Cyberbezpieczeństwo pracy zdalnej

SEQRED

Cyberbezpieczeństwo pracy zdalnej wymaga wdrożenia odpowiednich procedur oraz rozwiązań technologicznych. Odpowiednie przygotowanie systemów i urządzeń oraz przestrzeganie zasad bezpiecznego świadczenia pracy zdalnej pomoże zminimalizować ryzyko wystąpienia ataku hakerskiego, a tym samym poniesienia przez firmę strat, nie tylko finansowych.

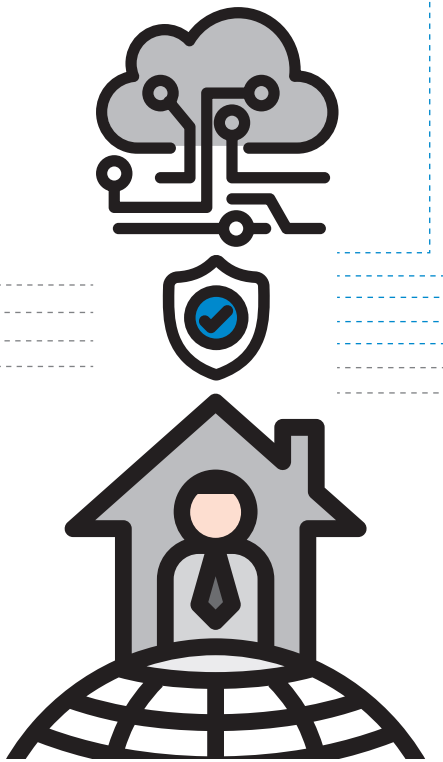
1. Pracodawca

OGRANICZ DOSTĘP
Ogranicz dostęp do wrażliwych systemów i danych tylko dla pracowników, dla których ten dostęp jest niezbędny do wykonywania pracy.

ZAPEWNIJ BEZPIECZEŃSTWO ROZWIĄZAŃ DO PRACY ZDALNEJ
Zapewnij systemom, z których korzystają pracownicy adekwatne mechanizmy szyfrowania oraz uwierzytelniania.

ZDEFINIUJ PROCEDURY
Zdefiniuj procedury na wypadek wystąpienia incydentu cyberbiezpieczeństwa. Przekaż pracownikom informacje na temat sposobu reagowania – jaką podjąć czynność, do kogo się zgłosić w sytuacji awaryjnej.

ZADBAJ O SZKOLENIA
Podnoś kwalifikacje swoich pracowników w zakresie bezpieczeństwa pracy zdalnej oraz bezpiecznego korzystania z Internetu. Przeprowadź szkolenie wprowadzające oraz regularne szkolenia uzupełniające.



2. Pracownik

BEZPIECZNIE KORZYSTAJ Z ZASOBÓW FIRMY
Korzystaj z VPN przy łączeniu się do zasobów firmy. Szyfruj przesyłane e-maile i pliki. Korzystaj z firmowego komputera i dysków, skonfigurowanych pod względem bezpieczeństwa. Nie przenoś firmowych danych na prywatne komputery i urządzenia mobilne.

BEZPIECZNIE KORZYSTAJ Z INTERNETU*
Nie tylko komputery, ale także smartfony, tablety oraz inne podłączane do Internetu urządzenia, wymagają ochrony przed wirusami i złośliwym oprogramowaniem.
**Szczegółowe zalecenia na dole strony.*

ZADBAJ O AKTUALIZACJE
Aktualizuj programy antywirusowe oraz system operacyjny i oprogramowanie. Korzystaj z automatycznego sprawdzania dostępności aktualizacji w celu ochrony przed nowymi zagrożeniami.

TWÓRZ KOPIE ZAPASOWE
Regularnie twórz kopie zapasowe ważnych dokumentów i plików oraz przechowuj je w bezpiecznym miejscu. Pomogą one odzyskać utracone (np. w przypadku ataku ransomware) dane.

UWAŻAJ NA CYBERPRZESTĘPCÓW
Hakerzy wykorzystują nasze emocje do pozyskania poufnych danych wysyłając fałszywe e-maile lub dokonując przekierowań na fałszywe strony internetowe. Nie otwieraj podejrzanych e-maili, nie podawaj poufnych danych, nie klikaj podejrzanych linków i nie otwieraj załączników.

BLOKUJ KOMPUTER
Blokuj komputer kiedy od niego odchodzisz. Takie działanie utrudni osobom nieuprawnionym uzyskanie dostępu do Twojego komputera i znajdujących się na nim danych.

NIE PRZECIĄŻAJ ŁĄCZA INTERNETOWEGO
W trakcie telekonferencji nie ściągaj danych oraz nie wykonuj aktualizacji. Pozwoli to na płynne przekazywanie obrazu i dźwięku.

Bezpieczna praca

Dobre nawyki

3. Bezpiecznie korzystaj z Internetu

Jeśli to możliwe – nie korzystaj z otwartych sieci publicznych (wi-fi).

Korzystaj z bezpiecznych standardów szyfrowania (WPA2, WPA3).

Zmień/uaktualnij hasło do routera/sieci.

Korzystaj z silnych haseł (Passphrases) – unikalnych dla kont.

Aktualizuj software/ firmware na swoim urządzeniu sieciowym.

SEQRED S.A.
biuro@seqred.pl
www.seqred.pl