SEO-SERVICES.PL
SEO & Content Marketing

Ochrona firmowej poczty elektronicznej

Poczta elektroniczna to jeden ze słabszych punktów bezpieczeństwa w firmie. Nic więc dziwnego, że internetowi przestępcy wykorzystują ten obszar do swoich ataków. Z drugiej strony trudno jest sobie wyobrazić nowoczesne firmy, które nie korzystają z wiadomości e-mail. W związku z tym bardzo ważną rolę odgrywa odpowiednie zabezpieczenie firmowych skrzynek elektronicznych.

Dlaczego należy chronić firmową pocztę elektroniczną?

Poczta elektroniczna to jeden z najpopularniejszych środków komunikacji nie tylko wśród firm, ale również wśród wielu osób prywatnych. Każdego dnia miliardy ludzi korzystają z takiej poczty i wysyłają łącznie nawet kilkaset miliardów wiadomości dziennie. Razem z wiadomościami często wysyłane są różne ważne dane czy też dokumenty.

Duża popularność poczty e-mail sprawia, że jest ona narażona na wiele internetowych zagrożeń, takich jak wirusy, scam czy też ataki phishingowe mające na celu zdobycie danych osobowych użytkownika poczty. Złośliwe programy mogą utrudnić działanie firmy, a nawet dokonać całkowitego jej paraliżu. Dodatkowo kradzież danych do kont bankowych czy też danych osobowych pracowników i klientów to bardzo poważny problem. Przestępcy mogą bowiem korzystać z kredytów i pożyczek w imieniu takich osób. Nieodpowiednie zabezpieczenie danych może również nieść dla firmy poważne konsekwencje w związku z RODO.

W jaki sposób chronić pocztę elektroniczną wykorzystywaną w firmie?

Na rynku dostępne są specjalne zabezpieczenia technologiczne, programy i rozwiązania IT. Stosowanie tych uniwersalnych metod z pewnością pozwoli na znaczne zwiększenie poziomu bezpieczeństwa w firmie poprzez niwelowanie wielu czynników ryzyka. Przede wszystkim powinno się zadbać o zastosowanie protokołu szyfrowania SSL, dzięki któremu wszystkie dane wysyłane do firmy lub na zewnątrz, są zakodowane i żadne osoby niepowołane nie uzyskają do nich dostępu. Protokół SSL zapewnia bezpieczeństwo danych HTML. Kolejnym protokołem godnym polecenia jest SMTP odpowiedzialny za autoryzację użytkownika. Dzięki temu ze skrzynki może korzystać tylko osoba, która ma do tego odpowiednie uprawnienia. Wyłączenie nieszyfrowanego dostępu do poczty na serwerze jest więc bardzo dobrym zabezpieczeniem.

Jeśli mówimy o kwestii bezpieczeństwa to należy zwrócić uwagę na rozwiązania i poziom zabezpieczeń, które są oferowane przez dostawcę poczty elektronicznej. Na rynku dostępnych jest wiele firm hostingowych i część z nich nie przykłada dużej wagi do bezpieczeństwa. Dobry hosting powinien oferować filtry antyspamowe i antywirusowe. Warto więc dokładnie przeanalizować dostępne oferty i wybrać firmę, która zapewnia wysoki poziom bezpieczeństwa.

Nie bez znaczenia jest również stosowanie na firmowych komputerach odpowiedniego programu antywirusowego i jego konfiguracja umożliwiająca ochronę przed wieloma różnymi zagrożeniami internetowymi. Program taki musi być regularnie aktualizowany – dzięki temu będzie zapewniał ochronę przed coraz nowszymi wirusami i innymi zagrożeniami. Odpowiedzialne zachowanie użytkowników poczty (unikanie wiadomości z niepewnych źródeł, nie klikanie w podejrzane linki, itp.) również odgrywa istotną rolę.