STRAŻNIK+

Bezpieczeństwo pracy zdalnej

Praca zdalna to wyzwanie zarówno dla firmy, jak i dla pracowników. Domowe środowisko pracy nie zapewnia zwykle tych samych zabezpieczeń, co praca w biurze. Dlatego też, przed wdrożeniem pracy zdalnej warto przygotować procedury i zasady bezpieczeństwa, do których będzie stosował się zespół i poszczególni pracownicy. Pozwoli to na kontrolę nad danymi firmy i zabezpieczenie ich przed zagrożeniami.

Metody infekcji

E-mail
zawierający zainfekowany załącznik lub link do złośliwej strony internetowej

Internet
strona zawierająca złośliwy kod lub podszywająca się pod znany serwis w celu wyłudzenia poufnych informacji

Pobieranie / transfer plików
z wbudowanym trojanem infekującym komputer

APT
(ang. Advanced Persistent Threats) atak, którego efektem jest niedozwolony i długotrwały dostęp do sieci w celu pozyskiwania z niej cennych danych.

Wskazówki i porady

DLA PRACODAWCY

Określ jasne procedury i zasady bezpieczeństwa w firmie

Wdrożenie odpowiednich praktyk powinno stać się priorytetem, a przestrzeganie zasad codziennością wszystkich pracowników.

Bezpieczny dostęp zdalny

Stwórz pracownikom warunki do bezpiecznej pracy zdalnej zapewniając im bezpieczne połączenie z siecią komputerową firmy za pomocą VPN z uwierzytelnianiem wieloetapowym.

Zapewnij odpowiednie i bezpieczne narzędzia do pracy i komunikacji

Wprowadź odpowiednie środki bezpieczeństwa, takie jak szyfrowanie dysku twardego i wymiennych nośników danych (np. dyski USB) czy automatyczne wylogowane po okresie bezczynności.

Zabezpiecz sieć firmową i monitoruj jej stan

Systematycznie skanuj sieć w poszukiwaniu nieautoryzowanych urządzeń i ataków. Zwiększaj poziom bezpieczeństwa w przypadku ataków związanych z VPN.

Kontroluj dostępy sieciowe

Dostępy sieciowe powinny być przypisane do pracownika, a nie do stanowiska, dzięki czemu niezależnie, na którym dozwolonym urządzeniu pracownik zaloguje się do sieci, zawsze zostaną mu przypisane tylko jego własne dostępy.

Zapewnij bezpieczne kanały komunikacji

Korzystaj z dostawcy usług, który gwarantuje pełną poufność przesyłanych informacji. Odpowiednio zabezpiecz dane przesyłane pocztą elektroniczną lub innych kanałów komunikacji.

DLA PRACOWNIKA

Używaj wyłącznie urządzeń służbowych i oprogramowania dostarczonego przez pracodawcę

Pamiętaj, aby nie udostępniać służbowych urządzeń osobom postronnym, czy członkom rodziny. Nie korzystaj z niesprawdzonych i nierzetelnych aplikacji niewiadomego pochodzenia.

Zadbaj o aktualizację komputera

Zweryfikuj, czy systemy z których korzystasz (w tym system operacyjny oraz system antywirusowy) są aktualizowane. Zwracaj uwagę na alerty, a gdy zauważysz nietypowe albo podejrzane działania na swoim urządzeniu, niezwłocznie poinformuj o tym pracodawcę lub Dział IT.

Nie korzystaj z otwartych sieci publicznych

Nie udostępniaj plików i nie wykonuj ważnych operacji w trybie publicznym. Korzystaj z urządzenia zabezpieczonego antywirusem, a z siecią firmową łącz się tylko przez firmowy VPN.

Korzystaj z silnych haseł

Hasła powinny składać się z co najmniej 8 znaków, w tym małych i dużych liter, cyfr lub znaków specjalnych, a ich zmiana powinna następować w cyklach 30-dniowych. Nigdy i nikomu nie udostępniaj swojego hasła!

Twórz kopie zapasowe i szyfruj nośniki danych

Karty pamięci, pendrive, dyski zewnętrzne i inne nośniki danych powinny być odpowiednio zaszyfrowane. Nie umieszczaj danych w publicznych chmurach obliczeniowych, komunikatorach czy innych usługach, które nie są autoryzowane przez Twoją firmę.

I-BS.PL

www.i-bs.pl
email: **dh@i-bs.pl**
tel: **604 223 619 / 728 403 586**