CryptoPanel

edycja #25

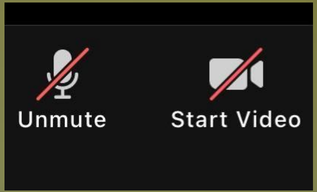
Już za moment zaczynamy...

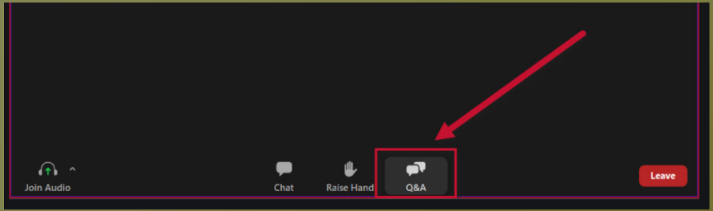
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

edycja #25

Audytowanie sprzętowych modułów kryptograficznych. Praktyczne podejście.

CryptoPanel

TEST WIEDZY #25

Audytowanie sprzętowych modułów kryptograficznych. Praktyczne podejście.

CryptoPanel

dziś dyskutują

Piotr Wróbel

Regional Sales Manager
Piotr.Wrobel@thalesgroup.com
mob. +48 669 88 99 76

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

problem

Nasze wyzwania (czyli „co nas boli…”).

- **Zajmujemy się audytami i przeglądami systemów informatycznych na co dzień**
- **Zdarza się, że przychodzi nam skontrolować rozwiązanie klasy HSM**
- **Posiadamy wypracowane procedury audytowe dla podstawowych elementów infrastruktury (sieć, serwery aplikacyjny, stacja robocza, chmura,…), które dostosowujemy dla konkretnego zlecenia czy przypadku**
- **Jak jest specyfika rozwiązań HSM?**
  - Co warto uwzględnić podczas audytu tak aby przegląd przyczynił się do zwiększenia bezpieczeństwa?
  - O co zapytać?
  - Co sprawdzić?
- **Prowadzimy biznes w mocno regulowanym rynku.**
- **Okresowo przechodzić obowiązkowe audyty.**
- **Dział IT wykonuje regularne przeglądy infrastruktury i wystawia rekomendacje dla działów utrzymania.**
  - Ma to m.in. na celu utrzymywanie gotowości do „przejścia audytu”.
- **Jak sprawdzać HSM? Na jakie aspekty zwrócić uwagę?**
  - O co może zwrócić uwagę audytor?
  - Jak rozmawiać z audytorem (np. PCI DSS)?
- **Czy istnieją „dobre praktyki” dla utrzymaniu rozwiązania HSM?**

CryptoPanel

rozwiązanie

Geneza

Słownik języka polskiego PWN*

geneza

1. «czynniki, które złożyły się na powstanie i rozwój czegoś»
2. «sposób powstawania i rozwoju czegoś»

Słownik języka polskiego pod red. W. Doroszewskiego*

Geneza

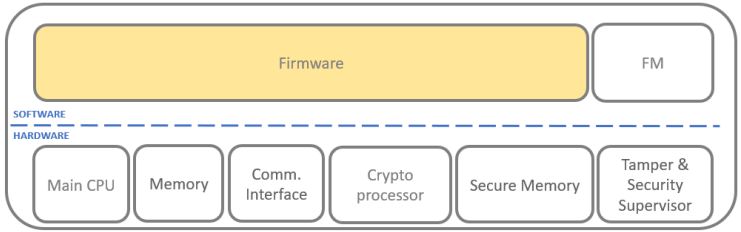
- Coraz szersze stosowanie kryptografii a co za tym idzie, …
- Coraz powszechniejszej występowanie rozwiązań HSM w środowiskach IT, oraz…
- Fakt, że „kryptografia jest mocna w teorii”, ale w praktyce jest tak samo podatna na błędy (w fazie projektu, wdrażania czy eksploatacji)* jak każdy inny element systemu informatycznego, powoduje…

Konieczność dokonywania przeglądów tej klasy rozwiązań pod kątem bezpieczeństwa i zgodności z uwzględnieniem swojej specyfiki.

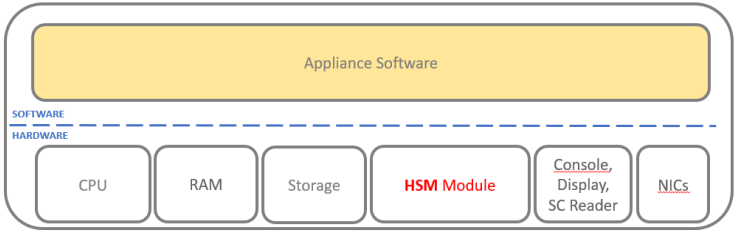
* - nie dotyczy zagadnień audytu mechanizmów kryptograficzny zaimplementowanych w rozwiązaniu HSM

Poznać przeciwnika. Sprzętowy moduł kryptograficzny (HSM).

1. Sprzętowo zabezpieczony zasobnik do przechowywania materiału kryptograficznego.
2. Mechanizmy wykrywania ataku logicznego i fizycznego oraz sabotażu.
3. Specjalizowany procesor kryptograficzny przyśpieszający operacje na kluczach.
4. Urządzenie zdolne do losowej generacji liczb.
5. Archiwizowanie i odtwarzanie materiału kryptograficznego.
6. Uwierzytelnienie dostępu do materiału kryptograficznego.
7. Zapewnienie niezaprzeczalnego śladu audytowego operacji na kluczach szyfrujących.



Ogólna budowa modułu HSM (karta PCI lub urządzenie USB)



Ogólna budowa sieciowego urządzenia HSM

1. W/w cechy potwierdzone w rozpoznawanych na rynku certyfikacjach (FIPS, CC, NITES, PCI, …)
2. Szeroki zestaw narzędzi do integracji (SDK/Toolkits)
3. Długi czas życia i eksploatacji (7-10lat)

Karta PCI | Urządzenie USB | Urządzenie sieciowe

THALES

Poznać przeciwnika. A to nie jest HSM!

Rozwiązania klasy HSM od bardzo podobnych rozwiązań, i co prawda związanych z kryptografią, ale nie zapewniających cech i mechanizmów bezpieczeństwa jak HSM. Należą do nich m.in.:

1. sprzętowe akceleratory kryptograficzne
2. offloadery SSL
3. moduły bezpieczeństwa jak np. TPM
4. HSM-y programowe (emulatory)
5. karty inteligentne

Dodajmy, że urządzenia HSM są towarami podwójnego zastosowania. Zgodnie z Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/821 z dnia 20 maja 2021 [10] i ich wywóz poza granicę Unii Europejskiej wymaga uzyskania odpowiedniego zezwolenia, zaś zamiar ich przywozu na teren Wspólnoty wymaga uprzedniego przesłania informacji do odpowiedniego organu kontroli.

THALES

Można i tak… ☺

Justice Department Indicts Tech CEO for Falsifying Security Certifications

[2024.10.18] The *Wall Street Journal* is reporting that the CEO of a still unnamed company has been indicted for creating a fake auditing company to falsify security certifications in order to win government business.

EDITED TO ADD (11/14): More info.

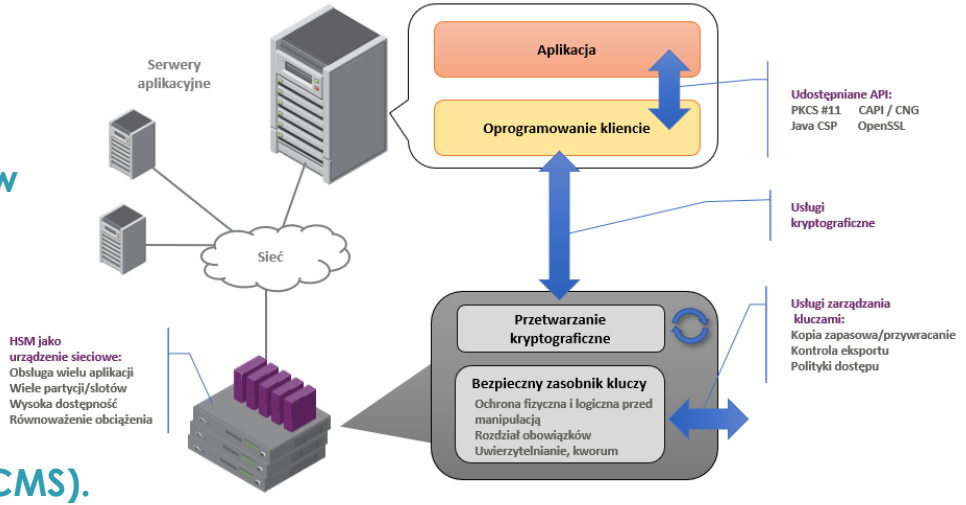
„Deepak Jain, identified as the CEO of a Maryland IT services firm that goes unnamed in a grand jury indictment [PDF] made public on Wednesday, has been charged with six counts of major fraud and one count of making false statements after allegedly telling the financial watchdog that his firm's datacenter in Beltsville, Maryland, had secured the "Tier 4" certification required for a to qualify for an SEC colocation contract.
Such certifications are offered by the Uptime Institute, which defines tier-4 facilities as offering expected uptime of 99.995 percent thanks to the presence of various resilience measures. Jain's unnamed firm allegedly provided fraudulent certification documents to the SEC in 2011 during contract negotiations, leading to it landing the tech deal.
But the certifier – an entity called Uptime Council – didn't exist at all. The DoJ alleges it was created by Jain to falsely certify his business as a tier-4 datacenter operator, and that the fib helped him and several unnamed co-conspirators to cash in."

Poznać przeciwnika. Podział.

PŁATNICZE (Payment)	OGÓLNEGO PRAZNACZENIA (General Purpose)
• Główne funkcje związane z kluczami symetrycznymi (szyfrowanie/deszyfrowanie) • Brak standardu interfejsu aplikacyjnego • Wymagane certyfikacje: PCI HSM, dopuszczalnie: FIPS 140-2 • Import kluczy tylko z użyciem bezpiecznych urządzeń • Silne uwierzytelnianie do funkcji administracyjnych • Podwójna kontrola • Fizyczne oddzielenie ruchu aplikacyjnego od administracyjnego i monitorującego	• Główne funkcje związane z kluczami asymetrycznymi (podpis, PKI) oraz symetrycznymi (szyfrowanie/deszyfrowanie) • Standardy interfejsu aplikacyjnego: PKCS#11, CNG, Java JCE/JCA • Wymagane certyfikacje: FIPS 140-2/3, CC, eIDAS (QSCD), … • Opcjonalnie: o Silne uwierzytelnianie do funkcji administracyjnych. o Kworum. o Moduł funkcjonalny. o Elementy kryptografii post-kwantowej.

Poznać przeciwnika. Zastosowania i typowa implementacja

- Ochrona kluczy prywatnych w infrastrukturze PKI.
- Ochrona kluczy prywatnych sesji SSL/TLS.
- Rozwiązania elektronicznego podpisywania dokumentów.
- Podpisywanie kodu wykonywalnego i obrazów kontenerów.
- Szyfrowanie baz danych (ochrona klucza głównego).
- Blockchain.
- Systemy zarządzania kartami inteligentnymi (CMS).
- Wsparcie bezpiecznego wytwarzania (*secure manufacturing*) dla IoT i OT.
- Ochrona transakcji płatniczych.



THALES

Audyt

WIKIPEDIA
Wolna encyklopedia

Audyt – niezależna ocena danej organizacji, systemu, procesu, projektu lub produktu.

Przedmiot audytu jest badany pod względem zgodności z określonymi standardami, wzorcami, listami kontrolnymi, przepisami prawa, normami lub przepisami wewnętrznymi organizacji (polityki, procedury).

Przygotowanie i przeprowadzenie audytu

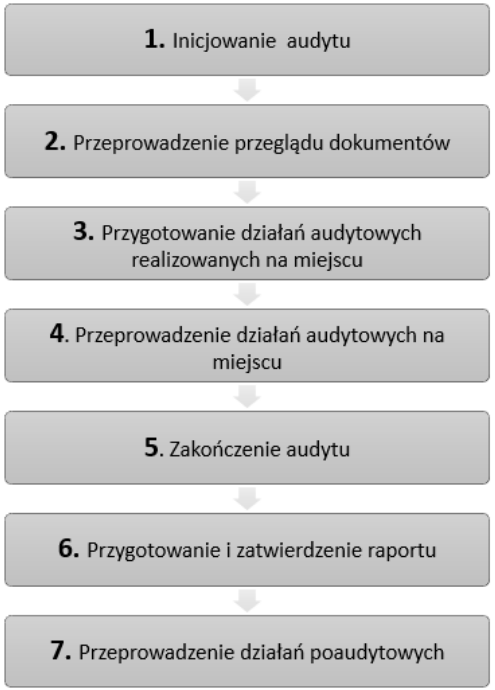
1. Normy i standardy stosowane do przygotowania:

- ISO/IEC 27001, Załącznik A,
- ISO/IEC 27002
- NIST Cybersecurity Framework
- ITIL
- PCI DSS
- Regulacje branżowe, np. KNF
- Regulacje: NIS2, DORA.

2. Elementy przygotowania:

- Określenie celu
- Zdefiniowanie zakresu
- Wybór narzędzi i technik
- Zgromadzenie zespołu audytowego
- Harmonogram prac
- Określenie kanałów komunikacji
- Przygotowanie dokumentacji
- Wstępna ocena ryzyka i plan działań.

3. Etapy przeprowadzania:



A w kwestii audytu co uwzględnić? 1 słowem, wszystko…

THALES

A w kwestii audytu co odróżnia HSM od „szarości”?

- **Przeciętny HSM przechowuje i chroni tzw. *klejnoty koronne* – czyli klucze szyfrujące i rożne poświadczenia**
- **Obszary wykorzystania rozwiązań HSM są z reguły silnie regulowane:**
  - PCI DSS, FIPS, KNF, CC/eIDAS Ustaw o podpisie cyfrowym, …
- **Przeciętny HSM jest dłużej eksploatowany niż inne elementy infrastruktury IT (jak serwery, przełączniki, itp.)**
  - Perspektywa 7-10+ lat
- **HSM to nie „bastion host” – coś co ma wytrzymać wszystkie ataki**
- **Zapominamy, że HSM nie jest doskonały i niezawodny - też może mieć błędy i podatności albo się zepsuć.**

Projekt w audycie

Powinniśmy zapoznać się z założeniami jakie legły u podstaw projektu i wdrożenia

W dalszej części zweryfikować czy zostały zrealizowane i ew. wskazać „czego zabrakło”

- Np. Jeżeli projekt przewidywał uzyskanie zgodności (np. z regulacjami lub certyfikacją) to należy to zweryfikować czy rozwiązanie pracuje w takiej konfiguracji np. „tryb FIPS” czy uwierzytelnianie MFA dla administratorów
- Np. zweryfikować czy w projekcie operacyjnym uwzględniono długi czas eksploatacji urządzeń HSM i perspektywę technologiczną
  - Czy HSM w formie karty PCI Express będzie za 5-6-10 lat dalej do umieszczenia w dostępnych na rynku serwerach?)
  - Rotację kadr (przekazywanie obowiązków i poświadczeń)
  - Utrzymanie kopii zapasowych
  - PQC,

Inne…

Dostawa i przyjęcie

- Często traktowane po macoszemu a mogące mieć wpływ na późniejsze działania – np. przejście audytu PCI czy eIDAS do wydania QSeal
- Wielu producentów umożliwia dostawę w „trybie bezpiecznym”, który pozwala potwierdzić zgodność dostawy z zamówieniem oraz brak naruszenia urządzenia w obszarze fizycznym i logicznym (np. czy pojawił się obcy materiał lub ustawienia)
- Jak u Ciebie wygląda(ła) dostawa i odbiór HSM?
  - Zweryfikowaliście zgodność ilościowo-jakościową z zamówieniem (patrz: projekt)?
  - Sporządziliście z tego protokół podpisany przez obie strony?
  - W razie potrzeby możesz to wykazać przed audytorem (PCI, eIDAS, czy innym)?

1. Bierzemy udział w ceremonii generowania pary kluczy w HSM (zdalnie lub fizycznie), której wynikiem jest plik żądania certyfikacyjnego pkcs#10.
2. Dokonujemy oględzin urządzenia: nazwę, model, nr seryjne, tabliczki znamionowe, plomby itp.
3. Weryfikujemy dokumentację HSM: dowód zakupu, protokół odbioru od dystrybutora, protokół z odbioru urządzenia (plomby itp.), certyfikat QSCD, Common Criteria.

2. Sprawdzamy tozsamosc osoby reprezentującej klienta której zostanie przekazany certyfikat kwalifikowany.

```
lunacm:> stm show

        STM State Flags ->
                Transport Mode:             1


Command Result : No Error

lunacm:>
```

Instalacja

Jak wygląda instalacja urządzenia i zastosowane zabezpieczenia fizyczne?

- Dostęp do serwerowni, dostęp do szafy,…?
- Zabezpieczenie przed kradzieżą i dostęp do samego urządzenia (np. dostęp do portu konsoli)
- Poprawność montażu (szyny i maskownice i klucze), dywersyfikacja źródeł zasilnia, itp.
- Podłączenie interfejsów sieciowych

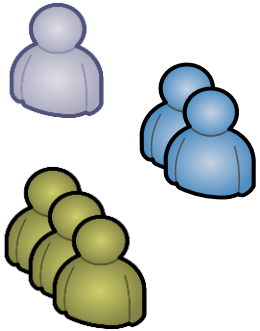
Stacja administracyjna, zdalne zarządzanie…

- Wydzielony komputer z kontrolą dostępu fizycznego…
- Składowanie i przechowywanie elementów pomocniczych (jeżeli takowe występują): karty, tokeny, czytniki, PEDy, itp.
- Czy brak drobnego lementu pomocniczego nie stanowi pojedynczego punktu awarii (np. tylko 1 czytnik dla puli urządzeń)?

Czy sporządzono dokumentację techniczną?

Konfiguracja #1/2

Czy wdrożona konfiguracja odzwierciedla przyjęte założenia (znowu: projekt)?



- Przyjęty podział ról, rodzaj uwierzytelnienia, rozmiary kworum („MzN", „KzN", itp..)
- Polityki haseł, PINów, poświadczeń, blokowania kont, resetowanie poświadczeń dla kont
- Ustawienia zgodne z certyfikacjami: FIPS, PCI czy CC/eIDAS. Wielu chce niewielu ma…
- Wysoka dostępność, nadmiarowość,
- Konfiguracja sieciowa m.in.: odpowiednie zabezpieczanie dostępu sieciowego do HSM, separacja ruchu aplikacyjnego od zarządzania i monitoringu, itp.), połączenie z systemem monitorowania (SNMP, syslog, inne)

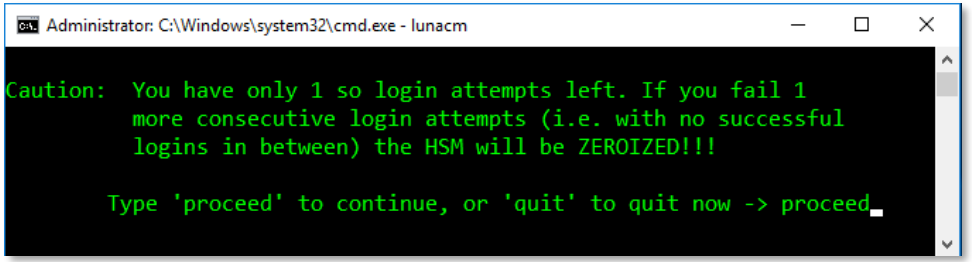
Czy wdrożenie uwzględnia zabezpieczenie przed utratą kworum lub poświadczeń?

- Rotacja, utrata kadr
- Zwykłego zgubienia lub zapomnienia
- Katastrofa…

Konfiguracja #2/2

Czy dokładnie wiemy w jakiej sytuacji HSM dokona zniszczenia materiału (*tamper*) w celu jego zabezpieczenia?

- Uwzględnione w procedurach operacyjnych?
- Ujęte w szkoleniu operatorów i administratorów?



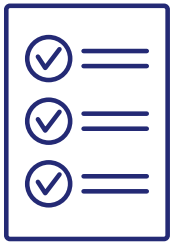
Niewygodne pytanie: Czy sporządzono dokumentację techniczną? Kopię konfiguracji?

- Przez tydzień jeszcze wszystko pamiętamy ale po kwartale czy pół roku trudno przypomnieć sobie co zostało zrobione..
- Czy dokumentacja jest aktualna?

Eksploatacja i utrzymanie #1/3

Procedury obsługi (czy w ogóle istnieją?):

- Bieżącej (w tym weryfikowania np. HA i wykonywania kopii zapasowej)
- Odtwarzania po awarii (DR). Kiedy ostatnio była testowana?
- Przekazywania obowiązków (i poświadczeń). *Staszek odchodzi, przychodzi Janusz…*



Procedura okresowej weryfikacji poświadczeń, haseł, PINów, kluczy, kart, tokenów wykorzystywanych do obsługi HSM

- Warto aby takowa była połączona z procedurą wykonywania kopii zapasowej gdyż to właśnie wtedy potrzebujemy poświadczeń, kart, PIN-ów itp..

Polityka i procedura zgłaszania zgubienia/zapomnienia: haseł, PINów, kluczy, kart, tokenów wykorzystywanych do obsługi HSM?

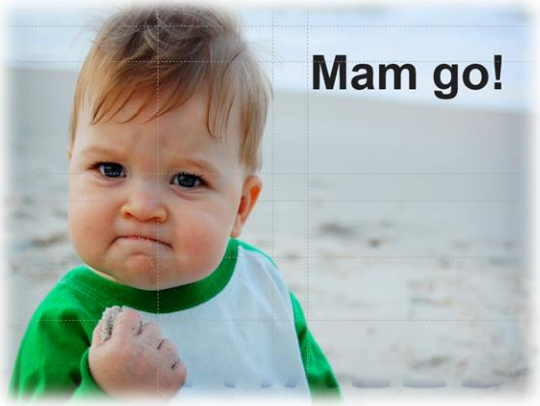
- Operatorzy powinni być uczulenie na takie przypadki i zgłaszać je natychmiast do administratorów

THALES

Eksploatacja i utrzymanie #2/3

Kopia zapasowa – czy naprawdę ją masz?

- Jaką strategię wykonywania kopii materiału kryptograficznego przyjęto?
  - Rekomendacja1: po każdej istotnej zmianie (np. po generacji nowych kluczy, zmianie polityk)
  - Rekomendacja2: raz na pół roku
- Kiedy ostatnio wykonano kopię zapasową? Czy wszystkie wymagane poświadczenia i urządzenia pomocnicze były dostępne?
- Kiedy ostatnio próbowano odtworzyć kopię zapasową? Udało się?
- Gdzie jest składowana i jak zabezpieczona kopia zapasowa materiału kryptograficznego?
- Jak wygląd procedura operacyjna odtwarzania kopii materiału?
- Itd., itp.



Eksploatacja i utrzymanie #3/3

Kiedy ostatnio dokonano wizualnej inspekcji urządzenia i elementów pomocniczych?

- Weryfikacja zabezpieczeń fizycznych (serwerownia, szafa, urządzenie, …)
- Sprawdzenia stan baterii wewnętrznej, wentylatorów, zasilaczy, …
- Stan podłączania kabli sieciowych i zasilania

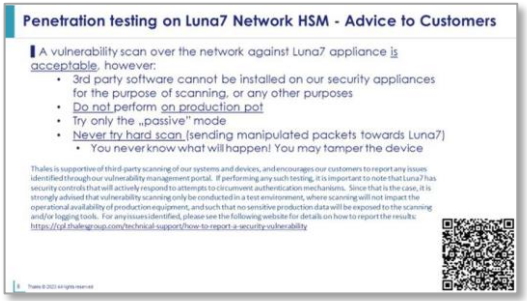
netHSMTamperBattery1	R	DisplayString	Voltage of Tamper Battery 1
netHSMTamperBattery2	R	DisplayString	Voltage of Tamper Battery 2

Aktualizacja rozwiązania

- Czy posiadamy aktywny dostęp do pomocy technicznej producenta (zgłaszanie problemów, pobieranie aktualizacji, newslettery, itp.)?
- Kiedy ostatnio sprawdzano dostępne aktualizacje dla HSM oraz dla urządzeń pomocniczych (oprogramowanie klienta, firmware, itd.)
- Jakie aktualizacje zostały zastosowane? Czy wykonano kopie zapasową po aktualizacji?

Przegląd podatności (tzw. skan „po sieci”)?

- Czy skan jest wykonywany na środowisku produkcyjnym?
  - Czy takie postępowanie rekomenduje producent?
  - Czy mamy świadomość ew. konsekwencji?
- Czy i jak intepretowany i wykorzystywany jest raport z przeglądu?



Przykład szczegółowej listy sprawdzania

Przekładowa lista sprawdzania dla konfiguracji HSM sieciowego Luna 7 (bez modułu FM) pod kątem zgodność z CC dla zastosowania jako QSCD/QSealCD:

Wersja 1.1, data: 2023-06-01, w. językowa: PL

Opracowano na podstawie: "Thales Luna K7(+) Cryptographic Module: COMMON CRITERIA USER GUIDANCE - PART 1, 007-013968-001, Rev. H, 6 May 2022"

Lp.	Opis wymagania	Pytania	Zakres odp.	Dowód audytowy	U.
1.	Spełnienie wymagań wstępnych	Jakie urządzenie zostało zamówione? Jakie urządzenie zostało przyjęte?	Opis	Kopia zamówienia, Raport z przyjęcia dostawy Zdjęcia plomb na opakowaniu i obudowie	
2.	Weryfikacja zatwierdzonej wersji sprzętu	Przedstaw jak zweryfikowano, że otrzymano zatwierdzony wariant sprzętu przez CC (TOE) i oprogramowania (*firmware* i *appliance software*)	Opis	Zdjęcie etykiety numery partii (PN) z urządzenia oraz wynik polecenia `Lunash> hsm show`	
3.	Weryfikacja montażu fizycznego	Opisz jak i gdzie urządzenia zostało zamontowane? Jak zabezpieczono dostęp fizyczny do urządzeń	Opis	Zdjęcia z montażu w szafie 19". Zdjęcie szafy w DC.	
4.	Tryb transportowy	Czy z urządzeniem były dostarczone kody producenta do wyjścia z trybu	Tak/Nie	Email lub PDF z kodami STM od producenta	
5.	Wyjście z trybu transportowego	Jak przeprowadzon wyjście z trybu transportowego? Czy kod wyjścia został poprawnie zweryfikowany	Opis	Raport `Lunash> stm show`	
6.	Minimalny zestaw ról dla zgodności CC	Czy włączono i zainicjowano role HSM SO i Audit User?	Tak/Nie	Lista kont użytkowników na urządzenie (z uwidocznieniem stanu)	
7.	Zgodność ustawienia polityk HSM	Jaki jest stan polityk HSM?: HSM Policy (43) Allow low-level math acceleration must be set to **true**; HSM Policy (46) Disable Decommission must be set to **false**; HSM Policy (52) Restrict FM Privilege Level must be set to **true**	Opis	Wynik polecenia: `Lunash> hsm showpolicies`	
8.	Zgodność ustawienia polityk partycji	Jaki jest stan polityk partycji do przechowania QSCD/QSealCD?: Partition Policy (15) Ignore failed challenge response must be set to **false**; Partition Policy (40) Require Per-Key Authorization Data must be set to **true**; and Partition Policy (41) Partition Version must be **1**.	Opis	Wynik polecenia: `lunacm:> partition showpolicies -verbose`	
9.	Zainicjowanie logu audytu bezpieczeństwa	Opisz jak został skonfigurowany log audytu bezpieczeństwa? Czy zdarzenia docierają do systemu zewnętrznego	Opis	Wynik polecenia: `Lunash> audit show` Kopia fragmentu logu pozyskana z	

Z grubsza, „To by było na tyle”

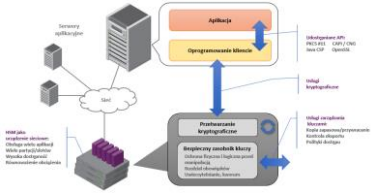
NARODOWE CENTRUM KULTURY

Dawno, dawno temu, jakoś tak pod koniec XX w., aktor, satyryk i radiowiec co się zowie Jan Tadeusz Stanisławski pozwolił sobie - na antenie - na żart językowy: zakończył swój monolog słowami „To by było na tyle”. Była to kontaminacja (świadoma oczywiście) dwóch formułek kończących: „to byłoby wszystko” i „to tyle na dziś”. Nowe sformułowanie, żartobliwe a krągłe, spodobało się publiczności, więc

CryptoPanel

podsumowanie

Coś na wynos



- **Przedstawione zagadnienia związane z audytem urządzeń HSM nie obejmują wszystkich możliwych obszarów.**
- **Wskazaliśmy te nieoczywiste i typowe związane z charakterystyką rozwiązań HSM.**
- **Rozwiązania HSM pełnią kluczową rolę w ochronie zasobów kryptograficznych środowisk IT.**
  - Bezpieczeństwo HSM-ów potwierdzają certyfikacje (FIPS, CC, PCI, NITES, …)
  - W praktyce rozwiązanie HSM może zostać wdrożone i eksploatowane w sposób, który nie zapewni żadnej ochrony, a nawet spowoduje zagrożenie utraty danych.
- **Sprzętowe moduły kryptograficzne należy poddawać regularnym audytom bezpieczeństwa ale z *uwzględnieniem ich specyfiki*, konkretnego przeznaczenia a nawet konkretnego wdrożenia.**
- **Obszary audytu powinny uwzględniać możliwie szeroki kontekst: projekt i założenia, dostawę, instalację wraz z konfigurację oraz eksploatację.**

THALES

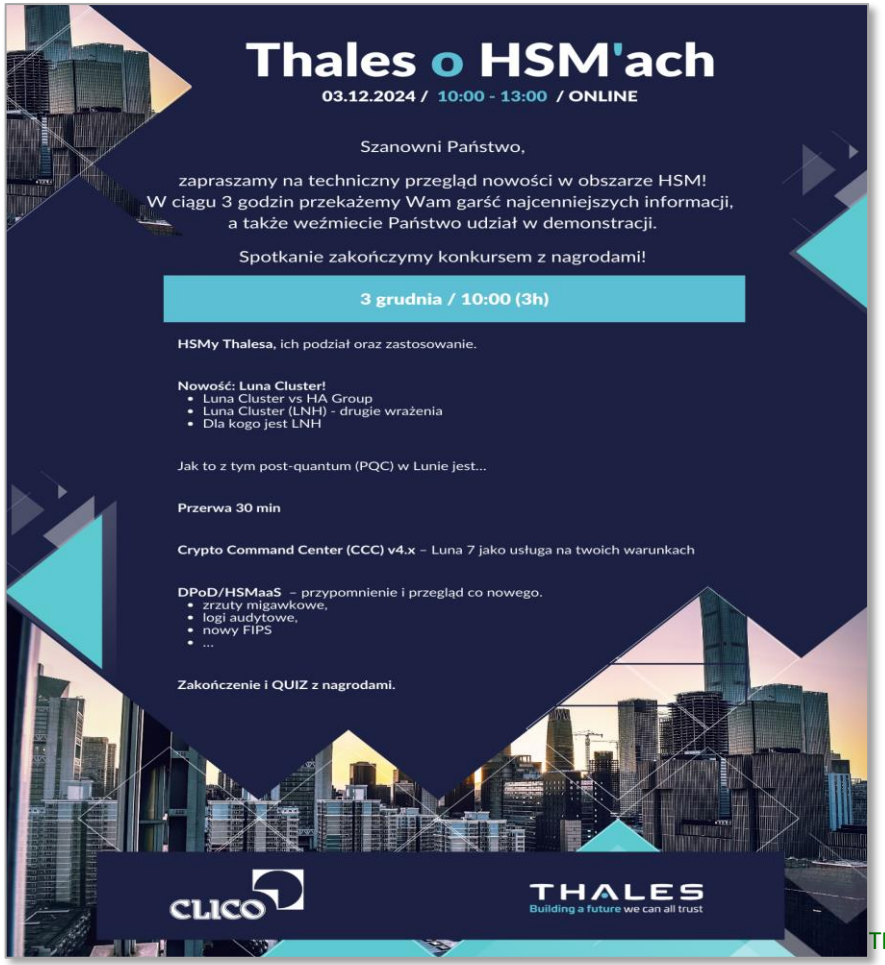
Czego potrzebujemy aby przeprowadzić dobry i skuteczny audyt?

- **Aby audyt został skutecznie przeprowadzony potrzebna jest współpraca audytowany-audytor**
  - Okopanie się na swoich stanowiskach bez próby zrozumienia drugiej strony nie doprowadzi do konsensusu i wypracowania kolejnych kroków.
- **Opracowane i wykonywane procedury utrzymania codziennego oraz DR ułatwią audyt**
- **Thales nie przeprowadza audytów własnych rozwiązań**
  - Audyt to niezależna opinia!
- **Ale dostarczamy sprawdzenia *stanu zdrowia***

BOM:

- **2x**
- **PRO SERVICES, ADD-ON, HSM, HEALTH CHECK, SERVICEPACK 4 190,00 020-000308-001-000**

I jeszcze zaproszenie…



https://partner.clico.pl/zasoby/thales-e-security/webinarium-thales-o-hsmach-03.12.2024

THALES

CryptoPanel

CryptoPanel

A teraz quiz z upominkami