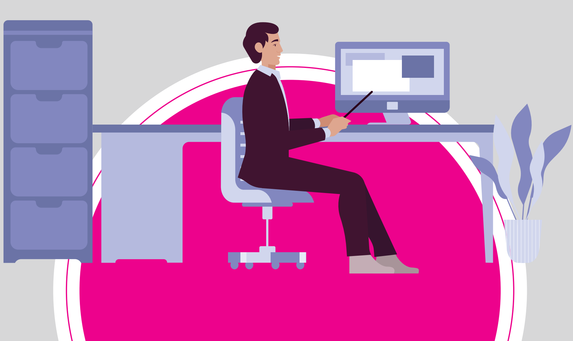
15 najczęstszych (cyber)błędów firm

1. Brak jednoznacznej i wymuszonej polityki wprowadzania zmian w hasłach.
2. Brak szkoleń wprowadzających pracowników w świat ataków socjotechnicznych.
3. Brak procedur na wypadek różnego rodzaju cyberincydentów.
4. Brak atencji do urządzeń sieciowych innych niż komputery, np. firmowych drukarek.
5. Niewystarczająca dbałość – typowy grzech administratorów – o aktualizowanie oprogramowania – aplikacji, systemów operacyjnych czy oprogramowania firmware.
6. Udostępnianie poufnych plików przez publicznie dostępny, firmowy serwer WWW. Dane tymczasem mogą zostać zindeksowane przez Google i pojawiać się w wynikach wyszukiwania.
7. Brak uregulowania lub niedotrzymania procedur dla pracy w trybie BYOD (Bring Your Own Device) i BYOW (Bring Your Own Wearables).
8. Niedbałość o odpowiednią, zgodną ze standardami i dobrymi praktykami, konfigurację urządzeń podłączonych do sieci.
9. Brak monitoringu i kontroli nad kontami użytkowników o podwyższonych uprawnieniach.
10. Dostarczanie użytkownikom aplikacji bez wcześniejszych testów w zakresie bezpieczeństwa. Rzadko kiedy programiści dbają o dobrą jakość kodu źródłowego.
11. Używanie na etapie tworzenia aplikacji i jej testów rzeczywistych danych produkcyjnych, np. osobowych. Powoduje to utratę kontroli nad tymi informacjami, co jest sprzeczne z RODO!
12. Brak odseparowanej sieci Wi-Fi dla gości.
13. Brak polityki tworzenia i przechowywania kopii zapasowych, a w skrajnych przypadkach całkowity ich brak.
14. Częsty brak uregulowania kwestii bezpieczeństwa IT w umowach o współpracy z partnerami i zewnętrznymi dostawcami.
15. Nieprowadzenie regularnych testów, które pozwoliłyby wyszukiwać luki w aplikacjach lub systemach bezpieczeństwa sieciowego.

ZOBACZ GRZECHY PRACOWNIKÓW