WYTYCZNE

W zakresie bezpieczeństwa pracy na komputerze przy wykonywaniu pracy zdalnej

PODSTAWOWA OCHRONA

1. **Blokuj komputer przy wyjściu na każdą przerwę** (choćby "tylko na chwilę"). Pod Windows umożliwia to skrót klawiaturowy Win+L, w macOS: control+command+Q
2. **Używaj odpowiednio złożonych haseł dostępowych** (obecnie cztery-pięć względnie losowo dobranych słów stanowi solidne hasło).
3. **Korzystaj z managerów haseł**.
4. **Skonfiguruj automatyczne blokowanie komputera po pewnym krótkim czasie bezczynności** ("Raz kot mi przeleciał przez klawiaturę i wysłał wiadomość do osoby z firmy").
5. Nie pożyczaj komputera firmowego (a w szczególności Twojego zalogowanego konta!) innym osobom.
6. Nie używaj komputera firmowego do grania czy wspólnego oglądania filmów (szczególnie pirackich :P).
7. Zamykaj komputer po zakończonej pracy (pamiętaj o "zamykaniu" nie "usypianiu" czy "hibernowaniu").
8. W miarę możliwości zadbaj o osobny pokój do pracy.

Administratorzy mogą dodatkowo zadbać o:

1. Przekazanie pracownikom kont nieposiadających uprawnień administracyjnych.
2. Aktualizacje zarówno oprogramowania systemowego (np. Windows) jak i dodatkowego (np. przeglądarki internetowe, czytnik PDF, …)
3. Włączenie firewalla (zapory sieciowej) – najlepiej w trybie całkowicie uniemożliwiającym nawiązanie połączenia do komputera pracownika z zewnątrz (czytaj: z kompletnie niezabezpieczonej, domowej sieci WiFi).
4. Dostarczenie i bieżące aktualizacje oprogramowania antywirusowego.
5. Wymuszenie zakazu instalacji oprogramowania niezatwierdzonego przez firmę.

Korzystanie z sieci WIFI

Zapewne przytłaczająca większość osób w trakcie pracy zdalnej korzystała będzie ze swojej domowej sieci WiFI. **Nie korzystać z otwartych sieci WIFI**.

Komunikatory

1. Używać bezpiecznych komunikatorów np. SIGNAL lub nie przesyłać istotnych informacji przez inne komunikatory.
2. Częsta komunikacja z wieloma pracownikami poprzez telefon czy mail. Możliwe, ale uciążliwe. Czasem wygodniej jest użyć komunikatora.
3. Od strony użytkownika – pamiętaj żeby nie uruchamiać „na boku" alternatywnego komunikatora.

4. Od strony administratora – jeśli komunikator dostępny jest również w trybie pracy zdalnej to zastanów się czy zadbaliście o odpowiednią ochronę kryptograficzną przesyłanych wiadomości. Standardowo – warto również kontrolować aktualizacje po stronie serwerowej i klienckiej.

Dostęp do poczty e-mail

firmowego czy łatwego sposobu na dzielenie się firmowymi dokumentami.

W przypadku korzystania z rozwiązania typu webmail, warto:

1. Sprawdzić czy używasz odpowiednio skomplikowanych haseł dostępowych (idealnie jeśli dodatkowo administratorzy skonfigurowali tzw. 2FA).
2. Po zakończonej pracy wyloguj się z webmaila.

Drukowanie dokumentów

OBOWIĄZUJE ZAKAZ DRUKOWANIA DOKUMENTÓW W DOMU

Pamiętajcie, że część drukarek posiada wbudowane nośniki pamięci – warto zatem zadbać żeby nie znalazły się tam poufne dane (w szczególności jeśli będziemy drukarkę sprzedawać / wyrzucać).

Szyfrowanie danych na komputerze [administratorzy]

1. Ustawić odpowiednio złożone hasło dostępowe (nic nam z szyfrowania dysku jeśli hasłem będzie: Katarzyna1).
2. Mieć przygotowany plan na wypadek utraty / zapomnienia hasła dostępowego.

tą, za którą się podaje. Wypracujmy tutaj sobie odpowiednie procedury.

Opracowano na podstawie:

https://sekurak.pl/bezpieczenstwo-pracy-zdalnej-poradnik-dla-uzytkownika-i-administratora/