Polityka bezpieczeństwa

Polityka bezpieczeństwa

- Formalny dokument opisujący strategię bezpieczeństwa.
- Oczekiwana zawartość:
- –cele,
- –standardy i wytyczne,
- –zadania do wykonania,
- –specyfikacja środków,
- –zakresy odpowiedzialności.

Aby osiągnąć cele polityki bezpieczeństwa należy:

- Określić reguły i procedury bezpieczeństwa informacji,
- Wdrożyć system zabezpieczeń,
- Szkolić i uświadamiać personel,
- Monitorować poziom bezpieczeństwa,
- Dostosowywać system i metody zarządzania do zmieniających się zagrożeń i warunków otoczenia.

M. Kaliski, A. Kierzkowska, G. Tomaszewski, Ochrona informacji i zasobów relacyjnych przedsiębiorstwa oraz lojalnośc personelu [w] Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu, Dom Organizatora, Toruń 2010

Fazy życia polityki bezpieczeństwa

- –wytworzenie,
- –wdrożenie,
- –zarządzanie (aktualizacja, monitoring, audyty).

Polityka Bezpieczeństwa Firmy

- Polityka Bezpieczeństwa Firmy (PBF) jest zintegrowanym zbiorem ogólnych zasad i dyrektyw wewnętrznych w zakresie bezpieczeństwa. Odzwierciedla uregulowania obejmujące Centralę i oddziały Firmy.
- PBF ma charakter przymusowy, czyli żaden pracownik nie może działać inaczej bez specjalnej zgody kierownika jednostki organizacyjnej Firmy.

Dyrektywy Generalne

Realizując PBF, we współpracy ze służbami bezpieczeństwa państwa, Pełnomocnik Ochrony – Dyrektor Biura Ochrony Firmy - dba o interes Firmy w zakresie bezpieczeństwa.

Pełnomocnik Ochrony

- Pełnomocnik Ochrony – Dyrektor Biura Ochrony - koordynuje działania Firmy w zakresie bezpieczeństwa.
- Dyrektor Biura Ochrony Firmy kieruje pionem ochrony - wyodrębnioną wyspecjalizowaną komórką organizacyjną Firmy

Pełnomocnik Ochrony zapewnia

- ochronę informacji niejawnych,
- ochronę systemów i sieci teleinformatycznych,
- ochronę fizyczną Firmy,
- koordynację ochrony fizycznej jednostek organizacyjnych,
- kontrolę ochrony informacji niejawnych,
- przestrzeganie przepisów o ochronie informacji niejawnych,
- okresową kontrolę ewidencji materiałów i obiegu dokumentów,
- opracowanie planów ochrony i nadzorowanie ich realizacji,
- szkolenie pracowników banku w zakresie ochrony informacji niejawnych.

Informacje niejawne to takie, których wytwórca przyznał im jedną z czterech klauzul tajności:

- **ściśle tajne,** czyli takie których ujawnienie spowoduje zagrożenie niepodległości, suwerenności czy integralności terytorialnej Rzeczpospolitej Polskiej;
- **tajne,** których nieuprawnione ujawnienie uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- **poufne,** których nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub chronionego prawnie interesu obywateli oraz
- **zastrzeżone,** czyli takie, których nieuprawnione ujawnienie wiąże się ze szkodą dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej.

http://www.bezpieczneit.com/dane_osobowe_informacje_niejawne/ochrona-informacji-niejawnych-w-systemach-teleinformatycznych/ [dostęp 11.04.2015]

Uzgodnienia przedsięwzięć Firmy

Wszyscy kierownicy jednostek organizacyjnych Firmy mają obowiązek uzgodnienia z Dyrektorem Biura Ochrony, na etapie planowania realizacji oraz kontroli, wszystkich przedsięwzięć organizacyjnych i działań dotyczących bezpieczeństwa. W szczególności uzgodnieniu podlegają:

1. Infrastruktura Firmy: lokalizacja budynków, warunki najmu, architektura i budowa, infrastruktura techniczna.
2. Systemy teleinformatyczne: lokalizacja, sprzęt i oprogramowanie, systemy zabezpieczeń.
3. Współpraca z podmiotami zewnętrznymi świadczącymi usługi na rzecz banku.
4. Inne sprawy bieżące wymagające uzgodnień w zakresie bezpieczeństwa.

Cyberslacking

- Cyfrowe bumelanctwo. Wykorzystywanie IT w pracy do prywatnych celów.

Co zawiera umowa o pracę?

- Kwestię użytkowania firmowego łącza internetowego (oraz służbowego komputera i telefonu) do celów prywatnych regulują przede wszystkim wewnętrzne przepisy danego przedsiębiorstwa.
- Obowiązują regulaminy korzystania z Internetu, sprzętu komputerowego i oprogramowania oraz takie dokumenty jak „Polityka Bezpieczeństwa" i „Instrukcja Zarządzania Systemami Informatycznymi", tworzonymi obowiązkowo przez każdą firmę przetwarzającą dane osobowe.

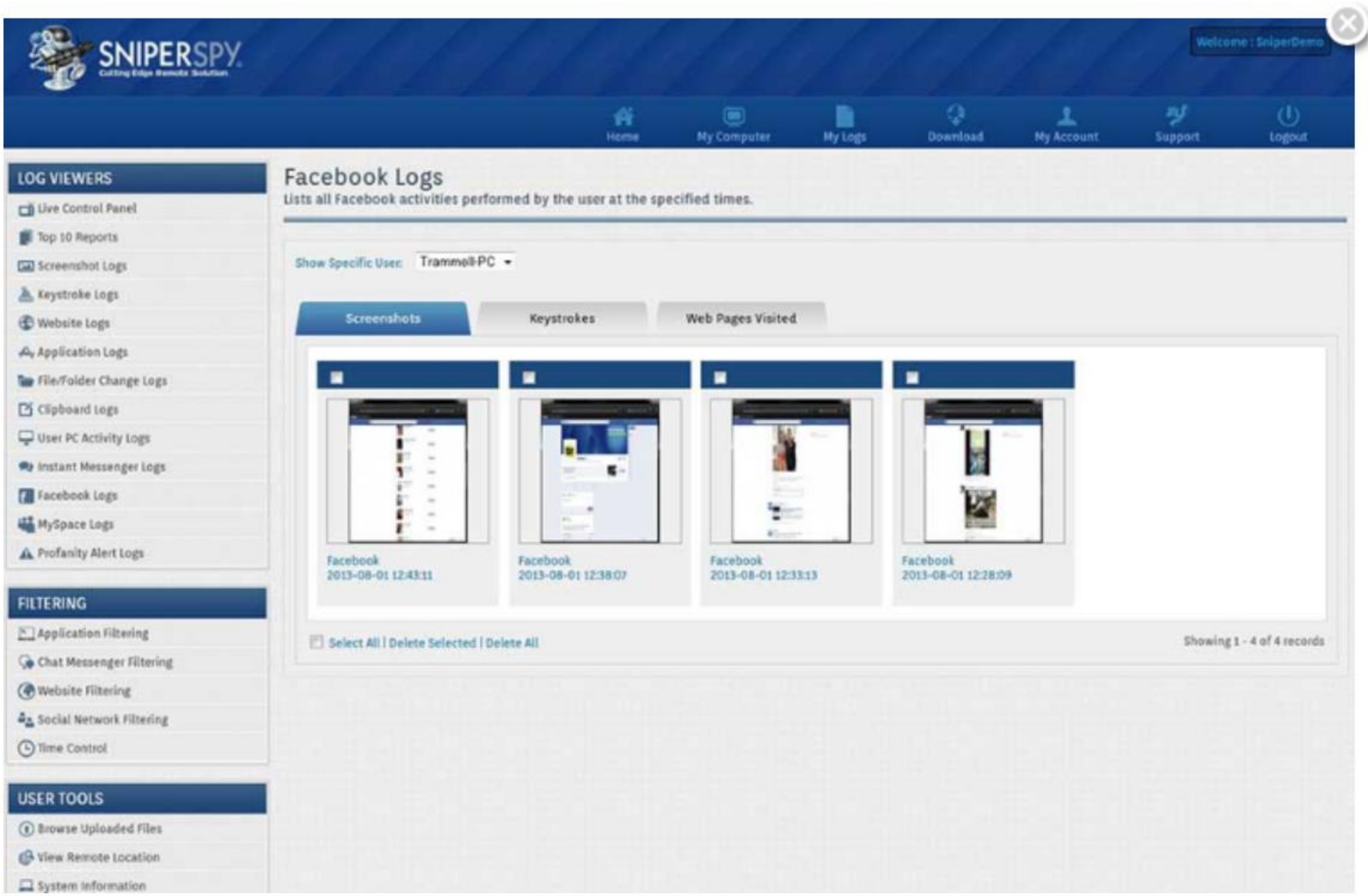
FIRMOWY WIELKI BRAT

- Szef ma prawo nadzorować podwładnych w czasie pracy - dotyczy to również ich aktywności w Internecie.
- pracownicy muszą zostać poinformowani o wprowadzeniu monitoringu. Używanie przez szefa oprogramowania śledzącego bez wiedzy pracownika jest tak samo nielegalne jak podglądanie podwładnych za pomocą ukrytej kamery.
- zasady korzystania ze służbowego sprzętu komputerowego oraz łącza internetowego w miejscu pracy muszą zostać jasno sformułowane w formalnie przyjętym regulaminie.
- Kontrolowany pracownik musi wiedzieć, jakie działania są akceptowane przez jego przełożonych, a za jakie grożą mu sankcje. Również zakres i forma kontroli powinny zostać jednoznacznie określone.

KWIECIEŃ 2016 CHIP.PL

SniperSpy Remote PC Monitoring

Activities Monitored	LIVE Monitoring Tools
✔ Facebook	✔ View the Screen LIVE
✔ Websites Visited	✔ View Locations on a Map
✔ Keystrokes Typed	✔ Browse the File System
✔ Applications Used	✔ Download Remote Files
✔ PC Activity	✔ View / Kill Processes
✔ Clipboard Activity	✔ View Browser History
✔ Instant Messengers	✔ System Information and more!
✔ More	


SNIPERSPY
Welcome : SniperDemo
Home
My Computer
My Logs
Download
My Account
Support
Logout
LOG VIEWERS
Live Control Panel
Top 10 Reports
Screenshot Logs
Keystroke Logs
Website Logs
Application Logs
File/Folder Change Logs
Clipboard Logs
User PC Activity Logs
Instant Messenger Logs
Facebook Logs
MySpace Logs
Profanity Alert Logs
FILTERING
Application Filtering
Chat Messenger Filtering
Website Filtering
Social Network Filtering
Time Control
USER TOOLS
Browse Uploaded Files
View Remote Location
System Information
Facebook Logs
Lists all Facebook activities performed by the user at the specified times.
Show Specific User:
Tramm@-PC
Screenshots
Keystrokes
Web Pages Visited
Facebook
2013-08-01 12:43:11
Facebook
2013-08-01 12:38:07
Facebook
2013-08-01 12:33:13
Facebook
2013-08-01 12:28:09
Select All | Delete Selected | Delete All
Showing 1 - 4 of 4 records

Bezpieczeństwo informacji

- Reguły związane z tworzeniem informacji
- Ogólne zasady obiegu i przechowywania informacji
- Proces niszczenia informacji

Dane osobowe

- Informacje zawierające dane osobowe powinny podlegać ochronie jako informacje niejawne stanowiące tajemnicę służbową oznaczone klauzulą „zastrzeżone”.
- Zbiory danych osobowych powinny być tworzone i przetwarzane (w rozumieniu ustawy o ochronie danych osobowych), w sposób zapewniający zachowanie ich tożsamości i odrębności.
- W trakcie przetwarzania danych należy w szczególności zapewnić uzyskanie dokładnych informacji na temat ich udostępnienia (komu, kiedy, w jakim zakresie, w jakim celu, w jaki sposób, przez kogo) oraz niezwłoczne i zupełne zniszczenie danych nieaktualnych lub, gdy cel, w którym były przetwarzane, został osiągnięty.

Odpowiedzialność za ochronę tajemnicy państwowej

Zgodnie z ustawą z 22 stycznia 1999 roku o ochronie informacji niejawnych osobą odpowiedzialną za ochronę tajemnicy państwowej i służbowej jest kierownik jednostki organizacyjnej, w której informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane.

Ochrona informacji niejawnych w Firmie

- Bezpieczeństwo systemów i sieci teleinformatycznych Firmy powinno być zapewnione przed przystąpieniem do przetwarzania informacji w danym systemie lub sieci.
- Obowiązujące zasady w tym zakresie zawarte są w Szczególnych Wymaganiach Bezpieczeństwa Systemów i Sieci Teleinformatycznych (SWB).
- Integralną częścią każdego eksploatowanego lub wdrażanego systemu teleinformatycznego powinien być podsystem ochrony, a jego formalnym uzupełnieniem są Procedury Bezpiecznej Eksploatacji (PBE).

Bezpieczeństwo teleinformatyczne

- 1. Organizacja i administracja bezpieczeństwem systemów i sieci teleinformatycznych
- 2. Bezpieczeństwo fizyczne systemów i sieci teleinformatycznych
- 3. Bezpieczeństwo sprzętu i oprogramowania
- 4. Bezpieczeństwo personelu
- 5. Bezpieczeństwo dokumentów
- 6. Bezpieczeństwo łączności teleinformatycznej
- 7. Zabezpieczenie antywirusowe
- 8. Plany awaryjne i zapobiegawcze (zailanie, kopie zapasowe)
- 9. Szkolenia i ćwiczenia

Regulacje prawne

- Ustawa o ochronie danych osobowych z 29 sierpnia 1997
- Zgłoszenie bazy do GIODO
- Rozporządzenie MSWiA z 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych
  - **Dane osobowe:** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
  - **Co identyfikuje?** Cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe bądź społeczne lub nr identyfikacyjny np. PESEL
  - **Zgoda** na przetwarzanie musi być dobrowolna

Bezpieczeństwo osób i mienia

- Przedmiot bezpieczeństwa.
- Obowiązki osób funkcyjnych.
- Ochrona fizyczna
- Techniczne zabezpieczenie budynków
- System zabezpieczeń technicznych w Firmie
- Zabezpieczenia zewnętrzne
- Zabezpieczenia wewnętrzne