AUDYT BEZPIECZEŃSTWA INFORMACJI

ZAKRES I TECHNIKI

Michał Głowacki
Instytut Audytu Sektora Publicznego

Ministerstwo Finansów
26 marca 2013 r.

Przegląd zagadnień

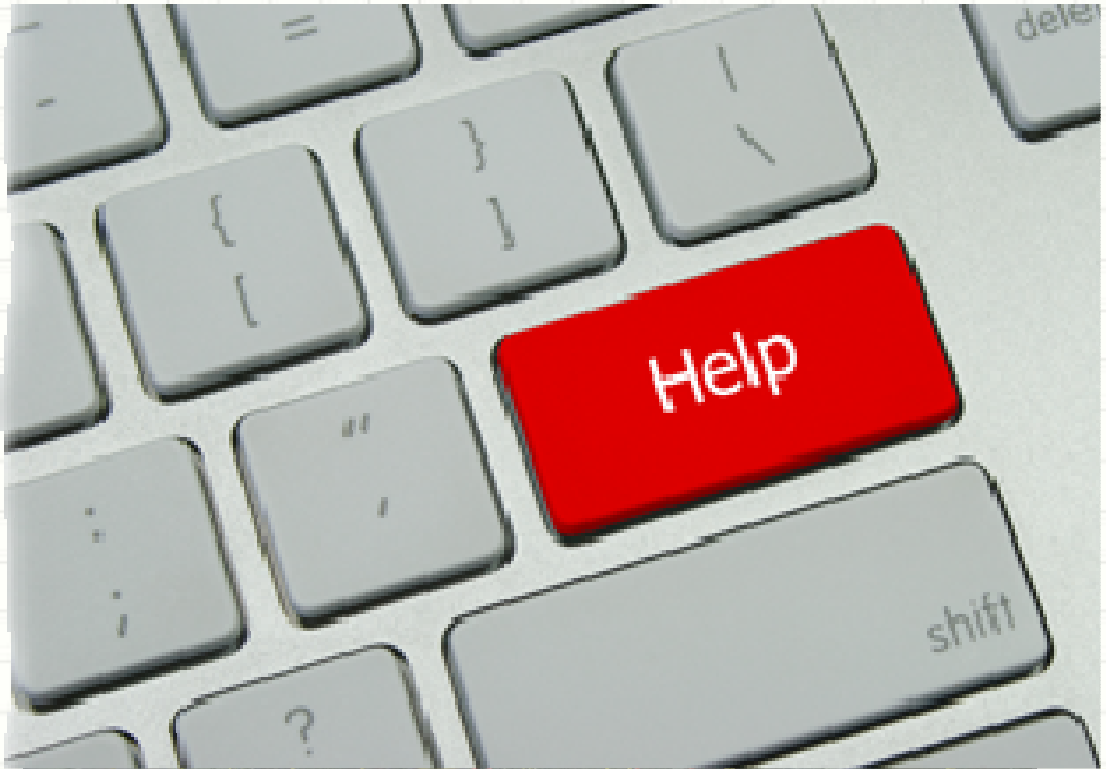
1. Rola informatyki w działalności jednostki
2. Ustalenie zakresu audytu
3. Zakres podstawowy
4. Najczęściej spotykane zagrożenia
5. Kluczowe systemy informatyczne
6. Czynności sprawdzające

1

ROLA INFORMATYKI W DZIAŁALNOŚCI JEDNOSTKI

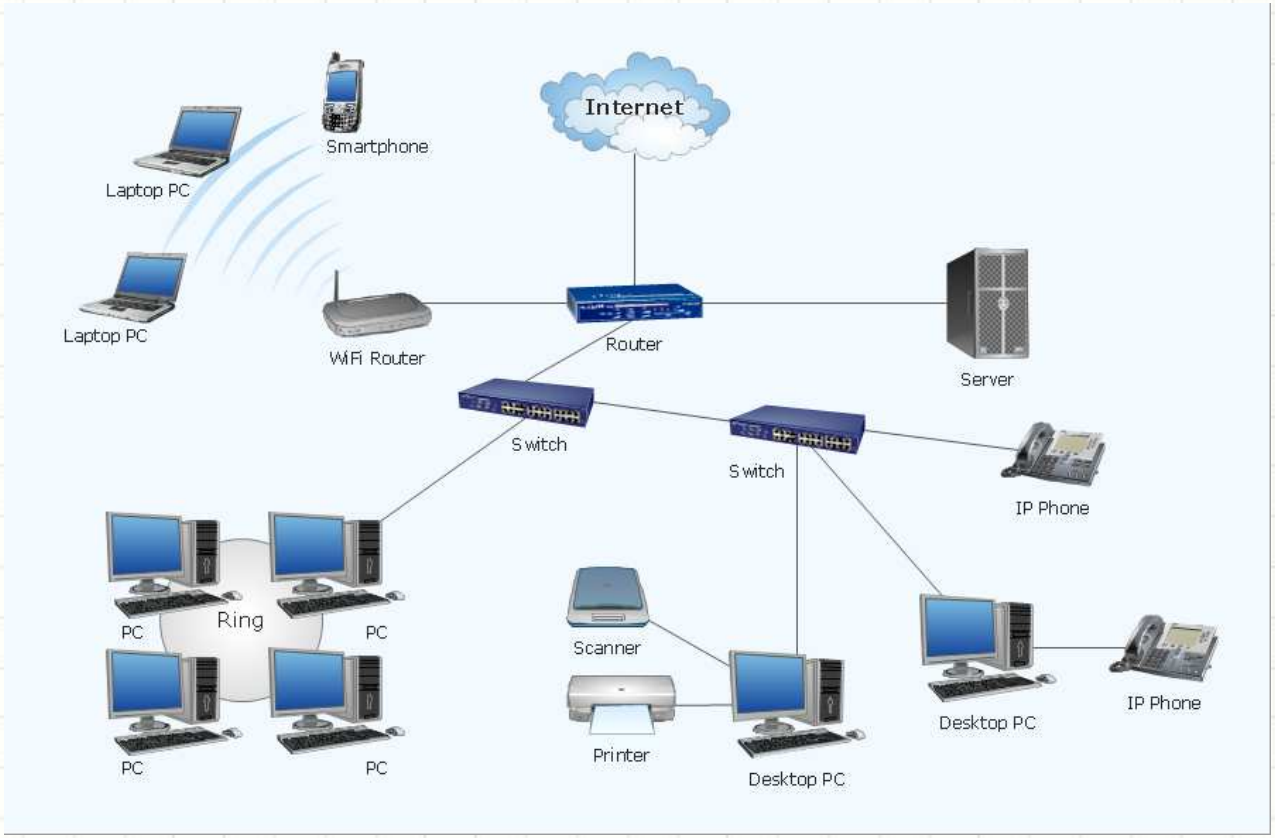
INFORMATYKA W JEDNOSTCE

- „A u mnie działa!” -> jednostka jest dla IT
- „Jakoś” -> wszyscy tak mają
- „Jakość” -> rola służebna



INFORMATYKA W JEDNOSTCE – PORZĄDEK MUSI BYĆ!

- **Procedury dotyczące jednostki (PBI)**
- **Procedury wewnętrzne Działu Informatyki**



PROCEDURY W SYSTEMACH INFORMATYCZNYCH

- System ABC
  - Kto jest właścicielem systemu
  - Kto wnioskuje o zmiany
  - Kto zatwierdza
  - Kto wykonuje

2

USTALENIE ZAKRESU AUDYTU

ZAKRES

- Co chcemy chronić i dlaczego
  - Zasoby kluczowe
  - Zasoby mniej istotne
  - Sprzęt
    - Utrata ciągłości działania
  - Oprogramowanie
    - Brak funkcjonalności
  - Informacje (dane)
    - Uszkodzenie
    - Wykradzenie

ZAKRES

- Co może zrobić audytor bez specjalistycznej wiedzy
  1. Procedury
  2. Licencje
  3. Sprzęt
  4. Konta w systemach

ZAKRES

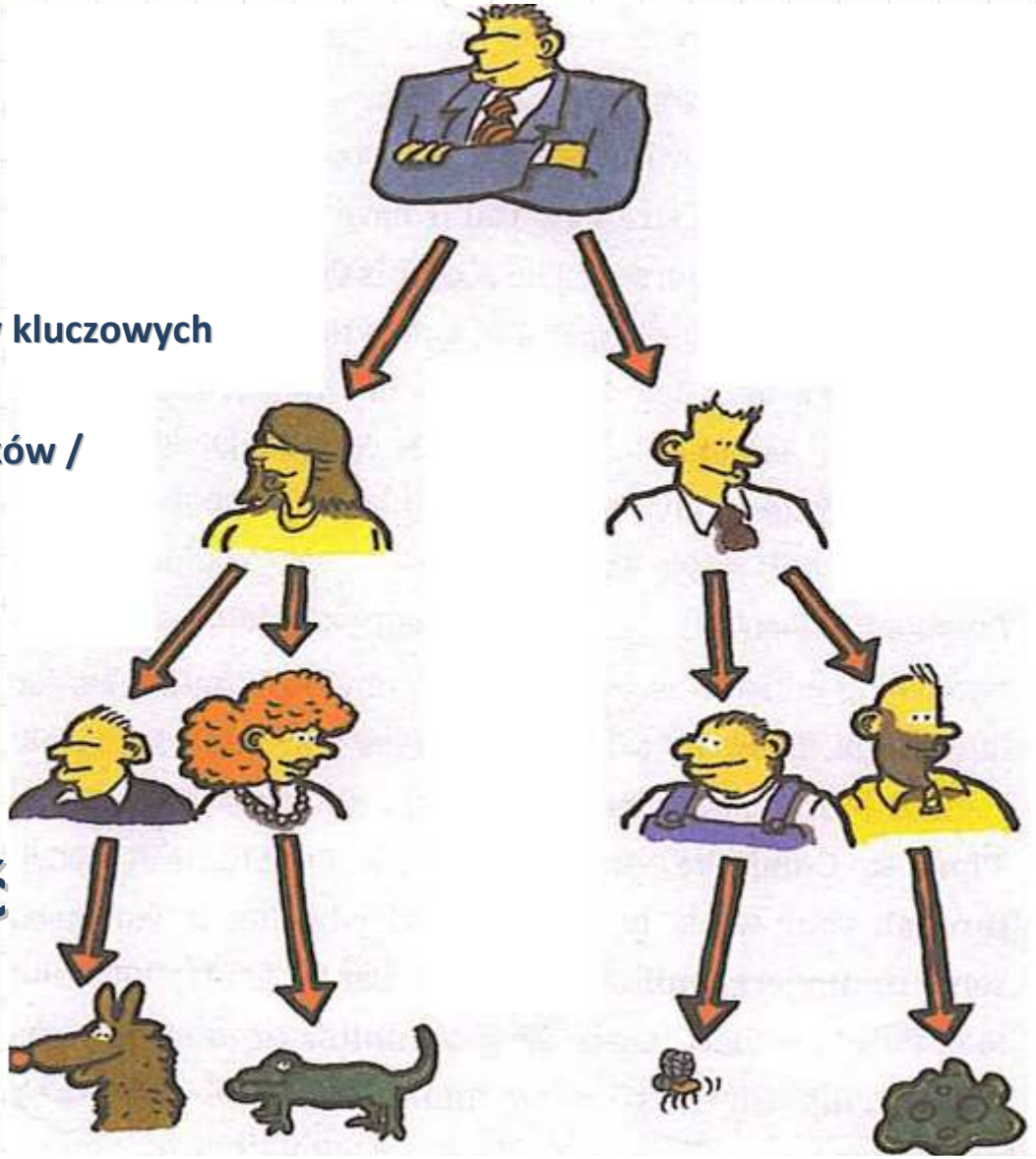
- Co może wymagać pomocy
  - Aktualizacje oprogramowania na stacjach roboczych i na serwerach (np. automatycznie przez serwer Microsoft WSUS lub ręcznie)
  - Ustawienia parametrów (dla grup)
  - Przegląd logów systemowych (2 lata)
  - Konta administratorskie (admin, root-sudo)
  - Procesy usługowe i interaktywne
  - Struktura (topologia) sieci
  - Wydajność sieci
  - Ustawienia dostępów z zewnątrz
  - Testy penetracyjne sieci

3

ZAKRES PODSTAWOWY

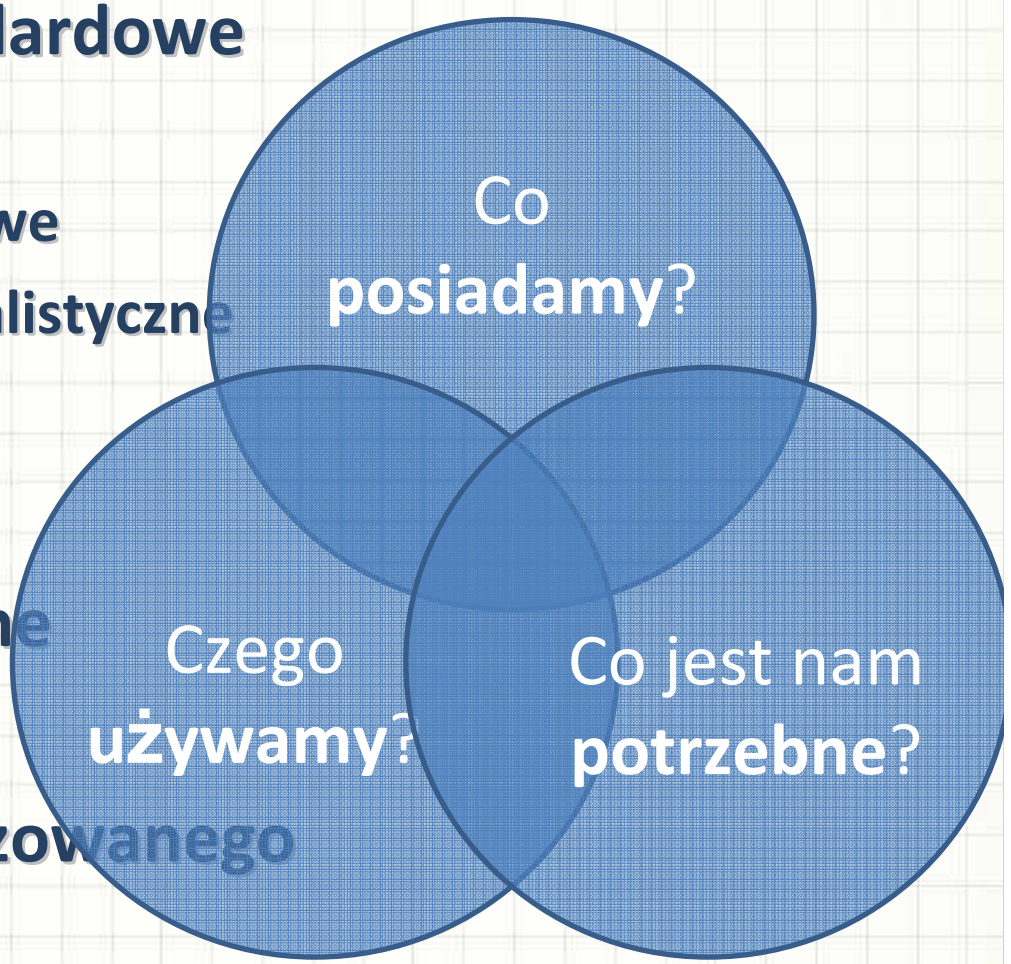
AUDYT PROCEDUR

- **Role**
  - GRUPY
  - UŻYTKOWNICY
  - INFORMATYKA
    - Administratorzy systemów kluczowych
    - Administrator sieci
    - Administrator serwera plików / serwera pocztowego / archiwizacji danych
    - Analityk
    - Tester
    - Programista
    - Helpdesk
- **Odpowiedzialność**
  - Środowiska: TEST/PROD



AUDYT LICENCJI

- **Oprogramowanie standardowe**
  - **Systemy operacyjne**
  - **Oprogramowanie biurowe**
  - **Oprogramowanie specjalistyczne**
    - **Finanse-Księgowość**
    - **Kadry-Płace**
    - **…**
- **Programy specjalistyczne**
- **Wykrywanie nieautoryzowanego oprogramowania**
- **Zabezpieczanie przed instalowaniem**



AUDYT INFRASTRUKTURY

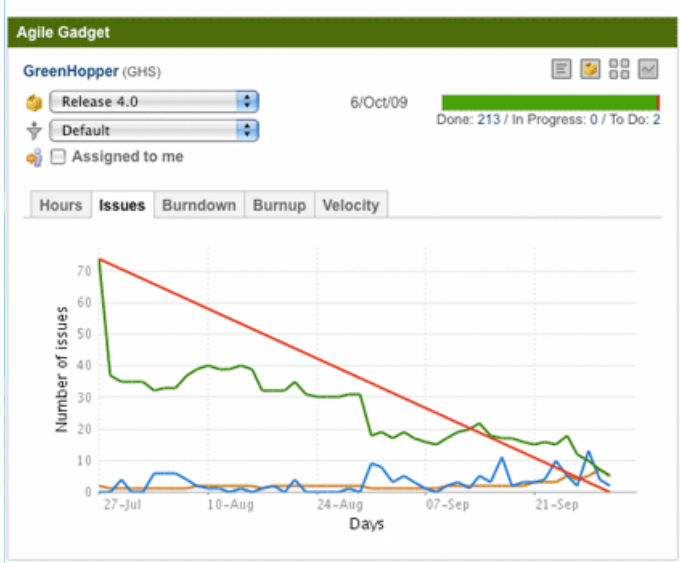
- **SPRZĘT czyli: Informatyka nie jest tania**
  - Serwery
  - Urządzenia sieciowe
  - Serwerownie
  - UPS
  - Centra zapasowe
  - Komputery i notebooki

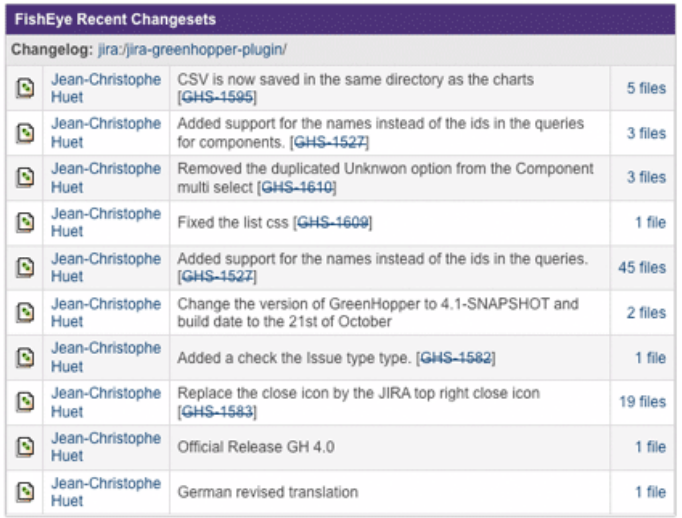
AUDYT INFRASTRUKTURY

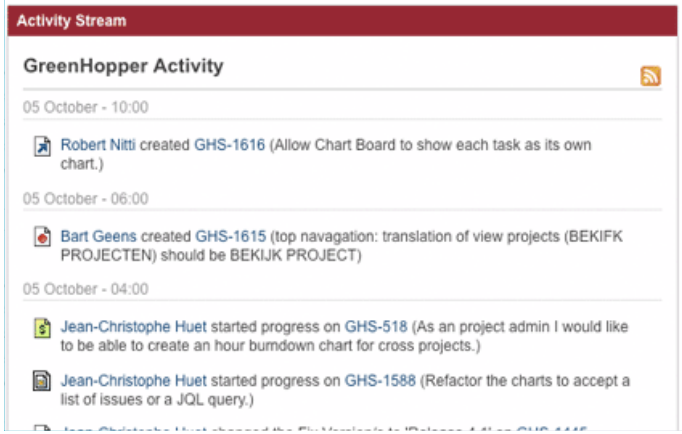
- CO WARTO SPRAWDZAĆ:

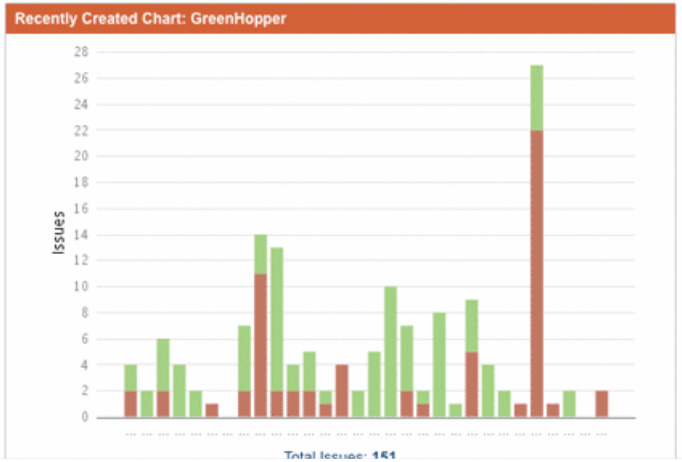
3. Odtwarzanie danych

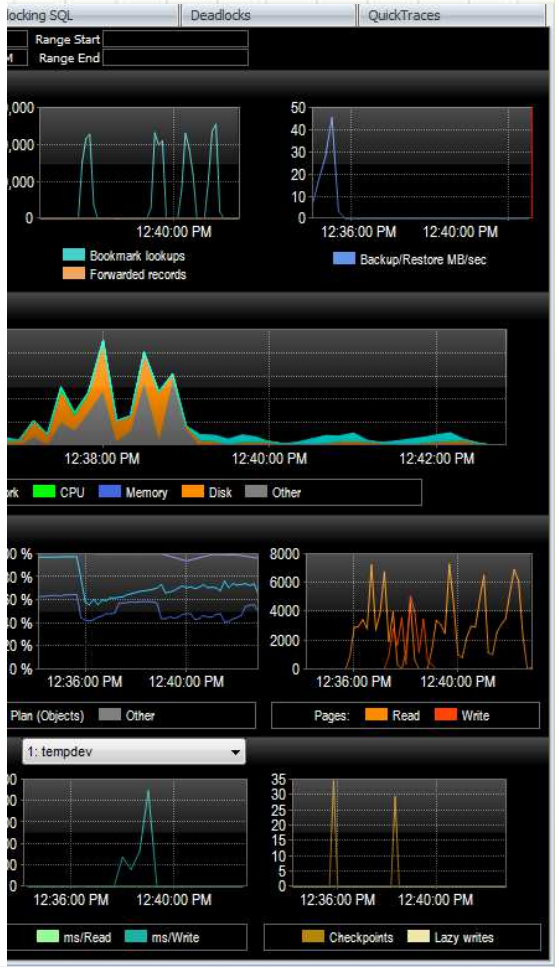
1. Użycie zasobów sprzętowych





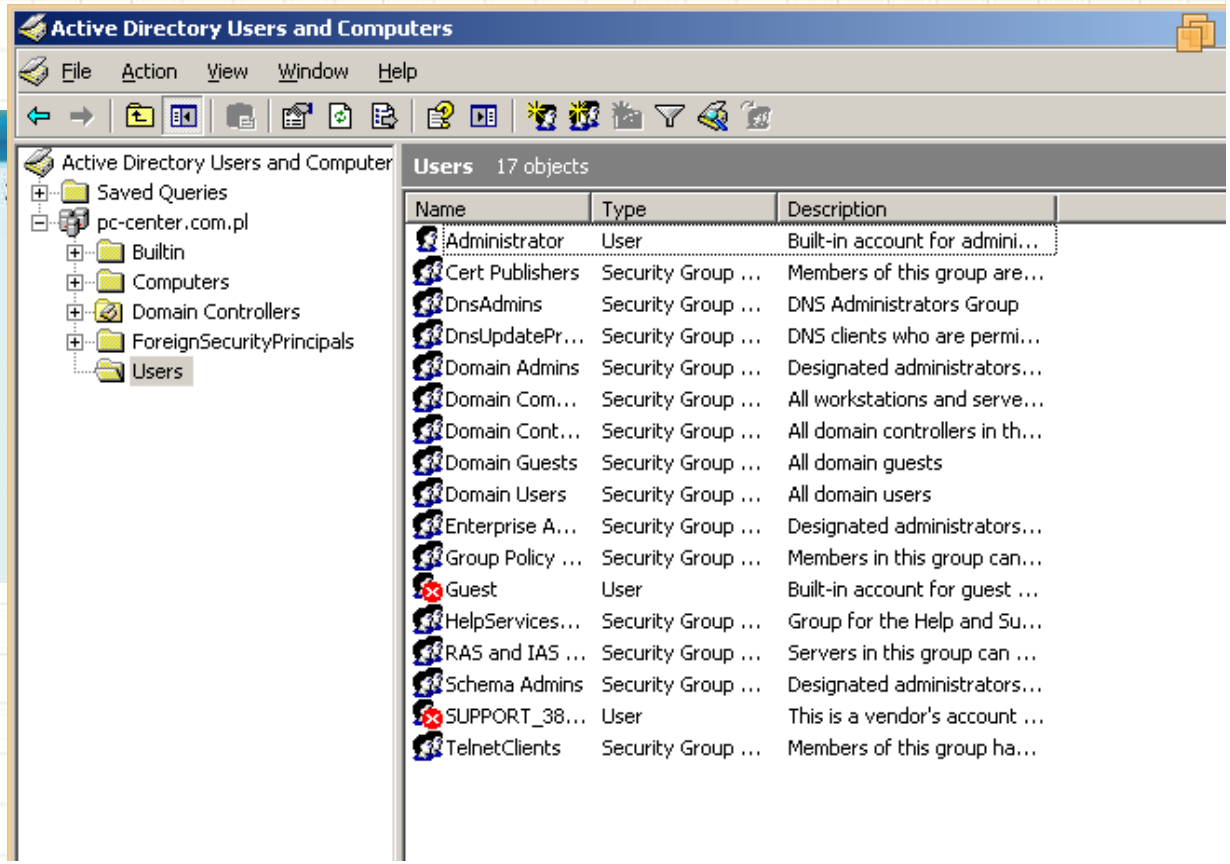






AUDYT UŻYTKOWNIKÓW I UPRAWNIEŃ

- Lista kont użytkowników
- Lista uprawnień WYBRANYCH użytkowników w WYBRANYCH systemach

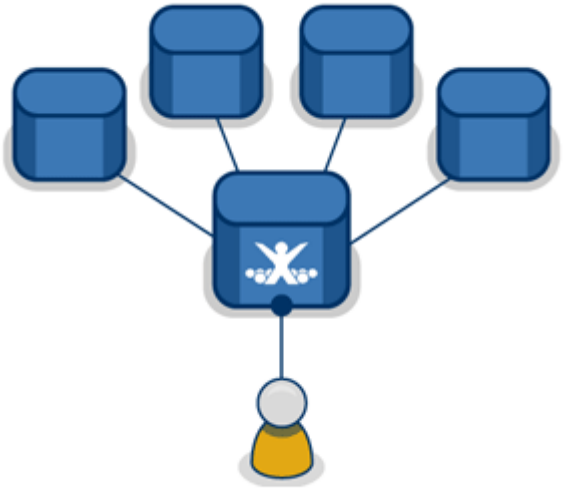


4

NAJCZĘŚCIEJ SPOTYKANE ZAGROŻENIA

AKTYWNA OCHRONA INFORMACJI

1. Dostęp do systemów
2. Punkty wejścia do sieci (SSO)
3. Dostęp lokalny / zdalny



AKTYWNA OCHRONA INFORMACJI

- Świadomość zagrożeń, szkolenia,
- Social engineering

AKTYWNA OCHRONA INFORMACJI

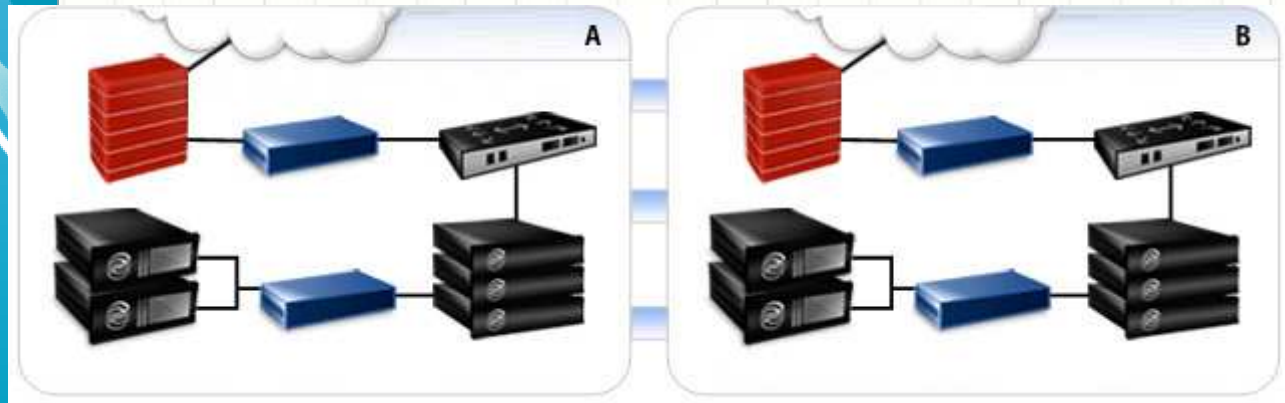
- Bezpieczeństwo notebooków -> szyfrowanie dysków, szyfrowanie połączeń
- Działanie czynników zewnętrznych (woda, dym, ogień, przepięcia) -> archiwizacja

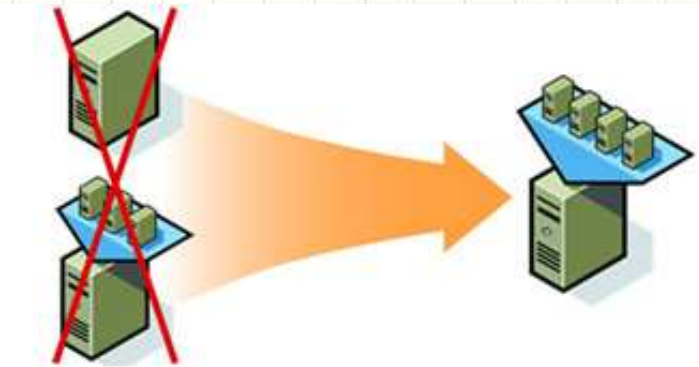
5

KLUCZOWE SYSTEMY INFORMATYCZNE

OCHRONA SYSTEMÓW KLUCZOWYCH

- **Wszystko, co wspomniano wcześniej ORAZ:**
  - **Plan Ciągłości Działania(Plan Odtworzenia Działalności)**
  - **Zapasowe Centrum Przetwarzania Danych**



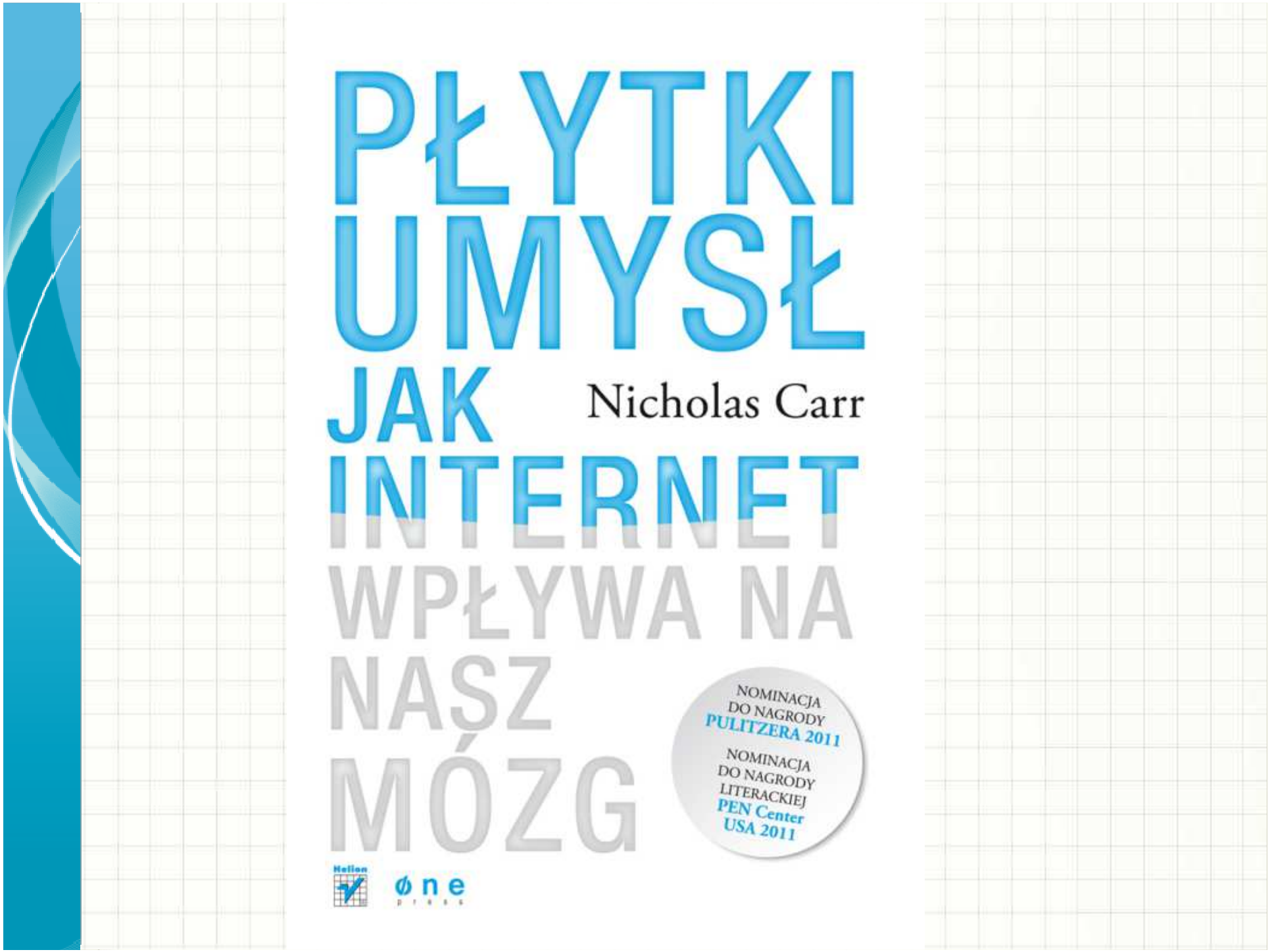


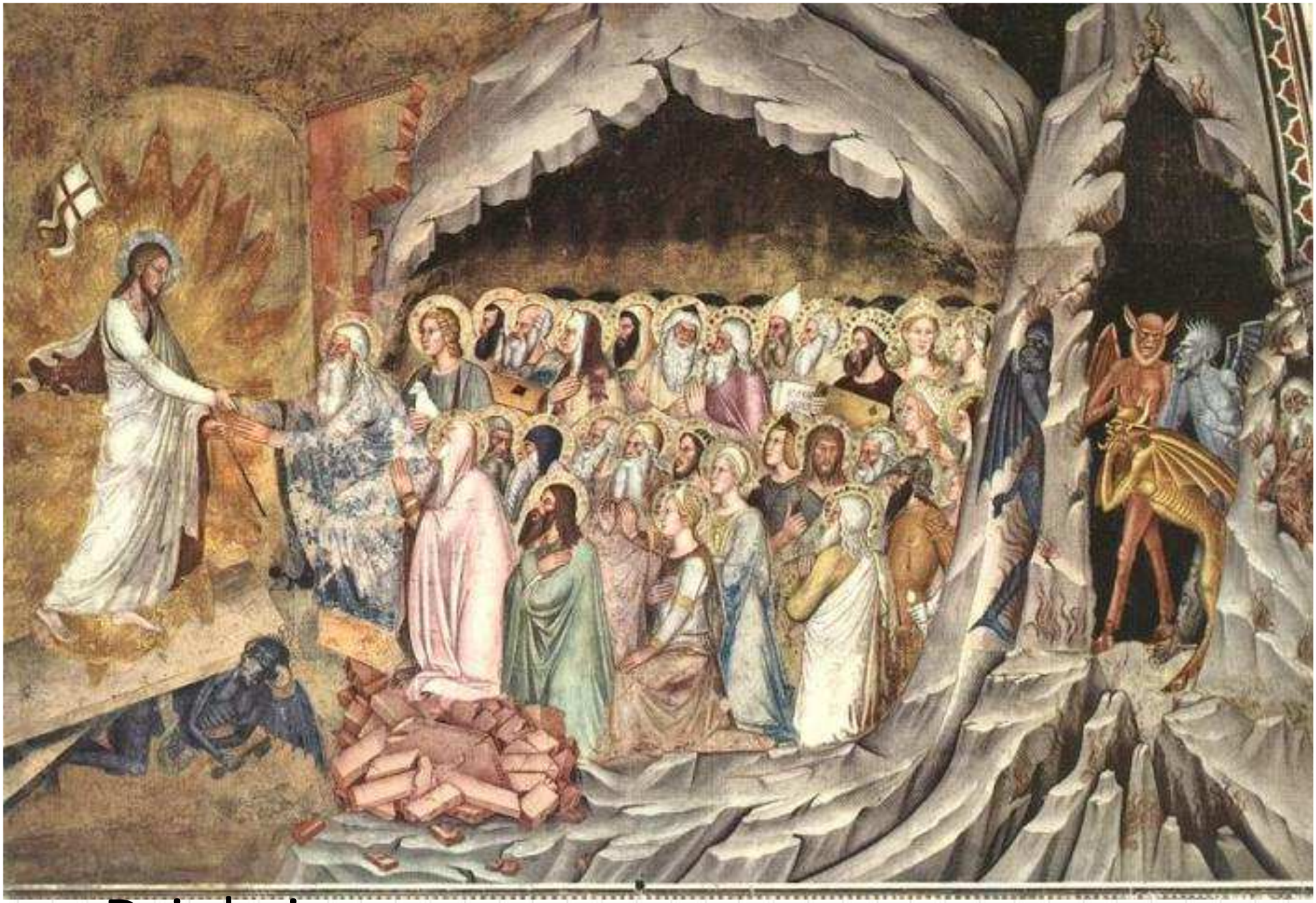
6

CZYNNOŚCI SPRAWDZAJĄCE

CZYNNOŚCI SPRAWDZAJĄCE

- **Monitorowanie wdrożenia zaleceń**
- **Aktualizacja analizy ryzyka**


PŁYTKI
UMYSŁ
JAK
Nicholas Carr
INTERNET
WPŁYWA NA
NASZ
MÓZG
NOMINACJA
DO NAGRODY
PULITZERA 2011
NOMINACJA
DO NAGRODY
LITERACKIEJ
PEN Center
USA 2011
Helion
one
press



Dziękuję za uwagę

Michał Głowacki
m.glowacki@inasp.pl