BIZNESPLAN

OPIS DZIAŁALNOŚCI 2
KLIENCI DOCELOWI 4
WYKSZTAŁCENIE, SZKOLENIA I KWALIFIKACJE 5
ANALIZA RYNKU 7
MARKETING 9
UZASADNIENIE ZAKUPÓW 10
PRZYCHODY, KOSZTY, ZYSKI 14

OPIS DZIAŁALNOŚCI

Moja działalność będzie obejmować kompleksowe usługi w zakresie testowania penetracyjnego systemów informatycznych. Zakres mojej działalności Skoncentruje się na przeprowadzaniu testów penetracyjnych, które są metodą oceny bezpieczeństwa systemów komputerowych, sieciowych, aplikacji internetowych oraz innych elementów infrastruktury informatycznej.

Oferowane usługi skupiać się będą na identyfikowaniu potencjalnych luk w zabezpieczeniach systemowych i aplikacji, które mogą być wykorzystane przez potencjalnych intruzów do nieautoryzowanego dostępu lub ataków na infrastrukturę informatyczną moich klientów. Będę przeprowadzać testy penetracyjne zarówno na żądanie klienta, jak i w formie regularnych audytów bezpieczeństwa po wcześniejszym uzgodnieniu okresów kontroli, aby zapewnić stałą ochronę przed zagrożeniami cybernetycznymi.

Jako specjalista w tej dziedzinie, posiadam wiedzę i doświadczenie w zakresie różnorodnych technologii i systemów informatycznych, co pozwoli mi skutecznie identyfikować słabości i defekty w zabezpieczeniach moich przyszłych klientów. Moje raporty z testów penetracyjnych będą zawierać szczegółowe informacje na temat znalezionych luk w zabezpieczeniach oraz zalecenia dotyczące ich naprawy i wzmocnienia.

Ponadto, jako część mojej działalności, zaoferuję także doradztwo w zakresie poprawy ogólnej strategii bezpieczeństwa informatycznego moich klientów oraz szkolenia dla personelu, aby zwiększyć ich świadomość w zakresie zagrożeń cybernetycznych i sposobów ich zapobiegania.

Moim celem jest zapewnienie klientom kompleksowych rozwiązań w zakresie bezpieczeństwa informatycznego, które pomogą im w ochronie przed coraz bardziej zaawansowanymi zagrożeniami cybernetycznymi. Jestem gotowy dostosować moje usługi do indywidualnych potrzeb i wymagań każdego klienta, zapewniając im spokój i pewność, że ich systemy są odpowiednio zabezpieczone przed atakami i wyciekami danych, co może być niezwykle kosztowne – dobrym przykładem jest tutaj firma związana z badaniami laboratoryjnymi ALAB, której baza danych zawierająca informacje wrażliwe o klientach (dane kontaktowe, schorzenia, wyniki laboratoryjne) wyciekła po uprzednim ataku hakerskim[1]. Przy regularnych audytach i wykorzystaniu technologii testów penetracyjnych, taka sytuacja nie miałaby miejsca, jednak

[1] [illegible]

firma z powodu swoich zaniedbań musiała ponieść wielomilionową karę nałożoną przez UOKiK. Warto wspomnieć, że firma po pierwszym wycieku w żaden sposób nie zareagowała i doszło do kolejnych, tym razem związanych z informacjami kadrowymi. Dlatego pentesting i cyberbezpieczeństwo jest tak niezwykle istotne przy tworzeniu jakichkolwiek serwisów i aplikacji, gdyż pozwala uniknąć wycieku danych, a także zabezpieczyć się przed nałożeniem dotkliwych kar finansowych.

Jak wygląda pentesting? Po ustaleniu z klientem obszaru działań zaczyna się etap zbierania danych na temat środowiska technicznego oraz sieci klienta. Następnie skanowane są porty, działające programy oraz systemy operacyjne w sieci klienta w poszukiwaniu podatności na ataki metodami automatycznymi jak i manualnymi. Przeprowadzane są kontrolowane, niedestrukcyjne ataki na infrastrukturę sieciową klienta w celu wykorzystania podatności i zdobycia wszelkich możliwych informacji mogących naruszyć bezpieczeństwo sieci. Po skutecznym wejściu do struktury sieciowej klienta i zdobyciu potrzebnych mi informacji tuszuję swoją obecność w sieci klienta. Ostatnim krokiem jest usunięcie się z sieci i sporządzenie raportu moich działań, które mogą usprawnić i wdrożyć strategię informatyczną, uwzględniając procedury cyberbezpieczeństwa.

Poniżej przedstawiam planowany cennik moich usług:

Usługa	Cena
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Moją rolą będzie kompleksowe prowadzenie i rozwój działalności, a także samodzielne realizowanie usług zdalnie oraz w siedzibie klienta. Będę odpowiedzialny za opracowywanie strategii biznesowej, planowanie działań oraz podejmowanie decyzji, które będą miały realny wpływ na rozwój mojej firmy. Zakres moich usług obejmie przeprowadzanie testów penetracyjnych, identyfikację luk w zabezpieczeniach systemów informatycznych oraz przygotowywanie raportów z wynikami testów. Będę także doradcą bezpieczeństwa informatycznego dla moich klientów. Moja rola polegać będzie na doradzaniu klientom w zakresie poprawy ich strategii bezpieczeństwa informatycznego oraz wspieraniu ich

w identyfikacji i eliminacji potencjalnych zagrożeń. Jako doradca, będę świadomy najnowszych trendów i technologii w dziedzinie bezpieczeństwa informatycznego oraz umiem dostosować rozwiązania do indywidualnych potrzeb i wymagań moich klientów. Oczywiście będę także zajmował się promowaniem mojej firmy poprzez np. budowanie relacji z klientami, pozyskiwanie nowych kontraktów oraz reklamowanie usług mojej działalności. Jestem osobą komunikatywną, zorientowaną na klienta i umiem skutecznie prezentować korzyści wynikające z korzystania z moich usług.

KLIENCI DOCELOWI

Moje usługi pentestingu będą skierowane do różnorodnych grup docelowych, które obejmą zarówno przedsiębiorstwa, instytucje publiczne, jak i organizacje pozarządowe. Poniżej przedstawiam główne grupy docelowe, do których skieruję moje usługi:

- **Przedsiębiorstwa korporacyjne** to duże korporacje z różnych sektorów jak np. finanse, przemysł, technologia, opieka zdrowotna itp., często są narażone na zaawansowane zagrożenia cybernetyczne ze względu na rozległe sieci i złożone systemy informatyczne. Moje usługi pentestingu będą dedykowane takim przedsiębiorstwom, pomagając im w identyfikacji i likwidacji luk w zabezpieczeniach, co przyczyni się do zwiększenia odporności na ataki cybernetyczne.
- **Małe i średnie przedsiębiorstwa**, które często nie dysponują wystarczającymi zasobami ani wiedzą, aby skutecznie zarządzać bezpieczeństwem informatycznym. Moje usługi pentestingu będą skierowane do takich firm, pomagając im w identyfikacji słabości w zabezpieczeniach i implementacji odpowiednich rozwiązań bezpieczeństwa, które pomogą im chronić swoje dane i infrastrukturę przed atakami cybernetycznymi.
- **Organizacje rządowe i sektor publiczny** są często celem ataków cybernetycznych ze względu na wrażliwe dane, które przechowują i przetwarzają. Moje usługi pentestingu będą skierowane również do instytucji rządowych i sektora publicznego, pomagając im w zabezpieczeniu swoich systemów informatycznych i danych przed nieautoryzowanymi dostępami i atakami.
- **Szkoły, uczelnie i inne instytucje edukacyjne** gromadzą dużą ilość wrażliwych danych o uczniach, studentach i pracownikach. Dlatego też są one często celem ataków cybernetycznych. Moje usługi pomogą im w identyfikacji i likwidacji potencjalnych luk w zabezpieczeniach, co pomoże w ochronie danych osobowych i infrastruktury informatycznej.

- **Organizacje non-profit, fundacje czy środowiska aktywistów** chociaż mogą działać z ograniczonym budżetem bazującym wyłącznie na sponsorach i darczyńcach, również są narażone na ataki cybernetyczne – zwłaszcza z grup wyznających inne wartości. Moje usługi mogą pomóc zabezpieczyć ich serwisy oraz dane, co pozwoli im skoncentrować się na realizacji swoich misji i celów społecznych.

Wszystkie te grupy docelowe mają różnorodne potrzeby i wymagania w zakresie bezpieczeństwa informatycznego, dlatego moje usługi będą elastyczne i dostosowywane do indywidualnych potrzeb i sytuacji każdego klienta. Dzięki mojej wiedzy jestem w stanie pomóc klientom w zapewnieniu bezpieczeństwa ich systemów informatycznych i danych, co pozwoli im skupić się na swoich głównych działaniach biznesowych i misji organizacyjnej.

Dodatkowo, chcę podkreślić, że posiadam kilka listów intencyjnych od potencjalnych klientów, którzy wyrazili chęć skorzystania z moich usług po uruchomieniu działalności. Jest to sygnał o realnym zapotrzebowaniu na planowane przeze mnie usługi. Deklaracje współpracy dołączam do wniosku.

WYKSZTAŁCENIE, SZKOLENIA I KWALIFIKACJE

[illegible]

[illegible]

[illegible]

- [illegible]
- [illegible]

- Identyfikacji systemów operacyjnych w celu zoptymalizowania ataków.
- Zdobywania informacji ze źródeł publicznych w celu przyjęcia strategii ataku.
- Identyfikowania luk w zabezpieczeniach.
- Oceniania zgromadzonych informacji w zakresie możliwych naruszeń.
- Kompilowania pozyskanych danych z plików.
- Zdobywania informacji o użytkownikach sieci/systemu.
- Przesyłania plików w inne miejsca w celu zabezpieczenia ich posiadania po ataku (umożliwia to także usunięcie danych u klienta i żądanie okupu – co jest niezwykle częstą praktyką w cyberprzestępczości podczas ataków na duże przedsiębiorstwa, a także organizacje publiczne).
- Zbierania danych logowania (w tym zakodowane hasła).
- Identyfikowania i modyfikowania tzw. exploitów.
- Minimalizowania możliwości wykrycia podczas przekierowywania strumienia danych.
- Identyfikowania luki w zabezpieczeniach aplikacji internetowych.
- Lokalizowania ukrytych plików i katalogów.
- Przeprowadzania tzw. ataków brute-force oraz wiele innych.

[illegible]

- Praca na najpopularniejszych systemach serwerowych (Linux, Windows Server).
- Omijanie zabezpieczeń sieciowych.
- SIEM i SOC.
- Przyznawanie przywilejów (np. administratora) w sieci atakowanego celu;
- Wykorzystywanie języków programowania w celu przeprowadzania ataków hakerskich.
- Testy penetracyjne w aplikacjach webowych, desktopowych i mobilnych.

Posiadam również certyfikat znajomości **języka angielskiego na poziomie C1**, co jest niezbędne w celu świadczenia profesjonalnych usług z cyberbezpieczeństwa, nie tylko dla międzynarodowych klientów, ale również i polskich, gdyż całość świata informatycznego bazuje przede wszystkim na języku angielskim i w taki sposób również tworzona jest infrastruktura IT we wszystkich na świecie firmach. Wszystkie posiadane przeze mnie certyfikaty dołączam do wniosku.

ANALIZA RYNKU

Cyberbezpieczeństwo to obszar dziedziny informatyki, w którym bardzo ciężko jest znaleźć zatrudnienie, a jeszcze ciężej stworzyć własną działalność gospodarczą w tym zakresie. Nie wynika to wcale z przesycenia rynku tą specjalizacją – wręcz przeciwnie, specjalistów z zakresu cyberbezpieczeństwa wciąż brakuje i jest to jeden z najbardziej opłacalnych i potrzebnych sektorów IT na podstawie ostatniego raportu JustJoinIT.

Trudno rozpocząć pracę w tym segmencie, ponieważ wymagana jest naprawdę ogromna wiedza, a w przypadku działalności gospodarczych – potwierdzenie rzetelności swoich usług. Niewiele osób decyduje się na taką karierę, ponieważ kursy potwierdzające kwalifikacje w cyberbezpieczeństwie i jednocześnie zwiększające rzetelność specjalistów prowadzących własną działalność są niezwykle kosztowne – sam ukończyłem wcześniej wspomniane szkolenie HackerU Red Team, które wyniosło ok. 23 000 zł za niecałe 600 godzin praktycznych zajęć. Dlatego konkurencja na rynku jest bardzo niewielka i osobie, która będzie posiadać niezbędną wiedzę oraz zdobędzie certyfikaty potwierdzające kompetencje z cyberbezpieczeństwa, będzie dużo łatwiej wejść na rynek.

Obecnie w Polsce znajduje się garstka przedsiębiorstw i startupów ze sporym finansowaniem, które zajmują się testami penetracyjnymi. Dla większości polskich przedsiębiorstw, organizacji i instytucji jest to zbyt duży wydatek, choć warto odnotować fakt cyklicznego wzrostu budżetu przeznaczanego na cyberbezpieczeństwo[2].

[illegible]

[2] [illegible]

przez co usługi są bardzo kosztowne. Większość przedsiębiorstw (zwłaszcza polskich), które nie są ogromnymi korporacjami, nie może pozwolić sobie na cykliczne korzystanie z testów bezpieczeństwa i ograniczają się do stosunkowo rzadkich (nowe metody ataków są cyklicznie tworzone przez cyberprzestępców, dlatego ważne, by testy były przeprowadzane regularnie) kontroli wydajności systemów ochronnych.

Bardzo dobrym rozwiązaniem w tym przypadku jest korzystanie z usług jednoosobowych działalności gospodarczych, których w Polsce nadal jest zdecydowanie za mało, wyspecjalizowanych w kontekście testów penetracyjnych, co umożliwia optymalne kosztowo kontrolowanie sieci i całej infrastruktury informatycznej. Tak naprawdę każda organizacja gromadząca jakiekolwiek dane jest narażona na ataki – szkoły, instytucje publiczne, małe, średnie i duże przedsiębiorstwa, sklepy e-commerce, zakłady produkcyjne, placówki badawcze, korporacje, uniwersytety – są to potencjalne cele cyberprzestępców, które powinny być gotowe do odparcia najnowocześniejszych form ataków. Tak szeroka grupa docelowa i stale rosnący popyt na tego typu usługi umożliwi mi szybkie stworzenie rentownej działalności gospodarczej, stały rozwój w tej dziedzinie i oferowanie moim klientom najwyższej jakości usług z zakresu testów penetracyjnych.

Z uwagi na specyfikę branży, moje potrzeby dostawcze będą ograniczone. Obecnie prowadzę rozmowy z biurem księgowym z którego usług planuję skorzystać. W razie potrzeby będę zaopatrywał się w materiały biurowe, głównie do drukowania raportów. Moimi głównymi dostawcami będą dostawcy oprogramowania.

MARKETING

Zdaję sobie sprawę, że by zaistnieć na dzisiejszym rynku (zwłaszcza krajowym), niezwykle istotne są działania marketingowe. Poniżej przedstawiam wstępny plan, który zamierzam realizować w celu zwiększenia rozpoznawalności firmy od samego początku jej funkcjonowania:

- Stworzenie profesjonalnej strony internetowej z dokładnym opisem usług, danymi kontaktowymi i cennikiem.
- Zlecenie zaprojektowania identyfikacji wizualnej firmy.
- Opracowanie strategii content marketingowej, która może obejmować tworzenie treści na blogu i publikacje w mediach społecznościowych.
- Aktywne prowadzenie kont firmowych w mediach społecznościowych (Facebook, Instagram, TikTok, Twitter).
- Opracowanie strategii SEO dla poprawy widoczności w wynikach wyszukiwania.
- Planowanie działań promocyjnych, konkursów, akcji rabatowych itp. – zwłaszcza w celu przyciągnięcia klientów z segmentu małych i średnich przedsiębiorstw oraz instytucji.
- Realizacja działań public relations, współpraca z mediami, konferencje, wystąpienia publiczne – zwiększanie świadomości na temat cyberbezpieczeństwa w biznesie;
- Zlecenie stworzenia kampanii reklamowych Google Ads, Facebook Ads i LinkedIn Ads.
- Udział w targach branżowych, konferencjach i festiwalach, gdzie można promować usługi i nawiązywać kontakty biznesowe.
- Zachęcanie klientów do udostępniania opinii i recenzji o usługach na stronie internetowej czy w mediach społecznościowych.
- Współpraca z influencerami lub osobami znanymi w branży, którzy mogą promować moje usługi w swoich kanałach społecznościowych lub na swoich blogach.

Jestem przekonany, że powyższe działania będą w zupełności wystarczające i - co najważniejsze w branży cyberbezpieczeństwa – przedstawią mnie w roli eksperta ds. testów penetracyjnych.

UZASADNIENIE ZAKUPÓW

Komputer stacjonarny jest podstawowym wyposażeniem w tego rodzaju działalności gospodarczej. Jest to kosztowny sprzęt, jednak każdy jego podzespół ma swoje zastosowanie w testach penetracyjnych. Proces testów penetracyjnych wymaga od komputera pracy w zróżnicowanych warunkach oraz wykorzystania specjalistycznych narzędzi i programów. Wysokiej wydajności procesor, który stanowi sporą część tej kwoty, jest kluczowy dla szybkiego przetwarzania dużej ilości danych i wykonywania skomplikowanych operacji, które są często potrzebne podczas testów penetracyjnych. Procesory z wieloma rdzeniami i wysokimi częstotliwościami zegarowymi mogą przyspieszyć proces analizy i testowania systemów, co w przypadku bardziej skomplikowanych rozwiązań cyberbezpieczeństwa jest niezwykle istotne. Duża ilość pamięci RAM pozwala na jednoczesne wykonywanie wielu zadań i obsługę złożonych aplikacji i narzędzi testowych. Testy penetracyjne wymagają pracy z dużymi zbiorami danych i złożonymi programami, więc wystarczająca ilość pamięci RAM jest kluczowa do optymalizacji prowadzonych testów. Szybki oraz pojemny dysk SSD umożliwi sprawny dostęp do danych i szybkie uruchamianie aplikacji, a także przechowywanie pozyskanych informacji, co jest kluczowe podczas kontrolowanych ataków, gdzie czas reakcji i dostęp do zasobów systemowych ma kluczowe znaczenie. Kolejną sporą składową kwoty jest karta graficzna. Jej moc obliczeniowa jest konieczna w testach penetracyjnych, ponieważ wiele zastosowanych w nich technik i narzędzi opiera się na szybkim przetwarzaniu dużych ilości danych. Karty graficzne, zwłaszcza te z wysoką mocą obliczeniową, potrafią przyspieszyć operacje związane z analizą danych, szyfrowaniem, dekodowaniem czy tworzeniem wizualizacji. Jest to niezbędne do profesjonalnego testowania infrastruktury informatycznej, gdyż zapewnia wymaganą szybkość wykonywania konkretnych operacji w procesie audytu. W testach penetracyjnych często wykorzystuje się algorytmy szyfrowania, łamanie haseł, analizę pakietów sieciowych oraz tworzenie graficznych prezentacji wyników. Moc obliczeniowa karty graficznej jest niezbędna, aby znacznie przyspieszyć te procesy, skracając czas potrzebny na wykonanie skomplikowanych obliczeń. Dzięki temu testy penetracyjne będą wykonywane bardziej efektywnie i sprawnie, co jest konieczne w środowisku, gdzie czas jest często czynnikiem kluczowym. W rezultacie, karta graficzna o dużej mocy obliczeniowej ma znaczący wpływ na wydajność i efektywność procesu testów penetracyjnych, co przełoży się na osiągnięcie wymaganych rezultatów i szybkie wykrywanie potencjalnych luk w zabezpieczeniach systemów informatycznych. Jedynie taki zestaw komputerowy pozwoli mi na realizowanie oferowanych usług w sposób profesjonalny.

Laptop, który planuję kupić, oferuje wysoką wydajność obliczeniową, co jest kluczowe podczas przeprowadzania testów penetracyjnych w terenie, czyli w siedzibie klienta. Dzięki potężnym procesorom, kartom graficznym oraz dużej ilości pamięci RAM, laptop ten może obsłużyć zaawansowane narzędzia i aplikacje używane do skanowania, analizowania oraz penetracji sieci i systemów klienta. Laptop ten charakteryzuje się solidną konstrukcją i trwałością, co jest istotne podczas pracy w różnorodnych warunkach środowiskowych, typowych dla testów penetracyjnych na miejscu klienta. Ergonomiczna klawiatura, wygodny touchpad oraz matryce o wysokiej rozdzielczości, są niezbędne dla efektywności podczas przeprowadzania testów penetracyjnych w terenie. Jest to także ważne z perspektywy zdrowia – ergonomia urządzeń peryferyjnych pozwala na zmniejszenie ryzyka powstawania zwyrodnień, jak np. zespół cieśni nadgarstka, czy w przypadku matrycy – problemów ze wzrokiem, jak np. zaćma czy znamiona barwnikowe. Istotną cechą sprzętu jest także zaawansowany system chłodzenia, który jest niezbędny w utrzymaniu niskich temperatur podczas intensywnego obciążenia sprzętu spowodowanego testami penetracyjnymi, co z kolei wpływa na konieczną stabilność pracy i wydajność urządzenia. Wydajność oraz chłodzenie laptopa są tak naprawdę kluczowymi czynnikami, które w ogóle umożliwiają realizowanie takich usług w siedzibie klienta. Dodatkowo – aspekty mobilne takie jak kompaktowa konstrukcja, niska waga oraz długi czas pracy na baterii są dodatkowym atutem przemawiającym na korzyść tego zakupu, ponieważ dzięki temu będę miał możliwość przeprowadzenia złożonych testów w miejscach wyznaczonych przez klienta, co jest konieczne, abym mógł świadczyć planowane usługi.

Dysk zewnętrzny jest niezbędny, aby zapewnić dużą ilość miejsca na przechowywanie danych. Testy penetracyjne generują mnóstwo informacji, a do tego konieczne jest, aby przechowywać kopie zapasowe, logi, obrazy dysków oraz inne pliki. Dysk o dużej pojemności zapewni mi konieczną przestrzeń na przechowywanie tych danych bez konieczności usuwania ich w celu zwolnienia miejsca, co jest istotne podczas obsługi wielu klientów. Dysk SSD pozwala na szybkie transfery danych, co jest kluczowe podczas przenoszenia dużej ilości informacji między różnymi urządzeniami. Sprzęt ten jest również wyposażony w mechanizmy zabezpieczające jak np. szyfrowanie, co jest niezbędne, abym mógł chronić poufne informacje przed nieuprawnionym dostępem. W branży cyberbezpieczeństwa, gdzie pracuje się z wrażliwymi danymi klientów, bezpieczeństwo danych jest kluczowe. Testy penetracyjne będą przeprowadzane w różnych lokalizacjach, a przenośny dysk umożliwi mi konieczne przenoszenie danych między różnymi miejscami pracy.

Urządzenie wielofunkcyjne oferuje funkcje drukowania, skanowania i kopiowania, co jest kluczowe dla tak naprawdę każdej działalności gospodarczej. Urządzenie to jest niezbędne do wydruku dokumentów firmowych, faktur, a także analiz i raportów z testów, umów czy innych materiałów koniecznych podczas wizyt u klientów. Wybrane przeze mnie urządzenie charakteryzuje się niskimi kosztami eksploatacji dzięki zastosowaniu systemu zbiorników z atramentem, co sprawia, że jest bardziej ekonomiczne w użytkowaniu w porównaniu do innych urządzeń. To istotne, gdyż będę często używać drukarki do wydruku raportów i dokumentacji związanych z kontrolą infrastruktury sieciowej. Zakup tego urządzenia jest również konieczny ze względu na to, że oferuje ono łatwą integrację z różnymi systemami operacyjnymi oraz sieciami, co pozwoli mi na bezproblemowe podłączenie urządzenia do infrastruktury sieciowej klienta, a to z kolei jest niezbędne, aby świadczyć usługi u klienta.

Monitor jest niezbędny, aby zapewnić wysoką jakość obrazu i szeroki zakres kolorów, co jest istotne podczas analizy danych związanych z testami penetracyjnymi. Precyzyjne odwzorowanie kolorów i szczegółów jest niezbędne do identyfikacji wzorców, anomalii oraz potencjalnych zagrożeń w systemach i sieciach. Duża przestrzeń robocza pozwoli na jednoczesne wyświetlanie wielu aplikacji, okien i dokumentów, co jest konieczne do osiągnięcia odpowiedniej efektywności pracy podczas testów penetracyjnych. Monitor jest niezbędny, abym mógł skutecznie korzystać z komputera stacjonarnego, a tym samym świadczyć usługi.

Krzesło biurowe jest niezbędne dla efektywnego prowadzenia działalności, gdyż większość zadań wymaga wykonywania ich przy komputerze. Ergonomiczny design i wysoka jakość wykonania tego wybranego modelu są kluczowe, ponieważ minimalizują ryzyko problemów zdrowotnych związanych z długotrwałym siedzeniem, takich jak bóle pleców czy schorzenia kręgosłupa. Dlatego właściwe dopasowanie krzesła biurowego do potrzeb ergonomicznych jest niezbędne dla zapewnienia wydajności pracy oraz zapobieżenia potencjalnym chorobom zawodowym.

Słuchawki nauszne z mikrofonem są niezbędne, abym mógł efektywnie komunikować się zarówno z klientami, jak i członkami zespołu informatycznego. Dźwięk wysokiej jakości zapewni klarowną i wyraźną komunikację, co jest kluczowe podczas rozmów. Dzięki wyciszeniu zewnętrznego hałasu i komfortowym nausznikom mogę pracować przez długie godziny bez zmęczenia, co jest kluczowe dla efektywności mojej pracy. Solidna konstrukcja tych słuchawek zapewnia ich niezawodność, co czyni je nieodzownym narzędziem dla mojej produktywności i skuteczności w wykonywaniu zadań.

Klawiatura komputerowa jest niezbędnym narzędziem podczas codziennych zadań wykonywanych na komputerze stacjonarnym. Jest to podstawowe urządzenie wejściowe, które umożliwi mi konieczną interakcję z komputerem. Dodatkowo, możliwość programowania skrótów klawiszowych (którą oferuje ta klawiatura) jest niezbędna, aby zwiększyć efektywność pracy, zwłaszcza podczas wykonywania powtarzalnych zadań czy szybkiego dostępu do często używanych funkcji.

Mysz komputerowa jest niezbędna podczas przeprowadzania testów penetracyjnych, zwłaszcza podczas operacji, które wymagają precyzyjnego sterowania kursora, takich jak analiza pakietów sieciowych, czy przeglądanie kodu źródłowego. Ergonomia myszki jest kluczowa dla użytkowników, którzy spędzają długie godziny przed komputerem, a moje przyszłe zajęcie zawodowe właśnie do tego się sprowadza.

PRZYCHODY, KOSZTY, ZYSKI

Lp.	KATEGORIA	Kwiecień	Maj	Czerwiec	Lipiec	Sierpień	Wrzesień
A	**PRZYCHODY**	**12 000 zł**	**12 000 zł**	**12 000 zł**	**13 000 zł**	**13 000 zł**	**13 000 zł**
B	**KOSZTY, W TYM:**	**3 750 zł**	**3 750 zł**	**3 750 zł**	**3 770 zł**	**3 770 zł**	**3 770 zł**
	Materiały biurowe (tonery, papier)	200 zł	200 zł	200 zł	200 zł	200 zł	200 zł
	Czynsz (w tym opłaty eksploatacyjne)	1 100 zł	1 100 zł	1 100 zł	1 100 zł	1 100 zł	1 100 zł
	Transport	310 zł	310 zł	310 zł	330 zł	330 zł	330 zł
	Koszty telekomunikacyjne (telefon, Internet)	150 zł	150 zł	150 zł	150 zł	150 zł	150 zł
	Usługi księgowe	350 zł	350 zł	350 zł	350 zł	350 zł	350 zł
	Reklama/promocja	650 zł	650 zł	650 zł	650 zł	650 zł	650 zł
	Ubezpieczenie firmy (dodatkowe)	80 zł	80 zł	80 zł	80 zł	80 zł	80 zł
	Amortyzacja komputera stacjonarnego	610 zł	610 zł	610 zł	610 zł	610 zł	610 zł
	Oprogramowanie	300 zł	300 zł	300 zł	300 zł	300 zł	300 zł
	Składki społeczne własne ZUS	0 zł	0 zł	0 zł	0 zł	0 zł	0 zł
C	**ZYSK BRUTTO (A-B)**	**8 250 zł**	**8 250 zł**	**8 250 zł**	**9 230 zł**	**9 230 zł**	**9 230 zł**
D	Składka zdrowotna własna (9%*C)	743 zł	743 zł	743 zł	831 zł	831 zł	831 zł
E	Podatek dochodowy (12%*C)	990 zł	990 zł	990 zł	1 108 zł	1 108 zł	1 108 zł
F	**ZYSK NETTO (C-D-E)**	**6 518 zł**	**6 518 zł**	**6 518 zł**	**7 292 zł**	**7 292 zł**	**7 292 zł**

Lp.	KATEGORIA	Październik	Listopad	Grudzień	Styczeń	Luty	Marzec
A	**PRZYCHODY**	**15 000 zł**	**15 000 zł**	**15 000 zł**	**16 000 zł**	**16 000 zł**	**16 000 zł**
B	**KOSZTY, W TYM:**	**4 248 zł**	**4 248 zł**	**4 248 zł**	**4 268 zł**	**4 268 zł**	**4 268 zł**
	Materiały biurowe (tonery, papier)	250 zł	250 zł	250 zł	250 zł	250 zł	250 zł
	Czynsz (w tym opłaty eksploatacyjne)	1 100 zł	1 100 zł	1 100 zł	1 100 zł	1 100 zł	1 100 zł
	Transport	350 zł	350 zł	350 zł	370 zł	370 zł	370 zł
	Koszty telekomunikacyjne (telefon, Internet)	150 zł	150 zł	150 zł	150 zł	150 zł	150 zł
	Usługi księgowe	350 zł	350 zł	350 zł	350 zł	350 zł	350 zł
	Reklama/promocja	650 zł	650 zł	650 zł	650 zł	650 zł	650 zł
	Ubezpieczenie firmy (dodatkowe)	80 zł	80 zł	80 zł	80 zł	80 zł	80 zł
	Amortyzacja komputera stacjonarnego	610 zł	610 zł	610 zł	610 zł	610 zł	610 zł
	Oprogramowanie	300 zł	300 zł	300 zł	300 zł	300 zł	300 zł
	Składki społeczne własne ZUS	408 zł	408 zł	408 zł	408 zł	408 zł	408 zł
C	**ZYSK BRUTTO (A-B)**	**10 752 zł**	**10 752 zł**	**10 752 zł**	**11 732 zł**	**11 732 zł**	**11 732 zł**
D	Składka zdrowotna własna (9%*C)	968 zł	968 zł	968 zł	1 056 zł	1 056 zł	1 056 zł
E	Podatek dochodowy (12%*C)	1 290 zł	1 290 zł	1 290 zł	1 408 zł	1 408 zł	1 408 zł
F	**ZYSK NETTO (C-D-E)**	**8 494 zł**	**8 494 zł**	**8 494 zł**	**9 268 zł**	**9 268 zł**	**9 268 zł**