Il ruolo del Security Manager

ovvero

il referente per la sicurezza

Claudio Allocchio
GARR

… una cosa nuova?

- … veramente…. Sono **circa 8 anni** che ogni organizzazione della Pubblica Amministrazione dovrebbe essersi dotata di una figura interna che si occupa di sicurezza informatica (Framework Nazionale per la Cybersicurezza), con aggiornamenti dovuti al GDPR, alla direttiva NIS, ora alla NIS2…

- Ne abbiamo discusso ampiamente al WS GARR 2021 (vedi presentazioni)

Insomma…. Tanto nuova proprio non direi ☺

Ma questa è la parte «amministrativa» … che dice comunque che va nominato formalmente l'Access Security Manager (ASM).

Contesto di riferimento

- **È una figura che si aggiungebbe ai ruoli già identificati da GARR:**
  - **Delegato del Rettore (università)**
  - **APA**
  - **APM**

- **Esistono già ruoli specifici per «servizi» (IDEM, eduroam)**

- **GEANT Security Baseline**

  « per tutte le NREN la sicurezza dei servizi, degli utenti e delle operazioni e' fondamentale. Al fine di armonizzare il livello di sicurezza delle NREN, e' stata creata la Security Baseline come quadro comune”

- **Framework Nazionale Cybersicurezza**

  « *aiutare le organizzazioni nel definire un percorso volto alla cybersecurity e alla protezione dei dati coerente con i regolamenti stessi*"

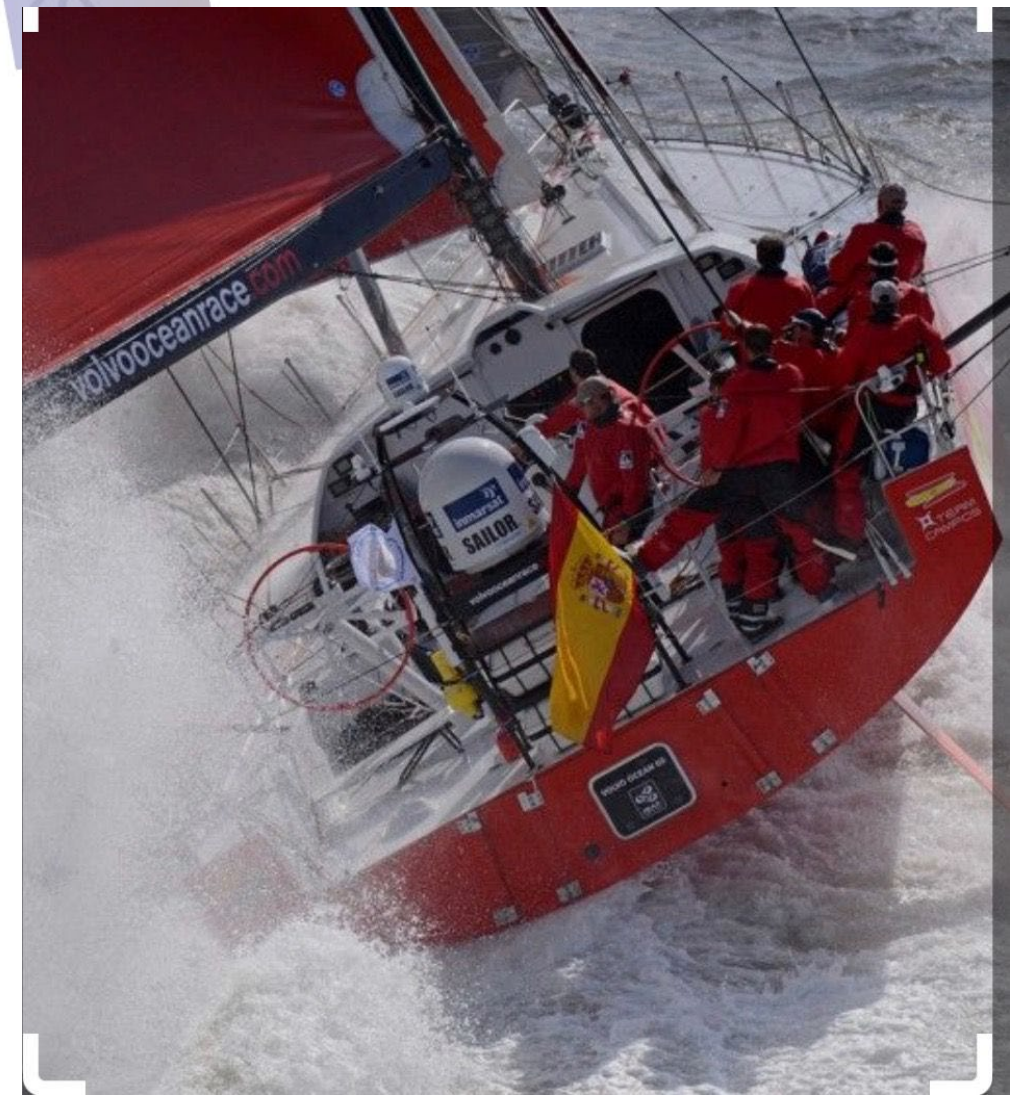
ASM – proposta di definizione del ruolo

- **Rappresenta il punto di contatto ufficiale di GARR-CERT per la gestione di tutte le problematiche di sicurezza**

- **Deve essere formalmente ed ufficialmente nominato dal proprio ente a trattare tutte le informazioni relative a incidenti e problemi di sicurezza**

- **Deve gestire, in base alle procedure definite internamente al proprio ente, le varie azioni relative alla sicurezza, interagendo secondo procedure definite con gli altri ruoli esistenti (APM, APA, DPO, RTD, Amministratori di Sistemi e Rete, etc…)**

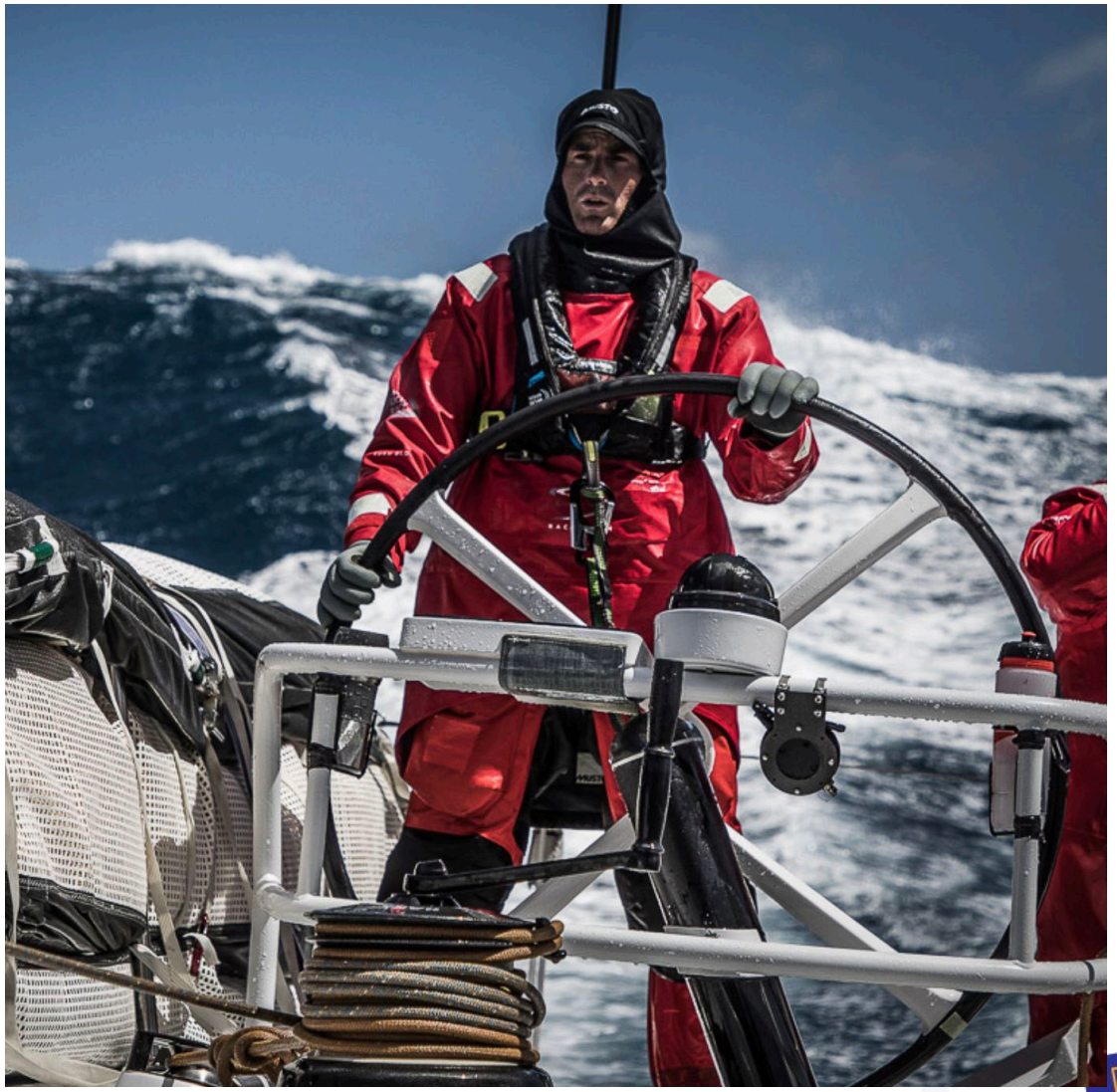
Ci sarà una lettera di richiesta formale di GARR a tutti gli enti (con tutti I riferimenti dettagliati alle normative, ma sopratutto anche al ruolo operativo richiesto) per la nomina dell'ASM.



Navighiamo un po’

non sempre è tutto calmo e dolce…

Ma il «Security Manager»
è la dietro e sa cosa fare…



Un esempio esterno: **una vela d'altura che incontra una tempesta in mare aperto:**

- **Ogni membro dell'equipaggio ha il suo ruolo e sa cosa fare**
- **Lo skipper da gli ordini, e tutti eseguono**
- **Si comunica posizione e situazione di bordo**
- **Si tengono informati i passeggeri (se ci sono)**

ASM – cerchiamo di essere «pratici»

- **La gestione di incidenti e problemi di sicurezza richiede:**
  - **Rapidità ed efficacia d'intervento (… poche ore… minuti meglio, esecuzione di azioni senza discussione)**
  - **Procedure precise e collaudate (fare "esercitazioni" non è una cattiva idea)**
  - **Una squadra interna dove ognuno sa cosa deve fare**
  - **Il coordinamento stretto ed immediato con GARR-CERT**
  - **Un "coordinatore unico" che gestisce la situazione (l'ASM)**
  - **La gestione corretta ed efficace della "comunicazione" (interna ed esterna)**

Come lo implemento?

- **Non c'è una ricetta "unica", ogni ente internamente crea gli schemi e procedure che più si adattano alla propria situazione**

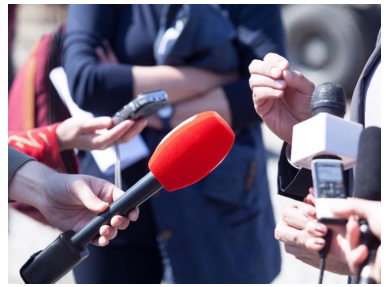
- **Non serve inventarsi tutto da capo! Ci sono già tanti esempi funzionanti a cui ci si può ispirare!**

  - **Istituto Nazionale di Fisica Nucleare**
  - **European University Institute**
  - **Politecnico di Torino**
  - **Università di Bologna**
  - **Università di Firenze**

Più esempi si aggiungono, più diventa facile "ispirarsi e copiare"

Non siete soli in mezzo al mar…

- **Il vostro canale VHF16 e la Guardia Costiera sono il GARR-CERT**
- **Ci sono le altre navi vicine a voi (quelli che hanno già in essere le procedure e vi possono assistere con qualche dritta)**
- **Si possono stabilire collaborazioni per supporto reciproco (GARR potrebbe fare il broker aiutandovi a trovare i partner)**
- **Esistono procedure consolidate di come gestire l'aspetto "Comunicazione" di gestione di una crisi, e la comunità può aiutarti (vedi anche training di GEANT etc).**



Riferimenti normativi

- CAD Codice Amministrazione Digitale, D.L. 7 marzo 2005, n. 82, modificato con D.L. 22 agosto 2016 n. 179, e D.L. 13 dicembre 2017 n. 217 per attuare I diritti di cittadinanza digitale Codice Amministrazione Digitale, in particolare art.17 comma C.

- MMSPA Circolare AGID 18/04/2017 Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni

- GDPR il Regolamento Europeo n.679 del 27/04/2016 "General Data Protection Regulation" relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati

- DIRETTIVA NIS DIR_UE 2016/1148 del 06/07/2016 "Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Cybersecurity ACT REG_UE 2019/881 del 17/04/2019: relativo a "ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione

- Quadro normativo relativo al Perimetro di Sicurezza Nazionale Cibernetica (cfr. D.L. 105 del 21/09/2019 Perimetro e misure correlate) ed alla "recente" istituzione della Agenzia per la Cybersicurezza Nazionale

- NIS 2 (Direttiva NIS2). Entro il 17 ottobre 2024, gli stati aderenti promulgheranno le rispettive leggi nazionali di adozione della direttiva NIS2(pdf). 14/9/23: Commission Guidelines on the application of Article 3(4) of Directive (EU) 2022/2555 (NIS 2 Directive).

- DPR 81 13/6/23 Decreto del Presidente della Repubblica 13 giugno 2023, n. 81 Utilizzo delle tecnologie informatiche: [...] L'amministrazione, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati.[...]

… e non ultimo: articolo 14.3 Statuto GARR

“Ciascun associato, nel rispetto delle procedure previste dal proprio ordinamento, sulla base di apposite convenzioni, si impegna a mettere a disposizione del GARR le conoscenze tecniche, le capacità professionali e le risorse infrastrutturali e di personale necessarie per il migliore conseguimento dell’oggetto sociale."

→ se guardate quali sono missione e obiettivi di GARR, "sicurezza" e "affidabilita’” sono chiaramente presenti

La Sicurezza non ha confini… Siamo qui per lavorarci insieme,

TUTTI !

Grazie! Domande?

Claudio.Allocchio@garr.it

cert@garr.it

E grazie a Leonardo ☺ !