CYBERUSLABS
BEZPIECZNY ŚWIAT

10 PUNKTÓW
POLITYKI BEZPIECZEŃSTWA FIRMY, KTÓRE MUSISZ ZNAĆ

Jeśli stanąłeś przed zadaniem stworzenia polityki bezpieczeństwa firmy i nie wiesz od czego zacząć, to dobrze trafiłeś.

Poznaj 10 punktów wartościowej polityki bezpieczeństwa.

Efektywna polityka w tym zakresie to podstawa podejścia całej firmy do zagadnienia bezpieczeństwa. Dokument powinien być odzwierciedleniem kultury firmy oraz pozostać w harmonii z praktykami biznesowymi. Wymaga jednak dokładnego zaplanowania, rozwoju oraz nadzoru, aby stał się wartością dla Twojej firmy. Rozpoczynając prace nad polityką bezpieczeństwa możesz trafić na zupełną pustkę lub też na starsze wersje tego dokumentu. Niezależnie jaki scenariusz jest aktualny, zadanie wydaje się dość przytłaczające. Jednak warto wiedzieć od czego zacząć i od razu mieć w świadomości, że polityka bezpieczeństwa niestety nie będzie adekwatna do wszystkich sytuacji w firmie.

Podążaj według naszych wskazówek, aby nie zgubić się podczas procesu tworzenia polityki bezpieczeństwa.

1 Rozwijaj politykę, którą możesz egzekwować

Wdrażanie polityki nad którą nie sprawujesz kontroli nie ma żadnego sensu. Jeśli dokument będzie zawierał zapis mówiący o korzystaniu z Internetu tylko w celach biznesowych, ale nie będziesz mieć możliwości blokowania stron np. Facebooka czy monitorowania aktywności pracowników na komputerze, wdrażanie polityki bezpieczeństwa jest bezużyteczne.

2 Wytłumacz powód powstania polityki bezpieczeństwa firmy

Bądź pewny, że właściwie wytłumaczyłeś wszystkim pracownikom przyczyny wdrażania nowych procedur. Daj im odczuć, co dokładnie usprawnia i na co wpływa polityka.

3 Buduj politykę bezpieczeństwa, która nie wymaga zbyt częstego uaktualniania

Jeśli sformułowana polityka wymaga zbyt częstych aktualizacji, oznacza to, że jest zbyt szczegółowa lub zbyt restrykcyjna.

4 Rozróżnij politykę od standardów oraz rekomendacji

Polityka ma być dokumentem jak najbardziej uniwersalnym i ogólnym, który zabezpieczy we właściwy sposób zasoby i procesy Twojej firmy. Jednak starając się ująć problem bardziej szczegółowo powinieneś odnieść się do rekomendacji oraz standardów. Na przykład w polityce bezpieczeństwa może istnieć zapis „Każda transmisja danych wysyłana poprzez otwartą sieć powinna być szyfrowana". Standardy firmy mogą uszczegółowić ten zapis stanowiąc, że minimalny poziom szyfrowania to 128-bitów. Twoja rekomendacja może dotyczyć rodzaju szyfrowania DES czy AES. W ten sposób wraz ze zmianami i rozwojem technik szyfrujących Twoja polityka bezpieczeństwa nie musi ulegać zmianie.

5 Nie buduj polityki w próżni

Ważne, aby polityka bezpieczeństwa była tworzona z ludźmi i dla ludzi. Rekomendujemy, żeby zaprosić do tworzenia dokumentu pracowników z poszczególnych działów. Pomogą oni z pewnością w odnalezieniu słabych punktów czy też nowych wyzwań, które powinny być ujęte w polityce bezpieczeństwa.

6 Polityka bezpieczeństwa powinna być dostępna dla wszystkich

Zadbaj o to, aby kopia dokumentu znalazła się w firmowym intranecie lub w innym publicznym miejscu. Często zdarza się, że nowy pracownik otrzymuje zapis polityki bezpieczeństwa do przeczytania w pierwszym dniu swojej pracy. Nie licz na to, że po tygodniu będzie cokolwiek z niej pamiętać. Lepiej przypominać co jakiś czas o udostępnionej wersji dokumentu i zachęcać do jego przeczytania.

7 Twoja polityka bezpieczeństwa powinna być zrozumiała

Zadbaj o to, żeby dokument był napisany prostym językiem, a skróty czy trudniejsze sformułowania wyjaśnione. Zbyt długa lub skomplikowana polityka nie zachęci nikogo do jej przeczytania, ani tym bardziej do jej przestrzegania.

8 Wymagaj zapoznania się z polityką bezpieczeństwa

Zawsze, ale to zawsze wymagaj, aby każdy pracownik podpisał dokument stwierdzający zapoznanie się z polityką bezpieczeństwa firmy. Powinien on zawierać informacje stwierdzające przeczytanie, otrzymanie kopii oraz zgody na wypełnianie założeń polityki.

9 Dowiedz się co jest wymagane w firmie, aby uznano politykę bezpieczeństwa za oficjalną

Często w firmach odpowiednia procedura lub osoba musi być włączona w proces legitymizacji nowego dokumentu. Stąd tak ważne jest, abyś dowiedział się jakie kroki musisz wykonać, aby polityka bezpieczeństwa byłą oficjalnie uznana za obowiązującą.

10 Zaangażuj dział prawny

Kiedy polityka bezpieczeństwa jest niezwykle ważna i jej nieprzestrzeganie może doprowadzić do negatywnych skutków prawnych należy włączyć dział prawny w prace nad dokumentem. Przede wszystkim prawnicy powinni odnieść się do poszczególnych punktów zapisu oraz je zrecenzować.

Dobrze przeprowadzony proces planowania, a potem tworzenia dokumentu zapewni Ci właściwe określenie obszarów, które musisz ująć w polityce bezpieczeństwa. Pamiętaj, że nie sam zapis jest istotny, ale jego adekwatność oraz przestrzeganie przez pracowników.