Monitorowanie pracowników

Aspekty prawne i organizacyjne

Zagrożenia

- Bezpieczeństwo danych (kradzież, nieautoryzowana edycja)
- Bezpieczeństwo IT (sniffing, spoofing, proxy anonimizujące, tunelowanie i przekierowanie połączeń, tabnabbing, clickjacking, DoS, DDoS, SQL Injection, ARP Cache Poisoning, Password Guess)
- Przestępstwo, naruszenie zasad postępowania
- Spadek wiarygodności, utrata klientów, straty finansowe
- Osobista odpowiedzialność kierownictwa

Cele monitorowania pracowników

- Monitorowanie pracy, poprawa jej wydajności
- Pełne wykorzystanie czasu pracy pracownika
- Nadzór właściwego wykorzystania infrastruktury/zasobów IT (sprzęt, sieć, oprogramowanie – legalność)
- Wymuszenie zgodności działań pracowników z zasadami pracy
- Bezpieczeństwo danych i firmy
- Zbieranie dowodów

Rodzaje monitoringu

- Zapobiegawczy
- Ciągły
- Incydentalny

Monitoring zapobiegawczy

- Działania prewencyjne
- Weryfikacja zaangażowania w pracę
  - Czas pracy, wykorzystanie aplikacji
  - Dostęp do zasobów, sieci i Internetu
  - Raportowanie i wsparcie działu IT
- Zgodność działań z regulaminami firmy i IT
- Wymuszenie polityki bezpieczeństwa – **obowiązek pracodawcy**
  - zapobieganie wyciekowi danych
  - Bezpieczeństwo informacji w systemach IT – proces szacowania ryzyka
  - Ustanawianie, wdrażanie, monitorowanie i utrzymywanie bezpieczeństwa informacji

Monitoring incydentalny

- Podejrzenie działania niezgodnie z regułami
- Podejrzenie kradzieży danych
- Podejrzenie popełnienia przestępstwa (również dopuszczalny monitoring ciągły)

Monitoring – uprawnienia pracodawcy

- Aktywność w Internecie, kategoryzowanie treści
- Dostęp do zasobów
- Wykorzystanie aplikacji, instalacja/deinstalacja aplikacji
- Zmiany sprzętowe
- Podgląd pulpitu
- Monitorowanie aktywności stacji roboczej: uruchomione procesy, otwarte porty, powiązania w warstwie 2, transmisje, analiza komunikacji, logi aplikacji i systemowe

Podstawy prawne

- Brak szczegółowych regulacji prawnych
- Możliwość „naginania” przepisów przez pracownika i pracodawcę
- Trudność z określeniem legalności sposobu monitorowania
- Brak wskazania dopuszczalnych sposobów technicznych w obowiązujących przepisach

Podstawy prawne – prawa i obowiązki pracodawcy

- Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy: art. 11, art. 15, art. 22, art. 94
- Ustawa z dnia 29 VII 1997 r. o ochronie danych osobowych: Rozdział 5
- Rozporządzenie MSWiA z 29 IV 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do tego służące
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe: pkt. 10 lit. e Załącznika nr 1

Podstawy prawne – prawa i obowiązki pracownika

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.: art. 47, art. 49, art. 51
- Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy: art. 100, art. 114-122, art. 128 §1
- Ustawa z dnia 29 VII 1997 r. o ochronie danych osobowych: art. 39 ust. 2
- Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny: art. 23-24

Podstawy prawne – odpowiedzialność pracodawcy

- Ustawa z dnia 29 VII 1997 r. o ochronie danych osobowych: art. 49, art. 51-52
- Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny: art. 23-24
- Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny: art. 218, art. 267

Procedury

- Plan wdrażania monitorowania i kontroli działań pracowników: zakres i forma, zastosowane narzędzia, projekt techniczny, przygotowanie procedur bezpieczeństwa, regulaminów, procedur wewnętrznych, dokumentacji
- Określenie celu monitorowania:
  - Ochrona danych i tajemnicy przedsiębiorstwa
  - Zabezpieczenie interesów pracodawcy
  - Ochrona mienia firmy
- Określenie zasad korzystania z infrastruktury IT:
  - Wykorzystanie sprzętu i poczty do celów prywatnych
  - Podłączanie prywatnego sprzętu
  - Zasady postępowania ze sprzętem, oprogramowaniem, pocztą, systemami IT

Procedury

- Minimalizacja możliwości naruszenia prywatności pracownika
- Określenie dostępu, miejsca i formy przechowywania danych z monitoringu
- Publikacja zasad i zapoznanie z nimi pracowników:
  - Pisemna publikacja reguł i sposobów monitoringu **przed uruchomieniem**
  - Miejsce publikacji: umowa o pracę, regulamin pracy, polityka bezpieczeństwa IT/informacji, układ zbiorowy pracy
  - Zgoda pracownika nie jest wymagana
- Monitoring pracownika bez jego wiedzy jest dopuszczalne, jeśli powiadomienie go uniemożliwi osiągnięcie celu monitorowania, np. zbieranie dowodów popełnienia przestępstwa

Dokumentacja

Bezpieczeństwo informacji - w dokumentacji powinno określić się:

- Ogólne cele, zakres i strategię bezpieczeństwa informacji
- Osoby odpowiedzialne za bezpieczeństwo informacji
- Procedury postępowania z zasobami IT, zasady używania systemów teleinformatycznych oraz zasady dostępu do systemów i zasobów
- Przypadki, w których przeprowadzane jest postępowanie dyscyplinarne
- Zasady używania środków służbowych do celów prywatnych
- Zasady kontroli wejścia i wyjścia
- Postępowanie przy dostępie osób trzecich
- Sposoby monitorowania bezpieczeństwa przetwarzanych danych
- Sposoby i miejsca wykorzystania zabezpieczeń kryptograficznych

Dokumentacja

Bezpieczeństwo informacji - w dokumentacji powinno określić się:

- Procedury i zasady postępowania ze sprzętem: zakup, odbiór i montaż; konserwacja i naprawa; wycofanie sprzętu i niszczenie nośników
- Zasady dostępu do zasobów sieciowych zarówno dla pracowników jak i z zewnątrz oraz monitorowanie tego dostępu:
  - Kontrola i monitorowanie dostępu do sieci firmowej oraz sieci publicznej
  - Kontrola dostępu do systemów i aplikacji
  - Polityka haseł
  - Kontrola wydruków
  - Monitoring, analiza, zgłaszanie oraz postępowanie z incydentami naruszenia bezpieczeństwa.

axence

Dokumentacja

Zasady IT, bezpieczeństwo informacji:

- Zasady użytkowania komputerów przenośnych
- Zasady dostępu zdalnego i pracy zdalnej
- Zasady IT
- Zgłaszanie i zarządzanie incydentami naruszenia bezpieczeństwa
- Polityka kontroli dostępu – przyznawanie praw dostępu
- Monitorowanie
- Wykrywanie włamań
- Uprawnienia administratorów systemów
- Zarządzanie ciągłością działania

Dozwolone formy nadzoru

Kontrola dozwolona ze względu na ochronę interesów pracodawcy:

- Kontrola sprzętu pracownika, danych służbowych
- Pracownik ma obowiązek udostępnienia hasła zabezpieczającego dane
- Pracownik może przechowywać prywatne dane tylko za zgodą pracodawcy
- Poczta służbowa może podlegać kontroli – prywatna **nie**, dlatego należy zablokować dostęp do prywatnej poczty oraz wprowadzić zakaz jej używania (ze względu na możliwość wycieku danych) – uwzględniając programy lokalne oraz dostęp przez WWW.
- **UWAGA**: Zapoznanie się z prywatną pocztą pracownika narusza ustawę o ochronie danych osobowych oraz tajemnicę korespondencji. Może mieć poważne konsekwencje wynikające z Kodeksu Karnego.

axence

Dozwolone formy nadzoru

- Najlepsze rozwiązanie pod względem prawnym, w zakresie bezpieczeństwa, to ograniczanie dostępu oraz automatyczna kontrola (prawa dostępu, prawa do wykonywania określonych czynności)
- Kontrola dostępu do informacji w Internecie ze względu na zapewnienie bezpieczeństwa oraz kontrolę efektywności pracy
- Ruch sieciowy może być rejestrowany – z ograniczeniem możliwości analizy treści pakietów danych

Ustawa o ochronie danych osobowych

- Dopuszczalność przetwarzania danych (art. 23.1):
  - Gdy osoba, której dane dotyczą, wyrazi na to zgodę (za wyjątkiem usuwania danych)
  - Gdy jest to niezbędne do realizacji uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa
  - Gdy jest to konieczne do realizacji umowy, gdy osoba jest stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie tej osoby
  - Gdy jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego

Ustawa o ochronie danych osobowych

- Dopuszczalność przetwarzania danych (art. 23.1)
  - Gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
  - Za prawnie usprawiedliwiony cel, o którym mowa w art. 23 ust. 1 pkt 5, uważa się w szczególności: marketing bezpośredni własnych produktów lub usług administratora danych; dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

Ustawa o ochronie danych osobowych

Zakres przetwarzania danych:

- Zakres przetwarzanych danych powinien być adekwatny do celu przetwarzania.
- Zakres nie powinien obejmować m.in.:
  - Danych korespondencji prywatnej
  - Informacji nie wymaganych w celu zapewnienia bezpieczeństwa danych
  - Informacji nie wymaganych w celu oceny efektywności wykonywanej pracy.

Ustawa o ochronie danych osobowych

Zabezpieczenie danych:

- Pracodawca ma obowiązek zabezpieczyć dane przed dostępem osób nieupoważnionych
- Należy zastosować środki organizacyjne oraz techniczne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności należy zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Ustawa o ochronie danych osobowych

Archiwizacja danych:

- Pracodawca ma prawo przetwarzać dane nie dłużej niż do momentu osiągnięcia celu przetwarzania
- Celem przetwarzania jest zapewnienie bezpieczeństwa informacji oraz kontrola efektowności pracy użytkownika komputera i sieci
- Zwyczajowo archiwizuje się dane z monitoringu z trzech ostatnich miesięcy.

Incydenty naruszenia bezpieczeństwa

- Incydent naruszenia bezpieczeństwa – zdarzenie umożliwiające nieuprawniony dostęp lub go stanowiące. Również zdarzenie, które potencjalnie może prowadzić do spowodowania strat w organizacji poprzez ujawnienie danych, dezinformację lub utratę danych.
- Wykrycie i określenie rodzaju incydentu naruszenia bezpieczeństwa w systemie informatycznym jest jednym z obowiązków Administratora Systemu.
- Przed incydentem: przygotowanie procedur i konfiguracji systemów mających na celu zbieranie możliwie jak największej liczby zapisów pozwalających na późniejszą analizę.
- Po incydencie: podjęcie działań mających na celu identyfikację intruza; zebranie dowodów (śladów elektronicznych) z komputera, serwera lub urządzenia sieciowego (dyski, zapisy logów, zrzuty ekranów, inne).

Monitorowanie legalności wykorzystania oprogramowania

Ryzyko popełnienia przestępstwa, gdy:

- Organizacja posiada nielegalne oprogramowanie i kierownictwo nie podejmuje niezwłocznie działań naprawczych
- Osoby pracujące w firmie na komputerach instalują (kopiują) oprogramowanie samodzielnie bez wiedzy i zgody osoby odpowiedzialnej
- Osoby wykonują dla swoich celów domowych kopię programu zainstalowanego w firmie (i odwrotnie).

Przykłady niebezpiecznych działań pracowników

Anonimizacja:

- Wykorzystanie web proxy publicznego – https://hidemyass.com/. Użytkownicy serwisu łączą się ze stronami WWW poprzez mało znane niezablokowane serwery. Przykład linku do witryny http://sympatia.pl: http://5.hidemyass.com/ip-1/encoded/Oi8vc3ltcGF0aWEub25ldC5wbC8%3D
- Wykorzystanie web proxy: pobranie z Internetu listy proxy i wykorzystanie jednego z nich do zmiany adresu IP i kraju, z którego się łączymy np. http://anonymizer.nntime.com/
- Wykorzystanie proxy publicznego: pobranie z Internetu listy publicznych proxy i wpisanie w konfiguracji przeglądarki. Listę proxy można znaleźć np. pod adresem http://proxy.net.pl.

Przykłady niebezpiecznych działań pracowników

Anonimizacja:

- Wykorzystanie proxy prywatnego: uruchomienie własnego serwera proxy na adresie lub domenie dostępnej z sieci firmowej, a następnie tunelowanie połączeń.

Tunelowanie:

- Wykorzystanie serwera SSH: uruchomienie własnego serwera SSH lub wykorzystanie innego, na którym użytkownik ma konto. Następnie uruchomienie na komputerze programu putty.exe, (nie wymaga instalacji). Po zestawieniu połączenia z serwerem SSH wystarczy skonfigurować przeglądarkę tak, aby korzystała z serwera proxy.

Przykłady niebezpiecznych działań pracowników

Tunelowanie:

- Wykorzystanie przeglądarki i TOR: TOR jest darmowym projektem stworzonym w celu zachowania anonimowości użytkownika. Wpisując w przeglądarce jako proxy socket otwarty na wskazanym porcie, ruch przeglądarkowy zaczyna trafiać do sieci TOR. Połączenia pomiędzy węzłami TOR są szyfrowane i podlegają zmianie (rozwiązywaniu poprzednich i tworzeniu nowych połączeń). Kolejną zasadą w sieci TOR jest częściowa tylko informacja o drodze pakietu w pojedynczym węźle.