

Caraf

Crypto Agility Risk Assessment Framework

Analisi dei Rischi

Autore: Pietro Conte

Proferressa: Alessandra De Benedictis

Risk Assessment



La sicurezza informatica

L'importanza della sicurezza cresce nel tempo, seguendo l'evoluzione delle minacce digitali.

INCREASE IN
CYBER THREATS



L'importanza della crypto-agility

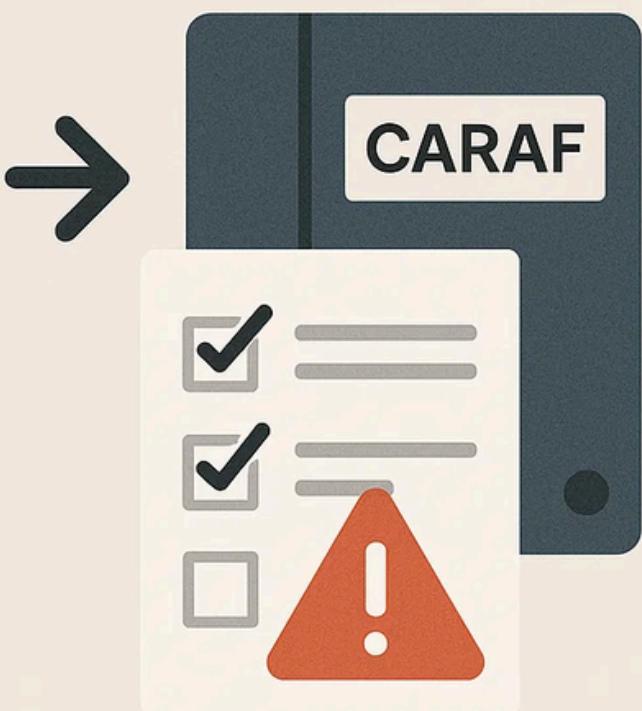
Mancanza di crypto-agility → rischi significativi

Nel caso di Enigma, la mancanza di crypto-agility limitò la capacità dei Nazisti di reagire a una vulnerabilità critica.

Crypto-agilità



Valutazione dei rischi derivanti dalla mancanza di crypto-agilità



Tecnologie sotto minaccia

Le nuove tecnologie, possono creare enormi problemi alle organizzazioni.

- algoritmo di Shor;
- algoritmo di Grover



Algoritmo	Tipo	Impatto Quantum
AES	Simmetrica	Usare chiavi più lunghe
SHA	HASH	Output maggiore
RSA/ECC	Pubblica	Non più sicuro

Tra le vulnerabilità reali recenti, spicca particolarmente la vulnerabilità ROCA (2017)



Come valutare il rischio?

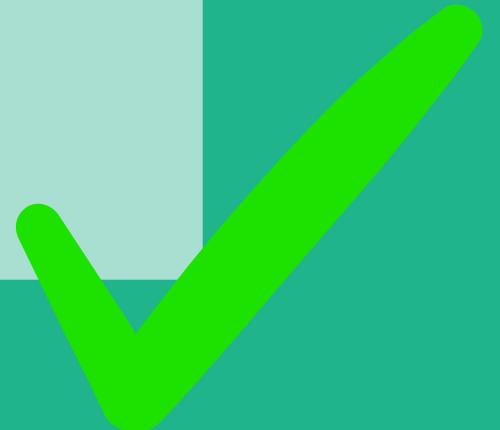
Problema individuato

La mancanza di crypto-agility non rappresenta soltanto una sfida tecnica, ma costituisce un vero e proprio rischio aziendale.



Come lo risolvo?

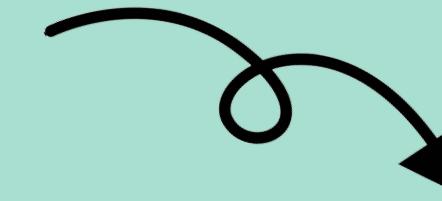
In questo lavoro viene presentato il Crypto Agility Risk Assessment Framework (CARAF), un modello a cinque fasi (5D) che consente di valutare il rischio associato alla mancanza di crypto-agility.



Contributo del Framework



Cosa ha di importante questo framework?



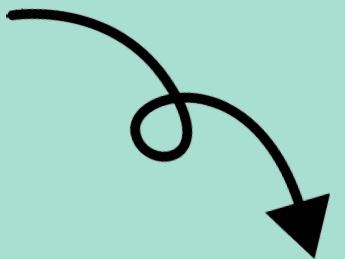
Il contributo di questo lavoro è un framework per affrontare la sicurezza e la gestione del rischio in modo **proattivo** invece che **reattivo**.

Questo framework cerca di anticipare i problemi invece di reagire solo quando si verificano incidenti.

Threat modeling operativo

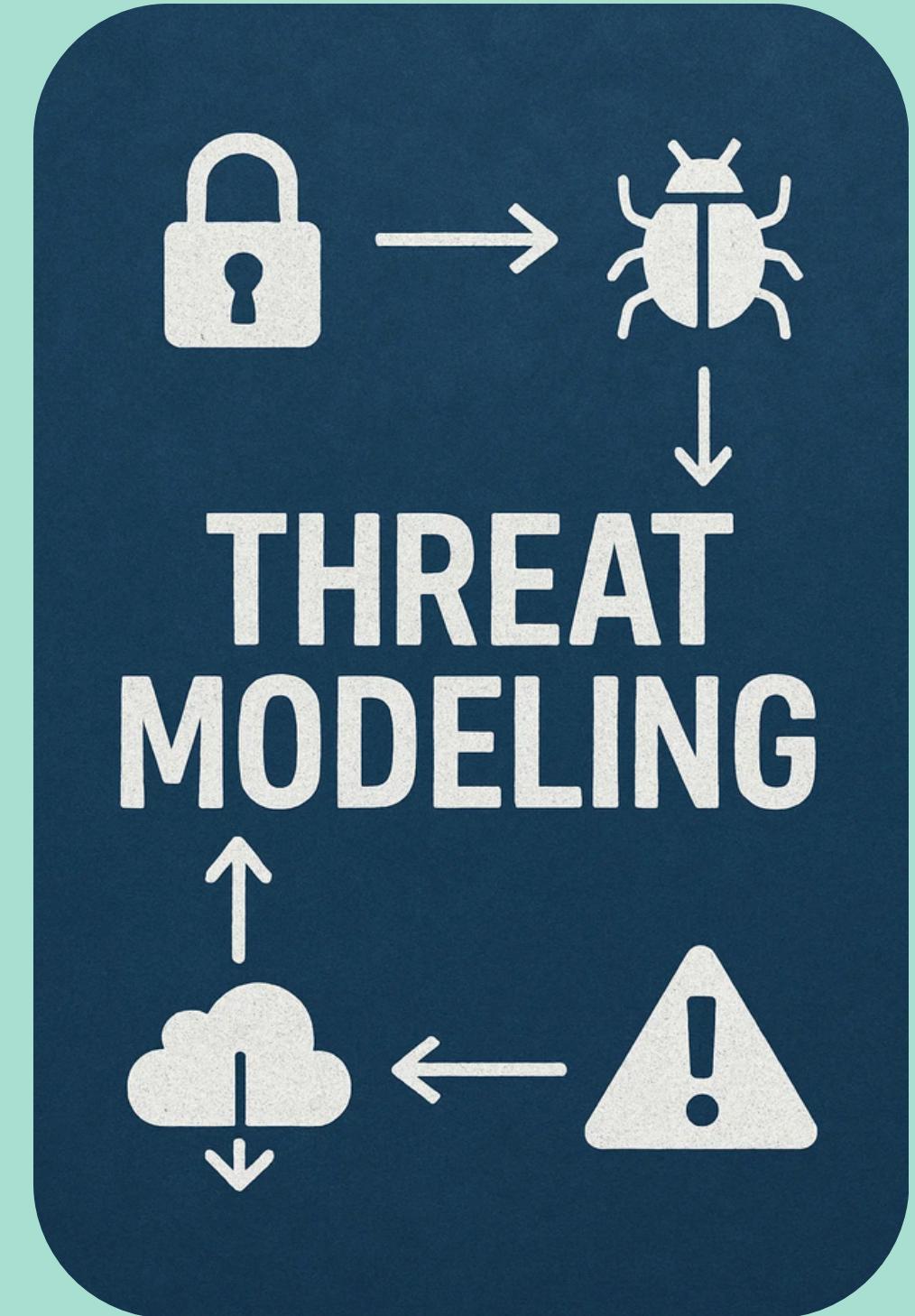
Processo sistematico volto a identificare:

- 1) attori ostili;
- 2) le loro capacità;
- 3) le loro motivazioni;
- 4) vettori d'attacco



Per fare cosa? Quale è l'obiettivo?

L'obiettivo è la produzione di scenari di minaccia direttamente utilizzabili nella valutazione del rischio secondo CARAF



Le 5 fasi di CARAF

01. Identificazione della minaccia

In questa fase individua il vettore di minaccia che giustifica la valutazione del rischio.

Questa fase serve per rendere l'organizzazione preparata a eventuali danni.

02. Inventario degli assets

Creazione di un inventario dettagliato degli assets crittografici impattati. Ci sono vari aspetti da considerare, tra cui: l'ambito, la sensibilità e la crittografia.

03. Stima del rischio

Rischio = Tempistica × Costo

La tempistica si basa sul Modello di Mosca

Il costo dipende principalmente dall'infrastruttura e dalla complessità

04. Strategie di Mitigazione

In questa fase si definiscono le azioni da prendere per ridurre il rischio

05. Roadmap organizzativa

Definizione della roadmap operativa per implementare la strategia scelta

Riassunto delle fasi



Caso di studio

Obiettivo: usare il framework CARAF per valutare il rischio e prendere decisioni su come mitigarlo.

Passo 1: Individuazione della minaccia.

- > Chi punta? I dispositivi IoT che usano TLS basato su crittografia;
- > Si vanno a compromettere algoritmi a chiave pubblica;
- > Soluzione, quantum-safe PQC.

Passo 2: Inventario degli asset.

- > Si identificano tutti gli asset impattati;
- > Ci sono 4 aspetti da considerare:
 - 1) Ambito: TLS;
 - 2) Sensibilità: dispositivi IoT;
 - 3) Crittografia: chiave pubblica;
 - 4) Gestione del ciclo di vita: dispositivi devono rispettare politiche di aggiornamento e sostituzione.



Caso di studio

Passo 3: Stima del rischio

--> Si usa un approccio chiamato MOSCA (XYZ);

Durata in anni	Livello
0-5	Critico
5-10	Alto
10-20	Medio
20+	Basso

Table 2: Tabella durata anni.

- Asset con supporto quantum: 5-10 anni;
- Asset senza supporto quantum: 11-20+ anni

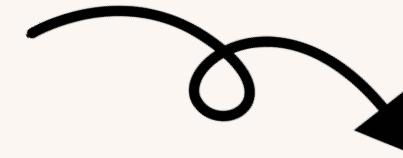
L'ultimo fattore è (X), ossia la durata di vita. I dispositivi IoT hanno una durata che va da 2 a 20+ anni.

Tempistica	1–Rischio Basso	2–Rischio Medio	3–Rischio Alto	4–Critico
X (Durata/Vita utile)	5	10	20	20+
Y (Mitigazione)	0-5	6-10	11-20	20+
Z (Minaccia)	20+	10-20	5-10	0-5

Table 3: Stima del rischio di tempistica in anni.

Come viene interpretato?

Se $X + Y > Z$ vuol dire che il rischio è alto o critico, perchè la minaccia arriva prima che l'asset possa essere aggiornato.



Esempi:

1) Esempio B (basso rischio): $X=3$ anni, $Y=2$ anni, $Z=10$ anni $\rightarrow 3+2=5 < 10 \rightarrow$ rischio BASSO \rightarrow Azione: pianificazione ordinaria;

2) Esempio C (critico): $X=12$, $Y=10$, $Z=5 \rightarrow 22 > 5 \rightarrow$ critico \rightarrow Azione: eliminazione graduale / sostituzione urgente.

Invece, il costo di mitigazione varia in base al tipo di asset (se supporta già pQC):

- Asset già compatibili PQC \rightarrow costo basso;
- Asset non compatibili PQC \rightarrow costo alto.

Rischio	Significato
1	Basso
2	Medio
3	Alto
4	Critico

Table 4: Tabella di rischio

Caso di studio

Passo 4: Strategia di mitigazione

In base al rischio e al costo, in questa fase, si deve decidere cosa fare. Si può:

1. Accettare il rischio → se basso o se la gestione costosa;
2. Mettere in sicurezza → aggiornare a PQC o a soluzioni ibride;
3. Eliminare gradualmente → sostituire gli asset obsoleti o non aggiornabili;

Passo 5: Roadmap organizzativa

L'ultimo step specifica come implementare le azioni prese in considerazione.

Ad esempio, se il rischio è basso, si continuerà con i piani attuali.

Fase 4 e Fase 5:
**FASI
FINALI**

Conclusioni

Questo lavoro tratta il Risk Assessment, che si basa sul framework CARAF per aiutare le organizzazioni ad affrontare i rischi derivanti dalla mancanza di crypto agility.



Risk Assessment

Grazie per l'attenzione

Presentato da Pietro Conte

