...making excellence a habit.™

BSI Kitemark™ dla bezpiecznych transakcji cyfrowych

Rafał Śmiłowski: Dyrektor Operacyjny, C&R

By Royal Charter

BSI Kitemark™ dla bezpiecznych transakcji cyfrowych

- Bezpieczeństwo transakcji cyfrowych- problem i jego rozwiązanie
- Kitemark™ - jak to działa?
- ISO / IEC 27001 (Standard Zarządzania Bezpieczeństwem Informacji)
- Standard OWASP ASVS v2
- Model wyceny podatności CVSS (Common Vulnerability Scoring System)
- Kroki do uzyskania Kitemark™
- Testy penetracyjne

Bezpieczeństwo transakcji cyfrowych -problem

- W ciągu każdego miesiąca 4 mld operacji finansowych odbywa się poprzez smartfony
- Ostatnie badania przeprowadzone przez BSI wykazały, że:

- 30% ludzi nie ufa aplikacjom, które używane są do obrotu/ transmisji ich pieniędzmi
- 42% ludzi ma obawy o bezpieczeństwo swoich danych osobowych, gdy dokonuje zakupów online
- 81% organizacji doświadczyło naruszenia bezpieczeństwa (dane za rok 2014r)
- 31% najgorszych naruszeń bezpieczeństwa spowodowane było przez przypadkowy, ludzki błąd
- 60% organizacji nie zagwarantowało szkoleń w zakresie bezpieczeństwa informacji
- 73% organizacji doznało infekcji przez wirusy lub złośliwe oprogramowanie*

- W jaki sposób banki i właściciele aplikacji są w stanie zapobiegać oszustwom?
- W jaki sposób banki mogą chronić swoją reputację?
- Czy klienci mogą ufać aplikacjom, z których korzystają?

* Dane BSI

Rozwiązanie

- BSI Kitemark ™ dla bezpiecznych transakcji cyfrowych wychodzi naprzeciw oczekiwaniom **podmiotów chcących realnie zabezpieczać dane** wrażliwe swoich klientów dokonujących transakcjach elektronicznych.

- BSI Kitemark został opracowany, aby **pomóc konsumentom pewnie i łatwo zidentyfikować strony internetowe lub aplikacje, którym mogą ufać**

- BSI Kitemark ™ dla bezpiecznych transakcji cyfrowych wymaga, aby **strony internetowe lub aplikacje poddawane były rygorystycznym testom w** celu zapewnienia odpowiedniej kontroli bezpieczeństwa w obrocie danymi finansowymi i/lub osobowymi.

- Producenci i dostawcy stron internetowych lub aplikacji (od bankowych po rozrywkowe) będą mogli przekonać swoich klientów przez umieszczenie znaku BSI Kitemark ™ na swoich produktach lub materiałach reklamowych **o posiadaniu mechanizmu chroniącego przetwarzane dane w transakcjach elektronicznych.**

- BSI Kitemark ™ został opracowany wspólnie z Barclays Bank oraz Gotham Digital Sciences (GDS)

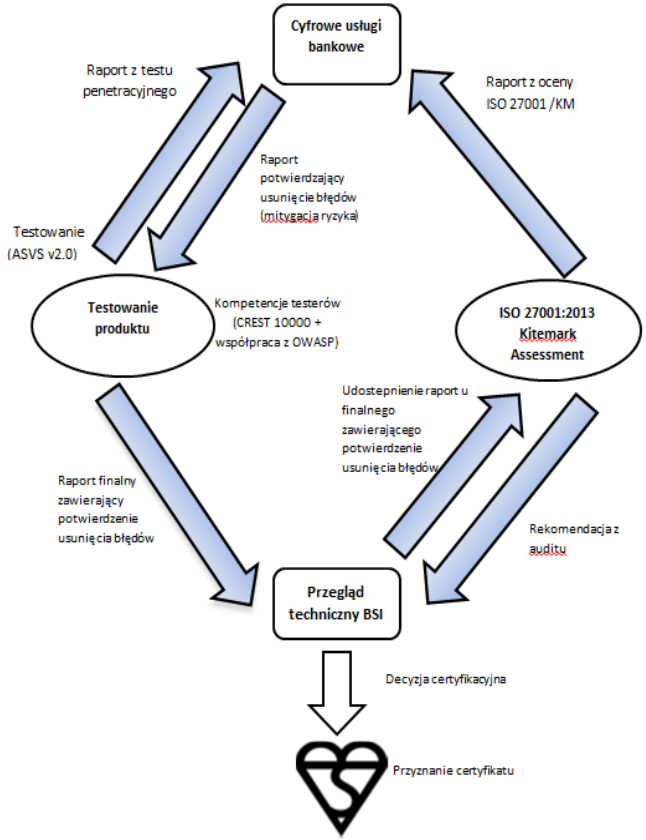
Jak działa BSI Kitemark ™ dla bezpiecznych transakcji cyfrowych

- Produkt BSI określa sposób i wymagania do niezależnego testowania aplikacji

- Klienci aplikujący o uzyskanie Kitemark™ poddani ocenie na 2 poziomach:
- Audit zgodności z wymaganiami standardu ISO/IEC 27001 w zakresie stosowanych aplikacji
- Penetracyjne testy aplikacji w oparciu o OWASP standard ASVS V2.0

Jak działa BSI Kitemark ™ - mechanizm działania

- Ocena programów aplikacyjnych wykorzystując ISO 27001
- Wykonanie testów penetracyjnych w programach aplikacyjnych przy użyciu standardu OWASP ASVS V2.0
- Testy muszą być przeprowadzane przez wykwalifikowanych testerów (poziom CCT-CREST 10000 hours tester)
- Analiza wyników dokonywana jest w ramach modelu wyceny podatności CVSS (Common Vulnerability Scoring System).
  Wyniki oceny określają poziom podatności aplikacji na zagrożenia (krytyczny, wysoki i średni) oraz aplikacje, które przeszły test



Utrzymanie certyfikacji

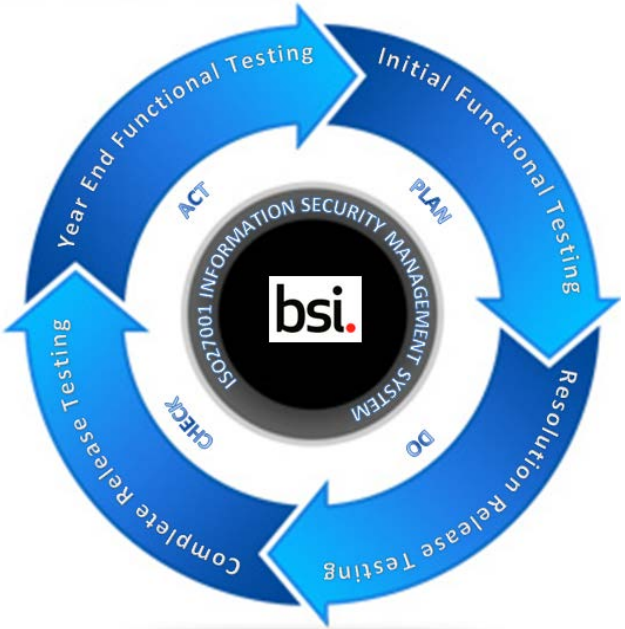
- 1 raz w roku 4 pełne tetsty (EtE)
- Co 3 miesiące osoba wykonująca testy penetracyjne dostarcza do BSI raport podsumowujący uzyskane wyniki
- Cykliczne audity nadzorcze (27k) w siedzibie klienta wykonywane przez auditorów BSI w celu przeglądu wyników testów

➢ Podniesienie dużej niezgodności wymaga poinformowanie dyrektora ds. Certyfikacji w BSI i zawieszenie certyfikatu do czasu usunięcia przyczyny źródłowej problemu

- Przegląd roczny BSI:

➢ 4 raporty z testów penetracyjnych z wynikiem pozytywnym

➢ 4 raporty z wizyt nadzorczych w zakresie ISO 27001 z wszystkimi zamkniętymi niezgodnościami



...making excellence a habit.™

Testy penetracyjne aplikacji

Wojciech Dworakowski: Securing

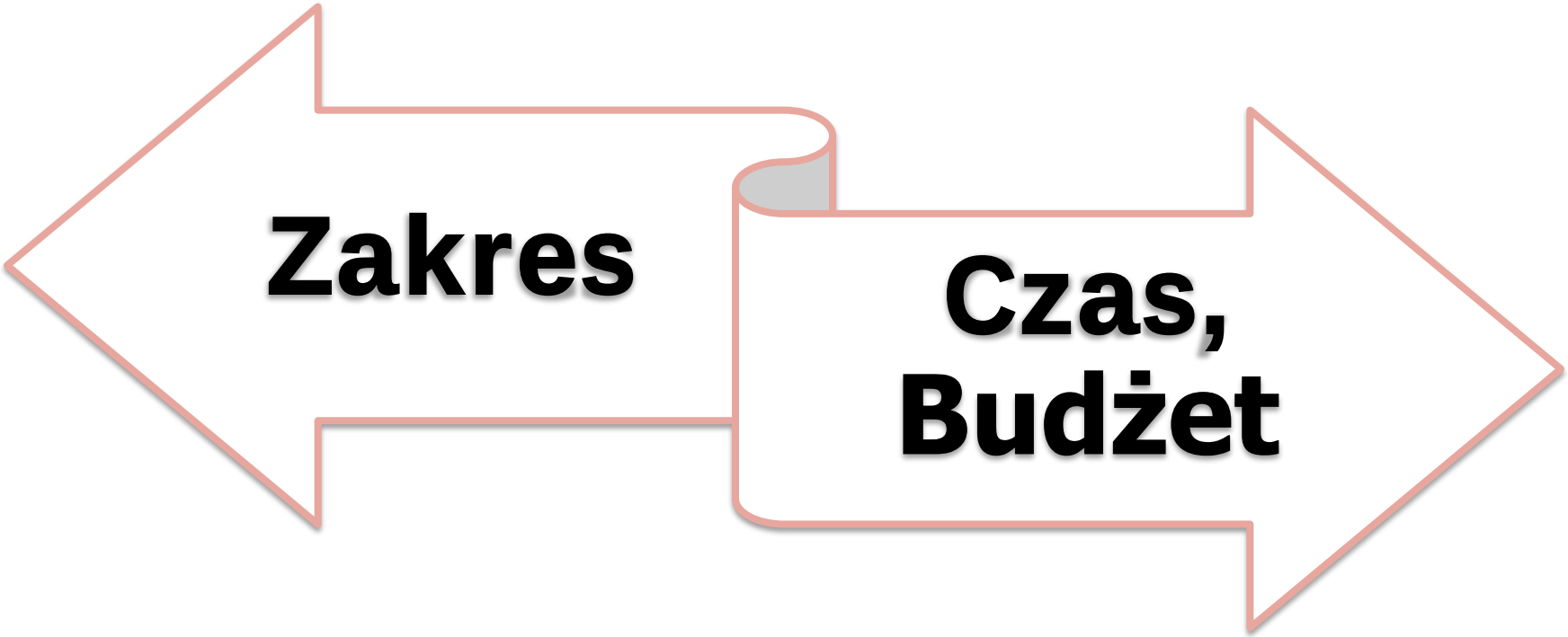
Testy penetracyjne - wyzwania

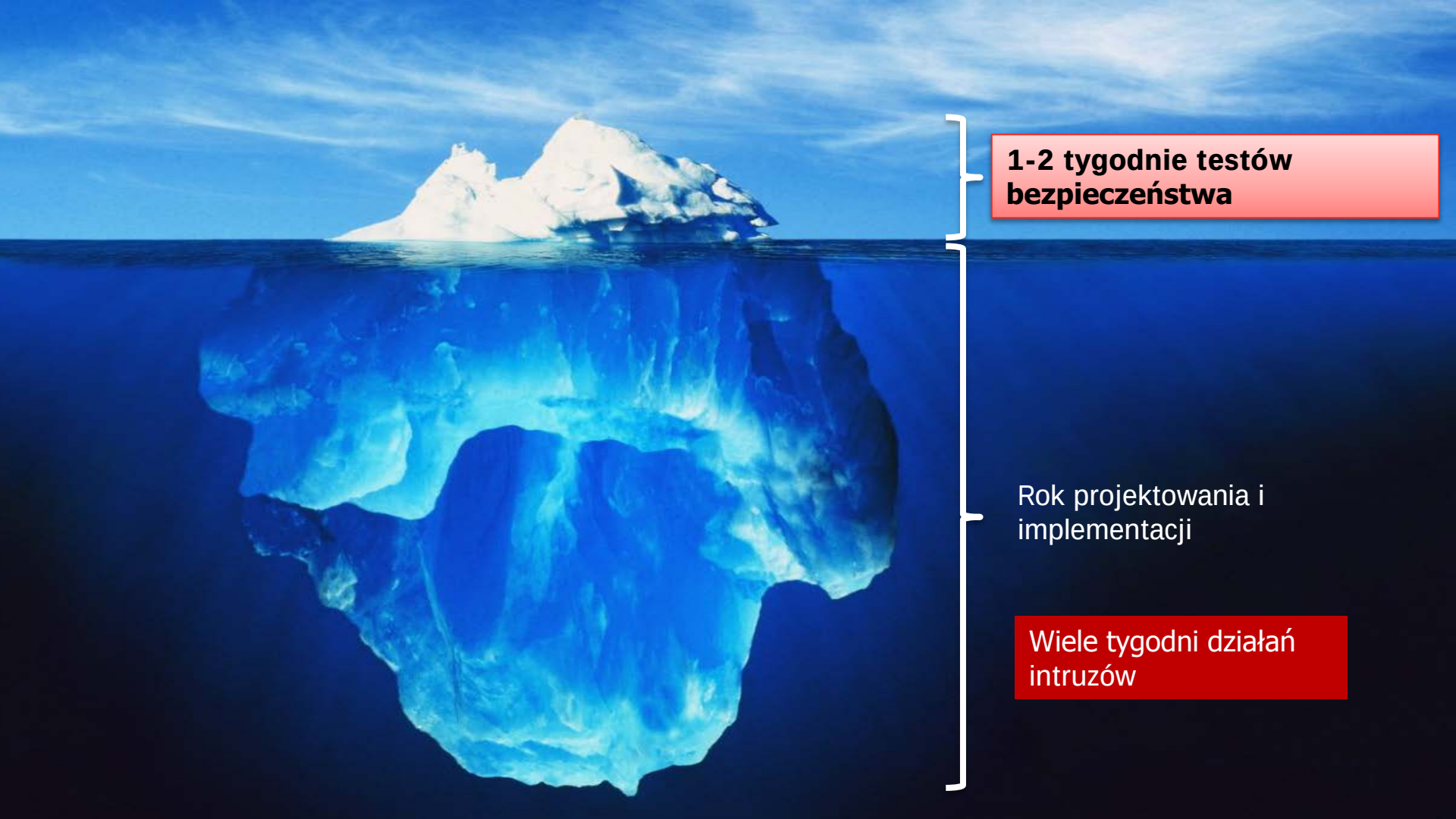
- Znaleziono N podatności
  ale…

- Czy znaleziono wszystkie istotne podatności?
- Czy testy objęły wszystkie istotne zagrożenia?
- Czy szukano tam gdzie trzeba?
- Czy test symuluje realne zagrożenie (atak)?

bsi.

Testy penetracyjne - wyzwania




1-2 tygodnie testów bezpieczeństwa
Rok projektowania i implementacji
Wiele tygodni działań intruzów

ASVS - Application Security Verification Standard

- Projekt fundacji OWASP
  - Aktywnie rozwijany: v1 - 2007, v2 - 2013, v3 - 2015
- Standard darmowy i otwarty
- Lista kontrolna typowych zabezpieczeń
- Pogrupowana na zakresy (uwierzytelnienie, autoryzacja, walidacja, ...)
- 3 poziomy dokładności sprawdzeń

bsi.

Grupy wymagań (rozdziały) ASVS v2

- V1. Uwierzytelnianie
- V2. Zarządzanie sesją
- V3. Kontrola dostępu
- V4. Walidacja wejścia
- V5. Szyfrowanie
- V6. Obsługa błędów i logowanie
- V7. Ochrona danych
- V8. Bezpieczeństwo komunikacji
- V9. Bezpieczeństwo HTTP
- V10. Ochrona przed złośliwym kodem
- V11. Logika biznesowa
- V12. Pliki i zasoby
- V13. Aplikacje mobilne

bsi.

V8: Communications Security Verification Requirements

The table below defines the corresponding verification requirements that apply for each of the verification levels. Verification requirements for Level 0 are not defined by this standard.

	COMMUNICATIONS SECURITY VERIFICATION REQUREMENT	LEVELS		
		1	2	3
V8.1	Verify that a path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and that each server certificate is valid.	✓	✓	✓
V8.2	Verify that TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.		✓	✓
V8.3	Verify that backend TLS connection failures are logged.		✓	✓

ASVS i Kitemark for Secure Digital Transactions

- ASVS Level 3
- ASVS definiuje minimalny zakres testów, można (i trzeba) go rozszerzać
- Testy powinny zostać zaprojektowane w oparciu o **realne ryzyko dla danego systemu**
- Powinny uwzględniać specyfikę aplikacji i stosowanych zabezpieczeń

Produktem testów bezpieczeństwa jest raport

- **Lista kontrolna ASVS**
  - Rezultaty sprawdzeń
  - Komentarz do każdej sesji
- **Opisy podatności**
  - scenariusz testowy / proof of concept,
  - warunki i skutki wykorzystania,
  - wycena podatności

- Zalety:
  - Dobrze zdefiniowany zakres
  - Lista wykonanych testów
  - Informacja o tym co działa poprawnie (a nie tylko o defektach)

bsi.

Wycena podatności - CVSS

- **CVSS** (Common Vulnerability Scoring System)
- Jednoznaczny i powtarzalny sposób wyceny podatności
- Standard darmowy i otwarty

- Algorytm uwzględniający 14 metryk
  - Metryki bazowe – stałe w czasie i niezależne od wdrożenia
    - Możliwość wykorzystania podatności – np. złożoność ataku, wymagane przywileje
    - Wpływ na poufność, integralność, dostępność
  - Metryki środowiskowe – dodatkowe zabezpieczenia lub podatności
  - Metryki zależne od czasu – np. dostępność „exploita”, łatek