UE7-D - Organizzare i processi per garantire la sicurezza informatica dell' dell'azienda e del suo ambiente

UE7- D2 Gestire la comunicazione interna ed esterna con collaboratori, fornitori, clienti

Comunicazione

- Promemoria, prevenzione , Rischio, piano d'azione
- Gli attori della crisi
- Comunicazione di crisi

SEMESTRE 10					
UE 7 - Attuare una politica di sicurezza informatica efficace		**BC 3**	**45**	*6*	**6**
UE7-A - Definizioni dei concetti di sicurezza e protezione			**15**	**2**	**2**
UE7-A-1	Sicurezza e protezione, due ambiti distinti ma di pari importanza				
UE7-A-2	Cybersicurezza: una visione condivisa tra utenti, progettisti di apparecchiature, reti di trasmissione, servizi di gestione dei dati				
UE7-C - Assicurare il rischio legato agli attacchi informatici			**15**	*2*	**2**
UE7-C-1	Identificare i settori funzionali, mapparli e garantirne l' interoperabilità sicura - Esigenze, constatazioni, analisi				
UE7-C-2	Assicurazione per coprire i costi causati dagli attacchi informatici ai sistemi informativi				
UE7-D - Organizzare i processi per garantire la sicurezza informatica dell'azienda e del suo ambiente			**15**	*2*	**2**
UE7-D-1	Le fasi dell'azione: anticipare e monitorare, reagire e combattere, ripristinare				
UE7-D-2	Gestire la comunicazione interna ed esterna verso i collaboratori, i fornitori, i clienti				

Promemoria

- Rischio
- Prevenzione
- Piano d'azione

Comunicazione

Rischio informatico (promemoria)

Organismi interessati

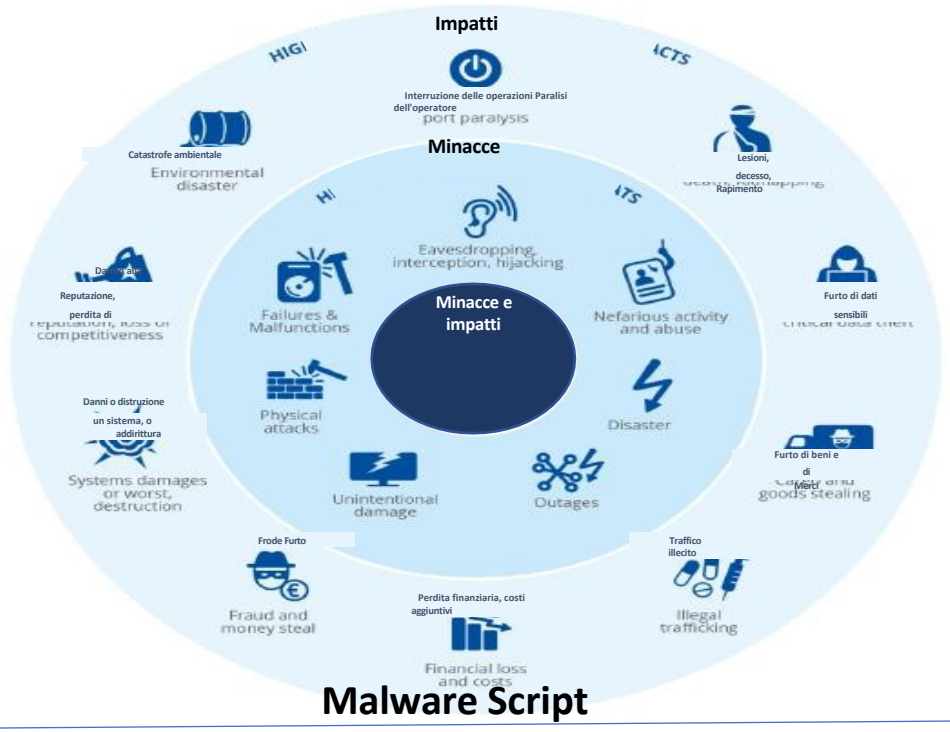
- Riservatezza
- Integrità
- Disponibilità
- Non ripudiabilità
- Autenticazione

Cosa

Come

Dove

Chi



Livello	Normativa	Porti	Navi	Attività offshore	Minacce
OIV	**ECI Dir** (2008) **LPM** (2007)	Grandi porti sicuri	Raramente sono OIV	Petrolio e gas	Attacchi informatici Terrorismo Catastrofi
OSE	**Direttiva NIS** (2020)	Alcuni porti non OIV	In alcuni paesi	EMR e cavi sottomarini	Terrorismo Attività criminali (comprese quelle informatiche)
User	**RGPD** (2018)	La necessità di aumentare il PPCM della sicurezza informatica è imprescindibile in un settore fortemente digitalizzato e connesso			Attività criminali Influenza

Malware Script

kiddy

Dipendente malintenzionato

Gruppo terroristico

Organizzazione criminale Stato

Sicurezza / Protezione
Prevenzione / Rischio

Esempio di piano d'azione

SENSIBILIZZAZIONE – PIANO D'AZIONE

I	Sensibilizzare e formare	STANDARD	RINFORZATO
1	Formare i team operativi alla sicurezza dei sistemi informativi		
2	Sensibilizzare gli utenti alle buone pratiche di base in materia di sicurezza informatica		
3	Controllare i rischi dell'outsourcing informatico		
II	Conoscere il sistema informativo		
4	Identificare le informazioni e i server più sensibili e mantenere uno schema della rete		
5	Disporre di un inventario completo degli account privilegiati e mantenerlo aggiornato		
6	Organizzare le procedure di arrivo, partenza e cambio di funzione degli utenti		
7	Autorizzare la connessione alla rete dell'entità solo alle apparecchiature controllate		
III	Autenticare e controllare gli accessi		
8	Identificare nominalmente ogni persona che accede al sistema e distinguere i ruoli utente/amministratore		
9	Assegnare i diritti corretti sulle risorse sensibili del sistema informativo		
10	Definire e verificare le regole di scelta e dimensionamento delle password		
11	Protezione delle password memorizzate sui sistemi		
12	Modificare gli elementi di autenticazione predefiniti su apparecchiature e servizi		
13	Privilegiare, quando possibile, un'autenticazione forte		

SENSIBILIZZAZIONE – PIANO D'AZIONE

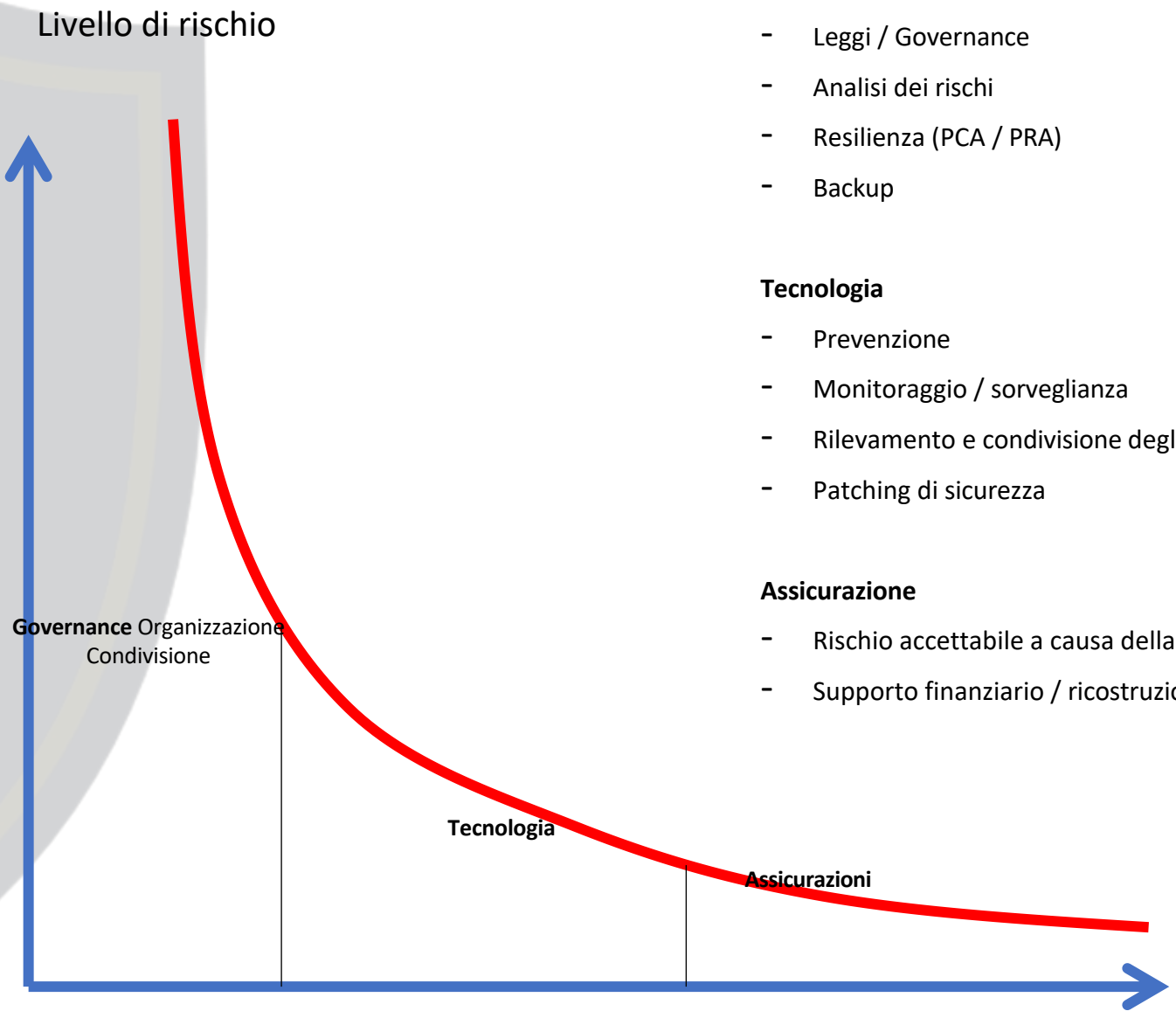
IV	Proteggere le postazioni		
14	Implementare un livello minimo di sicurezza su tutto il parco informatico		
15	Proteggersi dalle minacce relative all'uso di supporti rimovibili		
16	Utilizzare uno strumento di gestione centralizzata per uniformare le politiche di sicurezza		
17	Attivare e configurare il firewall locale delle postazioni di lavoro		
18	Crittografare i dati sensibili trasmessi via Internet		
V	Proteggere la rete		
19	Segmentare la rete e creare una separazione tra queste zone		
20	Garantire la sicurezza delle reti Wi-Fi e la separazione degli utilizzi		
21	Utilizzare protocolli sicuri non appena disponibili		
22	Implementare un gateway di accesso sicuro a Internet		
23	Separare i servizi visibili da Internet dal resto del sistema informativo		
24	Proteggere la propria posta elettronica professionale		
25	Proteggere le interconnessioni di rete dedicate con i partner		
26	Controllare e proteggere l'accesso alle sale server e ai locali tecnici		

SENSIBILIZZAZIONE – PIANO D'AZIONE

VI	Rendere sicura l'amministrazione		
27	Vietare l'accesso a Internet dai computer/server amministrativi del sistema informatico		
28	Utilizzare una rete dedicata e separata per l'amministrazione del sistema informativo		
29	Limitare i diritti di amministrazione sulle postazioni di lavoro alle strette necessità operative		
VII	Gestire il nomadismo		
30	Adottare misure di sicurezza fisica dei terminali nomadi		
31	Crittografare i dati sensibili, in particolare quelli presenti su dispositivi che potrebbero andare persi		
32	Proteggere la connessione di rete dei dispositivi utilizzati in mobilità		
33	Adottare politiche di sicurezza dedicate ai dispositivi mobili		
VIII	Mantenere aggiornato il sistema informativo		
34	Definire una politica di aggiornamento dei componenti del sistema informativo		
35	Anticipare la fine della manutenzione dei software e dei sistemi e limitare le aderenze software		
IX	Supervisionare, controllare, reagire		
36	Attivare e configurare i registri dei componenti più importanti		
37	Definire e applicare una politica di backup dei componenti critici		
38	Eseguire controlli e audit di sicurezza regolari, quindi applicare le azioni correttive associate		
39	Nominare un referente per la sicurezza dei sistemi informativi e comunicarlo al personale		
40	Definire una procedura di gestione degli incidenti di sicurezza		
X	Per approfondire		
41	Condurre un'analisi formale dei rischi		
42	Privilegiare l'uso di prodotti e servizi qualificati dall'ANSSI		

Ridurre il rischio / agire

Riduzione del rischio informatico



Governance / organizzazione

- Leggi / Governance
- Analisi dei rischi
- Resilienza (PCA / PRA)
- Backup

Tecnologia

- Prevenzione
- Monitoraggio / sorveglianza
- Rilevamento e condivisione degli incidenti
- Patching di sicurezza

Assicurazione

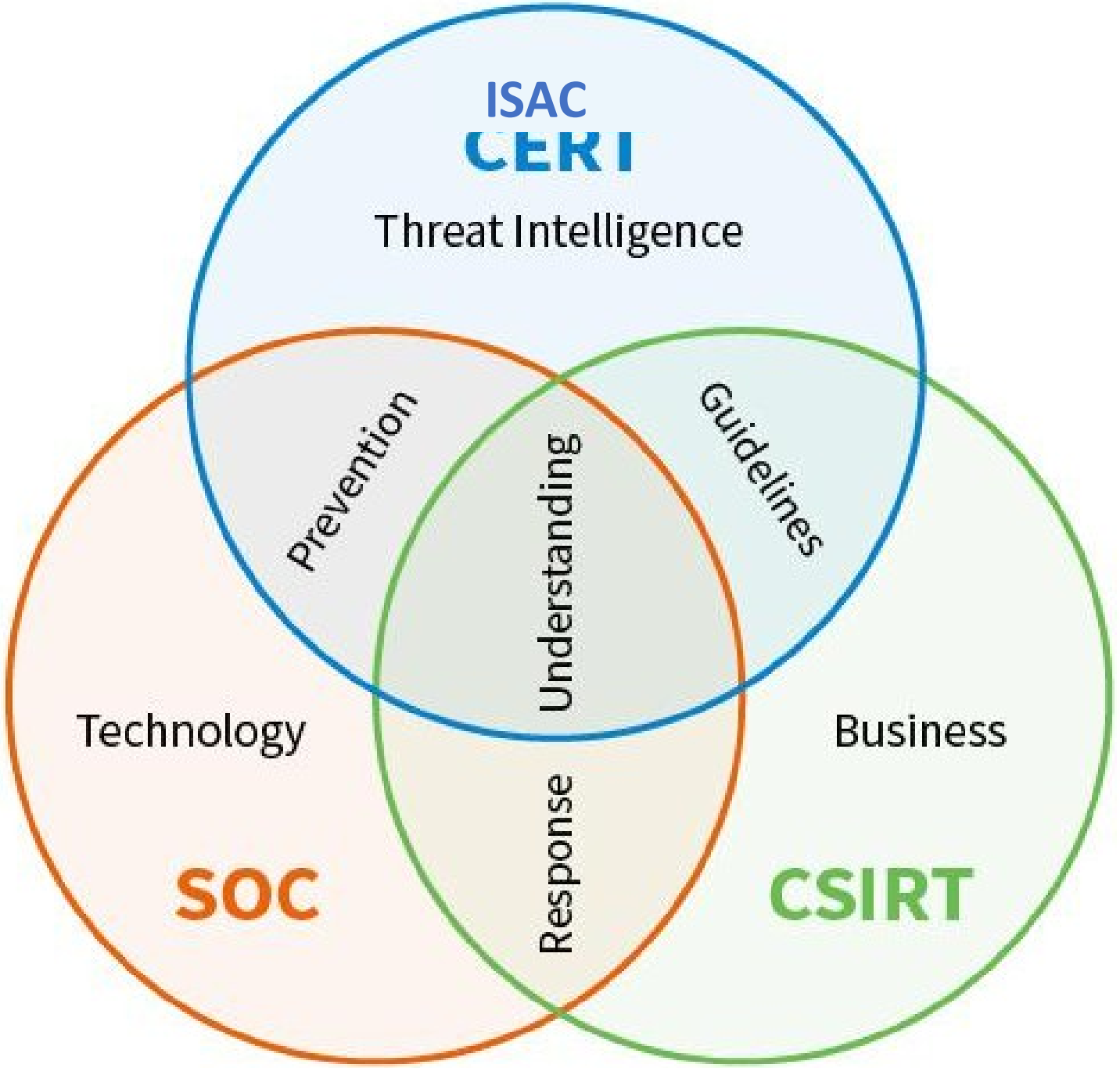
- Rischio accettabile a causa della bassa frequenza
- Supporto finanziario / ricostruzione

Domanda posta

-

Come organizzarsi di fronte alle minacce informatiche

?



Le 10 regole di base per limitare i rischi di attacchi informatici (1/2)

Condurre un'analisi dei rischi

- identificare le risorse aziendali essenziali, la loro criticità e l'impatto in caso di incidente;
- mappare gli stakeholder dell'organizzazione;
- identificare i requisiti legali e normativi applicabili;
- definire gli scenari di minaccia e i rischi operativi.

Redigere una specifica completa dal punto di vista funzionale e della sicurezza

Esigenze relative alla progettazione, allo sviluppo, alla MCO/MCS e alla reversibilità.

Esigenze di protezione contro le leggi di portata extraterritoriale (RGPD, SecNumCloud, legge di blocco, ecc.).

Tenere conto della guida relativa alle «clausole generiche di sicurezza nei contratti» dell'ANSSI e della Direzione degli acquisti dello Stato (DAE).

Affidarsi a un fornitore di servizi di hosting affidabile per i trattamenti e i dati più sensibili

Per le tecnologie cloud, la certificazione SecNumCloud consente di garantire un livello di affidabilità e di proteggersi dalle leggi extraterritoriali.

All'interno dell'infrastruttura di hosting, occorre prestare particolare attenzione ai principi di separazione, in particolare:

- tra le risorse dei diversi clienti dell'infrastruttura;
- tra i diversi ambienti di sviluppo, pre-produzione e produzione;
- tra le risorse aziendali e quelle dedicate alla gestione e all'amministrazione.

Garantire buone pratiche di sviluppo/progettazione (comprese verifiche periodiche)

Protezione delle infrastrutture, delle applicazioni e dei terminali amministratori e utenti, interni o propri dei subappaltatori.

Controllo e protezione delle interconnessioni

Le interconnessioni tra i sistemi con sistemi informativi di terzi e/o fornitori di servizi sono punti di attenzione fondamentali. Queste determinano la superficie di esposizione alle minacce e agli attacchi. È opportuno:

- mapparle;
- valutare e mantenere il livello di sicurezza;
- garantire il rilevamento degli incidenti di sicurezza.

In particolare, occorre considerare anche le interconnessioni interne all'entità, soprattutto per gli accessi in mobilità.

Le 10 regole di base per limitare i rischi di attacchi informatici (2/2)

Proteggere la gestione delle identità, i meccanismi di autenticazione e i controlli di accesso

Gestione delle identità e meccanismi di autenticazione.

L'ANSSI mette a disposizione delle guide che propongono raccomandazioni per rafforzare la sicurezza di un sistema informativo:

- *Raccomandazioni relative all'autenticazione multifattoriale e alle password.*
- *Guida all'igiene informatica: rafforzare la sicurezza del proprio sistema informatico in 42 misure*.
- *Raccomandazioni di sicurezza relative a un sistema GNU/Linux*.

Proteggere le risorse amministrative dei sistemi informativi

Queste risorse sono particolarmente prese di mira dagli hacker in quanto consentono di assumere rapidamente il controllo dell'intero sistema informativo.

La guida *Raccomandazioni relative alla gestione sicura dei sistemi informativi* dell'ANSSI fornisce indicazioni alle entità.

Garantire il mantenimento delle condizioni di sicurezza dei sistemi informativi

Correzioni di sicurezza delle piattaforme tecniche utilizzate.

Il sito CERT-FR pubblica in tempo reale gli avvisi di sicurezza.

Garantire e proteggere i backup dei dati e dell'infrastruttura

Il backup offline e off-site e i processi di ripristino sono fondamentali per risolvere una situazione di crisi, derivante o meno da una compromissione informatica.

Implementare un sistema di rilevamento degli incidenti di sicurezza (compresa la registrazione) e di gestione delle crisi

Consente di identificare rapidamente una minaccia e di intraprendere le azioni conservative e di riparazione necessarie prima che si verifichi una situazione di compromissione.
Questi dispositivi si basano necessariamente su un'infrastruttura di raccolta e centralizzazione dei registri degli eventi di sicurezza, che alimentano i servizi di rilevamento (vedere le guide *Raccomandazioni di sicurezza per l'architettura di un sistema di registrazione* e *Raccomandazioni di sicurezza per la registrazione dei sistemi Microsoft Windows in ambiente Active Directory*).

Definire i processi e le procedure di gestione delle crisi informatiche

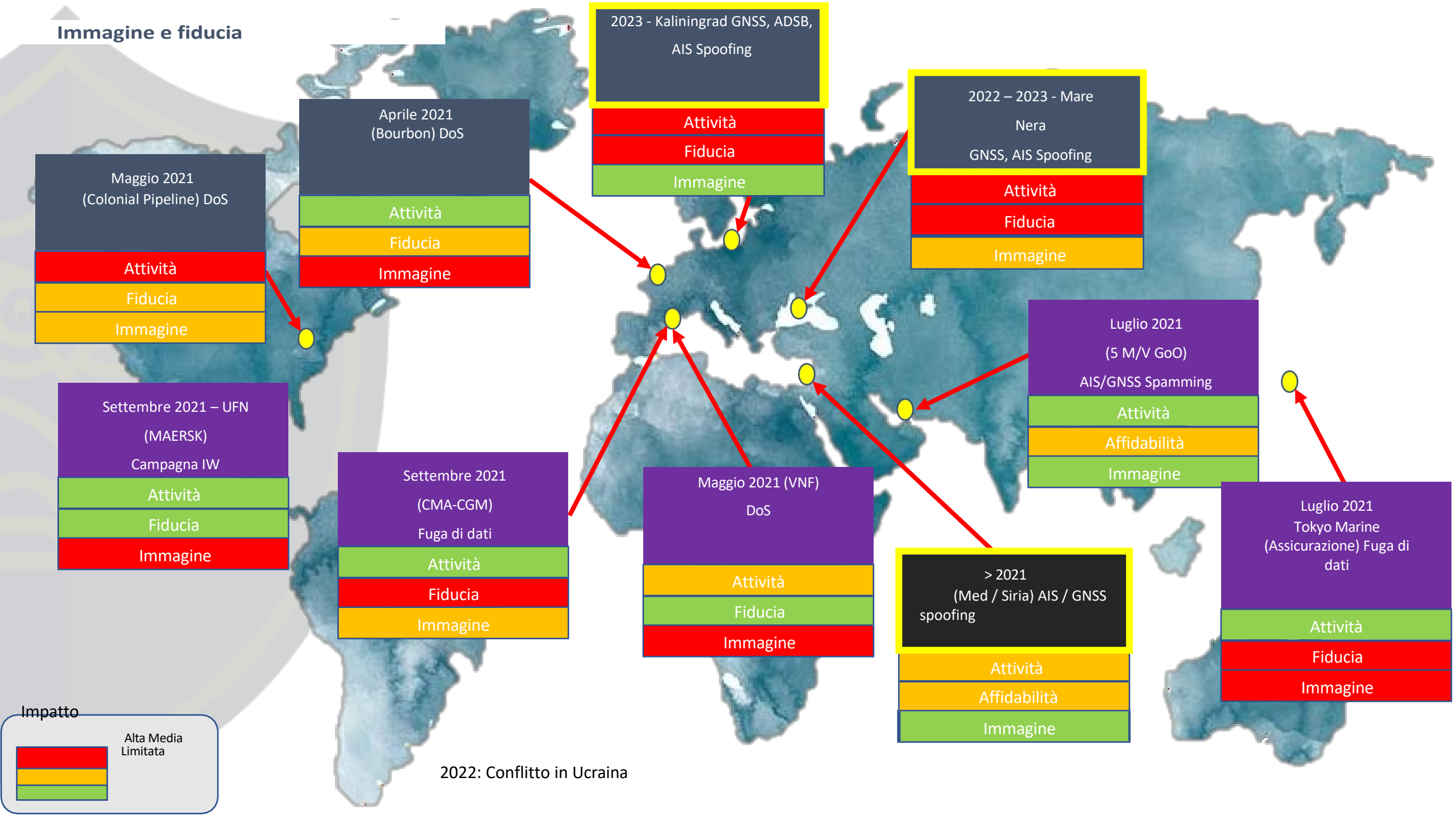
Per quanto riguarda la risposta agli incidenti, affidarsi a fornitori qualificati in materia di risposta agli incidenti di sicurezza (PRIS).

Comunicare in situazioni di crisi

Comunicazione e crisi

- È necessario comunicare?
- A chi
- Come
- Quando
- La trasparenza
- I limiti

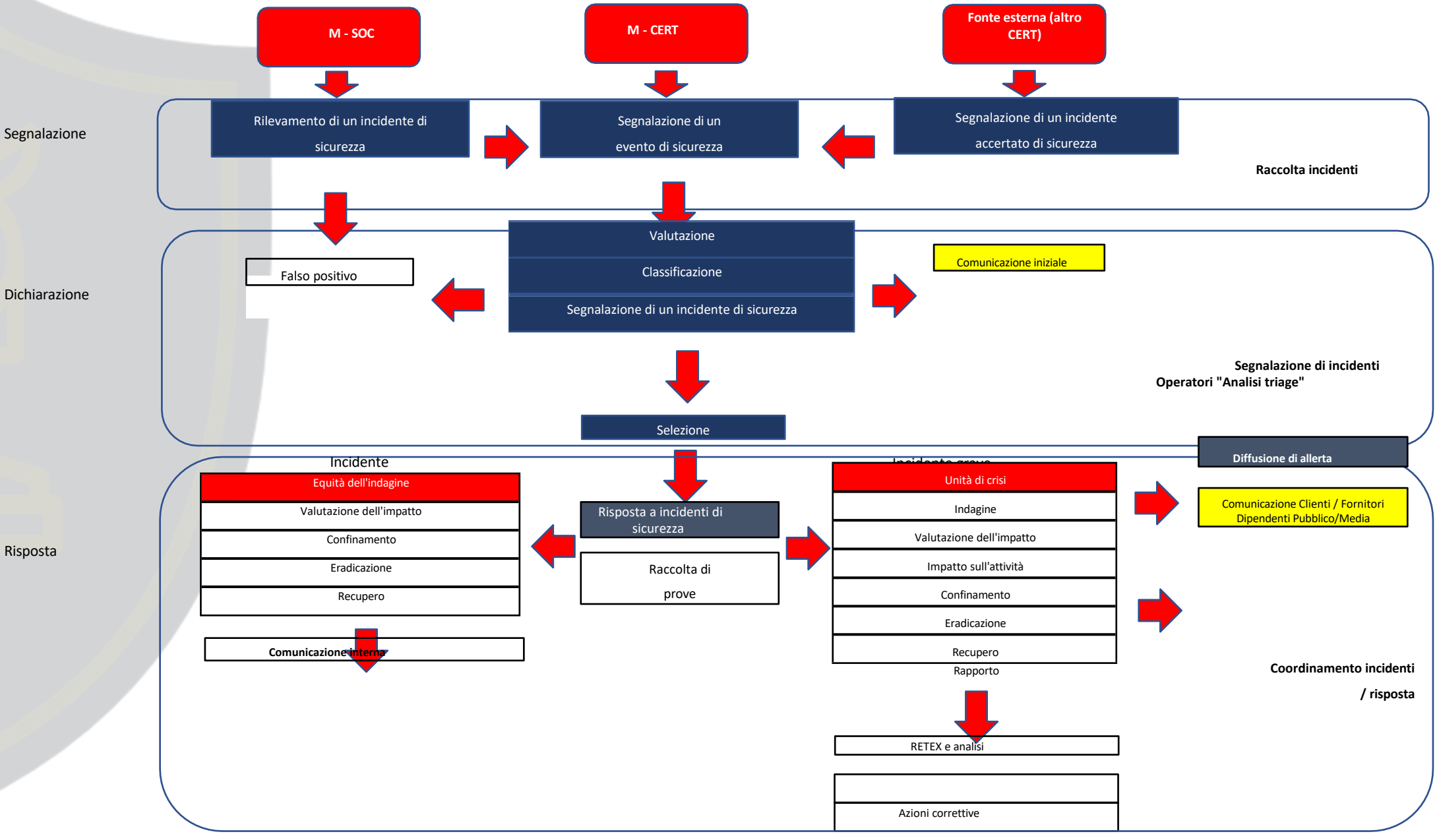
Immagine e fiducia



POSITIONNER UNE CRISE CYBER FACE AUX ÉVÈNEMENTS PORTANT ATTEINTE AUX ACTIVITÉS MÉTIERS D'UNE ORGANISATION

Promemoria – Gestione delle crisi

Organigramma di gestione degli incidenti



Le fasi della comunicazione di crisi

FASE 1: avviare un dialogo con i team informatici e IT al di fuori dei periodi di crisi

FASE 2: anticipare gli scenari di crisi e le risposte da fornire in materia di comunicazione FASE 3: elaborare una strategia di comunicazione per rispondere alla crisi

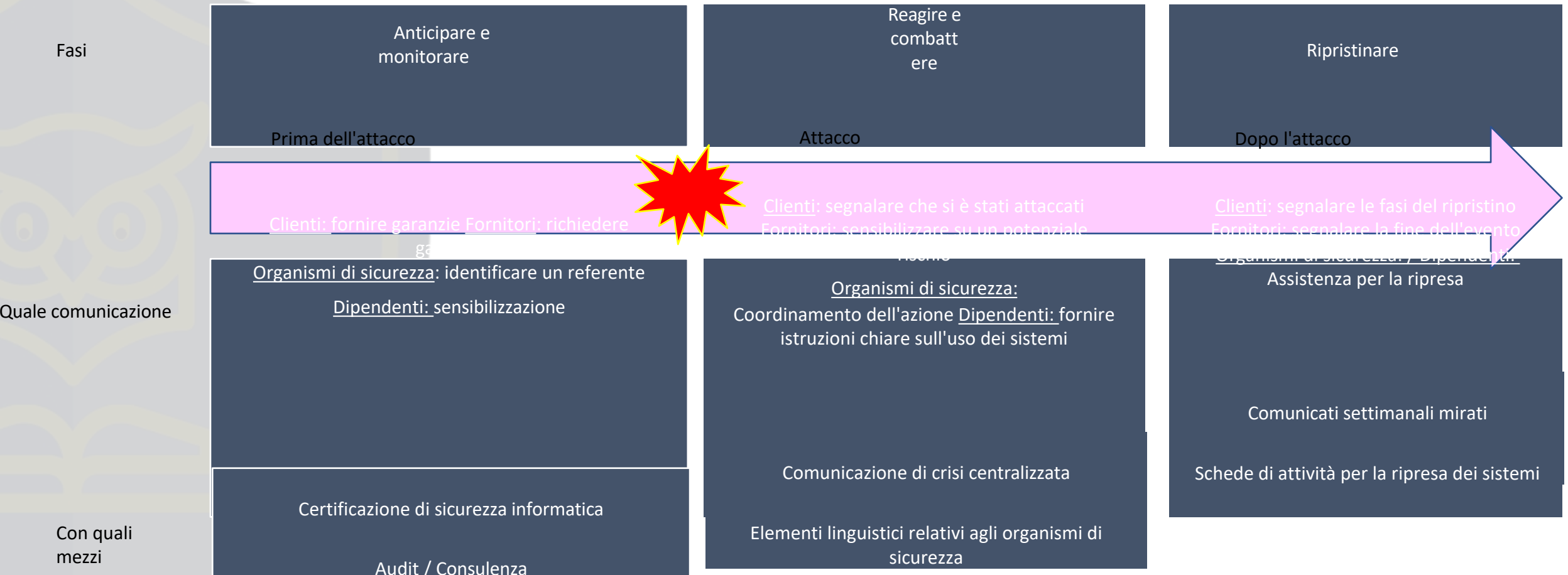
FASE 4: integrare la funzione di comunicazione nell'organizzazione della gestione delle crisi informatiche

FASE 5: organizzare la comunicazione di crisi

FASE 6: creare un kit di strumenti dedicato alla gestione di una crisi informatica

FASE 7: formare i propri team alla gestione della comunicazione

Comunicare prima, durante e dopo



Caso pratico

Scenario: compromissione dei vostri sistemi informativi tramite una terza parte

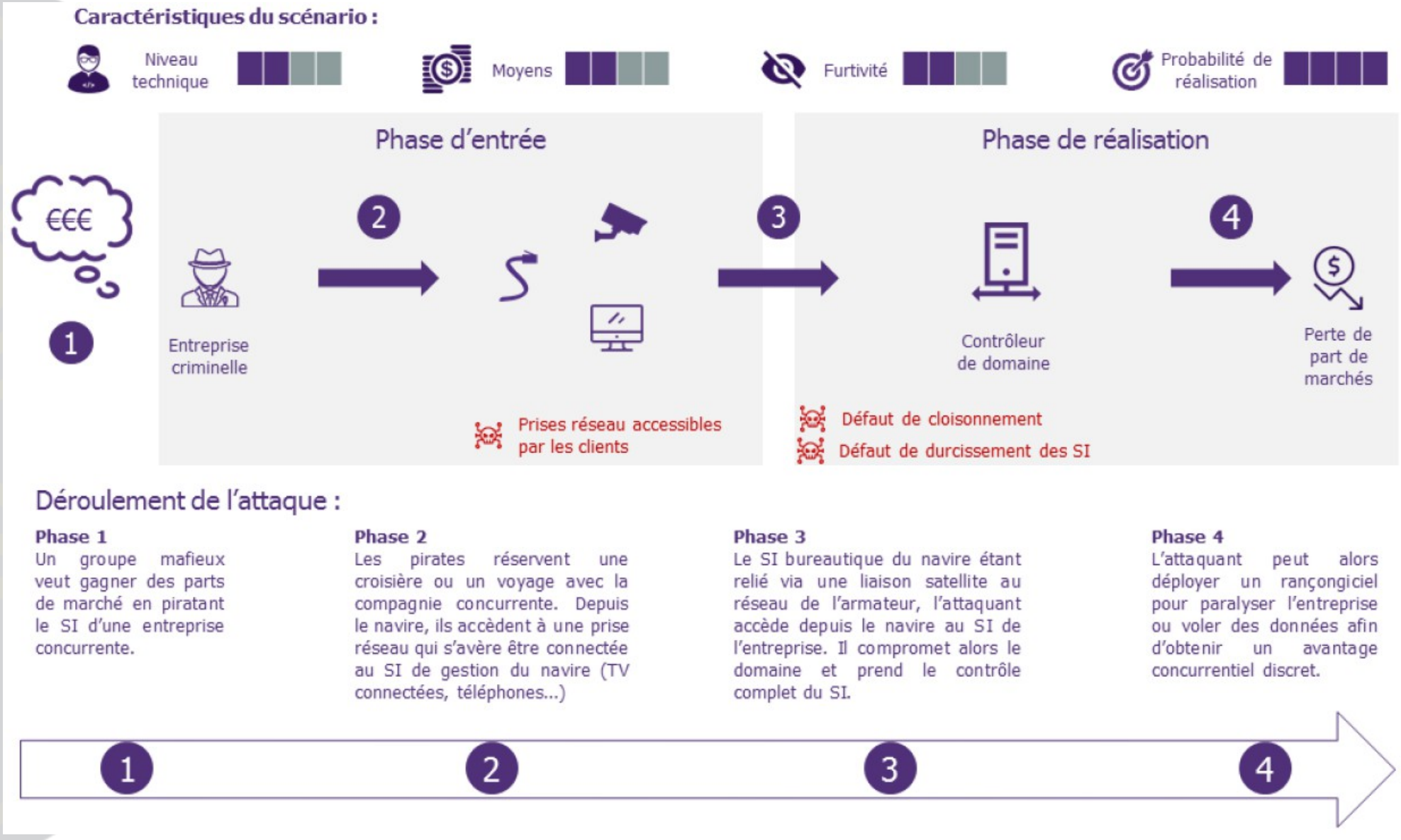
Un aggressore desideroso di aumentare la propria quota di mercato danneggiando un'azienda concorrente accede, una volta entrato in uno dei siti della sua vittima, a una presa di rete presente in un'area accessibile al pubblico e non protetta. Si diffonde all'interno del sistema informatico e, tramite Internet, alla vostra rete per raggiungere i vostri sistemi informatici.

La configurazione del controller di dominio presenta alcune vulnerabilità, l'aggressore ne sfrutta una e acquisisce

diritti di amministratore. A quel punto ha il controllo totale del vostro sistema informatico.

Una compartimentazione debole o inesistente, nonché l'assenza di sorveglianza delle reti, rendono i sistemi informatici di terzi potenziali punti di ingresso.

Fasi dell'attacco



Reazioni / Misure da adottare

Comunicazione una volta scoperto l'incidente

- ***Clienti***
- ***Fornitori***
- ***Collaboratori / dipendenti***
- ***Organismi di sicurezza (in caso di crisi)***
- ***Grande pubblico (per grandi gruppi/operatori)***

Misure di sicurezza raccomandate

→ Implementazione di una soluzione di controllo dell'accesso alla rete

Le prese di rete situate in aree accessibili al pubblico devono essere, per quanto possibile, disattivate. Quando tali prese

sono utilizzate per la fornitura di un servizio, è necessario implementare un controllo dell'accesso alla rete.

Gli armadi e i locali tecnici devono essere chiusi a chiave.

→ Compartimentazione tra le diverse reti
Quando la rete è "piatta", senza alcun meccanismo di separazione, ogni macchina della rete può accedere a qualsiasi altra macchina. La compromissione di una di esse mette quindi a rischio l'intero sistema informativo, compresi i server critici.

È quindi necessario implementare un'adeguata separazione tra le diverse reti della nave e, più in generale, della compagnia.

→ Rafforzamento e mantenimento delle condizioni di sicurezza dei sistemi
Poiché gli hacker sfruttano vulnerabilità generalmente note per diffondersi e aumentare i propri privilegi all'interno dei sistemi informativi, un rafforzamento e un aggiornamento costante dei sistemi consentono di impedire o limitare l'avanzata di un hacker.

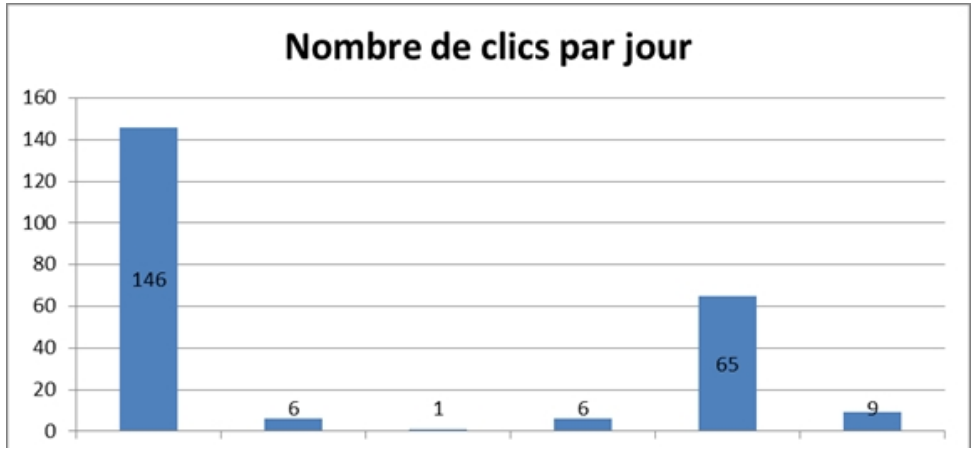
SENSIBILIZZAZIONE - PHISHING

NOME	**PHISHING – HAMECONNAGE**		
DEFINIZIONE	Tecnica utilizzata da truffatori truffatori per ottenere informazioni informazioni personali. Far credere alla vittima di rivolgersi a una terza parte di fiducia.	**OBIETTIVO**	Usurpar di di identità.
		COME	Posta elettronica.

COME REAGIRE	Per qualsiasi messaggio ricevuto,	➢ Non aprire gli allegati ➢ Non cliccare mai sui link ipertestuali ➢ Controllare l'indirizzo del mittente ➢ Controllare l'ora e la data di invio ➢ Verificare l'oggetto del messaggio ➢ Verificare che il messaggio non richieda informazioni insolite/personali ➢ Prestare attenzione ai messaggi di avviso visualizzati dalla propria casella di posta elettronica

IN CASO DI DUBBIO	➢ Non aprire gli allegati	➢ Non cliccare su alcun link proposto	➢ Non rispondere al messaggio
	Avvisare il responsabile della sicurezza dei sistemi informativi		

CASO CONCRETO	**ESERCIZIO DI PHISHING CONDOTTO IN UN GRANDE GRUPPO**



Una campagna di phishing ha preso di mira 1000 dipendenti del gruppo.

In **6 giorni**, il server "maligno" ha raccolto **233 clic**.

NOTA: il 14 e il 15 (fine settimana), il 16 giorno festivo.

Alla fine, **178 persone hanno cliccato (18%)** su uno dei link contenuti nell'e-mail trappola.

In caso di attacco reale, un solo clic avrebbe potuto compromettere l'intera azienda.

13 14 15 16 17 18

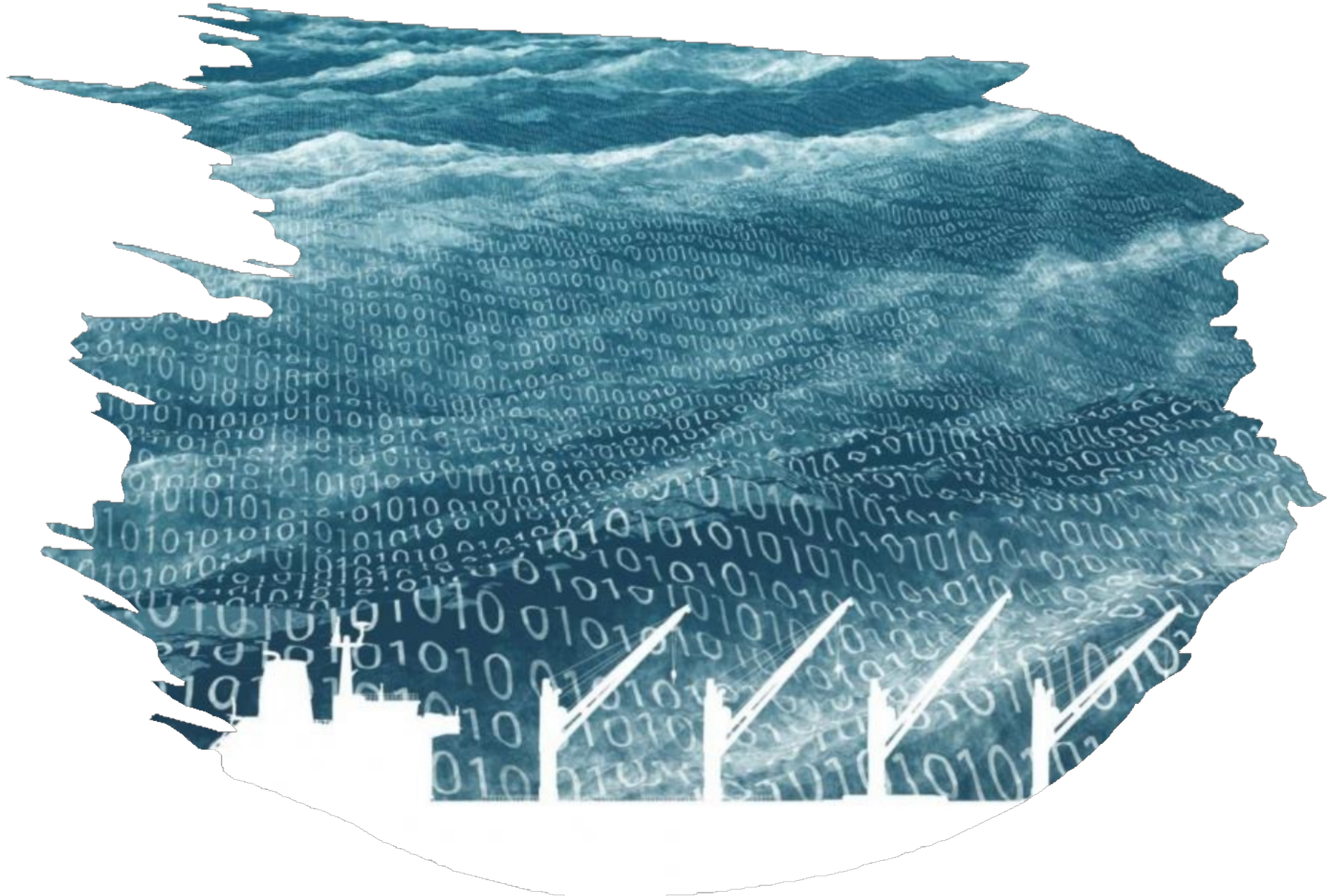
SENSIBILIZZAZIONE SSI - RANSOMWARE «LOCKY»

NOME	**LOCKY**	**TIPO**	RANSOMWARE	**DATA DI COMPARSA**	FEBBRAIO 2016
		SISTEMA INTERESSATO	SISTEMA OPERATIVO WINDOWS	**LUOGO**	EUROPA

IMPATTO	SEQUESTRO DEI VOSTRI DATI PERSONALI MEDIANTE CRITTOGRAFIA	
OBIETTIVO	RICHIESTA DI RISCATTO PER POTER RECUPERARE I DATI	
DIFFUSIONE	SI DIFFONDE TRAMITE E-MAIL TRAMITE **BOTNET** (vedi definizione)	
	ALLEGATO INFETTO CONTENUTO IN UN'E-MAIL	
METODO DI ATTACCO	RICEVIMENTO DI UN'E-MAIL CON UN ALLEGATO INFETTO:	OGGETTO (per ora): ATTN: Fattura J-XXXXXXX
		CORPO DEL MESSAGGIO: REDAZIONE CORRETTA, ALLEGATO IN FORMATO .DOC (IL PIÙ SPESSO, MA NON SOLO…)
		MITENTE: MAI LO STESSO
	ALL'APERTURA DELL'ALLEGATO I DOCUMENTI DEL MESSAGGIO VENGONO CRITTOGRAFATI (FORMATO .LOCKY)	
	IL BLOCO NOTE SI APRIRÀ PER VISUALIZZARE UNA RICHIESTA DI RISCATTO	
	I LINK WEB INDICANO LA PROCEDURA PER RECUPERARE I DATI CON L'AIUTO DI UN DECODIFICATORE (CHIAMATO LOCKY DECRYPTOR PRO, LA CUI EFFICACIA NON È PROVATA)	
SOLUZIONE	**NESSUNA AD OGGI – PERDITA TOTALE DEI DATI**	
RACCOMANDAZIONI	NON PAGARE IL RISCATTO AI RAPITORI PERCHÉ:	L'EFFICACIA DEL SOFTWARE DI DECODIFICA NON È PROVATA
		PERDITA DI DENARO
		INCORAGGIA I CYBERCRIMINALI A CONTINUARE
MISURA PREVENTIVA ATTUALE	AGGIUNTA NEL REGISTRO DI SISTEMA DI WINDOWS DI UNA CARTELLA .LOCKY SENZA DIRITTO DI MODIFICA QUESTO METODO, IN CASO DI APERTURA DI UN ALLEGATO INFETTO, BLOCCA L'INSTALLAZIONE DI LOCKY E QUINDI LA CRITTOGRAFIA DEI DATI	
DEFINIZIONE BOTNET	UN **BOTNET** (DALL'INGLESE, CONTRATTURA DI "ROBOT" E "RETE") È UNA RETE DI PROGRAMMI CONNESSI A INTERNET CHE COMUNICANO CON ALTRI PROGRAMMI SIMILI PER L'ESECUZIONE DI DETERMINATI COMPITI.	

DOMANDE?

- PAUSA



**"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."**