



Bezpieczeństwo w pracy zdalnej



pawel.krawczyk@hush.com

Agenda

- Pracownik w firmie, a pracownik zdalny - różnice
- Praca zdalna - nowe wyzwanie z punktu widzenia bezpieczeństwa
- Przepisy prawa
- Możliwe techniki obrony

Informacja wrażliwa

- Informacje wrażliwe
 - } Ustawa o ochronie danych osobowych
 - } Ustawa o informacji niejawnej
 - } Tajemnica przedsiębiorstwa
- Dystrybucja informacji musi podlegać ochronie
 - } Praca w biurze – centralny punkt ochrony
 - } Praca zdalna – nowe zagrożenia, wiele punktów ochrony

Czego powinna obawiać się firma?

- Ryzyko utraty wrażliwych danych
 - } Wejście na otwarty udział sieciowy pracownika
 - } Kradzież haseł z komputera pracownika
 - } Kradzież danych i plików z komputera pracownika
 - } Kradzież całego komputera pracownika
- Ryzyko związane z podłączaniem do sieci firmy
 - } Możliwość przyniesienia trojanów i wirusów

Pracownik lokalny

- Pracownik lokalny w sieci macierzystej
 - } Za firewallem i serwerem proxy
 - Filtrowanie większości zagrożeń z zewnątrz
 - Antywirus, ochrona przed phishingiem, filtrowanie stron z malware
 - } Opieka administratora
 - Aktualizacje systemu i innego oprogramowania
 - Poprawna konfiguracja zabezpieczeń w systemie
 - Możliwość wymuszenia polityki ochrony informacji

Pracownik zdalny

- Pracownik zdalny w sieci domowej
 - } Słaba ochrona lub brak ochrony na poziomie sieci
 - Prosty router DSL, WLAN lub kablowy
 - Dostęp do wszystkich stron w sieci, brak filtrów
 - } Brak nadzoru administratora
 - Brak aktualizacji lub instalowane wybiórczo
 - Pirackie oprogramowanie
 - Programy P2P, komunikatory, gry
 - Mniejsze możliwości wymuszenia polityki

Środki bezpieczeństwa

□ Ochrona poufności danych

} Szyfrowanie systemu i dysków

- Full Disk Encryption + Password Based Authentication
- Produkty: Utimaco SafeGuard Easy, CompuSec, SecureDoc, Bitlocker (Microsoft Vista), PGP, TrueCrypt (darmowy)
- Chroni przed kradzieżą notebooka

} Szyfrowanie transmisji

- Cała łączność przez VPN
- Poczta elektroniczna POP3 IMAP przez SSL

Środki bezpieczeństwa

- Produkty typu IRM
 - } Information Rights Management
 - Kto ma prawa do czytania i dystrybucji tego pliku?
 - Czy można kopiować ten plik na zewnątrz?
 - Jak zapewnić by po skopiowaniu na USB ten plik był nieczytelny (szyfrowanie)?
 - } Kontrola dystrybucji informacji w firmie
 - } Produkty: Utimaco LAN Crypt, McAfee Data Loss Prevention, Microsoft Office Information Rights Management

Środki bezpieczeństwa

- Bezpieczne logowanie
 - } Konieczne wymuszenie silnych ustawień
 - W przeciwnym razie na 100% hasła typu „marysia123”
 - } Polityka silnych haseł
 - 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

- **Brak uprawnień administratora w systemie**
- Centralne zarządzanie oprogramowaniem i politykami bezpieczeństwa
 - } Group Policy Objects (GPO) w domenie Windows
- Centralny monitoring potencjalnych zagrożeń

Środki bezpieczeństwa

- Firewall osobisty i program antywirusowy
 - } Chroni przed niektórymi atakami, wirusami i trojanami
- Wymuszona aktualizacja systemu operacyjnego
 - } Utrudnia przejęcie kontroli za pomocą dziur w systemie
- Aktualizacja innych programów zainstalowanych 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)

Pomocne normy i akty

prawne

- PN-ISO/IEC-17799, PN-ISO/IEC-27001, PN-ISO/IEC-13335
- ISACA COBIT
- Akty prawne
 - } Ustawa o ochronie informacji niejawnej
 - } Ustawa o ochronie danych osobowych
 - } Kodeks karny („przestępstwa komputerowe” – art. 269)
 - } Ustawa o zwalczaniu nieuczciwej konkurencji

Pytania?



pawel.krawczyk@hush.
com