64. Podstawy bezpieczeństwa w commerce - Artur Pajkert - Cyber Folks

Cześć! Nazywam się Grzegorz Frątczak, a to jest podcast „Rozmowy na zapleczu”, w którym wraz z właścicielami sklepów internetowych i e-commerce menagerami zgłębiam tajniki prowadzenia biznesu sieci. Szczerze, bez pudrowania rzeczywistości i po ludzku, bo to ludzie sprzedają, ludzie kupują i ludzie pracują, żeby to wszystko sprawnie działało. Zapraszam!

Cześć! Dzisiaj o tym, jak niebezpieczni ludzie mogą zagrozić Twojemu sklepowi. Czyli będzie o tym, jak ludzie mogą podrabiać Twoje domeny i co się z tym, wiąże. O złośliwym oprogramowaniu wstrzykiwanym w Twój sklep, o kopiach zapasowych, o filtrowaniu ruchu, by twój sklep nie dawał się złoczyńcom wysyłającym miliony botów do Twojego sklepu. A z kim będę rozmawiał? Z Arturem Pajkert, który od 20 lat zajmuje się hostingiem, a temat bezpieczeństwa jest mu bardzo bliski. To będą podstawy, więc jak jesteś zielony, albo chciałbyś odświeżyć wiedzę o tym, jak i co złoczyńcy mogą Ci zrobić na sklepie, to zapraszam do posłuchania. Trochę specjalnie tutaj straszymy, bo strachu w tym przypadku warto trochę mieć by się zmobilizować do działania i do zabezpieczenia własnego sklepu, bo ataków hackerskich na sklepy jest coraz więcej, więc ten podcast ma być mobilizującym Cię do działania i zabezpieczenia. Zanim zacznę to bardzo gorąco zapraszam Cię do zapisania się na newsletter na stronie convertis.pl/newsletter, dzięki temu żaden nowy odcinek podcastu Ci nie umknie, a dodatkowo dostaniesz newsy z pracy o e-commerce i nie tylko. A teraz już zapraszam do słuchania.

Grzegorz Frątczak: Cześć Artur!

Artur Pajkert: Cześć Grzegorz!

G.F: Drodzy dzisiaj zaprosiłem Artura Pajkerta z Cyber_Folks, który opowie nam o bezpieczeństwie i, który uwielbia żółty kolor. Tak, czy nie?

A.P: Nie, nie. Żółty to jest najlepszy kolor polskiego Internetu. To jest nasz firmowy kolor, po prostu. Ja mam wszystko żółte, a żeby nie było wiem, że teraz słuchacze nie mogą tego zobaczyć, ale żebyście widzieli minę Grzegorza, jak mu teraz pokazuje żółtą klawiaturę, którą

mu teraz pokazuję do kamerki, jak nagrywamy ten odcinek podcastu. To się nazywa wczuć się w swoją markę.

G.F: Okej, ja lubię pomarańczowy, dlatego Convertis ma pomarańczowe kolory, ale przyznaję nie mam nic pomarańczowego obok i chyba mnie zainspirowałeś, że chyba muszę sobie sprawić pomarańczowe rzeczy. To wiesz ciekawie. Dzisiaj właśnie z Arturem będziemy rozmawiać o bezpieczeństwie i z Cyber Folks i żeby było jasne my mamy własną, jakąś tam małą firmę, która nas wspiera od strony bezpieczeństwa. Ale Artur tak fajnie w różnych miejscach opowiada o bezpieczeństwie, że stwierdziłem, że go zaproszę, no bo to i sztuka i ładnie mówić i ciekawie mówić, tylko merytorycznie.

A.P: Dzięki wielkie za zaproszenie. No słuchajcie bezpieczeństwo to jest temat szalenie ważny, nie? Ważny dzisiaj dla nas wszystkich, coraz ważniejszy, bo coraz mocniej przenosimy nasze życie zarówno prywatne, jak i zawodowe do Internetu. 10-20 lat temu byliśmy mniej uzależnieni od sieci i komputerów, ale z każdym rokiem jesteśmy coraz bardziej społeczeństwem cyfrowym. No i dlatego te zagrożenia warstwy cyfrowej dotyczą nas w stopniu coraz większym.

G.F: Artur, ja mam takie pytanie podchwytliwe. Jak wpływa doktorat z filozofii na mówienie o bezpieczeństwie?

A.P: Mój doktorat jest z dziedziny nauk ekonomicznych, więc nie umiem się do tego odnieść.

G.F: Tu piszę Doctor of Philosophy, więc…

A.P: Bo tak się tak się P.G skrót, jakby rozkodowuje.

G.F: Aaaa.

A.P: A tak naprawdę to nie mówi dokładnie, w jakiej dziedzinie ktoś defakto się doktoryzował, bo właściwie, jak już poruszyłeś ten temat. To jest ciekawe zagadnienie. Czy doktorat się ma, czy doktorem się zostaje.

G.F: Czy doktorem się bywa.

A.P: Czy doktorem się bywa, dokładnie. Nie, bo to są takie „a co Ty umiesz robić?" „mam magistra". „Mam magistra", nie? Czasami takie można spotkać. Tak już całkiem teraz bez żartów, akurat moim obszarem zainteresowań naukowych był marketing na tym hostingowym rynku i to był mój przedmiot. Czyli zajmowałem się procesami wyboru dostawy usług hostingowych i pewnymi systemami wspierającymi decyzje konsumenckie w tym obszarze,

więc to takie połączenie trochę informatyki, bo dużo tam takich narzędzi, jak systemy ekspertowe, sieci neuronowe, sporo liczenia, obliczania jakichś wag, wariantów, drzew decyzyjnych i tego typu spraw, więc dużo matematyki i takiego informatycznego aparatu. Z drugiej strony też psychologii, która jest potrzebna, no bo umówmy się jesteśmy ludźmi, a nie maszynami i dobrze, w jakiś sposób uwzględniać to, w jaki sposób działają nasze procesy umysłowe. To jest bardzo ciekawa dziedzina, więc starałem się tutaj łączyć z jednej strony takie miękkie obszary psychologiczne, a bardziej z drugiej te twarde z obszaru matematyki, czy informatyki.

G.F: Wiesz co? Dzięki za to, że wiem w końcu P.G od czego to jest, bo nie wiedziałem. Człowiek uczy się całe życie. Myślałem, że tylko doktor jest, ale okej. Wracając do naszego tematu. No właśnie, jakie jest według Ciebie takie must have dla e-commerce zabezpieczeń, żeby to w ogóle miało ręce i nogi, żebyśmy mogli spokojnie w nocy spać.

A.P: W zasadzie nic nie jest tak niebezpieczne w e-commerce, jak po prostu ignorancja. Jak to, że my w ogóle nie myślimy o tym bezpieczeństwie. Niestety jest ona też powszechna i to jest największe zagrożenie. Nie ataki, nie SQL injection, nie fishing. Tylko po prostu nasza ignorancja, bo ona się będzie przekładać na wystawienie naszego sklepu na różnego rodzaju zagrożenia, które spływają na nas z sieci. Teraz, dlatego ja się tak osobiście angażuje w tą edukację w tym obszarze bezpieczeństwa z naciskiem na właścicieli sklepów i stron internetowych, ponieważ ogólnie muszę powiedzieć, że bardzo się poprawia edukacja w zakresie bezpieczeństwa użytkowników Internetu. W sensie takich konsumentów, osób, które kupują w sklepach, po prostu sobie chodzą po Internecie, przeglądają posty na Facebooku, itd. Czyli tak, jak korzystasz z Internetu po prostu prywatnie to możesz znaleźć dużo informacji typu nie loguj się na podejrzanych stronach, włącz sobie dwuskładnikową autentykację, żeby Ci tam konta nie ukradli na Facebooku, itp. rzeczy. Nie klikaj w linki te dziwne, co w SMS-ach do nas przychodzą, bo masz tam 1 zł dopłaty, do jakiejś przysyłki kurierskiej. Te akcje są coraz lepiej nagłaśniane dzięki mediom społecznościowym. Jakby na tym polu wydaje się, że jest taki rosnący poziom edukacji, chociaż jest to moje osobiste przekonanie. Niestety nie poparte żadnym twardym badaniem. Natomiast, kiedy tak obserwuję w ogóle, co się mówi o bezpieczeństwie, to moim zdaniem jest spora luka w komunikacji. Właśnie do właścicieli stron i sklepów, jak przygotować się, z jakimi zagrożeniami w ogóle może się mierzyć mój sklep internetowy. Umówmy się ktoś, kto zakłada sklep internetowy, to zazwyczaj bezpieczeństwo jest, gdzieś na szarym końcu jego listy. On myśli skąd wziąć towar, jak sprzedać ten towar, jak zorganizować obsługę klienta, jak to zrobić, żeby ten towar

paczkomatem, gdzieś tam trafił, jak zintegrować sobie różne wtyczki, jak optymalnie ustawić, jakąś kampanię Adsową, w Google Ads. To są te problemy, tak mi się wydaje, na których się koncentruje ten przedsiębiorca na początku, trochę mu się nie dziwię, bo przecież te rzeczy realnie się przekładają na przychód. Podczas, gdy bezpieczeństwo, ono wydaje się głównie kosztem, nie? Przecież musisz za coś zapłacić, kupić, jakiegoś antywirusa, kupić jakiś certyfikat, zapłacić, jakiemuś informatykowi, deweloperowi, adminowi, Bóg wie komu, za jakieś rozwiązanie dodatkowe i nie masz bezpośrednio z tego przychodu, nie? To nie jest takie przekładalne, więc myślę, że to dlatego jest to tak, gdzieś na końcu, a poza tym, no umówimy się jest też takie trochę trudne i wymaga eksplorowania wiedzy, co nie daje Ci takiego natychmiastowego poczucia stopy zwrotu. W sensie, jak np. uczysz się marketingu internetowego, dzięki czemu lepiej ustawisz sobie kampanię załóżmy, jakąś reklamową, to masz taki natychmiastowy zwrot, nie? Wow, to teraz sprzedaje więcej, np. efektywność każdego 1000 zł wydanego na moją reklamę jest teraz lepsza. Moja sprzedaż rośnie i czujesz to tak od razu fajnie w portfelu. A jeżeli zainwestujesz te same godziny w naukę nie marketingu, tylko bezpieczeństwa, no to nie masz tego poczucia, że dzięki temu Ci stan portfela rośnie, prawda. Trochę się trudno dziwić tym właścicielom sklepów, że nie jest to, gdzieś tam na topie ich zainteresowań, to bezpieczeństwo. Tym niemniej warto się, tym bezpieczeństwem się interesować, bo ono wpływ na przychody również może mieć. Choćby poprzez ekspozycję Twojego sklepu w wyszukiwarce, bo się okazuje, że jeżeli np. złośliwe oprogramowanie się wedrze do Twojego sklepu i Google to zauważy, to może zablokować Twoją domenę i bye, bye przychody. Google ma cały katalog kar dla stron, które zawierają złośliwe oprogramowanie. Wśród tych kar jest m.in. wykluczenie z wyników wyszukiwania, czyli po słowach kluczowych nie będzie Cię. Już nie chodzi o to, czy będziesz na pierwszej, czy na drugiej stronie, w ogóle Cię może nie być w wynikach wyszukiwania. Może, to też jest taka bardzo ciekawa sankcja, znalazłem w Internecie, że nakładana przez Google ok. 50 tys. razy tygodniowo w skali globalnej, to nie, że w Polsce, tylko na świecie. To jest zablokowanie strony internetowej, domeny na poziomie przeglądarki Chrome. Ona jest w tej chwili najbardziej popularna i ludzie korzystają w praktycznie każdym systemie operacyjnym z tej przeglądarki. Teraz to polega na tym, że jeżeli ktoś wejdzie na link do Twojego sklepu, z reklamy, czy na forum, jakimś przeczyta, to nie ma znaczenia. To zobaczy wielką czerwoną stronę z informacją, że ta strona jest prawdopodobnie niebezpieczna, czy na pewno chcesz kontynuować przygodę z tym adresem i bye, bye konwersje, bo nikt się nie zdecyduje na zakupy w takim sklepie, jeżeli w ten sposób przeglądarka wita Cię, jak próbujesz wejść do sklepu. Także te działania, które podejmujemy w zakresie bezpieczeństwa mimo że nie od

razu przekładają się na nasze zarobki, ale mogą nas uchronić przed spadkiem przychodu, bo jeżeli tak się stanie to nasz przychód spadnie. Drugim przykładem, takim dosyć częstym, niezależnym już nawet od Google. Jest to, że jeżeli masz sklep internetowy, czyli rodzaj strony, jakiejś, gdzie są pewne formularze, czyli np. zapis do newslettera, to ktoś może po prostu rozesłać spam z Twojego formularza, jeżeli on jest źle zabezpieczony, a w takim wypadku, jest wysokie prawdopodobieństwo, że Twoja domena bądź adres IP trafią na tzw. czarne listy. Wtedy serwery pocztowe u wielu dostawców przestaną przyjmować od Ciebie maile. Czyli będziesz wysyłał, jakiś newsletter sprzedażowy do swoich klientów, a on nigdzie nie dotrze, bo będzie klasyfikowany jako spam. No i to będzie bezpośrednio uderzać w Twój przychód, prawda? No, bo jeżeli potencjalni klienci, czy obecni klienci nie będą otrzymywać od Ciebie korespondencji, wiadomo to wtedy, to obniża Twoje szanse na generowanie zysków. Także tutaj przykładów można jeszcze pewnie kilka wymienić, ale jest jasne, że nie dbanie o bezpieczeństwo radykalnie podnosi ryzyko uszczerbku na Twoich przychodach.

G.F: To, o które rzeczy Twoim zdaniem warto zadbać. Takie TOP 5, a może 7, a może 10.

A.P: Śpiwory wzięliście wszyscy?

G.F: Mamy jeszcze pół godziny Drogi Panie, więc dasz radę.

A.P: Okej! Wiecie co? Słuchajcie kochani z bezpieczeństwem jest tak. Moim zdaniem, żeby trochę usystematyzować to myślenie, to możemy najpierw pomyśleć o pewnych warstwach, nie? Np. warstwa samej domeny, tak jak już wspomniałem. Tutaj zadbajmy o to, że domena jako ta podstawa funkcjonowania naszego sklepu była bezpieczna. Pierwsze takie źródła zagrożeń są dosyć takie śmieszne, ale to życie pisze takie scenariusze. To jesteśmy, my sami właściciele, a właściwie abonenci, bo domena ma abonenta, a nie właściciela, bo jest tylko na jakiś czas wynajmowaną nazwą domenową z rejestru, więc to jest bardziej odpowiednie określenie. No, ale o co chodzi. Tutaj Tomek Polak na I love marketing zachwycił mnie świetnym przykładem. Pokazał stronę Komitetu Parlamentarnego Prawa i Sprawiedliwości KP PiS. Teraz, ktoś tam po prostu zapomniał odnowić tą domenę i ona trafiła do puli domen wolnych i teraz pod tą domeną, pod którą kiedyś jedna z partii miała swój serwis bardzo oficjalny, jest Klub Pieczywa i Sera, bo skrót akurat pasował. Tak, więc ktoś zrobił sobie taki żarcik, rejestrując tą nazwę domenową, ale to pokazuje, że nawet taki prosty czynnik, jak pamiętanie o tym, żeby ta domena nie wygasała, to już jest pierwszy czynnik ryzyka. Jeżeli masz sklep internetowy, to po prostu nie przegapiaj tych maili. Dostaniesz pierwsze

powiadomienie z firmy hostingowej „Twoja domena wkrótce wygaśnie, opłać sobie na kolejny rok”.

G.F: Tak.

A.P: To nie rób tego błędu, że „a dobra jest piątek, to ja się zajmę tym po weekendzie”, bo jest spora szansa, że się tym nie zajmiesz, bo zapomnisz, bo gdzieś zleci już na dół w Twoim programie pocztowym i jest duża szansa takiego przykrego zdarzenia, jak to, że domena Ci przepadnie. Drugi przykład. No to, kiedy zaczynasz, zwłaszcza ze sklepem, zadbaj o to, żebyś to Ty był abonentem tej domeny. To, co z mojego doświadczenia wynika, to, że często, kiedy ktoś zleca przygotowanie sklepu developerowi i jakiejś agencji, ale zwłaszcza freelancerom, bo to się częściej chyba zdarza przy tych mniejszych projektach. To po prostu taki freelancer zakłada sobie hosting, jakby na siebie i domenę też. Na swoje dane i teraz chodzi o to, że w razie, jakiegokolwiek konfliktu później z taką osobą, która była wykonawcą. No to właściciel tego sklepu nie ma w zasadzie, jak udowodnić, że ma, jakiekolwiek prawda do tej nazwy domenowej, jeżeli to nie on jest tam wpisany jako abonent. Dlatego bardzo ważne, kiedy rejestrujemy nazwę domenową dla swojego sklepu. Pamiętajmy, żeby były tam nasze dane jako przedsiębiorcy jako właściciela tego sklepu, za nie dane, jakiegoś freelancera, albo developera, który technicznie to wykonuje. To czaszami nie musi być konflikt, to czasami może być taka sytuacja, że życie napisało taki scenariusz. Do mnie się zgłosiła Pani, która rok temu powierzyła komuś przygotowanie sklepu internetowego, to był taki micro projekcik i ta osoba wyjechała, gdzieś za granicę, nie ma z tą osobą żadnego kontaktu i to nawet nie, to, że się pokłócili o cokolwiek tylko zwyczajnie ten ktoś miał już inny pomysł na swoje życie. Żyje gdzieś teraz na drugiej półkuli, a ta domena wygasła i Pani nie ma żadnego dostępu do swojego sklepu i nawet nie może udowodnić za bardzo, że to jest jej sklep. Pamiętajmy o tym, żeby podawać swoje dane. Kolejne zagadnienia i przykłady, to są te zagrożenia związane z podrabianiem nazw domenowych, żebyśmy się tutaj zmieścili w czasie przewidzianym na nasz odcinek, to może poruszę tylko kilka. Jednym z najciekawszych wydają mi się ataki homograficzne i homofoniczne, to są ataki. Na czym to polega i dlaczego to jest ciekawe. One zostały opisane już 20 lat temu przez izraelskich naukowców. Oni zarejestrowali domenę Microsoft, korzystając z cyrylicy. Dlatego wydaje mi się to wydaje ciekawe, w sytuacji geopolitycznej i różnych cybernetycznych zagrożeń ze wschodu, które w tej chwili nam zagrażają, bo sami choćby w zeszłym miesiącu padliśmy ofiarą grup sympatyzujących z Rosją, które mściły się na firmach wspierających Ukrainę. To się dzieje i w cyrylicy jest tak, że niektóre znaki z cyrylicy graficznie są bardzo podobne do naszego łacińskiego alfabetu,

czyli np. to, co po rosyjsku czytamy jako s, wygląda, jak nasze c, co po rosyjsku czytamy jako t, wygląda, jak nasze m, itd., itd. No i to powoduje, że można spreparować nazwę, która wygląda łudząco podobnie, do jakiejś polskiej nazwy domenowej np. do nazwy Twojego sklepu, ale jest zapisana z użyciem cyrylicy po prostu. No i dla osoby zwłaszcza w pośpiechu jest to bardzo trudne do rozróżnienia, czy to jest prawidłowa nazwa, czy tylko taka podróbka. Zwłaszcza, kiedy znaki są podobne. mBank też padł ofiarą takiego ataku niedawno. Tam był taki atak słynny, że napisano mBank, ale a było z taką malutką kropeczką, ale to nie było z cyrylicy, tylko akurat, z jakiegoś innego alfabetu. To było z takim jednym pikselkiem tylko, taką kropką na dole. Niestety nie wiem, z jakiego języka pochodzi taka litera a, ale to bardzo ładnie pokazuje, że każdy pomyśli, że to tylko paproch na ekranie, to jest jeden piksel malutka kropeczka i dużo osób tego nie zauważy, a kiedy strona jest łudząco podobna graficznie do tej Twojej strony, to ktoś się może bardzo łatwo nabrać. Chyba, że jest osobą niewidomą, bądź niedowidzącą, bo jak niedawno się dowiedziałem na Work Campie w Warszawie i to był bardzo insite po moim wystąpieniu na temat bezpieczeństwa, że na te ataki homograficzne, narażone są osoby widzące, ale nie osoby niewidome. One korzystają z Internetu przy użyciu czytników, które po prostu czytają i tutaj graficzna reprezentacja znaków z oczywistych powodów nie ma znaczenia. Natomiast te osoby są narażone na atak homofoniczny, czyli można spreparować napis, który wygląda może i inaczej, ale czyta się bardzo podobnie. Czyli np. mBank mPank. O tak powiedzmy, no nie? Wtedy już taka osoba niewidoma jest na to bardzo narażona, na taką fałszywą nazwę domenową. No i dlaczego to jest groźne? Dlatego że, jeśli ktoś spreparuje kopię Twojego sklepu, co jest bardzo proste. Wystarczy screenshot zrobić i już będzie wyglądać, jak Twój sklep, nałoży na to, jakiś fałszywy formularz logowania, to jeżeli przekona Twoich klientów, żeby podali tam swoje dane login i hasło pod byle pretekstem np. Twoje zamówienie ma jakieś opóźnienie. Sprawdź status swojego zamówienia, albo musieliśmy anulować Twoje zamówienie, no whatever, prawda? Jakiś byle pretekst i trafi to do Twojego klienta i nie daj Boże, któryś z tych klientów się nabierze i zostawi tam swoje dane, to oczywiście jest w dużym kłopocie, bo jego dane w tym momencie przejmuje, jakaś przestępcza organizacja, bądź osoba po drugiej stronie i raczej będzie starała się je maksymalnie wykorzystać. Będzie się np. próbowała logować do banku, zmieniać hasła, no na różne sposoby może próbować to wykorzystać, albo nawet przyjmie zamówienie w skrajnym przypadku, tylko nie wyśle towaru. No i oczywiście, to do Ciebie przyjdzie policja, czy prokuratura potem wyjaśniać tą sprawę, nie?

G.F: A później jest zonk.

A.P: Tak, dokładnie. No ale wiesz co? Moim zdaniem najgorszą opcją, która może się zdarzyć, to na nawet nie jest to. Tylko sytuacja, w której prowadzisz już sobie ten sklep i wyobraź sobie, że masz 500-1000 stałych klientów i niech tylko 10 poda omyłkowo swoje dane komuś, kto się pod Twój sklep podszywa. To teraz ta osoba, która pozyskała te dane idzie do Ciebie i mówi „hej, ukradłem Twoją bazę klientów, mam loginy hasła, wszystkie dane osobowe, wszystkie numery kart kredytowych, wszelkie dane, masz tutaj 5-10 loginów i haseł, żebyś sobie sprawdził, że to jest faktycznie Twoja baza i tutaj masz adres portfela bitcoin, kup w wysokości takiej, a takiej, masz 48h, dziękujemy". No i co? Już się będziesz zastanawiał, czy to już jest atak serca, czy jeszcze nie, ta nagła duszność, którą w tym momencie czujesz, nie? No, bo skąd masz wiedzieć, czy on ma całą bazę, czy nie. Łatwo Cię może szantażować taka osoba w tym momencie. Także tych wektorów ataku może być bardzo dużo, dlatego dobrze też tej swojej tożsamości, strony po prostu pilnować.

G.F: A jeszcze tak trochę krócej proszę. Jakieś dodatkowe rzeczy odnośnie bezpieczeństwa sklepu, jak zabezpieczyć sklep?

A.P: Bardzo ważny jest certyfikat SSL i tutaj w sklepie dobrze mieć certyfikat na wyższym poziomie walidacji niż popularne bezpłatne letsencrypty. Dlatego że tylko wyższe poziomy walidacji tzn. OV, bądź EV, zapewniają to, że jak ktoś kliknie w tą kłódkę to w szczegółach zobaczy adres Twojego sklepu i nazwę Twojej firmy. W przeciwnym wypadku tak jak 80-85% firm w Polsce korzystasz z bezpłatnego certyfikatu to nie dajesz żadnej szansy użytkownikowi na zweryfikowanie, czy jest na właściwej stronie. To nie jest drogie zabezpieczenie, bo taki certyfikat, to jest dużo taniej, niż comiesięczna składka ZUS. Tu mówimy o kwotach w skali roku, to wydasz na taki certyfikat kilkaset złotych, nie wiem 300-500, to są kwoty tego rzędu nie mówimy tu o wielkich pieniądzach, a naprawdę to znacząco może poprawić bezpieczeństwo Twojego sklepu. Kolejna sprawa, to, co warto mieć włączone, to jest zapora sieciowa tzn. WAF. No i to są takie sprawy, ze każdy operator hostingowy ma tutaj swoje rozwiązania. Warto się zorientować, jakie rozwiązania tutaj w tym zakresie oferuje Twój hosting. Dobrze, jeżeli one są castomizowane, bo każdy z nas ma sklep z innej branży, ma inne wymogi, co do bezpieczeństwa. Dobry przykład znowuż napisało życie. W naszym Wafie jest m.in. filtrowanie żądań zawierających znaki z chińskiego alfabetu, ponieważ zakładamy, że 99% naszych klientów prowadzi strony w języku polskim, skierowane do Polaków, to jeżeli ktoś próbuje mieć, jakąś interakcję z tą stroną, używając chińskich znaków, to zakładamy, że nie ma on dobrych zamiarów i na 99%, to jest po prostu, jakiś spam. My zaproponowaliśmy zablokowanie tych chińskich znaków i byliśmy z siebie

bardzo zadowoleni, widząc, jak dużo z nich blokujemy. Dopóki nie zadzwoniła Pani, która mówi „co się stało, że mój adres IP został zablokowany?" „No to proszę opowiedzieć." No to ona opowiada, że ona ma u nas stronę i strona to jest hodowla chińskich piesków i ona wystawia tam szczeniaki, chciała nadać szczeniakowi, jakieś imię, używając tego chińskiego alfabetu i wtedy jej IP zostało nagle zablokowane.

F.G: I co? Znaleźliście przyczynę?

A.P: No przyczyna była taka właśnie, że sama Pani powiedziała, że próbowała tego chińskiego znaku użyć, nieświadoma, że sobie włączyła to zabezpieczenie przed chińskimi znakami i dlatego jej IP zostało zablokowane. Wyjaśniliśmy Pani, na czym polegają te zabezpieczenia i w jej przypadku nie można takich reguł filtrujących używać i w tym obszarze musiała sobie wyłączyć tą zaporę. Oczywiście mogła sobie pozostawić filtrowanie tam innych rodzajów ataku, ale akurat nie ten związany z chińskimi znakami. To jest dobry przykład na to, że bezpieczeństwo, to nie jest jedno rozwiązanie dla każdego, to jest przykład tego, że bezpieczeństwo trzeba szyć na miarę. Jak masz hodowlę chińskich piesków, to nie filtruj sobie chińskich znaków, ale jak masz sklep z modą i najpopularniejsze kategorie to: ubrania, obuwie, dom i ogród, to tam prawdopodobieństwo używania tych chińskich znaków jest znikome i tam będziesz mieć więcej dobrego z filtrowania takiego ruchu, niż złego, nie? Podobnież z cyrylicą, czy innymi egzotycznymi bardziej alfabetami, bo one bardzo często prowadzą do spamowania Twojej strony, czy Twojego sklepu.

G.F: Czyli trzeba uważać na podrabianie domen. Zaraz może porozmawiamy, co możemy zrobić. Z drugiej strony zabezpieczenie przed atakami, takimi trochę, żeby obciążyć nasz sklep, czyli tzw. dds, czyli ruch, który jest nam nie potrzebny. No a z trzeciej strony zostaje jeszcze serwer, czyli, jak chronić się przed tym, że ktoś próbuje się do nas dostać i zrobić nam ziaju, prawda?

A.P: No tak, bo to warto rozróżnić, że te dds szeroko rozumiane i, które mają na celu albo wysycenie łącza, albo przeciążenie serwera. A z drugiej strony mamy ataki, które są skierowane na zainstalowanie w naszym sklepie, jakiegoś złośliwego oprogramowania. To złośliwe oprogramowanie może próbować wykraść naszą bazę danych. Przykładowo w sklepach często stosuje się gotowe motywy graficzne, choćby w Wordpresie. To było kilka lat temu popularny taki pakiet RevSlajder po prostu slajder obrazów, ponieważ to tak ładnie wygląda, dużo osób chciało mieć ten slajder. Okazało się, że on miał dosyć dużą lukę, która pozwoliła tak preparować żądanie, żeby zamiast obrazka na slajderze, który się gdzieś tam

przesuwa, wyświetlić plik konfiguracyjny Wordpressa, na którym są dane dostępowe do bazy danych. W związku, z czym przez podatność w tej wtyczce można było uzyskać dosyć szybko i łatwo dostęp do bazy danych Wordpressa, a co za tym idzie mieć pełną kontrolę nad tym Wordpressem. A w szczególności, gdyby tam był sklep, to wykraść dane o zamówieniach, dane osobowe klientów, itd., itd. Także konsekwencje mogłyby być bardzo poważne, czyli z jednej strony są te ataki, takie obciążeniowe, które mają przeciążyć łącza, albo serwery. A z drugiej strony są te ataki z próbami wykonania, bądź zainstalowania złośliwego kodu, złośliwego oprogramowania.

G.F: No właśnie, czyli mamy takie 3 kategorie, czy coś byś jeszcze dodał?

A.P: Myślę, że tak, że możemy iść dalej. Mamy jeszcze kategorie związaną z kopiami zapasowymi w ogóle i z hackowaniem właściciela sklepu. Zwłaszcza, kiedy nie jest on zawodowym informatykiem, to też jest bardzo ciekawe. Wyobraź sobie tą sytuację, w której prowadzisz sklep internetowy, ale nie jesteś z wykształcenia informatykiem, deweloperem i oglądasz sobie coś na YouTube, jak zmienić coś w ścieżce konwersji, przestawisz coś niby, w jakiejś wtyczce i coś będzie lepiej w Twoim sklepie. No i próbujesz to zrobić, niby wszystko robisz, tak jak na filmie, ale sklep się rozwala. No i teraz wyobraź sobie tą sytuację, że ktoś robi w tym sklepie zakupy, a Ty próbujesz zoptymalizować sobie, jakąś konwersję, dodać, jakiś skrypcik i powodujesz, że on widzi błąd. Klienta już, wtedy na pewno stracisz, ale zaczniesz się bardzo szybko pocić i denerwować, jak to teraz odwrócić to swoje działanie, nie? Czy możesz łatwo się cofnąć i naprawić ten swój błąd. Tutaj są dwie kategorie: pierwsza kategoria, to jest to, żeby wszystkie takie zmiany robić na osobnym środowisku. Czyli po prostu sklonuj sobie ten swój sklep z tymi samymi ustawieniami wersji PHP, żebyś wiedział, że to jest dokładnie to samo, z tymi samymi danymi, co masz na produkcji, niektóre hostingi mają taką funkcję nazywa się Staging i na tej kopii sobie testuj, nanoś i dopiero, jak będziesz mieć pewność, że to, co tam chcesz zrobić nie psuje Ci tego sklepu, to dopiero, wtedy rób, to w środowisku produkcyjnym. Także to nie jest taki atak z zewnątrz, ale to jest po prostu ludzki błąd właściciela, który może mieć duże konsekwencje dla tego biznesu. No i ważne jest w związku z tym regularne wykonywanie kopii zapasowych. To jest niby trywialne, ale może ja powiem dwa słowa na temat tych kopii. Dużo osób sobie myśli „zapytam firmę hostingową, czy robi backup", no i ta firma powie „tak, robimy codziennie", no to będzie „uf to już nie muszę" i to będzie uczucie takiej pewnej ulgi. Natomiast to nie do końca tak funkcjonuje, nie do końca tak działa. Po pierwsze, jeśli prowadzisz sklep, to moim zdaniem dobrze, żeby ta kopia była wykonywana wielokrotnie w ciągu dnia, zwłaszcza kopia bazy

danych. Kiedy ten Twój sklep ma już pewną skalę, to jest możliwe, że przetwarzasz dziesiątki, a nawet i setki zamówień każdej doby. Jeżeli będziesz robić kopię zapasową tylko raz na dobę i cokolwiek się popsuje i będziesz mieć potrzebę przywrócenia danych z tej kopii, to wtedy tak na zdrowy rozsądek, możesz stracić cały dzień zamówień. Skoro tylko raz dziennie są wykonywane kopie. Dlatego po prostu zwracaj uwagę na to, jak często te kopie są wykonywane i dużo lepsze rozwiązanie, no to, żeby one były wykonywane, co kilka godzin, tak? Co 4-6 godzin, a nie, co 24 godziny. Druga sprawa, to, to, jak długo te kopie są przechowywane. Te kopie zapasowe, które wykona dla Ciebie hosting, bądź te, które Ty wykonasz. Zaraz powiemy sobie jeszcze o tych, które robi hosting, o tych, które Ty robisz. Wyobraź sobie tą sytuację, że masz sklep internetowy i ktoś się włamał i zainstalował Ci wadliwy skrypt, jakiś w tym sklepie, który, co 10 klientowi zamiast Twojej oferty wyświetla trupią czachę, albo cokolwiek. Nie pożądany w każdym razie, złośliwy skrypt, a Ty jesteś akurat na urlopie i wracasz po 14 wspaniałych dniach w ciepłych krajach i widzisz, że masz trupią czachę na sklepie i co? Bierzesz kopię zapasową, nie? Tylko, że jeżeli przechowujesz tylko 3 ostatnie kopie zapasowe, to jest duża szansa, że w tej najstarszej kopii też masz trupią czachę. Dlatego dobrze jest po prostu wybierać takie rozwiązania, czy tak sobie skonfigurować te kopie zapasowe, żeby odpowiednio długo mieć tą ostatnią kopię, żeby mieć do czego sięgnąć. Tu są ogromne różnice pomiędzy firmami hostingowymi na rynku, bo niektóre przechowują tylko ostatni dzień, niektóre 2-3 dni, a niektóre praktycznie miesiąc. Warto sobie to wybrać, myśląc na jakie długie urlopy jeździsz. Jeśli w ogóle nie jeździsz na urlopy to być może Ci wystarczy kilka dni, jeśli coś robisz na tej stronie. A jeżeli miewasz takie dłuższe wyjazdy, czy jakieś okresy, gdzie nie śledzisz tej strony tak cały czas, to wtedy radzę postawić na dłuższy okres przechowywania tych kopii. No i ostatnia sprawa, no może jeszcze nie ostatnia, ale jest jeszcze sprawa lokalizacji, z której też dużo osób tak do końca sprawy sobie nie zdaje. Tutaj zawsze lubię zabrać słuchacza w przeszłość w lata 40. p.n.e, kiedy wojska Juliusza Cezara zdobywały Egipt Północny i tam w czasie działań wojennych doszło do pożaru biblioteki aleksandryjskiej. Biblioteka aleksandryjska niczym centrum antycznego świata, pełna zwojów, papirusów z całą wiedzą tam zebraną wówczas i niestety znaczna część tego księgozbioru spłonęła. Mija 2000 tys. lat i dzieje się, to samo w Europie Zachodniej w Strasburgu. Płonie jedno z największych centrów danych w Europie i tysiące serwerów, jak to mówią złośliwi przenosi się do chmury. Mimo że minęło 2000 tys. lat i my już tych danych nie zbieramy na papirusie, tylko na twardych dyskach. Mimo tych wszystkich zabezpieczeń, mimo tych wszystkich detekcji, które potrafią w wielkiej hali wykryć 1 spalony zasilacz, mimo tych wszystkich butli z gazami wypierającymi tlen z powietrza wciąż się to

zdarza. Nawet w Polsce się zdarzyło w archiwum krakowskim przecież, nie taki dawny słynny pożar. A to tylko pokazuje, że myśląc o kopiach zapasowych, warto pamiętać o tym by jedną kopię trzymać w odrębnej lokalizacji, żeby to nie było tak, że my te wszystkie kopie trzymamy w jednym budynku, w tym samym mieście wręcz, bo w razie, jakiegoś wielkiego, katastroficznego wydarzenia, powódź sobie wyobraźmy, albo jakiś ogromny pożar, to wtedy te dane stracimy bezpowrotnie. A jeśli te dane przechowujemy w innym mieście, bądź w innym kraju nawet, to wtedy możemy czuć się o wiele, wiele bezpieczniej. Z jednej strony te kopie wykonywane przez firmy hostingowe są fajne i wygodne, bo robią się same, ale jest jeszcze jeden taki czynnik ryzyka. Nazwijmy to prawno-organizacyjny, czyli jeśli robisz dodatkową kopie całkiem samodzielnie, całkowicie niezależnie od firmy hostingowej. Masz wtedy taką polisę ubezpieczeniową na wypadek, gdyby z tą firmą jako przedsiębiorstwem cokolwiek się stało. Możemy sobie wyobrazić zwłaszcza w przypadku mniejszych podmiotów, że no nie wiem właściciel umiera i firma się, gdzieś rozsypuje. Różne rzeczy się mogą zdarzyć, więc żebyśmy byli niezależni organizacyjnie od tej konkretnej firmy, to dobrze sobie, gdzieś taką kopię trzymać całkowicie poza infrastrukturą i związkiem z daną firmą hostingową. Myślę, że to jest takie zdrowe podejście. Ostatnia sprawa z kopiami, dobrze jest sobie, jednak testować, czy to, co my gromadzimy w tych kopiach daje się w ogóle przywrócić. To też jest istotne w IT, że nie tylko, żeby te kopie wykonywać, ale też, żeby je po prostu weryfikować. Może się zdarzyć, że coś mamy źle ustawione w tym mechanizmie kopii zapasowych, że nie w całości ta nasza strona zostanie skopiowana. Nie wiem, że zabraknie miejsca na urządzeniu, na którym ma być ta kopia zapisana. No różne rzeczy się mogą wydarzyć. Lepiej sobie, jednak sprawdzić, czy z tej kopii daje się przywrócić nasz sklep i zamówienia, więc taki wariant minimum, że sobie tam wyrywkowo sprawdzajmy np. raz w miesiącu, czy te dane da się w ogóle odczytać.

G.F: Okej, super. A tak się zastanawiam odnośnie tego, bo jeśli wracając, jak się przed tym zabezpieczyć. To jeśli mamy te różne problemy z domenami, czy podszywanie się pod domeny, to co mam wykupić 50 domen bliskoznacznych pod to? Czy to zależy od skali? Jak to wygląda z Twojej perspektywy?

A.P: Na pewno skala, skala ma wpływ. Bezpieczeństwo jest akurat dosyć dobrze skalowane. Teraz, jeżeli masz wiele domen i wiele różnych stron pod tymi domenami, bo to jest jeszcze dosyć istotne, czy są tylko domeny, czy to są faktycznie działające serwisy. Jeżeli to masz np. na jednym serwerze, przechowujesz, w jakiejś firmie, to wchodzi dosyć istotne zagadnienie tzw. separacji domen. Ta separacja domen polega na tym, że którakolwiek z tych stron będzie

mieć słaby punkt, przez którykolwiek dostaje się, jakaś infekcja, jakieś złośliwe oprogramowanie, to ono nie będzie w stanie się rozprzestrzenić na Twoje pozostałe usługi, na Twoje pozostałe strony. Jeżeli nie masz tej separacji domen, to w takim wypadku narażasz się na to, że jedna z Twoich stron zostanie skutecznie zaatakowana, a tego typu oprogramowanie może wykryć, że masz też inne domeny i inne strony i automatycznie zainstalować się także na nich. Z punktu widzenia bezpieczeństwa, zatem taka separacja, to dobry pomysł.

G.F: A co rozumiesz przez separacje? Oddzielne serwery?

A.P: Separacja polega na tym, że Ty kupujesz jedno konto na serwerze w firmie hostingowej. Natomiast, jakikolwiek skrypt, który jest wykonany w folderze, gdzie masz daną domenę, zasięg jego działania nie może wyjść poza ten folder. Teraz, jakikolwiek wirus, który załóżmy masz na serwerze. Masz kilka katalogów: katalog1, katalog2, katalog3 i masz domenę 1, 2, 3 odpowiednio skierowane, czyli coś Ci zaatakuje katalog, gdzie masz tą domenę 3, to jakikolwiek skrypt tam jest wykonywany, to jego skutki działania nie wyjdą poza ten katalog3. W związku z tym nie zainfekują katalogów 1 i 2, ale są też pewne minusy z tym związane. Np. takie, że niektóre instalacje multisite potrzebują tego, żeby jeden skrypt działał na wielu domenach. Mniej więcej, to polega na tym, że budujesz stronę i masz taki jeden wspólny silnik i potem wiele różnych domen, prawda? Wtedy potrzebujesz czegoś takiego, albo ktoś potrzebuje przy poczcie, żeby mieć jedną skrzynkę na serwerze pocztową i żeby ona obsługiwała maile z różnych domen. Kiedy takiej rzeczy potrzebujesz, to wtedy ta separacja, to już nie jest taki dobry do końca pomysł, nie, więc są plusy i minusy, takiej separacji.

G.F: Artur, tutaj bardziej pytałem o te problemy homograficzne, Mam nie wiem domenę convertis.pl. Jest przez C i przez V, to ktoś może kupić sobie domenę przez K i przez W. Czyli jedyna szansa, aby zabezpieczyć się przed podrabianiem tych domen, to jest wykupienie wszystkich podobnych potencjalnych domen?

A.P: No wiesz, to jakoś ogranicza ryzyko, ale też wydaje się dosyć drogie, aby utrzymywać tyle różnych domen, ale powiedzmy kilka wariantów, które uznajesz za najbardziej niebezpieczne, to jeżeli masz już pewną skalę biznesu, to może Ci się opłacać to kupić. Nie tylko dlatego że ktoś będzie podrabiał, ale ktoś może wykorzystywać podobieństwo tej domeny i czerpać korzyści z ruchu, który by trafiał do Ciebie po prostu. Natomiast to, co jest tutaj pewną formą zabezpieczenia, to właśnie te lepsze certyfikaty SSL, bo wtedy zawsze możesz uświadamiać swoich klientów „słuchajcie, jakbyście chcieli się logować, zawsze sprawdzajcie, co tam jest pod tą kłódką” i wtedy oni przeczytają pod kłódką convertis, kod,

miasto, województwo, kraj, itd. Tego nie będą mieć ci, którzy się podrabiają, bo żeby taki certyfikat wyrobić, to musi być zgodność z danymi z rejestru handlowego. Jeśli jesteś wpisany w rejestrze sądowym, czy rejestrze działalności gospodarczej, to ta osoba musiałaby podszyć się pod Ciebie na tyle skutecznie, żeby mieć odpowiedni wpis w CEiDG, czy w KRS-ie.

G.F: Chciałem tylko powiedzieć, że właśnie sprawdzam i ktoś sobie wykupił domenę convertis przez w i jest kup, wyprzedź konkurencję. Czy chodziło Ci o convertis, Chrome tutaj podpowiada. Akurat ta moja homofoniczna nazwa już ktoś sobie kupił i się może pode mnie podszywać.

A.P: Może, może, albo niekoniecznie się musi podszyć, ale może wykorzystać, jeśli Twoja marka Convertis przez v będzie popularna. Zobacz to jest przykład takiej marki, która rodzi pewne wyzwanie w dyktowaniu. Jeśli mówisz komuś przez telefon wejdź sobie na Convertis, to on tak do końca nie wie, czy przez C, czy przez K, czy przez W, czy przez V, prawda? Można na kilka sposobów, to napisać, więc taka osoba, jeśli miałbyś już taką popularną markę z dużym ruchem, dlatego że ludzie przypadkowo tam wejdą. Nie musi bardzo pod Ciebie podszywać, nie mus mieć aż tak złowrogi zamiarów, ale może zrobić ale może zrobić przekierowanie na Aliexpress z jakimś reflinkiem, dzięki któremu, jeśli ktoś by zrobił zakupy na Aliexpress, to sobie będzie po prostu ta osoba zarabiać. Czyli ktoś po prostu będzie zarabiać na popularności Twojej strony, a Ty nie dostaniesz z tego ani grosza. Także tak też może być. Onat, Onet. Jak sobie wejdziesz na Onet, nie popularny portal informacyjny polski, a Onat. No właśnie, ja dostałem przekierowanie z reflinkiem na Aliexpress, więc gdybym sobie kupił toster w Chinach, to ktoś by sobie zarobił na takiej pomyłce.

G.F: Teraz to idzie do jednego z bardziej popularnych sklepów RTV.

A.P: No, więc generalnie różnego rodzaju programy afiliacyjne.

G.F: Ten ktoś zarabia na polskim sklepie, znaczy chyba jakaś jedna firma, która ma reflinki do nich i tu można powiedzieć, że tu zarabia trade tabler… coś tam i można pójść tam.

A.P: No widzisz. Ja podejrzewam, że za każdym odświeżeniem możesz dostać całkiem inny wynik, bo to często się, gdzieś tam rotuje, to nie będzie tak, że zawsze będzie to samo. Może tak być. Już czujesz ten mechanizm, prawda? Podobna nazwa, jedna literka różniąca i ktoś

sobie po prostu zarabia na takim ruchu użytkowników, którzy chcieli wejść do Ciebie, a tak naprawdę wchodzą, gdzie indziej.

G.F: A jak się chronić przed atakiem takim ruchu, że mamy bardzo duży ruch na naszą stronę. Czy tylko te WAF'e, o których mówiłeś nas chronią, czy są jeszcze?

A.P: Wiesz co? Tutaj Ty jako taki przeciętny właściciel sklepu masz ograniczone pole działania, bo zazwyczaj jest tak, że tego typu ataki wymagają już reakcji poziom wyżej. Czyli najczęściej jest tak, że…

G.F: Czyli dzwonię do Artura „Artur".

A.P: Tak dzwonisz do swojego operatora hostingu. Do mnie możesz zadzwonić jasne, jak tylko do nas przyjdziesz na hosting zapraszam. Możesz, jak najbardziej zadzwonić do swojego operatora hostingu, czy tam napisać, jaką masz tam z nim formę kontaktu. Teraz w zależności od tego, jak to jest rodzaj ataku, bo tu chodzi o to, że Ty jako właściciel strony, to kiedy ten ruch trafia na Twoją stronę, to Ty masz nad tym pełną kontrolę. To już jest za późno, po prostu trzeba zatrzymać go, zanim on dotrze do Twojej strony, więc może to zrobić firma hostingowa, ale bywa tak przy dużych atakach, że nawet ona nie jest odpowiednio wcześnie zatrzymać i musi jeszcze wyżej iść do operatora telekomunikacyjnego. Żeby na odpowiednim poziomie telekomunikacyjnym wprowadzić odpowiednie zmiany w ruchu sieciowym. Także jest pewien taki łańcuszek, który idzie w górę, więc przy tego typu atakach najczęściej, to jest taka sprawa, że trzeba po prostu szybciutko się skontaktować ze swoim operatorem, wyjaśnić to z nim. On albo będzie w stanie samodzielnie, to jakoś ogarnąć, albo jeszcze wyżej będzie musiał pójść do operatorów telekomunikacyjnych.

G.F: A złośliwe oprogramowanie rozumiem, że ktoś może nam zaimplementować złośliwe oprogramowanie, a nasza niezabezpieczona strona, czyli jakieś różne dodatki, które mają dziurę w całym, więc tu pewnie warto aktualizować i śledzić to. Z drugiej strony złośliwe oprogramowanie z poziomu nie wiem serwerowni, ktoś może tam jakoś nam zapakować, czy tylko najczęściej to jest z poziomu naszej strony? Właściwie też wiele z poziomu paneli do administracji serwerem i z poziomu przeglądarki, z poziomu FTPa, itd., więc tutaj się logujemy za pomocą loginu i hasła i mam nadzieje, że nie macie najbardziej popularnych loginów i haseł typu dupa123. No właśnie, jak to jest?

A.P: Generalnie jest pewna prawidłowość, najwięcej absolutnie ataków jest przez niezabezpieczone strony, przez strony nieaktualne, gdzie masz przestarzałe wtyczki, itd. To

jest absolutnie najwięcej tego typu incydentów. Na drugim miejscu dopiero są takie incydenty, które są z komputera użytkownika. Tzn. to są takie sytuacje, gdzie użytkownik np. ma swojego laptopa. Użytkownik z mojego punktu widzenia, czyli mam na myśli tego właściciela sklepu internetowego, mojego klienta. On po prostu ma, jakiegoś laptopa, nie dba tam o bezpieczeństwo, nie ma tam żadnego antywirusa, loguje się w otwartych sieciach Wi-Fi Internetu. Z takiego zbiorowiska loguje się np. niech będzie przez FTP na swój serwer, żeby umieścić na nim jakieś pliki, coś zrobić. No i niestety to zostaje podsłuchane, kiedy ta komunikacja nie jest w żaden sposób zabezpieczona, to ktoś ją może przechwycić i poznać taki login i hasło, albo tzw. keylogger, czyli urządzenie, które loguje wszystkie klawisze naciskane. Można w ten sposób przechwycić taki login i hasło i następnie wykorzystać, to do zalogowania się w celach, takich już złośliwych. To jest, jak najbardziej wykonalne, natomiast z naszego doświadczenia, to jest bardzo sytuacja już rzadka. W tych czasach, wciąż, jak najbardziej się zdarza, ale bez porównania, bo to infekcje przez strony internetowe królują, jakby u nas. Średnio strona jest atakowana w Polsce 6 tys. razy rocznie. Tyle przynajmniej my złapaliśmy ataków, bo może nie wszystkie łapiemy, więc może być tych ataków jeszcze więcej, ale to wystarczy, że jeden się powiedzie.

G.F: Bardziej mi chodzi, co znaczy 6 tys. rocznie?

A.P: Tyle łapiemy incydentów średnio, ta strona internetowa, takie WAFe i kolejne warstwy tych zabezpieczeń. Łapią nam 6 tys. incydentów ataków, czyli prócz np. złamania haseł, zalogowania się do kokpitu Twojego Wordpressa, np. prób instalacji złośliwego oprogramowania, czy wstrzyknięcia Ci spamu z chińskimi znakami. Suma różnych klas ataków. Od takich typu właśnie zaspamowanie chińskimi znakami, aż po takie poważniejsze, jak np. próba SQL injection, czyli zapytania, które wykorzystując luki w oprogramowaniu, wykonuje złośliwe kwerendy SQL-owe na bazie np., żeby zniszczyć tą bazę, albo skompromitować poufne dane, które w tej bazie się znajdują. Tutaj, to już różnego rodzaju to są ataki.

G.F: Czyli, podsumowując, czyli mamy 6 tys. prób.

A.P: Tak, to jest średnia, czyli może być powyżej średniej.

G.F: Ale, jeśli mówimy o stronie internetowej, inaczej sklepie, bo mamy różne poziomy, tak? Z jednej strony próbujemy się do backendu sklepu zalogować jako właściciel, czy tam administrator i to jest jedna rzecz i tutaj podwójna autoryzacja, czyli no.

A.P: Podwójna autentykacja jest, wszędzie, gdzie możemy róbmy tą podwójną autentykacje. Uważam, że to jest dzisiaj naprawdę bardzo skuteczna metoda chronienia się przed różnego rodzaju zagrożeniami, bo ona faktycznie nam pozwoli na to, że sam login i hasło nie wystarczą, musi być ten drugi czynnik, prawda? Poza hasłem, zazwyczaj jest to albo z Google Authentication, czyli z aplikacji taki specjalny kodzik. Czaszami to są inne rzeczy, może to być kod wysłany mailem, może być kod wysłany w SMS-ie, ale coś dodatkowego, jakby puszczone innym kanałem.

G.F: Do tego menedżer hasła, haseł. Tych menedżerów jest kilka i szczególnie, jak macie firmę, to są za darmo wersje i są płatne.

A.P: Są różne, to jest bardzo dobre rozwiązanie. Tak, ja polecam bardzo menedżery haseł, bo raz, że przechowują te hasła, a dwa, że one robią, coś takiego, że podpowiadają Ci trudne i złożone hasła, których jako człowiek byś sobie nie wymyślił po prostu, nie?

G.F: Tak i musisz zapamiętać jedno hasło, jak masz pracowników to takie menedżery pomagają przy współdzieleniu i wykrywaniu różnego niebezpieczeństw i to jest to. Natomiast, to co się zastanawiam i nad czym się zazwyczaj większość właścicieli sklepów nie orientuje i nie ogarnia, to jest to, że można sprawdzać, czy mam dobrą stronę, bo można zrobić tak, że jak ktoś wejdzie na serwer. Znaczy o to, co powiedziałeś, że wrzucenie tego, czyli musimy aktualizować mieć bezpiecznie. A z drugiej strony to, co ja się ten, są różnego rodzaju FTPy do logowania na serwery, tak?

A.P: No tak, ale bym powiedział, że te zagrożenia FTP-owe w moim przekonaniu z czasem będą coraz mniej ważne, bo my coraz mniej używamy tak po prostu klientów FTP ze swojego komputera w coraz mniejszym stopniu. Dlatego że po prostu nie instalujemy tak, jak kiedyś tego Wordpressa, wrzucając po FTP-ie, jakąś swoją paczkę tylko zazwyczaj korzystamy, z jakiegoś autoinstalatora już na serwerze, albo sobie trzymamy, gdzieś w jakich repozytoriach serwerowych. Jest troszkę mniej tej komunikacji moim zdaniem, niż kiedyś pomiędzy laptopami użytkowników, czy komputerami użytkowników, a serwerami. Wspomniałeś jeszcze o aktualizacjach, chciałbym tutaj jeszcze uzupełnić, bo to jest mega ważne, co wspomniałeś, żeby pamiętać, że wszystkie wersje były aktualne. Natomiast tu jest ważne, co to znaczy aktualna wersja. Teraz, jak się logujesz do Wordpressa, to tam widzisz takie warningi, że jakieś komponenty są nieaktualne. Np., że motyw jest nieaktualny, albo jakaś wtyczka jest nieaktualna i możesz sobie to zaktualizować. To jest bardzo dobry mechanizm, natomiast, kiedy to się pojawi i warto zaktualizować? Wtedy, kiedy ta nowa wersja wyszła, to

wtedy można to zaktualizować. A teraz wyobraź sobie tą sytuację, że korzystasz, z jakiejś wtyczki napisanej 7 lat temu i od 7 lat nie wyszła żadna aktualizacja. Wtedy Wordpress Ci nie wyświetli „zaktualizuj do najnowszej wersji", bo po prostu nie ma nowszej wersji. Nie masz wtedy, do czego tego zaktualizować. Ważne, żeby myśląc o aktualności oprogramowania bazować nie tylko na tym, czy Ty widzisz przycisk aktualizuj, ale również na to, czy nie masz zbyt starych komponentów np. zbyt starych wtyczek, które zostały porzucone przez swoich deweloperów i nikt do nich nie wydaje nowszych wersji. Tak też może być, dlatego pamiętaj nie tylko o tym, czy jest przycisk do zaktualizowania, ale pamiętajmy też o tym z kiedy pochodzą dane komponenty, bo może się okazać, że to, że nie widzimy przycisku oznacza tylko tyle, że nie ma aktualizacji, ale to wcale nie znaczy, że mamy wersję bezpieczną. Także warto na to również uwagę zwracać.

G.F: Trochę tego jest. Mam nadzieję, że słuchacze wzięli sobie coś fajnego dla siebie. Powiedz mi Artur, czy coś jeszcze na koniec byś dodał?

A.P: Wszystkie zagrożenia informatyczne są do opanowania, tylko po prostu poświęcajmy czas, a w zasadzie lepsze słowo inwestujmy swój czas w to, żeby zdobywać troszkę więcej wiedzy na temat tego bezpieczeństwa, bo łatwo o tym zapominamy. To, co powiedziałem na wstępie, łatwo o tym zapominamy, myśląc tylko o sprzedaży, o marketingu, czy obsłudze klienta, a jednak kiedy prowadzisz sklep internetowy, kiedy prowadzisz e-commerce, to po prostu jest to ważne. Jest to ważne, bo jesteś narażona bądź narażony w stopniu ponadprzeciętnym, umówmy się e-commerce, to atrakcyjne cele. Jako przedsiębiorca masz więcej kasy, niż przeciętna osoba, więc powiedzmy zapłacisz większy okup, a po drugie jest Cię po, co atakować, bo masz cenne dane. Czyli jest Ci, co ukraść, albo coś Ci zniszczyć. Sklepy internetowe są ponadprzeciętnie atrakcyjnymi celami dla atakujących i dlatego moim zdaniem właściciele też ponadprzeciętnie powinni podchodzić do spraw związanych z bezpieczeństwem.

G.F: Tak, warto o tym pamiętać i zwrócić uwagę. Ja mam taką patologię i wymuszamy na naszych klientach przesyłanie hasła, cały proces, jak to robić. Nie będę go tu podawał, bo jedno z ochrony to jest tajność procesu, a nie mówimy o nim, jak wygląda. Natomiast wysyłanie haseł i loginów w e-mailu nie jest najlepszą rzeczą. Z drugiej strony czasem warto przejrzeć te hasła i loginy, które są i je usunąć zbędne. A do tych aktualnych np. zmienić hasła dla wszelkiego bezpieczeństwa, bo przecież ludzie się zmieniają, różne rzeczy się dzieją. A też to trudno ogarnąć i tutaj pomagają menedżerowie haseł, gdzie można sobie ustawić, które hasła, kiedy mają się zmieniać. A jest w tym wyzwanie, tak,

ale też to ułatwia, bo jeśli mamy menadżera hasła, to możecie łatwiej obserwować, kiedy zostało zmienione hasło, jak było zmienione, całe raporty można sobie robić i tutaj parę rzeczy jest. Dobra! Artur wielkie dzięki za podzielenie się Twoim doświadczeniem.

A,P: Dzięki wielkie!

G.F: Czego Ci życzyć na końcu? Oprócz trochę chłodu, bo dzisiaj 35 stopni.

A.P: A wszyscy sobie życzmy po prostu bezpiecznego Internetu.

G.F: Bezpiecznego Internetu. Do usłyszenia w takim razie drodzy.

A.P: Dzięki i do usłyszenia! Cześć!

To już koniec! Jakie masz przemyślenia na temat bezpieczeństwa? Coś zrobisz, coś nie zrobisz? Polecam, jednak wypisać sobie plan działań na najbliższy miesiąc-dwa, żeby pewne rzeczy sobie zabezpieczyć, a materiały, linki i transkrypt na stronie convertis.pl/numer odcinka. A ja ponownie zapraszam do zapisu na nasz newsletter z ciekawymi newsami z całego świata convertis.pl/newsletter, a tymczasem do usłyszenia. Do zobaczenia! Cześć!