62. Włamania - Ataki hakerskie na PrestaShop - studium przypadku

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! Z tej strony Grzegorz Frątczak szef Convertis. Dziś odcinek specjalny, który jest ważny dla każdego właściciela sklepu, e-commerce menagera, ale także programisty pracującego na Prestach. Dlaczego? Bo nagranie poświęcone jest bezpieczeństwu, a właściwie niebezpieczeństwu. Czyli włamaniu hackerów na sklepy internetowe. Opowiemy w tym odcinku o trzech włamach u naszych trzech klientów, które odbyły się w lipcu i sierpniu 2022 roku sklepach zbudowanych na PrestaShop. Jest to związane ze znalezieniem przez PrestaShop pewnej podatności samego PrestaShop, które powodowały takie możliwości i te dziury zostały już załatane przez PrestaShop. Natomiast zdarzyły się, nie były to może jakieś wielkie włamy. Natomiast warto o tym mówić, że warto zabezpieczyć swój sklep i korzystać ze wsparcia oraz mieć to na uwadze, bo konsekwencje mogą być duże. Dzisiaj do odcinka zaprosiłem programistę Pawła, który zajmował się tymi włamami, a także koordynatora Piotra, który zajmował się jednym z klientów i dzisiaj w trójkę opowiemy Wam o tych trzech włamach do sklepów, o konsekwencjach dla sklepów i o tym, co z tym można w ogóle zrobić. Czy jest w ogóle czego się bać, a jest. Jak takie rzeczy my ogarniamy, jak wy możecie to ogarniać. Co w ogóle powinno być alarmujące dla Was, że coś takiego się dzieje w waszym sklepie, bo to nie jest takie hop-siup, że od razu widzimy włam na naszych sklepach. To trochę, jak z tym oprogramowaniem Pegasus, gdzie większość osób nie wiedziała, że ma takie oprogramowanie u siebie. A do tego na końcu damy trochę wskazówek i jak przed tym się bronić. Ta rozmowa jest tak trochę na gorąco, bo ciągle pracujemy nad procesem, który ma w razie czego lepiej wspierać naszych klientów. A mój własny, osobisty plan jest taki, by tym procesem dzielić się z Wami na bieżąco, więc udostępniamy pliki, które są ciągle aktualizowane i poprawiane, bo współpracujemy z różnymi specjalistami, z

właścicielami, ale też i z konkurencją trochę nad tym, żeby taki proces budować i chce żeby te rzeczy były dla Was udostępnione za darmo. Żebyście mogli sobie z tym poradzić. Wszystkie szczegóły znajdziecie w opisie odcinka, a teraz zapraszam Was do posłuchania tej rozmowy i do komentowania. Jeśli znajdziecie jakieś dziury w całym, to zapraszam powiedzcie nam o tym, bo nie jesteśmy idealni. Zdarzają się różne rzeczy, jeśli chcecie nam pomóc to rozpropagujcie ten odcinek. Znaczy pomagacie nie tylko nam, ale też wszystkim właścicielom, bo trzeba o takich rzeczach mówić głośno, żeby każdy właściciel sklepu opartego o PrestaShop, jak najszybciej zaktualizował te sklepy, więc dajcie nam znać, co o tym myślicie i dzielcie się tym. Zapraszam do słuchania!

Grzegorz Frątczak: Dzień dobry! Witam wszystkich!

Paweł Kryst: Cześć!

Piotr Trojanowski: Cześć! Witam!

G.F: Cześć! Dzisiejszy odcinek jest specjalny, bo niedawno został odkryty dość poważny i krytyczny problem w PrestaShop. Wyjątek związany z bezpieczeństwem. Dzisiaj właśnie porozmawiamy, co się z tym działo, dzieje i co warto zrobić i co my jako Convertis zrobiliśmy w ramach naszej współdziałalności i dlatego zaprosiłem ludzi kompetentnych z zespołu Convertisa, czyli najważniejsza osoba bym powiedział – Paweł, który jest u nas cenionym programistą. Paweł powiedz coś o sobie krótko.

P.K: Ja jestem programistą PHP i specjalizuje się w obsłudze sklepów PrestaShop i programuję już od kilkudziesięciu lat, więc trochę już.

G.F: Ilu lat?

P.K: No kilkudziesięciu już.

G.F: Dobra! W przypadku Pawła rzeczywiście to może być już kilkadziesiąt. Chociaż Paweł wygląda strasznie młodo. Nie wiem, czy powinienem komentować to ale okej. W każdym razie sam się zdziwiłem. Piotrek, a Ty powiedz coś o sobie.

P.T: W Convertis pracuje od 3 lat. Zajmuję się koordynowaniem prac programistycznych. Głównie ta praca polega na tym, że kontaktuję się z klientem, przyjmuję zlecone przez niego prace, przekazuję tę pracę programistom, planuję programistom harmonogram tych zadań i taka praca ogólnie bardzo ogarniająca wiele obszarów.

G.F: Tutaj Piotrek jest bardzo skromny dla siebie. Myślę, że to jest bardzo istotna rola, która powoduje zadowolenie klienta i sukcesy wszystkich prac, bo bez tego było by ciężko na styku pracy programistycznej i klient. No dobrze, to wiecie już drodzy słuchacze kim są nasi interlokutorzy. Tak to się chyba nazywa, czyli goście. No właśnie Paweł, bo Ty pewnie wiesz najlepiej. Co zostało 22 lipca ogłoszone przez PrestaShop, a ja chciałbym powiedzieć, że my to nagrywamy 8 sierpnia, więc trochę już czasu minęło.

P.K: Trzeba zacząć od tego, że nasiliły się, w jakimś ostatnim czasie ataki internetowe. Poszukiwano dziury i analizowano różne przypadki. Skąd się to bierze i stwierdzono, że faktycznie jest luka bezpieczeństwa, która wiąże się z modułem listy i troszkę z takimi elementami core'a i wydano łatkę, która ma to zabezpieczyć i temu przeciwdziałać.

G.F: No właśnie i myślisz, że z tej komunikacji, która została wydana przez PrestaShop. To taki programista, jak i właściciel jest sobie w stanie wszystko załatać, że jest to proste?

P.K: W tym wypadku raczej nie. Łatka jest wydana oficjalnie, więc programista jest w stanie to przeczytać, pobrać i zainstalować. Natomiast czy właściciel sklepu? No nie bardzo, nie bardzo. Tzn., jeżeli ma najnowszą wersję Presty i nie ma zbyt wielu modyfikacji i jest w stanie zrobić sobie automatyczną aktualizację Presty, to tak. Wystarczy zaktualizować Prestę 1.7 do najnowszej wersji, czyli tą, która zawiera odpowiednie poprawki i już.

G.F: No właśnie, bo z tego, co nas niestety spotkało, bo mieliśmy 3 przypadki, gdzie jeden klient już na początku lipca ok. 7 lipca został zaatakowany i musieliśmy łatać i działać. Później w połowie lipca dostaliśmy sklep, który gdzieś tam nas znalazł, i któremu pomagaliśmy. W sumie teraz na początku sierpnia trzeci sklep został zaatakowany, bo nie zdążyliśmy tych łatek załatać, bo to bardzo, bardzo skomplikowany sklep i żeby to dobrze działało musieliśmy to przetestować i w momencie, gdy już wszystko było gotowe do implementacji to się okazało, że sklep został zaatakowany na nieszczęście. No właśnie, bo tam zauważyliśmy 2 rodzaje takich ataków. Rodzaje w sumie przez jedną taką dziurę, ale dwa efekty. Czyli prośba o podanie danych kart kredytowych z poziomu koszyka. Było to bardzo hardcorowo zrobione i trochę głupio bym powiedział, bo cały ten formularz był taki zaimplementowany, w którymś tam kroku koszyka i pytania były po angielsku. A wszystkie sklepy są po polsku, więc większość ludzi powinna się zorientować, że coś jest nie tak. A w drugim przypadku było

takie hardcorowe przekierowanie ze sklepu na jakiś serwis „jak zarobić miliony", tak? Czy dolary wręcz po angielsku. Dobrze mówię Piotrek, bo to był Twój?

P.T: Tak jest.

G.F: Więc to było takie hardcorowe i z poziomu już wyszukiwarki i to od razu było przekierowane, pewnie, jak się wpisało domenę sklepu, to też pewnie było przekierowane, tak?

P.T: Tzn., w momencie, kiedy wpisywało się domenę sklepu bezpośrednio w pasek adresu, to nie było żadnego przekierowania wewnątrz sklepu, można było normalnie się przeklikać. Było też jakieś działanie, które powodowało, że jednak ten sklep nie działał poprawnie, bo podczas klikania, dodania produktu do koszyka coś mieliło, w jakiś sposób. W każdym razie wewnątrz sklepu można było się przeklikać, ale wchodząc z wyniku wyszukiwania Google, bądź Bing lub innych wyszukiwarek od razu było przekierowanie na jakąś taką stronę. Nie będziemy podawać adresu tej strony, bo może na tej stronie są jakieś wirusy. Natomiast najprawdopodobniej była to strona o bardzo niskiej jakości pod względem SEO. Tutaj mam taką hipotezę, że ten atak był głównie pod depozycjonowanie tej strony. Myślę, że właśnie ci hackerzy mieli taki zamysł. Dlatego że po kilku godzinach tych przekierowań tzn. na dobrą sprawę nie wiem, jak długo to trwało. Po godzinie, jak się o tym dowiedzieliśmy to zaczęliśmy wdrażać już, jakieś działania. W każdym razie Google zaczął przeindeksowywać powoli strony właściciela sklepu na ten adres. W sensie zaczął wyindeksowywać może te strony, które dotyczyły tego sklepu, więc bardzo prawdopodobne jest to, że cel działania był właśnie taki, żeby ten sklep zdepozycjonować.

G.F: To jest bardzo ciekawe, że jeśli jesteś właścicielem sklepu to zazwyczaj spisujesz adres z ręki i wpadasz do sklepu, więc tutaj możesz testować. Rzadko kiedy wpisuje się i wyszukuje sklep z poziomu wyszukiwarki.

P.T: Dokładnie i to dlatego to mogłoby zrobione w taki sposób, żeby to ukryć. Przed właścicielem tego sklepu, a tylko użytkownicy, którzy z zewnątrz wchodzą, bądź Google, roboty Google widziały, że tego typu działanie jest podjęte. To, co odkryliśmy to może przy okazji powiem, jak już jestem tutaj przy głosie. Polegało to na tym, że został wstrzyknięty złośliwy kod w głównym pliku index PHP, który nie wiem czy tutaj profesjonalnie powiem w każdym razie dodawał na froncie GS, który był tak skonstruowany, że przekierowywał tylko strony pochodzące z Google, Bing, MSN jeszcze. Także, na jakąkolwiek stronę się nie trafiło

to po prostu. Każda strona, czy to strona główna, czy strona jakiejś kategorii była przekierowywana na tą stronę, taką brzydką, że tak powiem.

G.F: I to był nasz trzeci najpóźniejszy z sierpnia i rozumiem, że zorientowaliśmy się, bo ktoś zobaczył, że strona działa nie, tak jak potrzeba, prawda? Jak się klikało w środku sklepu to, to nie działało dobrze, tak? Dobrze mówię Piotrek?

P.T: Tzn., no wewnątrz sklepu można było się przeklikiwać. A problem przypadkowo został odkryty ten problem.

G.F: Pomimo tego, że już się przygotowaliśmy do łatania tej dziury i się okazało, że już jest. To był jeszcze chyba poniedziałek po południu, gdzie klient zadzwonił i powiedział „Hej! Chyba jest problem.", tak?

P.T: Dokładnie, dlatego ja wiem, że zaraz na koniec tej rozmowy, jakieś wnioski podejmiemy. Natomiast nie wiem na ile słuchacz dotrwa do końca. Myślę, że tutaj taką dobrą nauką jest to, żeby wszelkich poprawek bezpieczeństwa po prostu nie testować, zwyczajnie na kopii, bo choćby na produkcji wywali się front na godzinę i zaraz to załatamy, gdzieś tam, w jakiś sposób poprawimy. Niż wdrażać poprawki na sklep deweloperski, później testować sprawdzać, czy aby na pewno wszystko fajnie wygląda i wszystko fajnie chodzi. Dopiero później, jak już jesteśmy pewni to wdrażać zmianę na sklep produkcyjny. Tutaj z tej perspektywy właśnie tak chcieliśmy to zrobić bezpiecznie, fajnie. Okazało się, że nie ma na to czasu. Po prostu trzeba wdrażać od razu. Lepiej później w locie poprawić, jakiś błąd ewentualny przez naniesienie tych poprawek, niż później ratować ten sklep, tak jak my ratowaliśmy, co kosztowało nas bardzo dużo wszystkiego. Nie tylko czasu, ale stresu, glukozy, no nie wiem. Później pewnie jeszcze trochę o tym pogadamy.

G.F: No właśnie, to był ten trzeci przypadek. Natomiast tutaj widzicie, że był problem z pozycjonowaniem samego sklepu, które utraciło swoją, jakąś wartość. Później na szczęście odzyskało to, ale to inna już historia. Pierwszy przypadek, to było to, że próbowali wykraść numery kart kredytowych, czy debetowych klienta. Tak trochę hardcorowo, bo cały formularz był wstrzyknięty, że to było po angielsku i to było widać, że coś tam jest nie tak. No i drugi przypadek, to chyba to samo było, że próba wykradzenia numerów kart kredytowych, tak? Dobrze mówię?

P.T: Tak, drugi przypadek, to też był ten sam, jakby skutek. Czyli na formularzu zamówienia taki wklejony, nie adekwatny do reszty strony formularz do wpisania karty kredytowej. Ja

może tutaj jeszcze troszkę rozszerzę, bo tak jakby zaczęliśmy od tego, że PrestaShop wydała łatkę i można to załatać, zrobić aktualizację najnowszej wersji i mamy temat, jakby zamknięty. A to nie do końca tak jest. Musimy mieć świadomość, że to, co wykryto, to dotyczy Presty 1.7. W wersjach 1.7 w określonym przedziale. Muszę sobie przeczytać oraz modułu whitelisty. Natomiast prawda jest taka, że tak naprawdę należałoby robić sobie takie audyty i my to zleciliśmy dla każdego naszego klienta. Takie audyty bezpieczeństwa, ponieważ sklep internetowy nie jest takim jednolitym programem, który się kupuje w pudełeczku, jest zamknięty hermetycznie i tam jest jakiś monolit. Tylko to jest zestaw, jakichś elementów. To jest PrestaShop, w jakiejś wersji, jakieś modyfikacje, jakieś moduły i takie włamanie bardzo rzadko wykorzystuje, jakąś jedną lukę, a najczęściej wykorzystuje kilka, jakichś podatności. Musi być zbieg okoliczności, że akurat w danym sklepie hacker ma te 2 lub 3 różne elementy. Tutaj w przypadku tego, co akurat zostało oficjalnie ogłoszone, to byłą faktycznie drobna taka nieścisłość w core'rze i ewidentne zaniedbanie w module whitelisty. Ale pierwszy przypadek, który mieliśmy włamania jeszcze zanim w ogóle Presta odkryła te ruchy, to był w Preście 1.6. U klienta, który miał ostatnią wersję 1.6., która została wypuszczona, czyli taką, która już była z wszystkimi poprawkami bezpieczeństwa, a mimo to ktoś się włamał. My jako programiści po tej dobrej stronie, którzy robimy coś ze sklepem, to jest taka walka dobra ze złem. My jesteśmy po tej dobrej stronie, to zawsze na słabszej pozycji jesteśmy, bo nie myślimy mentalnie, tak jak Ci włamywacze źli. Jest nam ciężko znaleźć, jak następuje taki włam „dobrze, ale jak oni to zrobili?" „Jak oni się włamali?" Jeśli chodzi o ten pierwszy przypadek nie wiemy do dzisiaj. Nie wiemy do dzisiaj, ani modułu whitelisty nie było, ani nie jest to Presta 1.7. Przeanalizowaliśmy listę modułów, które tam są, sprawdziliśmy i 2 potencjalne miejsca znaleźliśmy, gdzie może coś udałoby się wgrać, ale też nie do końca jesteśmy pewni. Trzeba pamiętać, że włamanie do sklepu może nastąpić z zupełnie prozaicznego wektora spoza PrestyShop. Najprościej jest włamać się na skrzynkę pocztową klienta, albo gdzieś zdobyć jego hasło do backendu. Wtedy niezależnie, jak mamy dobrze zabezpieczony sklep, to hacker może zalogować się do backendu Presty jako administrator dograć swój własny moduł hackerski za pomocą, którego może już zrobić wszystko w sklepie.

G.F: Właśnie i o tym, jak zabezpieczać sklep jeszcze będziemy mówić. Tutaj będziemy opowiadać, co się nam zdarzyło. Natomiast, to też trzeba zauważyć, że to jest chyba pierwsza taka znacząca dziura, która została znaleziona w Preście. W sumie, z którą my od 5 lat mieliśmy do czynienia, gdzie był taki kryzys bezpieczeństwa, tak? PrestaShop

jako firma zareagowała dość szybko i usilnie chciała to naprawić. Myślę, że to jej zajęło z tydzień, może 2. Trudno mi powiedzieć, bo rozmawiałem z ludźmi i ten pierwszy nasz przypadek, był jednym z pierwszych i rzeczywiście, to ciężko znaleźć, bo Paweł nie wspomniał, ale z tego, co wspomniał poza tym nagraniem tych plików, które mogą być zaatakowane jest ok. 1000. Dobrze mówię Paweł? Czy ja tutaj coś przekręcam?

P.K: No tak, tak, tak, tak. Presta jest oprogramowaniem PHP, który ma kilkadziesiąt tysięcy plików PHP, a w tym są miliony linijek kodu, więc ciężko czasami coś znaleźć. My jeżeli robimy wdrożenie, to instalujemy nową wersję Presty, instalujemy, jakieś standardowe moduły, jakieś swoje moduły mniej, więcej wiemy, co tam jest. Natomiast większość klientów przychodzi do nas już, z jakimś bagażem, tak? Z jakąś starszą wersją Presty, z ilomaś modyfikacjami, które były robione z jakimiś modułami od różnych dostawców i ciężko jest ogarnąć to wszystko.

G.F: Właściwie, to co jest ważne tutaj przy tych sklepach PrestaShop, bo ja mam takie przemyślenia, taką hipotezę, że raczej wątpliwe, żeby ktoś chciał Was bezpośrednio zaatakować jako Prestę, bo znalezienie dziury w całym to jest od groma pracy. To tak jak my musielibyśmy poświęcić dziesiątki, setki, a nawet tysiące godzin, żeby załatać wszystkie dziury i szukać dziury w całym, to byłoby bardzo ciężkie. Tak samo włamywacz musi poświęcić bardzo dużo czasu, żeby znaleźć i pokombinować, jak można tu znaleźć dziurę w całym i później zacząć atak. Natomiast większość sklepów na PrestaShop to są małe sklepy, które mają tam mniejszy, większy obrót i nie opłaca się po prostu włamywaczom atakować poszczególnych sklepów. Natomiast, gdy już mamy przepis, to możemy zrobić sobie skrypt, gdzie będziemy sprawdzać podatność tych kilkudziesięciu tysięcy sklepów na tą dziurę i to już się opłaca. Z tego powodu, jak już PrestaShop…

P.T: Ja się z Tobą troszkę nie zgodzę.

G.F: Tak? O patrz.

P.T: Dlatego że ciężko nam jest znaleźć tą furtkę, w którą hacker wszedł. Natomiast możemy złapać miejsca, które zmodyfikował i sposób, w jaki modyfikował i np. w tych sklepach to nie był tylko taki efekt, że był formularz na stronie zamówienia, to był jeden z efektów, taki widoczny. Natomiast jeszcze w kilku miejscach w kodzie były takie furtki, które umożliwiały np. wykorzystanie sklepu jako takiej branki do innych ataków. Czyli to, czy masz dużą sprzedaż, czy nie, to nie ma znaczenia. Jeżeli były skanowane, a było to widać po rogach, że

były skanowane adresy URL, a różne dziury pomimo tego, że to była Presta, to były skanowane adresy charakterystyczne dla Wordpressa też. W 2-3 miejscach były takie bramki, które umożliwiały przysyłanie kodu, z jakiegoś serwera poprzez ten nasz sklep do innego serwera. No nie jesteśmy w stanie stwierdzić, co tam było przesyłane, bo to wszystko tak, czy siak było szyfrowane, ale to już było takie gubienie śladu, wykorzystanie tylko i wyłącznie jako bramki pośredniczącej.

G.F: Tutaj właśnie o tym mówię, że to też, bo jakby chodziło mi o to, że w takiej skali skanuje się wszystkie sklepy, bo bazę sklepów można znaleźć na PrestaShop, w Internecie, albo zrobić crawlera, który to przeskanuje cały Internet i znajdzie te kilkadziesiąt tysięcy sklepów. Po prostu sprawdzić, który jest podatny, a potem mu odpowiednie rzeczy wstrzykiwać. Nie tylko te rzeczy, które tu powiedzieliśmy w tych 3 przypadkach, ale też zrobić ze sklepów pośrednika do kolejnych włamów na kolejne sklepy, do gubienia tutaj śladu, więc moja hipoteza jest tak, że jeśli PrestaShop opublikował już przepis na to, gdzie jest dziura. To nie tylko tacy zawodowi hackerzy się tym zajmują, ale też i domorośli, którzy dostali przepis i posprawdzają. Z tego powodu według mnie, to jest bardzo istotne, żeby to ponaprawiać i z tego powodu tutaj, to robimy. Nagrywamy ten odcinek, żeby Wam opowiedzieć, co może Wam się zdarzyć. Jak warto z tym działać? Jakie są konsekwencje? A też chcemy Wam dać przepis dla Was lub dla Waszych programistów, żeby to ogarnęli. My niestety nie jesteśmy w stanie wszystkim sklepom pomóc osobiście, tu przez firmę, bo mamy ograniczone zasoby. Natomiast chcemy to tworzyć i dać Wam jako przepis do sprawdzenia i następnie poprawy tego wszystkiego przez Waszych programistów. Jeśli ktoś znajdzie dziurę i będzie trzeba jeszcze coś dodać, odjąć, to po prostu dajcie znaka, to poprawimy. No, ale tylko chciałem zaznaczyć, że PrestaShop to jest tysiące plików wykonywalnych, które mogą mieć w dowolnym miejscu dziurę. Nie wiadomo, gdzie jest. To też nie jest oprogramowanie bankowe, gdzie miliony, czy dziesiątki milionów się wydaje na przetestowanie jednej funkcjonalności, żeby tylko nie ukradli pieniędzy z banku, a zobaczcie, że tak się zdarza. No właśnie, więc tutaj to jest tego rodzaju sprawa. No i co chciałem jeszcze powiedzieć, że nie należy, mówiąc brzydko „srać w gacie”, bo to się pierwszy raz zdarzyło, jak się zabezpieczy i przypilnuje, to będzie dobrze. Tutaj też mieliśmy w przypadku drugim takiego zonka, że sam serwer był źle zabezpieczony. Tam w ogóle była mała katastrofa, prawda? Paweł, jak to tam było z tym serwerem?

P.K: Drugi przypadek to też był o tyle ciekawy, że to nie nasz klient, tylko trwały dopiero potencjalne rozmowy z tym klientem i klient nie był świadomy, że ma włamanie. Tylko w rozmowie z handlowcem stwierdził, że ma takie problemy ze sklepem, że co jakiś czas mu się jakiś skrypt na stronie wykonuje, on sobie ten skrypt kasuje i potem przez jakiś czas jest spokój. A potem znowu mu się to uruchamia i handlowiec tak troszkę otworzył oczy i handlowiec przekazał to do naszego działu do koordynatora, koordynator do programisty i to chyba nawet do mnie trafiło. Ja mówię „hej, ale to takie nie naturalne, to wygląda na włamanie". No i ten klient się zdecydował wykupić u nas taką kontrolę tego i faktycznie, faktycznie okazało się, że ma. Nie był nawet świadomy. Prawdopodobnie od 2-3 miesięcy już miał to włamanie i nie był tego świadomy. Tak faktycznie, faktycznie serwery są różne i bywa tak, że no może być ewidentna dziura, jakaś podatność, w którymś miejscu kodu, a może być tak, że serwer jest niewłaściwie zabezpieczony i to też się zdarza.

G.F: A co znaczy, że serwer jest źle zabezpieczony?

P.K: Może umożliwiać np. wgranie plików na serwer w nieodpowiednie katalogi i uruchomienie ich. Zazwyczaj, jeżeli mamy pliki PHP one nie powinny być uruchamiane z zewnątrz poza takimi wyjątkami konkretnymi, które pozwalają na działanie sklepu i wszystkie inne nie powinny się dać uruchomić, tak? Natomiast zdarza się, że czasami są takie luki, czy zabezpieczenia, że np. uprawnienia do plików są takie, że wszyscy mogą zapisywać, że można wgrać plik, że można uruchomić go z zewnątrz. Zdarza się.

G.F: Więc dlatego warto mieć dobrą serwerownię i dobrego serwer admina, który to dobrze poustawia.

P.K: Tak, tak.

G.F: A później ktoś najlepiej jeszcze skontroluje, bo to są błędy ludzkie i na po prostu się zdarza, tak?

P.K: Tak, tak jak już mówiłem nie jest to jedna przyczyna takiego włamania, tylko jest kilka przyczyn. Może być tak, że jest jakaś drobna podatność, w jakimś pliku, gdzieś w jakimś module, ale przez to, że reszta systemu jest dobrze przygotowana, że jest dobrze zabezpieczona, to hacker nie ma możliwości wykorzystania tego. A jeżeli jest kilka takich podatności, to może zrobić, co chce.

G.F: No właśnie. Tutaj takie tło chciałem drodzy chciałem Wam opowiedzieć, jak to wygląda. Natomiast chciałem też opowiedzieć o tym Wam, jak wygląda ogarnianie

takich ataków, jeśli już wiemy o tym. Przynajmniej z naszej perspektywy. O tym opowiemy, opowiemy o tych trzech przypadkach, jak to zaszło, co się stało, ile to wymagało działań. Jakie są te nasze wnioski i jak należy to zabezpieczać, żeby to dobrze działało. Paweł, to powiedz mi, jak wyglądał ten przypadek pierwszy, bo to chyba śmieszne było trochę, albo nie śmieszne. Tragiczne w swoich konsekwencjach.

P.K: No tak, tak. Dla nas może teraz zabawne z perspektywy czasu.

G.F: No, a klient no miał ciężkie chwile i to naprawdę bardzo ciężkie.

P.K: Tak, tak. Przypadek był taki, że akurat poprzedniego dnia nasz kolega wprowadzał na sklep modyfikacje. Wprowadził zmiany, sprawdził, przetestował. Wszystko było okej. To było jakoś tak na koniec dnia, a następnego dnia klient dzwonił, że jest awaria. Wyświetla mu się ten formularz na stronie zamówienia i zepsuliśmy mu sklep. Takie było zgłoszenie, więc troszkę awaryjne i nerwowe. Koordynator odebrał telefon przyjął temat i przekierował sprawę do mnie, ale bardzo szybko okazało się, że jest to włamanie, a nie nasza wina. A dlaczego akurat taki zbieg okoliczności? Dlatego że klient miał wyłączoną kontrolę aktualizacji plików, co powoduje, że te modyfikacje, które wrzucał hacker mogły zostać wgrane na serwer dużo wcześniej. Tylko one nie zadziałały, dlatego że cache nie został zaktualizowany. A dopiero w momencie, kiedy nasz kolega wprowadził modyfikacje na sklep i zresetował manualnie ten cache po to, żeby odświeżyć wszystko, to te modyfikacje zaczęły działać. Bardzo możliwe, że ten kod złośliwy już był wstrzyknięty kiedyś i hacker po prostu porzucił tą swoją instalację, bo stwierdził, że nie działa.

G.F: Czemu nie wiemy, kiedy hacker wrzucił te pliki?

P.K: No, bo był na tyle sprytny i przebiegły, że zatarł ślady. Daty modyfikacji plików są wsteczne. Mamy już w plikach złośliwy kod, który wiemy, że jest złośliwy, że coś robi. Natomiast ten kod sam w sobie też jest odpowiednio tak zmanipulowany, aby był trudny do wykrycia przez programy antywirusowe, a sposób łamania i komunikacji z serwerem jest taki, żeby trudno było to wyłapać w logach. Takie zapytania, które przychodzą na serwer są zapytaniami post, także nie widać parametrów, a jeśli są parametry, to są zakodowane. Albo są tak sformułowane, że parametry symulują, takie typowe parametry, które sklep używa np. ID produktu. Także ciężko jest określić, że akurat dane zapytanie jest zapytaniem hackerskim. A przychodzą z różnych serwerów, bo inne serwery wykorzystują jako bramki, więc mogą przychodzić zapytania z różnych serwerów. Jakby tutaj wykraczamy, analiza tego, w jaki sposób hacker się dostał, jakby wykracza poza nasze kompetencje, tak? My serwisujemy

sklep, ta sprawa została przekazana do administratora serwera, żeby sprawdził, czy są jakieś ślady na firewalle, w logach. No niestety nic nie znalazł, poza już efektami.

G.F: Trzeba też zwrócić uwagę, że logi nie są trzymane dłużej, niż ile Paweł?

P.K: To też zależy od serwera czasami to jest tydzień, czasami miesiąc.

G.F: Tak, więc trudno to określić, tak? Jeszcze nie wszystko jest logowane, więc to też trzeba wziąć pod uwagę.

P.K: Tak.

G.F: Okej, czyli po prostu był telefon od klienta. Wykryliśmy, że to nie błąd programisty z dnia poprzedniego tylko włam i zaczęliśmy szybko działać, tak?

P.K: Tak, tak. Tak po prostu usunęliśmy złośliwy kod i sklep działał właściwie nieprzerwanie, po tym fakcie. Natomiast dalej zgłosiliśmy sytuację z jednej strony do klienta, z drugiej do administratora, że trzeba podjąć odpowiednie działania, tak? Jeżeli ktoś już miał dostęp do sklepu, to trzeba pozmieniać wszystkie hasła, trzeba sprawdzić, czy nie ma jeszcze, jakichś wstrzyknięć w bazie danych i no cóż tu dużo mówić, tak jak mówiłem hacker mógł wejść przez np. jakieś konto pracownika, tak? Trzeba wszystkie hasła zmienić, wszyscy pracownicy firmy muszą sprawdzić sobie programami antywirusowymi, czy przypadkiem nie mają złośliwego oprogramowania na swoich telefonach, na swoich komputerach, które by np. przechwytywało hasła, czy komunikację pośrednią.

G.F: tak, tak jak Paweł wcześniej mówił nie byliśmy w stanie 100% pewnością stwierdzić skąd te włamy były. Nie udało się tego określić, a analiza tej Presty, która notabene jest 1.6, czyli nie najnowsza wersja. Znaleźliśmy 2 potencjalne dodatki, które mogły to powodować, ale no to nie daje gwarancji, więc teraz najważniejsze było zabezpieczenie odpowiednio Presty i tak poustawiane, że w razie zmian klient zostanie poinformowany, że kod został zmieniony i trzeba coś zrobić, bo źródła nie znaleźliśmy, tak? A szukanie źródła i dziury w całym to trochę, jak szukanie igły w stogu siana, tak? Jak to się mówi po polsku. Dużo to zajęło, te wszystkie analizy? Długo to trwało później te wszystkie prace?

P.K: No z mojej strony to kilka godzin. Takie wyczyszczenie sklepu, ale potem jeszcze analizowaliśmy. Troszkę zajęło nam wyszukiwanie właśnie tej przyczyny i dziury, tak? Analiza logów, analiza bazy danych. Także przypuszczam, że tam kilkanaście, kilkadziesiąt godzin zeszło.

G.F: Tak, więc klient miał takie szczęście, że miał tego cache'a i te zmiany nie były widoczne i zostały znalezione i szybko usunięte, bo jego klienci nie zostali skazani na skradzenie tych kart, tak? Tutaj mówimy o tym, że to było tak kiepsko przetłumaczone i to też się działo w nocy i rano naprawia, więc to działo się szybko. A drugi przypadek? Bo to też Paweł Ty robiłeś. To jest ten nasz klient, który przez przypadek przez handlowca został wykryty, że coś tam dziwnego się dzieje.

P.K: Jeszcze nie był naszym klientem, więc to nam zajęło trochę więcej czasu. Jeżeli już ktoś jest naszym klientem, to mamy całą komunikację już ustaloną, tak? Mamy dostęp do serwera, mamy hasła, możemy szybko zadziałać. Tutaj trzeba było najpierw to wszystko zdobyć, skonfigurować, połączyć i zweryfikować. Także akcja trwała trochę dłużej. Tu jest o tyle problem, że klient ma 4 sklepy. 3, czy 4, więc stwierdziliśmy faktycznie włamanie i złośliwy kod w jednym. U niego to już działało przez długi czas. Klient ten kod sobie usuwał, gdy był wstrzykiwany, ale nie wiedział, że w kodzie PHP są jeszcze inne kody złośliwe, które ten kod złośliwy wstrzykują, więc to funkcjonowało przez dłuższy czas, więc kiedy stwierdziliśmy, że faktycznie jest włamanie. Zrobiliśmy z tego raport, wypisaliśmy wszystkie miejsca, w które coś zostało wstrzyknięte i po prostu zaleciliśmy zamknięcie serwera dlatego że było takie zagrożenie, że jeśli naprawimy to w jednym sklepie, to nie zdążymy naprawić w drugim i trzecim, a hacker się zorientuje i zrobi coś gorszego. Tak zostało zrealizowane z tym, że ponieważ nie jesteśmy taką firmą, która działa jak pogotowie ratunkowe, że ktoś do nas dzwoni, a my zrywamy się, bo czekamy w pogotowiu i realizujemy od razu. Mamy jakieś swoje plany, mamy zadania, które realizujemy. Mamy zobowiązania wobec innych klientów, więc w tym momencie nam się trochę przeciągnęło. Ta realizacja i klient stwierdził, bo w tym samym czasie podjęliśmy się łatania i audytów u wszystkich naszych klientów, których już mamy już na abonamencie, więc stwierdził, że sam sobie za pomocą swoich administratorów i służb te sklepy połata.

G.F: Mhm, no i później trzeci przypadek, który już stał się chyba 1 sierpnia. Gdzie tutaj Piotrek trochę tu opowiadał. Piotrek, a jak tam to wyglądało? Akcja-Reakcja

P.T: To może tak od początku, w jakich okolicznościach dowiedziałem się w ogóle o tym. To był moment, kiedy u nas już większość programistów już kończyła pracę. Również ja też kończyłem swoją pracę. Żona z dziećmi podjechała po mnie i w samochodzie okazuje się, że dzwoni klient i mówi, że ma, jakieś podejrzane zachowanie na stronie. Tutaj przypomnę, że to była ta akcja z tym, że następowało przekierowanie z wyniku wyszukiwania na tą stronę słabej jakości. W momencie, kiedy dowiedziałem się o tym szybko chciałem się

skontaktować z Pawłem. Niestety do Pawła zadzwoniłem, to okazało się, że on nie może podjąć działania, bo już ma coś umówione, coś pilnego do zrobienia, więc było trochę stresów, ale okazało się, że jeszcze jest nasz jeden z programistów w pogotowiu Michał. Który akurat miał wolny wieczór można powiedzieć i też wcześniej przy tych wcześniejszych atakach w tym pierwszym i drugim, on brał udział we wszelkiego rodzaju analizach i poszukiwaniu tych dziur i innych tematów. Już jakiś szerszy kontekst znał i też wiedział, jak do tego podejść. Na pewno trzeba było bardzo szybko podejmować decyzje. Ja tutaj wiedziałem, że nie ma czasu zastanawiać się, czy ta decyzja będzie dobra, czy będzie zła. Trzeba było, jakoś podjąć tę decyzję, więc zdecydowaliśmy, że przywracamy sklep z backupu. Oczywiście tutaj w nawiasie powiem, że to nie był jeden sklep, to było kilka sklepów multi shop, więc tej roboty nie było kilkadziesiąt razy tyle, co z pojedynczego sklepu, ale na pewno było więcej, niż jakaś tam pojedyncza strona. Pierwsze, co zadecydowaliśmy to, to, że przywracamy z kopii zapasowej sklep. Na szczęście te kopie były utrzymywane i co jest ważne, żeby serwerownie te kopie utrzymywały. Przez chwilę trwała tylko decyzja, czy sprzed 2 dni, czy sprzed tygodnia. Najstarszą mieliśmy sprzed tygodnia, więc zadecydowałem, że bierzemy tą sprzed tygodnia, bo i tam będziemy mieli pracę w stylu dogrywanie zamówień właśnie z tego okresu, sprzed tygodnia, do dnia, w którym został sklep zaatakowany. To nie miało większego znaczenia, czy to będą zamówienia sprzed 2 dni, czy sprzed tygodnia, więc na pewno miało wpływ na to, czy tego ataku ktoś dokonał 2 dni temu, czy tego samego dnia, niż sprzed tygodnia, więc zdecydowaliśmy, że sprzed tygodnia. Tutaj też szukaliśmy szybkiego doraźnego rozwiązania, co zrobić na czas, kiedy ten sklep był przekierowywany, żeby to ukrócić, tak? Nie mogło tak być, że my będziemy coś robić w tle, a przekierowania nadal będą wyindeksować stronę w Google, więc spróbowaliśmy włączyć blokadę. Przerwę techniczną w Preście, ale niestety to nie zadziałało, więc wyłączyliśmy serwer Proxy i całkowicie odcięliśmy sklep od Internetu można tak powiedzieć. Można było się z nim połączyć tylko programistycznie z VPN o ile dobrze pamiętam. To już sprawiło, że te przekierowania nie następowały, tylko występował błąd 502, co jest raczej bezpieczniejszym rozwiązaniem, niż przekierowywanie na byle jaką stronę. Ktoś, kto wchodził na stronę, to dostawał po prostu białą stronę z błędem i też to był taki przedział czasowy, który nie był dość sprzyjający na prace serwerowe, bo serwerownia mimo że ma jakiś dyżur całodobowy w okrojonym składzie. To jest jednak tak, że od 18 robili sobie jakąś przerwę, więc trzeba było trochę nacisku wywrzeć na serwerowni, żeby jednak pomogła odzyskać nam ten sklep. Ja pracowałem chyba do 22.30, koordynując te prace, pracując wraz z Michałem, który też doradzał mi w tych kwestiach. Tak jak wspomniałem wcześniej trzeba

było przycisnąć serwerownie, żeby jednak chciała zabrać się do roboty, bo tam mówili, że chcieliby popracować, w jakichś takich normalnych godzinach, ale jednak musiałem dać im do zrozumienia, że nie ma takiej opcji, że trzeba działać natychmiastowo. Ok. godz. 20 zaczęliśmy przewracać ten sklep i z samego rana, jak już chłopaki zaczęli u nas pracę, to już mieli gotowy sklep przywrócony. Po kolej zaczęliśmy rozdzielać prace na dwóch programistów, co trzeba zrobić. Pierwszym, co zrobiliśmy jeszcze zanim sklep był odcięty, bo tam de facto sklep był odcięty 24 godziny w ogóle od Internetu, więc w tle przygotowywaliśmy poprawki. Naniesienie tych wszystkich łat, przeskanowanie jeszcze raz sklepu pod kątem tych dziur bezpieczeństwa, upewnienie się, czy wszystko, co na chwilę obecną wiemy zostało tam zaimplementowane. Tutaj też w nawiasie powiem, że mamy taką checklistę, z której korzystamy przy takim audycie bezpieczeństwa tego PrestaShop, mamy taką checklistę według, której postępujemy. Nanieśliśmy te poprawki, też w międzyczasie weryfikowaliśmy logi zaatakowanego sklepu, żeby sprawdzić, w którym momencie ktoś mógł się dostać. Szukaliśmy, jakichś takich podejrzanych śladów. Też przy okazji zweryfikowaliśmy dla wszystkiego moduły PayPal i PayU. Czy przypadkiem nie zaszły tam jakieś zmiany w tych modułach, bo np. tutaj mówiliśmy w przypadku tych dwóch ostatnich włamów, że były jakieś strony w koszyku, które zbierały dane kart. Natomiast jeszcze warto tutaj nadmienić, że jest w PrestaShopie taka dziura w module PayPala, że można się podszyć swoimi danymi dostępowymi do PayPala. Czyli tak hacker podmienia dane dostępowe w module PayPal i tym samym pieniądze zamiast spływać do właściciela sklepu, spływają do kogoś, kto założył sobie tam konto na słupa powiedzmy w PayPalu. Na to też warto zwrócić uwagę PayPal, PayU. Co jeszcze zrobiliśmy? Dla wszystkiego zmieniliśmy hasła w BackOffice dla wszystkich administratorów, również na stronie deweloperskiej. Zastosowaliśmy też takie bezpieczeństwo wokoło Presty, które blokuje w ogóle wgrywanie modułów do Presty. Czyli na dobrą sprawę administrator nie jest teraz w stanie wgrywać samodzielnie modułów po to, żeby jakiś hacker nie mógł tego zrobić. Jest to taka blokada po prostu zabezpieczająca przed tym, żeby nie wydarzyło się to o czym Paweł wcześniej mówił, że jakiś hacker instaluje sobie moduł, który potem może wszystko zrobić. Potem oprócz tego zmiana klucza webapp i zmiana haseł do baz danych. Przeskanowanie przywróconej kopii, jakiś skanerem antywirusowym też ze strony serwerowni podobna rzecz została sprawdzona. Po czym dograliśmy brakujące zamówienia od momentu, kiedy powstała kopia zapasowa, do mementu, kiedy postało ostanie zamówienie w jeszcze działającym sklepie. No i w momencie, gdy byliśmy już pewni wszystkiego. Tak, że mamy wszystko po dopinane, to w tym momencie wszystko uruchomiliśmy Proxy, żeby udostępnić sklep już użytkownikom. No

i później jeszcze byliśmy w takiej fazie czujności, żeby obserwować, czy wszystko jest w porządku. Cały proces trwał ok. 24 godzin zanim ten sklep został uruchomiony ponownie. No i przy tym, kosztowało to nas nie tylko czas, bo samych prac programistycznych było kilkadziesiąt. Z tego, co ostatnio liczyłem ponad 30. Licząc te prace koordynacyjne, prace programistyczne i to wszystko, to jednak tego wszystkiego się zebrało. Przy tym jeszcze straciliśmy mnóstwo glukozy, bo spada poziom glukozy, gdy trzeba podejmować trudne decyzje. Mieliśmy dużo stresu, ja miałem noc taką bardzo nieprzespaną. Było dość emocjonalnie w tym wszystkim, ale opanowaliśmy to. Tak to wyglądało z mojej perspektywy jako koordynatora, a tutaj więcej w temacie, jakichś programistycznych kwestii, to musiałby już Paweł dopowiedzieć.

G.F: A powiedz mi Piotr, znaleźliście w końcu, kiedy ten włam został zrobiony? Ile dni wcześniej?

P.T: Nie, tego nie znaleźliśmy. Znaczy myślę, że ciężko by było to znaleźć tak jak w poprzednich przypadkach, więc nie znaleźliśmy też źródła. Jednoznacznie też nie jesteśmy w stanie odpowiedzieć, która i z jakich podatności za to odpowiadała. Natomiast, tak jak już wcześniej wspomniałem na zimno, patrząc to myślę, że był to jakiś zautomatyzowany atak i raczej skierowany nie na wykradanie, jakichś danych, bądź pieniędzy, a raczej celu pod zdepozycjonowanie firmy, zepsucie wizerunku. Raczej nie wiem, może jakieś działania konkurencji wykupione na jakimś portalu hackerskim.

G.F: Różne symulacje są. Ja powiem tylko tyle, że Piotrek, że miał nieprzespaną noc i dużo stresu. Chciałem też zauważyć, że chłopacy stanęli na rzęsach, żeby to dokończyć. Jak rozmawiałem akurat z klientem z tego trzeciego przypadku, to klient z jednej strony bardzo się cieszył, że chłopaki tutaj stanęli na wysokości zadania i ogarnęli i widział ich zaangażowanie, że się troili, żeby to wszystko działało. A z drugiej strony powiedział „hej, ale powinniście opracować, jakąś procedurę krok po kroku", bo jednak było zamieszanie sprzed, kiedy przywrócić tą kopie, co zrobić, żeby zabezpieczyć to SEO i Google. Rzeczywiście tego nie mieliśmy opracowanego i tu było takie zastanowienie, kiedy i jak zrobić. Pomimo tego, że to szybko się działo, to pewnie taka procedura w razie ataku bardzo by pomogła. A też by zmniejszył ilość stresu po obu stronach i to na pewno wdrożymy i o tym myślimy, jak to zrobić, żeby to działało. Akurat z tym klientem rozmawiałem w tamtym tygodniu. Piotrek też miał pewnie, jakiś stres swój, ale myślę, że klient przecierpiał dużo więcej z tego powodu. Rozmawiałem też z klientem z pierwszego przypadku, to klient miał tam dużo więcej nieprzespanych nocy i się zastanawiał, czy

jak się obudzi kolejnego dnia to nie będzie znowu, jakiegoś ataku. Jednak tego źródła nie znaleźliśmy, zabezpieczaliśmy ten sklep, zrobiliśmy parę rzeczy i też tam na początku błądziliśmy, tak? Akurat w przypadku trzecim już mieliśmy miesiąc doświadczenia i wiedzieliśmy, co zrobić i klient się czuł z nami bezpieczniej. Przy pierwszym, to był też pierwszy taki nasz włam i też to widzieliśmy, ja to widziałem i rozmawiałem z ludźmi, że tą komunikację trzeba lepiej zrobić. W takich przypadkach koordynatorzy działają, żebym ja porozmawiał z klientem, bo czasami oni nie widzą tych emocji klienta, a ja tak trochę z zewnątrz działam, więc też potrafię pewne rzeczy wyłapać. Od stron komunikacji z klientem, żeby to działało, bo tam są takie niuanse, jak człowiek jest w emocjach i stresie to każdy się stara. Widziałem, że obie strony się starały jakoś przeciwdziałać i jeszcze do tego dochodzą inni klienci, którym trzeba też zabezpieczyć i pewne rzeczy mogą umykać. Tutaj porozmawialiśmy sobie z każdym z klientów chyba z godzinę, żeby to ogarnąć. Potem jeszcze ja dawałem informację zwrotną, co zrobić, co poprawić, czego klient oczekiwał. Tutaj moje takie wnioski są że potrzebujemy wdrożyć taką ogólną strategię, co zrobić krok po kroku. Z drugiej strony ja też widziałem taką pracę zespołową po pierwszym i po drugim włamie, że została stworzona taka cała checklista, co sprawdzić, i jak sprawdzić, bo wiedzieliśmy, że inne sklepy też trzeba będzie sprawdzić, prawda? To taka kilkunastopunktowa i wiem, że tu Paweł się udzielał i Michał i tutaj cały zespół działał, prawda? Paweł, jak to wyglądało, żeby to ogarnąć?

P.K: Tak, tak masz rację cały zespół. Tutaj już powiedzieliśmy, że to nie jest tak, że to jest ta jedna wersja Presty i ten jeden moduł. Tylko trzeba się było przygotować na to, że mogą być dziury w różnych wersjach, w różnych modułach, więc Michał tam przeanalizował ileś luk bezpieczeństwa wykrytych przez x lat w PrestaShop, w modułach do PrestaShop. Wyselekcjonował takie, jakie tam są potencjalne, groźne i też wzięliśmy pod uwagę to, że z takim jednym z podstawowych wektorów, które potencjalnie są używane do ataku i jest mechanizm Casha na bazie SQL i ten mechanizm trzeba zablokować, to jest taki element wspólny, który może być wykorzystywany. No i faktycznie przygotowaliśmy taką listę i taki mini audycik, który proponujemy u klientów. Trzeba było przygotować też, koordynatorzy mieli dużo pracy, bo musieli wysłać taką informacje do klientów, że coś takiego się dzieje i to jest też wyścig z czasem, tak? W momencie, kiedy PrestaShop opublikowała informację o tym, że jest taka luka, to już mamy w tym momencie wyścig z czasem, bo wszyscy już wiedzą, że jest luka w PrestaShop i każdy licealista może znaleźć informację na temat

włamanie na podstawie tego, co oficjalny komunikat PrestaShop głosi. To też nie jest taki audyt, taka kontrola sklepu klienta, to też nie jest taka prosta robota na godzinę, czy na pół godziny, tylko trzeba się, jednak temu przyjrzeć. Każdy klient ma inny sklep, każdy klient ma inne moduły, każdy klient ma inną wersję, troszkę inny hosting i kilka elementów trzeba sprawdzić.

G.F: Ile zajmuje taka checklista?

P.K: No nam zajmowała tak od 2 do 3 godzin. To jest po załatanie tego, co jest ważne. Czyli mieliśmy dla takiej wersji takie łatki, dla takiej wersji łatki, dla takiej wersji łatki. Musieliśmy sprawdzić, czy jest taki moduł, czy inny. Jeżeli te znane rzeczy zostały już załatane to jeszcze przeglądaliśmy tak mniej, więcej. Przeglądaliśmy stan modułów, jakie są moduły, w których miejscach są opcje wgrywania plików, czy jest kontrola wgrywania tych plików. To też jest jeden z częstszych miejsc, które hackerzy wykorzystują, aby wgrać coś na serwer, gdzie są dane pobierane z zapytań. Czy są walidowane, takie jest mniej, więcej sprawdzenie, czy wszystko jest okej.

G.F: Okej, czyli sprawdzenie tych dziur to było pierwsze 3 godziny, a tych modułów to pewnie z 2-3 godziny.

P.K: Raczej wszystko 3.

G.F: Raczej wszystko 3.

P.K: Sprawdzenie tych modułów to też jest takie, w jakiś sposób pobieżne. To już jest taka analiza, gdybyśmy chcieli wszystko dokładnie sprawdzić, to musielibyśmy dokonywać analizy linijka po linijce z zastanawianiem się, a czy w tym momencie w tym fragmencie kodu, to nie spowoduje, czegoś, co będzie w jeszcze innym miejscu kodu, prawda? To jest tak, że pewne fragmenty kodu wyglądają banalnie i poprawnie. Natomiast okazuje się, że ich działanie ma skutek dopiero wtedy, kiedy wejście, czy wyjście, w jakimś zupełnie innym fragmencie aplikacji powoduje coś innego. Nie jest, to takie bardzo proste.

G.F: To jest taki audyt i tutaj udostępnimy Wam taką checklistę, żebyście mogli to sprawdzać i od razu mówię, że ta checklistę może być nie pełna, bo zrobiliśmy to według naszej najlepszej wiedzy. Myślę, że jeśli macie, jakieś uwagi to z chęcią ją zaktualizujemy i udostępnimy. Chcemy po prostu pomóc wszystkim sklepom tutaj, które są na polskim rynku, żeby to ogarnęły. Jeśli nie macie programisty, żebyście mogli powiedzieć „zróbcie to mi" i mieć, jakąś tam większą szansę, że wszystko zostało dobrze

sprawdzone, bo jeśli nikt tego nie robił ani razu, to pewnie będzie szukał po całościach, albo zrobi to nie po całości. My tutaj i Paweł i Michał siedli i przeanalizowali wszystko i ułożyli to w całość, żeby to miało ręce i nogi i to daje, jakąś większą gwarancję, żeby to sprawdzić. Z drugiej strony trzeba to pouzupełniać dziury i żeby Wam się nie wkradali, żeby hasła do backendu nie mieć w stylu dupa1234. Tylko mieć lepsze te hasła, wręcz włączyć podwójne autentyfikacje, jeśli się da i parę innych rzeczy pewnie tam w tym pliku będzie. Będzie, czy nie będzie Paweł, bo ja widziałem go w tamtym tygodniu, ale już nie pamiętam.

P.K: Ja też nie pamiętam. Jeżeli chodzi o taką higienę, to chyba nie, bo tam są takie zalecenia dla nas, dla programistów, co trzeba zrobić.

P.T: Tutaj są na tej liście rzeczy związane głównie z PrestaShopem i jego modułami. Ja tutaj jeszcze mógłbym dodać taką rzecz, że tego typu zmiany trzeba wgrywać pilnie. Nie można być opieszałym w tych kwestiach i czekać, bo tutaj czas działa na naszą niekorzyść. Można tak powiedzieć, więc, jak tylko jest możliwość to tego typu zalecenia trzeba wdrożyć. Jednak nie ma co zwlekać, bo te wszelkiego rodzaju przypadki trzy, o których dzisiaj powiedzieliśmy, to one przecież nie były, jakieś zaplanowane. To wszystko było z zaskoczenia w najmniej oczekiwanych momentach.

P.K: Tutaj może to nie wybrzmiało tak, ale ten trzeci przypadek był taki, że my już z tym klientem uzgodniliśmy, że te łatki nanosimy. Tylko z tym klientem mamy wypracowaną taką procedurę obsługi, że te łatki zostały już naniesione tylko, że na wersje testową. Zawsze działamy tak, że klientowi przygotowujemy modyfikacje na stronie testowej, a klient to akceptuje i dopiero wgrywamy na produkcje. Można powiedzieć, że zadziałaliśmy już wcześniej, przygotowaliśmy to wszystko, ale nie zdążyliśmy tego wdrożyć na produkcji.

P.T: No właśnie i tutaj można powiedzieć, że tego typu podejście nie sprawdza się. Po prostu trzeba zaryzykować i od razu wdrażać na produkcję. Przynajmniej z mojej perspektywy, tak się powinno zrobić.

G.F: Tak to są takie nauczki z czasem, co warto zrobić, co jest bardziej niebezpieczne, jakie są koszty alternatywne takiego działania. No tak to jest czasami, działa się według procesu i człowiek się nie zastanowi myśli, że jeszcze się ma czas. Pamiętajmy, że to szybko zostało zrobione, to był bardzo skomplikowany sklep. Multi shop kilkadziesiąt sklepów, to jest skomplikowana rzecz, a tu się okazuje, że nie warto czekać przy sporym sklepie, który ma spory obrót dzienny. Tutaj do tej checklisty dodamy, jak zabezpieczać

serwer, bo chłopaki to gdzieś mają porozrzucane, a myślę, że warto, żebyście to wiedzieli. W jakiejś formie dodamy ten plik. Udostępnimy to, co mamy na ten moment złożone. Będziemy składać ten plik z kilku naszych innych plików, żebyście mieli. Jakieś finalne przemyślenia Piotrek na koniec, czy już powiedziałeś wszystko, co miałeś powiedzieć?

P.T: Wydaje mi się, że powiedziałem wszystko, co miałem powiedzieć. Nie, raczej na chwilę obecną nie mam nic do dodania.

G.F: Paweł, a Ty byś coś jeszcze dodał?

P.K: Zawsze zalecam dbanie o higienę sklepu i o higienę korzystania z haseł ze sklepu. Ja tak z uporem maniaka zawsze sprawdzam i monituje. Jeżeli mamy, jakieś moduły, które wgrywamy na serwer. Nie pasują nam, potem wyłączamy, kasujmy wszystko, co jest zbędne, wszystko. W sklepie powinny być tylko te moduły, które działają i, które są potrzebne. My to raczej staramy się stosować, ale jeżeli przychodzi do nas nowy klient, który ma już sklep od 3 lat. 2 firmy go serwisowały i jeszcze 10 programistów jeszcze coś tam. To zazwyczaj, to jest stajnia Augiasza. Jest 20-30 modułów różnych, pozostawiane pliki na serwerze. To zawsze może by gdzieś, jakaś furtka do włamania. Jeżeli tego jest, jak najmniej, to jest, jak najmniej punktów zaczepienia. My mamy potem, jak najmniej kodu do sprawdzenia. Nie korzystać z backendu sklepu przez publiczne sieci WiFi, Zabezpieczać swoje sieci WiFi, jeżeli korzystamy, obsługujemy sklep, to dotyczy wszystkich pracowników, bo teraz jest praca zdalna bardzo modna, ale jeżeli korzystamy z niezabezpieczonej sieci WiFi, to hacker może nam ukraść nasze ciasteczko. Może sobie wejść do naszego sklepu, albo podszyć się pod komunikację ze sklepem przez niezabezpieczone WiFi i może nam wykraść hasła i wcale nie potrzebuje, jakichś skomplikowanych ingerencji w kod PHP, bo po prostu ukradnie nasze hasło.

G.F: Po prostu ukradnie, tak. Ja tutaj jeszcze chciałem dodać na samym końcu, że jak rozmawiałem z chłopakami otworzymy te przypadki, pokażemy, co zrobiliśmy, a co nie zrobiliśmy. To chłopaki mówią „nie, ale może coś źle zrobiliśmy, może nie idealnie, może ktoś się doczepić, może znajdzie dziurę." Rzeczywiście tam może być, że to nie jest idealne. A ja stwierdziłem lepiej otwórzmy to, może komuś to pomoże, a z drugiej strony, jak ktoś nas skrytykuje i powiem „ej to mogliście zrobić tak, to mogliście zrobić inaczej", super, że nam mówisz wrzucimy w nasz proces, poprawimy to i pewnie udoskonalimy. Nie jesteśmy doskonali, pomimo to, że mamy 10 programistów i 5

koordynatorów i cały zespół tam, gdzieś działa i poprawia. Jak widzieliście ja bym dodał jeszcze o zabezpieczaniu serwera do tego pliku, bo chłopaki nie dodali, bo robią to inaczej. Dla Was to zrobimy i pewnie dopracujemy inne rzeczy przez kolejny miesiąc. Krok po kroku, bo to jest żyjący organizm. Jeśli macie uwagi ja z chęcią je przyjmę, przyjmę na klatę krytykę o błędy, które wykonaliśmy. Z chęcią pomożemy naszym klientom, którzy na tym na pewno skorzystają. Mam nadzieję, że wy skorzystacie. Jeżeli uważacie, że komuś, to wyślijcie to, bo ja to specjalnie otwieram krok po kroku, co może grozić, żebyście wiedzieli i ogarniali, tak? Też udostępniamy nasze wewnętrzne procesy dokładnie spisane, jak to jest zrobione, bo nam to nic nie da, że to trzymamy wewnątrz. Jest to coś naszego, ale za co nasi klienci w sumie zapłacili. Natomiast na rzecz Presty warto to udostępnić. A jak PrestaShop, która dość szybko zadziałała i udostępniła, bo taki miała obowiązek to zrobić i uprzedzić wszystkich o tym. To z jednej strony to jest super, a z drugiej strony otwiera potencjał, że każdy licealista może to, gdzieś tam wykorzystać. Może przesadzam, bo nie każdy, jednak trzeba się na tym trochę znać. Tutaj Paweł powiedział o hasłach. Ja myślę, że małe ryzyko jest to, że ktoś będzie nas śledził przez WiFi, ale hasła typu dupa123, albo wysyłanie haseł i loginów przez e-mail to już jest klęska. Tutaj polecam poczytać portal niebezpieczni albo jakiś inny, jak głupio można utracać różne dane. Już, nie mówiąc o blikach, a co dopiero, gdy można zaatakować sklep i ukraść kilkadziesiąt tysięcy, bo można zaszyfrować to wszystko, więc to tak jest. Dziękuję Wam drodzy, że z nami byliście. Wysłuchaliście! Dziękuję Paweł i Piotrek, że podzieliliście się swoimi historiami. Staraliśmy się tutaj powiedzieć, jak jest, a nie udawać, co jest. Uczymy się, uczcie się wy też i zabezpieczajcie własne sklepy. Dzięki wielkie i do usłyszenia.

P.K: Dzięki i do usłyszenia.

P.T: Do usłyszenia.