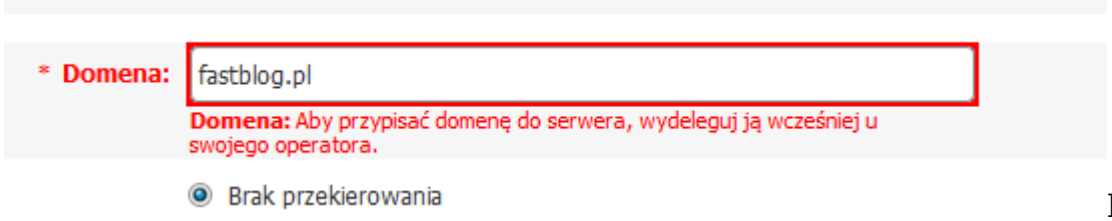
Tak więc – postanowiliśmy poszukać innego dostawcy. Padło na home.pl. Przejrzeliśmy ich ofertę i, żeby nie popełnić gafy, wysłaliśmy do home.pl maila z zapytaniem jaką ofertę nam polecają. Po 30 minutach na podany w zgłoszeniu telefon zadzwonił przemiły Pan z działu obsługi klienta (w sensie ten taki, co mu płacą pewnie 600 zł na rękę podstawy i 10 procent od tego co wciśnie ludziom). Pan z obsługi klienta bazując na naszym zapytaniu i kilku pytaniach zaproponował nam ofertę, która według niego będzie dla nas najlepsza. Dogadaliśmy się i po chwili mieliśmy zaklepany pakiet „Business Cloud Starter". I co dalej? To za chwilę. W ramach rekompensaty i, żeby zaostrzyć apetyt (a także po to, by później nie tłumaczyć), nasze wymagania podane w mailu brzmiały mniej więcej tak:

> Potrzebujemy usługi dającej nam możliwość korzystania z serwera mailowego u Państwa oraz osobnego serwera www hostowanego gdzie indziej.

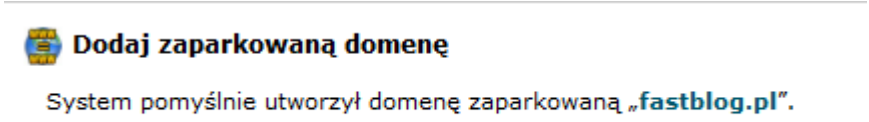
Akt II – Testy

Zaraz po wpłaceniu szekli na konto home.pl zabrałem się do testowania i próbnej migracji. Postanowiłem przemigrować projekt fastblog.pl, ponieważ był on tak samo skonfigurowany

jak s-m-s.pl (mordercy mają swój modus operandi, admini też – warto o tym pamiętać wykonując testy penetracyjne).
Pierwszym krokiem było dodanie skrzynki mailowej na serwerze dostarczonym przez home.pl. Zabrałem się za to tak jak należy. Panel home.pl poinformował mnie, że aby dodać skrzynkę pocztową, muszę dodać domenę do serwera. Więc postanowiłem tak zrobić.



Po chwili zastanowienia postanowiłem sprawdzić, czy w az.pl wymagana była identyczna procedura. Przypomnę, iż w tamtym momencie fastblog.pl podpięte było pod DNS Cloudflare.



Jak widać udało się, do tego bez kombinacji z DNS! Postanowiłem poszukać odpowiedzi, bo jak inaczej użyć CF nie podając go w DNS? Z odpowiedzią przychodzi oficjalne forum home.pl i user o nicku „Grzesiek”. Swoją drogą, jeśli „Grzesiek” jest pracownikiem home.pl a pozostali pracownicy charakteryzują się podobnym podejściem, to drżyjcie klienci home.pl, jeśli to kiedyś dupnie – nie będzie co zbierać. Pozwolę sobie zacytować tekst jednej z odpowiedzi tego usera na pytanie czemu CF nie działa.

> Aby poczta działała na home.pl, domena musi kierować na serwery DNS home.pl.

Jezu! Ja bym się cieszył gdyby ktoś chciał odciążyć moje serwery DNS, ale ja się nie znam, nie mam firmy wartej „pierdylion szekli”.

> CloudFlare nie będzie w tym przeszkadzało o ile w jego konfiguracji, faktycznie będzie przekierowanie na nasze serwery DNS (rekord NS).

Ale jak? No ja wiem, tam jest takie śmieszne ustawienie serwerów DNS (NS), ale z tego

co zauważyłem sprawdzenie, czy domena idzie na home.pl jest wykonywane za pomocą „whois” a więc i tak idzie na CF.

> W tym wypadku w panelu serwera lub podczas kontaktu z BOK, podajesz nazwę domeny która będzie przypięta do hostingu. I tylko w tej konfiguracji, domena jest widoczna w panelu jako obiekt przypięty/delegowany.
>
> Jeśli jednak domena nie będzie kierowała na nasze serwery DNS, a np. rekordem A skierowana na hosting, wtedy jest to zwykłe przekierowanie które nie podlega konfiguracji w panelu. Domena nie jest widoczna, a więc pozostała konfiguracja odbywa się po stronie pliku .htaccess (np. przekierowanie na podkatalog).

O Jezu! Ok, mamy 2016 rok. Używanie .htaccess sugeruje użycie Apache2… W erze Nginksa jest to co najmniej dziwne i nieprofesjonalne. To tak jakby Home.pl nie wspierał nowych, lepszych technologii.

> Poczta w tym wypadku nie jest obsługiwana u nas.
>
> Domena nie musi być u nas opłacana, ale musi kierować na DNS aby była u nas podłączona. Nie utrzymujemy „przekierowań pośrednich” ani nieaktywnych, chociażby ze względu na to że takie ustawienia mogą w przyszłości wpływać negatywnie np. na prawidłową konfigurację domeny u innego operatora.

Jak może wpłynąć negatywnie na innego operatora, skoro MOJA domena jest skierowana na innego operatora i tam skonfigurowana? Ale tak jak już mówiłem, nie znam się.

> Reasumując, jeśli przekierowanie domeny na CloudFlare umożliwia jej dalsze delegowanie na nasze DNS, wrócisz do pierwotnej konfiguracji. Jeśli tylko rekord A, przekierowanie ok, ale bez poczty.

„… jeśli przekierowanie domeny…” Grzesiek chyba nigdy nie czytał nawet co to jest CF. Smutne. CF jest czymś w rodzaju wielkiego proxy. Dlatego też to na ich DNS odbywa się cała magia.

> CloudFlare jest rozwiązaniem, którego działanie ma konkretny cel, czy jest jednak gwarancją bezpieczeństwa? Zależy jak na to patrzyć. Biorąc pod uwagę, że nie resetujemy ustawień rekordów domen oraz oferujemy kopie bezpieczeństwa z 3 ostatnich nocy, masz praktycznie 100% ciągłość działania serwisu. Jedyna różnica to ładowanie serwisu z wielu lokalizacji i stref, pytanie, czy odczujesz różnicę w prędkości a tym samym czy w ogóle jest Ci to potrzebne?

W tym momencie moje oczy zalały łzy rozpaczy. Oczywiście, po co komu CF, skoro home.pl filtruje ataki DDOS, SQLi, XSS i w ogóle wszystkie inne co robi CF.

Jak rozwiązałem problem? Postanowiłem, że skoro płacimy za hosting, to już na serwerze www umieszczę aplikacje i wrzucę im te cholerne DNS-y.

Akt III – Migracja

No! Można by powiedzieć „Pehat jest już na jakiejś 20-30 minucie roboty”. No właśnie nie. To był już kolejny dzień. Wrzuciłem info na socialmedia o migracji, przygotowałem backupy.

Przeniosłem domenę na serwery home.pl – po godzinie wszystkie globalne DNS podawały już serwer home.pl. Dodałem domenę s-m-s.pl do wykupionego serwera i wgrałem pliki. Dodałem bazy danych, kliknąłem ok. Wszystko było w porządku. Postanowiłem wejść na s-m-s.pl by sprawdzić jak działa. I co? Przeglądarka przypomniała mi, że s-m-s.pl ma ustawione HSTS, czyli wymuszenie komunikacji szyfrowanej po stronie przeglądarki. Naturalnym było dla mnie, że skoro mam serwer WWW w home.pl, muszę dodać certyfikat SSL. Domyśliłem się, że będzie możliwe dodanie jednego certyfikatu SSL per serwer. Tak przynajmniej było w az.pl. To co zastałem w home.pl spowodowało u mnie chwilowe załamanie nerwowe. O ile CF nie jest czymś, co jest jakoś specjalnie wymagane, zalecane, czy często spotykane wśród zaleceń bezpieczeństwa, to już użycie SSL-a jest czymś normalnym, jak dieta bezglutenowa czy noszenie butów. Niby można bez, ale można się na tym przejechać. A co robi home.pl? Jak widać, po home należy spodziewać się wszystkiego. Pozwolę sobie znów przytoczyć co ciekawsze fragmenty oficjalnych materiałów home.pl: https://pomoc.home.pl/baza-wiedzy/jak-zainstalowac-wydany-certyfikat-ssl-na-serwerze-w-home-pl/.

> Proces instalacji certyfikatu SSL jest prosty i w pełni zautomatyzowany – ogranicza się do kliknięcia jednego przycisku i podaniu nazwy oraz hasła dostępu do serwera w home.pl.

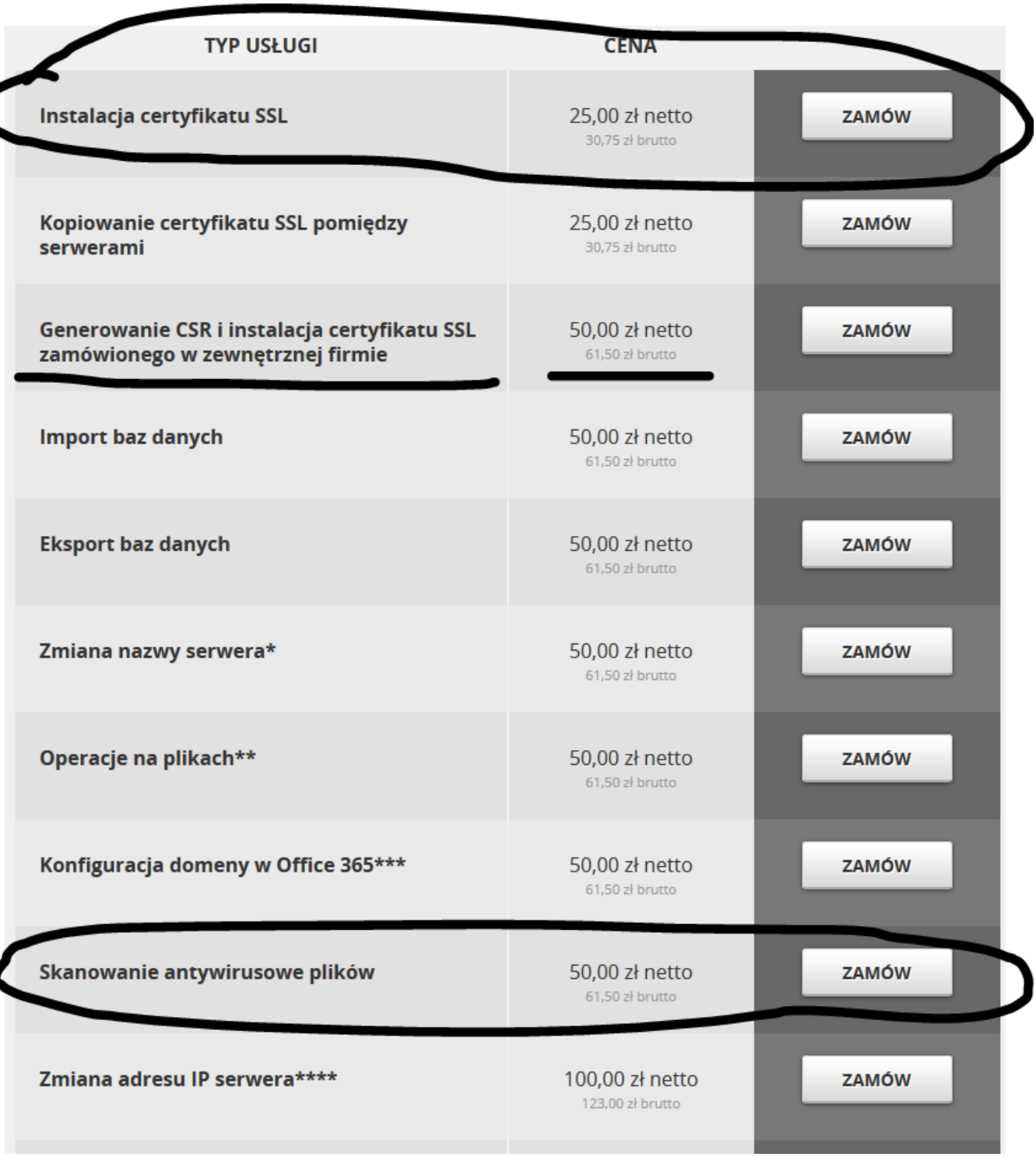
Tutaj miałem cichą nadzieję, że wyklikam to w kilka minut i pójdę spać.

> WAŻNE! Certyfikaty SSL w home.pl nie posiadają ograniczeń co do ilości serwerów, na których można je instalować. Oznacza to, że certyfikat SSL można zainstalować na wielu serwerach z tym ograniczeniem, że na jednym serwerze może zostać zainstalowany jeden certyfikat SSL.
> Przykład: zamówiony certyfikat RapidSSL Wildcard można zainstalować na dwóch, czterech lub nawet sześciu serwerach w home.pl (należy tylko pamiętać, że na tych serwerach nie mogą być już zainstalowane inne certyfikaty. W przeciwnym razie przytaczany w przykładzie RapidSSL Wildcard nadpisze certyfikat SSL znajdujący się na serwerze).

Zaraz zaraz…. Certyfikaty SSL w home.pl? Pewnie mówią ogólnie o tym.

> WAŻNE! Jeśli nie potrafisz samodzielnie zainstalować certyfikatu SSL, możesz skorzystać z oferty pomocy naszych administratorów. Instalacja certyfikatu SSL wykonywana jest przez administratora home.pl w ramach oferty Profesjonalne Usługi IT. Oznacza to, że instalacja zewnętrznego certyfikatu SSL zostanie wykonana przez naszych administratorów, po zamówieniu odpowiedniej usługi instalacji oraz po opłaceniu tego zamówienia.

No i „puff”… Ostatnia nadzieja prysła. Po tym co przeczytałem wiedziałem, że nieprędko skończę migracje, a co dopiero nawet pomyśleć o pójściu spać! Postanowiłem zobrazować i odnieść się do tych <hehe> „Profesjonalnych usług IT” (UWAGA, w trosce o przepełnienie oddziałów onkologii wrzucam tylko część usług).



TYP USŁUGI	CENA	
Instalacja certyfikatu SSL	25,00 zł netto 30,75 zł brutto	ZAMÓW
Kopiowanie certyfikatu SSL pomiędzy serwerami	25,00 zł netto 30,75 zł brutto	ZAMÓW
Generowanie CSR i instalacja certyfikatu SSL zamówionego w zewnętrznej firmie	50,00 zł netto 61,50 zł brutto	ZAMÓW
Import baz danych	50,00 zł netto 61,50 zł brutto	ZAMÓW
Eksport baz danych	50,00 zł netto 61,50 zł brutto	ZAMÓW
Zmiana nazwy serwera*	50,00 zł netto 61,50 zł brutto	ZAMÓW
Operacje na plikach**	50,00 zł netto 61,50 zł brutto	ZAMÓW
Konfiguracja domeny w Office 365***	50,00 zł netto 61,50 zł brutto	ZAMÓW
Skanowanie antywirusowe plików	50,00 zł netto 61,50 zł brutto	ZAMÓW
Zmiana adresu IP serwera****	100,00 zł netto 123,00 zł brutto	ZAMÓW

Przyjrzałem się tej rozpisce cen i stwierdziłem, że chyba pomyliły mi się czasy. Wydawało mi się, że żyjemy w 2016 roku, a nie w 1990, gdzie takie czynności jak wygenerowanie CSR i wgranie pliku z certyfikatem to za dużo dla przeciętnego użytkownika. Oczywiście

rozumiem, że płaci się za to, że ktoś zrobi to za mnie, ale chyba różnica 100% między wgraniem certyfikatu kupionego w home.pl a swoim własnym to zdecydowanie za dużo. W tym też momencie załamałem się całkowicie.

Co postanowiłem zrobić? Uciekłem się do starego, dobrego „ja sam". Kupiłem VPS w rootbox.com i w dwa dni przeniosłem wszystko czego potrzebowałem. SSL, Nginx, ZNC, shelle i wiele innych. Wniosek? Jeśli chcesz mieć zrobione dobrze – zrób to sam.

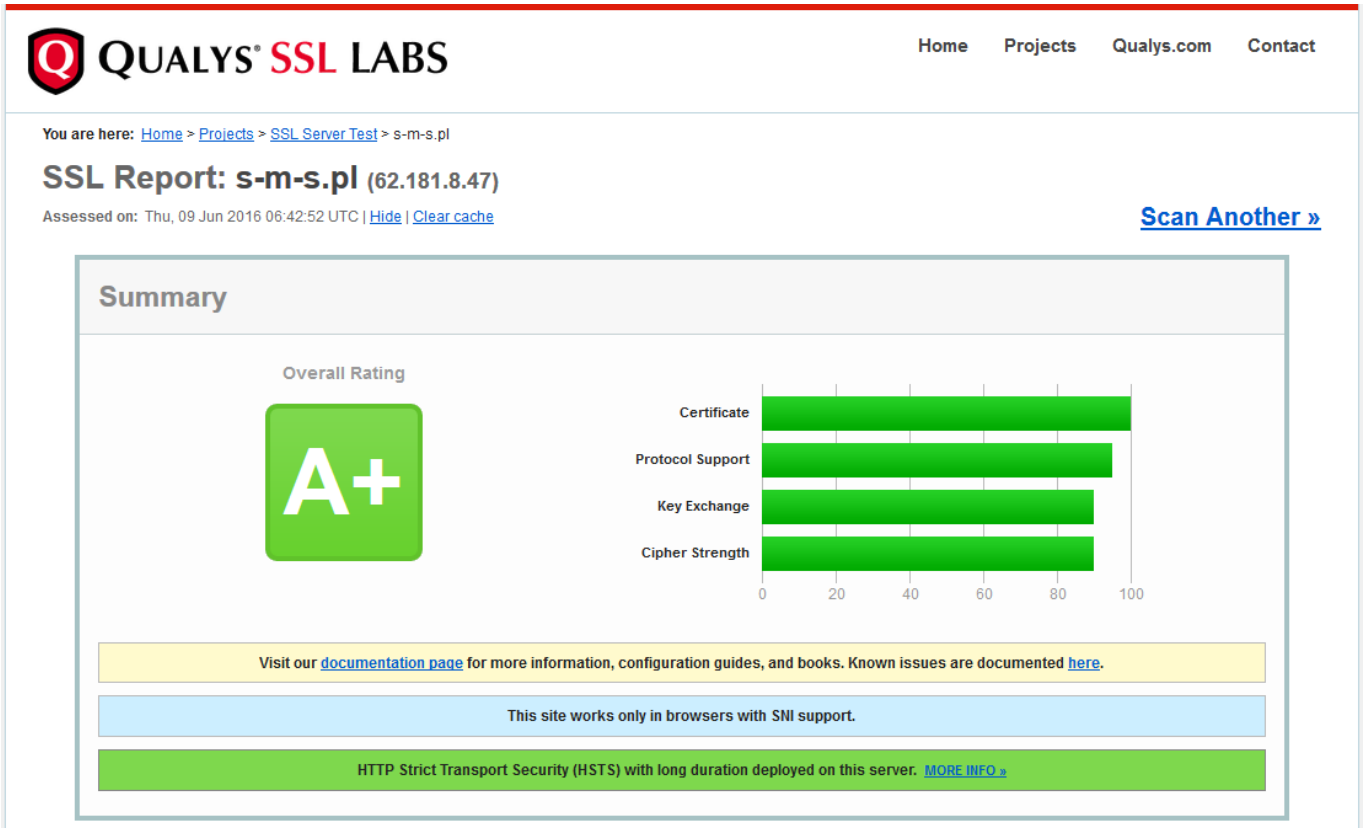
Akt IV – Podsumowanie

Wnioski z zaistniałej sytuacji są dosyć jasne. Lepiej zrobić coś całkowicie samemu, ewentualnie korzystając z pomocy realnych ludzi, a nie firm które twierdzą, że są liderem na rynku, a nie dostarczają podstawowych funkcjonalności. To smutne, że CI WIELCY LIDERZY NA RYNKU robią to, co robią, w tak zły i niechlujny sposób, wysysając przy tym każdą złotówkę od klienta.

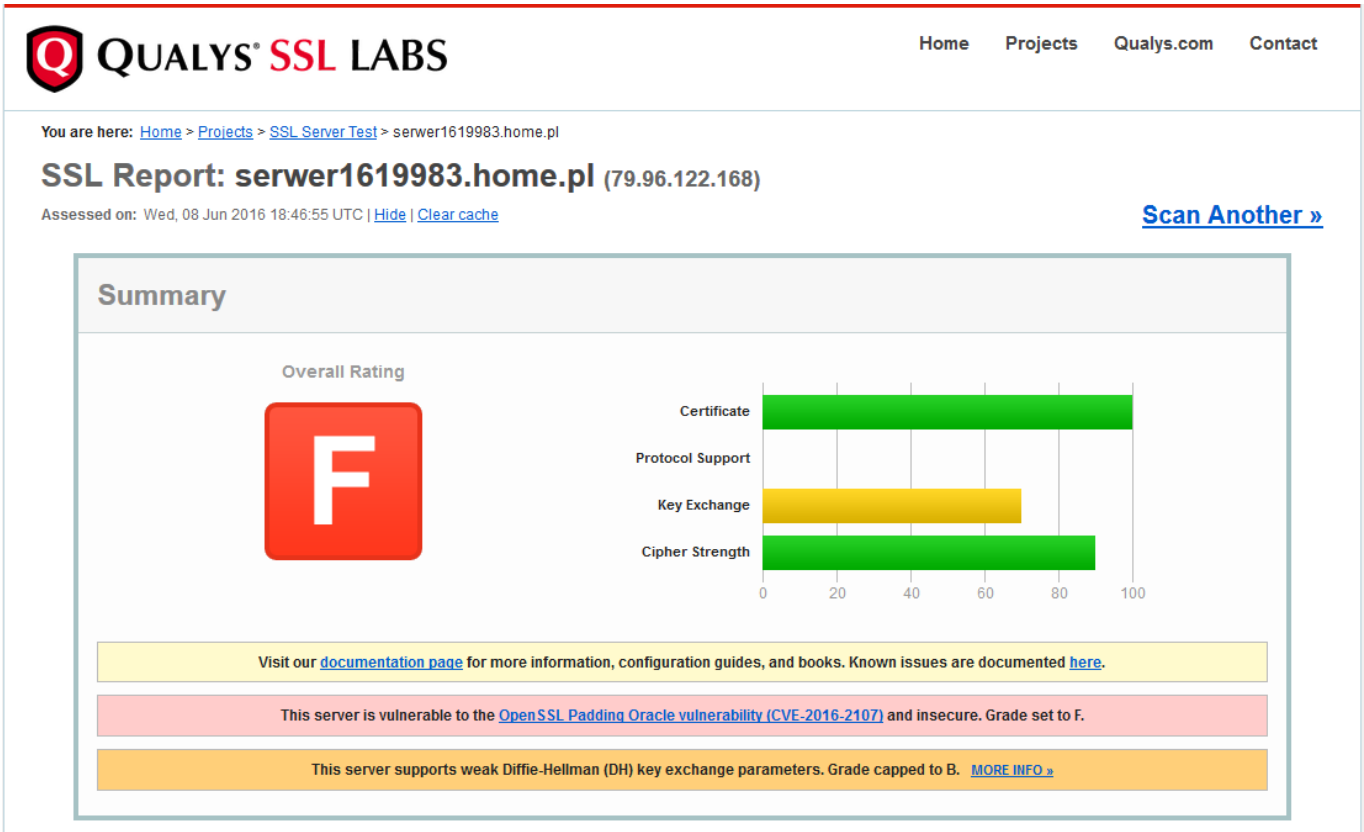
Ciekawostki!

Jak już tak się przyglądałem home.pl, postanowiłem sprawdzić ile tak naprawdę wart jest ten SSL od nich. Skonfigurowałem więc na VPS-ie wszystko tak jak potrzebuje, postawiłem SSL-a, wgrałem certyfikaty i porównałem za pomocą Qualys SSL Labs. Oto wyniki:

Dla s-m-s.pl


QUALYS SSL LABS
Home
Projects
Qualys.com
Contact
You are here: Home > Projects > SSL Server Test > s-m-s.pl
SSL Report: s-m-s.pl (62.181.8.47)
Assessed on: Thu, 09 Jun 2016 06:42:52 UTC | Hide | Clear cache
Scan Another »
Summary
Overall Rating
A+
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
This site works only in browsers with SNI support.
HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

oraz home.pl



Koniec końców, chyba jednak wolę wszystko robić samemu. Przynajmniej wiem, że robię to dobrze, a jeśli zrobię źle – mogę to poprawić. A jaki stąd wypływa morał dla ludzkości i potomnych? Home.pl powinno się zamknąć – dalece odstaje od standardów hostingu, jakich jako potencjalny klient spodziewałbym się po nich. Mam nadzieję, że ten artykuł gdzieś tam dotrze do zarządu home.pl i wezmę się oni za adminów i resztę ludzi odpowiedzialnych za taki stan rzeczy.

P.S.: W tym miejscu warto wspomnieć, że gdyby się dobrze pobawić serwerami od AZ, można by było się dobrać do backupów baz klientów. Fakt, to tylko moje przypuszczenia, żadnego konkretnego pentestu nigdy nie było. Dzięki bogu, home.pl ma usera w chroocie.

Drogie Home.pl oraz AZ Sp. z o.o.!

Z wielka przyjemnością zweryfikowałbym wasze zabezpieczenia oraz dokładnie opisał wasze oferty. Gdyby tylko nie fakt, że moglibyście oskarżyć mnie o naruszenie bezpieczeństwa…