Zalecenia dotyczące pracy zdalnej – o czym muszą pamiętać pracodawcy?

Poniżej prezentujemy listę środków bezpieczeństwa, o których powinni pamiętać administratorzy danych osobowych (ADO), których model współpracy obejmuje możliwość pracy zdalnej.

1. ADO powinien udostępnić swoim pracownikom bezpieczny kanał komunikacji z systemami znajdującymi się w infrastrukturze lokalnej. Zalecanym rozwiązaniem łączenia z siecią administratora jest wykorzystanie technologii wirtualnych sieci prywatnych (VPN - Virtual Private Network).
2. Do realizacji zdalnego dostępu powinno się wybrać się rozwiązania, które:
    - zapewniają poufność połączenia (szyfrowanie);
    - zapobiegają nieautoryzowanemu i nienadzorowanemu przez ADO zestawieniu połączenia;
    - wymuszają odpowiednie polityki uwierzytelniania;
    - nie posiadają podatności bezpieczeństwa, które nie zostały naprawione przez producenta.
3. Praca za pośrednictwem zdalnego dostępu powinna wiązać się z takimi samymi ograniczeniami uprawnień do systemów informatycznych i innych zasobów, jak w przypadku pracy w siedzibie ADO.
4. Rozwiązanie umożliwiające zdalny dostęp powinno zostać skonfigurowane w taki sposób, aby:
    - w przypadku bezczynności użytkownika automatycznie rozłączało jego sesję zdalną. Rekomendowany czas, po którym nastąpi automatyczne rozłączenie to 10 minut.
    - po zestawieniu zdalnego połączenia do sieci LAN automatycznie był blokowany dostęp do Internetu.
5. ADO powinien zapewnić warunki odpowiednie do pracy zdalnej, np. łącze odpowiedniej przepustowości, aby praca zdalna wielu użytkowników nie miała wpływu na dostępność systemów, w których przetwarzane są dane osobowe.
6. Wykorzystywanie prywatnych urządzeń do pracy zdalnej powinno być zatwierdzone przez ADO.

7. Zgoda na wykorzystywanie prywatnych urządzeń powinna wiązać się ze wcześniejszym sprawdzeniem, czy na urządzeniu:
    - zainstalowany został aktualny, wspierany przez producenta system operacyjny;
    - funkcjonuje aktualna aplikacja chroniąca przed szkodliwym oprogramowaniem oraz zapora aplikacyjna firewall;
    - funkcjonuje konto użytkownika standardowego z ograniczonymi do minimum możliwościami administrowania.
8. W miarę możliwości ADO powinien wykonać pełne skanowanie antywirusowe prywatnej stacji użytkownika oraz sprawdzić dziennik zdarzeń lokalnej zapory sieciowej.
9. W przypadku przechowywania na prywatnej stacji roboczej użytkownika danych osobowych ADO powinien zapewnić użytkownikowi środki kryptograficzne (szyfrowanie przy użyciu silnych haseł bądź innych metod zapewniających bezpieczeństwo uwierzytelniania) umożliwiające ich odpowiednie zabezpieczenie.
10. W przypadku konieczności przekazania danych uwierzytelniających do usługi zdalnego dostępu należy zachować szczególne środki ostrożności i wykorzystać bezpieczny kanał do ich przesłania.
11. W przypadku przechowywania na prywatnej stacji roboczej danych osobowych użytkownik powinien wyrazić zgodę na możliwość dostępu do niej ADO lub osobie przez niego wyznaczonej.
12. ADO powinien stworzyć instrukcję zarówno użytkowania, jak i bezpiecznego korzystania z rozwiązań umożliwiających zdalny dostęp do systemów przetwarzających dane osobowe.
13. ADO powinien monitorować zdarzenia związane ze zdalnym połączeniem użytkowników do sieci lokalnej.