

# BEZPIECZEŃSTWO PRACY ZDALNEJ

pawel.krawczyk@hush.com

# Agenda

---

- Praca zdalna z punktu widzenia bezpieczeństwa
- Czym się różni pracownik zdalny od lokalnego?
- Typowe zagrożenia
- Dostępne zabezpieczenia

# Bezpieczeństwo pracy zdalnej

## □ Podstawowe różnice

### ▣ Pracownik zdalny

- Praca w domu (sieć osiedlowa, kablowa, DSL)
- Komputer firmowy wykorzystywany do celów prywatnych

### ▣ Pracownik lokalny

- Praca w sieci firmowej
- Komputer firmowy wykorzystywany głównie do celów służbowych

# Pracownik lokalny

- Pracownik lokalny w sieci macierzystej
  - ▣ Za firewallem i serwerem proxy
    - Filtrowanie większości zagrożeń z zewnątrz
    - Antywirus, ochrona przed phishingiem
  - ▣ Opieka administratora
    - Aktualizacje systemu i innego oprogramowania
    - Poprawna konfiguracja zabezpieczeń w systemie
  - ▣ Mniejsze ryzyko przejęcia systemu

# Pracownik zdalny

- Pracownik zdalny w sieci domowej
  - ▣ Słaba ochrona lub brak ochrony na poziomie sieci
    - Tylko prosty router DSL, WLAN lub kablowy
    - Dostęp do wszystkich stron w sieci
  - ▣ Brak nadzoru administratora
    - Brak aktualizacji lub instalowane wybiórczo
    - Pirackie oprogramowanie
    - Programy P2P, komunikatory, gry
  - ▣ Duże ryzyko przejęcia systemu

# Ryzyko dla firmy

- Ryzyko utraty wrażliwych danych
  - ▣ Wejście na otwarty udział sieciowy pracownika
  - ▣ Kradzież haseł z komputera pracownika
  - ▣ Kradzież danych i plików z komputera pracownika
- Ryzyko związane z podłączaniem do sieci firmy
  - ▣ Możliwość „przywleczenia” trojanów i wirusów podczas wizyty w firmie
  - ▣ Możliwość przesłania zawirusowanych plików podczas połączenia przez VPN

# Środki bezpieczeństwa

- Ochrona poufności danych
  - ▣ Szyfrowanie dysków
    - Full Disk Encryption + Password Based Authentication
    - Chroni przed kradzieżą notebooka
  - ▣ Szyfrowanie transmisji
    - Cała łączność przez VPN
    - Poczta elektroniczna POP3, IMAP przez SSL
    - Dostęp do serwisów w intranecie przez SSL
    - Chroni przed kradzieżą haseł i podsłuchem

# Środki bezpieczeństwa

- Bezpieczne logowanie
  - ▣ Logowanie tylko w zaszyfrowanej sesji
  - ▣ Wymuszanie silnych haseł
    - Niekoniecznie takie: „*tUwu2edr*” (trudne do zapamiętania)
    - Na przykład takie: „*Czasopismo Ogrodnikow 242*”
    - Dobre hasło chroni przed automatycznym zgadywaniem
  - ▣ „Two-factor authentication”
    - Tokeny-generatory haseł jednorazowych, uwierzytelnienie przez hasło plus SMS
    - Chronią przed kradzieżą hasła lub tokenu

# Środki bezpieczeństwa

- Ochrona przed złośliwym oprogramowaniem
  - ▣ Firewall osobisty i program antywirusowy
    - Chroni przed niektórymi atakami, wirusami i trojanami
  - ▣ Brak uprawnień administratora w systemie
    - Uniemożliwia przypadkowe zainstalowanie trojana
  - ▣ Wymuszona aktualizacja systemu operacyjnego
    - Utrudnia przejęcie kontroli za pomocą dziur w systemie
  - ▣ Aktualizacja innych programów zainstalowanych w systemie
    - Dziury nie mniej groźne niż w systemie

# Środki bezpieczeństwa

- Rozwiązania organizacyjne
  - ▣ Dokument pt. „Polityka bezpieczeństwa”
    - Co wolno, czego nie wolno użytkownikom
    - Powinien uwzględniać specyfikę pracy zdalnej
    - Stanowi oficjalne uzasadnienie dla np. braku praw administratora (częsta kontrowersja)
  - ▣ Polityka określa jednoznacznie odpowiedzialność w razie naruszenia bezpieczeństwa
    - Użytkownik nie naruszył polityki (np. dziura w Windows)
    - Użytkownik naruszył politykę (np. przejęcie praw administratora)

# Pytania?

---

- Paweł Krawczyk <pawel.krawczyk@hush.com>