

1. Wprowadzenie

Temat bezpieczeństwa w kontekście prowadzenia biura rachunkowego może być rozumiany szeroko, jako zabezpieczenie ciągłości działania przedsiębiorstwa i utrzymanie jego dochodu.

W publikacji tej koncentrujemy się na trzech obszarach:

- 1) bezpieczeństwo prawne – rozumiane jako: jasna relacja z klientem i pracownikiem biura, zdefiniowane zakresy odpowiedzialności wszystkich stron i zminimalizowanie konsekwencji błędów,
- 2) bezpieczeństwo fizyczne – rozumiane jako bezpieczeństwo: lokalu, w którym prowadzona jest działalność, sprzętu, dokumentów, a także procedur obowiązujących pracowników,
- 3) bezpieczeństwo danych – rozumiane jako zabezpieczenie przed utratą, kradzieżą lub wyciekiem poufnych danych klientów.

Publikacja nie obejmuje innych zagrożeń dla prowadzonej działalności biura, np. związanych ze zmianami prawa, sytuacją makroekonomiczną czy zagadnieniami sukcesyjno-spadkowymi.

1.1. Znaczenie bezpieczeństwa w biurze rachunkowym

Bezpieczeństwo w biurze rachunkowym ma znacznie większe znaczenie niż w wielu innych rodzajach działalności ze względu na to, że wszystko, co nam się przytrafia, może poważnie odbić się na działalności dziesiątek lub setek obsługiwanych przez nas firm:

- kilkudniowa awaria systemów może skutkować nieobliczonym na czas podatkiem i konsekwencjami finansowymi,
- działanie pracowników poza ustalonymi kompetencjami może spowodować straty, doprowadzić do sporu z klientem i podważyć naszą reputację,
- wyciek danych może ujawnić elementy działalności operacyjnej naszych klientów, a poznanie ich przez konkurencję stanowi istotne zagrożenie dla kontynuacji działalności (np. dane dostawców, wynegocjowane ceny).

Dlatego biuro rachunkowe musi dołożyć szczególnej staranności w kwestiach bezpieczeństwa.

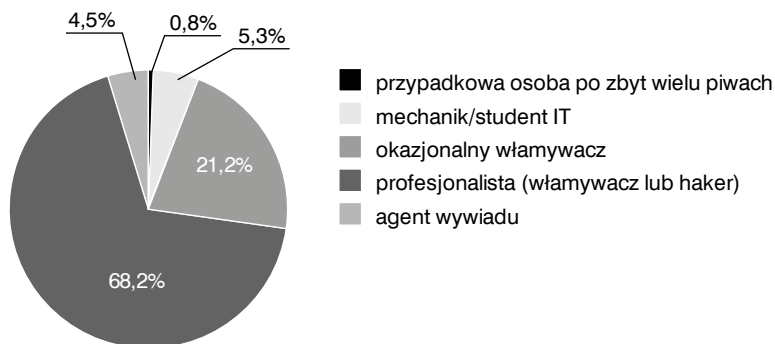
Jeśli tego nie zrobi, wiadomości o przydarzających się incydentach wcześniej czy później się rozniosą, a to doprowadzi do utraty klientów, zarówno obecnych, jak i potencjalnych. Na rynku biur rachunkowych istnieje spora konkurencja i nikt nie wybierze biura, które znane jest z lekceważenia kwestii bezpieczeństwa.

Możemy obrócić to również na swoją korzyść i wykorzystać podejście do bezpieczeństwa jako element naszej konkurencyjności wyróżniający nas na tle innych biur. Takie detale, jak solidne zamki, monitoring, szyfrowana poczta elektroniczna czy regularne audyty IT, mogą przekonać wrażliwego na bezpieczeństwo klienta, żeby wybrał właśnie nasze biuro.

Zdecydowana większość biur zdaje sobie sprawę z wagi podejścia do bezpieczeństwa i wysoko ocenia swoje ogólne przygotowanie w tym zakresie. W przeprowadzonej ankiecie (anonimowej) poprosiliśmy właścicieli biur o wskazanie, jaki poziom umiejętności włamywacza byłby potrzebny, żeby skutecznie włamać się do ich biura lub zagrozić bezpieczeństwu ich danych.

Aż 90 ze 132 biur wybrało poziom 4 (z 5 maksymalnie), określając, że tylko wykwalifikowany profesjonalista byłby w stanie przełamać ich zabezpieczenia.

Schemat 1. Poziom bezpieczeństwa w biurach rachunkowych



Wkładamy dużo wysiłku w to, żeby nasze biuro zorganizować w taki sposób, by świadczyło usługi na wysokim poziomie, z których nasi klienci będą zadowoleni, a także by było dochodowe.

Dołożenie do tego kwestii bezpieczeństwa nie musi być trudne. W większości przypadków da się je naturalnie wpleść w istniejące procedury, a regularne kontrole stawiające nas w górnych kilku procentach najlepiej zabezpieczonych biur to kwestia kilku roboczogodzin w miesiącu.

1.2. Bezpieczeństwo i poufność danych finansowych klientów

Nawet jeśli nie jesteśmy niczym księgowy mafii, którego wiedza może doprowadzić do całkowitego zniszczenia organizacji, to nie zaszkodzi czasami pomyśleć o sobie w ten sposób.

Ujawnienie tajemnic operacyjnych firmy to coś, czego klienci biur rachunkowych bardzo się obawiają. Nic dziwnego. Jeżeli prowadzą swoją działalność już od wielu lat, to stanowi ona znaczną część ich życia, ich tożsamości, a wypracowane przez lata sposoby prowadzenia biznesu woleliby powierzyć wyłącznie swoim spadkobiercom.

Jeśli dopiero zaczynają, często wierzą, że znaleźli pomysł wart miliony albo coś, co pozwoli im odmienić swoje życie (i innych) na lepsze.

Powierzając nam prowadzenie księgowości swojej firmy, klienci oddają w nasze ręce część swojego życia, nadzieje, plany, marzenia. Z pewnością chcieliby, by w naszych rękach były bezpieczne. Nie ma żadnego znaczenia, że ujawnienie tych kilku faktur albo dochodów firmy w praktyce najczęściej nic nie zmienia. Emocje, z którymi to się wiąże, są równie, jak nie bardziej istotne.

Zresztą jak postrzegać kompetencje i skuteczność biura, które nie potrafi nawet ochronić danych swoich klientów? Czy takie biuro może uznać za dokładne i rzetelne w innych, znacznie bardziej skomplikowanych kwestiach?

Utrata zaufania i reputacji to jedna strona medalu. Do dbałości o bezpieczeństwo i poufność danych zobowiązuje nas także prawo. Rozporządzenie o ochronie danych osobowych (RODO) przewiduje wymierne konsekwencje za zaniedbania w tym zakresie.

Tabela 1. Typowe zagrożenia czyhające na dane klientów biur rachunkowych

Lp.	Rodzaj zagrożeń	Przykładowe sytuacje
1.	Czynnik ludzki	a) błędy pracowników, b) niewłaściwe ujawnienie informacji, c) działania nieuczciwych pracowników itp.
2.	Zagrożenia fizyczne	a) kradzież, b) utrata danych, c) pożar, powódź itp.
3.	Zagrożenia cyfrowe	a) ransomware, b) phishing, c) malware itp.

Wszystkie te zagrożenia możemy oszacować i zminimalizować, czym zajmiemy się w kolejnych rozdziałach.