

8 WSKAZÓWEK, JAK CHRONIĆ INFORMACJE BIZNESOWE

1. **Uporządkuj dane** - odpowiedź na pytanie „Co mam i gdzie to jest?” to podstawowa zasada bezpiecznego zarządzania informacjami. Źle opisane dane nie tylko niekorzystnie wpływają na efektywność pracy, ale zwiększają też ryzyko utraty informacji. Trzeba stworzyć model przechowywania danych, który pokaże, jakie informacje mamy i gdzie są zlokalizowane. Dotyczy to zarówno danych tradycyjnych (dokumenty papierowe) jak i elektronicznych.
2. **Oszacuj ryzykowne dane, oceń zagrożenia** - zrozumienie niebezpieczeństw pozwala odpowiednio chronić dane, umożliwia znalezienie metody przeciwdziałania. Zwykła ocena zagrożenia pozwoli w bezpieczny i kompleksowy sposób ochronić powierzone informacje.
3. **Upewnij się, że możesz odzyskać dane** - możesz przechowywać dane na nośnikach, w zewnętrznych archiwach (poza Twoją firmą). Odkryj „chmurę”, jako bezpieczne rozwiązanie do przechowywania informacji, szczególnie tych, które muszą być szybko udostępniane. Powyższe rozwiązania wraz z Disaster Recovery (odzyskiwanie danych po awarii) i Planem Ciągłości Działania stanowią najbardziej niezawodne rozwiązanie, jak nie utracić powierzonych danych.
4. **Ustaw uprawnienia dostępu** – uprawnienia dostępu do danych muszą być skrupulatnie kontrolowane. Model firmowej polityki wewnętrznej ochrony danych, zezwalający na informację o użytkowniku, powinien bazować na specjalnym zezwoleniu lub stanowiskach. Uprawnienia dostępu muszą być czasowo sprawdzane.
5. **Przestrzegaj ustawowego okresu przechowywania danych** - Tak samo jak zwiększa się liczba przepisów regulujących przechowywanie danych, rośnie również liczba kar za ich naruszenie. Pamiętajmy o sprawdzaniu ustawowych okresach przechowywania danych.
6. **Jeden za wszystkich, wszyscy za jednego** – musisz mieć poparcie Zarządu we wszelkich działaniach związanych z polityką ochrony danych. To ułatwi Twoją pracę. Skorzystaj z procesu oceny ryzyka i wskaż obszary biznesu, które są najbardziej zagrożone.
7. **Szkolenia, szkolenia, szkolenia!** – pracownicy muszą być regularnie szkoleni w zakresie zasad bezpieczeństwa danych oraz reguł, które ustawowo dotyczą danych wrażliwych. Ludzie są najsłabszym ogniwem i największym zagrożeniem przy nadużyciach związanych z ochroną informacji. Ale odpowiednio wykwalifikowani mogą być również najlepszą obroną.
8. **Kompetencje** – nie wahaj się prosić o pomoc! Jest wiele organizacji, które mogą Ci pomóc w spełnianiu wymogów ochrony informacji. Najlepszym rozwiązaniem jest umożliwienie, szkolenie i egzekwowanie polityki bezpieczeństwa informacji. W połączeniu mogą doprowadzić do współpracy z ekspertami z branży i zapewnić bezpieczne zarządzanie informacjami.