

# Audyt wewnętrzny w zakresie bezpieczeństwa

Paweł Krawczyk

Kontakt z autorem:

[pawel.krawczyk@hush.com](mailto:pawel.krawczyk@hush.com)

Tel. +48-602-776959

Prezentacja udostępniona na licencji Creative Commons BY-NC-SA  
(„uznanie autorstwa”, „użycie niekomercyjne”, „na tych samych warunkach”)

<http://creativecommons.org/licenses/by-nc-sa/3.0/pl/>

# Konspekt

- Standardy i normy
- Pomiar bezpieczeństwa
- Audyty, testy penetracyjne
- Modele budowy bezpiecznych systemów

# Standardy i normy Bezpieczeństwa teleinformatycznego

# Terminologia

- ISMS – Information Security Management System
  - SZBI – System Zarządzania Bezpieczeństwem Informacji
  - Polityki, standardy, procedury, zasoby, delegacje odpowiedzialności i struktura organizacyjna służąca zarządzaniu bezpieczeństwem informacji
- Otoczenie prawne i normatywne związane z ISMS

# ISO 27001

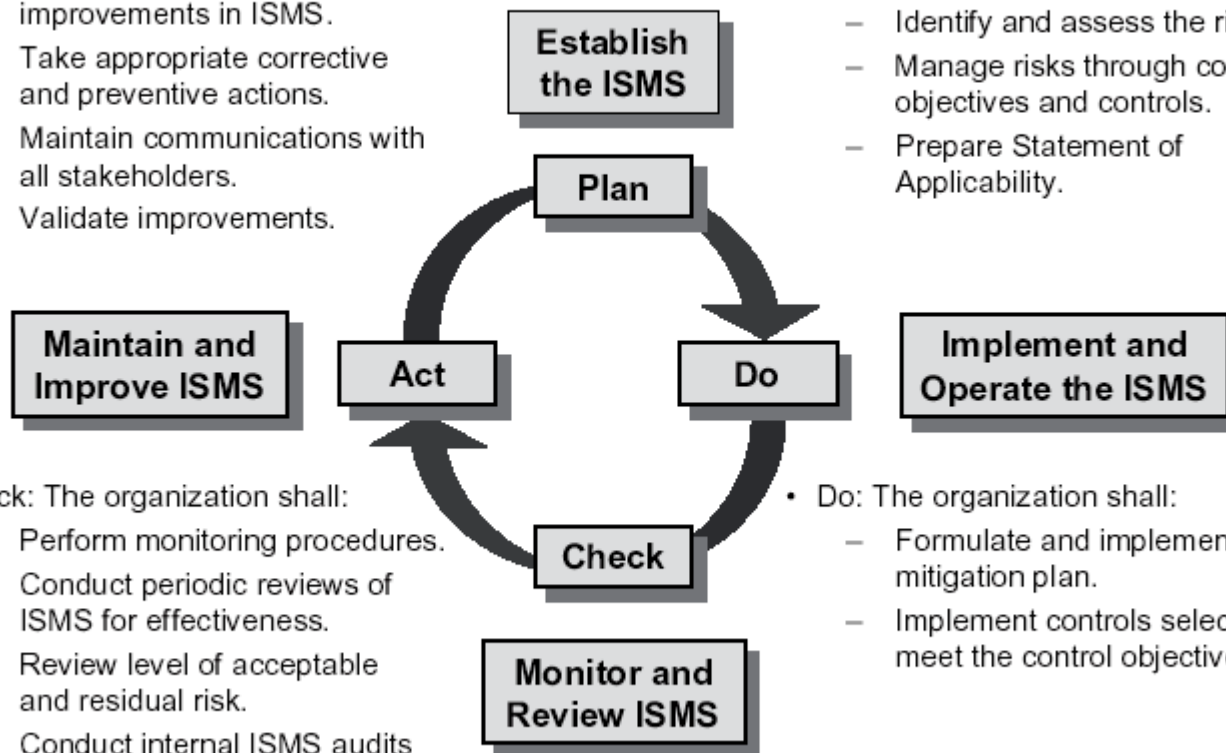
- ISO 27\* (27001,27002 i inne)
  - Model PDCA (Plan-Do-Check-Act)
  - Rekomendacje w zakresie podnoszenia poziomu bezpieczeństwa informacji
  - Wytyczne dla analizy ryzyka, oceny bezpieczeństwa
  - Kontrolna lista audytowa (ISO 27001)

# ISO 27001

- British Standards Institute (BSI)
  - BS 7799-2:1999
  - BS 7799-2:2002
- Przyjęte przez ISO
  - ISO/IEC **27001**:2005
- Certyfikacja ISO 27001
- Szereg wersji krajowych
  - Np. PN ISO/IEC 27001
  - Problem aktualności wersji krajowych

- Act: The organization shall:
  - Implement identified improvements in ISMS.
  - Take appropriate corrective and preventive actions.
  - Maintain communications with all stakeholders.
  - Validate improvements.

- Plan: The organization shall:
  - Define ISMS scope and policy.
  - Identify and assess the risks.
  - Manage risks through control objectives and controls.
  - Prepare Statement of Applicability.



- Check: The organization shall:
  - Perform monitoring procedures.
  - Conduct periodic reviews of ISMS for effectiveness.
  - Review level of acceptable and residual risk.
  - Conduct internal ISMS audits at planned intervals.

- Do: The organization shall:
  - Formulate and implement a risk mitigation plan.
  - Implement controls selected to meet the control objectives.

# ISO 27002

- **BS 7799-1:1999** (*uwaga! BS 7799-2 to ISO 27001*)
  - Przyjęte przez ISO jako ISO/IEC 17799:2000
- ISO/IEC 17799:2000
  - Nowa wersja ISO/IEC 17799:2005
- ISO/IEC 17799:2005
  - Zmiana numeracji na ISO/IEC **27002:2007**
- ISO/IEC 27002:2007
  - Większość aktualnych publikacji posługuje się nazwą ISO 27002
  - W Polsce 17799:2007 na bazie ISO 17799:2005

# Historia ISO 27001 i 27002



# ISO 27001 i 27002

- ISO 27001

- Jak nadzorować i monitorować ISMS?
- Annex A
  - Lista kontrolna zabezpieczeń
  - Co powinno być zrobione?
  - Lista audytowa
  - Numeracja odpowiada 27002

- ISO 27002

- Jak budować ISMS?
- Annex A
  - Lista kontrolna zabezpieczeń
  - Jak to zrobić?
  - Rekomendacje
  - Numeracja odpowiada 27001

# ISO 27001 jako standard audytowy

- ISMS zarządzany na podstawie 27002
- Poprawność działania weryfikowana z 27001
- Audyt wewnętrzny
  - Cykliczna weryfikacja poprawności ISMS
- Audyt zewnętrzny
  - Na żądanie klienta, regulatora
  - W celu uzyskania certyfikatu

# Certyfikacja ISO 27001

- Certyfikat na podstawie audytu
  - Np. A.10.10.6: *„System clocks on all systems should be synchronized based on a common time source”*
- Proces certyfikacji
  - Prowadzony przez niezależną organizację
  - Audytowany jest określony zakres (*scope*)
  - Zakres definiowany przez podmiot występujący o certyfikację

IS027k router security audit checklist.rtf - Microsoft Word

File Edit View Insert Format Tools Table Window Help

Type a question for help

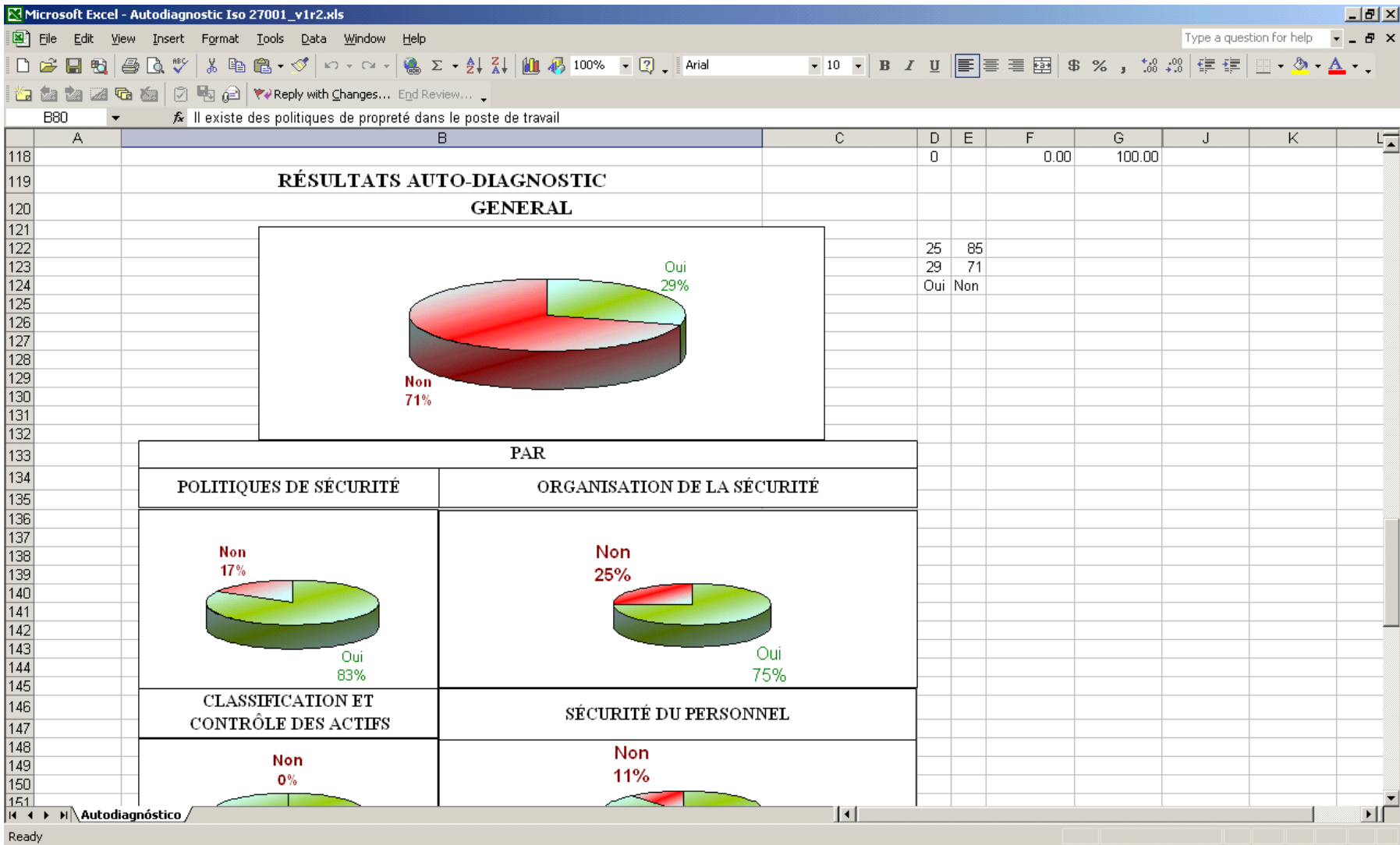
100% Normal Palatino 10 B I U

Write Right EN - British Final Showing Markup Show

### Router Technical Audit Checklist

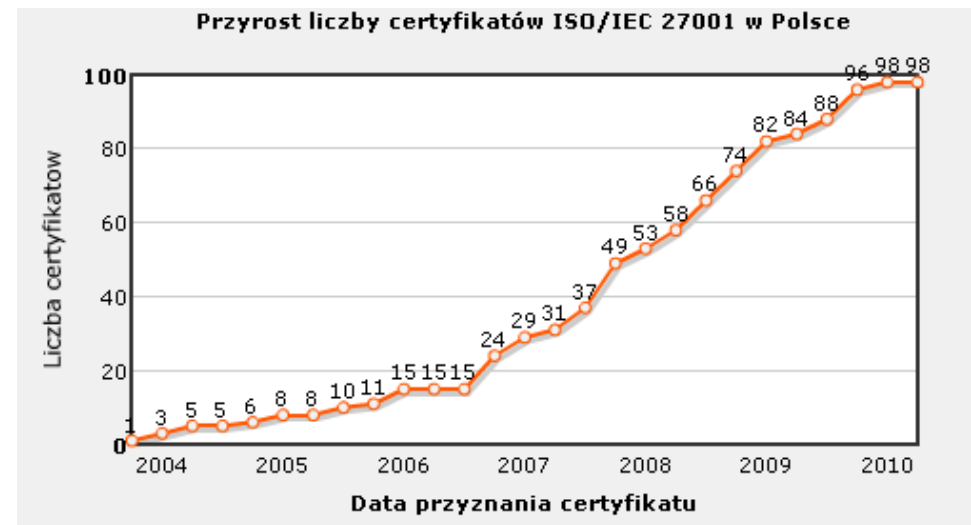
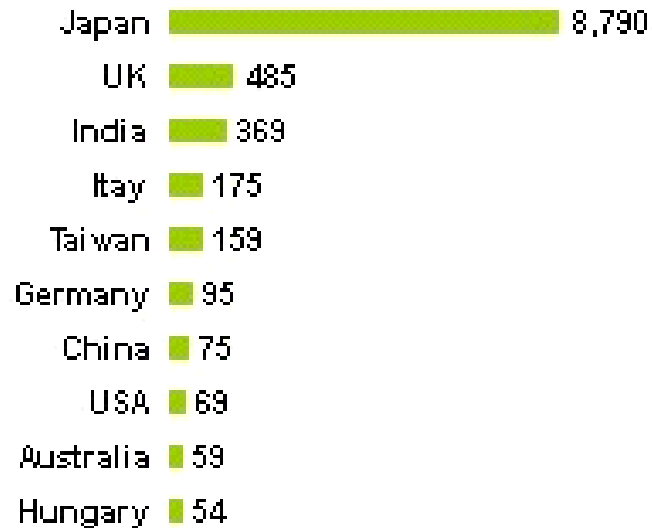
Questions	Findings		ISO 27001 Control	Standard/Best Practice
	Yes	No		
<i>Router Policy</i>				
Is a router security policy in place?	<input type="checkbox"/>	<input type="checkbox"/>	A.5.1.1 A.11.4.1	
<i>Disable Unneeded Services</i>				
Are unused interfaces disabled?	<input type="checkbox"/>	<input type="checkbox"/>	A.11.4.4	Unused interfaces on the router should be disabled. Router(config-if)# shutdown
Is DNS lookups for the router turned off?	<input type="checkbox"/>	<input type="checkbox"/>	A.11.5.4 A.12.6.1	This client service is enabled by default and is not required on most routers. The following command is used to turn DNS lookup off. Router(config)#no ip domain-lookup
Is TCP small servers and UDP small servers service disabled on the router? [applicable before Cisco IOS 11.3]	<input type="checkbox"/>	<input type="checkbox"/>	A.12.6.1	These services are rarely used and hence can be disabled. This is disabled by default after Cisco IOS 11.3 Router(config)#no service tcp-small-servers Router(config)#no service udp-small-servers
Is Cisco Discovery Protocol disabled on the router?	<input type="checkbox"/>	<input type="checkbox"/>	A.11.4.4 A.12.6.1.	CDP which is used to obtain information such as the ip address, platform type of the neighboring Cisco devices should be disabled on the router if not used by any application. Router(config)# no cdp run OR Router(config-if)# no cdp enable Unauthorized persons can use the

Page 1 Sec 1 1/8 At 1.8" Ln 4 Col 1 REC TRK EXT OVR English (U.S)

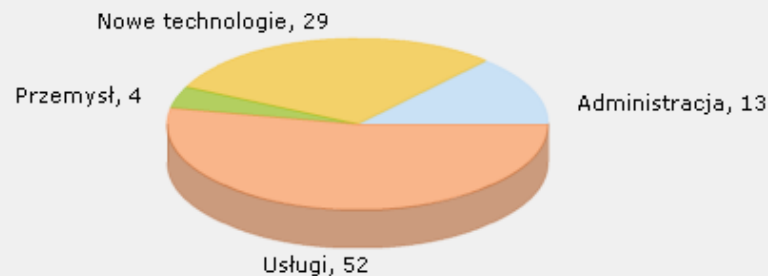


Microsoft Excel - Autodiagnostic Iso 27001_v1r2.xls									
Type a question for help									
B23 * Existe un responsable des actifs									
A	B	C	D	E	F	G	J	K	L
1	<b>FORMULAIRE POUR AUTO-DIAGNOSTIC</b>								
2	<b>(ISO 27001)</b>								
3	<b>POLITIQUES DE SÉCURITÉ</b>								
4	Il existe un document (s) de politiques de sécurité de SI	<input checked="" type="checkbox"/>	TRUE	1					
5	Il existe une réglementation relative à la sécurité de le SI	<input checked="" type="checkbox"/>	TRUE	1					
6	Il existe des procédures relatives à la sécurité de de SI	<input type="checkbox"/>	FALSE	0					
7	Il existe un responsable les politiques, de normes et de procédures	<input checked="" type="checkbox"/>	TRUE	1					
8	Il existe des mécanismes pour la communication aux utilisateurs des normes	<input checked="" type="checkbox"/>	TRUE	1					
9	Il existe des contrôles réguliers pour vérifier l'efficacité des politiques	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
10	<b>ORGANISATION DE LA SÉCURITÉ</b>								
11	Il existe des rôles et des responsabilités définis pour les personnes impliquées dans la sécurité	<input type="checkbox"/>	FALSE	0		83.33	16.67		
12	Il existe un responsable chargé d'évaluer l'acquisition et les changements de SI	<input checked="" type="checkbox"/>	TRUE	1					
13	La Direction et les secteurs de l'Organisation prend part des sujets de sécurité	<input type="checkbox"/>	FALSE	0					
14	Il existe des conditions contractuelles de sécurité avec des tiers et outsourcing	<input checked="" type="checkbox"/>	TRUE	1					
15	Il existe des critères de sécurité dans le maniement de tierces parties	<input checked="" type="checkbox"/>	TRUE	1					
16	Il existe des programmes de formation en sécurité pour les employés, clients et tiers	<input checked="" type="checkbox"/>	TRUE	1					
17	Il existe un accord de caractère confidentiel de l'information pour ceux qu'y accède.	<input checked="" type="checkbox"/>	TRUE	1					
18	On révise l'organisation de la sécurité périodiquement par une entreprise externe	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
19	<b>ADMINISTRATION DES ACTIFS</b>								
20	Il existe un inventaire des actifs mis à jour	<input checked="" type="checkbox"/>	TRUE	1		75.00	25.00		
21	L'inventaire contient des actifs de données, du software, équipements et services	<input checked="" type="checkbox"/>	TRUE	1					
22	On dispose d'une classification de l'information selon la criticité de de cette dernière	<input checked="" type="checkbox"/>	TRUE	1					
23	Existe un responsable des actifs	<input checked="" type="checkbox"/>	TRUE	1					
24	Il existe des procédures pour classer l'information	<input checked="" type="checkbox"/>	TRUE	1					
25	Il existe des procédures d'étiquetage de l'information	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
26	<b>SÉCURITÉ DES RH</b>								
27	On a définies responsabilités et rôles de sécurité	<input checked="" type="checkbox"/>	TRUE	1		100.00	0.00		
28	On prend en considération la sécurité dans la sélection et la baisse du personnel	<input checked="" type="checkbox"/>	TRUE	1					
29	Les conditions de confidentialité et responsabilités dans les contrats sont précisées	<input checked="" type="checkbox"/>	TRUE	1					
30	On distribue la formation adéquate sécurité et traitement d'actifs	<input type="checkbox"/>	FALSE	0					
31	Il existe un canal et des procédures claires à suivre en cas d'incident de sécurité	<input checked="" type="checkbox"/>	TRUE	1					
32	On reprend les données des incidents de manière détaillée	<input checked="" type="checkbox"/>	TRUE	1					
33	Informers les utilisateurs des vulnérabilités observées ou soupçonnées	<input checked="" type="checkbox"/>	TRUE	1					
34	On informe aux utilisateurs qu'ils ne doivent, sous aucune circonstance, divulguer les vulnérabilités	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			

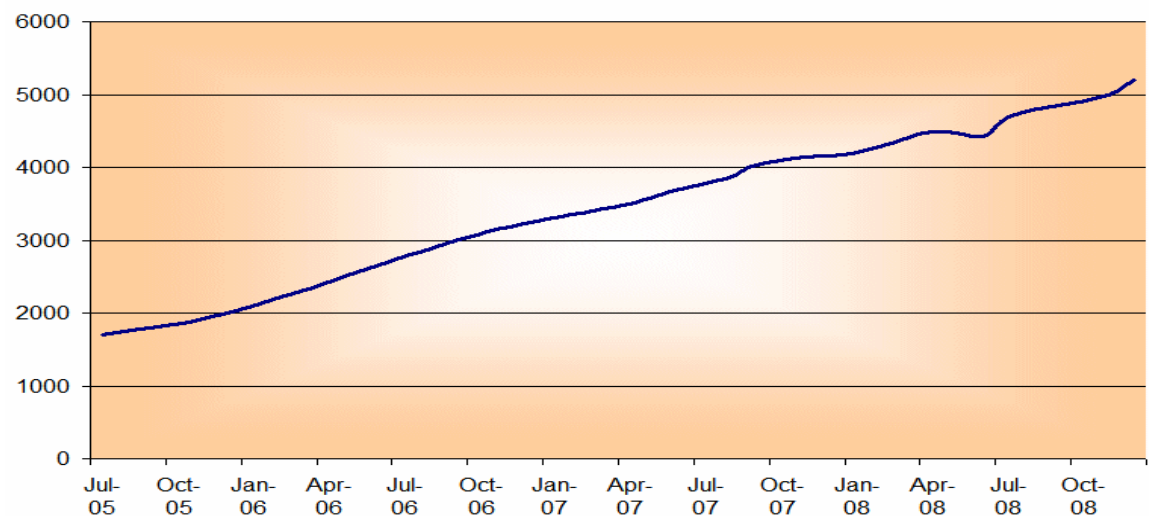
## The ten largest holders of ISO 27001 certificates



Podział certyfikatów według branż



Number of ISO/IEC 27001 (or equivalent) certificates



Inne standardy

# COBIT

- COBIT (*Control Objectives for Information and related Technology*)
  - Standardowe miary, wskaźniki, procesy i rekomendacje, kontrolna lista audytowa
  - Maksymalizacja efektywności systemów IT
  - Część DS5 – *Ensure Systems Security*
  - Kompatybilny z ISO 27002
  - Organizacja: ISACA
    - Wsparcie "Big 4"

# ITIL

- ITIL (*Information Technology Infrastructure Library*)
  - Model PDCA
  - Procesy i zalecenia dla maksymalizacji efektywności usług IT i zarządzania infrastrukturą IT
  - Kompatybilny z ISO 27002
  - Organizacja: Central Computers and Communications Agency (CCTA, UK)

# NIST

- National Institutes of Standards and Technology (NIST)
  - FIPS – Federal Information Processing Standards
    - Normy (wiążące dla amerykańskiej administracji)
  - SP – Special Publications
    - Rekomendacje, najlepsze praktyki
- Godne uwagi
  - Bardzo szeroki zakres
  - Częste aktualizacje
  - Także niskopoziomowe i techniczne

# NIST SP

- SP 800-39 „Managing Risk from Information Systems. Organizational Perspective”
- SP 800-60 „Guide for Mapping Types of Information and Information Systems to Security Categories”
- SP 800-53 „Recommended Security Controls for Federal Information Systems”
- SP 800-70 „National Checklist Program for IT Products-- Guidelines for Checklist Users and Developers”
- SP 800-53A „Guide for Assessing the Security Controls in Federal Information Systems”
- SP 800-37 „Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach”

# ISF SOGP

- ISF (*Information Security Forum*)
  - *Standard of Good Practice for Information Security*
- Integracja z innymi standardami
  - ISO 27002, COBIT, SOX, PCI DSS, BASEL II, Dyrektywa EU o ochronie danych osobowych

# Inne

- *SAS70 (Statement of Auditing Standards)*
  - *AICPA (American Institute of Certified Public Accountants)*
- *PCI (Payment Card Industry)*
  - *DSS (Data Security Standard)*
- *SOX (Sarbanes-Oxley)*
  - **PCAOB**
- **Europejska dyrektywa o ochronie danych osobowych**
  - **Ustawa o ochronie danych osobowych (uodo)**
  - **GIODO**

# ISO 27003

Information security management system implementation guidance

## **Guidance on using PDCA method**

1. Introduction
2. Scope
3. Terms & Definitions
4. CSFs (Critical success factors)
5. Guidance on process approach
6. Guidance on using PDCA
7. Guidance on Plan Processes
8. Guidance on Do Processes
9. Guidance on Check Processes
10. Guidance on Act Processes
11. Inter-Organization Co-operation

# ISO 27004

## **Information security management -- Measurement**

The standard is intended to help organizations **measure and report the effectiveness** of their information security management systems, covering both the security management processes (defined in ISO/IEC 27001) and the security controls (ISO/IEC 27002).

# ISO/IEC 27005

## Information security risk management

ISO/IEC 27005:2008 provides **guidelines for information security risk management**. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

- Por. **ISO 31000**
  - *Risk management -- Principles and guidelines on implementation*
- Por. **NIST SP 800-30**

# ISO 27007

## **Guidelines for information security management systems auditing**

This standard will provide **guidance for accredited certification bodies, internal auditors, external/third party auditors and others auditing Information Security Management Systems against ISO/IEC 27001** (i.e. auditing the management system for compliance with the standard) but may also offer advice to those auditing or reviewing ISMSs against ISO/IEC 27002 (i.e. auditing the organization's controls for their suitability in managing information security risks) although this may be covered instead by ISO/IEC TR 27008.

# Narzędzia

- ISO27k Toolkit
  - MS Excel
- EBIOS (Francja, DSSI)
  - Java
- SOMAP
  - Open Information Security Risk Assessment Guide
  - SOBF (*Security Officer's Best Friend*) – Java
- Duży rynek narzędzi komercyjnych

# Pomiary bezpieczeństwa

# Miary bezpieczeństwa

- Na potrzeby analizy ryzyka (*risk analysis*)
  - Jakościowa (*qualitative*) – Low/Medium/High
  - Ilościowa (*quantitative*) – SLE, ALE (\$)
- Na potrzeby zarządzania podatnościami (*vulnerability management*)
  - Standardyzacja podatności
    - CVE, CCE, CPE, CWE
    - BID, QID, Microsoft, Secunia...
  - Standardyzacja stopnia zagrożenia (*impact*)
    - Umowna klasyfikacja katalogowa (*severity*)
    - CVSS (*Common Vulnerability Scoring System*)

# Standardyzacja podatności

- NIST NVD (National Vulnerability Database)
  - CVE (Common Vulnerability Enumeration
    - *„Microsoft Windows Server Service Could Allow Remote Code Execution” (CVE-2008-4250)*
  - CWE (Common Weakness Enumeration)
    - *“Cross Site Request Forgery” (CWE-352)*
  - CCE (Common Misconfigurations Enumeration)
    - W trakcie opracowywania...
  - CPE (Common Platform Enumeration)
    - `cpe:/a:apache:apache-ssl:1.37`

# Standardyzacja podatności

- Inne katalogi podatności
  - SecurityFocus (BID), Secunia (SA), Qualys (QID), VUPEN, OSVDB...
- Klasyfikacja producentów oprogramowania
  - Microsoft, Sun, Cisco...

# Standardyzacja stopnia zagrożenia

- Umowna producentów (*severity*)
  - Opisowa (*Low/Medium/High/Urgent/Critical...*)
  - Liczbowa (1-5)
- NIST CVSS (*Common Vulnerability Scoring System*)
  - Obiektywizacja kryteriów
  - Umożliwia wycenę podatności w dużej skali
  - Wycena ułatwia przydział zasobów

# CVSS

- Base CVSS
  - Odzwierciedla stałą charakterystykę podatności
    - Zdalna/lokalna? Trudna/łatwa? Uwierzytelnienie?
- Temporal CVSS
  - Charakterystyka zmienna w czasie
    - Potwierdzona/niepotwierdzona? Exploit? Poprawki?
- Environmental CVSS
  - Zagrożenie w konkretnym środowisku lokalnym
    - E-CVSS danego serwera *versus* CVSS podatności

# Przykład CVSS

- Podatności w Microsoft RPC DCOM
  - CVE-2003-0352 (Blaster)
    - Nie daje uprawnień administratora – CVSS=7,5
  - CVE-2003-0715
    - Daje uprawnienia administratora – CVSS=10 (max)
  - Poza tym Base CVSS wysokie
    - Dostępna przez sieć
    - Łatwość ataku
    - Bez uwierzytelnienia

# Metody pomiaru bezpieczeństwa

- Audyt
  - Systematyczny, powtarzalny, obiektywny, ograniczony zakres oceny, globalnie rozpoznawany
- Test penetracyjny
  - Szerszy zakres , ocena całościowego stanu bezpieczeństwa, aktualny stan wiedzy, częściowo systematyczny, uzależniony od kompetencji zespołu
- Ocena bezpieczeństwa
  - Zastosowanie wiedzy i doświadczenia eksperta, aktualny stan wiedzy

# Metody pomiaru bezpieczeństwa

- Pomiar powtarzalne
  - Statystyki operacyjne z procesów biznesowych
    - Liczba eskalacji? Liczba opóźnień? Liczba fraudów?
  - Narzędzia do oceny podatności (*vulnerability assessment*)
    - Skanery działające w trybie ciągłym (tydzień, miesiąc)
    - Cykliczne testy penetracyjne
  - Analiza zdarzeń
    - Firewalle, systemy IDS/IPS
    - Logi systemowe (*system alerts*)

# Audyt bezpieczeństwa teleinformatycznego

# Audyty bezpieczeństwa systemu

"Dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną polityką bezpieczeństwa i z procedurami operacyjnymi oraz w celu wykrycia przełamania bezpieczeństwa i zalecenia wskazanych zmian w środkach nadzorowania, polityce bezpieczeństwa oraz w procedurach"

Źródło: PN-I-02000:2002, pkt 3.1.007

"usystematyzowany, niezależny i udokumentowany proces uzyskania dowodu z auditu i obiektywnej oceny w celu określenia w jakim stopniu spełniono uzgodnione kryteria auditu"

Źródło: PN-EN ISO 9000:2001, pkt 3.9.1

# Cele audytów

- Obiektywizacja kryteriów
  - Niewspółmierna rola systemów IT
- Minimalny standard jakości (*baseline*)
  - Różne poziomy dojrzałości uczestników rynku (*maturity levels*)
- Podstawa do przyjęcia zobowiązań
  - Łańcuch dostaw, podwykonawcy
  - SLA (*Service Level Agreement*)

# Cele audytu wewnętrznego

- Ocena zgodności procesów z celami organizacji
  - Optymalizacja procesów
  - Przywrócenie odpowiednich priorytetów zadań
  - Ograniczenie zjawiska "przesunięcia celów"
- Psychologiczne bariery audytu - zapobieganie
  - Audyt nie służy "zwalczaniu" kogokolwiek
  - Audyt to nie kontrola
  - Audyt ma pomóc, nie przeszkadzać

# Cele audytu zewnętrznego

- Zlecany przez organizację
  - Cele jak w audycie wewnętrznym
- Zlecany przez trzecią stronę
  - Zgodność z regulacjami (*legal compliance*)
  - Zgodność z deklaracjami organizacji
  - Ocena przed transakcją (*due dilligence*)

# Audyt niezależny

- Nie wykonuje go
  - Projektant, dostawca, wykonawca, integrator
- Audyt wewnętrzny (pierwszej strony)
  - Niezależność w hierarchii służbowej
- Audyt zewnętrzny (drugiej, trzeciej strony)
  - Niezależność organizacyjna

# Audyt systematyczny

- Powtarzalność
  - Plan audytu, metodyka, minimalne wymagania
- Obiektywność
  - Brak uznaniowości w interpretacji faktów
    - Co jest "wystarczająco bezpieczne" a co nie
  - Ściśle określone kryteria zgodności

# Audyt systematyczny

- Ustalona lista kontrolna (*checklist*)
  - Zamknięta, kompletna
  - Punkt odniesienia do protokołu rozbieżności (*gap analysis*)
  - Na podstawie standardów lub przepisów
  - Polityki, standardy, procedury organizacji
- Czy można prowadzić audyt bez punktu odniesienia?
- Wady listy kontrolnej
  - Wysokopoziomowa, statyczna

# Audyt udokumentowany

- Dowód (*evidence*) jako krytyczna część audytu
  - Na pytania z listy kontrolnej odpowiada audytor
    - Nie audytowany
  - Odpowiedzi na podstawie dowodów
- Źródła informacji audytowych
  - Ankiety, wywiady (próba statystyczna)
  - Wizja lokalna
  - Dokumentacja strategiczna i operacyjna
  - Analizy, testy i badania

# Warunki obiektywności

- Audytor ocenia dowody
  - Nie opinie audytowanego
- Audytor ocenia zgodność z założeniami
  - Ocenę rozbieżności prowadzi adresat audytu
- Audytor wybiera próbki audytowe
  - Ocena losowych próbek z dużych ilości obiektów
  - Czy próbka jest losowa?
  - Czy próbka jest reprezentatywna?
  - Dlaczego wybrano te, a nie inne obiekty?

# Istotne cechy audytu

- Ograniczony do zdefiniowanego zakresu
  - Brak oceny obiektu, który nie jest przedmiotem audytu
- Ograniczony do punktu odniesienia
  - Brak oceny obiektu wg kryteriów nie ujętych w liście kontrolnej
- Brak gwarancji "ogólnego bezpieczeństwa"
  - Produkt lub proces pozytywnie zaudytowany nadal może mieć istotne podatności

# Metodyka audytu

- LP-A (Liderman-Patkowski, WAT)
- Oparty o ISO 27001
- Skład zespołu audytowego
  - 2 audytorów, 3 specjalistów audytowych
  - Personel pomocniczy (ankieterzy itd)
  - Eksperti z poszczególnych dziedzin
- Narzędzia audytowe (skanery)

# Proces audytu #1

- Przygotowanie audytu
  - Udzielenie uprawnień, osoby kontaktowe, zasady komunikacji, harmonogram, szkolenie zarządu organizacji audytowanej
- Ścieżka formalna
  - Badanie jakości zarządzania ISMS – dokumentacja oficjalna, dokumenty operacyjne, ankiety

# Proces audytu #2

- Ścieżka techniczna
  - Analiza architektury systemów IT, analiza stanu faktycznego infrastruktury
  - Przegląd i ocena zabezpieczeń
- Prezentacja wyników audytu
  - Protokół rozbieżności
  - Zalecenia pokontrolne

# Testy penetracyjne

# Rola audytu i testu penetracyjnego

- Ograniczenia audytu
  - Szybkie zmiany w technologii
    - Czas życia standardów audytowych – lata
    - Czas życia typowych podatności w systemach – dni
  - Zakres oceny audytowej
    - Może nie obejmować wszystkich aspektów i scenariuszy
- Rola testu penetracyjnego
  - Ocena praktycznego, chwilowego stanu bezpieczeństwa,
  - Konkretny, działający system
  - Próba uzyskania dowodu nieskuteczności

# Cechy testów penetracyjnych

- Szeroki zakres
  - Testy od wysoko- do niskopoziomowych
  - Wszystkie komponenty systemu
  - Cel – dowolny scenariusz prowadzący do przełamania zabezpieczeń
- Utrudniona powtarzalność
  - Zależny od kompetencji zespołu
  - Zależny od aktualnego stanu wiedzy
  - Zależny od dostępu do informacji

# Próby standardyzacji

- Algorytm testu penetracyjnego
  - 1) Sprawdź wersję serwera WWW, 2) sprawdź w bazie znane podatności, 3) ...
  - Nadal ograniczone kompetencjami zespołu
  - Zbyt duża liczba scenariuszy
- Główna zaleta testu penetracyjnego
  - Możliwość odkrycia nowych ataków dzięki kreatywności zespołu
  - Możliwość wskazania niestandardowych scenariuszy ataku

# Co należy standardyzować?

- Kroki, które muszą być wykonane
  - Minimalne wymagania
- Zakres informacji dokumentowanej
- Zakres informacji raportowanej
- Zasady komunikacji
- Zakres testu
  - Np. daty i godziny wykonywania testów
- Wymagania formalne
  - Np. upoważnienie do testu

# Kwestie prawne

- Kodeks karny
  - Przeszępstwa przeciwko ochronie informacji
    - Art. 265-269b kk
    - "Oprogramowanie hakerskie" (art. 269b)
- Obowiązki zespołu testującego
  - Pisemne upoważnienie właściciela systemu
  - Precyzyjnie opisany zakres upoważnienia
  - Dokumentacja działań testowych
  - Dokumentacja kontaktów z klientem

# Kiedy test ma sens?

- Przed udostępnieniem aplikacji w sieci
  - Później może być za późno
- Prowadzony na produkcyjnej wersji systemu
  - Takiej, jaka będzie dostępna dla klientów
- Zakończone prace rozwojowe
  - Testy funkcjonalne, poprawki, zmiany
- Czas testu uwzględniony w harmonogramie
  - Jeśli wyniki mają być miarodajne

# Test penetracyjny a włamanie

- Test penetracyjny trudniejszy niż włamanie
  - Konieczność sprawdzenia wszystkich scenariuszy
    - Włamanie – najkrótszą drogą do celu
  - Konieczność dokumentacji działań
    - Włamanie – nie ma takiej potrzeby
  - Wymaganie wobec zespołu testującego
    - Kwestie etyczne, systematyczność, rzetelność

# Metody testowania

- "Black box"
  - Ograniczona wiedza zespołu testującego
  - Zalety – brak uprzedzeń, kwestie psychologiczne
  - Wady – brak widoczności niektórych trywialnych zagrożeń
- "Crystal box"
  - Pełny dostęp zespołu do "środka" systemu
  - Zalety – lepsza widoczność nietypowych scenariuszy
  - Wady – możliwość przyjęcia błędnych założeń

# Istniejące metodyki

- OSSTMM (Open Source Security Testing Methodology Manual)
- NIST SP800-42 „Guideline on Network Security Testing „
- NIST SP800-115 „Technical Guide to Information Security Testing“
- OISSG „ISSAF Penetration Testing Framework“
- P-PEN (Patkowski, WAT)
- MindCert Certified Ethical Hacker mind-map series
- OWASP (Open Web Application Security Project)
- Penetration Testing Framework (Kevin Orrey)

# Typowy scenariusz testu

- Enumeracja i inwentaryzacja zasobów
  - Skan podsieci IP
- Enumeracja usług
  - Skan portów, protokołów
- Enumeracja aplikacji
  - Skan odpowiedzi na portach, nagłówki, wersje...
- Wartość dodana
  - O czym klient nie wiedział wcześniej?

# Mapowanie podatności

- Zasoby, usługi, aplikacje
  - Jakie znane podatności?
    - Np. wykryta wersja serwera Apache/1.3.18
      - Jakie znane podatności?
        - Czy są praktyczne?
    - Cel – stwierdzenie podatności
      - Testowanie (exploit) tylko za zgodą klienta
  - Brak podatności, wersja – wartościowa informacja
    - Załączyć do raportu, ocena przydatności przez klienta

# Aspekt skali

- Różne zakresy testów
  - Jeden serwer? Sto serwerów? 10 tys. stacji roboczych?
- Testy zautomatyzowane
- Testy losowej próbki
- Dobre wyniki w jednorodnej grupie
  - Konieczność inwentaryzacji całości i agregacji podobnych grup

# Skannery automatyczne

- Ogólnego przeznaczenia
  - Nessus, OpenVAS, QualysGuard, IBM Internet Scanner...
- Wykrywanie sygnaturowe
- Zalety
  - Masowe, cykliczne skany podobnych zasobów
- Wady
  - Możliwość pominięcia nietypowych zasobów
  - Niska skuteczność wobec aplikacji webowych

# Skannery automatyczne

- Aplikacje webowe
  - IBM Rational AppScan (WatchFire), HP WebInspect, Acunetix
- Wykrywanie sygnaturowe plus uniwersalne techniki ataków
- Zalety
  - Przewaga w testach rozbudowanych aplikacji
- Wady
  - Możliwość pominięcia oczywistych, choć nietypowych podatności
  - Niska skuteczność w testowaniu logiki biznesowej

# Jakość testów penetracyjnych

- Metodyki testów penetracyjnych
  - Raczej "lista zadań" niż "lista kontrolna"
- Próby standardyzacji dokładności testu
  - OWASP ASVS (*Application Security Verification Standard*)
    - Level 1 – Automated verification
    - Level 2 – Manual verification
    - Level 3 – Design verification
    - Level 4 – Internal verification

# Statyczna analiza kodu

- Ograniczenia badania behawioralnego
  - Nietypowe scenariusze
  - Moduły nieujawnione w interfejsie
  - Błędy w logice biznesowej
- Statyczna analiza kodu (SCA – *Static Code Analysis*)
  - Ręczna
  - Automatyczna – Veracode, Fortify, Checkmarx, Ounce Labs...

Kontakt z autorem:

[pawel.krawczyk@hush.com](mailto:pawel.krawczyk@hush.com)

Tel. +48-602-776959

Prezentacja udostępniona na licencji Creative Commons BY-NC-SA  
(„uznanie autorstwa”, „użycie niekomercyjne”, „na tych samych warunkach”)

<http://creativecommons.org/licenses/by-nc-sa/3.0/pl/>

# Audyt wewnętrzny w zakresie bezpieczeństwa

Paweł Krawczyk

Kontakt z autorem:

[pawel.krawczyk@hush.com](mailto:pawel.krawczyk@hush.com)

Tel. +48-602-776959

Prezentacja udostępniona na licencji Creative Commons BY-NC-SA  
(„uznanie autorstwa”, „użycie niekomercyjne”, „na tych samych warunkach”)

<http://creativecommons.org/licenses/by-nc-sa/3.0/pl/>

2

Literatura:

<http://ipsec.pl/>

<http://securitystandard.pl/>

Andrew Jaquith, "Security metrics"

# Konspekt

- Standardy i normy
- Pomiary bezpieczeństwa
- Audyty, testy penetracyjne
- Modele budowy bezpiecznych systemów

# Standardy i normy Bezpieczeństwa teleinformatycznego

# Terminologia

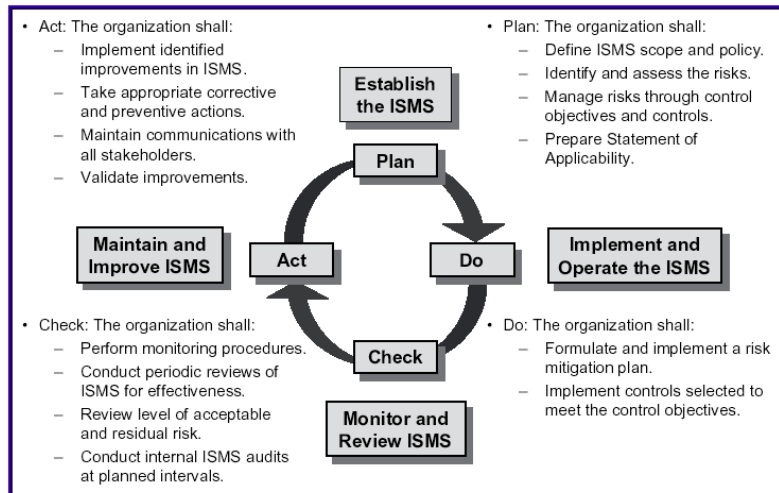
- ISMS – Information Security Management System
  - SZBI – System Zarządzania Bezpieczeństwem Informacji
  - Polityki, standardy, procedury, zasoby, delegacje odpowiedzialności i struktura organizacyjna służąca zarządzaniu bezpieczeństwem informacji
- Otoczenie prawne i normatywne związane z ISMS

# ISO 27001

- ISO 27\* (27001,27002 i inne)
  - Model PDCA (Plan-Do-Check-Act)
  - Rekomendacje w zakresie podnoszenia poziomu bezpieczeństwa informacji
  - Wytyczne dla analizy ryzyka, oceny bezpieczeństwa
  - Kontrolna lista audytowa (ISO 27001)

# ISO 27001

- British Standards Institute (BSI)
  - BS 7799-2:1999
  - BS 7799-2:2002
- Przyjęte przez ISO
  - ISO/IEC **27001**:2005
- Certyfikacja ISO 27001
- Szereg wersji krajowych
  - Np. PN ISO/IEC 27001
  - Problem aktualności wersji krajowych



# ISO 27002

- **BS 7799-1:1999** (*uwaga! BS 7799-2 to ISO 27001*)
  - Przyjęte przez ISO jako ISO/IEC 17799:2000
- ISO/IEC 17799:2000
  - Nowa wersja ISO/IEC 17799:2005
- ISO/IEC 17799:2005
  - Zmiana numeracji na ISO/IEC **27002:2007**
- ISO/IEC 27002:2007
  - Większość aktualnych publikacji posługuje się nazwą ISO 27002
  - W Polsce 17799:2007 na bazie ISO 17799:2005

# Historia ISO 27001 i 27002



# ISO 27001 i 27002

- ISO 27001
  - Jak nadzorować i monitorować ISMS?
  - Annex A
    - Lista kontrolna zabezpieczeń
    - Co powinno być zrobione?
    - Lista audytowa
    - Numeracja odpowiada 27002
- ISO 27002
  - Jak budować ISMS?
  - Annex A
    - Lista kontrolna zabezpieczeń
    - Jak to zrobić?
    - Rekomendacje
    - Numeracja odpowiada 27001

# ISO 27001 jako standard audytowy

- ISMS zarządzany na podstawie 27002
- Poprawność działania weryfikowana z 27001
- Audyt wewnętrzny
  - Cykliczna weryfikacja poprawności ISMS
- Audyt zewnętrzny
  - Na żądanie klienta, regulatora
  - W celu uzyskania certyfikatu

# Certyfikacja ISO 27001

- Certyfikat na podstawie audytu
  - Np. A.10.10.6: *„System clocks on all systems should be synchronized based on a common time source”*
- Proces certyfikacji
  - Prowadzony przez niezależną organizację
  - Audytowany jest określony zakres (*scope*)
  - Zakres definiowany przez podmiot występujący o certyfikację

ISO216 router security audit checklist.rtf - Microsoft Word

File Edit View Insert Format Tools Table Window Help

100% Normal Palatino 10 B / I U

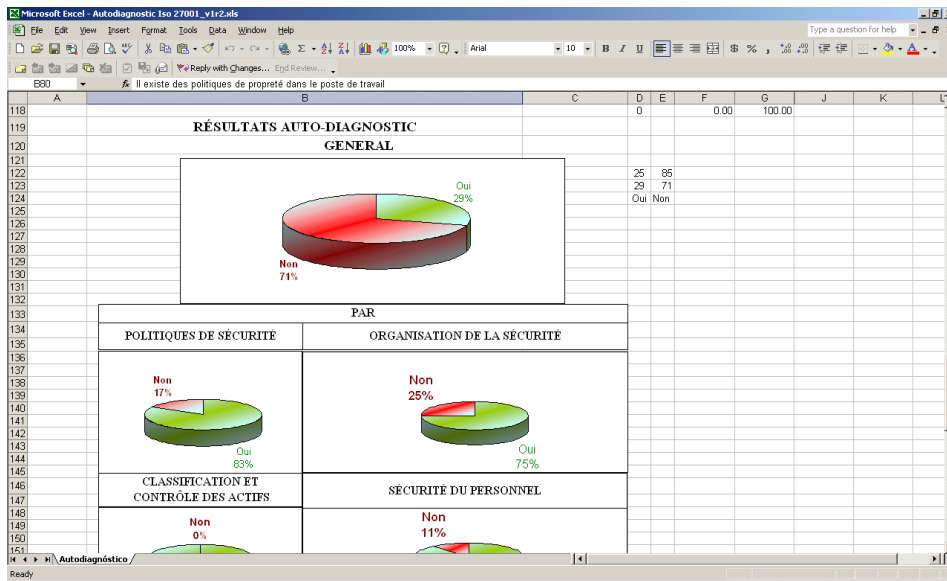
Write Eight EN - British Final Showing Markup Show

Type a question for help

Router Technical Audit Checklist

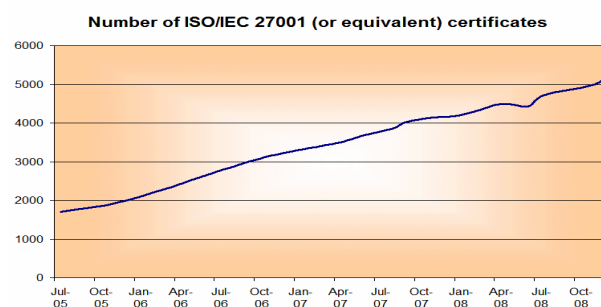
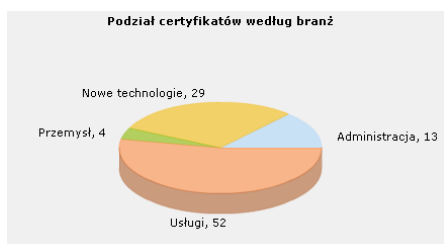
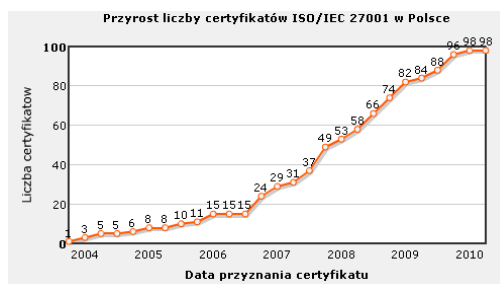
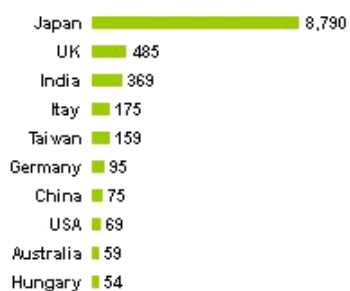
Questions	Findings		ISO 27001 Control	Standard/Best Practice
	Yes	No		
<b>Router Policy</b>				
Is a router security policy in place?	<input type="checkbox"/>	<input type="checkbox"/>	A.5.1.1 A.11.4.1	
<b>Disable Unneeded Services</b>				
Are unused interfaces disabled?	<input type="checkbox"/>	<input type="checkbox"/>	A.11.4.4	Unused interfaces on the router should be disabled. Router(config-if)# shutdown
Is DNS lookups for the router turned off?	<input type="checkbox"/>	<input type="checkbox"/>	A.11.5.4 A.126.1	This client service is enabled by default and is not required on most routers. The following command is used to turn DNS lookup off. Router(config)#no ip domain-lookup
Is TCP small servers and UDP small servers service disabled on the router? (applicable before Cisco IOS 11.3)	<input type="checkbox"/>	<input type="checkbox"/>	A.126.1	These services are rarely used and hence can be disabled. This is disabled by default after Cisco IOS 11.3 Router(config)#no service tcp-small-servers Router(config)#no service udp-small-servers
Is Cisco Discovery Protocol disabled on the router?	<input type="checkbox"/>	<input type="checkbox"/>	A.11.4.4 A.126.1.	CDP which is used to obtain information such as the ip address, platform type of the neighboring Cisco devices should be disabled on the router if not used by any application. Router(config)# no cdp run OR Router(config-if)# no cdp enable Unauthorized persons can use the

Page 1 Sec 1 1/8 At 1.8" Ln 4 Col 1 REC TRK EXT OVR English (U.S.)



A	B	C	D	E	F	G	J	K	L
<b>FORMULAIRE POUR AUTO-DIAGNOSTIC</b>									
<b>(ISO 27001)</b>									
<b>POLITIQUES DE SÉCURITÉ</b>									
4	Il existe un document (s) de politiques de sécurité de SI	<input checked="" type="checkbox"/>	TRUE	1					
5	Il existe une réglementation relative à la sécurité de SI	<input checked="" type="checkbox"/>	TRUE	1					
6	Il existe des procédures relatives à la sécurité de SI	<input type="checkbox"/>	FALSE	0					
7	Il existe un responsable des politiques, de normes et de procédures	<input checked="" type="checkbox"/>	TRUE	1					
8	Il existe des mécanismes pour la communication aux utilisateurs des normes	<input checked="" type="checkbox"/>	TRUE	1					
9	Il existe des contrôles réguliers pour vérifier l'efficacité des politiques	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
10	<b>ORGANISATION DE LA SECURITE</b>								
11	Il existe des rôles et des responsabilités définis pour les personnes impliquées dans la sécurité	<input type="checkbox"/>	FALSE	0					
12	Il existe un responsable chargé d'évaluer l'acquisition et les changements de SI	<input checked="" type="checkbox"/>	TRUE	1					
13	La Direction et les secteurs de l'Organisation prend part des sujets de sécurité	<input type="checkbox"/>	FALSE	0					
14	Il existe des conditions contractuelles de sécurité avec des tiers et outsourcing	<input checked="" type="checkbox"/>	TRUE	1					
15	Il existe des critères de sécurité dans le manieiment de tierces parties	<input checked="" type="checkbox"/>	TRUE	1					
16	Il existe des programmes de formation en sécurité pour les employés, clients et tiers	<input checked="" type="checkbox"/>	TRUE	1					
17	Il existe un accord de caractère confidentiel de l'information pour ceux qu'y accède.	<input checked="" type="checkbox"/>	TRUE	1					
18	On révisé l'organisation de la sécurité périodiquement par une entreeprise externe	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
19	<b>ADMINISTRATION DES ACTIFS</b>								
20	Il existe un inventaire des actifs mis à jour	<input checked="" type="checkbox"/>	TRUE	1					
21	L'inventaire contient des actifs de données, du software, équipements et services	<input checked="" type="checkbox"/>	TRUE	1					
22	On dispose d'une classification de l'information selon la criticité de de cette dernière	<input checked="" type="checkbox"/>	TRUE	1					
23	Existe un responsable des actifs	<input checked="" type="checkbox"/>	TRUE	1					
24	Il existe des procédures pour classer l'information	<input checked="" type="checkbox"/>	TRUE	1					
25	Il existe des procédures d'étiquetage de l'information	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
26	<b>SECURITE DES RH</b>								
27	On a définies responsabilités et rôles de sécurité	<input checked="" type="checkbox"/>	TRUE	1					
28	On prend en considération la sécurité dans la sélection et la baisse du personnel	<input checked="" type="checkbox"/>	TRUE	1					
29	Les conditions de confidentialité et responsabilités dans les contrats sont précisées	<input checked="" type="checkbox"/>	TRUE	1					
30	On distribue la formation adéquate sécurité et traitement d'actifs	<input type="checkbox"/>	FALSE	0					
31	Il existe un canal et des procédures claires à suivre en cas d'incident de sécurité	<input checked="" type="checkbox"/>	TRUE	1					
32	On reprend les données des incidents de manière détaillée	<input checked="" type="checkbox"/>	TRUE	1					
33	Informé les utilisateurs des vulnérabilités observées ou soupçonnées	<input checked="" type="checkbox"/>	TRUE	1					
34	On informe aux utilisateurs, suite ce dossier, sous aucune circonstance, d'évaluer les vulnérabilités.	<input checked="" type="checkbox"/>	TRUE	1	Oui	Non			
							83.33	16.67	
							75.00	25.00	
							100.00	0.00	

### The ten largest holders of ISO 27001 certificates



Źródła wykresów:

Certification News, 2008  
 PBSG, [www.iso27000.pl](http://www.iso27000.pl), 2010

Inne standardy

# COBIT

- COBIT (*Control Objectives for Information and related Technology*)
  - Standardowe miary, wskaźniki, procesy i rekomendacje, kontrolna lista audytowa
  - Maksymalizacja efektywności systemów IT
  - Część DS5 – *Ensure Systems Security*
  - Kompatybilny z ISO 27002
  - Organizacja: ISACA
    - Wsparcie "Big 4"

# ITIL

- ITIL (*Information Technology Infrastructure Library*)
  - Model PDCA
  - Procesy i zalecenia dla maksymalizacji efektywności usług IT i zarządzania infrastrukturą IT
  - Kompatybilny z ISO 27002
  - Organizacja: Central Computers and Communications Agency (CCTA, UK)

# NIST

- National Institutes of Standards and Technology (NIST)
  - FIPS – Federal Information Processing Standards
    - Normy (wiążące dla amerykańskiej administracji)
  - SP – Special Publications
    - Rekomendacje, najlepsze praktyki
- Godne uwagi
  - Bardzo szeroki zakres
  - Częste aktualizacje
  - Także niskopoziomowe i techniczne

# NIST SP

- SP 800-39 „Managing Risk from Information Systems. Organizational Perspective”
- SP 800-60 „Guide for Mapping Types of Information and Information Systems to Security Categories”
- SP 800-53 „Recommended Security Controls for Federal Information Systems”
- SP 800-70 „National Checklist Program for IT Products-- Guidelines for Checklist Users and Developers”
- SP 800-53A „Guide for Assessing the Security Controls in Federal Information Systems”
- SP 800-37 „Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach”

# ISF SOGP

- ISF (*Information Security Forum*)
  - *Standard of Good Practice for Information Security*
- Integracja z innymi standardami
  - ISO 27002, COBIT, SOX, PCI DSS, BASEL II, Dyrektywa EU o ochronie danych osobowych

# Inne

- **SAS70 (*Statement of Auditing Standards*)**
  - AICPA (*American Institute of Certified Public Accountants*)
- **PCI (*Payment Card Industry*)**
  - DSS (*Data Security Standard*)
- **SOX (*Sarbanes-Oxley*)**
  - PCAOB
- **Europejska dyrektywa o ochronie danych osobowych**
  - Ustawa o ochronie danych osobowych (uodo)
  - GIODO

# ISO 27003

Information security management system implementation guidance

## **Guidance on using PDCA method**

1. Introduction
2. Scope
3. Terms & Definitions
4. CSFs (Critical success factors)
5. Guidance on process approach
6. Guidance on using PDCA
7. Guidance on Plan Processes
8. Guidance on Do Processes
9. Guidance on Check Processes
10. Guidance on Act Processes
11. Inter-Organization Co-operation

# ISO 27004

## **Information security management -- Measurement**

The standard is intended to help organizations **measure and report the effectiveness** of their information security management systems, covering both the security management processes (defined in ISO/IEC 27001) and the security controls (ISO/IEC 27002).

# ISO/IEC 27005

## **Information security risk management**

ISO/IEC 27005:2008 provides **guidelines for information security risk management**. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

- Por. **ISO 31000**
  - *Risk management -- Principles and guidelines on implementation*
- Por. **NIST SP 800-30**

# ISO 27007

## **Guidelines for information security management systems auditing**

This standard will provide **guidance for accredited certification bodies, internal auditors, external/third party auditors and others auditing Information Security Management Systems against ISO/IEC 27001** (i.e. auditing the management system for compliance with the standard) but may also offer advice to those auditing or reviewing ISMSs against ISO/IEC 27002 (i.e. auditing the organization's controls for their suitability in managing information security risks) although this may be covered instead by ISO/IEC TR 27008.

# Narzędzia

- ISO27k Toolkit
  - MS Excel
- EBIOS (Francja, DSSI)
  - Java
- SOMAP
  - Open Information Security Risk Assessment Guide
  - SOBF (*Security Officer's Best Friend*) – Java
- Duży rynek narzędzi komercyjnych

# Pomiary bezpieczeństwa

# Miary bezpieczeństwa

- Na potrzeby analizy ryzyka (*risk analysis*)
  - Jakościowa (*qualitative*) – Low/Medium/High
  - Ilościowa (*quantitative*) – SLE, ALE (\$)
- Na potrzeby zarządzania podatnościami (*vulnerability management*)
  - Standardyzacja podatności
    - CVE, CCE, CPE, CWE
    - BID, QID, Microsoft, Secunia...
  - Standardyzacja stopnia zagrożenia (*impact*)
    - Umowna klasyfikacja katalogowa (*severity*)
    - CVSS (*Common Vulnerability Scoring System*)

# Standardyzacja podatności

- NIST NVD (National Vulnerability Database)
  - CVE (Common Vulnerability Enumeration
    - „*Microsoft Windows Server Service Could Allow Remote Code Execution*” (CVE-2008-4250)
  - CWE (Common Weakness Enumeration)
    - “*Cross Site Request Forgery*” (CWE-352)
  - CCE (Common Misconfigurations Enumeration)
    - W trakcie opracowywania...
  - CPE (Common Platform Enumeration)
    - `cpe:/a:apache:apache-ssl:1.37`

## Standardyzacja podatności

- Inne katalogi podatności
  - SecurityFocus (BID), Secunia (SA), Qualys (QID), VUPEN, OSVDB...
- Klasyfikacja producentów oprogramowania
  - Microsoft, Sun, Cisco...

33

Example: „Microsoft Windows Server Service Could Allow Remote Code Execution”

- CVE-2008-4250
- QID (Qualys Guard) – 90464
- BID – 31874
- Microsoft – MS08-067
- Secunia – SA32326
- VUPEN/ADV-2008-2902
- OSVDB 49253

# Standardyzacja stopnia zagrożenia

- Umowna producentów (*severity*)
  - Opisowa (*Low/Medium/High/Urgent/Critical...*)
  - Liczbowa (1-5)
- NIST CVSS (*Common Vulnerability Scoring System*)
  - Obiektywizacja kryteriów
  - Umożliwia wycenę podatności w dużej skali
  - Wycena ułatwia przydział zasobów

# CVSS

- Base CVSS
  - Odzwierciedla stałą charakterystykę podatności
    - Zdalna/lokalna? Trudna/łatwa? Uwierzytelnienie?
- Temporal CVSS
  - Charakterystyka zmienna w czasie
    - Potwierdzona/niepotwierdzona? Exploit? Poprawki?
- Environmental CVSS
  - Zagrożenie w konkretnym środowisku lokalnym
    - E-CVSS danego serwera *versus* CVSS podatności

# Przykład CVSS

- Podatności w Microsoft RPC DCOM
  - CVE-2003-0352 (Blaster)
    - Nie daje uprawnień administratora – CVSS=7,5
  - CVE-2003-0715
    - Daje uprawnienia administratora – CVSS=10 (max)
  - Poza tym Base CVSS wysokie
    - Dostępna przez sieć
    - Łatwość ataku
    - Bez uwierzytelnienia

# Metody pomiaru bezpieczeństwa

- Audyt
  - Systematyczny, powtarzalny, obiektywny, ograniczony zakres oceny, globalnie rozpoznawany
- Test penetracyjny
  - Szerszy zakres , ocena całościowego stanu bezpieczeństwa, aktualny stan wiedzy, częściowo systematyczny, uzależniony od kompetencji zespołu
- Ocena bezpieczeństwa
  - Zastosowanie wiedzy i doświadczenia eksperta, aktualny stan wiedzy

# Metody pomiaru bezpieczeństwa

- Pomiar powtarzalne
  - Statystyki operacyjne z procesów biznesowych
    - Liczba eskalacji? Liczba opóźnień? Liczba fraudów?
  - Narzędzia do oceny podatności (*vulnerability assessment*)
    - Skanery działające w trybie ciągłym (tydzień, miesiąc)
    - Cykliczne testy penetracyjne
  - Analiza zdarzeń
    - Firewalle, systemy IDS/IPS
    - Logi systemowe (*system alerts*)

# Audyt bezpieczeństwa teleinformatycznego

# Audyt bezpieczeństwa systemu

"Dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną polityką bezpieczeństwa i z procedurami operacyjnymi oraz w celu wykrycia przełamań bezpieczeństwa i zalecenia wskazanych zmian w środkach nadzorowania, polityce bezpieczeństwa oraz w procedurach"

Źródło: PN-I-02000:2002, pkt 3.1.007

"usystematyzowany, niezależny i udokumentowany proces uzyskania dowodu z auditu i obiektywnej oceny w celu określenia w jakim stopniu spełniono uzgodnione kryteria auditu"

Źródło: PN-EN ISO 9000:2001, pkt 3.9.1

# Cele audytów

- Obiektywizacja kryteriów
  - Niewspółmierna rola systemów IT
- Minimalny standard jakości (*baseline*)
  - Różne poziomy dojrzałości uczestników rynku (*maturity levels*)
- Podstawa do przyjęcia zobowiązań
  - Łącuch dostaw, podwykonawcy
  - SLA (*Service Level Agreement*)

# Cele audytu wewnętrznego

- Ocena zgodności procesów z celami organizacji
  - Optymalizacja procesów
  - Przywrócenie odpowiednich priorytetów zadań
  - Ograniczenie zjawiska "przesunięcia celów"
- Psychologiczne bariery audytu - zapobieganie
  - Audyt nie służy "zwalczaniu" kogokolwiek
  - Audyt to nie kontrola
  - Audyt ma pomóc, nie przeszkadzać

## Cele audytu zewnętrznego

- Zlecany przez organizację
  - Cele jak w audycie wewnętrznym
- Zlecany przez trzecią stronę
  - Zgodność z regulacjami (*legal compliance*)
  - Zgodność z deklaracjami organizacji
  - Ocena przed transakcją (*due dilligence*)

# Audyt niezależny

- Nie wykonuje go
  - Projektant, dostawca, wykonawca, integrator
- Audyt wewnętrzny (pierwszej strony)
  - Niezależność w hierarchii służbowej
- Audyt zewnętrzny (drugiej, trzeciej strony)
  - Niezależność organizacyjna

# Audyt systematyczny

- Powtarzalność
  - Plan audytu, metodyka, minimalne wymagania
- Obiektywność
  - Brak uznaniowości w interpretacji faktów
    - Co jest "wystarczająco bezpieczne" a co nie
  - Ściśle określone kryteria zgodności

# Audyt systematyczny

- Ustalona lista kontrolna (*checklist*)
  - Zamknięta, kompletna
  - Punkt odniesienia do protokołu rozbieżności (*gap analysis*)
  - Na podstawie standardów lub przepisów
  - Polityki, standardy, procedury organizacji
- Czy można prowadzić audyt bez punktu odniesienia?
- Wady listy kontrolnej
  - Wysokopoziomowa, statyczna

# Audyt udokumentowany

- Dowód (*evidence*) jako krytyczna część audytu
  - Na pytania z listy kontrolnej odpowiada audytor
    - Nie audytowany
  - Odpowiedzi na podstawie dowodów
- Źródła informacji audytowych
  - Ankiety, wywiady (próba statystyczna)
  - Wizja lokalna
  - Dokumentacja strategiczna i operacyjna
  - Analizy, testy i badania

## Warunki obiektywności

- Audytor ocenia dowody
  - Nie opinie audytowanego
- Audytor ocenia zgodność z założeniami
  - Ocenę rozbieżności prowadzi adresat audytu
- Audytor wybiera próbki audytowe
  - Ocena losowych próbek z dużych ilości obiektów
  - Czy próbka jest losowa?
  - Czy próbka jest reprezentatywna?
  - Dlaczego wybrano te, a nie inne objekty?

48

Przykład:

Na prośbę o dostarczenie próby 5% transakcji właściciel procesu biznesowego dostarcza 100 przypadków, które nie wykazują większych odchyień od określonych wartości brzegowych. Czy taki audyt można określić mianem obiektywnego?

## Istotne cechy audytu

- Ograniczony do zdefiniowanego zakresu
  - Brak oceny obiektu, który nie jest przedmiotem audytu
- Ograniczony do punktu odniesienia
  - Brak oceny obiektu wg kryteriów nie ujętych w liście kontrolnej
- Brak gwarancji "ogólnego bezpieczeństwa"
  - Produkt lub proces pozytywnie zaudytowany nadal może mieć istotne podatności

# Metodyka audytu

- LP-A (Liderman-Patkowski, WAT)
- Oparty o ISO 27001
- Skład zespołu audytowego
  - 2 audytorów, 3 specjalistów audytowych
  - Personel pomocniczy (ankieterzy itd)
  - Eksperti z poszczególnych dziedzin
- Narzędzia audytowe (skanery)

# Proces audytu #1

- Przygotowanie audytu
  - Udzielenie uprawnień, osoby kontaktowe, zasady komunikacji, harmonogram, szkolenie zarządu organizacji audytowanej
- Ścieżka formalna
  - Badanie jakości zarządzania ISMS – dokumentacja oficjalna, dokumenty operacyjne, ankiety

## Proces audytu #2

- Ścieżka techniczna
  - Analiza architektury systemów IT, analiza stanu faktycznego infrastruktury
  - Przegląd i ocena zabezpieczeń
- Prezentacja wyników audytu
  - Protokół rozbieżności
  - Zalecenia pokontrolne

# Testy penetracyjne

# Rola audytu i testu penetracyjnego

- Ograniczenia audytu
  - Szybkie zmiany w technologii
    - Czas życia standardów audytowych – lata
    - Czas życia typowych podatności w systemach – dni
  - Zakres oceny audytowej
    - Może nie obejmować wszystkich aspektów i scenariuszy
- Rola testu penetracyjnego
  - Ocena praktycznego, chwilowego stanu bezpieczeństwa,
  - Konkretny, działający system
  - Próba uzyskania dowodu nieskuteczności

# Cechy testów penetracyjnych

- Szeroki zakres
  - Testy od wysoko- do niskopoziomowych
  - Wszystkie komponenty systemu
  - Cel – dowolny scenariusz prowadzący do przełamania zabezpieczeń
- Utrudniona powtarzalność
  - Zależny od kompetencji zespołu
  - Zależny od aktualnego stanu wiedzy
  - Zależny od dostępu do informacji

# Próby standaryzacji

- Algorytm testu penetracyjnego
  - 1) Sprawdź wersję serwera WWW, 2) sprawdź w bazie znane podatności, 3) ...
  - Nadal ograniczone kompetencjami zespołu
  - Zbyt duża liczba scenariuszy
- Główna zaleta testu penetracyjnego
  - Możliwość odkrycia nowych ataków dzięki kreatywności zespołu
  - Możliwość wskazania niestandardowych scenariuszy ataku

## Co należy standardyzować?

- Kroki, które muszą być wykonane
  - Minimalne wymagania
- Zakres informacji dokumentowanej
- Zakres informacji raportowanej
- Zasady komunikacji
- Zakres testu
  - Np. daty i godziny wykonywania testów
- Wymagania formalne
  - Np. upoważnienie do testu

# Kwestie prawne

- Kodeks karny
  - Przestępstwa przeciwko ochronie informacji
    - Art. 265-269b kk
    - "Oprogramowanie hakerskie" (art. 269b)
- Obowiązki zespołu testującego
  - Pisemne upoważnienie właściciela systemu
  - Precyzyjnie opisany zakres upoważnienia
  - Dokumentacja działań testowych
  - Dokumentacja kontaktów z klientem

## Kiedy test ma sens?

- Przed udostępnieniem aplikacji w sieci
  - Później może być za późno
- Prowadzony na produkcyjnej wersji systemu
  - Takiej, jaka będzie dostępna dla klientów
- Zakończone prace rozwojowe
  - Testy funkcjonalne, poprawki, zmiany
- Czas testu uwzględniony w harmonogramie
  - Jeśli wyniki mają być miarodajne

# Test penetracyjny a włamanie

- Test penetracyjny trudniejszy niż włamanie
  - Konieczność sprawdzenia wszystkich scenariuszy
    - Włamanie – najkrótszą drogą do celu
  - Konieczność dokumentacji działań
    - Włamanie – nie ma takiej potrzeby
  - Wymaganie wobec zespołu testującego
    - Kwestie etyczne, systematyczność, rzetelność

# Metody testowania

- "Black box"
  - Ograniczona wiedza zespołu testującego
  - Zalety – brak uprzedzeń, kwestie psychologiczne
  - Wady – brak widoczności niektórych trywialnych zagrożeń
- "Crystal box"
  - Pełny dostęp zespołu do "środka" systemu
  - Zalety – lepsza widoczność nietypowych scenariuszy
  - Wady – możliwość przyjęcia błędnych założeń

# Istniejące metodyki

- OSSTMM (Open Source Security Testing Methodology Manual)
- NIST SP800-42 „Guideline on Network Security Testing „
- NIST SP800-115 „Technical Guide to Information Security Testing“
- OISSG „ISSAF Penetration Testing Framework“
- P-PEN (Patkowski, WAT)
- MindCert Certified Ethical Hacker mind-map series
- OWASP (Open Web Application Security Project)
- Penetration Testing Framework (Kevin Orrey)

# Typowy scenariusz testu

- Enumeracja i inwentaryzacja zasobów
  - Skan podsieci IP
- Enumeracja usług
  - Skan portów, protokołów
- Enumeracja aplikacji
  - Skan odpowiedzi na portach, nagłówki, wersje...
- Wartość dodana
  - O czym klient nie wiedział wcześniej?

# Mapowanie podatności

- Zasoby, usługi, aplikacje
  - Jakie znane podatności?
    - Np. wykryta wersja serwera Apache/1.3.18
      - Jakie znane podatności?
        - Czy są praktyczne?
    - Cel – stwierdzenie podatności
      - Testowanie (exploit) tylko za zgodą klienta
  - Brak podatności, wersja – wartościowa informacja
    - Załączyć do raportu, ocena przydatności przez klienta

64

Podatności:

Securityfocus.com

NVD (NIST)

OSVDB

Secunia.com

Exploity:

Packetstormsecurity.org

Metasploit.org

# Aspekt skali

- Różne zakresy testów
  - Jeden serwer? Sto serwerów? 10 tys. stacji roboczych?
- Testy zautomatyzowane
- Testy losowej próbki
- Dobre wyniki w jednorodnej grupie
  - Konieczność inwentaryzacji całości i agregacji podobnych grup

# Skannery automatyczne

- Ogólnego przeznaczenia
  - Nessus, OpenVAS, QualysGuard, IBM Internet Scanner...
- Wykrywanie sygnaturowe
- Zalety
  - Masowe, cykliczne skany podobnych zasobów
- Wady
  - Możliwość pominięcia nietypowych zasobów
  - Niska skuteczność wobec aplikacji webowych

## Skannery automatyczne

- Aplikacje webowe
  - IBM Rational AppScan (WatchFire), HP WebInspect, Acunetix
- Wykrywanie sygnaturowe plus uniwersalne techniki ataków
- Zalety
  - Przewaga w testach rozbudowanych aplikacji
- Wady
  - Możliwość pominięcia oczywistych, choć nietypowych podatności
  - Niska skuteczność w testowaniu logiki biznesowej

67

W3af – many modules (Python, command-line, GUI)

Sqlmap – many variants of SQL Injection (Python, command-line)

Nikto – „hidden” file and directory finder (Perl, command-line)

Wikto – „hidden” file and directory finder, supports Nikto (.NET, GUI)

JAD – Java decompiler (open-source)

PMD – static source code checker for Java (open-source)

Disassembly

– IDA Pro

Debuggers

– OllyDbg (open-source)

# Jakość testów penetracyjnych

- Metodyki testów penetracyjnych
  - Raczej "lista zadań" niż "lista kontrolna"
- Próby standardyzacji dokładności testu
  - OWASP ASVS (*Application Security Verification Standard*)
    - Level 1 – Automated verification
    - Level 2 – Manual verification
    - Level 3 – Design verification
    - Level 4 – Internal verification

# Statyczna analiza kodu

- Ograniczenia badania behawioralnego
  - Nietypowe scenariusze
  - Moduły nieujawnione w interfejsie
  - Błędy w logice biznesowej
- Statyczna analiza kodu (SCA – *Static Code Analysis*)
  - Ręczna
  - Automatyczna – Veracode, Fortify, Checkmarx, Ounce Labs...

Kontakt z autorem:

[pawel.krawczyk@hush.com](mailto:pawel.krawczyk@hush.com)

Tel. +48-602-776959

Prezentacja udostępniona na licencji Creative Commons BY-NC-SA  
(„uznanie autorstwa”, „użycie niekomercyjne”, „na tych samych warunkach”)

<http://creativecommons.org/licenses/by-nc-sa/3.0/pl/>

70

Literatura:

<http://ipsec.pl/>

<http://securitystandard.pl/>

Andrew Jaquith, "Security metrics"