PORADNIK PRACY ZDALNEJ DLA MŚP

10 kroków do bezpiecznej pracy zdalnej dla każdego administratora

W sytuacji, kiedy dotychczasowy sposób funkcjonowania społeczeństwa zostaje zakłócony, wdrożenie opcji pracy zdalnej staje się dla wielu firm koniecznością. Czasem jednak chęć zachowania ciągłości działania przedsiębiorstwa sprawia, że decyzja taka jest podejmowana w pośpiechu i naraża organizację na szereg nowych zagrożeń. Cyberprzestępcy nie zawahają się, żeby z takiej okazji skorzystać. Właśnie dlatego przygotowaliśmy 10 kroków, które należy podjąć, by zabezpieczyć firmę niezależnie od tego, skąd pracują jej pracownicy.

☐ Wprowadź skuteczną politykę haseł

Być może do tej pory byłeś w tej kwestii pobłażliwy, ale przyszedł czas, żeby wzmocnić politykę haseł. Powinny być długie i trudne do odgadnięcia, regularnie zmieniane, a kilkukrotne wprowadzenie błędnego hasła powinno blokować dostęp do danego konta. Wyjaśnij pracownikom dlaczego do służbowych zastosowań nie powinni wykorzystywać tych samych haseł, z których na co dzień korzystają prywatnie.

☐ Skorzystaj z wieloskładnikowego uwierzytelniania (MFA)

Wieloskładnikowe lub inaczej dwuskładnikowe uwierzytelnianie (2FA) to jedno z najskuteczniejszych narzędzi w walce z cyberprzestępcami. Dzięki temu możesz się ochronić m.in. przed atakami z wykorzystaniem skradzionych loginów i haseł oraz tzw. atakami brute force i password spraying, gdzie przestępcy losowo testują kolejne popularne hasła, aż w końcu znajdą to właściwe (i zazwyczaj w końcu znajdują). Jeśli Twoja firma korzysta z poczty i narzędzi w chmurze, włącz uwierzytelnianie wieloskładnikowe w ustawieniach. Jeśli pracownicy potrzebują dostępu do sieci firmowej, wzmocnij proces logowania dedykowanym rozwiązaniem uwierzytelniania wieloskładnikowego.

☐ Wymagaj VPN podczas łączenia z wewnętrzną siecią

Tunele VPN pozwalają szyfrować ruch pomiędzy komputerem pracownika i siecią firmową, dzięki czemu przestępcom jest go trudniej przechwycić. Dodatkową zaletą korzystania z VPN jest możliwość rozszerzenia stosowanych w firmie rozwiązań bezpieczeństwa, także na urządzenia zdalne. Jeśli twoja firma korzysta już z rozwiązania VPN, upewnij się czy może ono zagwarantować wystarczającą wydajność i liczbę licencji do obsłużenia zwiększonego ruchu. Jeśli zdalni pracownicy mają korzystać z zasobów dostępnych jedynie w sieci prywatnej, połączenie VPN i wieloskładnikowego uwierzytelniania jest koniecznością.

☐ Korzystaj z infrastruktury wirtualnych pulpitów (VDI), jeśli to możliwe

W ramach takiego rozwiązania użytkownicy łączą się z maszyną wirtualną, znajdującą się albo w chmurze, albo w twojej serwerowni, którą kontrolują zdalnie. Można ją skonfigurować w taki sposób, żeby wyglądała i zachowywała się dokładnie tak samo, jak komputer znajdujący się w biurze. Główną zaletą tej metody jest to, że firmowe pliki i dane przechowywane są wyłącznie na maszynie wirtualnej i nigdy nie są zapisywane na prywatnym komputerze pracownika.

☐ Przypomnij pracownikom o zasadach bezpieczeństwa w sieciach bezprzewodowych

Jedną rzecz, nad którą nigdy nie będziesz miał pełnej kontroli, jest środowisko sieciowe w domu pracownika oraz podłączone do niego urządzenia. Powiedz swoim pracownikom, żeby wyłączyli na komputerze, który mają zamiar wykorzystywać do pracy, wszystkie funkcje związane z udostępnianiem danych oraz żeby zweryfikowali czy na

swoim routerze Wi-Fi mają ustawione szyfrowanie WPA2 i silne hasło. Przypomnij im, żeby nigdy nie łączyli się z otwartymi sieciami Wi-Fi, które nie wymagają podania hasła.

Zainwestuj w pakiet bezpieczeństwa dla pracowników zdalnych

Podstawowy pakiet antywirusowy instalowany fabrycznie na komputerze to często za mało, by zagwarantować bezpieczeństwo firmowych danych. Lepiej zainwestować w płatny produkt z bardziej rozbudowanym zestawem funkcji, wykorzystujący kilka warstw ochrony do zwalczania szerokiego spektrum zagrożeń. Taki pakiet bezpieczeństwa powinien być wyposażony m.in. w firewall, ochronę przed stronami wyłudzającymi dane oraz funkcję skanowania nośników wymiennych pod kątem wirusów. W większości przypadków najlepszym rozwiązaniem będzie produkt biznesowy, którym firmowy zespół IT będzie mógł zarządzać zdalnie z poziomu centralnej konsoli.

Wymagaj szyfrowania wrażliwych plików

Jeśli w celu wykonania swoich obowiązków pracownicy będą zmuszeni do pobrania wrażliwych danych na swoje prywatne urządzenie, zadbaj o to, żeby były one zaszyfrowane. Zapewnij pracownikom niezbędne narzędzie i wymagaj, by firmowe dokumenty były przechowywane oddzielnie od prywatnych, najlepiej w przeznaczonym do tego celu zaszyfrowanym katalogu. Warto także wdrożyć politykę, w ramach której wszystkie zmodyfikowane dokumenty muszą być przetrzymywane na udziałach firmowych, dzięki czemu nie będziesz musiał martwić się o ich backup.

Wpajaj nawyk wylogowywania się

Kiedy pracownicy robią sobie przerwę na obiad, kończą pracę albo z jakiegokolwiek innego powodu odchodzą od swojego biurka, powinni wylogowywać się z firmowej sieci. Ta dobra praktyka staje się w zasadzie niezbędna, kiedy mówimy o komputerze, do którego dostęp mają także inni domownicy.

Przypominaj o aktualizacjach

Powiedz pracownikom zdalnym, żeby włączyli funkcję automatycznych aktualizacji na swoich urządzeniach. W ten sposób będzisz miał pewność, że są na nich zainstalowane wszystkie bieżące łatki bezpieczeństwa. Nie zapomnij także sprawdzić wszystkich wewnętrznych systemów i zainstaluj ewentualne brakujące aktualizacje. Dotyczy to przede wszystkim kluczowych elementów infrastruktury, gdzie instalacja kolejnych łatek mogła zostać zaniedbana ze względu na konieczność ciągłej pracy w trybie 24/7. Zwróć szczególną uwagę na pracowników, wykorzystujących do pracy komputery z systemem Windows 7. Wersja ta nie jest już wspierana, w związku z czym w większości przypadków nie może zagwarantować odpowiedniego poziomu bezpieczeństwa. Może się okazać, że będzie trzeba zablokować dostęp dla takich maszyn, dopóki nie zostaną zaktualizowane do nowszej wersji systemu.

Zapewnij szkolenia swoim pracownikom

Nie ma znaczenia z jak zaawansowanych zabezpieczeń korzysta Twoja firma - ich najsłabszym ogniwem zawsze pozostanie użytkownik. Fałszywe wiadomości od „administratora" z prośbą o potwierdzenie danych logowania lub polecenie od osoby podszywającej się pod przełożonego, by przelać środki na wybrane konto bankowe to tylko dwa przykłady oszustw, na które mogą nabrać się pracownicy. Dopóki wiele osób pracuje z domu, liczba tego typu wyłudzeń będzie cały czas rosła. Kluczem, żeby się przed nimi chronić, są przeszkoleni w zakresie cyberbezpieczeństwa pracownicy, którzy wiedzą jak rozpoznać tego typu oszustwa i nie dadzą się nabrać. Warto zadbać o zapewnienie im niezbędnej wiedzy, szczególnie w czasie, kiedy pracują zdalnie.

Mamy też dobrą wiadomość

Chmurowe zestawy narzędzi, współpraca na odległość dzięki czatom i rozwiązaniom do telekonferencji oraz inne technologie internetowe mogą sprawić, że praca zdalna będzie równie produktywna, co ta w biurze – a często nawet bardziej. Kiedy Twoi pracownicy zabierają swoją pracę do domu, zadbaj o to, żeby towarzyszyły im niezbędne środki bezpieczeństwa.

Więcej informacji znajdziesz na naszej dedykowanej **STRONIE INTERNETOWEJ**