Ewelina: Dzień dobry, bardzo miło mi powitać wszystkich w kolejnym odcinku. Dzisiaj mam przyjemność podyskutować z Kamilem Porembińskim, który zajmuje się m.in. marketing technology. Cześć!

Kamil: Cześć. Miło was słyszeć.

Ewelina: Kamil, od ponad 15 lat pomagasz freelancerom, firmom w informatyzacji marketingu, zwiększaniu dostarczalności kampanii mailingowych, stron internetowych. Czym jeszcze się zajmujesz się człowieku orkiestro?

Kamil: Tak naprawdę odkąd poznałem ten internet, to staram się w sumie rozjaśniać i tłumaczyć, jak działa internet przedsiębiorcom. Bardzo często spotykam się z osobami, które prowadzą biznes, jakiś sklep www, mailingi, ale zawsze odpowiadają: "Ja nie jestem techniczny, nie znam się". Próbuję to odczarować i wyjaśnić, że to nie jest takie skomplikowane i te rzeczy technologiczne nie są trudne. Przykładając się do nich i panując nad nimi sprawimy to, że nasze maile będą docierały lepiej. Ludzie będą je czytali, czy chociażby nasza strona www przeżyje w Black Friday a nie zostanie ofiarą sukcesu kampanii marketingowych. Wyobraźmy sobie tą sytuację, że wszyscy w jednym momencie wchodzą na sklep internetowy, przygotowaliśmy super promocję, a ten serwer, gdzie stoi nasz sklep, nie działa. Staram się robić tak, aby te biznesy przetrwały w sieci. Prywatnie zajmuję się nurkowaniem.

Ewelina: W międzyczasie pochwaliłeś mi się, że też jesteś podcasterem.

Kamil: Tak, z racji pasji do nurkowania założyłem podcast jedyny taki w Polsce "Podcast spod wody" - podcast o nurkowaniu.

Ewelina: Chciałam dzisiaj skupić się na temacie bezpieczeństwa przedsiębiorców działających w sieci. Czy zgadzasz się z tym, że bezpieczeństwo to jedno z najważniejszych aktywów w każdym przedsiębiorstwie?

Kamil: Tak, jedno z najważniejszych, ale moim zdaniem nie najważniejsze. To pewnie jest dziwne, bo jak czytamy o jakichś wyciekach internetowych, to jesteśmy przerażeni. Dlaczego jednak uważam, że bezpieczeństwo nie jest najważniejsze? Ciągłość biznesowa jest zdecydowanie bardziej istotna. Czyli to żebyśmy prowadzili biznes w sposób ciągły, nieprzerwany. Oczywiście cyberbezpieczeństwo jest jednym z elementów tej ciągłości. Przypomnijmy sobie czasy pandemii, kiedy ważniejsze było dla nas prowadzenie biznesu niż bezpieczeństwo. Nie było dylematów w stylu czy powinenem pracować z domu na prywatnym komputerze czy na firmowych zasobach, czy nagle mogę logować się cudzym hasłem gdzieś tam do sieci korporacyjnej... Ta ciągłość biznesowa była dla nas ważniejszym elementem. Dopiero po jakimś czasie w niektórych firmach pojawiły się jakieś procedury, checklisty jak robić to w sposób bezpieczny. Jednak ta ciągłość biznesowa, to też również odporność na ataki internetowe. Jeżeli dojdzie do jakiegoś ataku, to przestaje nasz biznes działać. Cyberbezpieczeństwo jest elementem ciągłości biznesowej, czyli zapewnia, że nasza organizacja/firma może skutecznie reagować w przypadku pewnych zakłóceń.

Ewelina: Czyli to się uzupełnia...

Kamil: Tak. Kiedyś, jak pamiętam dawne ataki, polegały bardziej na uszkodzeniu, wyłączeniu ich działania. Dzisiaj te ataki są zupełnie inne.

Ewelina: Do ataków jeszcze wrócimy. Zaczepiłeś temat pandemii - czy tym samym mam rozumieć, że pandemia i rozproszone w związku z tym informację, sprzyjały wyciekom danych?

Kamil: I tak i nie. Wiele firm od dawna pracuje zdalnie i jest przygotowana na pracę zdalną, więc dostęp do tych zasobów internetowych jest chroniony. Wielu solo przedsiębiorców też pracuje od zdalnie tak jakby zdalnie. Nie ma serwera w domu, tylko ten serwer z jego sklepem/witryną jest gdzieś w internecie. Czy nawet system do Fakturownia, Fakturownia, to nie jest system, który mam gdzieś w firmie, tylko on jest online. Więc wiele tych biznesów działało zdalnie i ta pandemia de facto nie zmieniła nic. Zauważmy to, że pracując z domu tak naprawdę jesteśmy bardziej bezpieczni niż z kawiarenki internetowej, gdzie nie wiemy, skąd pochodzi ten internet. Być może ktoś w takiej kawiatni siedzi i podgląda co tam robimy. Pandemia dla solo przedsiębiorców zrobiła wiele domu. Przenieśliśmy nasz biznes w bezpieczniejsze środowisko. Patrząc jednak z punktu widzenia korporacji te wszystkie zasoby posiadające wszystko wewnątrz, musiały się otworzyć na świat. Tutaj pojawiły się zagrożenia.

Ewelina: Rozmawiałam z Kasią z Lex Digital i pamiętam, że fajnie ujęła temat wycieków danych, a mianowicie największy wyciek danych dochodził na balkonach, bo kiedy się prowadziło calle, to właśnie niejednokrotnie rozkładając pranie czy po prostu spijając kawkę o poranku słyszała kto w jakiej firmie jaki robi deal i na jaką kwotę...

Kamil: Bardzo często przesiadując w jakiejś kawiarni, naprawdę dużo zdjęć potrafię zrobić zwykłym smartfonem, bo ktoś zostawił otwarty laptop i poszedł na chwilę na toalety czy na papierosa. Pandemia jednak zminimalizowała jednak dla osoby fizycznej to niebezpieczeństwo, ale korporacje musiały zbudować jakieś zasoby wewnętrzne, które do tej pory były dostępne tylko z biurowca firmy. I tutaj pojawił się problem, bo duże przedsiębiorstwa stanęły przed wyzwaniem, czy szybko zdołamy wprowadzić metody zdalnej pracy. Czy dla nas ważniejsza jest ta ciągłość i pozwolimy im się w sposób niebezpieczny łączyć i świadczyć usługi. Prostym przykładem jest to, że w trakcie pandemii moja żona kupiła samochód i nie mogła go odebrać, bo sprzedawca nie miał dostępu do sieci. 2 dni później robił to z konta prywatnego. Ta ciągłość biznesowa była ważniejsza. To przekładało się na pogorszenie bezpieczeństwa w firmie.

Ewelina: Zaczynam prowadzić firmę, która działa online. Od czego powinnam zacząć, aby dane moje i moich klientów były bezpieczne?

Kamil: Od wyłączenia usług internetowych (śmiech) Wtedy będą super bezpieczne! Weźmy sobie to na przykładzie, np. na własnym sklepie www. Taki sklep posiada dane klientów, bazę mailingową, to rozbudowana infrastruktura, która łączy się z systemami kurierskimi. Tych danych jest sporo. Jeżeli sami stworzyliśmy ten sklep czy zrobiła nam to firma zew., to ważne

jest, by dbać o tę witrynę, tak jak dbamy o samochód. Raz na jakiś czas jeździmy na przegląd, dolewamy jakieś płyny, wymieniamy opony. To samo powinniśmy robić z naszym sklepem www. To, że nam coś wyskakuje w panelu, jakaś aktualizacja, to znaczy, że należy ją wykonać. Tak samo aktualizować komputer. Cykliczne dbanie o aktualizacje, na jakim stoi nasz e-biznes, jest bardzo fajną metodą, aby być bezpiecznym. Stare oprogramowanie ma luki, które cyberprzestępcy wykorzystują do zdobycia naszych danych. Jeżeli będziemy dbać o te aktualizacje (sami lub przez firmy zew.), już jesteśmy do przodu. Kolejna taka rzecz, to cykliczny przegląd. Raz na jakiś czas, na tydzień, na miesiąc, przeglądać czy ta witryna, ten e-biznes działa. Sprawdzić, czy formularz faktycznie wysyła maile. Najprostsza metoda - mamy jakiś sklep, e-commerce, po prostu wejdźmy na tę stronę, wypełnijmy formularz i wyślijmy miejsca. Cyberprzestępcy niekoniecznie zepsują nam całą witrynę, ale np. będą próbowali przejąć taki formularz kontaktowy, wstawić tam swojego maila jako odbiorczy no i zbierać nasze leady. Sprawdzajmy, czy da się zalogować, zarejestrować, zrobić zakup. Nawet jeśli dojdzie do błędu/ataku, to będziemy w stanie to zanalizować.

Kolejną taką rzeczą jest sprawdzanie kto gdzie ma dostępy. Stworzyliśmy ten e-biznes, daliśmy dostępy programistom, agencjom marketingowym, ale jesteśmy tu i teraz. Wdrożenie się zakończyło, a firmy, które nie powinny mieć dostępu, dalej ten dostęp mają. Być może był to jakiś zewnętrzny informatyk, który na chwilę zalogował, by coś poprawić, a my mu potem tych dostępów nie zdjęliśmy. I mimo, że my będziemy super dbali o bezpieczeństwo naszego sklepu, naszych kont, jest fajne, ale może być, że zostawiliśmy agencji, która ignoruje zasady bezpieczeństwa i to przez jej konto doszło do włamania. Takie cykliczne weryfikowane kto ma dostęp, jakie są hasła, gdzie są te hasła zapisane do naszych usług biznesowych. Możemy skorzystać z programu do przechowywania haseł. Często są to fajne, bezpłatne narzędzia, w których zapisujemy nasze hasła i dostępy do usług. One pilnują czy hasła nie wyciekły, czy są silne.

W internecie to jest tak, że jeśli cyberprzestępca ma się gdzieś włamać, to raczej nie będzie atakował naszego sklepu, gdzie są 2 rodzaje śrubek i jeden śrubokręt, ale będzie raczej atakował wszystkie witryny oparte o Wordpressa i WooCommerce, w tym i nasz sklep. Jeżeli wyjdzie jakaś luka w danym oprogramowaniu, to witryny, które mają tę lukę, zostaną złamane. Jeżeli my zrobimy aktualizację i zrobimy cykliczny przegląd, również w dostępach, to już unikniemy masowych ataków i będziemy bezpieczni.

Hasła możemy przechowywać w specjalnych programach np. One Password. One posiadają mechanizm, który potrafi sprawdzić czy nasze hasło i login nie wyciekły w jakiejś innej bazie danych. Jest też taka strona Have I Been Pwned, na której możesz wpisać swój adres e-mail i zobaczyć, czy Twój mail wraz z danymi typu hasło, nie uległ jakiemuś wyciekowi. Wracamy do naszego sklepu www. Konto administratora zakładamy na naszego maila. A tego samego maila używamy w Inpoście do wysyłania paczek. I w naszym sklepie internetowym i w InPoście używamy tego samego hasła. Być może nikt nie włamał się na nasz sklep, ale ktoś włamał się do InPostu albo tam wyciekły dane, i tego samego loginu i hasła co tam używamy w naszym sklepie, to jest duże ryzyko, że ktoś włamie się do naszego sklepu. Wniosek? Do

każdej usługi miejmy osobny login i osobne hasło. Te programy będą nam tego pilnowały. Zapisujemy sobie to wszystko w programie, który pilnuje, gdzie mamy jaki login i jakie hasło. Gdy to zrobimy, to będziemy dużo do przodu.

Idąc dalej możemy pokusić się, jeżeli prowadzimy biznes w sieci, o oddzielenie konta naszego prywatnego od konta Facebooka z naszym kontem firmowym. Możemy założyć fake konto do zarządzania tylko naszą firmą. A jeżeli ktoś chciał by się włamać, to będzie to robił na nasze znane konto.

Kolejny sposób? Włączyć wszędzie dwuskładnikowe uwierzytelnienie. Prosta metoda polegająca na tym, że po podaniu loginu i hasła musimy przepisać kod z SMS-a czy aplikacji. To fajne zabezpieczenie, bo jak nam wycieką login i hasło z innego systemu, a używaliśmy tych danych w drugim systemie, to bez tego drugiego składnika cyberprzestępca nie dostanie się do naszych usług.

Ewelina: Lista zabezpieczeń jest całkiem zasobna. Powiedzmy, że jestem jakiś czas na rynku, działam z e-biznesem i wysłuchałam twojego podcastu i zorientowałam się, że nie robię aktualizacji. Niekoniecznie aktualizowałam Wordpressa, bo bałam się, że coś mi się wysypie. I dlatego chciałabym sprawdzić, czy moje dane są bezpieczne. Czy jest jakaś opcja, aby zrobić profesjonalny audyt, który potwierdzi lub zaprzeczy, że na ten moment moje dane, hasła są bezpieczne?

Kamil: Tak. Tutaj warto dokonać podziału na małych i dużych przedsiębiorców. Jeżeli jesteśmy małą firmą i mamy prostą stronę, np. naszego podcastu, to możemy porozmawiać twórcami tej strony, żeby raz na jakiś czas wykonał ten przegląd za nas. I żeby on wykonał aktualizację. Taki programista będzie wiedział, czy aktualizacja Wordpressa nic nie wysypie. Sprawdzi i wdroży to. Jeżeli się na tym nie znamy, to samodzielnie tego nie róbmy.

W większej firmie lub gdy wiedza tych programistów nam nie wystarcza, możemy udać się do firm, które zajmują się audytami witryn. Zlecamy innej firmie włamanie się na naszą witrynę (śmiech). Kontrolowany włam. I za to jeszcze musimy zapłacić (śmiech). Lepiej zapłacić takiej firmie za włamanie, niż potem płacić cyberprzestępcom za to, że kradną nam dane. Są różne scenariusze, to my decydujemy jaką część naszego biznesu chcemy sprawdzić. Czy to mają być ataki bezpośrednio na sklep www czy być może socjotechniczny na pracowników, by od nich wyciągnąć informacje. Jeśli w testach wyjdzie, że mamy luki w technologii, to zlecamy IT ich załatanie. Jeżeli wyjdzie, że problemem są nasi pracownicy, no cóż... Trzeba zająć się ich edukacją. Raz na rok warto takie testy wykonać, szczególnie jeśli jesteśmy dużym biznesem. Było wiele wycieków dużych sklepów www, które kończyły się karami z tytułu RODO za wyciek informacji.

Ewelina: Ostatnio była nawet całkiem pokaźna sumka 5 milionów z tytułu RODO. Powiedziałeś o tym czynniku ludzkim, który czasami zawodzi. Jak zmniejszyć ryzyko wystąpienia jakichkolwiek konsekwencji w tym przypadku? Pewnie chodzi o jakieś procedury, które powinni znać nasi pracownicy. Jak je opracować, kto powinien to zrobić?

Kamil: Może być taka sytuacja, że jesteśmy dużą korporacją i przetwarzamy bardzo tajne dokumenty. Możemy wydać miliony złotych na narzędzie, które uniemożliwi kopiowanie tych dokumentów na zewnątrz - będzie blokowało kopiowanie tych plików przez pendrive, wifi itd. Ale to zabezpieczenie polegnie, jeżeli nieuczciwy pracownik zacznie robić tajnym danym zdjęcia smartfonem. Niewyedukowany pracownik może przynieść duże konsekwencje. Szkolenia, szkolenia, szkolenia i informowanie pracowników co powinni, a czego nie powinni robić.

Pandemia była fajnym przykładem - nagle na komputerach prywatnych zaczęło przetwarzać dane firmowe. Wyobraźmy sobie, że na komputerze prywatnym nie mamy zabezpieczeń, antywirusów, otwieramy jakiś ważny dokument, pocztę służbową, a za chwilę dajemy dostęp dzieciakowi do komputera, żeby obejrzał sobie bajki... Lub był na zajęciach zdalnych. No i może się okazać, że przypadkowo chciał coś zanotować i skasował dokument firmowy, bo zostawiliśmy go otwarty. Szkolenie pracowników, co mogą robić na prywatnym komputerze i co prywatnego możemy robić na firmowym komputerze, jest bardzo ważne. Warto tutaj też korzystać z zewnętrznych firm.

Z audytów otrzymamy rekomendacje, co powinniśmy robić. Gdy jesteśmy solo przedsiębiorcom, to warto pamiętać, że internet jest kopalnią wiedzy. Można np. skorzystać gotowych checklist. Ale by tego nie komplikować, wróćmy do mojego przykładu, jak zadbać o to bezpieczeństwo. Stwórzmy sami taką checklistę, co powinniśmy robić cyklicznie. Czyli my jako właściciel firmy zbudujmy checklistę dla siebie i swoich pracowników. Niech oni sprawdzają np. raz na 2 tyg, czy nasza witryna jest zaktualizowana. Raz na tydzień niech wyklikają proces zakupowy. Raz na 2 dni niech sprawdzą, czy formularz kontaktowy dalej wysyła maile i te maile do nas przychodzą. Raz na miesiąc zalogujmy się do panelu sklepu i sprawdźmy, kto ma dostęp. To samo zróbmy z FB, IG itd. Raz na 2 miesiące sprawdźmy, czy nasze maile/dane nie wyciekły, sprawdzając przez menadżera haseł. Taką checklistę możemy zbudować sami np. na bazie tego podcastu. Taki przegląd co gdzie umieszczamy, jakie dane gdzie lądują. I to już nam pozwala od czegoś zacząć.

Sprawdzajmy też, kto ma dostęp do wysyłania danych poprzez kurierów. Sprawdźmy, gdzie zapisaliśmy karty kredytowe, gdzie płacimy za takie usługi. Ta checklista będzie żyła, ale z biegiem czasu stanie się potężnym, poważnym dokumentem.

Ewelina: Dzięki. Na dzień dobry powstanie pokaźna lista. Mówiliśmy też o atakach hackerskich. Jakie typu są to ataki? Jak możesz nas na to uczulić?

Kamil: Jeżeli cofniemy się w czasie i przypomnimy sobie czasy Neostrady, to większość takich ataków polegało na podmienieniu strony www. Cyberprzestępca zdobywał dostęp do witryny i zostawiał swoje logo, motto. Chodziło o to, aby stronę uszkodzić. Dzisiaj takie ataki nie mają miejsca, bo nie są opłacalne. Dzisiaj jeżeli cyberprzestępcy się gdzieś włamują, to tylko po to, aby zarobić. Wyobraźmy sobie, że jakiś cyberprzestępca dostaje dane do wszystkich klientów systemu typu Fakturownia. Jest to przecież ogromna baza maili, kontaktów, powiązań biznesowych, numery tel, imiona, nazwiska itd. Możemy mieć dwa typy takich ataków. Jeden to

taki atak, kiedy ktoś próbuje zaszyfrować dane, które posiadamy i wtedy musimy zapłacić, aby odzyskać dostęp. Miejmy nadzieję, że jak zapłacimy, to dostęp otrzymamy. A drugi typ to taki kiedy cyberprzestępcy wkradają się na naszą witrynę, a my tego nie widzimy. Gdy nasz biznes rośnie, a oni korzystają z naszej bazy, to mogą wysyłać im np. spam. Wtedy też zarabiają. Część ataków jest trudna do wykrycia. Niektórzy cyberprzestępcy potrafili kilkanaście miesięcy być w systemach banków, a bank się nie zorientował. Korzystali z danych, analizowali to, a bank nic nie wiedział. Jeśli przerabiamy dużo danych, a nie chce nam się jej czyścić, to możemy być łakomym kąskiem dla cyberprzestępców.

Ewelina: Nie brzmi to dobrze. Dobrze, że o tym mówimy. Kamil, nadszedł kryzys. Nie ma co się oszukiwać. Powiedz mi, czy twoim daniem kryzys gospodarczy dotknie też branżę e-commerce?

Kamil: Już dotknął. Wiele branż zawiera swoje serwery i działalności i przestaje prowadziće-biznes. Koszta serwerów, łączy, prąd - to wszystko rośnie. Więc utrzymanie witryny staje się coraz droższe. Gdy do tego dorzucimy audyty, aktualizacje oprogramowania, to staje się to sporym wydatkiem.

Ewelina: Czy masz jakąś poradę na ciężkie czasy dla przedsiębiorców?

Kamil: To się połączy trochę z tymi audytami. Jeżeli zrobimy taki audyt, kto gdzie ma dostęp i okaże się, że do naszej witryny mają dostęp 2 agencje i 3 firmy SEO, to wtedy może przemyślimy, czy potrzebujemy aż tyle wsparcia. I może zrezygnujemy z kogoś i zaktualizujemy. To samo z aktualizacją - poniesiemy jej koszta, ale nasza witryna zacznie działać lepiej i szybciej, co przełoży się na tańsze utrzymanie infrastruktury serwerowej. I wtedy e-commerce będzie działał bezpieczniej, a jak bezpieczniej, to nie narazimy się na wyciek, a z tym też związane są pewne koszta. To jak z samochodem - jeśli będziemy o niego dbać ponosząc koszty, to będzie to tańsze niż nagle wymiana silnika czy rozrządu, który prędzej czy później się rozleci.

Ewelina: Kamil, jeszcze chciałabym wrócić do tematy ataków hackerskich. Widziałam na Wasze stronie, że stawiacie na pomoc w zwalczaniu działalności hackerów, spamerów i nadużyć w sieci. Czy my jako randomowi użytkownicy sieci mamy jakieś narzędzia, poprzez które możemy zgłaszać nadużycia?

Kamil: Zdecydowanie tak. To nieoczywiste i jeżeli ktoś nam się włamie na stronę, potraktujmy to jak włamanie do naszego sklepu fizycznego czy mieszkania. Jak tak się stanie, to gdzie tym pójdziesz?

Ewelina: Na policję!

Kamil: Dokładnie tak samo jest z atakami na sklepy internetowe. Możemy to zgłosić na policję. Policja ma specjalne wydziały do walki z cyberprzestępczością. Przyjmą zlecenie i podejmą śledztwo. Również gdy ktoś nas okradnie przez internet.

A jeżeli dostajemy SMS-a z podejrzanym linkiem niby od gazowni, bo zalegamy z płatnościami, możemy to zgłosić chociażby do cert.pl. Tutaj klikamy w "Zgłoś incydent". Możemy też skontaktować się pod numerem telefonu: 799448804 i przekazać, że dochodzi do tego typu ataków. Jeżeli CERT dostanie dużo podobnych zgłoszeń (np. że dany numer spamuje), to ma możliwość szybkiej reakcji i blokady.

Ewelina: Przykład z mojego podwórka: w tamtym tygodniu bliska mi osoba otrzymała 2 SMS-y z serii "zalegasz za prąd" (nie zalegała) i drugi z cyklu "dopłata do kuriera". Nie pobiegła na policję z tymi SMS-ami. Po prostu wrzuciła je do spamu. Często nie reagujemy, bo jesteśmy zasypywani spamem. A tymczasem mamy na to wpływ.

Kamil: Ale sam fakt, że ktoś nie dał się nabrać, to jest naprawdę dobre. Jeśli taki cyberprzestępca zobaczy, że jego kampania nie zarabia albo się podda, albo wymyśli coś nowego (niestety).

Ewelina: W opisie podcastu podlinkuję CERT, by każdy mógł reagować szybko i sprawnie. Powiedz, jak trafiłeś do Fakturowni?

Kamil: Jestem u was od dawna. Gdy prowadziłem jedną z wcześniejszych firm, to szukałem systemu księgowego. Teraz w Fakturowni korzystam w 2 albo 3 spółkach. W jednej spółka, która jest małą firemką, podoba mi się pakiet Micro, który kosztuje 0 zł.

Ewelina: Tak, wielu mikroprzedsiębiorców może z tego korzystać, a na płatny plan mogą przejść, gdy ich firma się rozwija.

Czy coś zmieniło się w funkcjonowaniu twojej firmy odkąd korzystasz z Fakturowni?

Kamil: Generalnie jak na początku korzystałem z fizycznych księgowych, to miałem w sumie gdzieś system fakturowania. Jakieś dokumenty przekazywałem, coś się działo i coś trzeba było płacić. Gdy przeszedłem na taki system, to zacząłem bardziej panować nad tym. To był taki naturalny audyt, gdy dodałem wszystkie faktury kosztowe, to nagle się okazało, że to są zbędne faktury, których nie powinienem płacić. Druga rzecz to szybki dostęp do dokumentów. Gdy potrzebuję konkretnej faktury, to 2 kliki i już. Księgowość 2.0. w porównaniu do tradycyjnych metod. Wszystko jest uporządkowane w sposób elektroniczny, zabezpieczone, schowane.

Ewelina: Wyobraź sobie, że możemy cofnąć się w czasie. Co byś radził sobie jako osobie początkującej w biznesie?

Kamil: Troszkę o tym opowiedziałem. Jeżeli ktoś staje się przedsiębiorcom, to trzeba skupić się na prowadzeniu firmy. Jeżeli produkowałem meble i jestem super stolarzem i nagle chcę

zajmować się firmą, to albo będę stolarzem albo będę zajmował się firmą. Moja rada: skup się na procesach firmie, księgowości i zatrudnij ludzi, którzy będą dla ciebie pracować.

Ewelina: Bardzo dziękuję ci za tę radę i wiedzę, którą się dzisiaj podzieliłeś. Myślę, że wiele osób wyciągnie owocne wnioski.