62. Jak bronić się przed cyberpatałachami? Czyli o zapezpieczeniu sklepu internetowego - Piotr Nakonieczny - Niebezpiecznik.pl

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! Ostatnio mówiłem o włamach na PrestaShop i jak sobie radziliśmy z tym, a dziś rozmawiam z Piotrem Koniecznym założycielem portalu niebezpiecznik.pl. Piotr zajmuje się cyfrowym niebezpieczeństwem od ponad 16 lat. Szkoli z tego, edukuje i informuje. Polecam jego portal. A dziś właśnie specjalnie dedykowany odcinek o tym, jak chronić sklep z punktu widzenia właściciela sklepu internetowego. O tym, co mogą nam wykraść? O tym, jak to robią i jak trzeba się przed tym zabezpieczyć? O tym, które platformy sklepowe są najbezpieczniejsze. Od Piotra nauczyłem się by nie używać słowa hacker, ale cyber patałach. Podoba mi się, a Tobie? Jak chcesz wiedzieć, co taki cyber patałach może zrobić Twojemu sklepowi i jak się przed tym bronić to zapraszam do posłuchania, ale zanim zacznę, to bardzo gorąco zachęcam Cię do zapisania się na newsletter na stronie convertis.pl/newsletter dzięki temu żaden nowy podcinek podcastu Ci nie umknie, a dodatkowo dostaniesz najważniejsze z e-commerce z Polski i ze świata. Zapraszam! A teraz już do odcinka.

Grzegorz Frątczak: Cześć Piotr!

Piotr Konieczny: Cześć!

G.F: Dzisiaj zaprosiłem Wam Piotra Koniecznego z niebezpiecznik.pl. To taki sławny portal, który działa od wieków chyba, co? Od niepamiętnych czasów.

P.K: No mamy dokładną datę powstania. Możemy zrobić konkurs na jej namierzenie, ale myślę, że wszystko rozpoczęło się solidne 14 lat temu.

G.F: 14 no to kawał czasu i niebezpiecznik wyszedł na takiego lidera odnośnie bezpieczeństwa w Polsce takiego cyfrowego. Macie konkurencję, czy jesteście jedyni, niepowtarzalni?

P.K: Wiesz co? No sporo jest, zwłaszcza teraz osób, które w branże bezpieczeństwa wchodzi i komentuje i można powiedzieć ciągnie ją do przodu. Bardzo dobrze, bo nawet gdyby było 10 razy tyle osób ile się tym tematem zajmuje, to wciąż będzie to za mało niestety.

G.F: Tak, patrząc ile ludzi używa haseł typu dupa albo 12345678, to dużo pracy jeszcze przed wszystkimi nami, żeby uświadomiać, że jednak nie do końca.

P.K: Ja sam używam hasła dupa.8, takiego bardzo popularnego hasła, zwłaszcza w takich kręgach krakowskich związanych z pewnym Uniwersytetem. No, ale co z tego, mam takie hasło do Gmail-a powiedzmy. Sporo osób pewnie korzysta z tego serwisu internetowego i Ty nawet, jak znasz to moje hasło, to się na moją skrzynkę gmailową nie dostaniesz.

G.F: Rozumiem, że masz podwójne składnikowe hasło, gdzie musisz jeszcze podać urządzenie albo hasło SMS-em.

P.K: No właśnie mam dwukrokowe, dwuetapowe uwierzytelnienie, tak się chyba po polsku nazywa MFA, ale on też nie jest idealny. Jak ludzie mają taki kod, który przepisują z aplikacji Google Authentication, albo OFI, albo nawet z SMS-a ta troszeczkę starsza metoda, to, to hasło da się wyłudzić. Czyli mówimy tutaj o takim ataku, jak fishing. Bardzo popularnym, najczęściej używanym i szalenie skutecznym. Za pomocą którego jeśli ktoś się nie zorientuje, że jest na fałszywej stronie, a da się zrobić tak, żeby się nie zorientował. Ludziom, jak się mówi o fishingu to przed oczami stają im nędznie podrobione strony zrobione na domenach, na które jak się patrzy to od razu widać, że coś jest nie tak. Ja potrafię i wykorzystujemy ze swoim zespołem takie domeny, gdzie trzeba się mocno natrudzić, żeby zauważyć, że to nie jest ta domena tej instytucji, tego serwisu. No, ale właśnie do tego zmierzam, że to można wyłudzić i dlatego ja nie mam tak zrealizowanego drugiego składnika. Ja mam zrealizowany ten drugi składnik za pomocą klucza U2F. To jest wydatek ok. 160 zł, ale mocno polecam każdemu, komu zależy na bezpieczeństwie, żeby te 160 zł wydał, bo gwarantuje każdemu, że jeśli nastąpi nieautoryzowany dostęp do jego skrzynki podstawowej pocztowej, albo innego ważnego serwisu, który przecież też można zabezpieczyć kluczem U2F. To straty zarówno te finansowe, które mogą być związane z obsługą incydentu, straty związane z wyciekiem danych, które się na tym serwisie znajdowały, a czasem straty wizerunkowe, jeśli te dane mówią o Nas te rzeczy, których nie do końca chcielibyśmy publicznie zaprezentować, będą

zdecydowanie większe, niż 160 zł. Mając taki klucz, to jest najważniejsze, nawet jeśli będziemy nie za bardzo w formie, nawet jeśli nie wykryjemy tego fishingu, użyjemy tego klucza na fałszywej stronie, to absolutnie nic Nam się nie stanie i przestępca stojący za tą stroną, parszywy oszust i złodziej odbierze z tego klucza, jakiś sygnał, ale ten sygnał nie będzie pasował do prawdziwego serwisu, pod który taki oszust się podszywał. Dlatego że ten klucz, mówiąc w dużym uproszczeniu ma takie małe elektroniczne oczka i on patrzy na ten adres zupełnie inaczej, niż My ludzie. On widzi dokładnie, co tam się znajduje i odsyła w zależności od tego, co tam się znajduje inne odpowiedzi. A pamiętaj, że jak ktoś się podszywa pod Gmaila, to potrzebuje odpowiedzi do Gmaila. A nie np. do Gmailla, czy czegoś innego, więc nawet, jak damy się podejść, mając ten klucz nic złego nam się nie stanie. Ja lubię takie idiotoodporne rozwiązania, bo często jestem w dobrym humorze i mogę nie zauważyć, jakiejś literówki i taki klucz mnie wtedy ratuje.

G.F: Tak, rzeczywiście tak jest, że jak się człowiek coś chce szybko, albo coś to może zrobić o jeden klik za daleko. Kiedyś miałem taką sytuację, że prawie bym kliknął, bo się spieszyłem i coś mnie tknęło, że może jednak nie. Chyba z SMS-a dostałem o paczkę i podobne rzeczy, więc no dzieje się.

P.K: No to jest możliwe. Tak, tak.

G.F: U2F klucze to może nie dzisiaj. Tu na pewno Piotr ma na swojej stronie niebezpiecznik.pl dużo materiałów, albo w Internecie znajdziecie. 160 zł to naprawdę niewielka kwota, ale dzisiaj chciałem z Piotrem porozmawiać na temat sklepów internetowych i o tym, co w ogóle może Nam grozić. No właśnie Piotr, powiedz mi, czy są jakieś badania, które mówią, która platforma sklepowa dla właścicieli jest najbezpieczniejsza?

P.K: Ja myślę, że jest wiele takich badań. Zazwyczaj za tymi badaniami stoją twórcy tej platformy, którzy w mniej lub bardziej zaciemniony sposób próbują wpływać lub dobierać dane, żeby pokazywać to na czym im zależy. No, ale żarty na bok. Najbezpieczniejsza platforma to jest taki św. Grall, ja bym powiedział. Dlatego że każda technologia, każdy software miał błędy, będzie mieć błędy i tego nie zmienimy. Po prostu musimy się przygotować na to, że oprogramowanie, z którego korzystamy prędzej, czy później nawet bez winy firmy, która stoi za tym oprogramowaniem, twórców tego oprogramowania może nagle stać się dziurawe. Mamy problem z łańcuchem dostaw dzisiaj bardzo popularnej, nie chodzi mi o ten gospodarczy, chodzi mi o ten software'owy tzn. oprogramowanie bazuje na szeregu

bibliotek. Bibliotek tworzonych przez ludzi z różnymi pomysłami, z różnych krajów, którzy mają różny stan swojego zdrowia psychicznego i już kilka razy na przestrzeni ostatnich miesięcy zdarzyło się, że człowiek, który jest twórców tej biblioteki, nagle w tej bibliotece robi kuku, albo ją wyłącza i w ten sposób psuje różne zależności i wiele systemów, wiele oprogramowań przestaje dobrze pracować. Także ja bym się raczej skupił na tym, że jeśli ktokolwiek myśli o doborze, jakiejś platformy to powinien spojrzeć na problem w taki sposób. Czy ludzie, którzy stoją za tą platformą reagują na incydenty? Jak szybko reagują na ten incydenty? Jak są transparentni i to chyba byłoby najważniejsze. Jeśli ktoś chce spojrzeć na to, jaka platforma miała ile dziur w przeszłości, to moim zdaniem nie jest to najlepszy wyznacznik. Tak jak mówię wszystko ma dziury i to, że ktoś odnotował, jakiś problem, to nie oznacza, że ten problem będzie dotyczył wszystkich klientów w każdej konfiguracji. Trzeba mieć niestety wiedzę ekspercką, żeby umieć ocenić, czy 15 problemów 1 platformy, to jest gorzej, niż 3 najpoważniejsze problemy 2 platformy. Także tutaj raczej bym się skupił z punktu widzenia osoby, która chce dobrać, jakąś platformę na tym, czy zespół, który stoi za tą platformą wie, co robi. To każdy może ocenić w taki sam sposób, czyli patrząc na to, jak ten zespół przez lata reagował i komunikował swoje reakcje.

G.F: Z tego, co tutaj rozmawialiśmy poza nagraniem mówiłeś, że mieliśmy taki przypadek, że PrestaShop znalazła, jakąś tam dziurę i różnie hackerzy to wykorzystywali i powiedziałeś, że to głównie automaty chodzą i krążą po niezabezpieczonych sklepach i szukają dziury w całym. Tak sobie myślę, że te wszystkie małe sklepy są narażone na te wszystkie dziury, które nie są zaktualizowane, bo to automaty śledzą. Automaty są w stanie wszystko prześledzić w ciągu nie wiem, paru dni w zależności, jakie serwery się weźmie. A z drugiej strony duże sklepy, to już pewnie niektórzy się połaszą i zrobią personalizowane szukanie dziury w całym. A może się mylę?

P.K: Generalnie przedstawiłeś 2 najpopularniejsze typy ataków, w ogóle 2 możliwe typy ataków. Pierwszy tzw. atak masowy, gdzie atakującemu i ja stronię od tego, żeby tych ludzi nazywać hackerami, bo jednak etymologia tego słowa i zrozumienie tego słowa w naszych środowiskach jest trochę inne, niż w tzw. mass-mediach. Ci atakujący, złodzieje, przestępcy, patałachy oni mają na celu zarobić. Ich nie interesuje, czy zarobią na Twoim sklepie, na moim sklepie, czy na sklepie Janka. Oni chcą zarobić, więc oni działają masowo. Dzisiaj cały Internet pod katem portu 443, czyli czegoś, co większość ludzi utożsamia z usługą, którą udostępnia sklep internetowy, bo tym protokołem komunikujemy się ze sklepem

internetowym. Cały Internet można IPv4 można przeskanować w 4-5 minut. Czyli wyobraź sobie, że po 5 minutach dostajesz raport, gdzie w Internecie, na których adresach znajduje się sklep, który jest dziurawy. Masz taką listę, bardzo często…

G.F: W 5 minut?

P.K: Tak, w 5 minut. Tysięcy, a bardzo często setek tysięcy serwisów, do których możesz się teraz włamać. No i masowo to robisz, bo jak jesteś sprytnym patałachem, to nie będziesz przeklikiwał tego codziennie ręcznie, bo możesz ten czas poświęcić na coś zupełnie innego. Kolejne oszustwa, przekręty, czy pranie pieniędzy, które w ten sposób swoim procederem już wygenerowałeś. To robią automaty, automatyzuje się to, zresztą to jest proste do zautomatyzowania. Natomiast są też takie ukierunkowane, ta druga grupa, że jeśli mnie strasznie zdenerwuje ten Janek, albo jakaś duża firma prowadząca sklep internetowy, bo załóżmy kupiłem od niej buty. Miały być czerwone, a przyszły karmazynowe. Ja rozróżniam te 2 kolory, a oni mi reklamację odrzucają i mówią, że to nie jest kolor karmazynowy tylko czerwony. Ja jestem zdenerwowany i ja mogę teraz w zależności od moich zdolności i mojego czasu codziennie przez miesiąc, tydzień, nawet rok po godzince skubać sobie infrastrukturę tego sklepu. Zmapować ją, dowiedzieć się, jak wygląda stack technologiczny i nawet, jeśli on dzisiaj jest bezpieczny, czyli nie ma żadnej znanej publicznie dziury, błędu do możliwego ataku. To ten atak najprawdopodobniej pojawi się w ciągu miesiąca, tygodnia. Jak się pojawi ja się o tym dowiem z listy mailingowej Twittera, czy nie daj Boże teraz Tik-Toka, gdziekolwiek resarcherzy związani z bezpieczeństwem ujawniają takie błędy. To ja w 1 minucie, jak myślisz o kim pomyślę? Pomyślę dokładnie o tych oszustach, którzy mi sprzedali buty karmazynowe i nie uwzględnili reklamacji. W moim mniemaniu oczywiście i co ja zrobię w 2 minucie? Ja w drugiej minucie uruchomię ten atak na ten sklep. Ja będę to robił ręcznie, żeby się zemścić, coś dopisać, pozdrowić kogoś, itd. Jeśli moja złość zaślepi mi trochę moje zdolności logicznego myślenia, to mogę zostawić pewne ślady, które będą na mnie wskazywały, które powiążą mnie z tą reklamacją. Może nie dawajmy instruktarzu osobom, które się gdzieś włamują. Natomiast na tym dokładnie polegają te ataki. Z jednej strony masowe ataki i to tym, atakom wbrew pozorom powinniśmy najwięcej uwagi poświęcić jako właściciele platform, bo na nie jesteśmy narażeni praktycznie non stop. Jeśli ktoś z Was kiedykolwiek patrzył na logi dostępowe, te które zawierają próbę dostępu do Waszego serwera, czy to po takim protokole, jak SSH, który pozwala zarządzać, sterować serwerami, czy to nawet, po jakimś panelu logowania, który jest wystawiony na publicznym adresie IP. To praktycznie, co kilkadziesiąt sekund jest, jakaś próba połączenia. Czy to z Chin,

czy z Tajwanu, czy z Rosji, czy z Ukrainy, czy z Polski spod Radomia, czy np. z USA. Tam automaty chodzą i próbują się logować, bo na tych atakach masowych, to nie jest tylko tak, że podatne atak tylko są te serwisy, które mają błędy. Te, które nie mają błędów też są podatne na ataki i można byłoby zapytać, ale jak to? To bezpieczne wszystko, ale dalej się włamują. Tak to, ale wszystko wychodzi z konfiguracji. Jeśli np. ktoś chciał dobrze, ale zrobił źle np. chcieliśmy zwiększyć bezpieczeństwo Naszej platformy i zaznaczyliśmy kopie bazy zapasowej codziennie wieczorem i o 4 nad ranem, bo jak się coś znajdzie to mamy kopie. To jest dobre działanie, generalnie każdy chciałby coś takiego robić. A teraz są wtyczki do wielu platform, które to robią, ale tą bazę wystawiają w taki sposób, że ona jest publicznie dostępna. Jak ktoś wie, gdzie szukać, namierzy, że ktoś ma taką wtyczkę, to może sobie tą bazę wyssać. A z tej bazy odczytać dane dostępowe, a tymi danymi się zalogować. No i mamy problem, czy to był problem związany z oprogramowaniem dostawcy platformy? No nie, to był problem związany tak naprawdę z wtyczką napisaną przez firmę trzecią, a zazwyczaj, jakiegoś tam zmęczonego, doświadczonego mniej lub bardziej programistę po godzinach, który czegoś nie przewidział. No i właśnie pojawił się problem. To są takie problemy, które najczęściej chyba widzimy, jeśli chodzi o takie oprogramowania usługowe, wychodząc nawet szerzej poza branże sklepów internetowych. Tak, bo niektórzy mają sklepy internetowe, a inni mają serwery gier, jeszcze inni mają jakieś inne platformy, które udostępniają, czy zwykłe serwisy internetowe, bo serwisy internetowy się od sklepy dużo nie różni szczerze, mówiąc. Jeden i drugi udostępnia stronę internetową, na której coś można zrobić.

G.F: No właśnie, to czego powinni się bać właściciele sklepów, jak taki patałach, jak go nazwałeś. Muszę zacząć używać tego słowa, bo rzeczywiście dobre.

P.K: Cyber patałach.

G.F: Cyber patałach wejdzie nam do sklepu, to czego oni najczęściej szukają: danych, pieniędzy, innych skarbów? Jak to wygląda?

P.K: Czego oni szukają, no oni szukają pieniędzy.

G.F: Co oni chcą?

P.K: Tylko, że nikt nie trzyma pieniędzy w sklepie internetowym, w formie portfeli kryptowalutowych. Pieniądze, jest takie słowo, którego cyber patałachy używają. Montetyzacja danych zazwyczaj. Można zastosować w sklepie internetowym.

G.F: Jak wszystkie start-up'y chcą zmonetyzować swój biznes tak oni też.

P.K: 3 pomysły na monetyzacje do sklepu internetowego, do którego dostaliśmy nie autoryzowany dostęp. Jakież to będą. Pierwszy chyba najbardziej popularny. Mamy dostęp do cudzych danych, te dane możemy skopiować, czyli wykraść, a następnie sprzedać na czarnym rynku, bo cyber patałachów interesują pary login i hasło najczęściej. Czasem jeszcze dane kontaktowe. Po co? Po to, że za pomocą tych danych można spróbować wykonać taki atak, który się nazywa credential stuffing. Czyli, jak ja mam dane dostępowe do sklepu internetowego i wiem, że 80% ludzi używa do tego samego hasła do wielu miejsc. To ja sprawdzę, czy Twój klient janek@gmail.com, który miał hasło do sklepu: sklep123, czy nie ma tego hasła sklep123 do swojego gmaila, do Allegro. Chwila sklep123 dla gmaila nie bardzo pasuje, ale tutaj widać pewien sposób tworzenia hasła, to może to będzie poczta123, może to będzie allegro123, jeśli wiesz do czego zmierzam. Takie dane wykradzione one pozwalają przejmować inne konta i są inne grupy, które się tym zajmują, że na podstawie login, hasło, dodatkowe dane. Tworzą scenariusze ataków, przejmują kolejne konta, które też monetyzują. No bo z PayPala można łatwo zrobić transfer pieniędzy na zewnątrz, a jak ktoś ma takie samo hasło do PayPala, jak do sklepu internetowego, w którym założył sobie konto.

G.F: Zdradzisz, jeśli możesz ile kosztuje 1000 takich par login i hasło? 1000 sztuk.

PK: Tego się nie kupuje na tysiące, czy na kilogramy. Raczej patrzy się na to skąd te dane wyciekły, jak są świeże, kto już przez nie przeszedł, czyli co jeszcze można potencjalnie zrobić. Pamiętaj, że to jest czarny rynek. Tam oszuści i złodzieje sprzedają to oszustom i złodziejom. To nie jest tak, że jest oferta i pisze „świeża, nieśmigana baza", to ona jest nieśmigana. Często jest już mocno prześmigana. Jest też pewien system reputacji paradoksalnie na tych podziemnych forach po to, żeby można było zweryfikować, czy te dane są dostępne czy nie. Teraz na jednym z takich serwisów jest wystawiona na sprzedaż przez niezbyt wiarygodnego sprzedawcę, więc pytanie, czy temu wierzyć, czy nie. Niech każdy osądzi. Baza serwisu e-commerce, gdzie jest, jeśli dobrze kojarzę 35 tys., albo 350 tys. rekordów. W każdym razie cena, to było od 2-3 tys. dolarów. Czy to dużo, czy mało? Nie mnie oceniać, pewnie się znajdą tacy, którzy na tym zarobią zdecydowanie więcej, bo jeśli spojrzysz na bardzo popularny scam, który ma miejsce w Polsce od ponad już 2 lat, albo może nawet 3, to jest telefon od fałszywego pracownika banku. Czyli ktoś spoofuje rozmowę telefoniczną i podszywa się pod numer infolinii Twojego banku. Jak miałeś swój bank wpisany w swojej książce kontaktowej w smartfonie, to Ci się wyświetli, że dzwoni do Ciebie Twój bank. W tym momencie ktoś mówi „Panie Grzegorzu, bo ja dzwonię z banku", tutaj pada nazwa tego banku. W ogóle skąd on wie, że Ty masz konto w tym banku, a on stąd wie,

że w sklepie internetowym, z którego ukradł dane, płaciłeś kartą płatniczą, to po numerze karty płatniczej można dojść, który bank te kartę płatniczą wystawił. „Panie Grzegorzu dzwonię z banku 123 zaobserwowaliśmy podejrzaną transakcje na Pana koncie. Ja wiem, że teraz w mediach są różne ostrzeżenia, które mówią o pracownikach banku, którzy dzwonią z ostrzeżeniami, ale to jest sytuacja prawdziwa. Ja Panu to udowodnię. Proszę sprawdzić, z jakiego numeru ja dzwonię i sprawdzić, czy na stronie banku to jest ten sam numer. Jak to już mamy za sobą i słyszał Pan, że gdzieś można podrabiać numery banków. To ja Panu powiem, że mam 4 ostatnie cyfry Pana karty, mam wszystkie Pana dane, wiem, gdzie ma Pan adres zameldowania, adres zamieszkania.” Bo to też jest adres dostawy, jak ktoś nie zamawiał przez Paczkomaty. W ten sposób można w zależności od tego, jak nam się klei rozmowa zdolnością socjotechniczną jaką reprezentuje cyber patałach poprowadzić bardzo wiarygodną rozmowę, jaka skłoni Cię do tego, że on Cię okradnie w rozmowie. Ty sam się okradniesz, Ty sam wypłacisz pieniądze zgodnie z instrukcją, że Twoje konto jest zagrożone i musisz wypłacić środki. ”Ma Pan rachunek żony to może niech Pan wypłaci, a najlepiej to do bankomatu. A w ogóle założyliśmy panu rachunek techniczny i on jest super oprocentowany, bo jest taka sytuacja, że trochę się poczuwamy jako bank123 do odpowiedzialności, że to Pana spotkało. To teraz proszę wpłacić te środki, ja Panu podam kod blik one wylądują na tym naszym rachunku technicznym.” Ty jeśli jesteś przekonany, że rozmawiasz z pracownikiem banku, to właśnie się okradłeś, a to dlatego że serwis internetowy, niekoniecznie sklep internetowy stracił Twoje dane, a na tych danych popracowali ci przestępcy, którzy akurat ten scam realizują, więc tak to wygląda, ale to nie koniec.

G.F: Bardzo przekonujący jesteś Piotr, powiem tyle. Już mnie przekonałeś, już Ci idę przelać pieniądze, jeszcze dodajmy na wujka, albo na babcię.

P.K: Wiesz co? Są lepsze metody tylko ja ich tutaj nie ujawnię, dlatego że my, kiedy symulujemy takie działania atakujących pod kątem naszych klientów, kiedy do nich się włamujemy i chcemy oszukać np. Biuro Obsługi Klienta ich Infolinię, albo ich Zarząd. To używamy trochę innych argumentów, tylko nie do końca chce je tutaj przytaczać, bo znam ich skuteczność i 8/10 rozmów, kończy się tym, co mieliśmy mieć. Można to zrobić zdecydowanie lepiej, niż to, co przeciekło do mediów i to na czym bazowałem wcześniejszą rozmowę, bo to nie jest tajemnica. Te metody są już opisane, one są już znane, warto o nich mówić. Natomiast nie będę podsuwał tych, które są szalenie skuteczne, bo są świetnie dopasowane do realiów polskich firm. No, ale, wracając do tego naszego monetyzowania zaatakowanego sklepu, to przecież my niekoniecznie musimy pieniądze wyciągać, jak

zwierzęta od tych klientów. My możemy wyciągnąć od dostawcy sklepu internetowego, czyli zaszyfrować nam wszystkie dane i powiedzieć „a teraz zapłać.” A co powie właściciel takiego sklepu internetowego? Powie „nie zapłacę, bo ja mam kopie bezpieczeństwa.” Problem w tym, że one też mogą być zaszyfrowane, jeśli ktoś źle te kopie wykonuje. Na podstawie wejścia udało się oszustom i kopie bezpieczeństwa zaszyfrować. Załóżmy, że ktoś ma te kopie bezpieczeństwa na zewnątrz zgrywane, zabezpieczone w taki sposób, że rzeczywiście one nie ucierpiały. Potrafi sobie to wszystko odtworzyć. To, wtedy taki cyber patałach powie tak „to ja w takim razie ujawnię te wszystkie dane, bo nie tylko Ci zaszyfrowałem, ale część z nich wykradłem.” No i może Twoja konkurencja się dowiedzieć, jaki produkt jest najczęściej sprzedawany. Skąd są Twoi klienci i jaka jest Twoja struktura, którą chcesz utrzymać na rynku. Po prostu wywalę Ci bazę klientów do Internetu. Teraz już jest tzw. podwójny okup. Pierwszy jest za rozszyfrowanie danych, a jak on nie zadziała, to za nieujawnianie danych. No i Ty teraz zaczynasz się drapać po głowie mówisz. „Kurczę to mnie może zaboleć. Wszyscy się dowiedzą, że zostałem zaatakowany. A niektórzy uważają to za wstyd, czy to jest dobre myślenie, czy nie, to na razie zostawmy. A druga rzecz jest taka, że te dane pokazują problem dla moich klientów, więc może ja zapłacę. Jak zapłacisz, ja się wtedy ucieszę jako ten cyber patałach, bo właśnie zarobiłem. A jak mnie zdenerwowałeś, to przyjdę do Ciebie za 2 tygodnie i powiem „ale się dałeś sfrajerzyć, zapłaciłeś mi raz ja tych danych wcale nie skasowałem, jak obiecałem, teraz potrzebuje 2 razy więcej. No i mamy potrójny okup. Teraz jest pytanie, czy zaufać oszustowi, tak, czy nie? Czy negocjować z terrorystami, czy nie. To są dylematy, na które nie ma jednoznacznej odpowiedzi. To jest coś, co niestety trzeba rozważyć per przypadek, zrobić tzw. analizę ryzyka. Zweryfikować, czy te dane rzeczywiście wypłynęły, bo czas może wcale nie wypłynęły. Ktoś może kłamać, że je skasował lub miał większy dostęp, niż rzeczywiście pozyskał. To też jest taka możliwość. Jest jeszcze jedna możliwość, mogę Ci zalewać serwis internetowy, ruchem internetowym, żeby paraliżować dostęp do Twojego serwisu klientom. Jak klient chce kupić ramię do monitora firmy Dell. Trafia na Twój sklep, ale on coś wolno działa, nie ładuje się. To ten klient nie będzie czekał do jutra na ramię monitora, bo żyjemy w czasach natychmiastowych zakupów online. On pójdzie na drugi sklep internetowy, gdzie kupi to za prawdopodobnie 1.5zł drożej, bo wiemy, jak się różnią ceny w sklepach, zwłaszcza tych produktów IT. Właśnie straciłeś klienta i jak Twój sklep nie działa dzień, dwa, trzy, tydzień, to zaczynasz odczuwać ten spadek przychodów, obrotu i to jest problem. Teraz możesz próbować na wiele różnych sposobów chronić się przed tzw. atakami DDoS, ale prawda jest taka, że jeśli potrafi się je znowu dobrze zrobić, to takie standardowe ochrony, które są udostępniane przez serwerownie, czy nawet

operatorów łączy internetowych nie zawsze będą 100% skuteczne. Są takie ataki, które przez te filtry, blokady przechodzą i dalej paraliżują taki sklep. Wszystko zależy od tego, kto jest po drugiej stronie. Znowu tu nie będę podpowiadał tym złym. My symulacje takich ataków DDoS robimy i mogę Ci powiedzieć, że większość polskich banków padnie pod naporem ruchu, który da się wygenerować z dwóch Neostrad. Neostrad z dwóch należałoby teraz powiedzieć łącz Orange. Ale da się to zrobić, tylko nie jest to kwestia przepustowości ruchu. Ludzi lubią operować liczbami, bo to jest jakoś tam wymierne, wyobrażalne. Natomiast tak naprawdę chodzi o konfigurację tego, jaki ruch wysyłasz. Jak wiesz, jaką infrastrukturę ma klient, wiesz z jakich urządzeń on się składa, to czasem wysłanie mniejszych pakietów po mniejszej przepustowości sprawi, że te urządzenia zaczną się dusić i nie będzie to działało płynnie. W konsekwencji Ty będziesz tracił jako właściciel platformy pieniądze. A i jeszcze coś pewnie przyszłoby mi do głowy, jeśli miałbym monetyzować. Chociaż w przypadku ataków DDoS nawet nie mówimy o nieautoryzowanym dostępie, bo tam nie ma żadnego problemu z bezpieczeństwem, to może spotkać każdy serwis i spotyka. Jeszcze są oczywiście oportuniści, którzy wysyłają masowo informacje „cześć będę wystawiał Ci negatywne opinie, chyba, że zapłacisz.” „Cześć będę Cię DDoSował chyba, że zapłacisz”. Pokazują scenariusze, czasem takie ataki miały miejsce, a w rzeczywistości to są ludzie, którzy nie będą tego robili, ale jak masowo roześlą 2-3 miliony maili dziennie, to znajdą się 3-4, czy 15 osób, które dojdzie do wniosku, że zapłaci. Dla nich to jest good enough. Stwierdzą „dzisiaj zarobiłem 1000, ale się za bardzo nie narobiłem, bo to wszystko jest zautomatyzowane i codziennie mi ten 1000 wpada.” W skali miesiąca mamy 30 tys., więc odpowiedz sobie na pytanie, czy to jest wystarczające, czy nie.

G.F: Jak na warunki polskie, całkiem znośnie bym powiedział. Można pojechać na wakacje nad polskie morze.

P.K: A na warunki indyjskie pewnie jeszcze bardziej. Dokładnie, 1 kg ryby zjeść.

G.F: A powiedz mi, czy obserwujesz tutaj w naszym pięknym kraju w Polsce, takie jakieś mity odnośnie bezpieczeństwa sklepów internetowych, którymi wszyscy żyją, a to nie do końca jest prawda? A warto je zweryfikować.

P.K: Wiesz co? Nic mi tak nie przychodzi do głowy, jeśli chodzi o mity związane ze sklepami internetowymi. Natomiast mity związane z bezpieczeństwem. Zdarza się, że ludzie uważają, że coś ich spotka złego w Internecie. Przed tym się chronią, ale w rzeczywistości to jest mało prawdopodobne, żeby ich to spotkało, a coś innego, co ich może spotkać na każdym kroku

tego nie postrzegają jako zagrożenie. To jest popularny błąd poznawczy, wiele osób odczuwa strach przed lataniem, ale przecież samolot jest najbezpieczniejszą formą komunikacji i tu jest trochę wydaje mi się podobnie. Jeśli mielibyśmy mówić o takich kwestiach to ja bym chyba wskazał różnego rodzaju certyfikaty, czy odznaki platformy, nie chce tutaj nikogo urazić bezpiecznych kupujących, 100% bezpiecznego sklepu i inne takie bzdury, które pojawiają się w formie jpg'a, kiedy ktoś mówi, że ktoś jest wiarygodną firmą. Z wiarygodnością to może mieć wiele wspólnego, ale na papierze, a w rzeczywistości wystarczy jeden cwaniak, który się włamie i podmieni formularz zamówieniowy, czy nawet maila wysyłanego z numerem rachunku bankowego na swój numer rachunku bankowego i zanim się zorientujesz pewnie trochę czasu minie, jak klienci zaczną krzyczeć, że nie mają swoich zakupów. No to już trochę tych pieniędzy przepadło.

G.F: Rzeczywiście w Polsce jeszcze mamy takie warunki, że nie wiem, czy wszystkie, ale większość sklepów używa bramek płatności, więc tych danych płatności sklepy nie posiadają u siebie. O tyle według mnie klienci są bezpieczniejsi, że nawet włam do sklepu nie powoduje dostępu do kart, tylko trzeba znowu robić fishing. Z drugiej strony mogą też podmienić odpowiednie kody, żeby te odpowiednie rzeczy wyciągnąć od klientów. Żeby klienci podawali, albo żeby te płatności były realizowane, gdzie indziej. To też jest pewnego rodzaju monetyzacja, szczególnie te większe sklepy, ale można tak to zrobić. Tak mi teraz przyszło do głowy.

P.K: Znamy nawet takie przypadki, że w takich popularnych dużych sklepach padli ofiarą takiego ataku, a potem udawały, że takiego ataku wcale nie było. Pomimo tego, że ślady internetowe pozostały po tym ataku niezaprzeczalnie. Okazało się, że nawet właściciel platformy nie był świadomy, że został dojechany, a sprawa wyglądała tak, że udało się komuś włamać na stronę taką dedykowaną. Zbliża się promocja na Halloween i sklep sobie postawił landing halloween.sklep.pl, a potem o tym landingu zapomniał, bo to był Halloween 2018, a mamy teraz 2022. Oni sobie robią swój biznes na swojej platformie, która jest bezpieczna, a tamten landing wisi i się starzeje i tamte skrypty, biblioteki pojawiają się dziury. Ktoś to zauważa i ktoś się wbija na ten halloween.sklep.pl i mówi „kurde, jak tu jestem to, co mogę zrobić, mogę podmienić stronę główną, wrzucić cycki, będzie dużo śmiechu, niebezpiecznik o tym napisze, może nawet na Onet wpadnie". Ja mogę na tym zarobić, jak mogę na tym zarobić? Kopiujemy aktualną ofertę sklepu, przekreślamy cenę halloweenowa promocja o 30%. Nie za dużo, bo to będzie za dużo, ale te 30% będzie jeszcze w granicach normy i robimy przycisk kup, który kieruje na naszą formę płatności, podaj numer karty, czy tam

cokolwiek innego. Efekt jest taki, że jak Ci ktoś puści reklamy na prawdziwej domenie, z prawdziwą kłódką tylko na nie używanym przez Ciebie serwisie, kontrolowanym, podmienionym przez atakującego. To sporo osób, bazując na zaufaniu, na marce tego sklepu, stwierdzi, że to nie jest ściema, to jest ten sklep. Wszystko się zgadza kupuje, kupuje. Bramka płatności, czy podaj numer karty, a nawet bezpieczniejszej jest płacenie kartą i sporo osób się nabrało. Pokupowało sobie i zapłaciło za rzeczy, które nigdy do nich nie dotarły.

G.F: Jakże to przyjemne. No właśnie, to jak chronić swój sklep przed takimi różnymi, dziwnymi akcjami tych patałachów, cyber patałachów.

P.K: Cyber patałachów. Rady są znowu bardzo proste. Pierwsza jest taka, że jeśli nie mamy zdolności technicznych samodzielnie, a zakładam, że większość osób ich nie ma. To należy sobie zatrudnić osobę, która takie zdolności techniczne ma i dopilnować, żeby ta osoba dbała o tą platformę od strony takiej administracyjnej, gdzie administrację rozumiem od strony takiej stricte technologicznej. Administrowanie serwerami i oprogramowaniem. Pierwszą podstawową sprawą jest aktualizacja. Regularna aktualizacja oprogramowania. Błędy były, są i będą, ale są też usuwane przez twórców danych bibliotek, rozwiązań, które mamy. Warto te aktualizacje, jak najszybciej wdrażać. Jak najszybciej oznacza, że jeśli wdrożymy taką aktualizację po dłuższym czasie, niż 5 minut od jej pojawienia. To już wiesz, że jak ktoś napisał skrypt do scanowania, to w te 5 minut to już może być za późno. Także tu ładnie widać, jaka jest dysproporcja możliwości pomiędzy atakującym, a tym, który chroni platformę. Czas reakcji jest tutaj kluczowy. Dlatego warto byłoby poza aktualizacją, którą warto robić i to nie jest tak, że wszystkie sklepy padają w 5 minutach od opublikowania ataku, ale ten skrajny przypadek. Natomiast już w ciągu doby to warto robić i obowiązkowo. Poza tą aktualizacją jest druga rzecz, na którą trzeba zwrócić uwagę – monitoring. Musimy patrzeć, czy ktoś próbuje nam się dostać do platformy, czy nam się nie zmieniają opisy np. produktów, albo pojawiają się dodatkowe pod strony. To można zrobić, to nie jest miejsce ani widownia, której powinniśmy technicznie mówić, jakie są rozwiązania, jak często to robić, jak zaprojektować poprawnie, ale na tym polega praca tej osoby, którą się zatrudnia, żeby się tym zajęła, żeby to skonfigurowała i, żeby to monitorowała. Monitoring jest kluczowy, to nie jest tak, że ataki zdarzają się w godzinach pracy 6-16. Ataki zdarzają się często późnym wieczorem, kiedy ten administrator chciałby sobie pospać. Z drugiej strony, jak ktoś ma sklep internetowy, to też sprzedaje 24 godziny na dobę. Myślę, że każdy zauważy, że sprzedaż jest w godzinach nocnych mniejsza, ale czasem nam się zdarzy, że się trafi osoba, która o 4 nad ranem coś kupi. Dobrze, jej możliwość, jej wola, jej chęć, niech kupuje, niech nam daje

pieniądze. Ale po naszej stronie to taka trochę odpowiedzialność, że w tym momencie fajnie byłoby patrzeć na to, co się z tą platformą dzieje, czy ona nie jest atakowana. Jak ona zostanie zaatakowana o 4 nad ranem, to atakujący ma dostęp do tych samych danych, które są tam i o 8 i o 9 poprzedniego dnia, więc jednak gra jest warta świeczki. Trzecia rzecz, jak już monitorujemy i aktualizujemy, to byłoby dobrze raz na jakiś czas przetestować, zasymulować takie ataki. Wynająć, jakąś firmę, która jest w stanie symulować działania atakujących, wykonywać tzw. testy penetracyjne, mówiąc wprost przywalić w ten sklep. Zobaczyć, czy rzeczywiście on jest poprawnie skonfigurowany. Czy ktoś, czegoś nie przeoczył, czy tam jest ta wtyczka do backupów, czy ona jest dobrze skonfigurowana, czy przypadkiem panel logowania nie da się obejść w taki sposób, że przez procedurę resetu hasła można przechwycić żądania, a następnie za pomocą klucza, który był w nagłówku tego żądania uzyskać wymuszony reset hasła. Takie rzeczy też się zdarzają, albo odzyskać sobie hasło administratora na swój adres e-mail, jeśli się poda ten adres e-mail po średniku w polu login. Mnóstwo jest różnych błędów, ale od tego są eksperci, że oni znają te setki, czy tysiące błędów i pod kątem tych błędów testują daną platformę. A jeśli ktoś naprawdę poważnie podchodzi do bezpieczeństwa, to warto było by, żeby te teksty rozszerzył właśnie o pracowników. Czyli, żeby wykonał taki scenariusz ataku na Biuro Obsługi Klienta „dzień dobry, mam na imię Jacek, ja kupowałem ostatnio taki tutaj produkt mam z nim taki i taki problem.” Jaka jest procedura i czy ja mogę w sposób nie autoryzowany np. za pomocą rozmowy z takim pracownikiem Biura Obsługi Klienta wyciągnąć adres Pana Jacka. Ja nie jestem Jackiem, ja udaję, że jestem Jackiem. Mnie interesują dane Jacka, często pracownicy w dobrej wierze, próbując pomóc klientowi coś tam podpowiedzą np., gdzie podesłać kuriera po ten sprzęt. Ja powiem „no właśnie nie wiem, a jaki adres miałem ostatnio podany, bo się przeprowadzaliśmy.” „Ja tutaj mam ul. Armii Krajowej 12” „Dziękuję, o to mi chodziło, tak, na Armii niech będzie.” Jak ja zbieram jako atakujący informację o kimś, kto wiem, że był klientem danego sklepu, a mogę widzieć, że był klientem danego sklepu, bo np. sprawdzę sobie, czy mogę się zalogować na jego adres e-mail do platformy i mi wyskakuje błędne hasło, ale to jest potwierdzenie, że taki użytkownik jest, bo na komunikatach, które nie są niejednoznaczne można to określić. To jestem w stanie wyciągnąć informacje, pewne informacje. Mogę wreszcie wyłudzać, robić jakieś zwroty, sprawdzić, czy w ten sposób da się wygenerować już realne straty związane z tym, że np. może nie przytaczajmy konkretnych przykładów, ale są pewne scamy, które można odegrać na obsłudze sklepów internetowych Biurach Obsługi Klient. W taki sposób, żeby przekierować przysyłkę, żeby pozyskać towar, który jeszcze nie został opłacony, albo został opłacony przez osobę, która wcale nie powinna

mieć do niego dostępu. To są bardziej bym nazwał błędy nie techniczne, a procesowe. Jeśli nie mamy odpowiednich procesów w naszym w przypadku sklepie internetowym, chociaż naprawdę to dotyczy firmy, bo my się tutaj skupiamy na sklepach internetowych, ale to samo jest u dostawców energii, to samo jest w różnych innych biznesach, które oferują, jakąś wartość lub, z których można pewne usługi wyłudzić, więc takie procesy powinny być dograne. Myślę, że w takiej kolejności bym to robił, bo rzeczywiście pierwszym najpopularniejszym problemem są te ataki masowe, aktualizacja nam je rozwiąże. Drugim są te ataki masowe, które wykorzystują pewne błędy. To testy bezpieczeństwa, monitoring powinien nam to rozwiązać. A trzecim są wykwalifikowane, konkretne rzeczy, które polegają na pewnych wyłudzeniach. Ktoś odkrył coś, zauważył pewną lukę w sposobie myślenia, czy działania danej platformy i np. generuje sobie kody zniżkowe, albo generuje karty lojalnościowe. Je łączy i zanim się serwis zorientuje, co się dzieje, albo dlaczego mu pieniądze wypływają, co wyjdzie na jakimś remanencie, podsumowaniu kwartalnym, to już będzie za późno.

G.F: Piotr, bo wiele sklepów mniejszych, większych nie robi takich rzeczy, bo boi się wielu rzeczy. Czy to czasu, czy to skomplikowania, czy to ceny. Jeśli mamy te 3 sposoby, to jeśli mamy administrację, czy aktualizacje, to jeśli jesteśmy na SASach to zazwyczaj nasz pracownik to robi. Jeśli mamy opensource typu PrestaShop, Magento i parę innych jeszcze to w tym momencie warto mieć firmę, która jest programistycznie ogarnięta i potrafi te rzeczy ogarniać, poustawiać już, nie mówiąc o samych serwerach, które administratorzy serwera to zrobią. Plus szybka aktualizacja rozwiązań. Monitoring ja przyznaję, że w monitoringu akurat u nas w firmie nie jest to jakieś wielkie. Jest to, gdzieś tam jeszcze jakby to powiedzieć zaniedbane. To mówię tak otwarcie. Natomiast część robimy, część nie robimy, więc to jest na pewno dopracowanie z naszymi klientami, to też jest kwestia właśnie ceny. Rozumiem, że takie usługi monitoring poszczególnych to można kupić jako usługę. To są firmy, czy bardziej oprogramowanie, jak to z Twojej strony wygląda? Jak Ty to oceniasz? Co lepiej kupić, bo pewnie jest usługa i są automatyczne narzędzia, które robią monitoring. To się samemu nie uda zrobić.

P.K: Każde automatyczne narzędzie, które nie tyle robi monitoring, co gdzieś patrzy, w jakiejś logi, sygnały i może wysłać takie powiadomienie „tu dzieje się coś problematycznego” musi być zarządzane przez człowieka. Ktoś musi czytać logi i analizować. Są różnego rodzaju Security Center, które można wynająć i siedzą ludzie 24 godziny na dobę i patrzą. Obsługują wielu klientów i patrzą, czy świeci się gdzieś lampeczka na czerwono i trzeba reagować,

eskalować. Czy można to olać, bo jest to tzw. fail positive, których też jest dość sporo. Natomiast ja zachęcałbym przede wszystkim do podejścia takiego bardziej in house. Nikt nie zna tak dobrze naszej platformy, jak my. Naszych integracji, to, że ktoś ma sklep na Preście, czy na innym rozwiązaniu, to nie oznacza, że druga osoba, która korzysta z tego samego stacku technologicznego, ma wszystko tak samo skonfigurowane i to samo ryzyko biznesowe. W związku, z czym dobrze byłoby jednak kogoś swojego od IT, kto na to spojrzy, podepnie się pod odpowiednie mechanizmy i sprawdzi odpowiednie logi. Skonfiguruje to i wtedy ewentualnie da to do patrzenia komuś. Nawet nieprzeszkolonym osobom, bo to polega na tym, że wiesz ważna jest ta reakcja. Tą reakcje, jeśli się coś zaświeci na czerwono może wykonać z całym szacunkiem podrzędny pracownik, nie techniczny pracownik Call Center, czy Biura Obsługi Klienta. Tylko on musi dać znać, zadzwonić do kogoś i powiedzieć, że np. dzisiaj nasz Pan Staszek informatyk jest na urlopie i dzwonimy do Pana Józka, albo Pana Mietka. To jest ta kwestia, której po prostu nie można zaniedbać. A nawet, jeśli to jest zbyt skomplikowane bądź zbyt drogie dla wielu. To i tak warto ten mechanizm logowania skonfigurować, bo robimy to raz, a on jest nie ocenioną pomocą, kiedy dojdzie do incydentu i trzeba się zorientować, co tu się stało. Którędy oni weszli, do czego mają dostęp, co straciliśmy, co musimy zgłosić do PUODO, co nie musimy zgłaszać. My musimy to wiedzieć, a jeśli nie mamy logów, to tego nie wiemy, albo zakładamy najczarniejszy scenariusz zupełnie nie potrzebnie, stresując też wtedy klientów. Także mądry Polak po szkodzie. Ja znam takie przypadki, gdzie do klientów na analizę incydentów wchodzimy, próbujemy mieć dostęp do logów, bo to jest pierwsza rzecz, którą generalnie się realizuje, a logi są wyłączone. Pytamy się klienta „dlaczego logi są wyłączone?" Za chwilę jest to „ja sprawdzę, tutaj szef programistów" i wraca odpowiedź „a, bo my mieliśmy taką promocję i jak dużo osób wchodziło to nam zamulało i zauważyliśmy, że jak wyłączyliśmy logi, to działał szybciej serwis." Pytam „kiedy mieliście tą promocję?" „no 2 lata temu na Święta, ale już nigdy potem nie włączyliśmy tych logów."

G.F: No tak człowiek zapomina.

P.K: No to pięknie. Teraz dowiedź się, co, którędy i jak. Czasem jest to możliwe, czasem jest to bardzo utrudnione. Czasem jest to nie możliwe, więc warto, żeby wszyscy mieli świadomość, że są pewne rzeczy, które mogą nam pomóc się odnaleźć po incydencie, albo ułatwić obsługę incydentu, albo nawet uniemożliwić wystąpienie incydentu. Tylko o tym trzeba pomyśleć teraz, już zanim to się zdarzy. To nie jest tak, że po wypadku możemy sobie poduszkę powietrzną włączyć, albo pasy zapiąć, jak były niezapięte niestety. Warto te pasy i

tą poduszkę skontrolować wcześniej, zapiąć wcześniej, co nie oznacza, że przeżyjemy. Znamy przypadki takich ataków, wypadków, gdzie ktoś, kto jedzie 300km/h pomimo tych mechanizmów bezpieczeństwa poprawnie skonfigurowanych, poprawnie działających i tak nie przeżyje. Takie sytuacje też się zdarzają. Ja, jednak gdybyś mnie zapytał, czy wolę mieć przy wypadku samochodowym zapięte pasy i pewność, że moja poduszka powietrzna jest serwisowana i dobrze działa, to bym Ci odpowiedział, że wolałbym mieć do dyspozycji tą poduszkę, kurtyny boczne i pasy bezpieczeństwa. To minimalizuje, nie eliminuje ryzyka. Myślę, że o tym musimy wszyscy pamiętać, że 100% incydentu nie da się wyeliminować. Natomiast da się do incydentu dość dobrze przygotować i dzięki temu nie wpadać w panikę, kiedy to nastąpi. Wiedzieć, co mamy robić, podążać zgodnie z procedurą i spać spokojnie, że nawet jeśli gdzieś po drodze był jakiś problem, to on jest mniej zawiniony, a przez to być może w oczach różnych urzędów nadzorczych, czy też nawet naszych klientów będzie on rozpatrywany jako zrobili wszystko, co mogli po prostu nie wyszło. Zachęcam do prześledzenia kilku ujawnionych incydentów, reakcji firm na te incydenty i reakcji społeczeństwa na te incydenty np. na Facebooku, gdzie jest informacja o tych incydentach. Są marki, które dały ciała, opisują incydent i ludzie mówią „jesteśmy z Wami, nic się nie stało, przeżyjemy, trzymamy kciuki". Ja już znam kogoś kto może Wam pomóc w tym i w tamtym aspekcie. A są marki, które mówią o incydencie i wszyscy wieszają na nich psy. Chyba tak to się mówi najbardziej delikatnie. Życzę wszystkim, żeby byli w tej pierwszej grupie, ale to wymaga pewnych relacji z klientem i też pokazania, co się wcześniej robiło. Internauci nie są głupi oni wyczują, co robimy. W związku z czym dobrze jest mieć pewne dowody, które pokażą, że robiliśmy wszystko, co mogliśmy. Współpracowaliśmy z taką firmą, tym się zajmowali inni eksperci, bo my nie jesteśmy ekspertami od bezpieczeństwa, my jesteśmy ekspertami od sprzedaży, od produkowania toreb skórzanych, od robienia karmazynowych butów, czegokolwiek innego. Daliśmy to profesjonalistom, mamy teraz ogląd sytuacji, wygląda na to, że stało się to, to i to. My zawiniliśmy w tym aspekcie, albo tu nie ma w ogóle naszej winy, zawinił ktoś inny, albo jest jeszcze jakiś inny przypadek. Tak to wygląda, bo jesteśmy transparentni. Tego myślę jeszcze brakuje na polskim podwórku, takiej transparentności i takiego post mortem po danym incydencie, który pokazuje wprost, co się stało.

G.F: Tak, rzeczywiście to jest tak, że te nawet największe banki i instytucje, e-commerce pomimo setek tysięcy, milionów i dziesiątków milionów i tak padają ofiarą ataków i nie

potrafią sobie z tym poradzić, bo czekają właśnie na taką dziurę przez rok, bo oni mają czas, bo się nastawiają.

P.K: Tak, tylko wiesz, czym innym jest sytuacja, w której Ty mówisz „włamali się do mnie i wykradli moje dane, bo miałem hasło dupa123 i żadnego MFA", a czym innym jest, kiedy mówisz „wykradli wasze dane drodzy klienci, ale błąd był w bibliotece, która należała do firmy X, która nam wdrażała rozwiązanie Y i niestety ten błąd on nie był wcześniej opublikowany to jest pierwsze użycie tego błędu tzw. zero day. My współpracujemy z firmą XYZ, która oceniła na podstawie logów, które na szczęście mieliśmy skonfigurowane, że zakres tego włamania dotyczy tylko klientów z poprzedniego roku, bo przy okazji, wdrażając zalecenia po raporcie z testów bezpieczeństwa, które robiliśmy 2 lata temu, zaczęliśmy kasować toksyczne dane, których nie potrzebujemy, a które w wyniku ataku mogłyby zostać wykradzione. Także każdy z Was kto robił zakupy więcej, niż 6-12 miesięcy temu niech się nie przejmuje, bo waszych danych w ogóle nie było na naszej platformie." A nie, jak w niektórych platformach, gdzie ja skasowałem konto w sklepie X, dane wyciekają 5 lat później, a moje dane w tej bazie są. Dlaczego? Dlatego że, co oni zrobili, jak ja skasowałem konto, ale widzę, że w bazie danych jest rubryka skasował konto: tak, tak, nie, tak, nie, nie, a te dane dalej tam są. Jaki jest sens kasowania konta, jak ktoś dalej te dane trzyma w bazie? Po co to trzyma? Można byłoby to zrobić lepiej, rozsądniej.

G.F: To już inna historia. Piotr bardzo Ci dziękuję za podzielenie się doświadczeniem i pokierowaniem nas od A do Z w tej całej branży. Myślę, że ten temat rozwiązań, szukania, administracji, monitoringu, przetestowania, itd., to jest oddzielna para kaloszy i myślę, że jeszcze możemy się umówić na rozmowę. Jeśli przyjmiesz moje zaproszenie, a tymczasem bardzo dziękuję Ci za podzielnie się i powiedz mi. Czego Ci życzyć na sam koniec?

P.K: Spokoju.

G.F: Brakuje Ci ostatnio? Dużo się dzieje?

P.K: Wiesz co? Dużo się dzieje wszystkiego. Niestety to bezpieczeństwo przez lata było na naszym rynku bagatelizowane. W związku z czym teraz każdy, kto tym bezpieczeństwem się zajmuje ma po prostu ręce pełne roboty. Czasem do tego stopnia, że trzeba te ręce rozłożyć w geście politowania i powiedzieć, że komuś nie można już pomóc, bo pomaga się innym osobom i zasoby są pod korek zajęte. To też informacja dla osób, które chcą się przebranżowić. Dobra branża to bezpieczeństwo – wchodzić.

G.F: Wchodzić. Jakby, co to pewnie Piotr szuka dobrych speców dobrze mówię?

P.K: Zapraszam. W każdej ilości.

G.F: W każdej ilości widzicie. To tak trochę, jak w e-commerce. U nas też każdego e-commerce menagera się bierze. Dobrego z podziękowaniem wielkim. Wielkie dzięki Piotr i do usłyszenia, do zobaczenia.

P.K: Do usłyszenia! Cześć!