

Zalecenia do pracy zdalnej

Paweł Krawczyk

Zalecenia

Poniżej zaprezentowane zalecenia należy traktować jako punkt wyjścia – w szczególności należy zapoznać się z obowiązującymi w danej branży regulacjami szczegółowymi (branżowymi lub ustawowymi).

Wariant minimum należy uznać za właściwy dla mikroprzedsiębiorstwa lub niewielkiej jednostki administracji publicznej o ograniczonym budżecie, który nie pozwoli na szybkie wdrożenie specjalizowanych mechanizmów bezpieczeństwa. Obejmuje on elementy, których wdrożenie nie wymaga właściwie żadnych nakładów poza odrobiną pracy.

Wariant standardowy powinien być uwzględniony przez każdą instytucję, która uświadamia sobie problemy związane z bezpieczeństwem.

Wariant pełny jest zalecany dla organizacji, w których naruszenie bezpieczeństwa informacji jest znaczącym zagrożeniem ze względu na odpowiedzialność ustawową lub wartość przetwarzanej informacji.

Zestaw minimum

1. Poinformuj pracowników o odpowiedzialności związanej z przetwarzanymi przez nich danymi.
2. Szyfruj wrażliwe informacje za pomocą jakiegokolwiek dostępnego mechanizmu – choćby wbudowany w Windows EFS (Encrypted File System).
3. Regularnie aktualizuj wszystkie systemy operacyjne i zainstalowane na nich aplikacje. Wykorzystaj wbudowane w system mechanizmy aktualizacji i dostępne aplikacje (Secunia PSI).
4. Nie dawaj uprawnień administratora użytkownikom nowych systemów i buduj procedury instalowania aplikacji użytkownikom, dążąc w ten sposób do budowy korporacyjnego standardu.
5. Upewnij się, że wbudowane w systemy użytkowników mechanizmy bezpieczeństwa (firewall, antywirus) są poprawnie skonfigurowane i nie są wyłączone.
6. Edukuj użytkowników w zakresie bezpieczeństwa – np. haseł.

Zestaw standardowy

7. Szyfruj dane na komputerach przenośnych za pomocą jednego z dostępnych rozwiązań FDE (Full-Disk Encryption).
8. Rozważ wprowadzenie korporacyjnego standardu oprogramowania i egzekwuj go zarówno na nowych jak i dotychczas działających stanowiskach.

9. Zabierz uprawnienia administratora użytkownikom nowych i dotychczas stosowanych komputerów.
10. Zapoznaj się z normą PN ISO/IEC 17799:2007 – znajdziesz tam wiele tam zaleceń, które nie będą wymagać ze strony organizacji znaczących nakładów, a realnie zwiększą poziom bezpieczeństwa.
11. Jeśli przetwarzasz dane osobowe zapoznaj się z poradnikiem [„UODO Survival Kit” opublikowanym przez polski oddział ISACA](#)
12. Do komunikacji komputerów przenośnych z siecią macierzystą zawsze stosuj bezpieczne środki komunikacji (szyfrowanie poczty, VPN).

Zestaw pełny

13. Zbuduj politykę bezpieczeństwa zgodną z normą PN ISO/IEC 17799:2007.
14. Kontroluj dystrybucję informacji za pomocą jednego z dostępnych na rynku rozwiązań typu IRM (Information Rights Management) lub DLP (Data Loss Prevention), uzupełniając nim szyfrowanie komputerów przenośnych.
15. Przeprowadź audyt organizacji na zgodność z normą PN ISO/IEC 27001.
16. Regularnie prowadź testy penetracyjne i oceny bezpieczeństwa informacji w instytucji.
17. Stosuj silne mechanizmy uwierzytelnienia dla użytkowników – tokeny, generatory haseł jednorazowych, karty elektroniczne.