Ostatni gasi światło - cyber nie-bezpieczeństwo systemów SCADA/ICS od elektrowni jądrowych po platformy wiertnicze

Aleksander Gorkowienko
Menedżer zespołu testowania bezpieczeństwa cybernetycznego

Bezpieczeństwo ICS/SCADA – szybki przegląd

Specyfika systemów ICS/SCADA?

- Wyjątkowo **długa żywotność** (czasami ponad 20 lat) w połączeniu z integracją z nowszymi komponentami.
- Systemy **bardzo zróżnicowane** technicznie (sprzęt i oprogramowanie od różnych dostawców).
- Bardzo złożone systemy które najczęściej **nie są projektowane z myślą o bezpieczeństwie.**
- Systemy ICS/SCADA najczęściej są **zarządzane przez inżynierów**, a nie IT.
- **Specjalistyczne mechanizmy i protokoły** komunikacyjne, w tym wiele historycznie używanych starych protokołów ICS – które teraz są "w opakowaniu" TCP lub UDP.
- "**Bezpieczeństwo przez ukrywanie**" *(security by obscurity)* w rzeczywistości oznacza brak bezpieczeństwa.
- Totalny **mit o infrastrukturze "kompletnie odizolowanej“** *(air gapped)*.

Mit systemów “kompletnie odizolowanych”

Stacja robocza 1

Środowisko 1

Infrastruktura odizolowana:
nie ma żadnego połączenia pomiędzy środowiskiem 1 oraz 2

Stacja robocza 2

“Odizolowane” Środowisko 2

Mit systemów “kompletnie odizolowanych”

Stacja robocza 1

Środowisko 1

PROMIENIOWANIE ELECTROMAGNETYCZNE

- AirHopper exploit: manipulowanie emisją elektromagnetyczną z ekranów komputerowych lub kabli ekranowych (stają się one swego rodzaju nadajnikiem radiowym)
- Sygnały magnetyczne o niskiej częstotliwości generowane przez rdzenie procesora komputera
- Ukryte sygnały generowane poprzez pozycjonowanie głowic magnetycznych dysków twardych (wykrywane przez zwykły telefon komórkowy).

PROMIENIOWANIE OPTYCZNE

- Eksfiltracja danych przez migające diody LED klawiatury komputera, diody LED routera lub przełącznika sieciowego.
- Eksfiltracja danych poprzez szybko wyświetlane (migające) obrazy o niskim kontraście na ekranie komputera
- Wykorzystanie diod IR w kamerach bezpieczeństwa do transmisji danych

PROMIENIOWANIE CIEPLNE

- Modulowane ciepło generowane przez procesor CPU/GPU komputera jest odbierane przez zewnętrzny czujnik temperatury.

FALE AKUSTYCZNE

- Eksfiltracja danych za pomocą niesłyszalnych, ultradźwięków
- Dane zakodowane przez szum celowo generowany przez wentylator chłodzący komputer
- Słuchawki lub głośniki zamienione w mikrofon (technika zmiany przeznaczenia gniazd w komputerze stacjonarnym)
- Sygnały akustyczne emitowane przez ruchome ramię dysku twardego.

Stacja robocza 2

“Odizolowane” Środowisko 2

Hakowania ciąg dalszy: nowa generacja systemów SCADA – stare problemy z bezpieczeństwem

- **Atak na łańcuch dostaw** (najpierw hakowanie dostawców ICS następnie atakowanie głównego celu).
- **Przestarzałe laptopy i oprogramowanie** używane przez techników i inżynierów w terenie.
- Atak na **bezzałogowe obiekty w terenie.**
- **Rozrzucanie pendrive-ów USB** ze złośliwym oprogramowaniem (tak, stary, dobry sposób z czasów Stuxneta nadal działa).
- **Aplikacje webowe** do kontroli zdalnej z dostępem przez Internet są coraz popularniejsze.
- **Urządzenia mobilne** zaczynają być coraz częściej używane także w świecie ICS.
- Systemy SCADA mają **webowe interfejsy API**.

Przykład z życia wzięty: testujemy bezpieczeństwo FPSO

FPSO – a co to w ogóle jest?

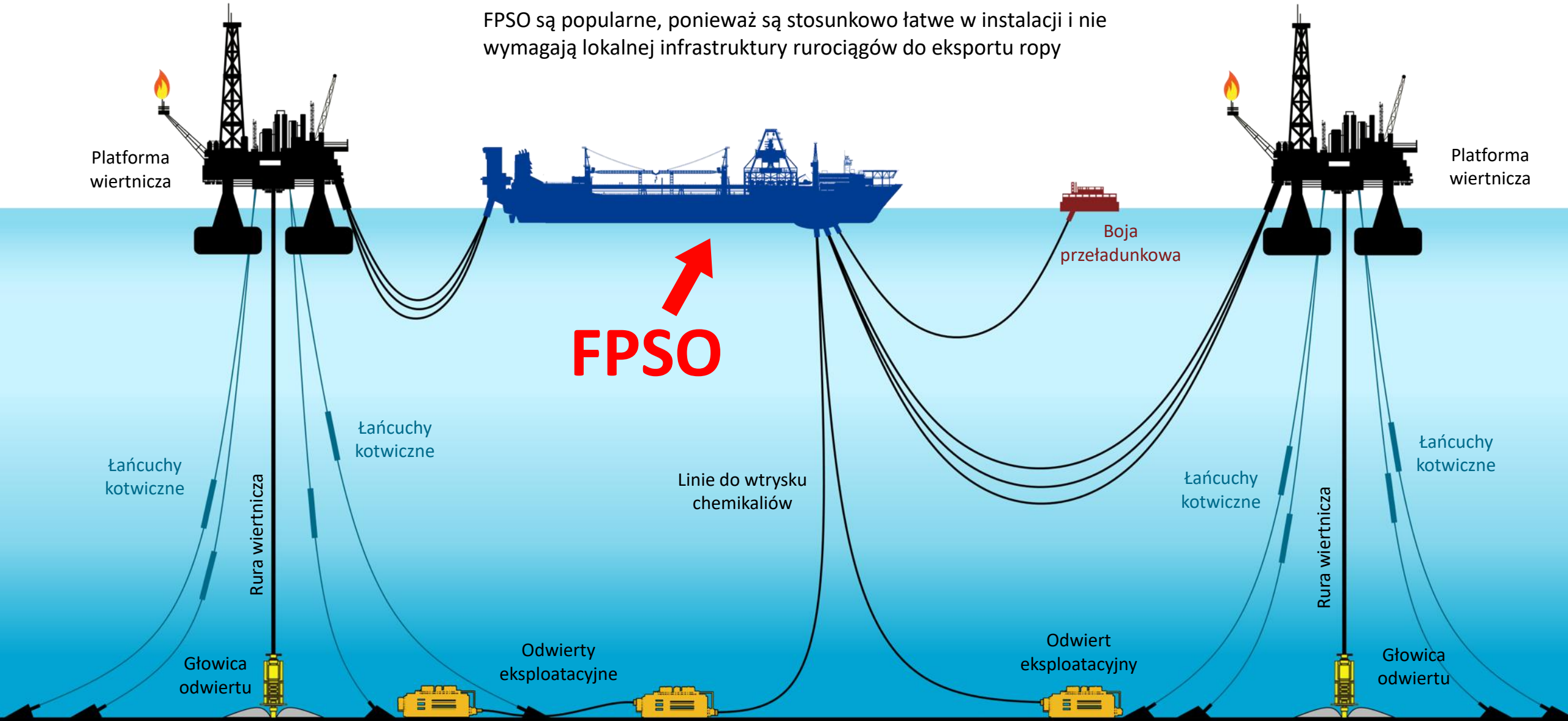
Przykładowy statek FPSO

FPSO (ang. *Floating Production, Storage and Offloading*, czyli: „pływający punkt produkcji, przechowywania i załadunku”) – jednostka pływająca, której zadaniem jest wydobywanie, wstępne oczyszczenie, przechowywanie oraz przeładunek ropy naftowej i/lub gazu ze złóż podmorskich.

FPSO przeznaczony jest do odbioru węglowodorów wydobytych samodzielnie lub z pobliskich platform, ich przerobu i magazynowania do czasu przeładunku na tankowiec (rzadziej: transportowany rurociągiem).

FPSO – a co to w ogóle jest?

FPSO są popularne, ponieważ są stosunkowo łatwe w instalacji i nie wymagają lokalnej infrastruktury rurociągów do eksportu ropy



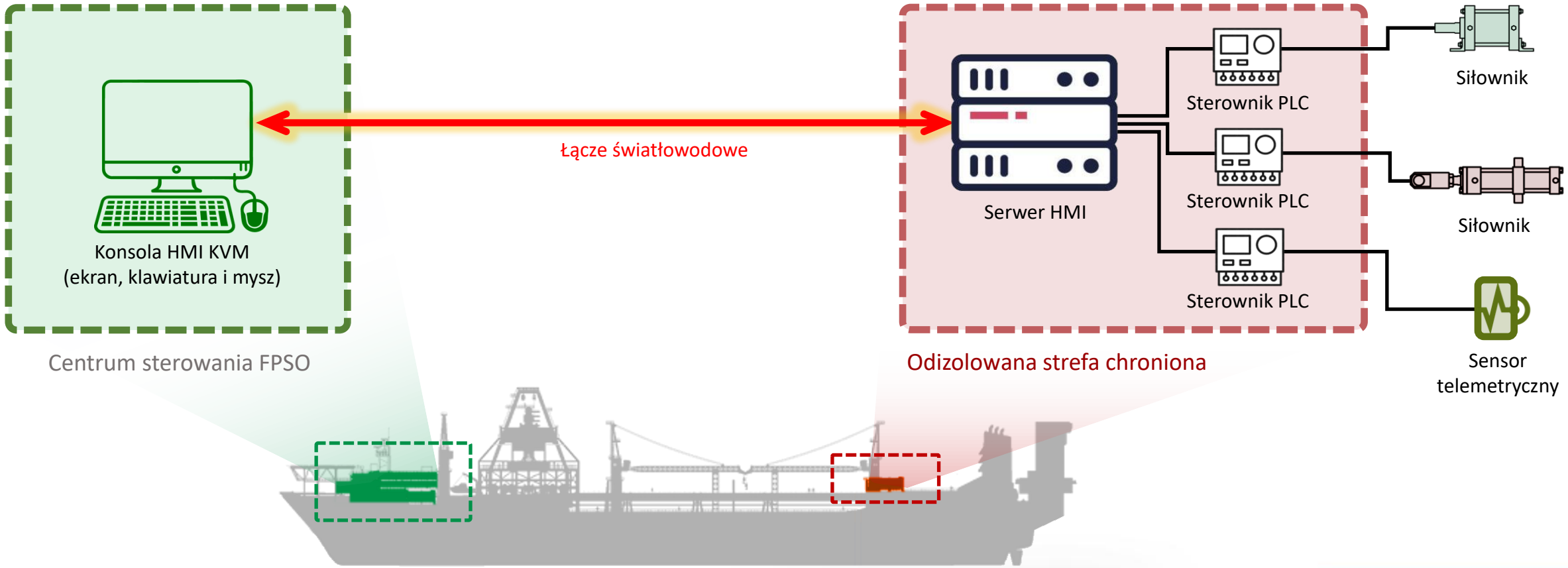
Co znaleźliśmy podczas testów bezpieczeństwa

- Możliwość nieautoryzowanego dwukierunkowego transferu danych i plików binarnych z/do izolowanego *(air gapped)* serwera HMI
- Nieautoryzowany dostęp do systemów sterowania krytycznymi procesami przemysłowymi oraz eskalacja uprawnień.
- Sterowniki PLC podatne na atak typu Man-in-the-Middle (MITM)
- Serwer NTP podatny na atak Man-in-the-Middle (MITM)
- Usługi Windows mogą być rekonfigurowane przez użytkowników którzy nie mają uprawnień administratora [serwer HMI]
- Nieautoryzowany dostęp do plików programów i usług [serwer HMI]
- Niepotrzebne otwarte porty [podsieć stacji roboczej HMI]
- Słabe mechanizmy szyfrowania w warstwie transportowej

Znaleziono ponad 25 różnych błędów bezpieczeństwa!

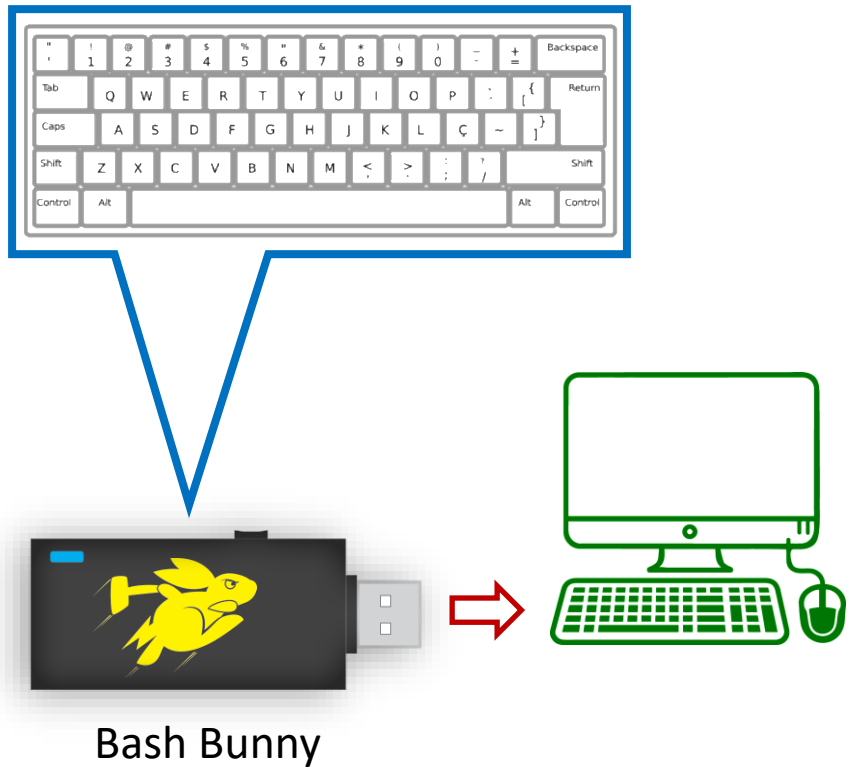
Na ile rzeczywiście “izolowany” jest ten serwer?

- Dostęp do serwera HMI [teoretycznie] można uzyskać wyłącznie przez przełącznik KVM
- Architekci systemu założyli, że *nie ma absolutnie żadnej możliwości* przesłania czegokolwiek na serwer przez KVM. *(Czy aby na pewno?...)*



Transfer czegokolwiek na serwer HMI i z powrotem

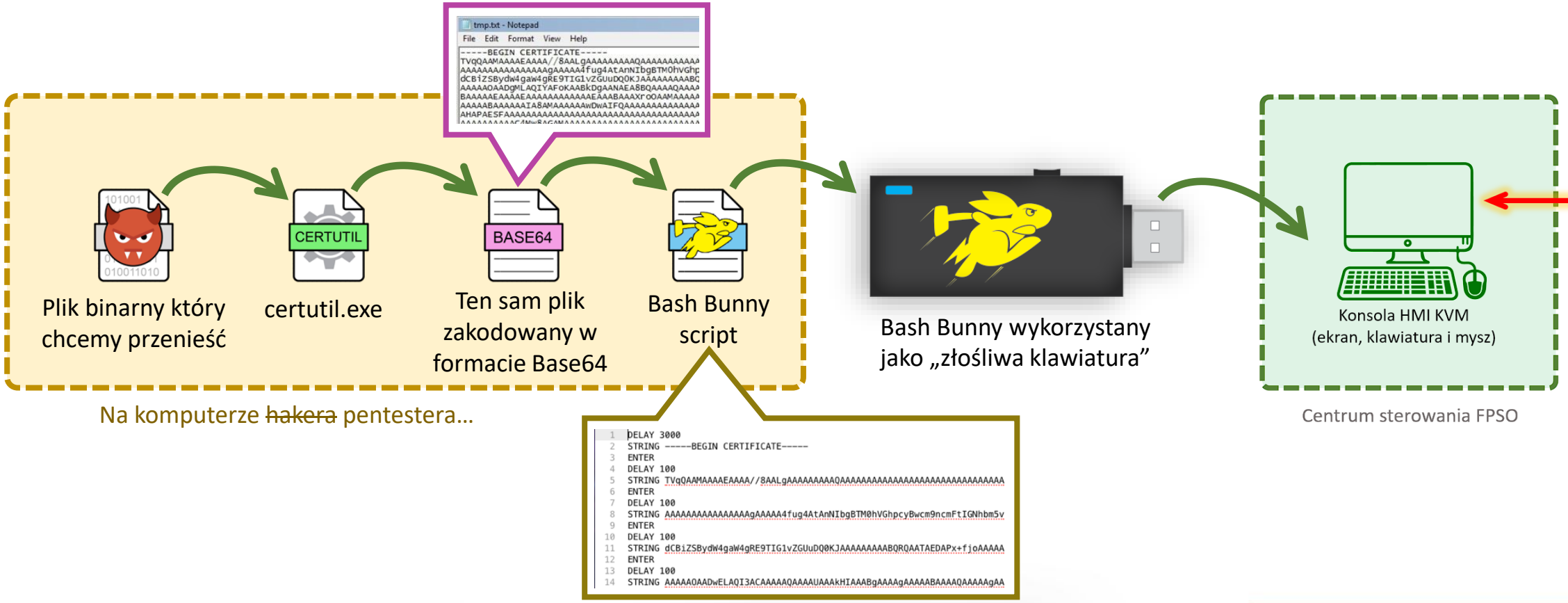
- Architekci systemu założyli, że jeżeli oprogramowanie na serwerze HMI będzie działać jako „kiosk” bez dostępu do systemu operacyjnego, to będzie bezpieczne. *Wcale tak nie było.* Uruchomienie konsoli zajęło *mniej jak minutę*.
- Zidentyfikowaliśmy system operacyjny: **Windows 7.** Żadnych uaktualnień i ani śladu AV!
- Na serwerze znaleziono narzędzie **certutil.exe** (plik z domyślnej instalacji Windows) i plik **notepad.exe**. Tylko tego nam było trzeba!
- Zamiast standardowej klawiatury DELL umieszczonej na białej liście KVM podłączyliśmy urządzenie **Bash Bunny** które dokładnie imitowało identyfikator urządzenia USB.
- Nasz „szkodliwy” plik [binarny] został przesłany na serwer *jako tekst* i potem przywrócony do postaci binarnej przy użyciu certutil.exe



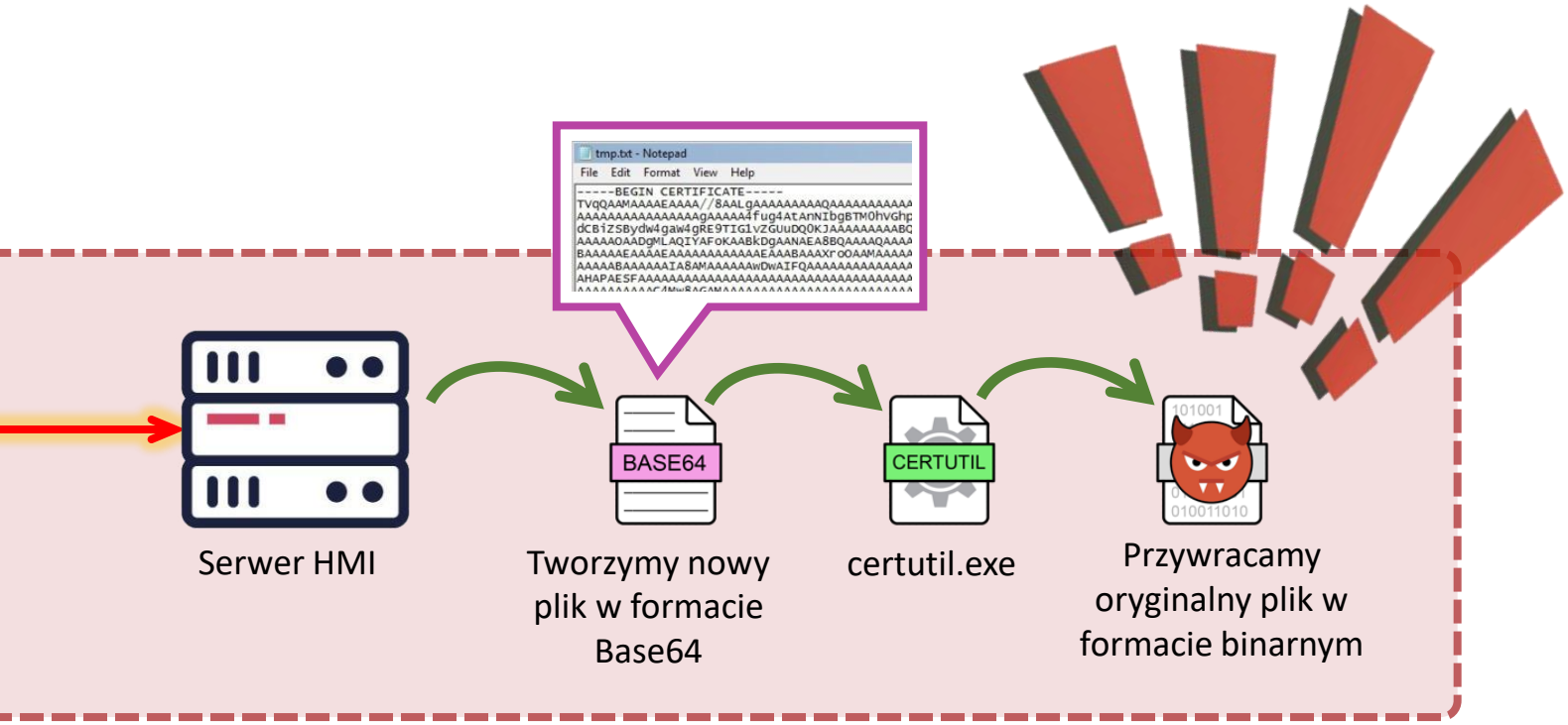
Bash Bunny

Transfer czegokolwiek na serwer HMI i z powrotem

- Na początku przekonwertowaliśmy przykładowy plik binarny (np. złośliwe oprogramowanie) na zestaw instrukcji dla Bash Bunny.
- Bash Bunny został podłączony do przełącznika KVM zamiast klawiatury.
- Bash Bunny symulował naciśnięcia klawiszy i w ten sposób skopiowaliśmy plik zakodowany w formacie Base64 do pliku tekstowego na serwerze HMI.



Transfer czegokolwiek na serwer HMI i z powrotem

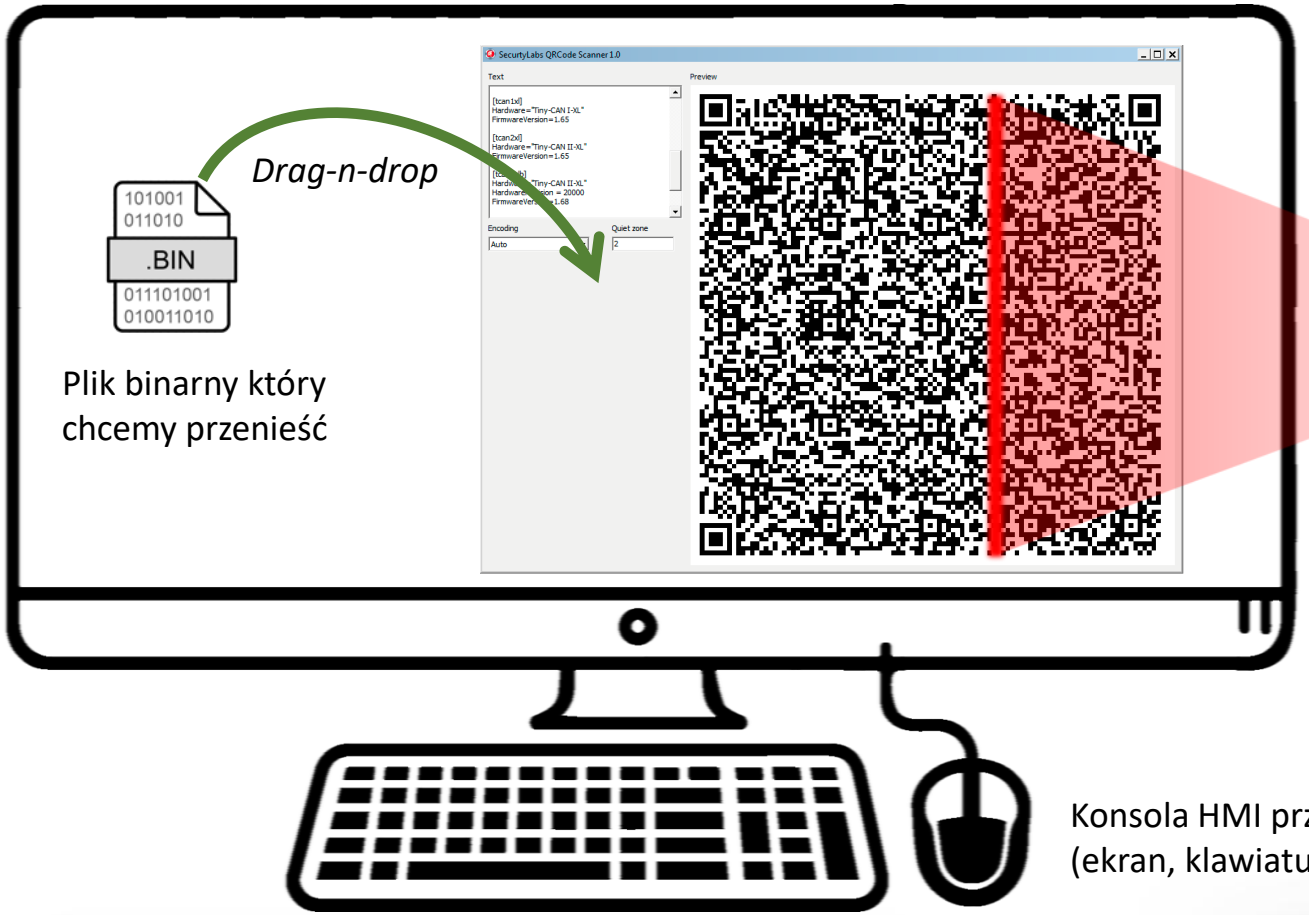


… tym czasem na serwerze HMI…

- Ponownie wykorzystaliśmy narzędzie **certutil.exe**, tym razem już na serwerze HMI. Przekonwertowaliśmy plik zakodowany w formacie Base64 do oryginalnej postaci binarnej.
- No i teraz możemy uruchomić nasz plik binarny na serwerze HMI bez ograniczeń!

A teraz kopiujemy dane z powrotem z serwera HMI

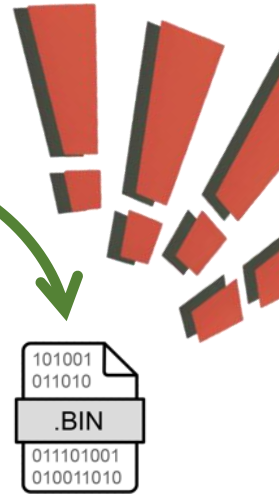
- Krok 1: Przesyłamy własne narzędzie (plik .exe) na serwer HMI
- Krok 2: Uruchamiamy narzędzie, przeciągamy na niego dowolny plik – zawartość pliku zostaje przekształcona w kod QR!
- Krok 3: Odczytujemy kod QR przy pomocy aplikacji mobilnej.



Plik binarny który chcemy przenieść

Konsola HMI przełącznika KVM (ekran, klawiatura i mysz)

Kod QR odczytywany z ekranu KVM przy pomocy aplikacji mobilnej i konwertowany z powrotem do postaci oryginalnej.



Mamy skopiowany nasz plik!

Usprawniamy bezpieczeństwo ICS

Zacznijmy od kardynalnej zmiany podejścia

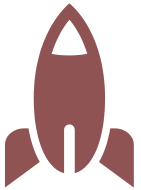
- Bezpieczeństwo cybernetyczne to **proces ciągły**, podczas którego organizacja nieustannie uczy się i ulepsza procesy biznesowe, technologiczne oraz poziom bezpieczeństwa.
- **Bezpieczeństwo to proces**, a nie produkt!

Ludzie

Człowiek wciąż pozostaje jednym z najsłabszych ogniw łańcucha bezpieczeństwa. Zbuduj solidny program szkoleniowy w zakresie świadomości bezpieczeństwa cybernetycznego.

Procesy

Zapewnij wybór i wdrożenie najlepszych praktyk i powiązanych ram zarządzania. Regularne rutynowe audyty procesów powinny być standardową częścią ciągłego ulepszenia *(continuous improvement)* procesów biznesowych i technologicznych.

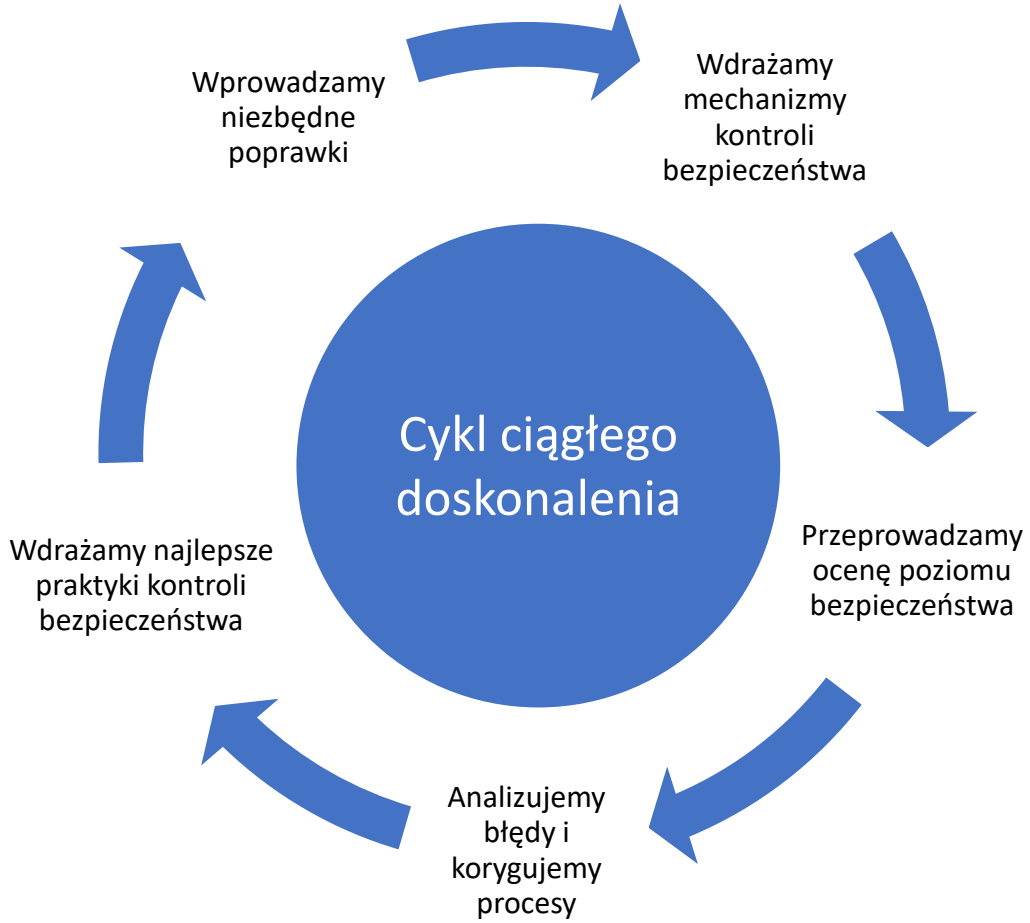


Technologie

Zwiększająca się częstotliwość ataków i rosnący poziom wyrafinowania oznaczają, że niezbędne jest ciągłe monitorowanie zmian technologicznych i “dotrzymanie kroku” w obszarze przeciwdziałań atakom.

Zacznijmy od kardynalnej zmiany podejścia

- Bezpieczeństwo cybernetyczne to **proces ciągły**, podczas którego organizacja nieustannie uczy się i ulepsza procesy biznesowe, technologiczne oraz poziom bezpieczeństwa.
- **Bezpieczeństwo to proces**, a nie produkt!



Zwiększamy poziom bezpieczeństwa ICS/SCADA

1. Zacznij od **skatalogowania** wszystkich swoich zasobów IT i OT
2. Zidentyfikuj i zaznacz **systemy krytyczne**
3. Zastanów się jak **zmniejszyć powierzchnię ataku**

Nigdy nie „zakładaj z góry” że jesteś bezpieczny.
Zawsze przetestuj. A potem przetestuj jeszcze raz!

SYSTEMY PRZEMYSŁOWE

Bądźmy w kontakcie

Aleksander Gorkowienko
Menedżer zespołu testowania bezpieczeństwa cybernetycznego
m: +44 (0) 20 3653 1234
e: aleksander.gorkowienko@riskcrew.com

Risk Crew Limited
5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom