

23 Settembre
2026

La cybersecurity non è più solo un problema IT. E' una questione di sicurezza nazionale ... e aziendale

Romano Stasi
Segretario Generale ABI Lab
Direttore Operativo CERTFin

TLP:GREE

Un modello integrato di «difesa ibrida»: individuare, dissuadere, difendere

Nell'ambito delle discussioni in corso presso il Cybersecurity Expert Group (CEG) del G7 è stato presentato un **modello integrato di gestione degli attacchi ibridi**, che si pone l'obiettivo di rafforzare la resilienza dell'ecosistema di sicurezza nazionale attraverso l'anticipazione delle minacce.

DETECT

Superiorità informativa

1 Intelligence strategica

Costruire e condividere con tutti gli attori coinvolti una lettura della minaccia per anticiparla e orientare rapidamente la risposta

2 Analisi forense finanziaria

Seguire i flussi finanziari per far emergere reti e leve concrete di contrasto attraverso una stretta collaborazione con le forze dell'ordine

5 Poteri dell'intelligence

Dotare l'intelligence di capacità, strumenti e coordinamento adeguati a operare efficacemente la risposta nel dominio ibrido

DETER

Misure mirate e proporzionate

3 Misure difensive asimmetriche

Rendere efficace la deterrenza attraverso risposte mirate e proporzionate, sviluppate in logica intersettoriale

4 Comunicazione strategica

Governare informazione per anticipare la disinformazione e rafforzare la credibilità della risposta

7 Consolidamento e cooperazione internazionale

Mettere a sistema le capacità nazionali e collegarle stabilmente ai meccanismi internazionali

DEFEND

Resilienza e continuità

6 Resilience by design

Integrare la resilienza nelle infrastrutture fin dalla progettazione, riducendo vulnerabilità e dipendenze critiche

8 Apprendimento, formazione e istruzione

Sviluppare competenze diffuse e una cultura della readiness attraverso formazione, esercitazioni e apprendimento continuo

9 Preparazione della società

Rendere istituzioni, imprese e cittadini più **consapevoli** e pronti a sostenere nel tempo una strategia di difesa ibrida

Dalla risposta nazionale a un modello di cooperazione internazionale

Il modello e la rete degli attori coinvolti collocano la gestione degli attacchi ibridi in una dimensione che supera i confini nazionali e richiede un **approccio strutturalmente internazionale**.

DETECT

DETER

DEFEND



ACN

Coordina postura cyber nazionale, CSIRT e integrazione operativa del quadro di minaccia



Intelligence e Difesa

Integra intelligence strategica e informazioni per costruire un quadro unitario della minaccia



Autorità settoriali

Traducono il modello in requisiti di vigilanza, monitoraggio e continuità operativa di settore



Forze dell'Ordine

Presidiano indagini e financial forensics, rendendo credibili conseguenze ed enforcement



Settori produttivi attraverso strutture di aggregazione (es. CERTFin)

Rilevano anomalie, condividono evidenze e rafforzano continuità, recovery ed esercitazioni



Dimensione internazionale

Sviluppare una rete di cooperazione di dominio e di settore per lo scambio informativo e il coordinamento della risposta

GRAZIE!