Uniknąć przypadku Wikileaks skuteczna ochrona danych

Tomasz Palonek
Program Manager

Agenda

- „Problem” danych
- Sposoby zabezpieczenia danych
- Szyfrowanie
- Data Loss Prevention
- Algorytmy wykorzystywane do analizy danych
- Bezpieczeństwo w firmie – bezpieczeństwo informacji

„Problem” danych

- Każda instytucja/firma posiada dane
  - Pracownicy
  - Klienci
  - Dane finansowe
  - Informacje marketingowe
  - Własność intelektualna
  - …
- Problem
  - Jak dane składować?
  - Jakie dane chronić?
  - Kto powinien mieć do nich dostęp?
  - W jaki sposób je zabezpieczyć?

Sposoby zabezpieczenia danych

- Zabezpieczenie danych przed fizycznym dostępem
- Backup
- Hasła
- Zabezpieczenie przed niepowołanym dostępem
- Szyfrowanie
- Kontrola stacji końcowej
- Zabezpieczenie przed wyciekiem danych

Szyfrowanie

- Partycje i dyski,
- Zasoby – pliki i foldery, zasoby sieciowe,
- Bazy danych,
- Certyfikaty,
- Pamięci przenośne,

Data Loss Prevention
ochrona przed utratą/wyciekiem danych

Ochrona przed utratą ważnych danych

- Tajemnica handlowa i własność intelektualna
- Dane finansowe, raporty giełdowe
- Poufne dane klientów

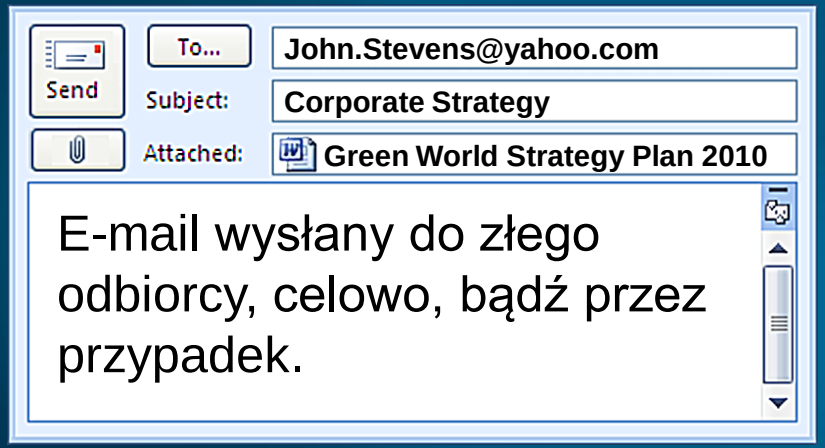
Konsekwencje utraty danych

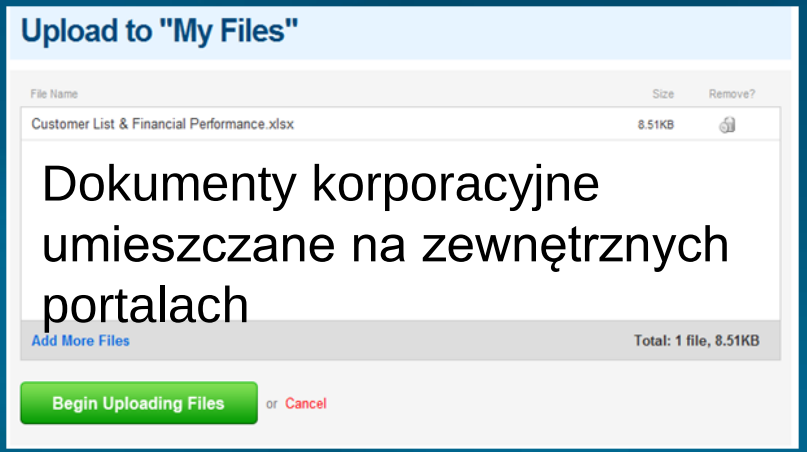
- Utrata wiarygodności, „zła prasa”
- Kary umowne
- Odpowiedzialność karna

SOLIDEX®
Integrujemy przyszłość®

Naruszenie bezpieczeństwa danych

80 - 90% incydentów ma charakter przypadkowy





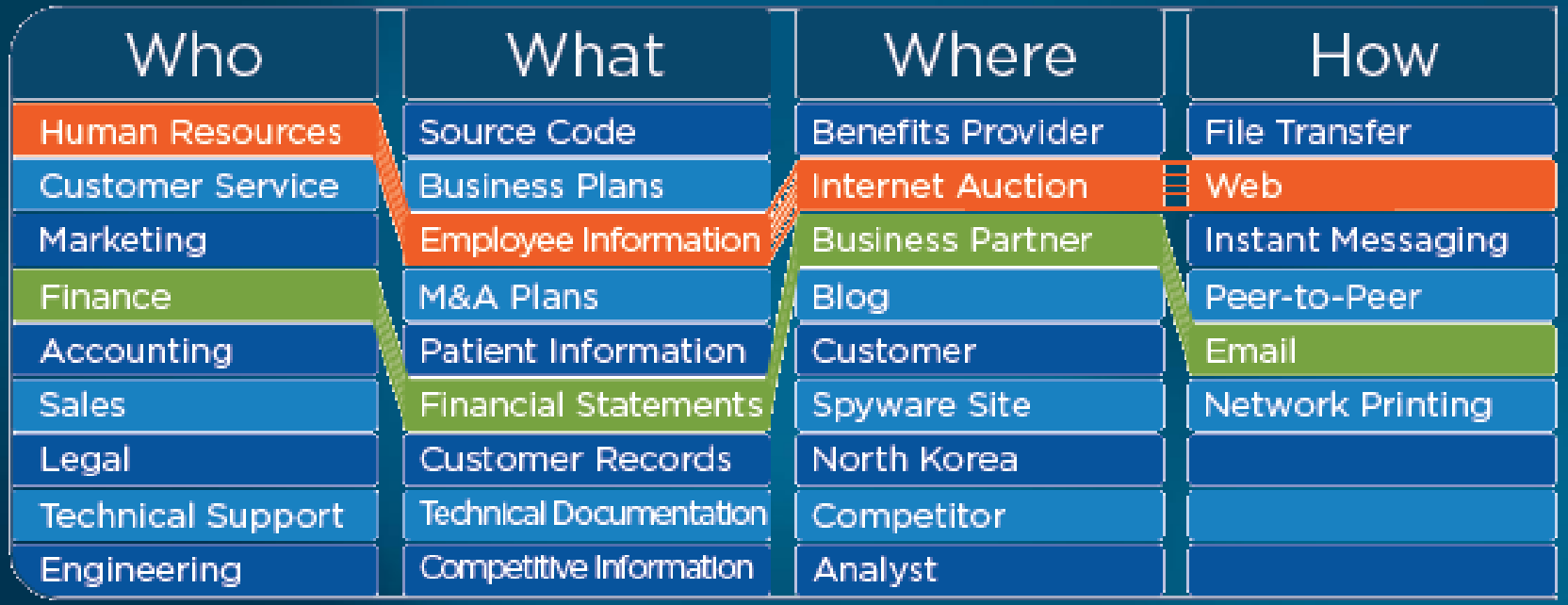
Takie ‚incydenty' zdarzają się każdemu z nas.

SOLIDEX®
Integrujemy przyszłość®

Charakterystyka rozwiązań DLP

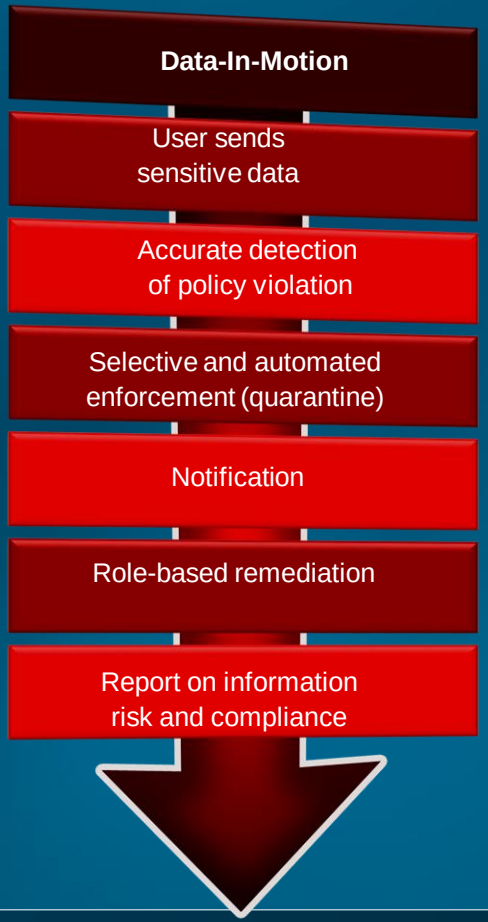
- Ludzie
  - Kto jest użytkownikiem?
  - Kto „produkuje” dane wrażliwe?
  - Kto posiada dostęp do danych?
  - Czy firma zatrudnia pracowników mobilnych?
- Dane
  - Jakie dane posiadamy?
  - Gdzie one są składowane i w jakiej postaci?
  - Jaki priorytet tym danym możemy nadać?
- Procesy biznesowe
  - Jakie kanały komunikacyjne wykorzystujemy?
  - Jakie zabezpieczenia stosujemy?
  - Jaki jest profil działalności firmy, Jakie standardy/regulacje musimy spełnić?

Charakterystyka rozwiązań DLP



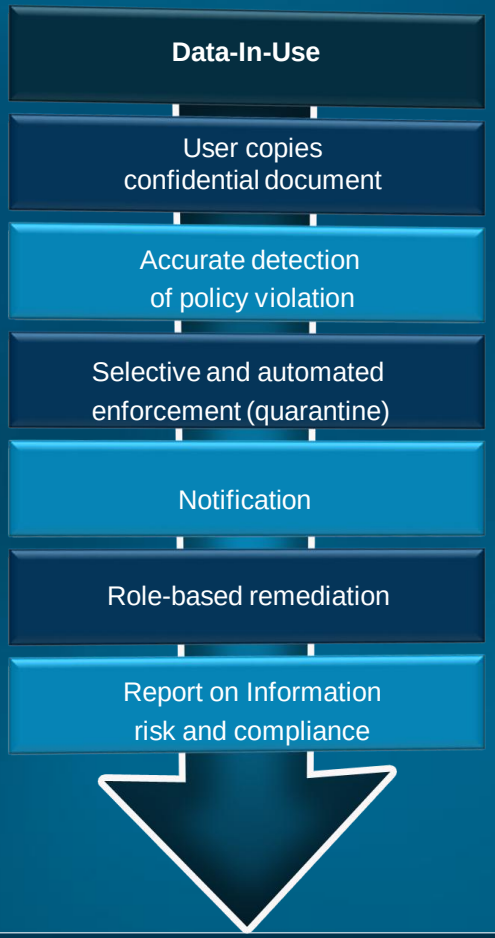
Data-in-Motion

- Informacje przesyłane z wykorzystaniem poczty, sieci web, oraz innych kanałów komunikacyjnych.
- Monitorowanie i ochrona danych w ruchu:
  - Monitorowanie sieci (pasywne, serwer proxy)
  - Email i Web – dwa najistotniejsze kanały komunikacyjne w kontekście ochrony danych
  - Oprogramowanie na stacji końcowej może monitorować i kontrolować ruch sieciowy



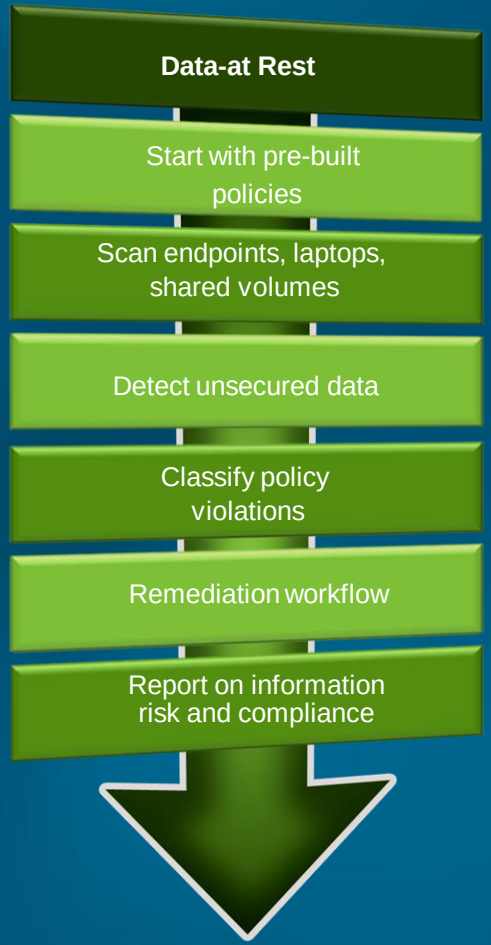
Data-at-Rest

- Informacje przechowywane w repozytoriach takich jak bazy danych oraz serwery plików
- Wyszukiwanie (discovery) danych w spoczynku:
  - Skanowanie zdalne – pozwala sprawdzić, do jakich danych ma dostęp regularny użytkownik usługi katalogowej
  - Lokalny agent pozwala wykryć nieautoryzowane kopie danych na serwerach w firmie i komputerach pracowników



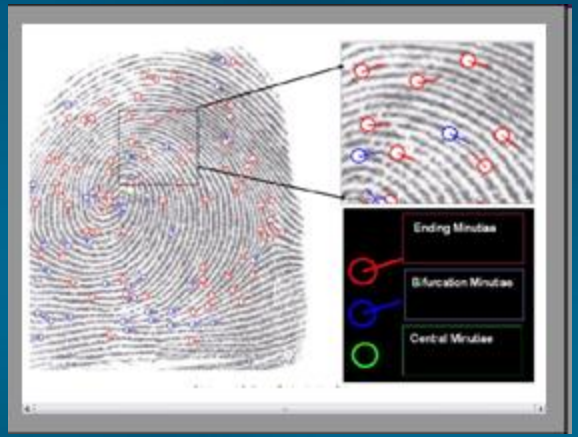
Data-in-Use

- Informacje wykorzystywane przez pracowników, np. kopiowane na nośniki USB, płyty CD/DVD, przetwarzane w aplikacjach.
- Ochrona realizowana przez oprogramowanie instalowane na komputerach pracowników :
  - Wymagane dla lokalnego discovery
  - Różne polityki wewnątrz i na zewnątrz sieci firmy
  - Opcja „Potwierdź”
  - …

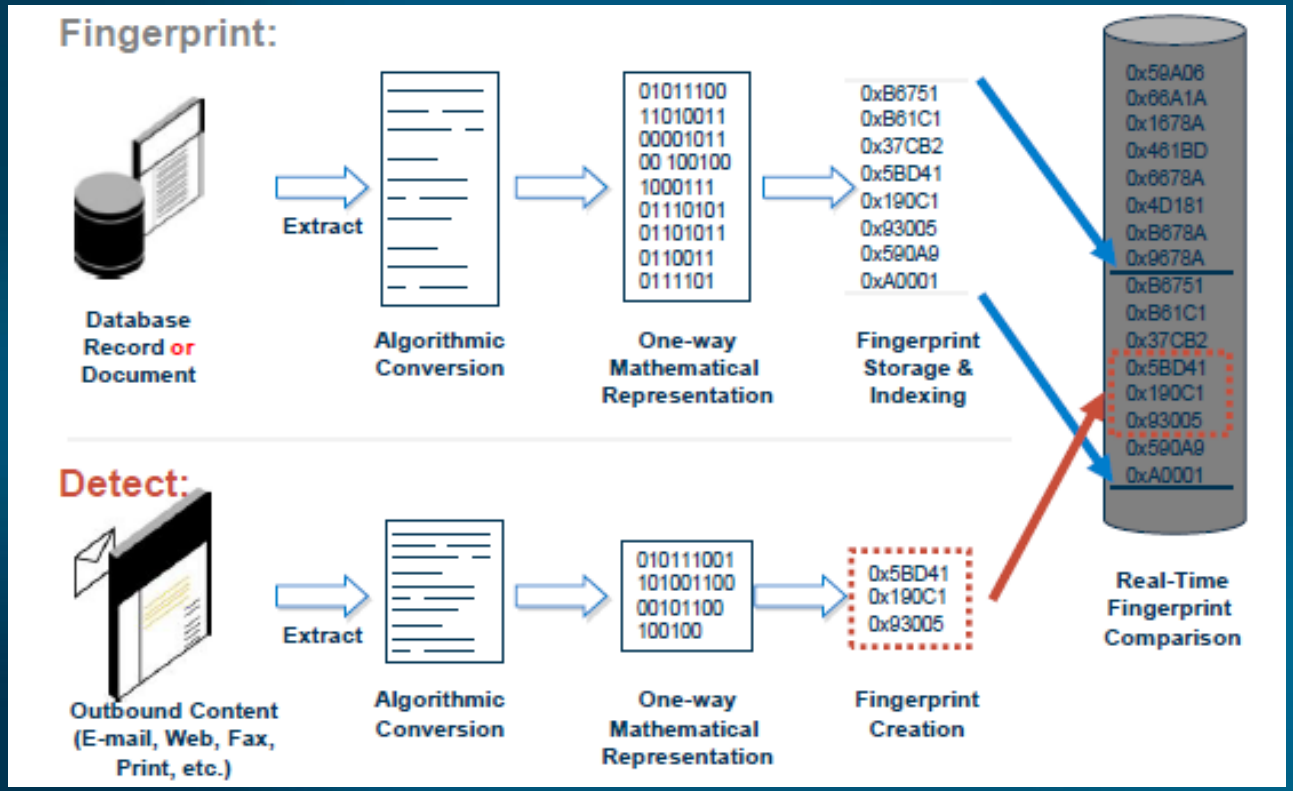


Algorytmy wykorzystywane do analizy danych

- Filtry globalne
  - Filtry bazujące na typach plików
  - Sygnatury binarne bazujące na plikach
  - Sygnatury binarne oparte na tekście
- Filtry bazujące na tokenach
  - Rozpoznawanie wzorca
  - Wyrażenie i słowa kluczowe
- Filtry kontekstowe
  - Zarządzanie rekordami
  - Tekstowe „odciski palca”
  - Macierzowe „odciski palca”
  - „Odcisk palca” CAD/CAM
  - „Odcisk palca” szablonów i formularzy



Mechanizmy wykorzystywane do analizy danych



SOLIDEX®
Integrujemy przyszłość®

Realizacja projektu

Ocena

- Wymagania biznesowe
  - Definicja danych
  - Kryteria sukcesu
- Wymagania techniczne
  - Magazyny danych
  - Prawa dostępu
  - Kanały komunikacji
  - Architektura sieciowa

Projekt

- Architektura rozwiązania
- Zestaw polityk
- Zarządzanie i reagowanie na incydenty
- Plan gotowości operacyjnej

Wdrożenie (etapami)

- Audyty i raporty
- Powiadomienia
- Egzekwowanie polityki

Strojenie i optymalizacja

- Strojenie i rozbudowa polityk
- Kolejne obszary pokrycia

SOLIDEX®
Integrujemy przyszłość®

Problemy związane z DLP

- Trudno opracować w 100% skuteczny algorytm wykrywania zdarzeń typu DLP:
  - Zasady DLP są zależne od kontekstu (co jest wysyłane, do kogo, kto wysyła)
- Analiza wykrytych zdarzeń jest dużym obciążeniem
  - Angażowanie zasobów (czas, ludzie, komputery, dyski)
  - Udostępnianie administratorom wglądu do poufnych danych
- Większość rozwiązań pracuje w trybie wykrywania (*detect*)
  - Uruchomienie w trybie blokowania (*Prevent)* może zatrzymać pracę przedsiębiorstwa

Bezpieczeństwo

- Firewall
- Intrusion Prevention System
- Security Web Gateway
- Email Gateway
- Zdalny dostęp (SSL VPN)
- Network Access Control (NAC)
- Data Leak Prevention (DLP)
- Wieloskładnikowa autentykacja
- Systemy SIEM (Security Information and Event Management),
- Szyfrowanie,
- Zabezpieczenie stacji końcowej,
- Systemy do wykrywania „podatności” w sieci

Zapraszamy do skorzystania z usług naszych SOLIDnych EXpertów.

Centrala

ul. J. Lea 124,
30-133 Kraków
tel. +48 12 638 04 80
fax: +48 12 638 04 70

www.SOLIDEX.com.pl

SOLIDEX®
Integrujemy przyszłość®