



“Progetto HP per l’Emissione del Permesso di Soggiorno Elettronico (PSE): metodologie, tool ed esperienza per un’analisi efficace del rischio ICT”

Cliente: Ministero dell’Interno,
Direzione Centrale Anticrimine,
Polizia Scientifica.

Ing. Antonino Lucantonio
ISO/IEC 27001 ICT Security Lead Auditor, PMP®
HomeLand Security Solutions, HP



Il Progetto sul Permesso di Soggiorno Elettronico per Criminalpol



- Il Permesso di Soggiorno Elettronico e' la nuova forma di Permesso di Soggiorno, costituita da una '**smart card**' dotata di micorchip a disposizione dell'extracomunitario, che certifica la validita' del soggiorno in Italia.
- Oltre ai dati anagrafici del possessore, la 'smart card' contiene anche **i dati biometrici quali la foto (in chiaro e nel chip) e l'impronta digitale (il template).**
- **HP** e' la societa' **mandataria** del progetto per il Ministero dell'Interno, Criminalpol, insieme a Finsiel e Siemens Informatica, entrambe mandanti.
- L'**emissione** del Permesso di Soggiorno coinvolge anche **altri attori** quali ad esempio **l'Istituto Poligrafico e Zecca dello Stato**, le **Poste**, altri dipartimenti interni al Ministero dell'Interno, quali le **Questure** ed i **Commissariati**

La metodologia HP

- Condurre un' **analisi** del rischio significa **identificare** e **quantificare tutti i rischi** associati alla sicurezza di un sistema informativo.
- **Gestire** il rischio e' la fase successiva che va dalla **definizione** delle **contromisure** alla relativa **attuazione, controllo** e supervisione.
- La misura del rischio e' funzione di:
 - Valore dell'oggetto dell'analisi, **per il cliente**
 - Valore delle minacce, **per il cliente**
 - Valore delle vulnerabilita' **per il cliente**
- La qualificazione e la quantificazione del rischio, condotte **con il cliente**, portano alla individuazione delle opportune contromisure atte a mitigare il rischio stesso

La metodologia HP

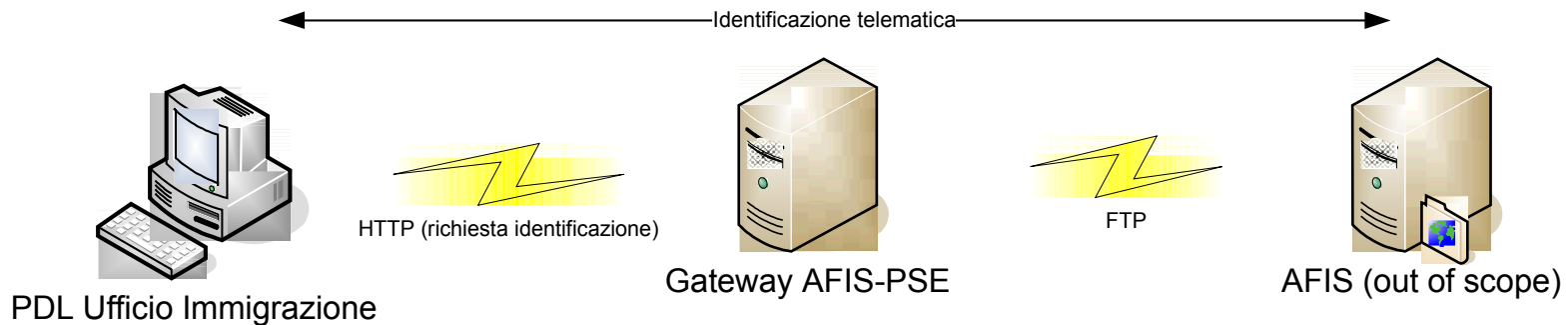
- Prevede la individuazione dei **processi** chiave di comunicazione o elaborazione delle informazioni
- Prevede la definizione di un **modello** e di un **contesto**, in cui operare l'analisi del rischio
- Prevede l'uso di un **tool e di un metodo accreditati** di supporto per l'analisi del rischio

I processi chiave su PSE

Sono stati identificati 6 processi chiave:

1. **Identificazione**: prevede la verifica dei dati anagrafici e biometrici dell'extracomunitario
2. **Comunicazione con altri SI** : prevede l'allineamento e la comunicazione dei dati con altri SI del Ministero
3. **Emissione**: prevede tutte le attività a valle dell'autorizzazione : dalla generazione del certificato digitale fino alla richiesta di produzione ad IPZS
4. **Sospensione, Revoca, PS**: prevede quanto legato alla manipolazione dei certificati digitali
5. **Attivazione PSE**: prevede quanto legato alla manipolazione dei certificati digitali
6. **Profilazione utenze** delle Questure e dei Commissariati, ovvero degli operatori che lavoreranno sulla soluzione PSE

Esempi di processo e modello del PSE



Data Asset: Data_Profilo Utenze Que/Com
End User Service: EUS_Profilazione utenze

```

Data_Profilo Utenze Que/Com
3
  ÄÄ EUS_Profilazione utenze -- Web Browsing
  3
    ÄÄ HW_PDL_Amm. Locale Utenze -- Workstation, Fixed Location Intelligent Workstation
    3
      ÄÄ HW_PDL_Amm. Super User CED -- Workstation, Fixed Location Intelligent Workstation
      3 3
        ÄÄ Sala CED -- Room
        3 3
          ÄÄ Palazzina CED -- Building
          3 3
            ÄÄ PS via Tuscolana -- Site
            3 3
              ÄÄ Ministero Interno -- Organisation
              3
                ÄÄ HW_SRV_Gw AFIS-PSE -- Host, File Server; Host, Application Server; Host, Database Server
                3
                  ÄÄ Sala CED -- Room
                  3
                    ÄÄ Palazzina CED -- Building
                    3
                      ÄÄ PS via Tuscolana -- Site
                      3
                        ÄÄ Ministero Interno -- Organisation
                    
```

Il tool ed il metodo utilizzati

- CRAMM (CRAMM Risk Analysis and Management Method) e' stato realizzato, a partire dal **1985**, per le national security authorities degli **UK**
- CRAMM permette di condurre una **risk analysis completa** sull'intero sistema ICT, oltre che di identificare i **requisiti di sicurezza** e le possibili **soluzioni**.
- CRAMM e' diviso in **due parti**:
 - Il **metodo** CRAMM che fornisce una **guida** nel condurre l'**assessment** del rischio e le **review successive**
 - Il **tool** di supporto costituito dal **software** che permette di **impostare e registrare i dati** della review

Applicazione di CRAMM

- E' possibile modellare l'asset in termini di:
 - **Data Asset**, ovvero le informazioni chiave soggette ad analisi
 - **End User Services** ovvero le modalita' di comunicazione
 - **Physical Assets**, ovvero l'hardware con le funzioni previste
 - **Locations**, ovvero il sito, la palazzina e la sala che ospitano gli asset fisici
 - **Software Applications**, ovvero le applicazioni che supportano la logica del processo
- E' possibile seguire un workflow standard di analisi
 - Quantificazione degli **impatti** sugli asset in termini di **confidenzialita', integrita', disponibilita'**
 - Valutazione delle **minacce**
 - Valutazione delle **vulnerabilita'**
- Risultato dell'analisi e' la **misura del rischio**

CRAMM nel contesto del PSE

– Identificati

- 6 Data Asset
- 6 End User Service
- 2 Application software
- 7 Physical asset

Per un totale di **6 modelli di asset;**

– Quantificati gli impatti sui 6 modelli in base a

- Confidenzialita', distruzione, disponibilita', modifica

– Applicate **30** tipologie di minacce e vulnerabilita'

- Da Masquerading of user identity
-
-
- A Terrorism



CRAMM nel contesto del PSE

- L'analisi del rischio dal punto di vista del **cliente**: "la sensazione di un **processo oscuro**, forse **inutile** che, via via che si susseguivano le interviste, e' diventato sempre piu' **chiaro**, utile ed **esaustivo**, fonte di criticita' non ipotizzate o immaginate sino a quel momento"
- Quattro cicli di incontri e interviste con attori interni ed esterni diversi:
 - La **comprensione** dell'importanza **dell'analisi del rischio** → **prendere coscienza** delle fasi dell'analisi
 - La **modellizzazione** dell'asset → la validazione del cliente grazie alla **conoscenza dei processi**
 - Le interviste sull'impatto → il **valore dell'asset per il cliente**
 - Le interviste sulle **minacce e le vulnerabilita'** → **la scoperta** di nuove e possibili minacce; le **assunzioni** e le **informazioni** su minacce e vulnerabilita' note al cliente, grazie a **esperienze** in contesti analoghi

CRAMM nel contesto del PSE

- L'analisi del rischio dal punto di vista del **consulente**:
- “la capacità’ di **dominare** un’analisi **‘approfondita’** per non perdere la **completezza** dell’analisi,
- mediata dal bisogno di avere una **sintesi chiara** sulla misura del rischio
- In grado di fornire gli opportuni **input** alla fase successiva di **gestione** del rischio
- Alcune considerazioni sulla **modellizzazione**:
 - Numero di **macroprocessi** ridotto
 - Solo i **data asset** strettamente **significativi** (le domande si ripetono)
 - Solo gli EUS significativi correlati ai **data asset**
 - Solo le **software application** significative (escludere i package commerciali)
- Alcune considerazioni sulle **interviste**:
 - Non perdersi d’animo se il cliente non accetta subito (c’è diffidenza)
 - **Pianificare con attenzione** i momenti di incontro e i giusti interlocutori
 - **Non accelerare i tempi** per il raggiungimento del risultato
 - Lasciare spazio alla **riflessione** ed **ascoltare**
 - Approfondire la domanda con esempi per **chiarire**
 - **Non** fare **assunzioni** personali ma lavorare con il cliente
 - Mantenere traccia cartacea e poi riportare i risultati sul tool CRAMM
 - **Non** presentare mai la **quantificazione** delle singole risposte ai questionari

La misura del rischio

- A ciascuna **risposta** viene assegnato un **punteggio** il cui valore cumulativo, associato alla struttura del modello, permette di **quantificare il rischio per ciascun asset**, secondo una scala a cinque valori, via via crescenti:
 - Very Low
 - Low
 - Medium
 - High
 - Very High
- CRAMM calcola **automaticamente la misura** del rischio

In piu'...

- Il tool CRAMM permette di;
- Determinare le contromisure da adottare
- Stabilire il livello di dettaglio delle contromisure:
 - Linee guida
 - Dettagli operativi
- Mantenere lo stato di attuazione delle contromisure
- Registrare lo storico delle review precedenti



i n v e n t