Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali

AGID

13 feb 2020

Indice

consultation

La consultazione pubblica relativa al presente documento è attiva dal **14 maggio** al **13 giugno 2019**. Questo documento raccoglie il testo delle Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali, disponibile per la consultazione pubblica.

CAPITOLO 1

Premessa

Le Tecnologie dell'Informazione e della Comunicazione (Information and Communication Technology, ICT) sono in rapida espansione e condizionano ormai completamente un numero crescente di settori vitali dell'economia e di servizi offerti dalle Pubbliche Amministrazioni. L'ampliamento dei settori coinvolti e delle conoscenze richieste è una conseguenza della digitalizzazione dell'economia e della dipendenza di numerose attività dai servizi digitali; molte azioni quotidiane si svolgono infatti nel cosiddetto spazio cibernetico o *cyberspace*[1]. In prospettiva la crescita dell'internet delle cose (*Internet of Things*, IoT), ossia l'insieme di dispositivi connessi in grado di svolgere operazioni nel mondo fisico, aprirà sia le attività domestiche alla dimensione cibernetica, in modo qualitativamente diverso rispetto a quanto accade attualmente. Alle nuove tecnologie si accompagnano tuttavia nuovi e crescenti rischi; tra questi particolarmente rilevante è quello cibernetico (*cyber risk*). I dispositivi, il software e le connessioni di rete che compongono lo spazio cibernetico presentano vulnerabilità tecnologiche e organizzative che possono essere sfruttate in modo malevolo, come dimostra il moltiplicarsi degli attacchi informatici che riguardano ormai i vari settori della società. Uno spazio cibernetico non sicuro costituisce una debolezza grave in una società digitalizzata, non solo per i danni diretti che gli attacchi possono arrecare alle strutture colpite, ma anche perché una diffusa percezione di insicurezza può minare il funzionamento di quei settori che si basano sulla disponibilità, sull'integrità e sulla riservatezza di dati digitali.

Il rischio cibernetico non è nuovo. Nelle fasi iniziali del processo di digitalizzazione tuttavia erano in numero limitato sia le potenziali vittime sia gli attori della minaccia. Solo i settori informatizzati (come la difesa e le telecomunicazioni) costituivano un target sufficientemente appetibile per gli attacchi cibernetici; inoltre le conoscenze e le risorse necessarie per progettare e sferrare tali aggressioni esistevano quasi esclusivamente in ambito militare e in alcuni centri di ricerca. Negli anni l'uso di dispositivi informatici e l'accesso alle reti telematiche si sono enormemente estesi, moltiplicando il numero di obiettivi. Inoltre le competenze necessarie per programmare codici malevoli sono ormai a disposizione di molte organizzazioni criminali, che sviluppano strumenti offensivi e talvolta li offrono a basso costo a un'ampia platea di clienti ed utenti. Anche ormai il cittadino e i suoi rapporti con la Pubblica Amministrazione sono divenuti nel tempo oggetto di attenzione per gli attacchi cibernetici, con la finalità di colpire e compromettere il legame di fiducia esistente tra gli stessi.

La sicurezza cibernetica dei sistemi informativi delle organizzazioni e della relativa rete di interconnessione viene assicurata dall'azione, e dal relativo coordinamento, di diverse strutture di gestione della cyber security operanti nei

[1] Il cyberspace è definito come «*l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete*», cfr. Presidenza del Consiglio dei Ministri (2013a).

diversi ambiti di competenza, tra cui i Computer Emergency Response Team (CERT[2]). Nel nostro ordinamento, come evidenziato più in dettaglio nelle successive sezioni del documento, l'attuale quadro legislativo ha determinato l'allocazione delle funzioni e dei compiti aventi rilievo per la sicurezza cibernetica a livello nazionale ad una molteplicità di attori istituzionali. In particolare, tale assetto è oggi in corso di evoluzione in risposta alle disposizioni provenienti dall'Unione Europea e che hanno portato alla costituzione del CSIRT Italia, che accoglierà al proprio interno le responsabilità e le competenze fino ad oggi ripartite tra CERT-PA e CERT Nazionale.

In accordo con gli indirizzi strategici nazionali[3], devono quindi essere create le condizioni per sviluppare un'azione integrata che metta a fattor comune le diverse attribuzioni istituzionali delineate, anche al fine di avere un maggior presidio ed assicurare una maggiore efficacia delle azioni sul territorio e nel rispetto delle esigenze delle relative *constituency*. In quest'ottica si inserisce l'esigenza di definire un modello organizzativo ed operativo per la costituzione e l'avvio di CERT regionali nell'ambito della Pubblica Amministrazione italiana, che possa delineare uno standard nazionale rispetto al quale basare ogni implementazione degli stessi su base locale, tenendo in considerazione ed indirizzando al meglio le esigenze dei singoli settori, dell'industria ed i vincoli specifici delle singole amministrazioni.

All'interno del presente documento sono illustrati gli aspetti significativi da considerare per poter avviare ed operare un CERT e che potranno essere presi a riferimento per la costituzione di CERT regionali. Tali aspetti riguardano:

- modello funzionale di riferimento;
- struttura amministrativa ed organizzativa;
- catalogo dei servizi da erogare;
- carta dei processi e matrice delle responsabilità;
- risorse necessarie, in termini di personale, informazioni (*modello dati*), modelli tecnologici e applicativi e facilities;
- requisiti di sicurezza fisica e logica da implementare;
- modalità di analisi e valutazione dei risultati raggiunti;
- opportunità di finanziamento per iniziative nel nostro Paese;
- piano di attuazione.

Nella definizione del modello sono state prese in considerazione le indicazioni e Best Practice fornite dalle organizzazioni internazionali di riferimento del settore (ENISA - *Agenzia Europea per la sicurezza delle reti e dell'informazione*; CERT/CC – *CERT Coordination Center della Carnegie Mellon University - Software Engineering Institute*; FIRST - *Forum of Incident Response and Security Teams*; TI - *Trusted Introducer*) e le pratiche attuate dal CERT-PA[4].

Il documento è organizzato nelle seguenti sezioni:

- **Sezione 1 -** *Cosa è un CERT*: presentazione degli aspetti fondamentali alla base della dell'organizzazione di un CERT e del contesto in cui lo stesso è chiamato ad operare (Cap. 4-7);
- **Sezione 2** - *Cosa fa un CERT regionale*: descrizione del modello funzionale di riferimento per un CERT regionale, con presentazione degli elementi costitutivi dello stesso in termini di servizi, processi e risorse necessarie; vengono inoltre illustrati alcuni modelli per l'analisi delle performance (metriche e indicatori) (Cap. 8-12);
- **Sezione 3** - *Come avviare un CERT regionale*: vengono inoltre forniti una panoramica sui fondi disponibili per finanziare la costituzione e l'esercizio di un CERT regionale e un possibile piano di attuazione (Cap. 13-14);
- **Appendici:** *Glossario dei termini*.

[2] Per ragioni di comodità espositiva si farà utilizzo nel resto del documento della denominazione CERT in luogo di altre con significati del tutto analoghi quali CSIRT (Computer Security Incident Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team) o SERT (Security Emergency Response Team). Si precisa tuttavia che l'utilizzo della denominazione CERT dovrebbe considerare i seguenti criteri di base: (i) l'acronimo CERT è un marchio registrato della CMU-SEI e pertanto l'utilizzo dello stesso deve essere autorizzato da tale organizzazione; (ii) la mission primaria del CERT, secondo le convenzioni internazionali associate all'utilizzo di questo acronimo, deve essere fondata sulla gestione degli incidenti di Cyber Security, anche se focalizzata su aspetti di coordinamento e supervisione.

[3] Indirizzo Operativo 5 "*Operatività delle strutture nazionali, di incident prevention, response e remediation*", Piano Nazionale per la protezione cibernetica e la sicurezza informatica, Marzo 2017.

[4] Si rimanda ai par. 2.2 e 2.3 per un elenco più dettagliato dei riferimenti considerati.

CAPITOLO 2

Riferimenti

2.1 Leggi

1. D.Lgs. 82/2005, "*Codice dell'Amministrazione Digitale*", con successive modifiche ed integrazioni
2. D.Lgs. 83/2012, "*Misure urgenti per la crescita del Paese*"
3. "*Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019-2021*" (https://pianotriennale-ict.italia.it)
4. Direttiva PCM 1 agosto 2015

2.2 Linee Guida e Standard

5. ENISA, "*Un approccio graduale alla creazione di un CSIRT*", Documento WP2006/5.1(CERT-D1/D2) (2006)
6. ENISA, "*Baseline capabilities for National / Governmental CERTs, Part 1*", Version 1.0 (2009)
7. ENISA, "*Baseline capabilities for National / Governmental CERTs, Part 2, Policy Recommendations*", Version 1.0 (2010)
8. ENISA, "*ENISA's recommendations on baseline capabilities*", Update, December 2014 (2014)
9. ENISA, "*NIS Directive and national CSIRTs*", Info Note, February 2016 (2016)
10. ENISA, "*CERT Operational Gaps and Overlaps*", Report, December 2011 (2011)
11. CMU-SEI, "*Handbook for Computer Security Incident Response Teams*", (2003)
12. CMU-SEI, "*Organizational Models for CSIRTs*", (2003)
13. FIRST, "*Computer Security Incident Response Team Services Framework*", Version 1.1 (2017)

CAPITOLO 3

Definizioni e Acronimi

Nel Glossario è riportato un elenco esaustivo di nozioni e termini utili per una corretta comprensione dei contenuti presentati all'interno di questo documento.

Tabella 3.1: Acronimi

Acronimo	Descrizione
AGID	Agenzia per l'Italia Digitale
CERT	Computer Emergency Response Team
CERT/CC	CERT/CC – CERT Coordination Center CMU-SEI
CMU-SEI	Carnegie Mellon University - Software Engineering Institute
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CSIRT	Computer Security Incident Response Team
ENISA	Agenzia Europea per la sicurezza delle reti e dell'informazione
FIRST	Forum of Incident Response and Security Teams
IOC	Indicators of Compromise
IRPA	Incident Response Pubblica Amministrazione
ISAC	Information Sharing and Analysis Center
NATO	North Atlantic Treaty Organization
ONU	Organizzazione delle Nazioni Unite
OSCE	Organizzazione per la Sicurezza e la Cooperazione in Europa
PP.AA.	Pubbliche Amministrazioni
PAC	Pubbliche Amministrazioni Centrali
PAL	Pubbliche Amministrazioni Locali
SOC	Security Operation Center
TI	Trusted Introducer

CAPITOLO 4

Contesto

4.1 Quadro di riferimento nazionale

L'architettura nazionale per la cyber security ha conosciuto in tempi recenti importanti interventi di modifica mirati a razionalizzare e potenziare progressivamente le capacità di difesa cibernetica del Paese. Nello specifico, nel 2013, con il cd. "Decreto Monti"[5], l'Italia ha delineato per la prima volta la sua architettura di sicurezza cibernetica, provvedendo a sistematizzare le molteplici competenze di settore distribuite tra diversi attori istituzionali. Ciò ha determinato una crescita delle capacità cyber nazionali, opportunamente guidata dagli atti della Presidenza del Consiglio dei Ministri sia di indirizzo strategico - "*Quadro strategico nazionale per la protezione dello spazio cibernetico*", con lo scopo di individuare strumenti e procedure per potenziare le capacità cibernetiche del Paese - che operativo - il "*Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*"- che traduce in indirizzi operativi le previsioni del Quadro strategico.

Il 17 febbraio 2017 è stato adottato il Decreto del Presidente del Consiglio dei Ministri "*Direttiva recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*" (cd."Decreto Gentiloni") che, nel sostituire quello del 2013, ha posto il Dipartimento Informazioni per la Sicurezza (DIS) al centro della governance nazionale in materia di cyber security. Il DIS presiede così il Nucleo per la Sicurezza Cibernetica (NSC), deputato all'adozione di misure di coordinamento per la gestione di incidenti cyber di particolare rilevanza e per la dichiarazione di crisi cibernetica nazionale, rispetto alla quale è chiamato a tenere costantemente informato il Presidente del Consiglio dei Ministri.

Più in dettaglio sono riportate ed illustrate a seguire le principali strutture organizzative che compongono l'architettura nazionale per la cyber security e che costituiscono i punti di riferimento essenziali per un CERT che opera all'interno del territorio italiano.

CISR (Comitato Interministeriale per la Sicurezza della Repubblica)[6]

Organo istituzionale di raccordo politico-strategico sul tema della sicurezza nazionale, con compiti di consulenza, proposta e deliberazione. È presieduto dal Presidente del Consiglio dei Ministri e composto, oltre che dall'Autorità delegata, ove istituita, dai Ministri degli Affari Esteri e Cooperazione Internazionale, dell'Interno, della Giustizia, della Difesa, dell'Economia e delle Finanze, dello Sviluppo Economico. Il Direttore Generale del DIS svolge le funzioni di

[5] D.P.C.M. 24 gennaio 2013.

[6] Fonte: https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/comitato-interministeriale-per-la-sicurezza-della-repubblica-cisr.html

segretario del Comitato. Il CISR svolge, inoltre, compiti di supporto al Presidente del Consiglio in caso di situazioni di crisi, anche per la sicurezza cibernetica.

DIS (Dipartimento Informazioni per la Sicurezza)[7]

Organismo di cui si avvalgono il Presidente del Consiglio dei Ministri e l'Autorità delegata, ove istituita, per l'esercizio delle loro competenze, al fine di assicurare piena unitarietà nella programmazione della ricerca informativa del Sistema di informazione per la sicurezza nonché nelle analisi e nelle attività operative dei servizi di informazione per la sicurezza. Nell'architettura nazionale cyber, il DIS ha un ruolo centrale ed è chiamato a definire ed attuare la governance in materia, sia a livello nazionale (anche attraverso la presidenza del Nucleo per la Sicurezza Cibernetica), sia in ambito UE, NATO, OSCE e ONU. In coerenza con tale framework, il Decreto legislativo 18 maggio 2018, n. 65, di recepimento della Direttiva NIS (si veda par. 4.2.1) prevede che il Dipartimento assuma il ruolo di *Punto di Contatto Unico NIS*, con il compito di coordinare, a livello nazionale, le questioni relative alla sicurezza delle reti e dei sistemi informativi e di svolgere una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità competenti NIS con quelle degli altri Stati Membri nonché con il Gruppo di cooperazione, istituito presso la Commissione Europea.

NSC (Nucleo per la Sicurezza Cibernetica)[8]

Organo costituito presso il DIS, a supporto del Presidente del Consiglio dei Ministri e del CISR, nella materia dello spazio cibernetico, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento, svolgendo funzioni di raccordo tra le diverse componenti dell'architettura istituzionale cyber. È presieduto da un Vice Direttore Generale del DIS ed è composto dal Consigliere militare del Presidente del Consiglio dei Ministri, da rappresentanti del DIS, dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI), dei Ministeri degli Affari Esteri e Cooperazione internazionale, dell'Interno, della Giustizia, della Difesa, dell'Economia e delle Finanze, dello Sviluppo Economico nonché del Dipartimento della Protezione Civile e dell'Agenzia per l'Italia Digitale; in caso di crisi, partecipano anche rappresentanti dei Ministeri della Salute, delle Infrastrutture e Trasporti nonché del Dipartimento dei Vigili del Fuoco, del Soccorso pubblico e della Difesa civile e dell'Ufficio del Consigliere militare del Presidente del Consiglio dei Ministri.

CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)[9]

Il CNAIPIC è incaricato della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale. Si avvale di tecnologie di elevato livello e di personale altamente qualificato, specializzato nel contrasto del cyber crime, che ha maturato concreta esperienza anche nei settori del cyber terrorismo e dello spionaggio industriale.

L'operatività del CNAIPIC è soddisfatta attraverso l'esercizio di un Settore Operativo e di un Settore Tecnico. Il Settore Operativo supporta le funzioni di: Sala Operativa, Intelligence e Analisi. Il Settore Tecnico è invece deputato alla gestione ed all'esercizio dell'infrastruttura tecnologica del CNAIPIC e dei collegamenti telematici con le Infrastrutture Critiche convenzionate, ai processi di individuazione, testing ed acquisizione di risorse strumentali ed alla pianificazione di cicli di formazione ed aggiornamento del personale.

CIOC (Comando Interforze per le Operazioni Cibernetiche)[10]

Il CIOC è una sezione dello Stato maggiore della Difesa con funzioni di cyber defense e cyber network defense. Il Comando è adibito alla verifica dell'integrità e delle disponibilità delle reti e dei dati, nonché all'attività di Vulnerability Assessment e Penetration Test.

All'interno del CIOC è costituito il CERT della Difesa italiana, che si articola su due pilastri fondamentali: il *CERT Coordination Center* ed il *CERT Technical Center*, che svolgono congiuntamente attività di indirizzo, coordinamento e informazione verso gli analoghi organi costituiti presso le Forze armate. Infatti ogni singola Forza armata ha un suo CERT che lavora in maniera coordinata con il CERT Difesa, sovrapposto agli altri non in termini organici, ma funzionali. Infatti, in caso di situazioni di crisi, il CERT Difesa assume il coordinamento delle attività da porre in essere.

[7] Fonte: https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html
[8] Fonte: https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html
[9] Fonte: https://www.commissariatodips.it/profilo/cnaipic.html
[10] Fonte: https://www.difesa.it/Protocollo/AOO_Difesa/SMD/Pagine/SCIOC.aspx

Autorità competente NIS[11]

Autorità incaricata di attuare il decreto di recepimento della Direttiva NIS, vigilando sulla sua applicazione nel settore di competenza ed esercitando le relative potestà ispettive e sanzionatorie. Nell'ordinamento nazionale le autorità coinvolte sono:

- il Ministero dello Sviluppo Economico per il settore energetico, per le infrastrutture di scambio del traffico telematico (le cosiddette infrastrutture digitali) e per i servizi digitali;
- il Ministero dei Trasporti e delle infrastrutture per il settore dei trasporti;
- il Ministero dell'Economia e delle Finanze, in collaborazione con la Banca d'Italia e con la Commissione Nazionale per le Società e la Borsa (CONSOB), per il settore bancario e delle infrastrutture dei mercati finanziari;
- il Ministero della Salute e, per quanto di competenza, le Regioni e le Province autonome di Trento e Bolzano per l'attività di assistenza sanitaria;
- il Ministero dell'Ambiente e, per quanto di competenza, le Regioni e le Province autonome di Trento e Bolzano per il settore di fornitura e distribuzione dell'acqua potabile.

CERT-PA[12]

Il CERT-PA, operativo dal 3 marzo 2014, opera all'interno di AGID e ha il compito di supportare le Pubbliche Amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica. In conformità con le regole tecniche per la sicurezza informatica delle PA, il CERT-PA è in grado di fornire alle amministrazioni richiedenti:

- servizi di analisi e di indirizzo, finalizzati a supportare la definizione dei processi di gestione della sicurezza;
- servizi proattivi, relativi alla raccolta e l'elaborazione di dati significativi ai fini della sicurezza cibernetica, l'emanazione di bollettini e segnalazioni di sicurezza;
- servizi reattivi, per poter gestire gli allarmi di sicurezza;
- servizi di formazione e comunicazione per promuovere la cultura della sicurezza cibernetica.

CERT-N[13]

Il CERT Nazionale, operante presso il Ministero dello Sviluppo Economico, sulla base di un modello cooperativo pubblico-privato, supporta cittadini e imprese attraverso azioni di sensibilizzazione, di prevenzione e di coordinamento della risposta ad eventi cibernetici su vasta scala.

I principali obiettivi del CERT Nazionale sono:

- fornire informazioni tempestive su potenziali minacce informatiche che possano recare danno a imprese e cittadini;
- incrementare la consapevolezza e la cultura della sicurezza;
- cooperare con istituzioni analoghe, nazionali ed internazionali, e con altri attori pubblici e privati coinvolti nella sicurezza informatica promuovendo la loro interazione;
- facilitare la risposta ad incidenti informatici su larga scala;
- fornire supporto nel processo di soluzione di crisi cibernetica.

CSIRT Italia[14]

Il D.lgs. 65/2018 di recepimento all'interno dell'ordinamento nazionale italiano della Direttiva NIS ha previsto l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico Computer Security Incident Response Team, detto "CSIRT Italia", che svolgerà i compiti e le funzioni degli attuali CERT-PA e CERT-N. Il CSIRT Italia, sulla base di

[11] Fonte: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/Dlgs-65_2018-NIS.pdf
[12] Fonte: https://www.cert-pa.it/
[13] Fonte: https://www.certnazionale.it/
[14] Fonte: https://www.csirt-ita.it/

un modello cooperativo pubblico-privato, avrà compiti di natura tecnica finalizzati a supportare la PA, i cittadini e le imprese attraverso azioni di sensibilizzazione, prevenzione e coordinamento della risposta ad eventi cibernetici su vasta scala, anche in cooperazione con gli altri CERT europei. In particolare, secondo quanto disposto dal decreto di recepimento, avrà i seguenti compiti:

- definire le procedure per la prevenzione e la gestione degli incidenti informatici;
- ricevere le notifiche di incidente, informandone il DIS, quale punto di contatto unico e per le attività di prevenzione e preparazione a eventuali situazioni di crisi e di attivazione delle procedure di allertamento affidate al NSC;
- fornire al soggetto che ha effettuato la notifica le informazioni che possono facilitare la gestione efficace dell'evento;
- informare gli altri Stati membri dell'UE eventualmente coinvolti dall'incidente, tutelando la sicurezza e gli interessi commerciali dell'operatore di servizi essenziali o del fornitore di servizi digitali nonché la riservatezza delle informazioni fornite;
- garantire la collaborazione nella rete di CSIRT, attraverso l'individuazione di forme di cooperazione operativa, lo scambio di informazioni e la condivisione di best practices.

La rilevanza dei CERT e dei servizi che questi possono fornire, è evidenziata anche a livello di strategia nazionale. In quest'ottica, il *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica* rimarca le esigenze di potenziamento degli attuali CERT e la necessità di istituirne di nuovi. In particolare, si sottolinea come l'approntamento di capacità di prevenzione e reazione ad eventi cibernetici richieda lo sviluppo dei CERT quali soggetti erogatori di servizi di assistenza tecnica, ricerca e sviluppo, formazione e informazione per i rispettivi utenti, pubblici e privati. Organismi, dunque, che siano in grado di assicurare un'effettiva capacità di assistenza e supporto attivo alla propria constituency in caso di evento cibernetico.

4.2 Impianto normativo applicabile ai CERT

4.2.1 Direttiva NIS (Directive on Security of Network and Information Systems)

La Direttiva 2016/1148 (c.d. "Direttiva NIS"), recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea, rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza cibernetica e delinea le azioni in capo agli Stati membri volte a migliorare le capacità di sicurezza dei singoli Paesi dell'Unione Europea. La Direttiva ambisce inoltre ad aumentare il livello di collaborazione nella prevenzione delle minacce cibernetiche e nell'implementazione di misure di risposta agli attacchi cyber. All'interno della Direttiva ampia rilevanza è assegnata al ruolo esercitato dai CERT, già esistenti o che verranno istituiti dagli Stati membri, cui saranno affidate funzioni di responsabilità del monitoraggio degli incidenti a livello nazionale.

Come si è visto, attraverso il D. Lgs. 65/2018, che ha recepito la Direttiva NIS all'interno dell'ordinamento nazionale italiano, è stato istituito il CSIRT Italia.

Con la Direttiva NIS il legislatore europeo ha altresì previsto che gli Stati membri si dotino di un'organizzazione in grado di vincolare gli operatori di servizi ritenuti essenziali e i fornitori di servizi digitali per l'economia all'adozione di stringenti misure di protezione. Come precedentemente illustrato, nel modello istituzionale scelto dal governo italiano, sono state designati 5 Ministeri quali Autorità Competenti NIS (Sviluppo Economico, Infrastrutture e Trasporti, Economia, Salute e Ambiente) ciascuno responsabile di specificare per uno o più settori rientrati nelle proprie aree di competenza gli operatori di servizi essenziali, definire le misure di sicurezza minime, vigilare sulla loro applicazione anche mediante ispezioni, comminare sanzioni.

Tra gli obblighi a carico degli operatori vi sarà quello di notifica"*senza ingiustificato ritardo*" a fronte di incidenti informatici con impatto rilevante sui servizi forniti. In tale ottica, tali organizzazioni saranno chiamate a sviluppare maggiori competenze e servizi specialistici per contrastare le minacce cibernetiche, che stanno crescendo in numero

e sofisticatezza, ma non tutti gli attori che compongono il tessuto economico e sociale possiedono dimensioni, risorse umane, tecniche ed economiche sufficienti per raggiungere tale risultato. La possibilità di accedere ad infrastrutture e risorse specializzate, messe a disposizione dai CERT, costituisce un elemento chiave per l'innalzamento del livello di sicurezza collettivo.

4.2.2 Ulteriori fonti

L'impianto normativo e regolamentare precedentemente illustrato si arricchisce di ulteriori prescrizioni ed indicazioni nelle forme di leggi e "*soft law*", sia a livello internazionale che nazionale, che devono essere debitamente tenute in considerazione ai fini dell'operato dei CERT. Tali fonti presentano un ambito di applicazione generale sui temi di cyber security ma anche più specifici su ambiti come l'analisi forense, le modalità di contrasto al cyber crime, il cyber warfare e le attività di intelligence.

Una lista, non esaustiva, dei provvedimenti più significativi in materia, è fornita a seguire, riportando una breve descrizione degli stessi ed alcuni riferimenti utili per un loro eventuale approfondimento.

Fonti internazionali

Regolamento CE n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004[15]

Con tale regolamento è stata istituita l'Agenzia Europea per la sicurezza delle reti e dell'informazione (ENISA, European Network and Information Security Agency), con sede a Heraklion (Creta), con la missione di assistere la Commissione Europea nel compito di assicurare un adeguato livello di sicurezza delle reti e dell'Informazione. L'Agenzia contribuisce allo sviluppo di una cultura della sicurezza ICT a beneficio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico dell'Unione Europea. L'Agenzia aiuta la Commissione, gli Stati membri e gli operatori economici a rispettare i requisiti relativi alla sicurezza delle reti e dell'informazione, ivi compresi i requisiti previsti dalla vigente e dalla futura normativa comunitaria. L'Agenzia è infine centro di consulenza per gli Stati membri e le istituzioni dell'Unione Europea su questioni relative alla sicurezza delle reti e dell'informazione. Al fine di assicurare la realizzazione degli obiettivi che le sono stati fissati, l'Agenzia è chiamata a svolgere i seguenti compiti:

- raccogliere ed analizzare i dati relativi ai rischi emergenti e agli incidenti connessi con la sicurezza;
- cooperare con i diversi soggetti che operano nel settore, in particolare con le imprese operanti a livello dell'Unione europea e/o a livello mondiale;
- svolgere attività di sensibilizzazione e di promozione dei metodi di valutazione e di gestione dei rischi;
- seguire l'evoluzione delle norme sulla sicurezza delle reti e dell'informazione per prodotti e servizi.

Il Regolamento è stato abrogato dal *Regolamento CE n. 526 del 21 maggio 2013*, che ha riconfermato il ruolo di ENISA e raffinato ulteriormente il mandato e il campo di azione dell'Agenzia.

Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio[16]

La Direttiva 2013/40 è stata adottata per perseguire il ravvicinamento del diritto penale degli Stati membri, oltre all'obiettivo, già fatto proprio dalla decisione quadro richiamata, di favorire la cooperazione tra le autorità giudiziarie e di polizia nel contrasto alla criminalità informatica. Gli Stati sono chiamati ad incriminare la condotta di intercettazione illecita di comunicazioni informatiche o telematiche, e ad introdurre la previsione della reclusione non inferiore nel massimo a due anni per le condotte di «fabbricazione, vendita, approvvigionamento per l'uso, importazione e distribuzione o messa a disposizione in altro modo» di software destinati o modificati principalmente al fine di commettere uno dei reati previsti dalla direttiva nonché di «password e codici d'accesso che permettono di accedere in tutto o in parte a un sistema di informazione» per la commissione degli stessi reati.

[15] Per consultare il testo del Regolamento: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32013R0526
[16] Per consultare il testo della Direttiva: https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A32013L0040

Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio (23 luglio 2014) in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE[17]

Il Regolamento 910/2014 sull'identità digitale - meglio noto come Regolamento eIDAS (*electronic IDentification Authentication and Signature)* - ha l'obiettivo di fornire un insieme di regole a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri ed ha piena efficacia dal 1 Luglio 2016. Il regolamento eIDAS fornisce una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e Pubbliche Amministrazioni e incrementa la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'Unione Europea. In particolare il Regolamento:

- fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;
- stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;
- istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web.

Rispetto ai sistemi di identificazione elettronica, eIDAS infine prevede che ciascuno stato membro possa notificare i sistemi di identificazione elettronica forniti ai cittadini e alle aziende per consentire un reciproco riconoscimento.

Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio (27 aprile 2016), relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio[18].

La Direttiva 680, emanata assieme al GDPR e alla direttiva 681 (vedere punto successivo) all'interno del pacchetto di riforma UE sulla protezione dei dati, è relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché salvaguardia e prevenzione di minacce alla sicurezza pubblica.

La Direttiva stabilisce che il trattamento può essere effettuato solo da una autorità competente, come titolare dello stesso, ovvero qualsiasi autorità pubblica competente nelle materie oggetto del trattamento o qualsiasi altro organismo o entità incaricati dallo Stato di esercitare l'autorità pubblica e i poteri pubblici. Un'autorità competente, per poter perseguire un reato, può effettuare indagini ovunque, quindi può raccogliere dati personali online e offline con gli strumenti più diversi. Le modalità con cui garantire la sicurezza del trattamento dei dati personali sono puntualmente elencate all'Art. 29 della Direttiva (es. controllo dell'accesso alle attrezzature, controllo dei supporti di dati, controllo della conservazione, controllo dell'utente, controllo dell'accesso ai dati, controllo della trasmissione, controllo dell'introduzione, controllo del trasporto).

Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio (27 aprile 2016) sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi[19]

La Direttiva 681 stabilisce le modalità di utilizzo dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. In particolare, i soggetti che intervengono nel trattamento non sono solo le autorità ma anche i vettori aerei che forniscono i PNR. I dati del PNR raccolti sono numerosi – sono elencati nell'Allegato della Direttiva - e legati inscindibilmente all'individuo. La Direttiva indica agli Stati membri l'applicazione delle stesse norme nazionali di attuazione degli articoli 21 e 22 della decisione quadro 2008/977/GAI per proteggere i dati dei PNR. Tale decisione, tuttavia, in Italia non è mai stata attuata, quindi si renderà necessario scrivere la norma ex novo. I dati dei PNR dovranno, inoltre, essere conservati per un periodo di cinque anni e, dopo sei mesi, resi (pseudo)anonimi mediante la mascheratura di alcuni elementi.

[17] Per consultare il testo del Regolamento: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32014R0910
[18] Per consultare il testo della Direttiva: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ITA
[19] Per consultare il testo della Direttiva: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016L0681

Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti[20]

La proposta di Direttiva, datata 13 settembre 2017, rinforza la decisione quadro 2001/413/GAI del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ritenuta non più pienamente idonea a far fronte alle nuove sfide e agli sviluppi tecnologici, quali le valute virtuali e i pagamenti tramite dispositivi mobili. La proposta persegue tre obiettivi specifici che affrontano i problemi individuati: l'istituzione di un quadro politico/giuridico chiaro, solido e tecnologicamente neutro, l'eliminazione degli ostacoli operativi che intralciano le indagini e le azioni penali ed il miglioramento della prevenzione.

Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cyber security su vasta scala[21]

Secondo la Raccomandazione 1584/2017 gli Stati membri e le istituzioni dell'UE dovrebbero istituire un quadro di risposta alle crisi di cyber security comune.

Il quadro dovrebbe individuare i soggetti interessati, le istituzioni dell'UE e le autorità degli Stati membri competenti a tutti i livelli necessari — tecnico, operativo, strategico/politico — ed elaborare, ove necessario, procedure operative standard che definiscano le modalità di nell'ambito dei meccanismi UE di gestione delle crisi. Le autorità competenti degli Stati membri dovrebbero collaborare per specificare ulteriormente i protocolli per la condivisione delle informazioni e la cooperazione. Inoltre, gli Stati membri dovrebbero provvedere affinché i meccanismi nazionali di gestione delle crisi reagiscano in modo adeguato agli incidenti di cyber security e creare le procedure necessarie per la cooperazione a livello dell'UE.

Risoluzione 2341 (2017) sulla protezione delle infrastrutture critiche da attacchi terroristici[22]

Con la risoluzione 2341 del 13 Febbraio 2017, l'ONU ha acquisito tra i propri obiettivi prioritari la sicurezza delle infrastrutture critiche – nello specifico quella dell'energia - in relazione ad Internet. In particolare, gli stati membri delle Nazioni Unite sono stati incoraggiati a coordinarsi fra loro tramite lo scambio reciproco di informazioni relative ad attacchi perpetrati nel web e a favorire la collaborazione tra Stati e tra le autorità a vario titolo coinvolte, anche attraverso il rafforzamento dell'interazione tra il settore pubblico e privato.

In particolare, gli Stati membri sono invitati a considerare lo sviluppo o l'ulteriore miglioramento delle loro strategie per la riduzione dei rischi per le infrastrutture critiche da attacchi terroristici, che dovrebbero includere, tra l'altro:

- l'esplorazione di modalità per scambiare informazioni pertinenti e cooperare attivamente alla prevenzione, alla protezione, alla mitigazione, alla preparazione, all'indagine, alla risposta o al recupero da attacchi terroristici previsti o commessi contro infrastrutture critiche;
- il rafforzamento dei partenariati nazionali, regionali e internazionali con le parti interessate, sia pubbliche che private, a seconda delle opportunità, per condividere informazioni e esperienze per prevenire, proteggere, mitigare, indagare, rispondere e recuperare da eventuali danni determinati da attacchi terroristici sulle infrastrutture critiche, anche attraverso la formazione congiunta e l'utilizzo o la creazione di reti di comunicazione o di emergenza pertinenti.

Fonti nazionali

Art. 615 ter codice penale "accesso abusivo sistema informatico"[23]

L'art. 615 introdotto dalla legge n° 547 del 1993 rende penalmente perseguibile l´accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza o il mantenimento in esso contro la volontà espressa o tacita dell´avente diritto. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico

[20] Per consultare il testo della proposta: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52017PC0489
[21] Per consultare il testo della Raccomandazione: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32017H1584
[22] Per consultare il testo della risoluzione: http://unscr.com/en/resolutions/2341
[23] Per consultare il testo dell'articolo: https://www.commissariatodips.it/approfondimenti/hacking/approfondimenti-normativi.html

ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Legge 18 marzo 2008, n. 48 «Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno»[24]

Grazie alla legge 48 del 18 marzo 2008 è entrata in vigore anche in Italia la Convenzione di Budapest del 2001 sulla criminalità informatica, approvata dal Parlamento il 27 febbraio 2008. La Convenzione ha come primo obiettivo la persecuzione di tutti gli atti criminali perpetrati attraverso l'uso del computer e di internet, allargando, quindi, gli orizzonti del problema; infatti, ad essere nel mirino sono tutti i reati che violano i diritti d'autore (il cosiddetto copyright), le frodi, la pedopornografia e la sicurezza delle reti. In ogni caso tutti i reati sono punibili anche se le prove raccolte sono in forma elettronica. È prevista in tal senso una stretta collaborazione tra gli Stati sottoscrittori, che dovrà essere la più ampia possibile e dovrà rispettare gli accordi internazionali.

La legge 48 non si limita a ratificare il documento di base, perché prevede anche l'adeguamento della nostra normativa in tale settore alla luce della Convenzione. Per quanto riguarda la pena, si va dai sei mesi a tre anni di reclusione per chi cancella, distrugge, deteriora, altera o sopprime informazioni, dati o programmi informatici altrui, per arrivare a rischiare dai tre agli otto anni di reclusione, se gli stessi atti sono diretti verso sistemi pubblici. Comunque, è previsto che tutte le pene possano subire un aumento, qualora a commettere il reato sia un operatore del sistema. Nel codice di procedura penale, invece, sono state inserite nuove norme sulle investigazioni e le acquisizioni di prove, che autorizzano l'autorità giudiziaria, ad esempio, al sequestro di oggetti di corrispondenza, anche se inoltrati per via telematica, presso chi fornisce i servizi postali, telegrafici, telematici o di telecomunicazioni. In seguito all'entrata in vigore della legge il Codice Penale è stato oggetto di importanti adeguamenti, così come il Codice della Privacy. Ulteriori modifiche sono state apportate al D.Lgs. 231/01 relativo alla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, mediante l'introduzione dell'articolo sui delitti informatici e sul trattamento illecito di dati (D.lgs. 231/01).

Circolare AGID 2/18.04.2017: Misure minime sicurezza ICT PA, circolare sostitutiva[25]

La circolare AGID n. 2 del 18 Aprile 2017, sostituendo integralmente la precedente circolare n. 1/2017 del 17 marzo 2017, recante: «*Misure minime di sicurezza ICT per le pubbliche amministrazioni (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)*», è volta ad indicare alle Pubbliche Amministrazioni italiane le misure minime per la sicurezza ICT da adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi. Tali misure consistono in controlli di natura tecnologica, organizzativa e procedurale, con tre livelli di attuazione:

- livello 1: obbligatorio per ogni Pubblica Amministrazione;
- livello 2: il livello minimo è obbligatorio per ogni Pubblica Amministrazione;
- i livelli successivi richiedono sistemi di protezione più completi, riguardando in particolare le organizzazioni maggiormente esposte a rischi per via della criticità delle informazioni trattate o servizi erogati.

Si riportano infine a seguire alcune importanti sentenze nel nostro ordinamento che hanno fornito orientamenti decisivi sull'interpretazione di alcune azioni nell'ambito della gestione della protezione dei dati.

Corte di Cassazione, Sezione VI Penale, Sentenza 4 ottobre - 14 dicembre 1999, n. 3067[26]

La Cassazione, con la sentenza n. 3067 del 1999, ha individuato il sistema informatico in tutte quelle apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione di tecnologie informatiche. Più tecnicamente la sentenza della Cassazione, sez. V penale, del 2 luglio 1998, ha individuato il sistema informatico"*in un apparato elettronico in grado di elaborare un elevato numero di dati/informazioni opportunamente codificato e*

[24] Per consultare il testo della legge: http://www.parlamento.it/parlam/leggi/08048l.htm
[25] Per consultare il testo della circolare: http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg
[26] Per consultare la sentenza: http://www.penale.it/giuris/cass_012.htm

capace di produrre come risultato un altro insieme di dati/informazioni codificato in maniera leggibile grazie ad un programma in grado di far cambiare lo stato interno dell'apparato e di variarne, all'occorrenza, il risultato". La caratteristica del sistema informatico è, quindi, la programmabilità e la variabilità dei risultati.

Telematico, invece, è il metodo di trasmissione e circolazione a distanza dei dati o delle informazioni, metodo che presuppone il collegamento tra due sistemi informatici (come può essere anche il sistema bancomat).

Corte di Cassazione, Sezioni Unite - Sentenza 26 marzo 2015 n. 17325[27]

Con tale sentenza, la Corte di Cassazione penale, a Sezioni Unite, ha risolto il contrasto giurisprudenziale relativo alla competenza territoriale del reato di cui all'art. 615-ter del codice penale. Secondo la Suprema Corte "*l'ingresso o l'introduzione abusiva, . . . , vengono ad essere integrati nel luogo in cui l'operatore materialmente digita la password di accesso o esegue la procedura di login, che determina il superamento delle misure di sicurezza apposte dal titolare del sistema, in tal modo realizzando l'accesso alla banca-dati*". Considerato che il reato si perfeziona nel momento e nel luogo dell'accesso o della permanenza al sistema informatico (non essendo necessaria la lettura dei dati protetti), il "*luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter cod. pen., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente*", che di fatto coincide col luogo nel quale si effettua la ricerca delle prove.

Corte di Cassazione, Sezioni Unite - Sentenza 7 febbraio 2012, n. 4694[28]

Le Sezioni unite penali della Corte di Cassazione con la sentenza n. 4694 hanno risolto una complessa questione interpretativa inerente la configurabilità del reato di accesso abusivo ai sistemi informatici o telematici che da tempo divideva diverse Sezioni della medesima Corte. La controversia interpretativa si incentra sulla configurabilità del reato nel caso in cui un soggetto, legittimamente ammesso ad un sistema informatico o telematico, vi operi per conseguire finalità illecite. La Corte ha precisato che è abusivo qualsiasi accesso dovuto a ragioni diverse da quelle per le quali è stata concessa l'autorizzazione. La Suprema Corte precisa che per la configurazione del reato non ha alcun rilievo lo scopo che ha motivato l'accesso, per cui l'uso delle informazioni acquisite (che può eventualmente configurare reati diversi) è cosa diversa dal motivo che spinge a commettere il reato, motivo che può essere rilevatore del superamento dei limiti dell'autorizzazione all'accesso del sistema. La semplice lettura di dati o di informazioni già stampate da altri, invece, non configura il reato in questione, in quanto l'agente non accede al sistema, bensì prende cognizione di dati al di fuori dello stesso sistema. In presenza di dati riservati, tuttavia, potrebbero essere configurabili altre ipotesi di reato.

Corte di Cassazione, Sezione V Penale, Sentenza 26 ottobre 2012 n. 42021[29]

La sentenza n. 42021/2012 ha tracciato i confini corretti del "domicilio informatico" disciplinato dall'art. 615-ter del codice penale. La Corte ha sottolineato che per "domicilio informatico" si intende lo spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, a cui viene estesa la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Tale tutela non riguarda solo i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma è offerta in maniera più ampia.

Corte di Cassazione, Sezione V Penale, Sentenza 12 novembre 2012, n. 43755[30]

Con la sentenza n. 43755/12 la Corte di cassazione ha stabilito un importante principio di diritto secondo il quale clonare carte di pagamento tramite "manipolazione dello sportello bancomat configura il reato di accesso abusivo a sistema informatico aggravato dalla violenza sulle cose. La Corte, infatti, ha stabilito che le carte di credito e debito costituiscono un sistema informatico capace di elaborare dati nel momento in cui si connettono all'apparecchiatura POS. L'accesso abusivo, quindi, non è solo quello al chip della carta ma anche al sistema informatico bancario che autentica l'utente grazie ai dati memorizzati sulla carta. La Suprema Corte ha anche precisato che il sistema finanziario ha natura di pubblico interesse, ed infine che la manomissione provoca un funzionamento anomalo e non voluto dall'utente legittimo, cosa che va ad integrare il requisito della «violenza sulle cose», aggravante del reato stesso.

[27] Per consultare la sentenza: https://www.penalecontemporaneo.it/upload/1430293136SU_17325_15.pdf
[28] Per consultare la sentenza: https://www.penalecontemporaneo.it/upload/1361977389Cass%20201204694.pdf
[29] Per consultare la sentenza: https://associazionecindi.files.wordpress.com/2012/11/cass-pen-sentenza-42021-12.pdf
[30] Per consultare la sentenza: https://www.penalecontemporaneo.it/upload/1430293136SU_17325_15.pdf

4.3 Organismi a supporto della Cyber Security

Oltre agli attori istituzionali precedentemente delineati, un CERT, nel corso della sua operatività, può interagire, per mandato o su base volontaria, con una pluralità di organizzazioni ed entità che operano a livello istituzionale e/o nell'ambito della ricerca e della promozione della cyber security a livello nazionale ed internazionale sia con l'intento di accreditarsi per entrare a far parte di network specifici che per acquisire ulteriori competenze.

4.3.1 Organizzazioni CERT

CERT-EU[31]

CERT EU è il team permanente di risposta alle emergenze informatiche per le istituzioni, le agenzie e gli organismi dell'Unione Europea. Il team è composto da esperti di sicurezza informatica delle principali istituzioni dell'UE (Commissione europea, Segretario Generale del Consiglio, Parlamento Europeo, Comitato delle Regioni, Comitato Economico e Sociale). Il CERT EU collabora strettamente con gli altri CERT degli Stati membri e con società specializzate nella sicurezza informatica. La sua constituency è composta da tutte le Istituzioni ed Agenzie dell'Unione Europea.

CERT-GARR[32]

CERT specializzato nella prevenzione e gestione degli incidenti di sicurezza informatica che coinvolgono gli enti collegati alla rete GARR (Rete Italiana dell'Università e della Ricerca). Offre alla sua comunità una vasta gamma di servizi, alcuni dei quali strettamente legati alla gestione e all'ampliamento della rete, ed altri, più orientati all'utilizzo della rete da parte degli utenti finali.

Con riferimento ai servizi in ambito cyber security il CERT assiste gli utenti nella gestione di incidenti di sicurezza informatica e nella realizzazione di misure di prevenzione. Il servizio diffonde informazioni sulle vulnerabilità più comuni e sugli strumenti di sicurezza da adottare; emana direttive sui requisiti minimi di sicurezza per le macchine con accesso alla rete e ne verifica il rispetto. Inoltre può essere richiesta dai referenti tecnici locali delle organizzazioni connesse a GARR l'esecuzione di test vulnerabilità sulle macchine della rete (SCARR, Scansioni Ripetute a Richiesta).

4.3.2 Associazioni / Centri di competenza

ENISA (European Network and Information Security Agency)[33]

L'Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'Informazione è un centro di competenza per la sicurezza informatica in Europa. L'ENISA contribuisce attivamente alla creazione di un elevato livello di sicurezza delle reti e dell'informazione (NIS) all'interno dell'Unione, allo sviluppo di una cultura della NIS nella società, contribuendo così al corretto funzionamento del mercato interno. L'Agenzia lavora a stretto contatto con gli Stati membri ed il settore privato per fornire consulenza e soluzioni. Ciò include le esercitazioni paneuropee sulla sicurezza informatica, lo sviluppo delle strategie nazionali di sicurezza informatica, la cooperazione e lo sviluppo di capacità dei CSIRT, ma anche studi sull'adozione sicura del cloud, risposta a problemi di protezione dei dati, tecnologie di miglioramento della privacy, ecc. ENISA sostiene inoltre lo sviluppo e l'attuazione delle politiche e del diritto dell'UE in materia di NIS.

CERT-Coordination Centre (CERT-CC)[34]

Il CERT Coordination Center è il centro di coordinamento del team di risposta alle emergenze informatiche (CERT) per il Software Engineering Institute (SEI) della Carnegie Mellon University, un centro di ricerca e sviluppo finanziato dagli Stati Uniti senza fini di lucro. Il CERT / CC ricerca le vulnerabilità che influiscono sulla sicurezza di software e

[31] Fonte: https://cert.europa.eu/cert/plainedition/en/cert_about.html
[32] Fonte: https://cert.garr.it/it/
[33] Fonte: https://www.enisa.europa.eu/
[34] Fonte: https://www.sei.cmu.edu/about/divisions/cert/index.cfm

Internet, pubblica ricerche e informazioni sulle sue scoperte e collabora con aziende e enti pubblici per migliorare la sicurezza del software e di Internet nel suo complesso.

Gli esperti CERT sono un gruppo eterogeneo di ricercatori, ingegneri informatici, analisti della sicurezza e specialisti di intelligenza digitale che lavorano insieme per ricercare vulnerabilità di sicurezza nei prodotti software, contribuire a cambiamenti a lungo termine nei sistemi di rete e sviluppare informazioni e formazione all'avanguardia per migliorare pratica di cyber security.

L'acronimo CERT è un marchio registrato della Carnegie Mellon University e pertanto l'utilizzo dello stesso deve essere autorizzato dall'Ente in questione.

FIRST (Forum of Incident Response and Security Teams)[35]

Confederazione di team certificati di sicurezza e risposta agli incidenti che gestisce in modo cooperativo incidenti di sicurezza informatica e promuove programmi di prevenzione. L'obiettivo di questa organizzazione è incoraggiare la cooperazione tra i diversi team tramite un mutuo scambio di informazioni, attività di ricerca congiunte e l'attuazione di strategie comuni di difesa in caso di attacchi su vasta scala.

Ad oggi raccoglie più di 400 membri a livello mondiale appartenenti all'ambito governativo, al mondo delle imprese e al settore accademico.

Trusted Introducer[36]

Trusted Introducer (TI) è un ente fondato in Europa nel 2000 con lo scopo di favorire e rendere efficace la cooperazione tra i vari CERT, aumentando conseguentemente il livello generale di sicurezza. Il TI alimenta una rete di fiducia con servizi specializzati aggiuntivi disponibili a tutti i team di sicurezza e risposta agli incidenti informatici accreditati e certificati sulla base delle best practices sviluppate e verificate nel corso degli anni all'interno della community.

Per raggiungere i propri obiettivi, il TI fornisce a tutti gli utenti l'accesso gratuito al database contenente l'elenco di tutti i team di risposta conosciuti e registrati che sono supportati dalla community del TI, fornendo una panoramica aggiornata del livello di maturità e capacità mostrato. Tali organizzazioni sono indicizzate all'interno del database per tipologia, paese o status.

MITRE[37]

MITRE è un'organizzazione americana no profit che opera nell'interesse pubblico di tutti i governi federali, statali e locali, nonché dell'industria e del mondo accademico. La società è responsabile della gestione di centri di ricerca e sviluppo finanziati a livello federale (FFRDCs), ovvero organizzazioni speciali incaricate della promozione di collaborazioni volte e risolvere problemi su larga scala. Esse fungono da partner strategici a lungo termine per il governo, fornendo una guida obiettiva in un ambiente privo di conflitti di interesse. Lavorano con i loro partner governativi, chiamati anche sponsor, per fornire assistenza in ambito di ingegneria dei sistemi e integrazione, ricerca e sviluppo, studio e analisi. Attraverso i FFRDC e le partnership pubblico-private, MITRE si pone l'obiettivo di affrontare i problemi che mettono in discussione la sicurezza, la stabilità ed il benessere dei cittadini. I settori interessati sono: Difesa e Intelligence, Aviazione, Sistemi civili, Sicurezza Nazionale, Giustizia, Sanità e Cyber security.

NIST (National Institute of Standards and Technology)[38]

Il NIST è un'agenzia del governo degli Stati Uniti d'America che si occupa della gestione delle tecnologie. Fa parte del Dipartimento del Commercio e il suo compito è la promozione dell'economia americana attraverso la collaborazione con l'industria al fine di sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio. Tra i contributi più significativi vi è lo sviluppo del Cybersecurity Framework, pensato per supportare le agenzie governative e le organizzazioni private a gestire i rischi legati alla sicurezza informatica.

OWASP (Open Web Application Security Project)[39]

[35] Fonte: https://www.first.org/
[36] Fonte: https://www.trusted-introducer.org/
[37] Fonte: https://www.mitre.org/
[38] Fonte: https://www.nist.gov/
[39] Fonte: https://www.owasp.org/index.php/Main_Page

Organizzazione no profit a livello mondiale incentrata sul miglioramento della sicurezza del software. L'obiettivo è certificare la sicurezza del software, per permettere agli individui ed alle organizzazioni di prendere decisioni informate. Operando come una comunità di professionisti, OWASP rilascia strumenti software e documentazione basata sulla conoscenza della sicurezza delle applicazioni.

ISACA (Information Systems Audit and Control Association)[40]

ISACA è un'associazione mondiale non a scopo di lucro forte di 140.000 professionisti diffusi in 180 paesi, che contribuisce a migliorare e globalizzare le capacità professionali di guida, adattamento e assicurazione nel campo dell'IT Audit, dell'IT Governance e della cyber security. ISACA, inoltre, sviluppa e attesta le conoscenze e competenze critiche per le imprese attraverso alcune certificazioni affermate in tutto il mondo.

ECSO (European Cyber Security Organization)[41]

L'Organizzazione europea per la sicurezza informatica è un'organizzazione senza scopo di lucro completamente autofinanziata. ECSO rappresenta la controparte contrattuale della Commissione europea per l'attuazione del partenariato pubblico-privato della Cyber Security. I membri dell'ECSO comprendono un'ampia gamma di parti interessate quali grandi aziende, PMI e start-up, centri di ricerca, università, utenti finali, operatori, cluster e associazioni, nonché amministrazioni locali, regionali e nazionali degli Stati membri dell'UE, parte dello Spazio economico europeo (SEE), l'Associazione europea di libero scambio (EFTA) ed i paesi coinvolti nel programma Horizon 2020.

CLUSIT (Associazione Italiana per la Sicurezza Informatica)[42]

Nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Tra gli obiettivi dell'Associazione, vi sono quelli di: diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini, anche attraverso la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza; partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo; promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

OCS (Osservatorio della Cybersecurity)[43]

Osservatorio nato e che opera all'interno dell'Istituto di Informatica e Telematica dell'Area della ricerca di Pisa del Consiglio Nazionale delle Ricerche (IIT-CNR). L'OCS fornisce delle informazioni analitiche, ottenute attraverso il coinvolgimento di esperti all'interno del campo della sicurezza informatica, per i diversi stakeholder tra cui enti pubblici ed imprese. Il ventaglio delle attività dell'OCS, fa leva su diversi asset di competenze e di ricerche sviluppate all'interno dello IIT-CNR.

Tra le principali attività dell'OCS, c'è quella di monitorare la crescita delle vulnerabilità, delle minacce e degli attacchi sulla rete, utilizzando diverse sorgenti, che siano pubbliche e private. In particolare, tali sorgenti utilizzeranno un meccanismo di raccolta dati processati in maniera semi-automatica o automatica. Altri servizi dell'OCS, sono l'utilizzo dei social-network e blog relativi alla sicurezza informatica per conoscere e comprendere nuove minacce e la loro ampiezza e velocità di diffusione e quello dell'analisi dei tweet che utilizzano parole chiave relative al dominio della Cyber-Security.

A vantaggio delle PMI è previsto un servizio di "self assessment", che offre uno strumento semplice e rapido per l'autovalutazione del calcolo del rischio cibernetico. Richiede due tipi di input: quelli relativi alle misure di sicurezza e quelli sulle risorse dell'azienda. A questionario completo, il servizio stima le perdite annuali previste per ogni minaccia e inoltre fornisce un valore sul rischio totale.

[40] Fonte: https://www.isaca.org/pages/default.aspx
[41] Fonte: https://ecs-org.eu/
[42] Fonte: https://clusit.it/
[43] Fonte: https://www.consorzio-cini.it/index.php/it/lab-cyber-security

4.4 Standard per la Cyber Security

Un CERT, nell'organizzazione dei propri processi ed attività, può prendere come riferimento alcuni framework e linee guida rilasciate a livello nazionale ed internazionale nell'ambito della cyber security, e standard tecnici e di processo necessari per poter interagire in modo efficace ed efficiente con la propria constituency e con la comunità di riferimento.

4.4.1 Framework e Linee Guida

ISO/IEC 27001

Lo standard ISO/IEC 27001 è una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, *dall'inglese Information Security Management System*), ed include aspetti relativi alla sicurezza logica, fisica ed organizzativa. L'obiettivo principale è quello di stabilire un sistema per la gestione del rischio e la protezione delle informazioni e degli asset informatici da minacce di diverso tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni. La norma è applicabile a tutte le imprese private o pubbliche, in quanto prescinde da uno specifico settore o dall'organizzazione dell'azienda.

I requisiti proposti dallo standard sono di due tipi:

- requisiti di sistema, quali quello di stabilire le politiche e gli obiettivi, condurre il processo di risk assessment e pianificare il trattamento del rischio, gestire la documentazione e le registrazioni, ecc., e presentati dai capitoli 4 e 8 della norma;
- controlli di sicurezza, di tipo tecnico, amministrativo e gestionale (35 obiettivi di controllo e 114 controlli in totale) riportati all'interno dell'Annex A, ed approfonditi separatamente dalla linea guida ISO/IEC 27002, che presenta delle best practices per la loro implementazione. Con riferimento ai controlli, alcune sezioni possono essere di specifico interesse per un CERT, quali a titolo esemplificativo – ma non esaustivo:
  - controlli legati al processo di gestione degli incidenti, volti a favorire l'adozione di un approccio coerente ed efficace alla gestione degli stessi e per la loro comunicazione verso tutte le parti interessate;
  - controlli legati al personale, volti ad assicurare che i dipendenti e tutte le terze parti gli appaltatori comprendano le proprie responsabilità e siano idonei rispetto ai ruoli per i quali sono considerati (si pensi alle abilitazioni di sicurezza richieste per poter trattare informazioni classificate, quali il Nulla Osta di Sicurezza, NOS).

ISO/IEC 27032

La Linea Guida ISO/IEC 27032 «*Information technology – Security techniques – Guidelines for cybersecurity*» fornisce indicazioni per migliorare il proprio stato di cyber security (o "*cyberspace security*"[44]). Delinea gli aspetti peculiari di tale attività e propone buone pratiche di sicurezza per operare nel cyberspace. In particolare, all'interno della linea guida sono forniti i seguenti contributi:

- panoramica generale sulla Cybersecurity;
- spiegazione della relazione tra Cybersecurity e gli altri domini di sicurezza, quali la sicurezza delle informazioni, la sicurezza delle applicazioni, la sicurezza della rete e la sicurezza dei servizi esposti su Internet;
- definizione delle parti interessate e una descrizione dei loro ruoli per la Cybersecurity;
- guida per affrontare problemi comuni di Cybersecurity;
- quadro di riferimento per consentire alle parti interessate di collaborare alla risoluzione dei problemi di sicurezza informatica.

[44] La *cyberspace security* è definita come la protezione della riservatezza, dell'integrità e della disponibilità dell'informazione nel cyberspace, ovvero il complesso ambiente risultante dall'interazione tra persone, software e servizi su internet attraverso i dispositivi tecnologici e le reti ad essa collegati.

ISO 31000

La norma ISO 31000 «Risk management - Principles and guidelines", è una guida che fornisce principi e linee guida generali per la gestione del rischio. È stata pubblicata per la prima volta il 3 novembre 2009, ma è stata rivista e riaggiornata in una nuova versione a febbraio 2018. Può essere utilizzata da qualsiasi organizzazione e non è specifica per industria o settore. La ISO 31000 può essere applicata nel corso dell'intero ciclo di vita di un'organizzazione, ed essere adottata per molte attività come la definizione di strategie e decisioni, operazioni, processi, funzioni, progetti, prodotti, servizi e beni. Può inoltre essere applicata a qualsiasi tipo di rischio, sia per conseguenze di tipo positivo che negativo.

Il modello gestionale di gestione del rischio proposto dalla norma si basa sulla relazione tra:

- *Principi* su cui si fonda il modello di risk management per creare valore nell'organizzazione e garantire l'adeguato livello di protezione, tra cui la governance, gli aspetti umani e culturali, la tempestività, il coinvolgimento di tutte le parti interessate, ecc.
- *Struttura*, ovvero le componenti del framework di risk management, rappresentate dall'integrazione, dalla progettazione, dall'implementazione, dalla valutazione e dal miglioramento continuo, che sono coordinate dal top management, che deve garantire leadership ed impegno.
- *Processo di gestione dei rischi*, che deve essere una disciplina di uso quotidiano, comprensibile sia alla Direzione sia al personale operativo su tutti i livelli. È articolato nelle fasi di identificazione, analisi, valutazione e trattamento dei rischi[45].

ISO 15408

Lo standard internazionale ISO 15408[46] recepisce i cosiddetti"*Common Criteria*", ovvero l'insieme dei criteri e dei principi generali per la valutare l'affidabilità di un prodotto informatico dal punto di vista delle misure di sicurezza implementate. In particolare, l'adozione dei Common Criteria garantisce che il processo di specificazione, implementazione e valutazione di un prodotto informatico dal punto di vista della sicurezza sia stato condotto in modo rigoroso, standard e ripetibile ad un livello commisurato all'ambiente di destinazione per l'uso.

Lo standard prevede sette livelli di garanzia crescenti, da EAL1 (*Evaluation Assurance Level*) a EAL7, dipendenti dall'estensione e formalità della documentazione usata in fase di analisi e sviluppo, nonché dalle modalità seguite nello sviluppo. Per avere prodotti rispetto ai quali avere un buon livello di fiducia, questi dovrebbero essere valutati almeno a livello EAL4 (quello a partire dal quale i valutatori iniziano ad analizzare il codice). Livelli superiori sono ovviamente migliori ma, data la complessità, i costi crescono notevolmente e sono giustificati solo se opportune analisi del rischio lo suggeriscono. Sono previsti ulteriori 3 livelli, utilizzati esclusivamente per prodotti che integrano prodotti diversi denominati CAP (*Composed Assurance Level*) dal livello A al C, validi solo ed esclusivamente per prodotti già certificati e non sottoposti a ulteriori sviluppi per la loro integrazione.

I prodotti e sistemi da certificare sono detti *Oggetto di Valutazione* oppure *Target of Evaluation* (TOE). I requisiti di sicurezza per una tipologia di prodotto o sistema sono descritti nel documento denominato *Protection Profile* (PP) o *Profilo di Protezione* (PP).

In Italia l'OCSI[47] (Organismo di Certificazione della Sicurezza Informatica) gestisce lo Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004). L'ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) del Ministero dello Sviluppo Economico è, per decreto, l'Organismo di Certificazione della Sicurezza Informatica nel settore della tecnologia dell'informazione.

Oltre ad aver predisposto le Linee Guida per la conduzione dei processi di valutazione e certificazione, l'OCSI gestisce l'accreditamento, la sospensione e la revoca dell'accreditamento dei Laboratori per la Valutazione della Sicurezza (LVS) e degli Assistenti di Sicurezza.

[45] A tal proposito è opportuno citare la linea guida *ISO 31010 – Risk Management-Risk Assessment Techniques*, che fornisce diverse tecniche per la valutazione dei rischi in diversi ambiti.

[46] Per ulteriori informazioni consultare: www.commoncriteriaportal.org/cc

[47] Fonte: http://www.ocsi.isticom.it/

ISO/IEC 27035[48]

Lo standard ISO/IEC 27035:2011 dal titolo "Information security incident management" fornisce delle linee guida per l'implementazione di procedure e controlli al fine di creare un approccio strutturato per la gestione degli incidenti informatici. Tale standard ha come obiettivo la minimizzazione degli impatti negativi che un incidente informatico può avere sul business aziendale, attraverso il contenimento dell'incidente, la rimozione della causa scatenante, l'analisi delle conseguenze e il successivo controllo di non occorrenza. Per poter garantire il raggiungimento degli obiettivi appena descritti il processo di gestione degli incidenti viene suddiviso in cinque fasi, ciascuna contenente determinate attività, incluse in un ciclo che dall'ultima ritorna poi alla prima:

- Pianificazione e preparazione:
  - politiche di gestione degli incidenti di sicurezza;
  - politiche di gestione della sicurezza e dei rischi;
  - sistema di gestione degli incidenti di sicurezza;
  - formazione del CERT/CSIRT/IRT;
  - supporto (tecnico e di altro tipo);
  - formazione sulla consapevolezza nella gestione degli incidenti di sicurezza;
  - test del sistema di gestione degli incidenti di sicurezza.
- Scoperta e notifica: scoperta di un incidente e notifica alle appropriate funzioni aziendali.
- Valutazione e decisione: valutazione dell'evento e decisione di classificarlo come evento di sicurezza o meno.
- Risposta:
  - risposte agli incidenti di sicurezza informatica, ivi incluse operazioni di analisi forense;
  - riprendersi da un incidente di sicurezza informatica;
  - eventuali attività di investigazione, ove necessario
- Lessons learnt:
  - analisi forensi più approfondite (se necessario);
  - identificazione della lezione appresa;
  - identificazione e attuazione dei miglioramenti al sistema di sicurezza;
  - identificazione e attuazione dei miglioramenti alle valutazioni dei rischi di sicurezza;
  - identificazione e attuazione dei miglioramenti al sistema di gestione degli incidenti di sicurezza.

ISO 27005[49]

Lo standard ISO 27005 dal titolo "Information technology – Security techniques – Information security risk management", aggiornato nel 2018, fornisce le linee guida per la gestione dei rischi relativi alla sicurezza delle informazioni e supporta i concetti generali specificati nello standard ISO/IEC 27001, con il quale si integra, con l'obiettivo di aiutare le organizzazioni nella tutela della sicurezza delle informazioni mediante un corretto approccio alla gestione del rischio.

Seguendo lo schema, il contenuto della ISO/IEC 27005 è suddiviso in 6 capitoli (quelli dal 7 al 12):

- stabilire il contesto;
- valutare il rischio (a sua volta suddiviso nelle tre sezioni relative all'identificazione, analisi e ponderazione del rischio);

[48] Fonte: https://www.iso.org/standard/44379.html
[49] Fonte: https://www.iso.org/standard/75281.html

- trattare il rischio;
- accettare il rischio;
- comunicare il rischio e consultare le parti interessate;
- monitorare e riesaminare il rischio.

Promuove un approccio alla valutazione del rischio basato sull'identificazione di asset, minacce e vulnerabilità, peculiare per la l'analisi dei rischi di sicurezza delle informazioni. Propone in appendice utili strumenti a supporto delle attività operative che approfondiscono ulteriormente alcuni aspetti della gestione del rischio (es. lista di minacce; tecniche di analisi dei rischi; ecc.).

ISO 29147[50]

Lo standard ISO/IEC 29147:2018 dal titolo "Information Technology – Security Techniques – Vulnerability Disclosure" delinea le modalità con cui fornitori di hardware e software e qualsiasi altra organizzazione che fornisce strumenti e/o applicazioni possono integrare il processo di gestione della divulgazione delle vulnerabilità nei loro normali processi aziendali.

In particolare fornisce delle linee guida su:

- su come ricevere informazioni relative a potenziale vulnerabilità nei prodotti o servizi online;
- su come divulgare le informazioni sulla risoluzione delle stesse;
- gli elementi informativi che dovrebbero essere prodotti attraverso l'implementazione del processo di divulgazione delle vulnerabilità e esempi di contenuto che dovrebbero essere inclusi negli elementi informativi.

ISO 27037[51]

Lo standard ISO 27037:2012 dal titolo "*Guidelines for identification, collection, acquisition, and preservation of digital evidence*", fornisce delle linee guida relative alla gestione delle potenziali prove digitali, concentrandosi in particolar modo sulle fasi di identificazione (ispezione), raccolta (sequestro), acquisizione (sequestro virtuale) e preservazione (conservazione e sigillo). Per ogni fase vengono indicate le best practices riconosciute per permettere che la potenziale prova possa essere utilizzata efficacemente in sede processuale, tenendo conto delle possibili (e più comuni) situazioni che l'investigatore può trovarsi a dover affrontare, come ad esempio:

- attività di base e aggiuntive relative a raccolta di sistemi digitali che vengono trovati accesi;
- attività di base e aggiuntive relative ad acquisizione di sistemi digitali che vengono trovati accesi;
- attività di base e aggiuntive relative a raccolta di sistemi digitali che vengono trovati spenti;
- attività di base e aggiuntive relative ad acquisizione di sistemi digitali che vengono trovati spenti;
- attività di raccolta o acquisizione di sistemi collegati in rete.

Vengono inoltre definite tre figure chiave, che si occupano e sono responsabili degli aspetti di gestione della prova digitale menzionati sopra:

- il DEFR o Digital Evidence First Responder è un soggetto autorizzato, formato e qualificato ad agire per primo sulla scena di un incidente per eseguire attività di raccolta ed acquisizione delle prove avendone inoltre la responsabilità di corretta gestione; è l'operatore che si approccia per primo ai sistemi (supporti di memorizzazione e dati) di potenziale interesse.
- il DES o Digital Evidence Specialist è un soggetto che ha le capacità di eseguire le stesse attività eseguite da un DEFR ed in più possiede conoscenze specialistiche ed è in grado di gestire una moltitudine di problematiche tecniche, ad esempio è in grado di portare a termine attività quali acquisizione di rete, di memoria RAM ed ha ampia conoscenza di sistemi operativi e/o Mainframe;

[50] Fonte: https://www.iso.org/standard/72311.html
[51] Fonte: https://www.iso.org/standard/44381.html

- l'Incident Response Specialist, che normalmente è una figura professionale interna all'azienda che si occupa del primo intervento post incidente informatico. Questa figura coincide spesso, in contesto aziendale, con l'amministratore dei sistemi informativi. La sua principale attività consiste nel mantenere operativi i sistemi informativi, per cui spesso, dopo il verificarsi di un incidente informatico, la sua attività va contro quella di un DEFR o DES poiché il ripristino dell'operatività dei sistemi può portare facilmente alla perdita di potenziali prove.

Sia DEFR che DES hanno il compito di portare a termine il lavoro nel miglior modo possibile, utilizzando al meglio le linee guida fornite dallo standard, che vanno comunque integrate con le normative in vigore all'interno dello Stato in cui essi operano, dato che gli standard di questa serie hanno carattere generale e quindi non sono legati ad uno specifico ordinamento giuridico.Le modalità con cui procedere alle successive attività di analisi e interpretazione delle prove digitali e di comunicazione dei risultati sono definite nello standard ISO 27042:2015 "*Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*"[52].

4.4.2 Standard tecnici

Nonostante i numerosi protocolli definiti negli ultimi anni per la condivisione delle informazioni utilizzate nell'analisi e nella risoluzione di un incidente, pochi sono attualmente divenuti gli standard de facto. Si raccomanda dunque ai CERT la conoscenza di tali protocolli per la corretta interpretazione e gestione delle informazioni ricevute.

In questo paragrafo saranno descritti i principali standard utilizzati per la classificazione e condivisione di informazioni da e verso il CERT.

Protocollo TLP

Le informazioni da condividere devono essere classificate in base al loro livello di sensibilità e, qualunque sia il metodo, dovrebbe poter essere utilizzato da entrambi i settori pubblico e privato senza la necessità di rimandi ai loro schemi di classificazione delle informazioni. Per essere univoci ed avere una base comune nel processo di condivisione delle informazioni spesso si utilizza un codice-colore abbinato alle informazioni di incidente, chiamato Traffic Light Protocol (TLP)[53], che prevede un insieme di requisiti per far sì che ogni informazione condivisa sia distribuita solo ai destinatari corretti.

Il protocollo TLP viene utilizzato in molti processi di condivisione delle informazioni. L'informazione viene classificata secondo quattro livelli (tag) - White, Green, Amber o Red (in ordine di crescente gravità) - che indicano le prescrizioni di confidenzialità e condivisibilità dell'informazione relativa all'incidente che i riceventi dovranno adottare nel gestirla:

- *WHITE – Illimitato:* deve essere adottato nel caso di comunicazioni che contengono informazioni che possono essere diffuse pubblicamente, in quanto irrilevanti ai fini dei rischi di sicurezza per l'organizzazione. Tali informazioni possono dunque essere liberamente condivise dai destinatari con soggetti terzi, nel rispetto delle norme a tutela dei diritti di proprietà intellettuali e con gli altri termini di legge.
- *GREEN - A livello di comunità*: le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità o organizzazione, in quanto utili ai fini della sensibilizzazione. Tuttavia, tali informazioni non dovrebbero essere pubblicate o rese di dominio pubblico su Internet, né rilasciate al di fuori della comunità.
- *AMBER - Distribuzione limitata:* i destinatari possono condividere questo tipo di informazioni con altri all'interno della propria organizzazione per finalità operative. Tali comunicazioni contengono infatti tipicamente informazioni che potrebbero essere sfruttate per causare impatti in termini di privacy e reputazione o deterioramento della normale operatività, se condivise all'esterno dell'organizzazione. Ci si può aspettare che il mittente specifichi i limiti previsti di tale condivisione, nel rispetto del principio del "need-to-know".
- *RED - Personale solo per i destinatari specificati:* la condivisione all'esterno del gruppo dei destinatari non è legittimata e l'utilizzo di tali informazioni al di fuori degli stessi può determinare seri impatti in termini legali,

[52] Fonte: https://www.iso.org/standard/44406.html
[53] Fonte: https://www.first.org/tlp/

reputazionali o di interruzione della normale operatività dell'organizzazione. Questo tipo di informazioni può essere utilizzato dai soli Destinatari, anche nelle comunicazioni tra loro, e non possono essere divulgate neppure all'interno della propria organizzazione, adottando la massima riservatezza. Nel contesto di una riunione faccia a faccia, ad esempio, la distribuzione delle informazioni RED è limitata ai soli presenti alla riunione.

Questo metodo di classificazione delle informazioni è ampiamente utilizzato poiché è molto semplice da comprendere e implementare, e può essere facilmente adottato anche in altri settori o al di fuori del territorio nazionale. Nella maggior parte dei casi, il mittente delle informazioni da condividere determinerà il suo colore di classificazione, ma talvolta i CERT possono decidere di elevarlo se ritengono che il livello definito sia troppo basso.

L'applicazione di tale protocollo si rende auspicabile anche per gestire il problema dell'anonimizzazione della sorgente di informazione, che si presenta, inevitabilmente, quando un'organizzazione partecipante non desidera essere identificata come vittima di un attacco (magari andato a buon fine) o come coinvolta in altro evento di sicurezza. Il CERT si impegna a garantire che questa richiesta di anonimato sia rispettata, assicurando che, anche omettendo l'identità dell'originatore, le informazioni trasmesse non contengano indizi o metadati aggiuntivi che potrebbero in alcun modo rivelare, portare a dedurre, suggerire o identificare l'originatore.

STIX

STIX (Structured Threat Information eXpression)[54] è un linguaggio di programmazione XML standardizzato per la specifica, l'acquisizione, la caratterizzazione e la comunicazione di informazioni relative a minacce cyber in un linguaggio comune che può essere facilmente compreso sia dagli individui che dalle tecnologie di sicurezza. STIX, originariamente sponsorizzato dall'ufficio di Cybersecurity and Communications del Dipartimento di Homeland Security degli Stati Uniti (DHS), è stato trasferito ad OASIS, un consorzio senza scopo di lucro che mira a promuovere lo sviluppo, la convergenza e l'adozione di standard aperti per la rete. Rappresenta dunque uno sforzo collaborativo teso a sviluppare un linguaggio standardizzato e strutturato, che identifichi le informazioni concernenti le minacce cibernetiche. I membri della community STIX contribuiscono allo sviluppo e alla gestione del linguaggio, ma in generale tutti i membri della comunità informatica sono invitati a dare il loro apporto.

Il linguaggio STIX trasmette l'intera gamma di potenziali informazioni sulle minacce informatiche e si pone per essere pienamente espressivo, flessibile, estensibile, automatizzabile e leggibile. L'obiettivo di STIX è quello di specificare, caratterizzare e acquisire informazioni. STIX affronta una gamma completa di casi d'uso delle minacce, tra cui analisi, acquisizione e specifica degli indicatori, gestione delle attività di risposta e condivisione delle informazioni, per migliorare la coerenza, l'efficienza, l'interoperabilità e la consapevolezza generale della situazione. STIX è un modello di dati grafico basato su *nodi* ed *edge*. I nodi sono STIX Data Objects (SDO), mentre gli edge sono STIX Relationship Objects (SRO). Gli SDO includono informazioni come Metodi di attacco, Identità, Dati osservati, Threat actor, Vulnerabilità, ecc. Gli SRO sono pensati per connettere gli SDO in modo che, nel tempo, gli utenti saranno in grado di sviluppare una conoscenza approfondita degli attori delle minacce e delle loro tecniche.

Il formato STIX 2.0 definisce 12 STIX domain Objects (SDOs). Il modello STIX è costituito almeno dalle seguenti entità:

- *Indicatori* e *Osservabili*: un attacco specifico di solito coinvolge schemi che ne consentono la caratterizzazione. Questi modelli possono essere artefatti e / o comportamenti di interesse all'interno di un contesto di sicurezza informatica e sono specificati in STIX da Observables che agiscono come indicatori per un attacco;
- *Incidenti*: si tratta di attacchi riusciti che dettagliano le informazioni sull'origine e sul target. I relativi Indicatori e Osservabili della minaccia forniscono informazioni su come tale attacco potrebbe essere rilevato;
- *Obiettivi di exploit*: vulnerabilità o punti deboli che consentono all'attaccante di attaccare con successo un target.
- *Tattiche, Tecniche, procedure (TTP)*: termine preso in prestito dall'ambito militare per rappresentare il comportamento o il modus operandi dell'avversario quando esegue l'attacco. Un TTP può contenere informazioni su quali siano le vittime dell'attore di minaccia, quali modelli di attacco e malware vengono utilizzati, e quali risorse (infrastrutture, strumenti, persone) vengono sfruttate;

[54] Per ulteriori informazioni consultare: https://stixproject.github.io/

- *Attori di minaccia*: una caratterizzazione dell'identità, della sospetta motivazione e dei presunti effetti intenzionali degli attaccanti;
- *Campagna*: rappresenta un insieme di attività e comportamenti che gli attori della minaccia eseguono per ottenere l'effetto desiderato in un periodo di tempo.
- *CourseOfActions (COA)*: sono misure specifiche da adottare in risposta ad un attacco o come misura preventiva prima di un attacco.

TAXII

Nato per soddisfare le esigenze di condivisione delle informazioni tra diversi settori di infrastrutture critiche, TAXII (Trusted Automated eXchange of Intelligence Information)[55] è un'iniziativa della comunità internazionale per standardizzare lo scambio affidabile e automatizzato di informazioni sulle minacce informatiche. Come per STIX, DHS ne ha affidato lo sviluppo e la manutenzione a consorzio OASIS. Si tratta di un protocollo applicativo basato su HTTPS. Definisce un insieme di servizi e scambi di messaggi che, una volta implementati, consentono la condivisione di informazioni sulle minacce informatiche utilizzabili attraverso i confini dell'organizzazione e dei prodotti / servizi per l'individuazione, la prevenzione e la mitigazione delle minacce informatiche.

Considerata la scelta del linguaggio STIX per la definizione delle minacce cyber ed il protocollo TAXII come meccanismo di trasporto per la condivisione delle stesse tra enti/organizzazioni differenti, l'obiettivo è quello di creare una rete efficace ed efficiente (community) in cui il semplice indicatore scambiato (IP, URL, SHA, etc.) diventi, dopo la sua qualificazione, un'informazione.

TAXII definisce due servizi primari per supportare una varietà di modelli di condivisione comuni:

- *Collection*: un'interfaccia per un repository logico di dati di cyber threat intelligence fornito da un server TAXII, che consente al mittente di ospitare dati che possono essere richiesti dal destinatario. I Client e server TAXII scambiano informazioni in un modello request/response.
- *Channel*: un canale mantenuto da un server TAXII consente ai mittenti di inviare dati a molti destinatari e a questi ultimi di ricevere dati da molti mittenti. I client TAXII scambiano informazioni con altri client TAXII in un modello asincrono di tipo publish/subscribe.

OpenIOC

L'Open Indicators of Compromise (OpenIoC) è un linguaggio XLM-based volto a raggruppare e comunicare informazioni. Esso permette di descrivere caratteristiche tecniche che identificano una minaccia nota, una metodologia di attacco, o altri indicatori di compromissione. Si concentra su artefatti malevoli, indicatori di compromissione e TTP specifiche.

OpenIOC stabilisce uno standard per la registrazione, la definizione e la condivisione di informazioni sia internamente che esternamente in un formato strutturato. Per finalità di analisi forense, lo strumento consente ad un investigatore di descrivere indicatori di compromissione in un formato standardizzato che può essere esportato e interpretato in maniera consistente. Inoltre OpenIOC specifica un formato di base estensibile per ospitare eventuali diversi tipi di IOC rispetto a quelli nativamente definiti.

Tra le caratteristiche principali vanno citati il supporto a query semplici e avanzate, la ricerca tramite hash di un file o specifici registri di windows, la combinazione di filtri riguardanti artefatti malevoli, autori, hostname e/o altri dati riguardanti un particolare evento malevolo.

Attualmente esistono diversi applicativi utilizzabili anche per la conversione da OpenIOC a STIX.

RFC 2350

La specifica RFC (Request for Comments) 2350[56] stabilisce alcune linee guida circa l'organizzazione e le modalità di comunicazione di un CERT/CSIRT. Attraverso la formalizzazione di tale specifica, il CERT rende noto alla propria consitituency in primo luogo quali sono le proprie aree di competenza e le proprie capacità, in secondo luogo le politiche e procedure operative adottate. Uno degli obiettivi della RFC2350 è proprio quello di definire un modello standard

[55] Per ulteriori informazioni consultare: https://taxiiproject.github.io/
[56] Per ulteriori informazioni consultare: http://www.rfc-base.org/txt/rfc-2350.txt

per la diffusione delle informazioni tra i CERT e il resto della comunità. Infatti, affinché vi sia una corretta interazione tra i CERT e i rispettivi constituent, all'intera comunità devono essere ben chiare le politiche e procedure dei response team, i loro rapporti con altri team o terze parti, quali canali di comunicazione utilizzano e come provvedono a renderli sicuri.

A seguire si riportano le principali informazioni che devono essere pubblicate da un CERT ai sensi del template RFC 2350 (tipicamente sul proprio sito web):

- Informazioni sul documento, quali data dell'ultimo aggiornamento, la lista di distribuzione per le notifiche, i luoghi (gli indirizzi) in cui la versione più recente del documento può essere trovato, ovvero tutte quelle informazioni utili alla constituency per poter accedere allo stesso ed ai suoi aggiornamenti;
- Informazioni di contatto: denominazione ufficiale del CERT, indirizzo, contatti telefonici/fax, indirizzo mail, chiavi pubbliche e tecniche crittografiche, membri del team, ecc.
- Charter, ovvero le informazioni sulla missione che si è prefissa il CERT e sulle autorità da cui dipende. Dovrebbe includere almeno quattro elementi:
  - mission statement: obiettivi e finalità del CERT;
  - constituency: soggetti/entità cui sono rivolti i servizi offerti dal CERT (ciò determina conseguentemente il perimetro di lavoro del CERT stesso);
  - sponsorship / affiliation: indicazione degli organismi che supportano e finanziano le attività del CERT;
  - authority: linea di riporto del CERT;
- Politiche e procedure, tra cui:
  - tipologie di incidente che il CERT è in grado di affrontare ed i livelli di supporto che offre durante la gestione;
  - cooperazione ed interazione con i soggetti con cui il CERT opera abitualmente (non solo per le attività di risposta agli incidenti), tra cui altri CERT, forze dell'ordine, organi di stampa, fornitori, ecc.;
  - comunicazione e autenticazione, ovvero indicazioni sulle modalità con cui il CERT assicura la sicurezza delle comunicazioni tra loro e la constituency (es. tecniche crittografiche utilizzate, condivisione delle le chiavi pubbliche, indicazione delle firme digitali, ecc.);
- Servizi offerti;
- Modalità e canali per le segnalazioni di incidenti e vulnerabilità.

SIM3[57]

SIM3 (Security Incident Management) è un modello per valutare la maturità della gestione degli incidenti di sicurezza. Il modello di maturità è costruito su tre elementi base:

- Parametri di maturità;
- Quadranti di maturità;
- Livelli di maturità.

I Parametri sono le quantità misurate in termini di maturità (sono previsti più di 40 parametri), ed appartengono individualmente a uno dei quattro quadranti, ovvero O – Organisation, H – Human, T – Tools, P – Processes. Nell'ambito del modello devono essere misurati i livelli di maturità per ciascun parametro, secondo una scala a 5 livelli da 0 a 4. Sono fornite indicazioni per stabilire le condizioni per passare da un livello ad un altro.

Tale modello è alla base dello schema di accreditamento definito da Trusted Introducer ma può essere impiegato anche per processi di autovalutazione.

eCSIRT.net Incident Taxonomy[58]

[57] Fonte: https://www.trusted-introducer.org/SIM3-Reference-Model.pdf
[58] Fonte: http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

Si tratta di una tassonomia per la classificazione degli incidenti di sicurezza molto diffusa presso i CERT e le organizzazioni di sicurezza. Ne è incoraggiato l'utilizzo anche per favorire attività di comparazione e statistiche sugli incidenti rilevati. Propone uno schema di classificazione degli incidenti fornendo esempi dettagliati utili a favorirne la tipizzazione.

CCoP - CSIRT Code of Practice[59]

Un codice di condotta è un insieme di regole o linee guida per i membri di un CERT su come comportarsi professionalmente, potenzialmente anche al di fuori del lavoro. Un esempio è quello sviluppato da Trusted Introducer, promosso oggi da ENISA come buona prassi per favorire lo sviluppo dell'etica professionale nella comunità professionale e aumentare complessivamente la maturità dei team.

[59] Fonte: https://www.trusted-introducer.org/TI-CCoP.pdf

CAPITOLO 5

Introduzione ai CERT

5.1 CERT: significato e definizioni generali

Il significato di CERT è comunemente associato ad un gruppo di professionisti dedicato alla gestione degli incidenti di sicurezza informatica, in grado di cooperare e coordinare gli interventi necessari per contenere il loro impatto e rispristinare le normali o accettabili condizioni operative nell'erogazione dei servizi. Al fine di attenuare gli impatti e ridurre al minimo il numero di interventi richiesti, la maggior parte dei CERT fornisce anche servizi di prevenzione e di formazione e sensibilizzazione per la propria comunità di riferimento.

Il funzionamento dei CERT si basa sulla gestione integrata dei flussi informativi provenienti dalla propria constituency e dal mondo esterno, in qualità di unica interfaccia operativa per le attività di *Information Sharing*. I CERT capaci di raccogliere, oltre alle segnalazioni di incidenti informatici, le vulnerabilità e le potenziali minacce, analizzano gli impatti che si potrebbero verificare sulle infrastrutture informatiche della propria constituency (o sull'organizzazione stessa) così da indentificare i rischi e dunque le più adeguate contromisure.

Nel contesto attuale lo scopo e la missione dei CERT sono stati estesi, e più che parlare di "Response" (risposta) si pone l'accento sulla nozione di "Readiness" (prontezza / preparazione). In particolare, a fronte dell'evoluzione dei servizi informatici, della crescente sofisticazione delle minacce e della rilevanza strategica dei target cui le stesse si rivolgono, ogni organizzazione, di fronte ad un incidente di sicurezza informatica, deve prepararsi per tempo, sviluppando la propria cultura e mettendo in campo azioni proattive e procedure tese a ridurre la probabilità ma anche l'impatto degli incidenti. Condurre le organizzazioni verso uno stato di "Readiness" in tema di cyber security vuol dire dunque sviluppare quella capacità di adattare i propri sistemi di difesa (non solo tecnologici, ma anche di processo e procedurali) sulla base dell'evoluzione delle minacce, della scoperta di nuove vulnerabilità e degli incidenti avvenuti sia internamente che subiti da altre organizzazioni.

Elementi fondamentali per assicurare la Readiness sono in particolare:

- capacità di rilevazione e risposta agli incidenti;
- capacità di comprendere ciò che sta avvenendo sulle proprie infrastrutture e sui sistemi, attraverso una conoscenza approfondita dei propri asset, incluse le configurazioni dei sistemi e le vulnerabilità;
- capacità di individuare le minacce esterne e le modalità con cui potrebbero essere colpiti i propri sistemi e servizi informatici;

- capacità di condividere informazioni, in modo efficiente, per consentire alle organizzazioni, alle amministrazioni, alle istituzioni, alle infrastrutture critiche di scambiarsi conoscenza al fine di anticipare eventuali attacchi, innalzando in questo modo il proprio livello di protezione.

5.2 Categorie di CERT

In funzione della finalità e del contesto operativo nel quale essi operano, è possibile distinguere diverse tipologie di CERT[60]:

Tabella 5.1: Categorie di CERT

Categoria di CERT	Finalità
Nazionale	Costituisce un punto di contatto unico per la sicurezza a livello di Paese, agendo da intermediario anche nei confronti degli altri CERT nazionali a livello comunitario e internazionale. Si parla in alcuni casi anche di CERT Regionali, quando i CERT nazionali sono connessi oltre i confini nazionali su un territorio più esteso (es. federale o continentale)[61]
Governativo	Supporta le agenzie governative e le Pubbliche Amministrazioni nella protezione da minacce e incidenti cyber.
Settoriale	Fornisce servizi nei confronti di una comunità di attori appartenenti ad uno stesso ambito o settore (ad esempio: ambito accademico, bancario, industriale, ecc.).
Militare	Fornisce servizi alle organizzazioni militari responsabili dell'infrastruttura IT necessaria per finalità di difesa.
Privato o interno	Fornisce servizi limitatamente all'organizzazione che lo ospita.
Commerciale	Offre servizi nei confronti di soggetti terzi all'organizzazione che lo ospita, con finalità di vendita sul mercato a fronte di un corrispettivo economico.

5.3 Mission dei CERT

Le attività critiche di un CERT dovrebbero comprendere almeno le seguenti:

- fornire supporto ed assistenza specialistica alla constituency nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
- agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cibernetici indirizzati a specifici settori, organizzazioni o territori;
- incentivare l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite;
- facilitare le attività di prevenzione e monitoraggio degli eventi cibernetici sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale;

[60] Si vedano anche [8] e [15].

[61] New America-GPPi "*CSIRT Basics for Policy-Makers",* pubblicato nell'ambito del progetto "Transatlantic Dialogues on Security and Freedom in the Digital Age".

- collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle organizzazioni in materia di cyber security;
- accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi a livello locale.

5.4 Identificazione della constituency

Nell'ambito del proprio funzionamento, ogni CERT interagirà con una vasta gamma di entità e soggetti. La più importante comunità tra queste è quella per cui il CERT stesso è stato fondato e a cui rivolgerà i propri servizi, ovvero la sua *constituency*, ovvero la comunità di utenti ed entità interni o esterni all'organizzazione cui il CERT appartiene e verso cui il CERT eroga istituzionalmente i propri servizi. Questa potrà essere illimitata (un CERT che fornirà servizio a chiunque ne faccia richiesta), oppure può essere limitata da alcune restrizioni, quali ad esempio:

- vincoli di natura finanziaria legati all'entità dei fondi iniziali ottenuti per la costituzione del CERT e l'avvio delle attività;
- vincoli di natura geografica o politica, come nel caso di CERT che dovranno supportare una constituency nazionale o legata a singole organizzazioni dell'apparato governativo o amministrativo di un Paese;
- vincoli di natura tecnico-organizzativa, quando ad esempio un CERT viene costituito all'interno di una determinata organizzazione oppure è avviato per offrire servizi verso una specifica clientela di mercato.

Il CERT, oltre che con la propria constituency, potrà comunque intrattenere rapporti con ulteriori entità non ricomprese in quest'ultima, organizzate all'interno di una o più community informali, più o meno strutturate (si pensi ad esempio ad attività di scambio di informazioni tra le parti regolate da specifici accordi o a regolamenti generali definiti dalle community stesse).

L'identificazione della propria constituency è un'operazione estremamente critica per l'efficacia di un CERT. Infatti, a seconda della gamma di servizi offerti da un CERT e della natura di tali servizi, un CERT potrebbe anche avere la necessità di definire più di una constituency. È altresì possibile che uno o più CERT offrano un determinato servizio a constituency che si sovrappongono, con il rischio di avere uno scarso coordinamento in termini di ruoli e responsabilità nonché una potenziale duplicazione degli sforzi e servizi inefficaci e/o in reciproco contrasto (si pensi ad esempio alla sovrapposizione di un CERT privato con uno governativo nell'ambito degli stessi servizi).

Con riferimento alle diverse tipologie di CERT individuati in **Tabella 5.2**, è possibile individuare specifiche constituency.

Tabella 5.2: Constituency di riferimento per tipologia di CERT

Categoria di CERT	Constituency di riferimento
Nazionale	Cittadini ed organizzazioni pubbliche e private appartenenti aduna specifica nazione.
Governativo	Cittadini, agenzie governative ed altre organizzazioni pubbliche.
Settoriale	Utenti ed organizzazioni operanti in specifici settori.
Militare	Personale appartenente a corpi militari/difesa o di entità organizzative strettamente correlate.
Privato o interno	Personale interno e dipartimenti/funzioni dell'organizzazione ospitante.
Commerciale	Clienti pubblici o privati che si avvalgono di un fornitore esterno.

Allo stesso modo, anche quando una constituency è molto circoscritta, un CERT potrebbe avere comunque la necessità di interagire con entità esterne al proprio ambito di intervento per raccogliere informazioni utili alla propria constituency. In tal senso, alcuni CERT possono agire come vero e proprio centro di coordinamento tra la propria constituency ed altre parti esterne (come altri CERT, forze dell'ordine, fornitori, media, ecc.) e tali relazioni possono prevedere il semplice inoltro di richieste di informazioni per arrivare a situazioni di completa condivisione dei dati e delle informazioni e alla piena collaborazione.

Una volta individuata e definite la constituency, il CERT dovrebbe promuovere sé stesso e i suoi servizi sia all'interno della propria constituency che al di fuori della stessa nel modo più ampio possibile per garantire una chiara comprensione del suo ruolo e dei servizi offerti ed ottenere un riconoscimento all'interno della più ampia comunità dei CERT. Tale promozione dovrebbe essere effettuata attraverso il maggior numero possibile di canali di comunicazione, inclusi quelli istituzionali (sito web, ecc.), organizzazione di workshop e in generale attività di sensibilizzazione.

5.5 CERT regionali

AGID[62], tramite le attività operative in carico al CERT-PA, supporta le PA nella prevenzione e nella risposta agli incidenti di sicurezza informatica che avvengono nel dominio costituito dalle stesse. Il CERT-PA è infatti la struttura responsabile per la conduzione e gestione delle attività operative e per il monitoraggio dello spazio cibernetico delle PA, anche tramite l'attivazione di specifiche collaborazioni con le comunità di riferimento nazionali ed internazionali.

Ai fini dell'efficacia del modello di interazione tra CERT-PA e PAL, si rende opportuna una decentralizzazione delle attività operative oggi in carico al CERT-PA, fondamentale per raggiungere in modo capillare tutte le amministrazioni del territorio nazionale. Infatti, l'attuale modello, basato su un unico CERT-PA centrale, risulta essere insufficiente rispetto alla nuova complessità del sistema, che ha visto un significativo aumento delle entità appartenenti alla *Constituency*[63]. Per operare efficacemente la sicurezza cibernetica a livello delle strutture locali della PA è dunque auspicabile la creazione di una rete nazionale di CERT periferici (*CERT Regionali*), supplementari al CERT-PA, i quali possano garantire, sulla base di un modello di interazione definito, un primo supporto diretto alle PAL, attivando un processo di escalation verso il CERT-PA in caso di necessità.

I CERT Regionali dovranno essere costituiti dunque con l'obiettivo di facilitare le attività di prevenzione e monitoraggio del CERT-PA, agendo come unità locali in grado di esercitare un controllo più diretto sul territorio, e di gestire tutti quegli incidenti di Cyber Security per i quali il CERT-PA non deve essere necessariamente coinvolto in maniera diretta, in quanto:

- sono limitati ad un singolo ente locale o ad un numero limitato di PAL;
- producono limitate implicazioni di sicurezza in termini di impatto su asset ed informazioni e sono pertanto gestibili nell'ambito delle normali attività operative della PAL stessa e/o di organismi periferici, quali i CERT Regionali;
- sono relativi a PAL che non hanno aderito al processo di accreditamento al CERT-PA.

Le PAL cercano da tempo di sviluppare maggiori competenze e servizi specialistici per contrastare le minacce cibernetiche che crescono in numero e sofisticatezza, ma non tutte possiedono dimensioni, risorse umane, tecniche ed economiche sufficienti per raggiungere tale risultato. La possibilità di accedere ad infrastrutture e risorse specializzate – messe a disposizione dai CERT regionali - costituisce un elemento chiave per l'innalzamento dei livelli di sicurezza di tali enti.

Nel modello unificato di CERT su scala nazionale, i CERT regionali rappresenteranno entità più vicine alle PAL in senso geografico, operando, da un lato, come strutture di supporto verso le stesse e, dall'altro, fungendo da elemento di raccordo fra periferia e centro (CERT-PA).

Per garantire omogeneità di comportamento e interoperabilità sia orizzontale che verticale è necessario che tutti i CERT della rete regionale operino secondo un modello organizzativo ed operativo comune, che individui e definisca struttura, organizzazione, risorse, servizi e processi e meccanismi di interazione con le PAL.

Il modello proposto nel documento definisce una serie di elementi e di aspetti chiave alla base della costituzione e dell'avvio dei CERT regionali, come di seguito illustrato:

- definizione della mission dei CERT regionali, ovvero la funzione di base che ha determinato la costituzione degli stessi, in termini di obiettivi ed attività fornite alla propria comunità di riferimento;

[62] Riferimento: Art. 20, c. 3 lett. b) del Decreto Legge 22 giugno 2012, n. 83.

[63] La Constituency originaria del CERT-PA nel 2015 comprendeva solo PAC, Regioni, Città metropolitane, per un totale di circa 70 Amministrazioni. La Constituency attuale comprende anche la PAL e tutte le Amministrazioni sul dominio *.gov.it (~22.600 Amministrazioni).

- definizione della Constituency da servire, ovvero la comunità di soggetti ed entità che potranno accedere ai servizi offerti dai CERT regionali e/o che si potranno mettere in contatto ed attuare relazioni di mutuo scambio di informazioni con gli stessi (es. altri CERT nazionali e governativi), e definizione delle relative modalità di ingaggio, di cooperazione e di affiliazione;
- sviluppo del catalogo dei servizi offerti dai CERT regionali, supplementare a quello offerto dal CERT-PA, determinando i benefici e le aspettative connesse a ciascun servizio;
- definizione del modello organizzativo ed amministrativo, del sistema di ruoli e responsabilità e dei livelli di delega, in accordo con gli indirizzi strategici nazionali e con le pratiche attuate dal CERT-PA;
- definizione dei processi operativi a supporto dell'erogazione dei servizi ed in particolare quelli di gestione degli incidenti, di escalation verso il CERT-PA e di comunicazione verso altri enti locali e/o centrali;
- formalizzazione delle responsabilità definite nell'ambito dei processi operativi;
- sviluppo delle capacità, in termini di Risorse, Tecnologie ed Infrastrutture, da implementare e/o migliorare per il funzionamento dei CERT regionali;
- definizione dei requisiti di sicurezza fisica e logica per la protezione degli spazi di lavoro, degli asset informatici e delle informazioni impiegati dai CERT regionali;
- definizione dei meccanismi di interazione e cooperazione, inclusa l'identificazione del modello di affiliazione e/o accreditamento più appropriato in funzione dei servizi offerti;
- definizione di una roadmap al fine di prioritizzare il rilascio dei servizi e delle capacità connesse sulla base del loro rapporto costi/benefici, valutando, al contempo, la possibilità di ricevere finanziamenti di tipo governativo sia livello nazionale che sovranazionale (i.e. europeo).

5.5.1 Mission dei CERT regionali

Come precedentemente illustrato, i CERT regionali si pongono come strutture istituite e operanti sul territorio con il ruolo di coordinare, supportare e monitorare le attività di prevenzione, risposta e ripristino degli incidenti critici di tipo cyber nell'ambito del dominio costituito dalle PAL.

Tenuto conto degli ambiti di responsabilità e di relativa specializzazione del CERT-PA e degli altri organismi centrali istituiti nell'ambito della strategia nazionale per la sicurezza cibernetica[64], le attività critiche dei CERT regionali dovrebbero comprendere:

- fornire supporto ed assistenza specialistica alle PAL nell'analisi dei dati relativi alle minacce informatiche emergenti e nella risoluzione degli incidenti di cyber security;
- agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cyber indirizzati a specifici settori e possibili impatti per le PAL e la loro utenza;
- incentivare a livello locale l'applicazione dei processi di gestione della sicurezza, delle metodologie e delle metriche valutative per il governo della sicurezza cibernetica definite a livello nazionale;
- facilitare le attività di prevenzione e monitoraggio del CERT-PA sul territorio, agendo come unità capaci di esercitare un controllo più diretto a livello locale, mediante azioni di aggregazione delle PAL;
- collaborare e cooperare con le altre organizzazioni nazionali ed internazionali nel potenziamento e miglioramento della capacità difensiva delle PAL in materia di cyber security;
- accrescere le competenze specialistiche degli addetti alla sicurezza cibernetica e migliorare le attività di sensibilizzazione su questi temi.

[64] Si veda Par. 4.1.

5.5.2 Constituency dei CERT Regionali

La Constituency dei CERT regionali è rappresentata dalla comunità delle PAL[65] che possono accedere e beneficiare dei servizi da questi erogati. Una lista, non esaustiva, delle categorie di PAL che possono essere serviti in linea di principio dai CERT regionali è fornita a seguire:

- Province
- Comuni
- Comunità montane e isolane
- Forme associative tra enti locali, ovvero enti territoriali che sperimentano la gestione associata dei servizi e delle funzioni, tra cui: le Unioni di Comuni, Centri Servizi Territoriali, consorzi intercomunali, ecc.
- Enti economici locali, quali aziende municipalizzate, le società in-house e le società miste.
- Aziende sanitarie e ospedaliere locali, inclusi gli istituti di ricovero e cura pubblici a carattere scientifico, ed altri enti di supporto al Sistema Sanitario Nazionale
- Camere di commercio
- Università ed Istituti di istruzione universitaria
- Altri enti locali, quali Agenzie regionali, Consorzi di bonifica, Fondazioni, Istituti regionali, Musei, ecc.

Dalle province al più piccolo degli enti locali, le PAL rappresentano i principali terminali dei servizi pubblici a cittadini ed imprese, nell'ambito di territori che presentano numerose specificità e differenze. Tali servizi coprono una pluralità di fabbisogni per la cittadinanza quali, a titolo puramente esemplificativo e non esaustivo:

- Servizi informativi (Ufficio Relazioni con il Pubblico, siti internet, ecc.)
- Servizi socio-assistenziali e sanitari
- Rilascio di certificati e documenti
- Servizi alle persone ed alle imprese per l'impiego
- Rilascio di autorizzazioni per l'avvio di attività commerciali e produttive sul territorio
- Accertamento e riscossione di tributi locali
- Servizi per l'infanzia e per l'istruzione
- Pubblica Sicurezza sul territorio

Tali servizi a carico delle Pubbliche Amministrazioni determinano la raccolta e il trattamento di un enorme volume di dati di tipo riservato (personali, sensibili, ecc.) e di altre informazioni di tipo cogente, rendendole di fatto un bersaglio estremamente appetibile nello spazio cibernetico, con potenziali rischi legati alla sottrazione, alterazione e distruzione di informazioni, al blocco ed all'alterazione di servizi, ecc. Tale situazione è ulteriormente accentuata considerando che gran parte dei servizi precedentemente elencati sono oggi offerti sul territorio tramite il web o l'utilizzo di dispositivi mobili.

Sono invece da ritenersi escluse dalla Constituency dei CERT regionali tutte le PAC e le relative articolazioni che continuano ad aderire al servizio di accreditamento offerto dal CERT-PA. Nel caso delle Regioni sono i CERT regionali, laddove costituiti, ad accreditarsi verso il CERT-PA, e l'ente "Regione" a beneficiare in maniera diretta dei servizi offerti da quest'ultimi.

Va comunque sottolineato che tutte le PA, centrali e locali, in assenza della costituzione di un CERT regionale competente per il territorio, sono da ritenersi parte della Constituency complessiva del CERT-PA.

[65] Un elenco aggiornato delle PAL è pubblicato in: http://www.indicepa.gov.it/public-services/docs-read-service.php?dstype=FS&filename=Categorie_ Amministrazioni.pdf

Le PAL potranno accedere ai servizi offerti dai CERT regionali a valle di un processo di accreditamento, tramite il quale:

- le PAL aderenti possono richiedere il coinvolgimento del CERT regionali per la gestione degli incidenti di sicurezza informatica sulla base di modalità attuative regolamentate da protocolli di comunicazione e da procedure operative di risoluzione ed escalation;
- i CERT regionali possono raccogliere in modo ufficiale tutte le informazioni tecniche ed organizzative per la gestione dell'incidente.

Potranno essere previsti più livelli di accreditamento rispetto ai quali profilare la Constituency, che si differenziano dal punto di vista della comunicazione e dell'interazione attesa tra il CERT regionale e la PAL e del livello di partecipazione attiva attesa di ciascun membro verso la comunità. In linea generale è possibile considerare almeno due livelli di accreditamento:

- Livello Base, caratterizzato da un'interazione puramente informativa, che richiede la registrazione della PAL sul portale del CERT regionale, attraverso il quale le sarà consentito di accedere ad un'area riservata ed ottenere informazioni (es. bollettini informativi, statistiche di settore, ecc.);
- Livello Avanzato, nell'ambito del quale potranno essere identificati enti che, per maturità dei presidi di sicurezza e di competenze specialistiche sviluppate al proprio interno, potrebbero essere in grado di fornire, ove ritenuto necessario, un contributo attivo all'erogazione dei servizi del CERT e/o al miglioramento dei servizi stessi.

CAPITOLO 6

Modello organizzativo

La struttura organizzativa del CERT è un aspetto critico per supportare operazioni efficaci e proattività nei confronti della propria constituency. In termini di responsabilità e coordinamento, il CERT può organizzarsi in modi diversi:

- *Livello di autorità completo*: può operare con piena autorità, guidando la constituency a compiere le azioni necessarie per migliorare la security posture dell'organizzazione o per recuperare da un incidente;
- *Livello di autorità condiviso:* può operare in un regime di autorità condivisa, collaborando con la constituency per influenzare il processo decisionale su quali azioni dovrebbero essere intraprese, senza tuttavia poterle imporre;
- *Livello di autorità assente:* può adottare un modello che non attribuisce autorità al CERT, limitandone la portata a azioni consultive per la constituency, senza alcun potere decisionale.

Si noti che alcuni servizi offerti tipicamente da un CERT (e presentati più avanti in dettaglio nel Cap. 9 "Servizi"), potrebbero essere offerti solo in presenza di un livello di autorità completo o parziale nei confronti della propria constituency. Si pensi ad esempio al caso di eventuali servizi di tracciamento degli incidenti e di monitoraggio e rilevamento di tentativi di intrusione, che solo in forza di specifici accordi contrattuali tra i membri della constituency coinvolti e il CERT potrebbero essere erogati.

Sulla base del modello di autorità, il CERT può operare con modelli distribuiti, centralizzati o coordinati. Il modello strutturale del CERT che si intende creare dipenderà sia dalla mission e dai servizi che si vogliono offrire, sia dalla constituency che sarà servita. In letteratura sono definiti tre modelli di CERT operativi[66]:

- Indipendente;
- Incorporato;
- Campus.

6.1 Modello indipendente

In questo modello il CERT viene sviluppato e agisce come organizzazione indipendente, con una propria direzione e proprie risorse, pur essendo collocato all'interno di un ente (che potrà essere a sua volta parte della constituency).

[66] ENISA, "*Un approccio graduale alla creazione di un CSIRT*", Documento WP2006/5.1(CERT-D1/D2) (2006)

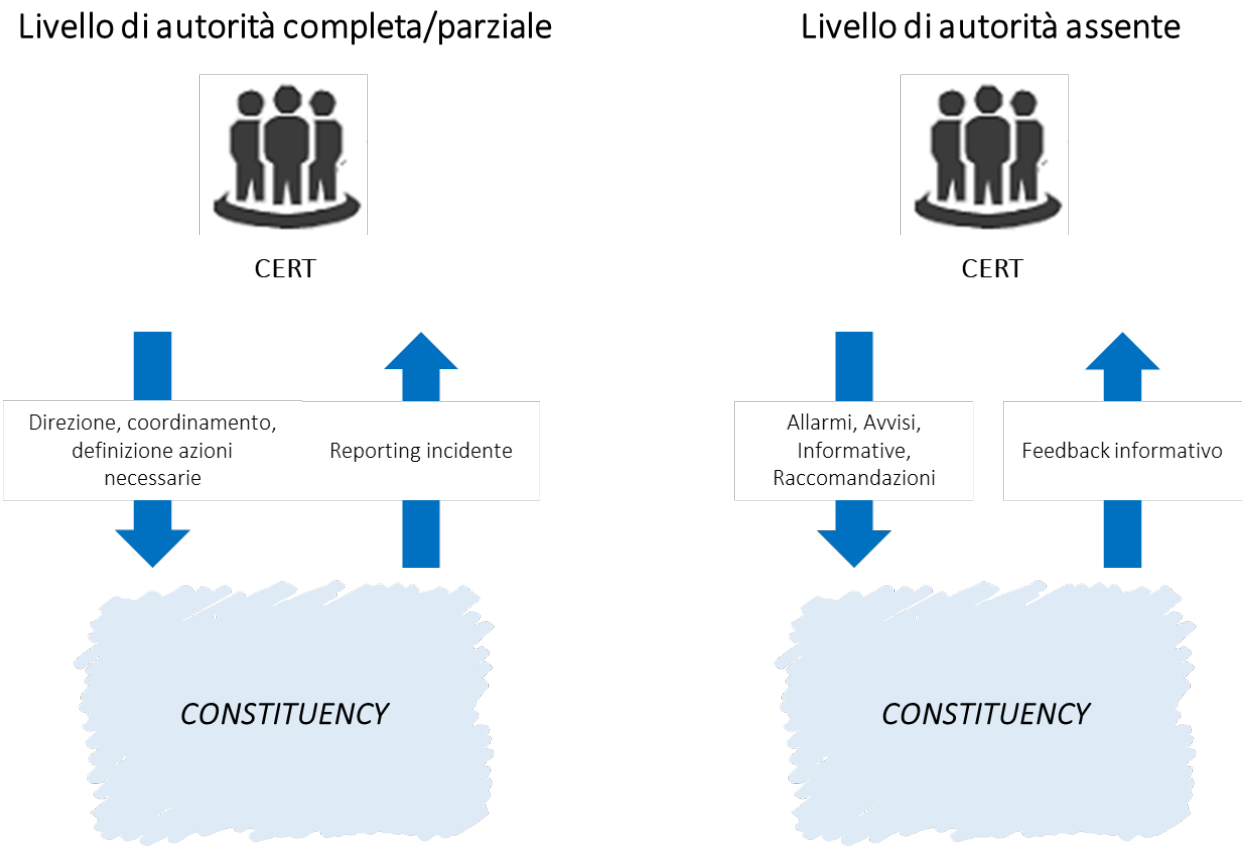

Fig. 6.1: Confronto tra livelli di autorità

Il modello indipendente è basato su un CERT dedicato e centralizzato che detiene la piena responsabilità e autorità per tutte le attività di analisi, gestione e risposta agli incidenti. Il personale operativo è assegnato formalmente e stabilmente al CERT, riportando al responsabile di questa unità (Responsabile CERT, si veda par. 10.1.1).

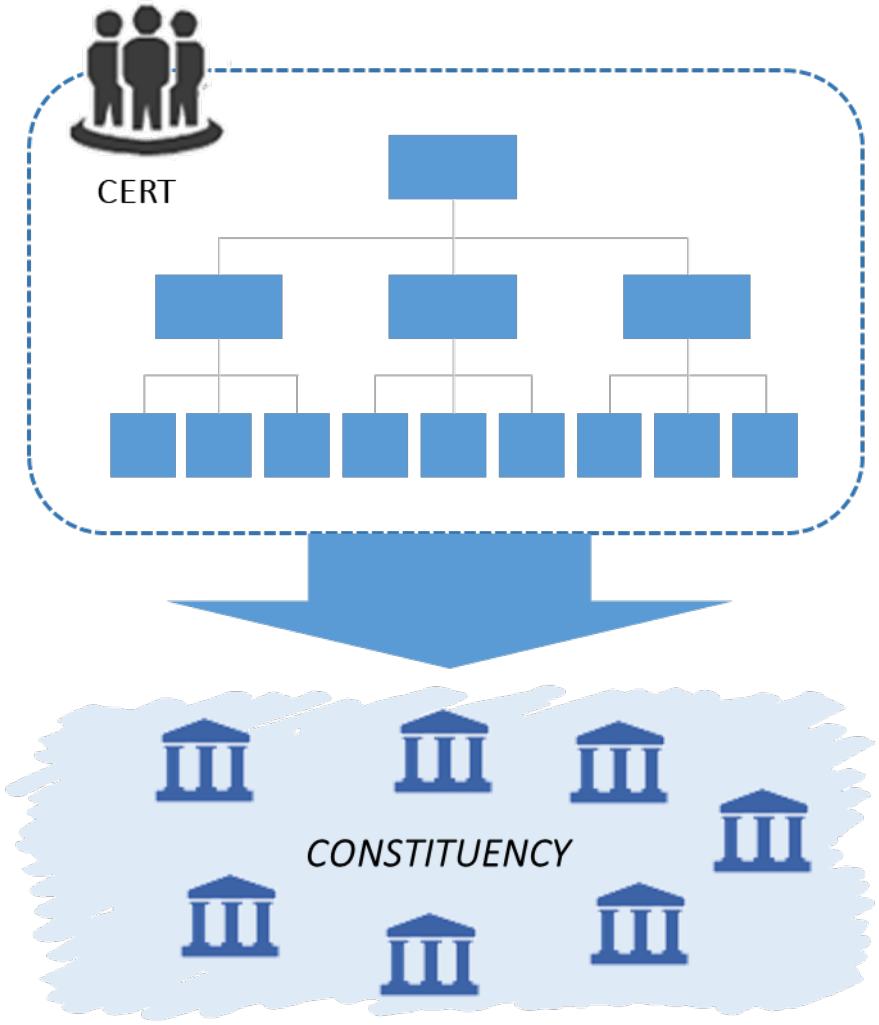

Fig. 6.2: Modello indipendente

6.2 Modello incorporato

Questo modello può essere usato se si intende creare un CERT all'interno di un'organizzazione esistente, facendo leva su risorse già operanti ed allocate presso altre strutture organizzative, che impieghi risorse dell'ente già allocate presso altre strutture organizzative interne, ad esempio la Funzione IT e di Sicurezza. Il CERT è guidato da un responsabile che risponde delle attività complessive del CERT. Il responsabile riunisce gli specialisti necessari per risolvere gli incidenti o lavorare alle attività del CERT e può chiedere assistenza all'interno dell'organizzazione per ricevere sostegno.

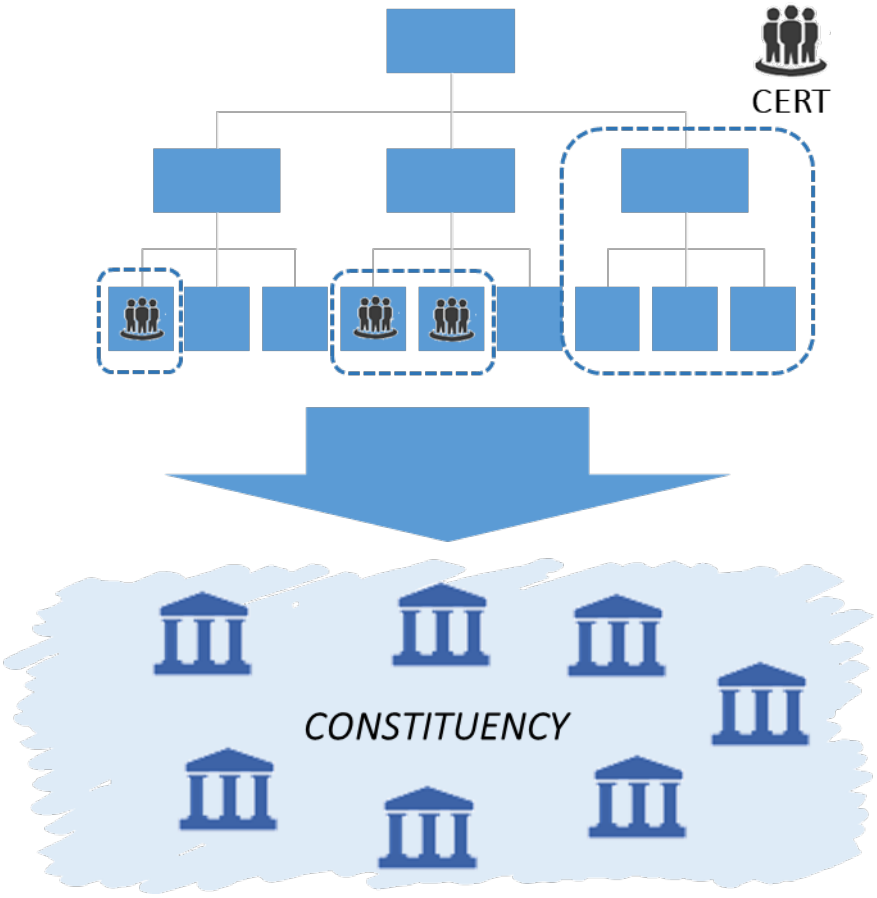

Fig. 6.3: Modello incorporato

6.3 Modello campus

Ogni entità del campus è indipendente dal CERT e da tutti le altre entità che compongono la constituency. Questo modello prevede che il CERT, pur essendo distaccato, impieghi, oltre al personale assegnato in modo permanente, le risorse che le altre organizzazioni appartenenti alla constituency sono in grado di metterle a disposizione (ad esempio perché dotati di un proprio SOC) tra i membri della constituency. Il CERT erogherà i suoi servizi sia verso gli enti che forniscono le risorse, sia verso tutti gli altri membri della constituency.

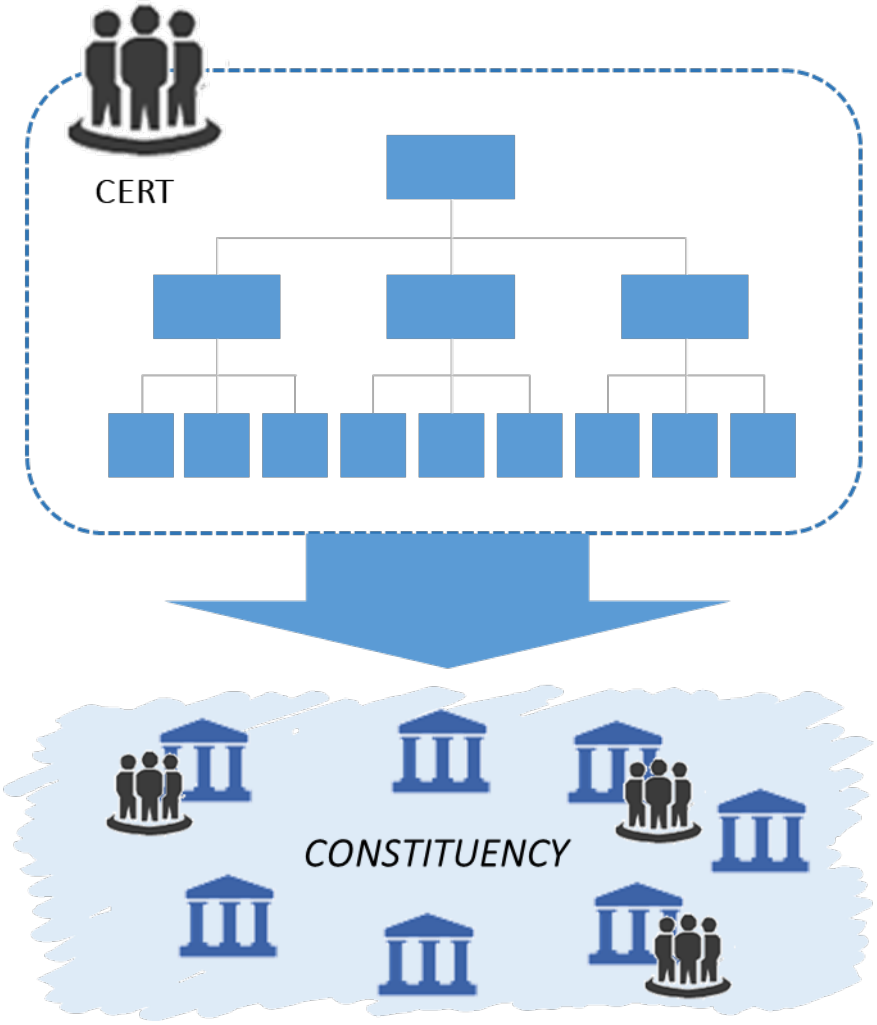

Fig. 6.4: Modello campus

Il modello campus è quello più adottato nei CERT di settore, tra i quali rientrano anche i CERT accademici/di ricerca e quelli militari, in quanto consente di bilanciare ottimamente le necessità di coordinamento centrale con quelle di autorità locale, come nel caso di utenti singoli o consorziati riconducibili ad uno stesso ambito professionale o caratterizzati da interessi comuni (ad esempio salute, trasporti, ecc.). Di contro, si possono considerare il modello indipendente ed incorporato come assetti più indicati per un CERT territoriale, anche in presenza di constituency caratterizzate da distribuzioni geografiche particolarmente estese, che può operare in maniera efficace sotto la supervisione dell'ente che lo ha istituito.

CAPITOLO 7

Modello amministrativo

Da un punto di vista amministrativo, i CERT possono adottare assetti differenti a seconda del fatto che:

- siano un'articolazione interna all'organizzazione ospitante, ovvero una funzione o un dipartimento, preposta a tale fine oppure cui vengono affidate responsabilità ulteriori;
- siano inseriti in una società in-house, già esistente o costituita ad-hoc, nella forma di soggetto giuridico il cui capitale è detenuto in toto o in parte, direttamente o indirettamente, da un'organizzazione che affida l'erogazione dei servizi.
- ci si affidi ad un'organizzazione esterna per la fornitura del servizio CERT, anche attraverso meccanismi di outsourcing.

Il primo scenario è caratterizzato da una minore complessità amministrativa in fase di start-up (adempimenti societari, gestione del personale, ecc.), dalla possibile riduzione dei tempi di avvio, legata al punto precedente, e da una maggiore efficienza operativa derivante dalle possibili sinergie con il resto dell'organizzazione. Di contro si evidenzia tuttavia che tale assetto può comportare la necessità di istituire pratiche e processi definiti a garanzia della separazione dei ruoli e delle responsabilità e volti ad impedire una possibile sovrapposizione degli stessi rispetto alle attività caratteristiche dell'ente che ospita il CERT.

Il ricorso ad un soggetto giuridico distinto rappresenterebbe, da un lato, una garanzia di unicità di scopo ed autonomia gestionale intrinseca, ma comporterebbe dall'altro una maggiore complessità amministrativa, soprattutto in fase di start-up, con evidenti tempi di avvio più lunghi nonché costi di gestione più elevati con potenziale duplicazione degli incarichi apicali.

Una soluzione percorribile per i CERT di una rete nazionale, e già percorsa ad esempio da alcune realtà territoriali nel nostro Paese, è quella di costituire dei gruppi di lavoro estesi ai quali potrebbero partecipare i diversi rappresentanti della constituency (imprese, enti territoriali, società in-house, ecc.) e i rappresentati dei settori di interesse.

I vantaggi di questo approccio sono molteplici:

- il coinvolgimento di ulteriori soggetti riduce la quota parte di costi fissi a carico di ogni ente con un incremento minimo dei costi variabili dovuti alla gestione di categorie di soggetti eterogenee;
- le competenze presenti sul territorio – o costituite secondo necessità – diventano un patrimonio comune di tutti i soggetti interessati, scoraggiando anche un potenziale turn over delle stesse tra i diversi CERT;

- il patrimonio informativo di conoscenze viene condiviso tra tutti i soggetti, favorendo una più pronta risposta ad eventuali incidenti grazie anche alla possibilità di coordinare i vari soggetti da un un'unica regia.

Un'ulteriore possibilità per implementare le capacità necessarie a garantire l'operatività della struttura, consiste nel ricorrere a competenze esterne reperibili nel settore privato per interi ambiti di servizio o per singole aree di intervento ad elevato tasso di specializzazione. I CERT dovrebbero poter disporre di staff con competenze ed esperienze su tutti i sistemi, le piattaforme e le infrastrutture informatiche impiegate dalla comunità servita.

Nell'ambito del contesto nazionale, in considerazione della ampia e variegata constituency identificata, e in assenza di un censimento completo degli asset tecnologici in uso presso gli utenti coinvolti, risulta tuttavia poco realistico e difficilmente percorribile nell'immediato poter disporre all'interno del singolo CERT di tutte le esperienze, conoscenze e competenze necessarie.

Alcuni dei principali benefici che possono portare un'organizzazione ad acquisire risorse e competenze esterne possono essere:

- riduzione dei costi e vantaggio economico conseguibile a fronte dell'affidamento ad un soggetto esterno caratterizzato da una maggiore specializzazione, ovviando dunque alla carenza di alcune professionalità o tecnologie abilitanti;
- possibilità di rispondere in tempi rapidi all'innovazione tecnologica, in determinati ambiti, spesso inattuabile a livello di singole organizzazioni locali che potrebbero operare in condizioni di risorse limitate;
- definizione di un corrispettivo contrattuale verso il service provider, vincolato ad un risultato o alle prestazioni;
- raccolta di indicazioni che emergono attraverso il confronto ed il benchmarking con altre esperienze e la scelta di riprodurre all'interno del CERT buone pratiche e casi di successo.

CAPITOLO 8

Servizi

8.1 Modelli di classificazione dei servizi

Secondo le pubblicazioni più autorevoli sul tema[67], i servizi offerti da un CERT possono essere suddivisi in quattro categorie principali:

- *Servizi Reattivi*: volti a gestire gli incidenti quando si verificano, riducendone il danno conseguente e a rispondere alle richieste di assistenza dalla constituency di riferimento. Possono avere origine da notifiche di terzi o dalle capacità interne/esterne di monitoraggio e individuazione delle minacce.
- *Servizi Proattivi*: orientati alla prevenzione degli incidenti, mediante la condivisione delle informazioni e/o l'utilizzo di strumenti specifici. Sono concepiti per migliorare quindi le infrastrutture e i processi di sicurezza della comunità di riferimento prima che si verifichi o sia rilevato un incidente o evento di sicurezza. Includono anche le attività volte a gestire e distribuire le informazioni ottenute da fornitori e altre comunità che possono aiutare a limitare la diffusione di attacchi analoghi o futuri.
- *Servizi di Gestione della Qualità della Sicurezza*: comprendono tutte le pratiche volte a migliorare la sicurezza generale di un membro della constituency, concepite per incorporare i riscontri e gli insegnamenti tratti sulla base delle conoscenze acquisite rispondendo a incidenti, vulnerabilità e attacchi.
- *Gestione degli Artefatti*: prevede la raccolta e l'analisi di qualsiasi elemento o evidenza (file, codici malevoli, tracce in memoria) che sono impiegati o in generale sono coinvolti nella realizzazione di azioni malevole.

Una possibile declinazione dei servizi afferenti alle categorie precedentemente illustrate è rappresentata nella tabella a seguire:

[67] ENISA, "*Un approccio graduale alla creazione di un CSIRT*", Documento WP2006/5.1(CERT-D1/D2) (2006); CMU-SEI "*Handbook for Computer Security Incident Response Teams*" (2003).

Tabella 8.1: Elenco dei servizi CERT (fonte: CERT/CC, ENISA)

Servizi reattivi	Servizi proattivi	Gestione della qualità della sicurezza	Gestione degli artefatti
• Allarmi e avvisi • Gestione degli incidenti • Analisi degli incidenti • Sostegno della risposta agli incidenti • Coordinamento della risposta agli incidenti • Risposta agli incidenti in loco • Gestione delle vulnerabilità • Analisi delle vulnerabilità • Risposta alle vulnerabilità • Coordinamento della risposta alle vulnerabilità	• Annunci • Controllo tecnologico • Revisioni e valutazioni della sicurezza • Configurazione e mantenimento della sicurezza • Sviluppo di strumenti di sicurezza • Servizi di rilevamento intrusioni • Divulgazione di informazioni relative alla sicurezza	• Analisi dei rischi • Continuità operativa e ripristino in caso di disastro • Consulenza sulla sicurezza • Sensibilizzazione • Istruzione / formazione • Valutazione o certificazione dei prodotti*	• Analisi degli artefatti • Risposta agli artefatti • Coordinamento della risposta agli artefatti

Nell'ambito della presente trattazione, si propone di adottare, ai fini della definizione del catalogo dei servizi essenziali offerti da un CERT Regionale, un modello alternativo di classificazione dei servizi, il modello "IRPA" (Incident Response PA), in uso presso il CERT-PA. Tale scelta è orientata alla possibilità di sfruttare eventuali sinergie e definire, con riferimento ai CERT Regionali, un insieme di servizi supplementari offerti rispetto a quanto oggi realizzato dal CERT-PA verso la propria constituency.

Gli obiettivi principali del modello IRPA nel dominio della PA italiana sono:

- prevenire e/o ridurre gli impatti di incidenti sulla sicurezza delle informazioni;
- stabilire un modello strategico per i ruoli e le responsabilità dei differenti attori nel processo di gestione degli incidenti di sicurezza informatica;
- raccordare e mantenere le diverse politiche e dottrine esistenti in un piano strategico di IRPA che sia unitario e contestualizzato;
- facilitare la consapevolezza, la condivisione delle informazioni, il coordinamento e l'esecuzione durante la gestione ordinaria e soprattutto durante la gestione delle crisi;
- stabilire quando e come le attività operative debbano scalare ad attività di risposta coordinata su tutta la PA o a livello nazionale;
- focalizzare gli incidenti con impatti sulla sicurezza, sulla salute, sull'economia dei cittadini e sulla credibilità della PA.

Il modello IRPA definisce pertanto un sistema di indirizzamento e coordinamento trasversale che supporta le Amministrazioni Pubbliche, le infrastrutture critiche e le organizzazioni private nelle:

- attività di analisi delle minacce e di nuovi scenari di rischio tecnologico o organizzativo;

- attività di prevenzione e contenimento dei rischi derivanti da incidenti informatici che possano pregiudicare, direttamente o indirettamente, il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale della Nazione e dei suoi Cittadini.

Il modello IRPA propone 16 servizi complessivi organizzati in cinque fasi distinte:

- *fase di preparazione e prevenzione*, finalizzata alla stesura delle regole da adottare su base nazionale sulla sicurezza della PA, basate anche sull'esperienza data dagli incidenti passati, nonché sulla diffusione di informative e/o alert di sicurezza che favoriscano l'innalzamento del livello di consapevolezza all'interno della PA verso tematiche di cyber security;
- *fase di rilevazione*, finalizzata al rilevamento di incidenti attraverso l'utilizzo di apparati di sicurezza di monitoraggio, la condivisione delle informazioni, l'open- e il closed-source intelligence;
- *fase di analisi*, finalizzata all'analisi e classificazione di incidenti segnalati dalle PA facenti parte della constituency, con ulteriore raccolta ed analisi approfondita delle evidenze;
- *fase di risposta*, finalizzata alla definizione e coordinamento delle attività di risposta tra le PA, gli ISP, i media ed il CERT-Nazionale, con contestuale valutazione ed applicazione delle normative di riferimento (ad es. ingaggio delle autorità competenti in caso di frodi o crimini informatici);
- *fase di ripristino*, finalizzata alla definizione delle modalità di ripristino dei servizi una volta che la minaccia è stata neutralizzata.

I servizi proposti dal modello IRPA sono illustrati nella tabella seguente:

Tabella 8.2: Modello dei servizi basato su IRPA

Fase Modello IRPA	Servizi
Preparazione e prevenzione	• Accreditamento e linee guida • Informative • Formazione e awareness • Supporto al risk mapping • Security assessment e consulenza
Rilevazione	• Ticketing • Threat intelligence
Analisi	• Correlazione • Analisi incidente • Triage & escalation
Risposta	• Coordinamento della risposta • Supporto alle azioni di risposta • Monitoraggio della risposta
Ripristino	• Analisi post-incidente e coordinamento • Monitoraggio del ripristino
Tutte le fasi	• Information Sharing

8.2 Servizi offerti dai CERT Regionali

I servizi che un CERT Regionale può offrire sono molteplici. La selezione dell'insieme dei servizi da offrire costituisce una decisione di cruciale importanza per il raggiungimento degli obiettivi prefissati e lo sviluppo delle relative capacità operative.

In primo luogo, i servizi offerti da un CERT Regionale dovranno essere determinati a partire dall'analisi delle necessità della propria constituency, identificando sin da subito i servizi minimi ed essenziali, o a maggior rilevanza per la comunità delle PAL interessate. Un approccio troppo ambizioso, volto all'erogazione di un numero di servizi eccessivo rispetto al reale fabbisogno della constituency o alla effettiva disponibilità di risorse del CERT, rischierebbe di minare in partenza la fattibilità realizzativa del costituendo CERT e, nel lungo periodo, la sua sostenibilità. L'attivazione di servizi specifici potrà avvenire progressivamente, potendo al termine di una fase pilota valutare eventualmente l'espansione del portafoglio di servizi offerti, aggiungendone di nuovi. Tale decisione sarà presa anche sulla base del riscontro dato dalla comunità di riferimento.

In secondo luogo, il modello di servizio definito dai CERT Regionali dovrà essere supplementare rispetto a quello definito ed implementato dal CERT-PA. È auspicabile in tal senso che il CERT Regionale, almeno in una fase iniziale, si impegni ad attivare quei servizi (*servizi di base/essenziali*) per i quali una maggiore prossimità al territorio potrebbe determinare significativi miglioramenti dei livelli di efficacia garantiti nei confronti della constituency locale rispetto a quanto possibile realizzare attraverso un'unica azione centralizzata da parte del CERT-PA.

Non si escludono comunque in linea di principio la possibilità e l'opportunità per i CERT Regionali di costruire ed attuare un percorso di crescita che passi attraverso il progressivo sviluppo di servizi caratterizzati da un maggiore livello di complessità tecnica e di contenuto. In tal senso, a fronte di livelli di maturità raggiunti più elevati, il CERT Regionale potrà valutare, in base alle risorse disponibili, quali ulteriori servizi offrire, basando tale valutazione, possibilmente, su un processo di valutazione dei rischi che identifichi le maggiori priorità per la constituency.

I due fattori da prendere in considerazione per individuare i servizi essenziali che il CERT Regionale dovrà offrire sono il grado di complessità realizzativa del servizio abbinato alla sua rilevanza per la comunità di riferimento. Nei paragrafi successivi sono illustrati i servizi di base per il CERT Regionale, ovvero quei servizi che un CERT deve necessariamente fornire alla propria constituency, considerando però anche il livello di risorse necessario all'erogazione.

8.2.1 Accreditamento

L'Accreditamento è un servizio che, relativamente a un CERT regionale, che è una struttura intermedia tra il CERT-PA e le PAL, presenta due aspetti:

1. il CERT regionale si accredita nei confronti del CERT-PA entrando a far parte della sua constituency
2. la singola PAL si accredita nei confronti del CERT regionale entrando a far parte della sua constituency

Per quanto riguarda il primo punto, il CERT-PA mette a disposizione della propria constituency un portale dedicato attraverso il quale

- ricevere aggiornamenti, in modo manuale e/o automatico[68], su nuove vulnerabilità/minacce. La modalità manuale comporta la distribuzione di News e Bollettini, blacklist e l'accesso al portale di Infosharing (https://infosec.cert-pa.it/). La modalità automatica fa uso di STIX/TAXII e MISP;
- accedere a un'area riservata ove poter scaricare materiale rivolto ai membri della constituency e informazioni riservate (IOC, dump di username/password disponibili sul "mercato" hacker);
- accedere ai servizi di Threat Intelligence
- utilizzare un canale riservato e criptato GPG per la trasmissione di informazioni sensibili o potenziali malware;
- partecipare ad eventuali eventi di formazioni organizzati dal CERT;

[68] Maggiori dettagli su questa modalità nel seguito

- ricevere assistenza consulenziale dedicata.

Nel secondo caso, invece, un potenziale membro della constituency di un CERT Regionale (nel senso che rispetta i requisiti[69] necessari per poterne far parte) ne richiede effettivamente l'ingresso. Le motivazioni sono quelle già viste e cioè la possibilità di usufruire dei servizi che il CERT mette a disposizione alla propria utenza. Al momento della richiesta di Accreditamento, il Referente della sicurezza informatica della PAL provvede a contattare il CERT Regionale attraverso i canali preposti e, dopo essersi fatto adeguatamente riconoscere cioè dopo aver fornito la prova della propria identità e ruolo nell'ente, si impegna a fornire al CERT le informazioni richieste per una corretta trattazione degli incidenti di sicurezza e, in particolare:

- *Identificazione delle persone dell'ente in grado di intervenire in caso di incidente informatico e comunicazione delle relative modalità di contatto* – le figure identificate devono essere in grado di poter gestire una crisi informatica in tutti i suoi aspetti con particolare riferimento al trattamento delle informazioni sensibili che possano essere state esfiltrate durante l'attacco cibernetico, alla comunicazione dell'incidente sia verso l'interno che verso l'esterno dell'organizzazione, al coordinamento di tutte le figure e le aree dell'organizzazione necessarie al contenimento del problema e al ripristino dell'operatività nonché alla raccolta di evidenze per eventuali prosecuzioni a livello processuale. Di tali figure dovrebbero essere forniti, oltre ai nominativi, il ruolo aziendale, le modalità di contatto (numero di telefono fisso, cellulare, e-mail e quant'altro necessario), la fascia oraria di contatto e, al di fuori di essa, degli eventuali sostituti. Tale elenco di informazioni deve essere assolutamente tenuto aggiornato nel tempo (a prova cioè di dimissioni, trasferimento di ruolo, pensionamento, trasferimento a altre sedi ecc.). Va tenuto presente che il Referente della sicurezza informatica della PAL, o la persona da lui preposta, è la prima persona che verrà avvertita in caso di un'eventuale crisi di sicurezza cibernetica e il fatto che non sia disponibile quando necessario può portare a un pericoloso ritardo nella gestione della crisi stessa.
- *La presenza o meno di una procedura documentata per la gestione di incidenti di sicurezza* – questa informazione serve al CERT per capire il livello di maturità dell'ente relativamente alla gestione dell'incidente e l'eventuale adozione di best practice al riguardo ma anche se l'ente è in grado di raccogliere le informazioni necessarie al trattamento dell'incidente.
- *La presenza o meno di una documentazione di analisi del rischio e della classificazione di informazioni* – questa informazione serve al CERT per capire se l'ente è conscio dell'eventuale effetto domino che un incidente di sicurezza può causare e, in particolare, se è in grado di valutarne l'impatto.
- *L'elenco dei domini e degli indirizzi di rete che afferiscono all'ente*
- *Un elenco dell'hardware e del software utilizzato* – questo permette al CERT di comunicare in modo più efficace eventuali nuove vulnerabilità scoperte inviando solo le informazioni di pertinenza e riducendo quelle non necessarie. L'informazione trasmessa, quindi, ha già subito un'iniziale scrematura.

Più in generale, il CERT deve essere visto come un servizio "amico" e di supporto, un prezioso partner nella gestione degli incidenti di sicurezza con cui condividere tutte le informazioni necessarie, ovviamente nel rispetto di regolamenti e policies. D'altra parte, un CERT non può assolutamente sostituirsi alle best practice interne all'ente e alla corretta gestione "da buon padre di famiglia". Un CERT deve avvertire, consigliare, aiutare (e tutto ciò in modalità best effort sulla base delle risorse assegnate) ma non può e non deve assolutamente coprire le mancanze nella gestione dell'ente facente parte della constituency e, in ultima analisi, non ha comunque responsabilità degli eventuali problemi interni all'ente causati da un incidente informatico.

Una volta che la procedura di Accreditamento è andata a buon fine l'ente in generale potrà accedere a tutti i servizi che il CERT regionale mette a disposizione della propria constituency.

8.2.2 Informative

Il servizio di Informative è lo strumento che permette al CERT-Regionale di diffondere alle PAL accreditate, sotto forma di alert periodici, bollettini di sicurezza, generiche informative o segnalazioni di sicurezza, informazioni su:

[69] Ad es. nel caso di un CERT regionale, che ha fondamentalmente giurisdizione territoriale, il fatto di avere la sede nel territorio di competenza

- nuovi scenari di rischio di tipo tecnologico, normativo ed organizzativo, che presentano un impatto rilevante per le PAL facenti parte della constituency;
- insorgenza di nuove minacce o di nuove vulnerabilità ai danni di sistemi e applicazioni in uso presso tali PAL;
- presenza di attacchi in corso ai danni di PAL, che possono determinare un certo grado di impatto per l'infrastruttura tecnologica gestita;
- azioni sviluppate da altri soggetti operanti nella comunità delle PAL in risposta ad eventi e/o incidenti di sicurezza.

Tale servizio è in grado di agevolare la diffusione di informazioni tempestive e immediatamente utilizzabili su nuovi scenari di rischio, attacchi in corso, trend di fenomeni cyber indirizzati a specifici settori e possibili impatti per le PAL e la loro utenza. Facilitando l'attività informativa di prevenzione sul territorio, i CERT Regionali possono quindi agire come unità capaci di esercitare un controllo più diretto a livello locale nei confronti della constituency e garantire in questo modo la divulgazione di informazioni mirate.

8.2.3 Formazione e Awareness

Il servizio di Formazione e Awareness è volto ad aumentare il livello di consapevolezza del personale delle PAL addetto alla gestione dei processi di sicurezza informatica su:

- principi di gestione della sicurezza delle informazioni e di cyber security;
- tematiche specifiche, quali risk management e gestione degli incidenti di sicurezza;
- processi e procedure adottate nel dominio della PA per favorire l'interazione e la cooperazione tra enti locali e CERT Regionali.

Tale servizio potrà essere attivato a fronte di richieste specifiche da parte delle PAL accreditate. Il servizio può prevedere corsi periodici di formazione in aula o da remoto (attraverso l'accesso a un sito di didattica remota), oppure essere realizzato attraverso iniziative di sensibilizzazione definite a tale scopo (workshop, eventi su base locale, ecc.). Inoltre, possono essere promosse campagne informative a livello territoriale rispetto ai rischi di sicurezza informatica affrontati dagli enti locali.

8.2.4 Ticketing

Il servizio di Ticketing costituisce il punto di ingresso per il processo di Incident Response ed ha il compito di tenere traccia di tutti i potenziali incidenti e delle informazioni ad essi correlate tramite l'ausilio di una piattaforma tecnologica di trouble ticketing. Utilizzando tale piattaforma:

- gli utenti abilitati di ciascuna PAL accreditata può aprire direttamente o richiedere l'apertura di un ticket verso il CERT Regionale per la segnalazione di incidenti di sicurezza all'interno del proprio Ente;
- gli analisti del CERT Regionale di riferimento aggiornano le informazioni contenute nei ticket attraverso l'inserimento dei risultati delle analisi effettuate in ciascuna fase del processo di gestione degli incidenti, allegando eventuale documentazione raccolta (mail scambiate con vendor, documenti analizzati, contenuto di eventuali comunicazioni verbali, ecc.).

Tramite la piattaforma di ticketing, gli analisti del CERT Regionale possono aprire a loro volta ticket ad altre strutture e monitorare lo stato di avanzamento nella lavorazione di ciascun evento segnalato. Possono inoltre tenere traccia dello stato di lavorazione di ciascun incidente segnalato, semplificando le attività di monitoraggio dei livelli di servizio e di tutte le attività effettuate dagli attori coinvolti.

Il servizio di ticketing offre inoltre l'opportunità di raccogliere e centralizzare tutte le informazioni relative agli incidenti, alimentando pertanto la knowledge base con la quale il CERT Regionale è in grado di effettuare tutte le analisi di propria competenza, correlando tra loro, ove necessario, segnalazioni provenienti da PAL distinte ed evidenziando eventi sospetti o schemi di attacco ripetuti.

8.2.5 Correlazione

Il servizio di Correlazione permette al CERT regionale di mettere in relazione le segnalazioni provenienti dal ticketing e le informazioni raccolte da altre fonti, tra cui il CERT-PA, per fornire al servizio di analisi dell'incidente una visione di insieme su ciascuna segnalazione pervenuta.

In particolare, tramite la piattaforma di trouble ticketing e la knowledge base da essa alimentata, si cercano correlazioni tra ticket diversi, indice di:

- pattern di attacco ripetuti nel tempo o verso target diversi;
- eventuali eventi ad impatto sistemico o trasversale tra diverse PAL.

8.2.6 Analisi degli incidenti

Rispetto ad un incidente segnalato e classificato autonomamente da una PAL, il gruppo di analisti di sicurezza del CERT Regionale attiva il servizio di Analisi Incidente, per:

- la verifica e l'analisi delle informazioni inviate dalla PAL e allegate al ticket;
- la verifica della classificazione effettuata dalla PAL e l'eventuale ri-classificazione dell'evento stesso, valutandone l'impatto in un'ottica di tipo sistemico ed incrociando le informazioni ricevute con ulteriori indicazioni ad esso correlate, ricevute da altre PAL.

8.2.7 Triage & escalation

Con il servizio di Triage e Escalation il CERT Regionale effettua una normalizzazione degli incidenti segnalati, esprimendo la criticità dell'incidente secondo una scala ordinale su più livelli di impatto[70].

Al termine della fase di triage il CERT Regionale può procedere con le seguenti azioni:

- de-classifica dell'incidente in caso di falso positivo, inviando una comunicazione alla PAL coinvolta e chiudendo il ticket, nel quale viene allegato il risultato delle analisi effettuate.
- modifica del livello di classificazione precedentemente assegnato e comunicato dalla PAL segnalante;
- avvio delle necessarie attività di trattamento dell'incidente, secondo le procedure operative condivise con le PAL in fase di accreditamento.

In caso di incidenti distribuiti, che presentano quindi impatti di sicurezza su PAL distinte appartenenti alla propria constituency, il CERT Regionale invierà una segnalazione urgente alle PA coinvolte, coordinando tutte le seguenti attività di gestione incidente.

In caso di incidenti di Livello massimo (es. livello 3 secondo la scala che verrà descritta più avanti), il CERT Regionale dovrà attivare lo stato di Emergenza ed effettuata un'escalation verso il CERT-PA, coordinandosi con lo stesso per tutte le seguenti attività di gestione incidente.

8.2.8 Supporto alle azioni di risposta

In fase di Supporto alle Azioni di Risposta il CERT Regionale supporta le PAL della propria constituency fornendo possibili soluzioni agli incidenti in termini di procedure, modalità ed eventualmente competenze sullo specifico attacco in caso l'Ente ne fosse sprovvisto.

In particolare il CERT Regionale supporterà la PAL nella definizione del piano di trattamento dove vengono indicati:

[70] Si suggerisce in tal senso l'adozione di una scala ordinale a cinque livelli di impatto (livello 0 - livello 4) analoga a quella in uso presso il CERT-PA e che verrà descritta più avanti.

- i servizi e i sistemi coinvolti nell'attacco, con il relativo livello di classificazione;
- le misure di contrasto e contenimento progettate per il trattamento dell'incidente ed il rientro nello stato ordinario;
- i risultati attesi dall'applicazione delle suddette contromisure.

Nel caso di incidenti a rilevanza sistemica, il CERT Regionale procede al coinvolgimento delle PAL interessate dall'incidente, inviando tutte le informazioni necessarie per il trattamento dell'incidente in corso.

8.2.9 Information Sharing

L'Information Sharing costituisce lo scheletro di funzionamento dei processi del CERT e di tutta la rete di CERT ed altre entità a livello nazionale ed internazionale con cui lo stesso può entrare in contatto, in quanto definisce le regole e le modalità di condivisione delle informazioni in ingresso ed in uscita con tutti gli interlocutori. L'Information Sharing deve assicurare la comunicazione tempestiva delle informazioni a tutte le parti interessate. Una corretta condivisione di informazioni deve consentire al CERT di raccogliere l'input, elaborare e processare l'output, mantenendo i livelli di classificazione previsti.

La condivisione di informazioni – quali ad esempio quelle ricavate attraverso il processo di Cyber Threat Intelligence - con altre strutture permette inoltre di aumentare la capacità reattiva e proattiva di tutti gli attori coinvolti, accrescendo il livello di maturità dei partecipanti al processo di Information Sharing oltre ad arricchire l'informazione originaria in modo da consentire valutazioni sempre più precise.

Condividere informazioni complesse in maniera non strutturata, non contestualizzata e in alcuni casi persino duplicata, non consente l'automazione necessaria ed utile a diminuire il caricamento e la relativa correlazione di quanto ricevuto. Le informazioni scambiate devono pertanto essere "*actionable*", ovvero immediatamente utilizzabili in ambito operativo e possono riguardare:

- minacce ed agenti di minaccia;
- campagne in corso;
- vulnerabilità;
- exploit[71];
- indicatori di compromissione (IOC).

Le informazioni condivise provengono sia dalle attività di monitoraggio e analisi (Threat Intelligence) svolte dal CERT sia da scambi informativi con altri soggetti qualificati della comunità di riferimento.

Alcuni dei principi alla base della condivisione delle informazioni sono:

- fiducia nei confronti dei soggetti e delle entità con cui si coopera nello scambio delle informazioni;
- adozione di schemi e modelli di classificazione delle informazioni. Molte iniziative di condivisione delle informazioni si basano ormai su schemi standard accettati dalla comunità professionale, come il *Traffic Light Protocol* (TLP, si veda successivamente per approfondimenti) per stabilire il modo in cui le informazioni da condividere devono essere gestite;
- definizione del livello di accuratezza necessario per consentire un'efficace azione di contrasto sulle minacce in esame. Il grado di accuratezza necessario dovrà essere valutato in coerenza con le reali necessità; ad esempio, in una situazione di emergenza potrebbe essere comunque accettabile la condivisione di informazioni seppure parziali e in corso di perfezionamento se necessarie a contrastare per tempo una minaccia;
- tempestività delle comunicazioni per contrastare adeguatamente l'azione di un attore malintenzionato;

[71] Ovvero programmi dannosi che contengono dati o codici eseguibili in grado di sfruttare una o più vulnerabilità di un software presente su un sistema.

- possibilità di anonimizzare la fonte delle informazioni e la presenza di qualsiasi dato sensibile o che non è possibile/opportuno condividere con la constituency nella sua interezza.

Le modalità di attuazione del processo di information sharing sono molteplici. In particolare si segnalano le seguenti come rilevanti con riferimento all'azione di un CERT:

- *Raccolta di informazioni da fonti multiple*: un CERT può raccogliere informazioni relative a minacce e vulnerabilità sia dall'esterno della propria constituency, come ad esempio da fornitori di servizi di Threat Intelligence (nelle forme di rapporti, interazioni, ecc.) o CERT operanti anche in altri settori rispetto alla comunità di appartenenza, che all'interno, attraverso le segnalazioni ricevute dai membri della consitituency relativamente ad eventi o incidenti di sicurezza registrati.
- *Distribuzione di alerts, bollettini, informative*: un CERT può inviare informazioni alla propria constituency fornendo i dettagli descrittivi e tecnici su nuove vulnerabilità e minacce, nella forma di alert, bollettini o generiche informative.
- *Comunicazioni periodiche*: il CERT può organizzare incontri periodici, workshop o seminari per condividere informazioni verso la propria constituency e/o community. A seconda del livello di confidenzialità dei temi da discutere tali eventi possono essere limitati ad un numero ristretto di partecipanti.

A fianco degli strumenti già descritti nel par 8.2.1 con cui può avvenire la condivisione di informazioni in modalità manuale (bollettini e Avvisi, portale di infosharing, mail, ecc.) è di fondamentale importanza stabilire anche strumenti e metodologie standard per la trasmissione automatizzata. Questo deve avvenire, in modo particolare, con le liste di IOC (Indicators of Compromise) da fornire in input a strumenti perimetrali come firewall, SIEM, IDS ecc. che possano così generare le opportune blacklist e gli allarmi relativi.

L'obiettivo è quello di creare una rete di CERT collegati tra loro che, utilizzando magari scelte tecnologiche anche differenti, possano scambiarsi informazioni in tempo reale in modalità Producer-to-Consumer usando standard comuni e una tassonomia condivisa, cioè un insieme di dati e metadati per la descrizione di eventi di sicurezza, campagne cyber, malware e così via.

CERT-PA in tal senso ha avviato da tempo una sperimentazione che ha coinvolto un gruppo di lavoro di attori pubblici e privati per la definizione di tali regole di trasmissione. Il risultato utilizza STIX 2.0 e TAXII per il trasporto. L'architettura usa anche Minemeld per aggregare, collezionare e processare i dati prima di inviarli al nodo di uscita. Lato Consumer, invece, è possibile utilizzare varie piattaforme compatibili con OpenTaxii tra cui MISP. A tal fine, CIRCL (Computer Incident Response Center Luxembourg) mette a disposizione una libreria per il pull dei dati da un Server TAXII locale o remoto.

I dettagli tecnici sono oggetto di un documento separato che verrà pubblicato nei prossimi mesi da AGID CERT-PA e che invitiamo a consultare come riferimento qualora si desideri implementare la trasmissione condivisa automatica di informazioni con il CERT-PA.

CAPITOLO 9

Processo di gestione degli incidenti di sicurezza

Gli obiettivi principali del processo di gestione degli incidenti di sicurezza informatica che occorrono nel dominio logico della PA sono:

- minimizzare l'impatto degli eventi malevoli;
- individuare ed attuare in maniera tempestiva idonee misure di contrasto/contenimento;
- individuare ed attuare tutte le attività di ripristino a seguito di un incidente;
- raccogliere dati per produrre statistiche in grado di alimentare il processo di analisi proattiva, finalizzato al rilevamento di eventi sospetti o di pattern comportamentali ripetuti nel tempo;
- attraverso i feedback ricevuti, aumentare all'interno della PA il grado di sensibilità verso le tematiche di sicurezza informatica e il livello di sicurezza delle infrastrutture tecnologiche gestite.

Data la possibile interconnessione delle infrastrutture appartenenti al dominio della PA il raggiungimento di tali obiettivi può avvenire in maniera efficiente ed efficace soltanto tramite una sinergia tra i vari soggetti che partecipano alla sua sicurezza. Gli attori coinvolti e le strutture preposte – PAL, CERT Regionale e CERT-PA in primis - devono pertanto svolgere il proprio ruolo con attitudine proattiva sia in fase di prevenzione che di gestione degli incidenti.

Al fine di garantire un efficace modello di interazione e cooperazione tra tutti gli attori coinvolti nel processo di gestione dell'incidente, è auspicabile che all'interno delle PAL sia identificato un responsabile per la gestione delle attività afferenti al dominio della Cyber Security (*Titolare o Referente Nominato della Sicurezza Informatica*), che possa sovraintendere i processi di gestione della sicurezza a livello locale e costituire il punto di contatto con il CERT regionale con riferimento ai servizi di cyber security acquisiti. Nei casi in cui sia stato designato all'interno dell'amministrazione, coincide con la figura del Referente Nominato della Sicurezza Informatica.

9.1 Definizioni

Si riportano di seguito le principali definizioni e convenzioni adottate nell'ambito del processo di gestione degli incidenti di sicurezza.

9.1.1 Evento di sicurezza

Con evento di sicurezza si indica qualsiasi situazione che si verifichi nell'ambito di un determinato asset informatico, comunque rilevata, la cui valenza è considerata significativa ai fini delle attività di gestione, controllo della sicurezza e contenimento dei rischi ad essa correlati.

Gli eventi di sicurezza sono classificati in base alla seguente scala gerarchica di importanza:

- *evento a basso impatto* (non significativo): qualsiasi evento gestito in maniera silente dal sistema di sicurezza della PAL interessata e che non richiede un trattamento ad hoc. Solitamente viene utilizzato a fini statistici;
- *evento significativo*: qualsiasi evento rilevato nell'ambito dei sistemi e delle infrastrutture ICT, che deve essere analizzato dal personale incaricato delle attività di monitoraggio (quali ad esempio, il rilevamento in tempo reale delle segnalazioni provenienti dai dispositivi di sicurezza, l'analisi dei log prodotti da tali dispositivi, la raccolta e la valutazione di comunicazioni su comportamenti anomali o eventi sospetti) e gestione degli allarmi di sicurezza;
- *evento critico*: qualsiasi evento significativo che, a seguito delle analisi effettuate dal personale incaricato, potrebbe sottintendere, direttamente o indirettamente, una violazione delle politiche di sicurezza applicate ai sistemi ed alle infrastrutture ICT.

Gli eventi di sicurezza, significativi e critici, sono ulteriormente classificati in *allarmi*, *incidenti* e *incidenti a rilevanza sistemica*, in accordo con le definizioni riportate nel seguito. A questo tipo di eventi si applica l'intero processo di gestione incidenti, suddiviso nelle fasi di **rilevazione**, **analisi**, **gestione** e **ripristino**.

Allarme di sicurezza o tentativo di attacco

Viene definito allarme di sicurezza o tentativo di attacco una segnalazione derivante dal rilevamento di uno o più eventi che costituiscono una criticità accertata per la sicurezza ICT, misurata sulla base di una scala di criticità predefinita. Gli allarmi di sicurezza non causano danni e sono associati ad attività che non costituiscono di per sé un pericolo diretto al patrimonio informatico, ovvero a comportamenti anomali da parte di utenti e applicazioni che non necessitano di un particolare intervento di contenimento, se non di un'azione di monitoraggio per prevenire o contenere eventuali attacchi susseguenti, ma che è, tuttavia, necessario registrare per una raccolta dei dati a fini statistici e di valutazione.

La maggior parte di questi eventi è costituita da *atti ostili* - ovvero azioni che cercano di pregiudicare un aspetto qualunque dei servizi o dei sistemi tecnologici, ma che vengono efficacemente respinte dalle contromisure poste in essere, e *prodromi di attacco* – ovvero attività di "raccolta delle informazioni" non intrusive, che possono preludere ad un successivo attacco vero e proprio.

Una lista, non esaustiva, di possibili allarmi è la seguente:

- azioni di enumeration (ad es. allarmi tipo ping sweep) dei nodi attivi su una sottorete;
- web crawling di un servizio web effettuato tramite tool automatici;
- scansioni di porte TCP/UDP aperte (host e port scan) effettuato una sola volta o comunque su destinazioni non particolarmente sensibili;
- accessi errati da parte di utenti che, pur comportando il lock di una singola utenza, non denotano una particolare attività illecita mirata al DoS, o all'accesso non autorizzato ai sistemi;
- fingerprinting su sistema operativo e applicativi installati sul sistema target;
- allarmi di tipo Policy Violations, determinati dalla presenza di software non autorizzato sui sistemi client (Instant Messaging, File Sharing, P2P, ecc.).

Incidente di sicurezza informatica

Viene definito incidente di sicurezza informatica qualsiasi evento o insieme di eventi che sottintendono una violazione delle politiche di sicurezza ICT fonte di danno per gli asset ICT ovvero per il patrimonio informativo dell'organizzazione e per il quale si rende necessaria l'applicazione di misure di contrasto e/o contenimento da parte delle strutture preposte. Da questa definizione si evince che l'elemento caratteristico distintivo di un incidente di sicurezza è rappresentato dal nesso di causa-effetto tra evento rilevato e danno subito dagli asset ICT.

In altri termini, un incidente di sicurezza rappresenta una particolare tipologia di allarme i cui eventi sottintendono una constatazione conclamata di danni, già subiti al momento del loro rilevamento e segnalazione. Una lista non esaustiva di possibili incidenti per la PAL è la seguente:

- accesso non autorizzato agli asset ICT;
- diffusione non autorizzata di informazioni riservate provenienti dagli asset ICT;
- impersonificazione di utenti, tramite la compromissione delle credenziali personali di autenticazione;
- perdita o modifica delle configurazioni di sistema;
- decadimento dei livelli di servizio standard;
- interruzione di servizi ICT;
- constatazione di illeciti o azioni criminose apportate con l'ausilio delle risorse ICT di una PAL ai danni della stessa PAL o di terzi.

Incidente di sicurezza informatica a rilevanza sistemica delle PAL

La correlazione sistemica tra le varie PA, in termini di servizi informatici e di connettività, comporta un aumento della possibilità che eventi dannosi che occorrono in un Ente possano ripercuotersi su altri Enti ad esso correlati. Un incidente a carico di una PAL può acquisire rilevanza sistemica qualora determini disservizi e/o alterazioni (in termini di riservatezza, integrità o disponibilità) ad altri servizi erogati da altre PA. In caso di incidente a rilevanza sistemica per la PA dovranno essere allertate e coordinate tutte le PA coinvolte nella catena di correlazione sistemica, ovvero tutte le PAL che presentano caratteristiche similari alla PAL primariamente impattata, sia in termini di servizi che di tecnologie. Una lista non esaustiva di possibili incidenti a rilevanza sistemica per la PAL è la seguente:

- attacco mirato, ad alto impatto in termini di riservatezza, integrità e disponibilità per i servizi ICT, specificatamente progettato per determinate piattaforme tecnologiche (sistemi operativi, middleware, applicativi di tipo infrastrutturale, ecc.) presenti in diverse PAL;
- interruzione di un servizio ICT che provoca un inaccettabile decadimento di prestazioni (o un'interruzione a sua volta) per altri servizi erogati da altre PAL sistemicamente correlate;
- perdita, alterazione o diffusione incontrollata di dati tali da provocare danni o alterazioni di servizio per altre PAL.

In tali casi, si renderà necessario attivare un processo di escalation verso il CERT-PA per la presa in carico e relativa risoluzione dell'incidente di sicurezza.

9.1.2 Criticità degli incidenti

Si definisce criticità di un incidente di sicurezza la misura qualitativa della gravita dello stesso, in termini dei seguenti cinque scenari di impatto:

- *Persone*: impatto sulla salute e la sicurezza fisica dei cittadini;
- *Economia*: impatto economico provocato dall'incidente;
- *Servizi PAL*: quantità e tipologia di servizi critici coinvolti dall'incidente;

- *Immagine*: visibilità dell'incidente (o danno di immagine);
- *Sociale*: impatti sociali provocati dall'incidente.

La criticità dell'incidente viene espressa secondo una scala ordinale a quattro valori o livelli di impatto (Livello 0 – Livello 3), secondo la seguente metrica valutativa (scala degli impatti):

Tabella 9.1: Classificazione degli incidenti di sicurezza

Scenario di impatto	Livello 0	Livello 1	Livello 2	Livello 3
Persone	Nessun impatto significativo	Impatti limitati solo all'interno dell'ente	Impatti limitati ma possibile interessamento di altre PAL o privati	Impatti limitati con interessamento di altre PAL o privati
Economia	Nessun impatto significativo	Impatto economico trascurabile e limitato all'ente	Impatto economico limitato con possibile interessamento di altre PAL	Impatto economico significativo o interessamento di altre PAL
Servizi PA	Nessun impatto significativo	Impatto limitato a servizi interni all'ente	Impatto limitato ma possibile interessamento di altre PAL o privati	Impatto limitato ma con interessamento di altre PAL o privati
Immagine	Nessun impatto significativo	Danno di immagine ma problema limitato all'ente	Danno di immagine con interessamento di altre PAL	Danno di immagine con interessamento esterno alla PAL
Sociale	Nessun impatto significativo	L'incidente provoca malessere nel personale dell'ente	L'incidente provoca malessere nel personale in altre PAL	L'incidente provoca malessere anche all'esterno della PAL

Come si evince dalla tabella precedente, il livello di impatto associato ad un evento di sicurezza rappresenta una misura qualitativa del danno provocato dall'evento stesso. In generale:

- incidenti di Livello 0 sono assimilabili ad eventi di sicurezza non significativi;
- nel caso in cui ci siano impatti limitati che rimangono confinati all'interno dell'ente locale, si attribuisce il Livello 1;
- nel caso in cui ci siano impatti limitati ma che potenzialmente potrebbero interessare anche altre PAL ovvero un numero limitato di soggetti privati, si attribuisce il Livello 2;
- nel caso in cui ci siano impatti significativi (o sistemici) che interessano sicuramente altre PAL ovvero cittadini o soggetti privati, si attribuisce il Livello 3, attivando contestualmente il processo di escalation verso il CERT-PA.

Nel caso in cui un incidente presenti diversi scenari di impatto, il livello di criticità è costituito dal massimo tra tutti i valori.

9.1.3 Priorità di gestione degli incidenti

La priorità di trattamento di un evento e le modalità di gestione sono attribuite in funzione del livello di impatto, secondo la metrica TLP a 4 valori (o colori) riassunta nella seguente tabella sinottica:

Tabella 9.2: Definizione dei livelli di priorità

Scenario di impatto	**Classificazione**	**Priorità**	**Modalità di gestione**	**Ruolo CERT Regionale**
Livello 0	Allarme	**Non rilevante**	Locale all'Ente coinvolto	-
Livello 1	Incidente	**Informativo**	Locale all'Ente coinvolto	Informato
Livello 2	Incidente	**Attenzione**	Condivisa	Supporto alla gestione / coordinamento per incidenti sistemici PA
Livello 3	Incidente	**Critico**	Condivisa	Supporto alla gestione / coordinamento e coinvolgimento CERT-PA

Come indicato nella tabella precedente, il livello di impatto dell'allarme/incidente determina la modalità ed il ruolo svolto dal CERT Regionale nelle attività di gestione.

9.2 Attori coinvolti e responsabilità

In questa sezione si definiscono gli attori coinvolti nel processo di gestione degli incidenti e le rispettive responsabilità.

9.2.1 Referente della Sicurezza Informatica della PAL

Il Referente di Sicurezza ha la responsabilità di:

- effettuare il monitoraggio continuativo degli eventi di sicurezza provenienti dai dispositivi di sicurezza gestiti o da altre fonti;
- effettuare l'analisi e la classificazione degli eventi rilevati;
- gestire gli allarmi, applicando le procedure interne per il contrasto/contenimento degli allarmi;
- definire il piano di intervento per il trattamento di incidenti, sottoponendolo al CERT Regionale;
- interfacciarsi con il CERT Regionale, inviando comunicazione sugli incidenti di Livello 1 occorsi;
- effettuare il coinvolgimento ufficiale del CERT Regionale nella gestione di incidenti di Livello 2 e Livello 3;
- valutare l'applicazione di procedure di change management sui dispositivi di monitoraggio per la rimozione di falsi positivi;
- coordinare l'applicazione delle misure di trattamento definite nel piano di intervento secondo le procedure interne di trattamento degli incidenti;
- chiudere formalmente gli incidenti di Livello 0 e Livello 1;
- chiudere internamente gli incidenti di Livello 2 e Livello 3, a seguito della chiusura formale da parte del CERT Regionale.

9.2.2 CERT Regionale

Il CERT Regionale ha le responsabilità di:

- effettuare l'analisi e la ri-classificazione degli incidenti segnalati;
- supportare le attività di risposta per incidenti di Livello 2 e Livello 3;
- integrare, ove necessario, il piano di intervento ricevuto dalle PAL con direttive di carattere strategico;

- coordinarsi con il CERT-PA per la gestione di incidenti di Livello 3;
- inviare al CERT-PA il risultato delle analisi effettuate e la strategia di gestione ipotizzata per il trattamento di incidenti di Livello 3;
- coinvolgere le PAL interessate in caso di incidenti a rilevanza sistemica;
- effettuare il coordinamento nella risposta degli incidenti a rilevanza sistemica o di incidenti a Livello 3;
- chiudere formalmente gli incidenti di Livello 2 e Livello 3;
- effettuare l'analisi post-incidente;
- monitorare le azioni di ripristino;
- rendicontare gli incidenti pervenuti per ciascun Livello e le azioni intraprese.

9.2.3 CERT-PA

Il CERT-PA ha la responsabilità di:

- assumere il coordinamento della gestione operativa degli incidenti di Livello 3;
- definire la strategia di contrasto in caso di incidenti di Livello 3, eventualmente verificando ed approvando quanto proposto dal CERT Regionale;
- coordinarsi con il CERT Regionale nella risoluzione degli incidenti di Livello 3.

9.3 Fasi del processo di gestione incidenti nelle PAL

Il processo di gestione incidenti è articolato nelle seguenti attività:

- **monitoraggio**, a carico delle singole PAL, finalizzato all'individuazione degli eventi rilevati automaticamente, ovvero alla ricezione delle segnalazioni di comportamenti anomali o sospetti;
- **analisi e** prima **classificazione** degli eventi di sicurezza rilevati a carico delle PAL coinvolte;
- attivazione del sotto-processo di **gestione degli allarmi o** di **gestione incidenti**, coinvolgendo o meno il CERT Regionale ed il CERT-PA, in funzione del livello di classificazione e dell'eventuale rilevanza sistemica dell'incidente;
- **monitoraggio delle attività di ripristino** ed analisi post-incidenti a carico del CERT Regionale.

La Figura 9.1 descrive il diagramma di flusso inter-funzionale del processo generale di gestione incidenti nelle PAL, attivato dal Referente della Sicurezza all'arrivo di una segnalazione di sicurezza; come evidenziato dalle linee tratteggiate, il processo di ripristino ed analisi post-incidente viene attivato al termine dei sotto-processi di gestione incidenti definiti per i diversi livelli di impatto.

9.3.1 Monitoraggio degli eventi di sicurezza

La responsabilità delle attività continuative H24 7x7 di monitoraggio degli incidenti di sicurezza è in carico al Referente di sicurezza della PAL, che eventualmente si coordina con altre strutture operative interne o esterne.

Il processo di gestione incidenti nelle PAL si attiva quando gli operatori responsabili del monitoraggio:

- rilevano le segnalazioni prodotte in tempo reale dai dispositivi informatici di monitoraggio, cui è affidato il compito di tracciare e segnalare tutti gli eventi di sicurezza ICT occorsi nel dominio degli asset ICT controllati;

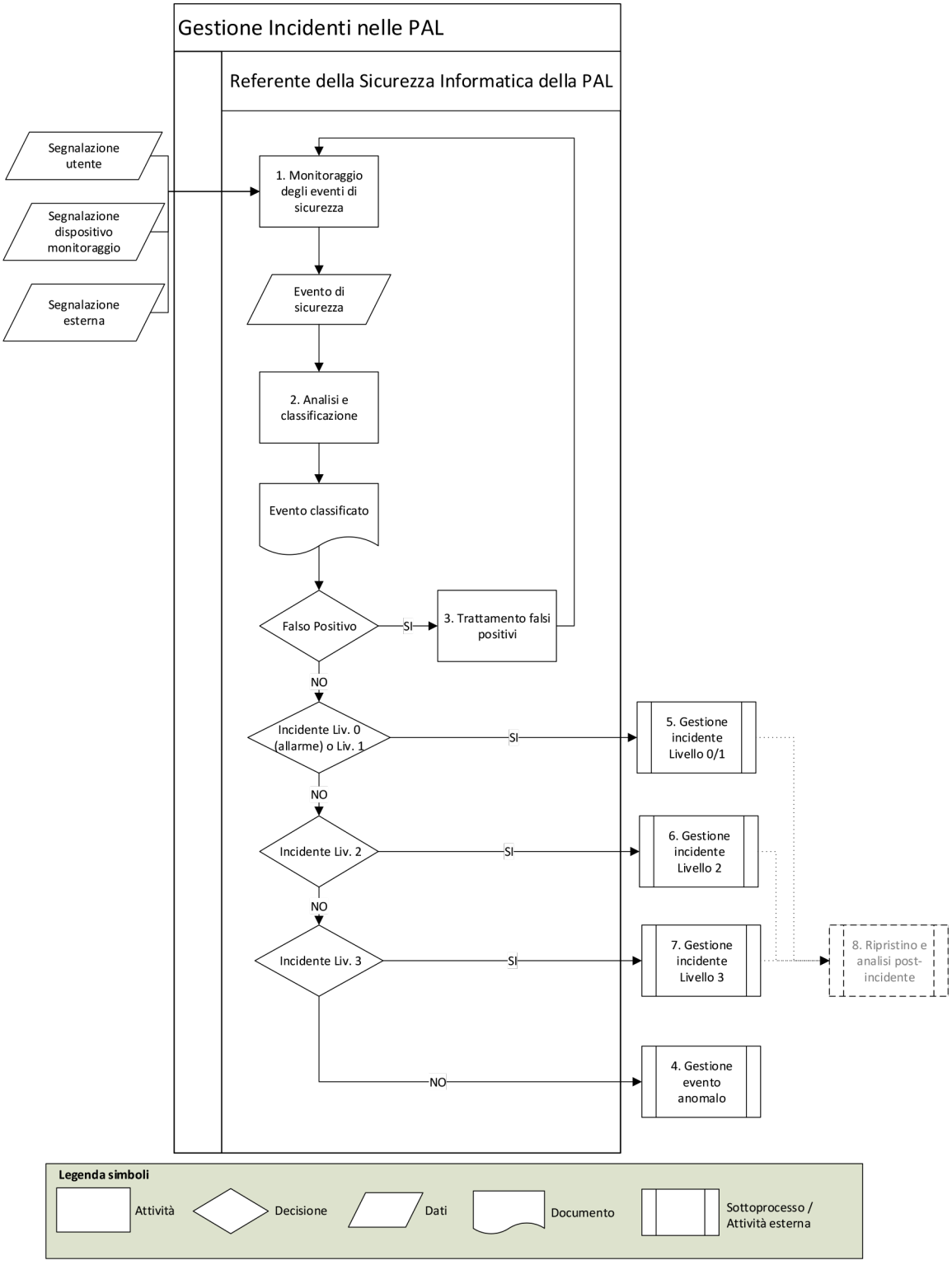

Fig. 9.1: Flusso di gestione incidenti nelle PA

- effettuano delle analisi periodiche dei log prodotti dai dispositivi di monitoraggio o da altre piattaforme di sicurezza gestite, per il rilevamento di pattern sospetti e/o eventi ripetuti, che possano evidenziare attività malevoli;
- raccolgono e valutano comunicazioni, verbali o scritte, di comportamenti anomali o di eventi sospetti provenienti da utenti o amministratori di sistema;
- raccolgono e valutano comunicazioni (sotto forma di alert o bollettini di sicurezza) provenienti da fonti esterne autoritative (tra i quali il CERT-PA e il CERT Regionale competente), circa nuovi scenari di rischio, comportamenti anomali o attacchi in corso ai danni di altri, che potrebbero avere impatto sul patrimonio tecnologico gestito.

L'output delle attività di monitoraggio è costituito dagli eventi di sicurezza da sottoporre alla successiva fase di analisi e classificazione.

9.3.2 Analisi e classificazione

Il personale preposto effettua l'analisi e la classificazione degli eventi segnalati, eventualmente avvalendosi di matrici diagnostiche e di procedure operative interne per il riconoscimento e la classificazione degli eventi di sicurezza.

L'output delle attività di analisi e classificazione è costituito dagli eventi, categorizzati secondo la metrica precedentemente definita. In particolare:

- in caso di falsi positivi, gli eventi vengono registrati e si procede al relativo trattamento;
- in caso di allarmi di sicurezza (o incidenti a Livello 0) dovrà essere aperta formalmente una scheda di gestione allarme ed attivato il corrispondente sotto-processo interno;
- in caso di incidente di sicurezza a Livello 1 dovrà essere aperta formalmente una scheda di gestione incidente ed attivato il corrispondente sotto-processo interno;
- in caso di incidente di sicurezza a Livello 2 e Livello 3 dovrà essere aperta formalmente una scheda di gestione incidente e inviata al Referente della Sicurezza Informatica della PAL, che attiva il corrispondente sotto-processo e si coordina con il CERT Regionale nelle modalità di seguito illustrate;
- in caso di eventi anomali, che presentano un impatto sulla sicurezza informatica e per i quali non è possibile effettuare una classificazione, viene inviata formalmente una richiesta di supporto al CERT Regionale, che procede alle attività di classificazione e di attivazione del corrispondente sotto-processo di gestione.

In caso di più eventi concorrenti, viene data priorità alla gestione degli eventi a maggior livello di criticità.

9.3.3 Trattamento falsi positivi

Gli eventi identificati come falsi positivi non danno seguito ad allarmi e, una volta accertati, deve essere valutata (in particolare nel caso di falsi positivi persistenti) la possibilità di far filtrare tali eventi dai sistemi di tracciamento, per non sovraccaricare le attività di monitoraggio con operazioni ripetitive.

Tali attività sono condotte internamente alle PAL, attivando procedure opportunamente codificate e documentate di change management degli apparati di sicurezza.

9.3.4 Gestione evento anomalo

Nel caso di eventi che presentano degli impatti sulla sicurezza, ma per i quali il Referente della Sicurezza Informatica della PAL non riesce ad effettuare in autonomia la classificazione, viene inviata al CERT Regionale una richiesta di supporto contenente:

- le evidenze rilevate,

- il risultato delle analisi eseguite e le motivazioni per le quali non si riesce ad effettuare la classificazione.

Il CERT Regionale, coordinandosi con il Referente della Sicurezza Informatica della PAL, provvede all'analisi dell'evento, alla sua classificazione secondo la metrica definita, e all'attivazione del corrispondente sotto-processo di gestione coinvolgendo, qualora necessario, il CERT-PA.

9.3.5 Gestione incidenti di Livello 0 (Non Rilevante) e Livello 1 (Informativo)

Il sotto-processo di gestione degli incidenti di Livello 0 (o allarmi) e incidenti a Livello 1 è un processo interno alla PAL, che prevede l'interazione con il CERT Regionale esclusivamente in fase di rendicontazione finale, al termine delle attività di trattamento.

Di seguito si riporta una descrizione di alto livello del sotto-processo, rimandando ad eventuali procedure interne di gestione che tengano conto delle specificità organizzative di ogni singola PAL.

Il diagramma di flusso inter-funzionale del sotto-processo di gestione incidenti di Livello 0 e 1 è il seguente.

Si dettagliano di seguito le attività indicate in Figura 9.2 (per la legenda dei simboli fare riferimento alla Figura 9.1).

Definizione delle attività di gestione

Il Referente della Sicurezza Informatica della PAL accerta l'entità e la natura degli eventuali danni subiti e definisce, in funzione delle evidenze raccolte, la strategia ottimale di contrasto per l'incidente rilevato, tenendo conto dei seguenti vincoli operativi:

- le misure di contrasto e contenimento individuate devono essere commisurate all'effettivo beneficio che si può ottenere, ovvero gli interventi devono arrecare il minor danno possibile agli asset ICT ed ai servizi da questi gestiti;
- i danni o i disservizi agli asset ICT, causati dall'attuazione delle misure di contrasto e contenimento, devono comunque essere inferiori a quelli conseguenti la violazione in essere;
- in nessun caso sono ammesse operazioni tali da comportare, direttamente o indirettamente, una violazione delle politiche di sicurezza in vigore, delle clausole contrattuali e delle vigenti leggi, ovvero non sono ammessi interventi che possano arrecare un qualsiasi danno, materiale o morale, a persone fisiche, sia dipendenti che esterni alla PAL coinvolta.

Durante questa fase il Referente di Sicurezza può interagire con altre strutture operative interne, in funzione delle procedure di trattamento degli incidenti di sicurezza definite localmente per ciascuna PAL. In particolare, deve essere richiesta l'autorizzazione a procedere, nel caso in cui le attività da porre in atto presentino un carattere di invasività o possano comunque comportare un disservizio sui sistemi coinvolti.

Al termine di questa fase viene redatto un piano di intervento, dove è riportata una descrizione dettagliata delle operazioni da effettuare per facilitare l'intervento delle diverse strutture operative coinvolte.

Trattamento incidente

Il Referente di Sicurezza coordina l'applicazione delle misure di trattamento definite nel piano di intervento, integrandosi con i gruppi operativi all'interno della PAL ed eventualmente effettuando l'escalation di responsabilità verso altre strutture, in funzione delle procedure interne di trattamento degli incidenti di sicurezza.

Al termine dell'applicazione delle procedure di trattamento, il Referente di Sicurezza valuta l'effettiva chiusura dell'incidente. Tali verifiche possono essere effettuate analizzando gli eventi rilevati dai sistemi di tracciamento, ovvero mediante ogni altra verifica volta a fornire l'evidenza del lavoro svolto.

Al termine di queste verifiche:

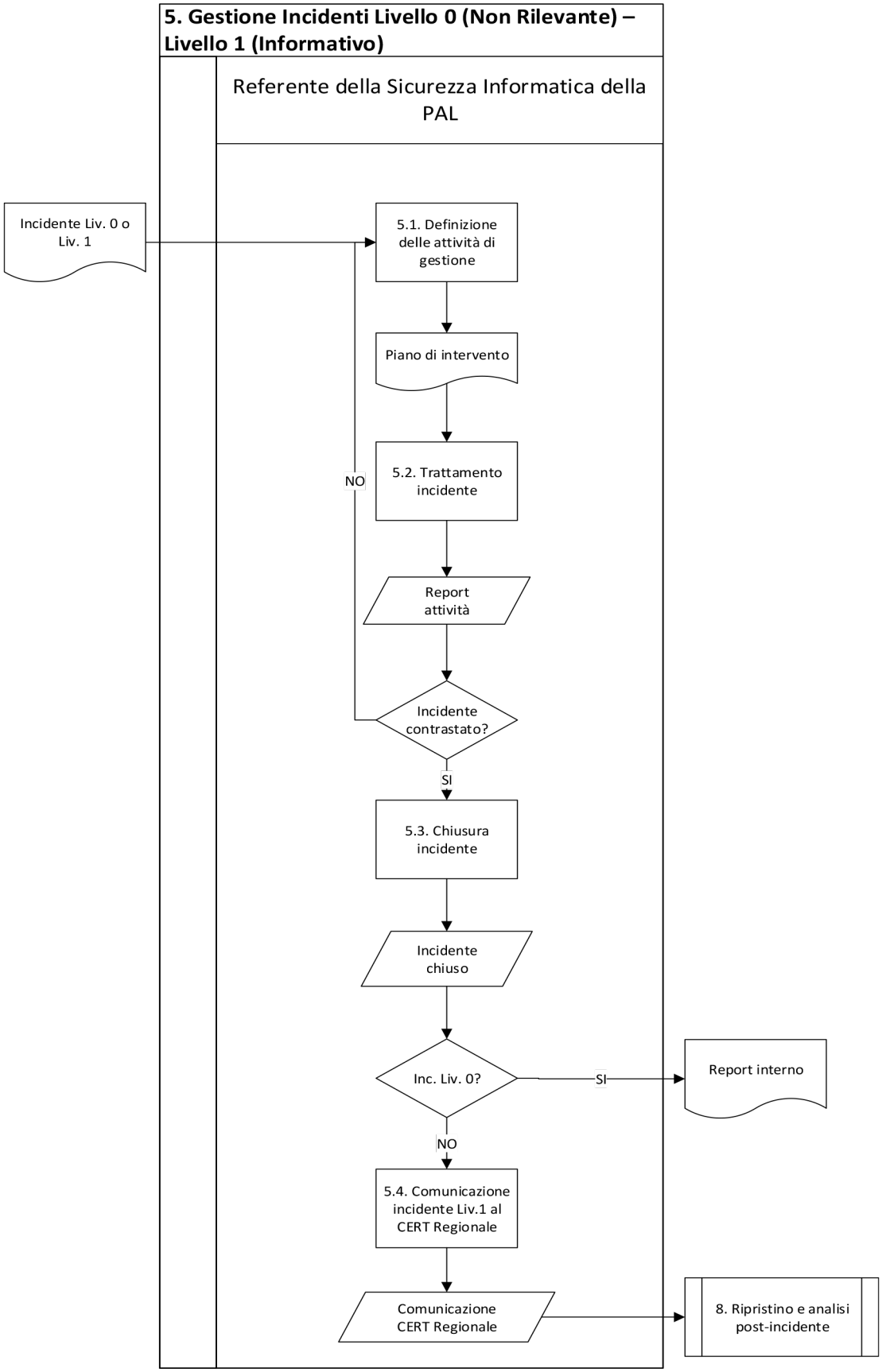

Fig. 9.2: Flusso di gestione incidenti Livello 0 e Livello 1

- se l'incidente non risulta effettivamente rientrato il Referente di Sicurezza continua con le attività di gestione, definendo un nuovo piano di intervento e valutando, se necessario, una ri-classificazione dell'incidente stesso;
- se l'incidente risulta rientrato, il Referente di Sicurezza provvede alla chiusura formale dell'incidente.

Chiusura incidente

Il Referente di Sicurezza effettua la chiusura formale dell'incidente e redige un report di chiusura formale che contiene, come minimo:

- codice univoco identificativo dell'incidente;
- data e ora di apertura della scheda di gestione incidente;
- rapporto di constatazione incidente, comprensivo del livello di classificazione e dell'elenco dei danni subiti;
- documentazione degli interventi posti in atto e delle attività di ripristino effettuate;
- data e ora di chiusura dell'incidente.

Se l'incidente subito è di Livello 0 non viene effettuata alcuna comunicazione al CERT Regionale archiviando localmente il report redatto. Se l'incidente è di Livello 1, viene inviata comunicazione formale al CERT Regionale.

Comunicazione incidente Liv. 1 al CERT Regionale

Il Referente della Sicurezza Informatica della PA invia, al termine delle attività di gestione e dopo la chiusura dell'incidente, una segnalazione informativa al CERT Regionale contenente i dettagli dell'incidente (di Livello 1) subito, attivando in tal modo il sotto-processo di ripristino e analisi post-incidente.

9.3.6 Gestione incidenti di Livello 2 (Attenzione)

Il diagramma di flusso inter-funzionale del sotto-processo di gestione degli incidenti di Livello 2 è riportato nella figura seguente.

Si dettagliano di seguito le attività indicate in Figura 9.3 (per la legenda dei simboli fare riferimento alla Figura 9.1).

Coinvolgimento CERT Regionale

Nel momento in cui viene identificato un incidente di Livello 2, il Referente della Sicurezza Informatica della PA coinvolge il CERT Regionale, inviando, mediante i canali condivisi, una richiesta formale di supporto per la gestione dell'incidente in corso.

Nella richiesta devono essere riportati tutti i dettagli necessari al CERT Regionale per poter effettuare l'analisi e fornire le indicazioni utili al trattamento dell'incidente. In particolare, devono essere indicate:

- data e ora di rilevamento evento;
- data e ora cui si riferiscono i danni rilevati;
- sistemi coinvolti dall'incidente;
- servizi coinvolti dall'incidente e relativa criticità;
- livello di classificazione assegnato;
- rapporto di constatazione incidente, comprensivo dell'elenco dei danni subiti.

Contestualmente alla richiesta di supporto, il Referente della Sicurezza sottopone al CERT Regionale il piano operativo di intervento dove sono dettagliate:

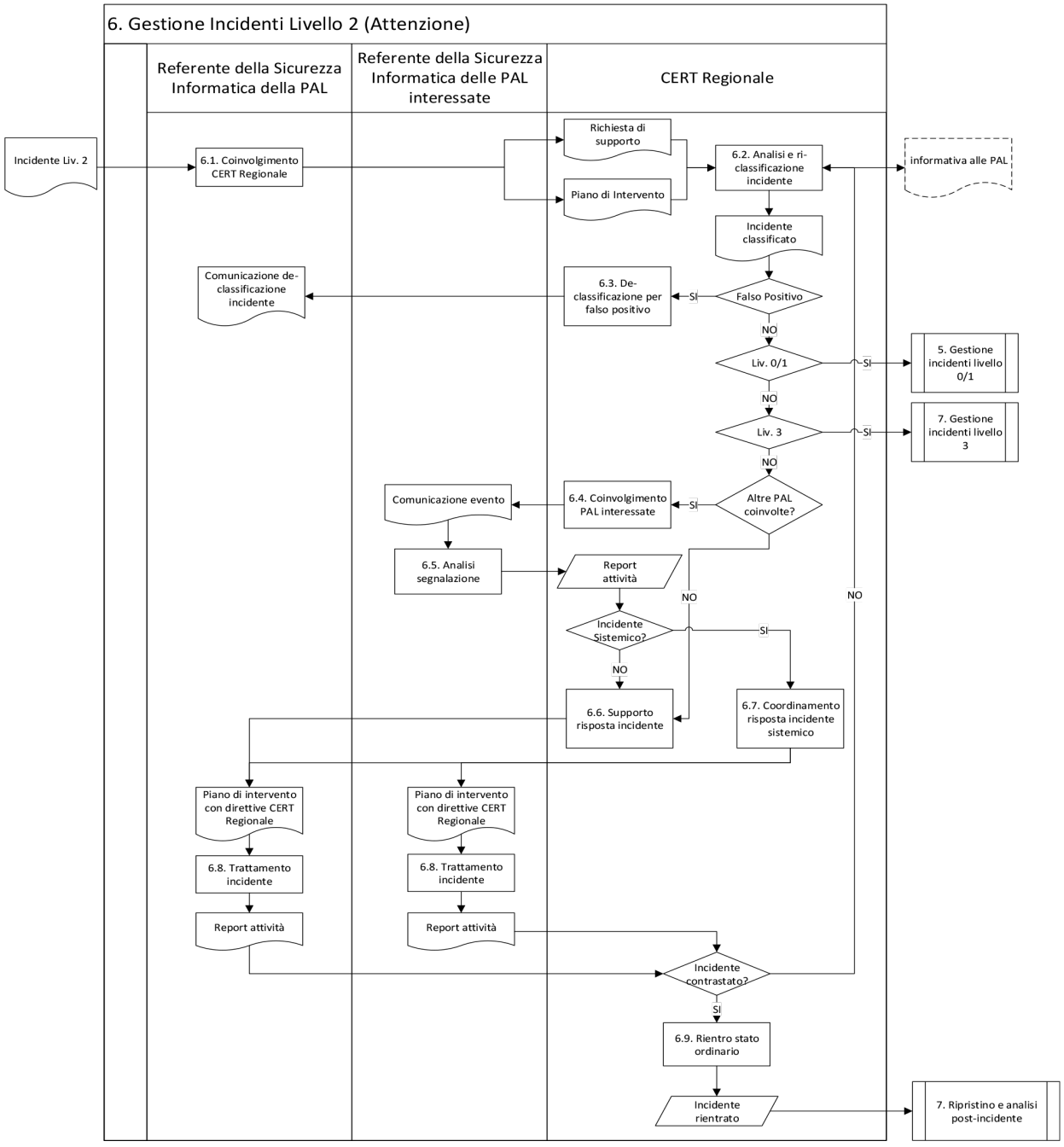

Fig. 9.3: Flusso di gestione incidenti Livello 2

- le attività di contrasto e contenimento fino a quel momento intraprese;
- i risultati riscontrati;
- le azioni suggerite, in funzione delle conoscenze acquisite sul patrimonio tecnologico gestito, degli eventi rilevati e dei sistemi da essi coinvolti;
- i risultati attesi dalle attività suggerite.

Analisi e ri-classificazione incidente

Il gruppo di analisti di sicurezza del CERT Regionale effettua una ri-classificazione dell'incidente segnalato, analizzandone l'impatto in un'ottica di tipo sistemico per la PAL e correlando le informazioni ricevute con ulteriori indicazioni eventualmente ricevute da altre PAL, da altri CERT Regionali o dal CERT-PA.

Al termine di questa classificazione, il CERT Regionale valuta se è necessario:

- passare alla de-classificazione dell'incidente in caso di Falso Positivo;
- de-classificare l'incidente a Livello 0 o 1, attivando il corrispondente sotto-processo e segnalandolo alla PAL coinvolta;
- aumentare la classificazione a Livello 3 attivando il corrispondente sotto-processo, ingaggiando il CERT-PA e segnalandolo alla PAL coinvolta.

In funzione della tipologia di incidente segnalato, il CERT Regionale può inviare un'eventuale informativa di sicurezza alle PAL accreditate, per segnalare l'occorrenza dell'incidente in corso ed innalzare il livello di attenzione su determinati scenari di minaccia o particolari aspetti tecnologici e organizzativi.

Se l'incidente (in base ai dati raccolti) presenta dei potenziali impatti sui servizi o le infrastrutture di altre PAL differenti da quella originante, il CERT Regionale procede al coinvolgimento di tutte le PAL interessate.

De-classificazione per falso positivo

Nel caso in cui gli analisti del CERT Regionale rilevino che l'incidente segnalato dalla PAL non presenta carattere di rilevanza e non sottintende direttamente o indirettamente ad alcuna violazione, lo de-classificano come falso positivo, inviando una comunicazione alla PAL coinvolta contenente:

- risultato dell'analisi;
- motivazioni della de-classificazione;
- eventuali indicazioni per il trattamento del falso positivo segnalato e su come rimuoverlo dai dispostivi di monitoraggio.

Coinvolgimento PAL interessate

In caso di incidente che presenti un potenziale impatto su diverse PAL, il CERT Regionale coinvolge formalmente tutte le PAL interessate dall'incidente, inviando ai relativi Referenti della Sicurezza Informatica una comunicazione contenente (come minimo):

- la data e l'ora dell'incidente;
- la tipologia di sistemi e servizi coinvolti dall'incidente (sistemi operativi, tecnologie utilizzate, ecc.);
- i possibili danni che potrebbero essere provocati;
- qualsiasi altra informazione ritenuta necessaria per il trattamento di eventuali altri incidenti sistemicamente connessi all'incidente rilevato.

Ove possibile la comunicazione inviata deve essere anonimizzata, garantendo la riservatezza delle informazioni e impedendo la circolazione di informazioni comunque critiche.

Analisi segnalazione

Il Referente della Sicurezza di ciascuna PAL analizza la comunicazione ricevuta dal CERT Regionale, coinvolgendo, all'interno della propria PAL, eventuali altre strutture operative in funzione delle procedure localmente definite.

In funzione della tipologia di evento segnalato, sono normalmente ipotizzabili i seguenti scenari:

- qualora i sistemi della PAL coinvolta non risultino vulnerabili alla minaccia segnalata, il Referente di Sicurezza della PAL invia al CERT Regionale un report di riscontro;
- qualora non vi siano specifiche evidenze di applicazione della minaccia segnalata, viene aumentato il livello di monitoraggio nei confronti della specifica segnalazione ricevuta ed inviato dal Referente di Sicurezza al CERT Regionale un report di riscontro;
- qualora, in funzione della segnalazione ricevuta, venga rilevato internamente alla PAL un incidente di sicurezza precedentemente non rilevato (o comunque già rilevato ed in corso di classificazione), il Referente di Sicurezza attiva il corrispondente sotto-processo di gestione incidenti, inviando un report di riscontro al CERT Regionale e rimanendo in costante contatto con il CERT Regionale che coordina tutte le attività di risposta.

In caso in cui l'incidente segnalato presenti reali impatti su altre PAL (incidente a rilevanza sistemica) il CERT Regionale procede al coordinamento delle successive attività di risposta, tracciando formalmente la presenza di un incidente sistemico. Negli altri casi il CERT Regionale offre il proprio supporto specialistico alla PAL coinvolta nel trattamento degli incidenti rilevati.

Supporto risposta incidente

Il CERT Regionale supporta il Referente della Sicurezza Informatica della PAL nella risposta all'incidente rilevato e nella definizione del piano operativo di intervento.

In particolare, il CERT Regionale analizza il materiale ricevuto dalla PAL e, ove necessario, integra il piano di intervento con indicazioni di carattere strategico, derivanti dalle informazioni desunte in fase di analisi e ri-classificazione o comunque raccolte grazie al proprio ruolo di coordinamento all'interno del dominio logico della Pubblica Amministrazione.

Il CERT Regionale condivide quindi il piano di intervento così integrato al Referente della Sicurezza Informatica della PAL.

Coordinamento risposta incidente sistemico PAL

Dopo la comunicazione formale di incidente sistemico della PAL, il CERT Regionale assume il coordinamento delle attività di gestione dell'incidente sistemico PAL.

Il CERT Regionale analizza il materiale ricevuto dalla PAL e, ove necessario, integra il piano di intervento con indicazioni di carattere strategico, derivanti dalle informazioni desunte in fase di analisi e ri-classificazione o comunque raccolte grazie al proprio ruolo di coordinamento all'interno del dominio logico della Pubblica Amministrazione sul territorio.

Durante tale fase il CERT Regionale coordina i Referenti della Sicurezza delle PAL coinvolte, con i quali condivide il piano degli interventi necessari al trattamento degli incidenti e dai quali riceve un aggiornamento costante sullo stato di avanzamento delle attività di trattamento.

Trattamento incidente

I Referenti della Sicurezza delle PAL coinvolte (la PAL originante e le altre PAL nel caso di incidente a rilevanza sistemica) ricevono il piano con gli interventi di propria competenza e, in base alle procedure interne di trattamento degli incidenti, curano l'applicazione delle misure di contrasto e contenimento ivi definite coinvolgendo, all'interno della propria PAL, eventuali altre strutture operative, in funzione delle suddette procedure.

Durante le attività di trattamento i Referenti della Sicurezza Informatica delle PAL rimangono costantemente allineati con il CERT Regionale, al quale inviano tutti gli aggiornamenti significativi sullo stato di avanzamento delle attività.

Al termine delle attività di trattamento, ciascuna PAL interessata redige un report di rendicontazione, che permette al CERT Regionale di capire se lo stato di emergenza è formalmente risolto o se è necessario procedere con una nuova analisi e ri-classificazione dell'incidente. Tali verifiche possono essere effettuate analizzando gli eventi rilevati dai sistemi di tracciamento, ovvero mediante ogni altra verifica volta a fornire l'evidenza del lavoro svolto.

Rientro stato ordinario

Nel momento in cui si chiude lo stato di emergenza, il CERT Regionale effettua la chiusura formale dell'incidente, redigendo un rapporto contenente (come minimo):

- codice univoco identificativo dell'incidente;
- data e ora di apertura della scheda di gestione incidente;
- rapporto di constatazione incidente, comprensivo del livello di classificazione, dell'elenco dei danni subiti e delle PAL coinvolte in caso di impatti sistemici;
- documentazione degli interventi posti in atto e dei risultati ottenuti, specificando, particolarmente per gli incidenti sistemici, i sistemi/servizi delle varie PAL coinvolti dalle attività di trattamento;
- data e ora di chiusura dell'incidente.

Tale rapporto deve essere inviato alle PAL coinvolte, che a quel punto provvedono internamente alla chiusura dell'incidente segnalato. Al rientro dello stato ordinario, il CERT Regionale attiva il sotto-processo di ripristino e analisi post-incidente.

9.3.7 Gestione incidenti di Livello 3 (Critico)

Il diagramma di flusso inter-funzionale del sotto-processo di gestione degli incidenti di Livello 3 è riportato nella figura seguente.

Si dettagliano di seguito le attività indicate in Figura 9.4 (per la legenda dei simboli fare riferimento alla Figura 9.1).

Per comodità espositiva, si dettagliano a seguire solamente le attività specifiche che caratterizzano l'attivazione del sotto-processo di gestione degli incidenti di livello 3. Per i dettagli relativi alle altre attività si rimanda alle precedenti sezioni del documento.

Coinvolgimento CERT-PA

Contestualmente alla segnalazione, il gruppo di analisti di sicurezza del CERT Regionale invia al CERT-PA il risultato delle analisi effettuate e la strategia di intervento posta in essere dalla PAL originante per il trattamento dell'incidente in corso, eventualmente integrata da ulteriori proposte definite dal CERT Regionale in fase di analisi.

La strategia dovrà dettagliare:

- la descrizione dell'attacco subito, i sistemi ed i servizi coinvolti e una descrizione dei danni subiti;
- le attività di contrasto poste in essere e quelle sulle quali si richiede il consenso;

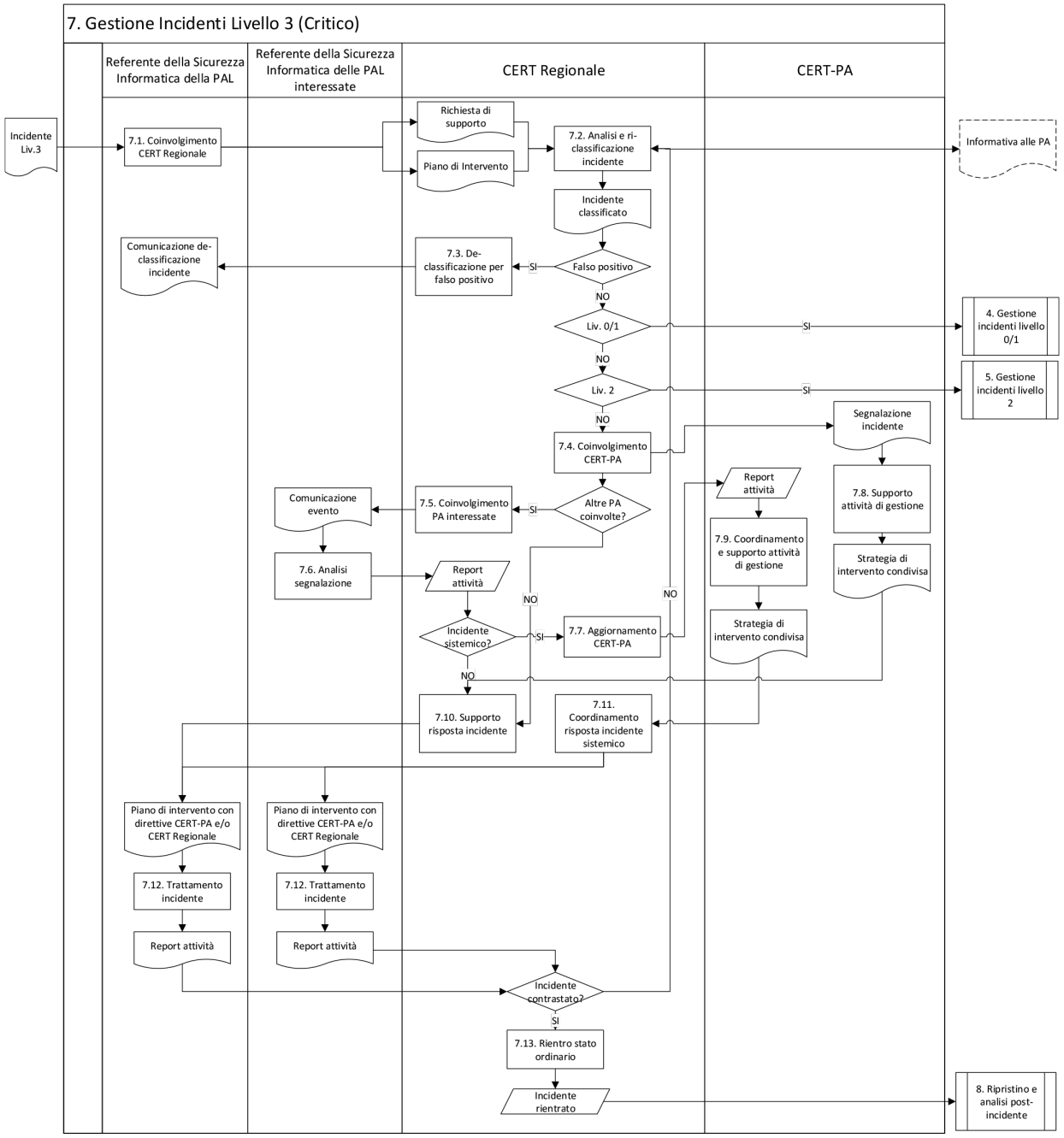

Fig. 9.4: Flusso di gestione incidenti Livello 3

- gli scenari di minaccia che si intendono contrastare ed i risultati attesi dalle attività individuate.

Se l'incidente (in base ai dati raccolti) presenta dei potenziali impatti sui servizi o le infrastrutture di altre PAL differenti da quella originante, il CERT Regionale procede al coinvolgimento di tutte le PAL interessate.

Aggiornamento CERT-PA

Nel caso in cui l'incidente segnalato presenti reali impatti su altre PAL (incidente a rilevanza sistemica), il CERT Regionale aggiorna il CERT-PA sullo stato dell'Emergenza in corso, inviando:

- i rapporti di riscontro ricevuti dalle diverse PAL coinvolte;
- ogni altra informazione utile alla definizione/aggiornamento della strategia di intervento elaborata dal CERT-PA.

Il CERT Regionale rimane in contatto con i Referenti della Sicurezza delle PAL coinvolte, dai quali riceve aggiornamenti sugli eventi in corso, che sottopone per aggiornamento al CERT-PA.

Supporto attività di gestione

Il CERT-PA una volta attivato dal CERT Regionale:

- supporta e si coordina con il CERT Regionale nella gestione dell'incidente, che a sua volta coinvolgerà il Referente della Sicurezza della PAL interessata;
- verifica e approva formalmente la strategia di intervento elaborata, eventualmente integrandola con indicazioni di carattere strategico desunte grazie al proprio ruolo di coordinamento a livello nazionale nel dominio della PA e di interfacciamento con altri CERT Regionali.

Il CERT Regionale offre quindi il supporto specialistico nel trattamento dell'incidente alle PAL coinvolte, in base alle informazioni/direttive provenienti dal CERT-PA contenute nella strategia di intervento condivisa con il CERT-PA, con il quale rimane costantemente allineato.

Coordinamento e supporto attività di gestione

Per Emergenze di carattere nazionale a rilevanza sistemica, il CERT-PA una volta attivato dal CERT Regionale:

- supporta e si coordina con il CERT Regionale nella gestione dell'incidente, che a sua volta coinvolgerà i Referenti della Sicurezza di tutte le PAL interessate;
- correla tutte le informazioni ricevute dalle diverse PAL, aggiornando la strategia di intervento in funzione delle comunicazioni ricevute, durante la gestione dell'incidente, dal CERT Regionale e delle indicazioni di carattere strategico desunte grazie al proprio ruolo di coordinamento a livello nazionale nel dominio della PA e di interfacciamento con altri CERT Regionali;
- verifica ed approva formalmente la strategia di intervento elaborata.

Il CERT Regionale assume quindi il coordinamento nel trattamento dell'incidente alle PAL coinvolte, in base alle informazioni/direttive provenienti dal CERT-PA contenute nella strategia di intervento condivisa con il CERT-PA, con il quale rimane costantemente allineato.

Supporto risposta incidente

Il CERT Regionale supporta il Referente della Sicurezza Informatica della PAL nella gestione dell'incidente rilevato e nella definizione del piano operativo di intervento.

In particolare, il CERT Regionale analizza il materiale ricevuto dalla PAL e, ove necessario, integra il piano di intervento con le indicazioni di carattere strategico provenienti dal CERT-PA e con le informazioni desunte in fase di analisi e ri-classificazione dell'incidente.

Il CERT Regionale condivide quindi il piano di intervento così integrato al Referente della Sicurezza Informatica della PAL.

Coordinamento risposta incidente sistemico PAL

Dopo la comunicazione formale di incidente sistemico della PAL, il CERT Regionale assume, in accordo con il CERT-PA, il coordinamento delle attività di gestione dell'incidente sistemico PA.

Il CERT Regionale analizza il materiale ricevuto dalla PA e, ove necessario, integra il piano di intervento con le indicazioni di carattere strategico provenienti dal CERT-PA e con le informazioni desunte in fase di analisi e ri-classificazione dell'incidente.

Durante tale fase il CERT Regionale coordina i Referenti della Sicurezza Informatica delle PAL coinvolte, con i quali condivide il piano degli interventi necessari al trattamento degli incidenti e dai quali riceve un aggiornamento costante sullo stato di avanzamento delle attività di trattamento.

Rientro stato ordinario

Nel momento in cui si chiude lo stato di emergenza, il CERT Regionale effettua la chiusura formale dell'incidente, redigendo un rapporto contenente (come minimo):

- codice univoco identificativo dell'incidente;
- data e ora di apertura della scheda di gestione incidente;
- rapporto di constatazione incidente, comprensivo dell'elenco dei danni subiti e di eventuali impatti sistemici;
- documentazione degli interventi posti in atto, specificando, particolarmente per gli incidenti sistemici, i sistemi/servizi coinvolti dalle attività di trattamento;
- data e ora di chiusura dell'incidente.

Tale rapporto deve essere inviato al CERT-PA e alle PA coinvolte, che a quel punto provvedono internamente alla chiusura dell'incidente.

Al rientro dello stato ordinario, il CERT regionale attiva il sotto-processo di ripristino e analisi post-incidente.

9.3.8 Ripristino e analisi post-incidente

Il sotto-processo di ripristino e analisi post-incidente viene dettagliato nella figura seguente.

Si dettagliano di seguito le attività indicate in Figura 9.5 (per la legenda dei simboli fare riferimento alla Figura 9.1).

Analisi post-incidente e follow up

Alla chiusura dell'incidente (di Livello 1 – 3), il Referente della Sicurezza Informatica della PA, invia al CERT Regionale tutti i dati relativi all'incidente gestito, necessari per consentire l'avvio dell'analisi post-incidente.

Tale analisi viene effettuata dal CERT Regionale relativamente al dominio logico di competenza, e va ad integrare le attività di analisi svolte parallelamente all'interno di ciascuna PA alla chiusura dell'incidente.

Tale processo consiste in una serie di attività programmate, volte a verificare:

- le caratteristiche dell'agente di minaccia responsabile dell'incidente;

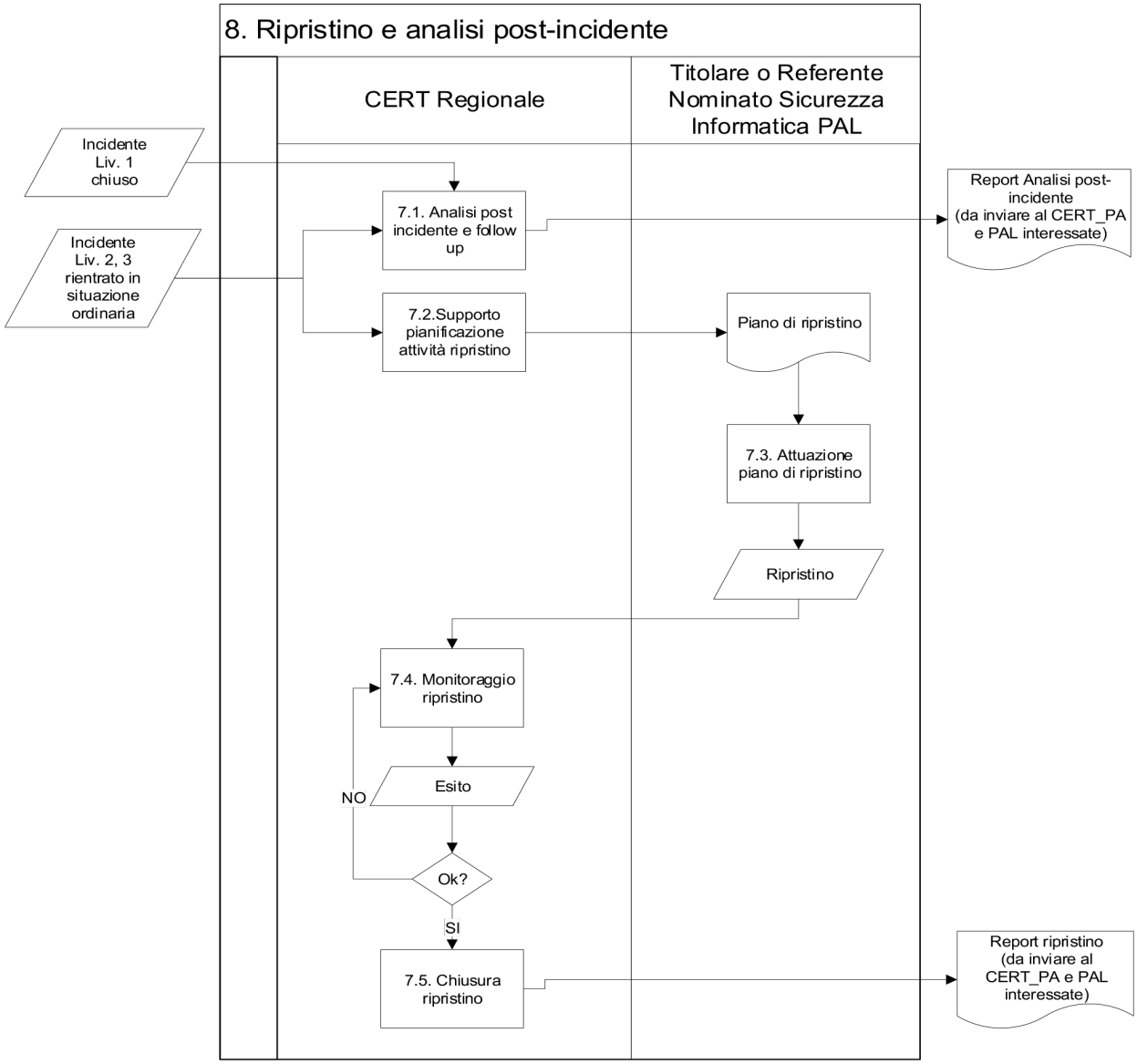

Fig. 9.5: Flusso di ripristino incidente

- le modalità di sviluppo dell'incidente, le circostanze e/o le vulnerabilità che lo hanno reso possibile;
- un eventuale piano propositivo per il miglioramento dello stato della sicurezza che tenda a contenere i rischi di nuovi incidenti di simile natura.

L'analisi post-incidente è un'attività posta sotto la responsabilità ed il coordinamento del CERT Regionale che si avvale del Referente della Sicurezza Informatica delle PAL e, ove necessario, di specialisti esterni. Essa comprende le seguenti attività:

- raccolta e isolamento dei dati relativi all'incidente;
- analisi degli asset coinvolti;
- analisi degli eventi correlati all'incidente;
- costruzione dello scenario causa-effetto;
- valutazione degli impatti e potenziali propagazioni degli incidenti;
- conservazione delle fonti di prova per fini probatori.

Al termine delle attività il CERT Regionale dovrà produrre un rapporto di analisi post-incidente, contenente le raccomandazioni necessarie ad evitare che un tale evento possa ripetersi, e lo invia al Referente della Sicurezza Informatica della PAL.

Nel corso di tutte le attività di analisi post-incidente deve comunque essere garantita la stretta osservanza delle leggi e delle normative in materia di privacy. Inoltre, tutto il personale componente il gruppo che effettua le analisi è sottoposto alla stretta osservanza di una clausola di riservatezza, che vieta la comunicazione a terzi di qualsiasi elemento o giudizio, anche a titolo di parere personale, relativo alle informazioni raccolte.

Tutte le attività di analisi post-incidente devono comunque essere formalmente autorizzate dal CERT Regionale, con l'indicazione delle finalità, del contesto, dei limiti temporali e delle modalità di esecuzione delle analisi. Qualora tali attività prevedano degli interventi all'interno della PAL, quest'ultimi devono essere concordati con il Referente della Sicurezza Informatica, condividendo un opportuno piano di azione nel quale devono essere dettagliate le attività svolte ed il personale coinvolto.

Salvo disposizioni differenti per contesti specifici, la copia elettronica del rapporto di analisi post incidente, dei dati raccolti nel corso delle analisi e delle raccomandazioni emesse, devono essere custoditi a cura del CERT Regionale per un periodo di dodici mesi solari. Dopo tale termine si provvederà alla loro rimozione ed alla distruzione dei supporti mobili di archiviazione.

Supporto pianificazione attività di ripristino

Alla chiusura formale dell'incidente che sancisce il termine dell'emergenza ed il rientro dello stato ordinario, il CERT Regionale supporta il Referente della Sicurezza Informatica della PA coinvolta dall'incidente nella definizione del piano di ripristino.

Il piano di ripristino è finalizzato a riportare il patrimonio informativo coinvolto dall'incidente nella situazione precedente all'incidente stesso e contiene (come minimo):

- PA e relativi asset ICT coinvolti dall'incidente;
- piano delle attività di rientro e descrizione dei passi operativi da svolgere;
- funzioni e responsabilità coinvolte dalle attività operative;
- date di rientro previste.

Generalmente il piano delle attività deve prevedere un rientro nei tempi più stretti possibile. Tuttavia, in funzione della tipologia, dell'estensione e dell'impatto registrato sul patrimonio informativo a seguito dell'incidente intercorso, è possibile avere piani di ripristino a lungo termine, che prevedano un rientro alla situazione antecedente all'incidente nell'arco di mesi o anni.

Attuazione piano di ripristino

Il Referente della Sicurezza Informatica della PA attua il piano di ripristino concordato con il CERT Regionale, attivando i gruppi operativi all'interno della PA ed eventualmente effettuando l'escalation di responsabilità verso altre strutture, in funzione delle procedure interne di trattamento degli incidenti di sicurezza.

Monitoraggio ripristino

Il CERT Regionale monitora periodicamente lo stato di avanzamento delle attività di ripristino, coordinandosi con il Referente della Sicurezza Informatica delle PA coinvolte e producendo dei SAL periodici sullo stato delle attività previste dal piano di ripristino.

Al termine delle attività, si passa alla chiusura formale delle attività di ripristino.

Chiusura ripristino

Il CERT Regionale chiude formalmente le attività di ripristino, redigendo un report di ripristino che contenga:

- data di chiusura delle attività di ripristino;
- riferimenti al piano di ripristino definito e alle sue eventuali ri-pianificazioni successive;
- riferimenti ai SAL effettuati durante l'attività di monitoraggio;
- esito delle attività di ripristino effettuate.

Tale rapporto deve essere inviato al CERT-PA e alle PA coinvolte, che a quel punto provvedono internamente alla chiusura dell'incidente.

9.4 Matrice delle responsabilità

Si riporta di seguito la matrice delle responsabilità relativa al processo di gestione incidenti della PA, indicando per ciascuna attività sopra descritta, l'attore coinvolto ed il grado di coinvolgimento, secondo la convenzione:

A	Analizza
R	Riceve
V	Valida/Verifica
E	Effettua
S	Supervisiona
I	Viene Informato
U	Supporta

Tabella 9.3: Matrice delle responsabilità

Id	Attività	Referente Sicurezza Informatica PA	CERT
1	Monitoraggi o degli eventi di sicurezza	E	
2	Analisi e classificazione	E	
3	Trattamento falsi positivi	E	
4	Gestione evento anomalo	U	E
5	**Gestione Incidenti Livello 0 (Non Rilevante) – Livello 1 (Informativo)**		
5.1	Definizione delle attività di gestione	E	
5.2	Trattamento incidente	E	I

Continua

Tabella 9.3 – continua dalla pagina precedente

Id	Attività	Referente Sicurezza Informatica PA	CERT
5.3	Chiusura incidente	E	
5.4	Comunicazio ne incidente Liv.1 al CERT Regionale	E	R
6	**Gestione Incidenti Livello 2 (Attenzione)**		
6.1	Coinvolgimento CERT Regionale	E	
6.2	Analisi e riclassifi cazione incidente	I	E
6.3	De-classificazione per falso positivo	I	E
6.4	Coinvolgimento PAL interessate	I	E
6.5	Analisi segnalazione	E	I
6.6	Supporto risposta incidente	R	E
6.7	Coordinamento risposta incidente sistemico PA	R	E
6.8	Trattamento incidente	E	I, S
6.9	Rientro stato ordinario	I	E
7	**Gestione Incidenti Livello 3 (Critico)**		
7.1	Coinvolgimento CERT Regionale	E	
7.2	Analisi e ri-classificazione incidente	I	E
7.3	De-classificazione per falso positivo	I	E
7.4	Coinvolgimento CERT-PA	U	E
7.5	Coinvolgimento PA interessate	I	E
7.6	Analisi segnalazione	E	I
7.7	Aggiornamen to CERT-PA	U	E
7.8	Supporto attività di gestione		R
7.9	Coordinamento e supporto attività di gestione		R
7.10	Supporto risposta incidente	R	E
7.11	Coordinamento risposta incidente sistemico PAL	R	E
7.12	Trattamento incidente	E	I, S
7.13	Rientro stato ordinario	I	E
8	**Ripristino e analisi post- incidente**		
8.1	Analisi post-incidente e follow-up	U	E
8.2	Supporto pianificazione attività di ripristino	U	E
8.3	Attuazione piano di ripristino	E	I
8.4	Monitoraggio ripristino	I, U	E
8.5	Chiusura ripristino	R	E

CAPITOLO 10

Risorse

10.1 Struttura organizzativa e risorse umane

Per raggiungere gli obiettivi definiti per la strategia del CERT è consigliato definire adeguatamente una struttura organizzativa in grado di evolversi coerentemente con lo sviluppo dei processi e dei servizi offerti dal CERT nel tempo, i ruoli chiave e le rispettive competenze e responsabilità.

L'organizzazione interna deve essere infatti oggetto di revisione nel tempo al fine di determinare un corretto dimensionamento e livello di specializzazione della struttura in relazione al volume ed alla tipologia di eventi ed incidenti di sicurezza gestiti, alle fonti informative e di intelligence analizzate ed alle relazioni di information sharing attivate verso la constituency.

L'articolazione organizzativa di un CERT dipende innanzitutto dalla struttura esistente nell'organizzazione ospitante e dalle caratteristiche della comunità di riferimento, nonché dalla possibilità, e relativa facilità, di poter ricorrere, in modo permanente o in funzione di specifiche esigenze, alle competenze di figure specialistiche presenti all'esterno.

A prescindere dalle considerazioni precedentemente espresse, per avviare le attività di un CERT è auspicabile definire una struttura organizzativa in grado di presidiare le seguenti aree:

- *Management*: che detiene la responsabilità dei compiti di pianificazione strategica, direzione ed indirizzo del CERT nonché di attivare le relazioni con la constituency e stabilire accordi di collaborazione con le altre organizzazioni pubbliche e private;
- *Operations*: con responsabilità della gestione complessiva e dell'operatività dei servizi erogati nei confronti della constituency. Figure che tipicamente rientrano in tale categoria sono costituite dagli operatori e dagli analisti, affiancati da team di esperti specializzati in singole aree di competenza (es. specialisti di prodotto, ecc.). A fronte di portafogli di servizi più articolati e definiti, potrebbe affiancarsi a questa anche un'area di specializzazione relativa ai servizi riconducibili alla Ricerca e Sviluppo – altrimenti parte della più ampia area delle Operations.
- *Processi di supporto*, che consentono il funzionamento complessivo dell'intera struttura; come si è visto, tale area comprende i processi di amministrazione e controllo, la gestione delle infrastrutture IT, inclusi i server e gli strumenti in uso esclusivo al CERT, la gestione ed amministrazione del personale, ecc. All'intero di tale ambito rientrano anche processi fondamentali per l'espletamento delle funzioni del CERT, quali quello di gestione della comunicazione interna ed esterna e l'area legale.

Si noti che durante il periodo di avvio del CERT, in cui non tutti i ruoli potrebbero essere formalmente assegnati, dovranno essere in ogni caso identificate le figure che, durante il periodo transitorio, assumeranno le rispettive responsabilità.

Una struttura organizzativa, che vede il coinvolgimento delle figure professionali necessarie per presidiare le aree precedentemente descritte, potrebbe essere rappresentata come segue:

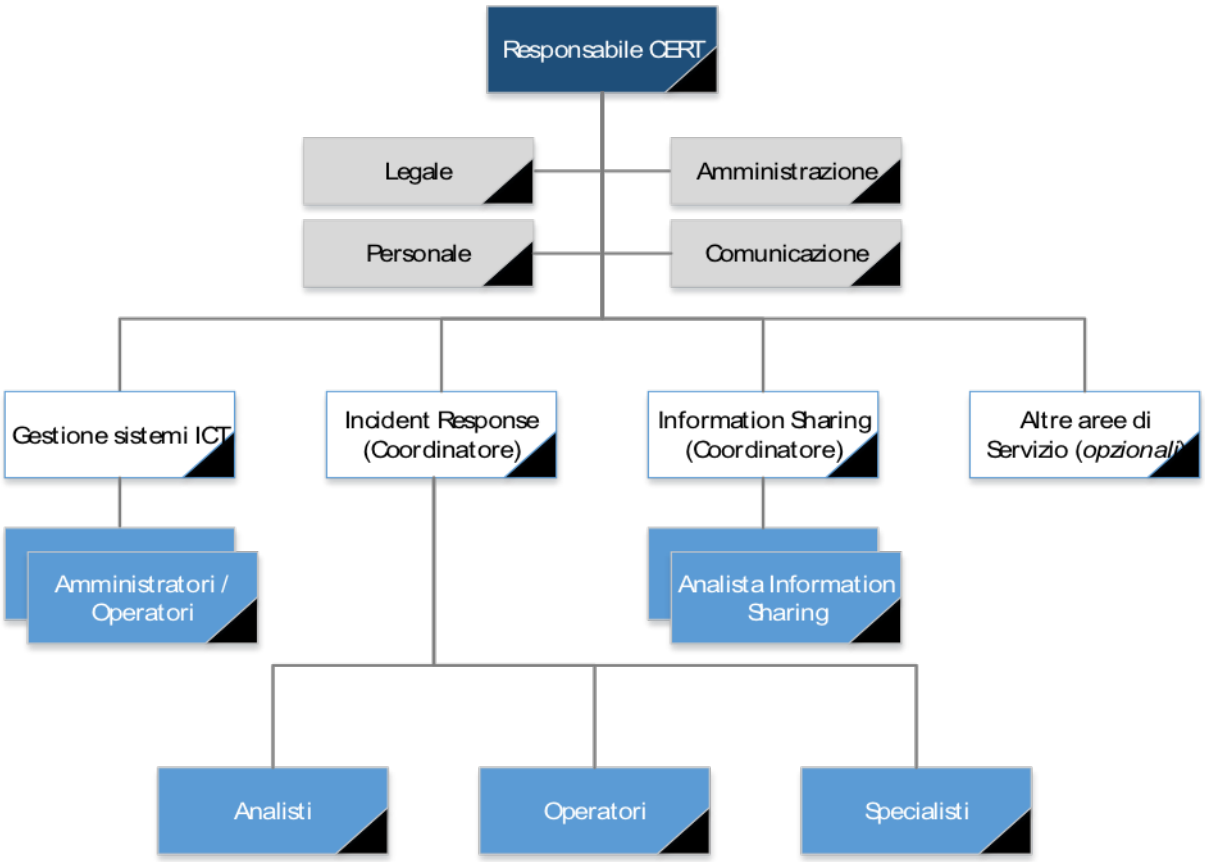

Fig. 10.1: Esempio di struttura organizzativa

Tale rappresentazione prende in considerazione le aree e i profili che devono essere attivati per soddisfare i fabbisogni riconducibili alla gestione dei servizi "core". Atri profili sono da ritenersi come opzionali in fase di avvio all'interno dell'organico del CERT, anche in relazione ad eventuali ulteriori servizi offerti verso la constituency ("Altre aree di Servizio").

I ruoli chiave che devono essere definiti nell'ambito del modello di CERT proposto, e le principali responsabilità e competenze richieste, necessari per garantire il corretto funzionamento dei servizi erogati ai soggetti accreditati, sono delineati nei paragrafi seguenti. Per ciascun ruolo viene inoltre proposta una possibile mappatura rispetto ad alcuni dei profili delineati all'interno del modello fornito dall'*e-CF*, *European e-Competency Framework*[72] (CWA 16458-1:2018 (E)).

10.1.1 Management

Responsabile CERT

Riferimento e-CF: *Information Security Manager Role*

[72] http://www.ecompetences.eu/ict-professional-profiles/

Responsabilità

- Identificare, definire e progettare i servizi CERT in base ai requisiti della constituency ed alle esigenze di protezione.
- Sviluppare, implementare e mantenere processi, policy e procedure e definire le linee guida per il miglioramento.
- Allocare le risorse necessarie per garantire un corretto funzionamento del CERT.
- Definire il piano di sviluppo e potenziamento per processi, risorse e tecnologie.
- Gestire e organizzare il team del CERT (formazione, incarichi di ruolo, ecc.).
- Rappresentare il punto di contatto con la constituency, con la comunità di riferimento e con i soggetti istituzionali in merito all'esecuzione dei servizi.
- Definire e gestire le comunicazioni verso l'esterno e supervisionare i processi di escalation.
- Definire e riesaminare gli indicatori di prestazione e qualità chiave.
- Assicurare la conformità alle policy e alle procedure del CERT.

Competenze richieste

- Conoscenza delle esigenze della constituency.
- Capacità di esercitare una presenza autorevole e di comando, come esperto in materia, durante le situazioni di crisi per gestire le comunicazioni relative agli incidenti di sicurezza.
- Capacità di gestire e allocare le risorse del team, assegnando le diverse priorità per ottenere risultati misurabili nel corso del programma.
- Forti capacità decisionali, con una comprovata capacità di valutare costi e benefici delle possibili azioni e identificare quelle più appropriate.
- Forti abilità comunicative nei confronti di diversi tipi di interlocutori.

Il Responsabile CERT deve designare, e rendere noto alla constituency e alla comunità, all'interno del team un soggetto delegato che lo possa sostituire e/o farne le veci in casi di assenza o indisponibilità temporanea o prolungata.

10.1.2 Operations

Coordinatori (Incident Response / Information Sharing)

Riferimento e-CF: *Service Manager Role*

Sono figure con compiti di indirizzo e coordinamento dei team di rispettiva competenza, necessarie a guidare l'efficacia e l'efficienza dei servizi e processi gestiti, dei quali monitorano le prestazioni, valutando e suggerendo raccomandazioni per il miglioramento continuo.

Analista Incident Response

Riferimento e-CF: *Systems Analyst Role, Systems Architect Role, Technical Specialist Role*

Responsabilità

- Analizzare e gestire i ticket relativi agli incidenti di sicurezza e documentare le azioni intraprese.
- Applicare la classificazione degli incidenti in base ai livelli di classificazione previsti dalla metodologia adottata.
- Analizzare e riportare gli incidenti rilevanti al Team Leader, definendo con questi un piano di risposta agli incidenti per gestire tutte le attività richieste.
- Fornire supporto nell'identificazione degli step di ripristino.

- Aggiornare la Knowledge Base con i risultati dell'analisi post-mortem sugli incidenti, al fine di sviluppare / aggiornare le procedure di risposta agli incidenti.
- Fornire i dati di input per il monitoraggio delle prestazioni dei processi di gestione degli incidenti.

Competenze richieste

- Capacità di eseguire analisi sugli allarmi e sulle segnalazioni di incidenti di sicurezza.
- Conoscenza delle tecniche di analisi degli incidenti e di analisi del malware e dei casi di utilizzo.
- Capacità di comprendere ed implementare soluzioni per la correzione e risoluzione di vulnerabilità tecniche.
- Conoscenza dei sistemi operativi e delle tecnologie in uso presso la constituency di riferimento.

In funzione del livello di specializzazione richiesta e dei servizi attivati, l'analista potrebbe presentare livelli di seniority differente e/o ambiti di competenza specifici. Ad esempio, potrebbero essere reclutati analisti dei malware con competenze specifiche sull'analisi del codice eseguibile, sia in modalità statica che dinamica, così come analisti forensi, dedicati a gestire la raccolta di evidenze e l'analisi delle stesse in concomitanza di un incidente relativo alla sicurezza delle informazioni, documentando il tutto in modo che sia correttamente presentabile in sede processuale[73].

Operatore Incident Response

Riferimento e-CF: *Technical Specialist Role*

Responsabilità

- Monitorare i dispositivi e l'infrastruttura in tempo reale, analizzando i log degli eventi e tutti gli altri input ricevuti.
- Rappresentare il punto di contatto verso gli utenti.
- Aprire ticket per tutte le segnalazioni interne ed esterne, richieste di lavoro e di informazioni.
- Eseguire una prima analisi dell'incidente ed effettuare il triage.
- Definire la strategia di risposta iniziale agli incidenti.
- Gestire l'escalation verso le altre entità coinvolte secondo le procedure stabilite.
- Fornire i dati di input per il monitoraggio delle prestazioni dei processi di gestione degli incidenti.

Competenze richieste

- Capacità di comprendere e riconoscere vulnerabilità tecniche.
- Conoscenza e capacità di utilizzo ed amministrazione di strumenti di trouble ticketing.
- Conoscenza dei sistemi operativi e delle tecnologie in uso presso la constituency di riferimento.

Specialista Incident Response

Riferimento e-CF: *Service Support Role*

Tali figure detengono una ampia conoscenza delle tecnologie che degli strumenti utilizzati per esaminare la sicurezza di sistemi e reti e competenze estese all'ingegneria e sviluppo del software, alla programmazione ed ai linguaggi di scripting.

Responsabilità

- Gestire e monitorare eventi di sicurezza e il comportamento dei prodotti di sicurezza.
- Fornire supporto nell'aggiornamento della Knowledge Base.

[73] Si veda a tal fine lo studio pubblicato da CLUSIT ("*Certificazioni Professionali in Sicurezza Informatica 2.0*", disponibile al seguente link: https://clusit.it/wp-content/uploads/download/Q09_web.pdf) che propone una raccolta delle diverse certificazioni professionali in materia di sicurezza informatica, presentate nei diversi ambiti applicativi (organizzativo, organizzativo/tecnologico, tecnologico vendor neutral e tecnologico di prodotto).

- Monitorare e misurare le metriche associate ai controlli di sicurezza.
- Lavorare a stretto contatto con altri analisti per identificare e affrontare le minacce in modo tempestivo.
- Gestire e risolvere i problemi operativi che coinvolgono i controlli di sicurezza.

Competenze richieste

- Capacità di eseguire analisi sugli allarmi e sulle segnalazioni di incidenti di sicurezza.
- Conoscenza dei sistemi operativi e delle tecnologie in uso presso la constituency di riferimento.
- Capacità di analizzare i flussi di pacchetti per identificare le anomalie.
- Esperienza nell'implementazione e nell'aggiornamento dei controlli di sicurezza e delle best practices.

Analista Information Sharing

Riferimento e-CF: *Information Security Specialist Role*

Responsabilità

- Supportare il Team Leader nella definizione della strategia di comunicazione in caso di minacce e/o attacchi in corso.
- Selezionare i contenuti da diffondere all'esterno in base ai livelli di confidenzialità delle informazioni.
- Identificare e gestire i canali per la diffusione e la comunicazione delle informazioni verso l'esterno.

Competenze richieste

- Conoscenza delle tecniche di comunicazione e gestione dei rapporti con i media.
- Esperienza nella redazione e pubblicazione di contenuti tematici.
- Conoscenza delle caratteristiche e dei servizi offerti dal CERT.

10.1.3 Personale di supporto

L'operatività del CERT dipende anche dalla presenza e dalle attività condotte da personale di supporto ai processi operativi, quali:

- personale dell'area Information Technology, che ha la responsabilità di implementare, gestire e mantenere aggiornati i sistemi e le infrastrutture informatiche in dotazione al CERT – sia di funzionamento che a supporto dell'erogazione dei servizi alla constituency[74];
- personale dell'area Amministrazione e Finanza, con responsabilità di gestire le risorse contabili al fine di garantire un adeguato controllo amministrativo, fiscale e finanziario dell'organizzazione, oltre a consentire la gestione del personale sotto il profilo amministrativo;
- personale dell'area Comunicazione, con il compito di supportare il management nella gestione delle comunicazioni con gli stakeholder del CERT e di mantenere costantemente aggiornati i contatti all'interno ed all'esterno dell'organizzazione, ad esempio attraverso la preparazione e distribuzione di news e bollettini e la gestione dei canali di comunicazione attivati dal CERT;
- personale dell'area Legale, che fornisce un supporto specialistico in materia normative e in merito alla possibilità di divulgare le informazioni in accordo con le policy del CERT, le leggi ed i regolamenti applicabili.

Pur riconoscendo la centralità delle attività di formazione del personale interno, la velocità di cambiamento degli scenari di rischio potrebbe richiedere talvolta l'intervento di figure esterne specializzate, in grado di fornire supporto mirato, nonché le linee guida per l'internalizzazione di competenze specifiche sulla base dei progetti svolti in collaborazione con figure consulenziali esterne.

[74] Le competenze richieste a tali figure possono essere individuate nei seguenti profili proposti dall'e-CF: ICT Operations Manager Role; Network Specialist Role, Systems Administrator Role; Data Administrator Role.

È difficile fornire requisiti ragionevoli per un dimensionamento iniziale di un CERT regionale, poiché vari fattori influenzano il numero di risorse necessarie. Prendendo in considerazione le esperienze di CERT di tipo nazionale/governativo[75], un dimensionamento adeguato da cui partire è compreso tra 3 e 5 FTE (quando i servizi sono forniti solo durante l'orario d'ufficio), fino ad arrivare a 6-8 FTE nel caso di realtà amministrative più complesse.

Al fine di fornire livelli di servizio sostenibili, indipendentemente dalla posizione per cui sono stati assunti, le risorse dovrebbero detenere un'ampia gamma di competenze per poter ricoprire più ruoli in una fase di avvio dei servizi. L'ipotesi di operatività 24/7/365 nell'ambito della constituency dovrà essere valutata in ragione del portafoglio di servizi, della struttura e delle responsabilità del team, considerando anche opzioni di reperibilità da remoto, al fine di garantire comunque tempi di risposta rapidi, specialmente per i rapporti sugli incidenti.

10.2 Modello dati e informazioni

I dati gestiti da un CERT seguono un ciclo vitale, costituito da cinque distinte fasi:

- raccolta;
- conservazione;
- utilizzo;
- diffusione;
- distruzione.

La creazione di un CERT è finalizzata a consentire ai membri della constituency di mettere in atto una risposta ottimale – in funzione preventiva o reattiva – a minacce o violazioni in ambito informatico. Per perseguire questo obiettivo, il CERT presumibilmente costituirà e gestirà una specifica banca dati in cui memorizzare le violazioni riscontrate e le eventuali minacce preventivate, creata mediante le segnalazioni dei vari utenti. Il CERT, pertanto, potrà considerarsi il gestore di tale banca dati.

È presumibile che le informazioni fornite da ciascun utente segnalante rivestano un elevato tasso di riservatezza, volto a tutelarne l'immagine; di conseguenza, è altrettanto probabile che l'utente interessato sia disponibile a condividere queste informazioni a condizione che le stesse siano trattate nel rispetto di rigorose regole di confidenzialità. Queste regole di confidenzialità determinano precisi obblighi di comportamento che vincolano il CERT ed i membri della constituency; a tal proposito si potrebbe anche valutare un diverso livello di trasparenza nei flussi informativi:

- dal segnalante al CERT;
- dalla banca dati CERT agli altri membri della constituency.

Il primo flusso potrebbe avvenire "in chiaro", in modo da permettere al CERT di effettuare tutte le valutazioni del caso senza condizionamenti di sorta. Diversamente, il flusso di informazioni dalla banca dati CERT al resto della constituency potrebbe vedere "oscurate" le informazioni identificative del segnalante, in aggiunta all'obbligo di confidenzialità dei partecipanti. In sintesi, gli obblighi di confidenzialità potrebbero prevedere il divieto di:

- divulgare ogni informazione del CERT a terzi non autorizzati ad accedervi;
- utilizzare tali informazioni per finalità o con modalità diverse da quelle espressamente previste;
- lasciare incustodite tali informazioni in modo da permetterne l'acquisizione da parte di terzi non autorizzati.

In linea teorica, si dovrebbe propendere per ritenere che i flussi informativi oggetto del servizio CERT non contengano informazioni suscettibili di identificare, direttamente o indirettamente, un individuo; cioè, che tali flussi non abbiano necessità dei "dati personali" per perseguire le finalità evidenziate. Infatti, è presumibile che le informazioni contenute possano essere riconducibili ad organizzazioni o ad altre entità impersonali ma non ad individui.

[75] Si vedano anche ENISA, "Baseline capabilities for National / Governmental CERTs, Part 1", Version 1.0 (2009), ENISA, "Baseline capabilities for National / Governmental CERTs, Part 2, Policy Recommendations", Version 1.0 (2010), ENISA, "ENISA's recommendations on baseline capabilities", Update, December 2014 (2014)

10.2.1 Dati in movimento e dati statici

Con dati in movimento si intendono tutti quei dati in transito da un punto ad un altro attraverso la rete. Tutti i dati coinvolti nei flussi informativi diretti al o provenienti dal CERT si possono considerare dati in movimento. La protezione di questi dati si rende necessaria e critica dal momento che i dati in movimento sono considerati maggiormente vulnerabili.

I dati statici sono dati del CERT che, non essendo attivamente in movimento, si trovano conservati o archiviati in dispositivi adibiti a tale scopo. In generale si tende a considerare i dati statici come meno vulnerabili rispetto ai dati in movimento, ma molto spesso chi attacca ritiene più conveniente dirigere i suoi sforzi verso dati statici.

Il profilo di rischio dei dati in generale, siano essi in movimento o statici, dipende in ogni caso dal livello delle misure di sicurezza che si adottano per proteggere entrambe le categorie di dati. Adottare misure adeguate in tal senso è divenuto un imperativo per ogni tipo di organizzazione, dal momento che gli attacchi volti a sottrarre o compromettere dati sensibili stanno costantemente crescendo in termini di sofisticatezza.

Come detto, i dati possono essere esposti al rischio sia se in movimento che se statici; sarà pertanto necessario prevedere delle forme di tutela per entrambe le situazioni. La cifratura gioca un ruolo di primo piano quando si parla di protezione dei dati, siano questi in movimento o statici. Nel caso dei dati in transito, la cifratura viene impiegata prima di muovere i dati che si intende proteggere. I dati statici vengono cifrati prima dell'archiviazione, altrimenti è possibile cifrare il dispositivo stesso utilizzato per l'archiviazione.

Un'inadeguata protezione dei dati sensibili gestiti espone un'organizzazione a dei rischi, rendendola vulnerabile a potenziali attacchi. Oltre alla cifratura, le best practices in termini di protezione dati - in movimento o statici – suggeriscono di:

- realizzare robusti controlli di sicurezza della rete. Forme di protezione come firewalls o sistemi di controllo accessi contribuiranno a rendere maggiormente sicura la rete impiegata per la trasmissione dei dati, proteggendola da attacchi ed intrusioni;
- non fare totale affidamento su forme di sicurezza reattiva per proteggere i propri dati, ma impiegare anche misure di sicurezza proattiva che identifichino i dati potenzialmente a rischio in modo preventivo, predisponendo un sistema di sicurezza adeguato;
- scegliere soluzioni di protezione dei dati con criteri che consentano all'utente di richiedere, bloccare o cifrare automaticamente i dati sensibili in transito, ad esempio quando i file vengono allegati a un messaggio di posta elettronica o spostati sul cloud, in unità rimovibili o trasferiti altrove;
- predisporre politiche al fine di categorizzare sistematicamente e classificare tutti i dati gestiti dall'organizzazione - indipendentemente dalla loro ubicazione - al fine di garantire che vengano approntate forme di protezione mentre i dati restano fermi e attivate le misure adeguate quando i dati classificati come a rischio sono accessibili, utilizzati o trasferiti.

Se dati in movimento e dati statici possono avere profili di rischio talvolta diversi, il rischio intrinseco dipende principalmente dalla sensibilità e dal valore dei dati stessi. Coloro che attaccano cercheranno di accedere a dati sensibili sia in movimento che statici, a seconda di quale sia lo stato più facile da violare. Ecco perché un approccio proattivo che includa la classificazione e la categorizzazione dei dati sensibili è il modo più sicuro ed efficace per proteggere entrambe le categorie di dati.

10.2.2 Tipologie di dati trattati dal CERT

Oltre alla distinzione precedentemente illustrata tra dati in movimento e dati statici, è possibile distinguere tra varie tipologie di dati gestiti/trattati/diffusi da un CERT nel modello previsto, differenti tra loro sia a seconda del contenuto che della provenienza o destinazione – da o verso altri CERT e altri enti, da o verso i membri della constituency.

Tra queste:

- dati riguardanti i membri della constituency raccolti attraverso il processo di accreditamento, inclusi dati sull'organizzazione ed eventuali dati personali;

- dati contenuti nelle segnalazioni di incidente provenienti dai membri della constituency (es. log, files, asset, indirizzi IP, timestamp, ecc.);
- dati raccolti attraverso il processo di threat intelligence (svolto internamente o in outsourcing), ovvero IoC (in diversi formati STIX, TAXII, JSON), dump relativi a data breach, e tutti gli attributi necessari o che concorrono ad identificare puntualmente una minaccia (domini, indirizzi IP, URL, hash di file, stringhe, ecc.);
- dati riguardanti nuove vulnerabilità provenienti da altri CERT e da vendors;
- dati riguardanti minacce emergenti provenienti da enti collocati a livello superiore.

In funzione dei servizi attivati e delle parti con cui un CERT interagisce, è possibile definire un modello dati come quello rappresentato nella figura seguente:

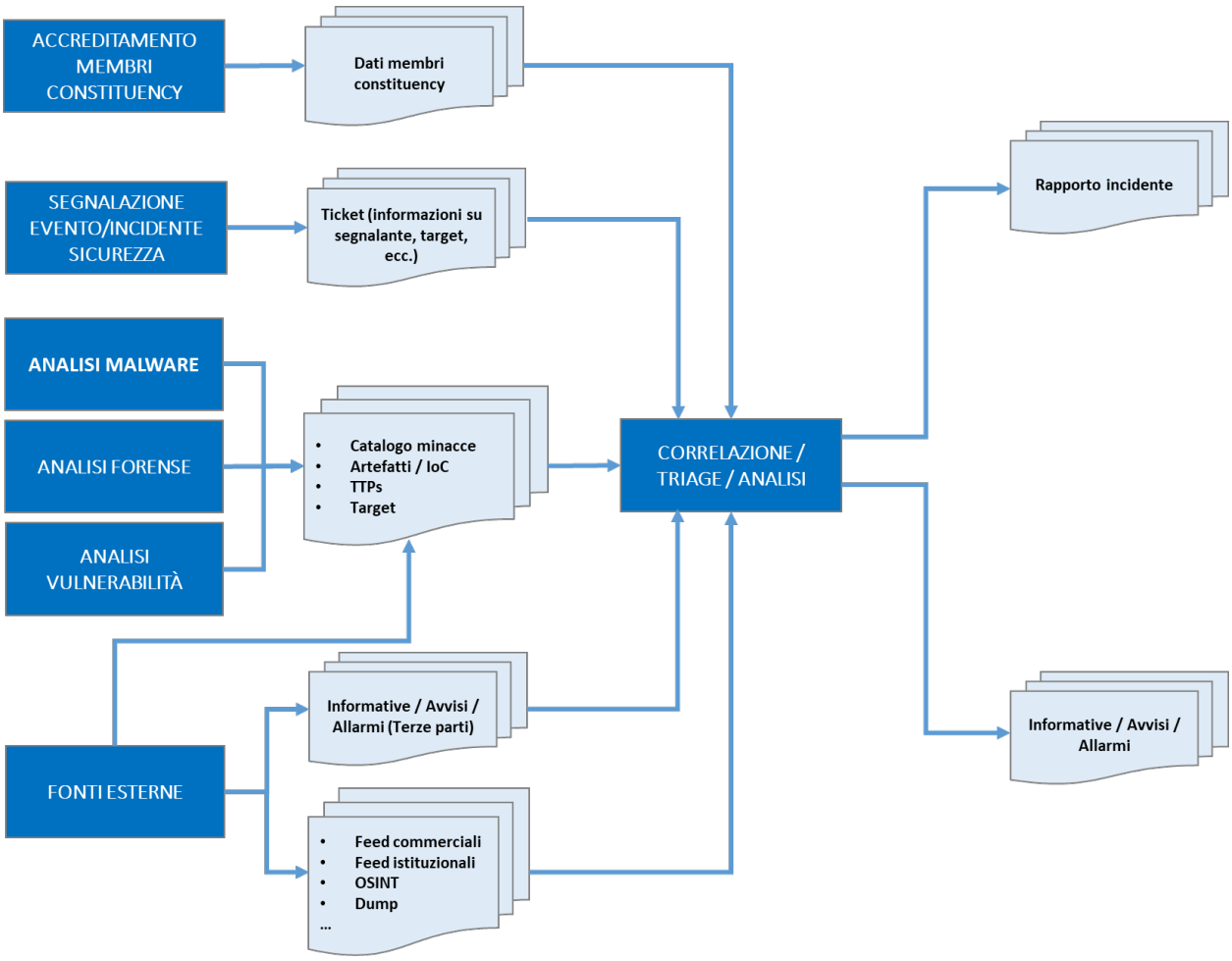

Fig. 10.2: Modello dati di un CERT

10.2.3 Criteri di classificazione delle informazioni

Le informazioni devono essere classificate e quindi trattate a seconda della classificazione assegnata, ovvero del livello di riservatezza assegnato alle stesse. Attraverso il processo di classificazione viene stabilito chi è autorizzato ad accedere alle singole informazioni e modificarle e quali misure di protezione fisica, logica e tecnica devono essere adottate dal momento della sua origine fino a quello della sua distruzione o declassifica.

In ambito civile, i tipici livelli di classificazione assegnati alle informazioni sono quello di: informazione pubblica, informazione ad uso interno dell'organizzazione e informazione ad uso ristretto. Altri livelli possono basarsi sulla normativa Privacy (ad esempio, la normativa italiana distingue tra dati personali, personali sensibili e personali giudiziari, per i quali sono da applicare diverse misure di sicurezza).

10.3 Modelli tecnologici e applicativi

Per garantire l'operatività del CERT, devono essere identificate opportunamente le tecnologie necessarie per il funzionamento complessivo dell'organizzazione e per supportare i processi di analisi e risposta agli incidenti e di comunicazione verso tutte le parti interessate.

Uno dei requisiti chiave è consentire che il CERT possa operare in un ambiente completamente separato ed indipendente da altre infrastrutture ICT esistenti. In altri termini, il CERT deve operare attraverso propri sistemi, applicazioni e infrastrutture di rete.

Per una maggior completezza dei temi trattati in questo documento, in coda ad alcuni paragrafi saranno presentate delle schede di approfondimento riguardo le tecnologie open source al momento utilizzate dai principali CERT a livello internazionale.

10.3.1 Infrastruttura di rete

L'infrastruttura di rete del CERT deve seguire una configurazione tale da garantire da un lato il soddisfacimento dei livelli di servizio richiesti, dall'altro la protezione dei dati e delle informazioni trattate.

Risulta quindi necessario a tal fine un'infrastruttura di rete in grado di soddisfare i requisiti di operatività, protezione e continuità rispetto ai servizi offerti alla constituency, nonché individuare gli strumenti di comunicazione necessari e le piattaforme applicative.

A livello logico è auspicabile l'impiego di uno o più firewall per segmentare la rete in più aree indipendenti (VLAN) in base ai servizi da queste erogati. Una possibile configurazione è la seguente:

- segmento di rete (DMZ esterna) utilizzato esclusivamente per ospitare i servizi pubblici (web, mail, portale, ecc.) esposti su Internet. Questi possono essere mirati per la propria constituency o comprendere altre attività (es. bollettini, linee guida) volte ad una diffusione più ampia.
- la rete interna (CERT LAN), dedicata allo svolgimento delle attività di amministrazione e gestione e di operatività del CERT. In questo caso è auspicabile definire un'ulteriore segregazione tra la LAN destinata ad ospitare le postazioni e le dotazioni assegnate al personale del CERT ed un segmento di DMZ interna per ospitare i file server, i sistemi di ticketing e i server a supporto degli strumenti per l'erogazione dei servizi alla constituency. In questo modo è possibile definire un'area sicura per la conservazione, l'accesso e il trasferimento di dati da e verso il CERT, nonché per una gestione interna al CERT, secondo il principio di *need-to-know*. Le informazioni legate ad incidenti rilevati all'interno della propria constituency dovrebbero infatti essere mantenute con la massima riservatezza su server (fisici/virtuali) dedicati, non raggiungibili dall'esterno.
- segmento di rete dedicato ad un'area di test (laboratorio), essenziale nel caso in cui il CERT eroghi servizi di analisi degli artefatti o di investigazione forense. Tale area non solo deve permettere la gestione in sicurezza di artefatti malevoli, ma comprendere un'architettura (fisica/logica) isolata, che può includere macchine virtuali e device dedicati, dove riprodurre, in ambiente controllato, situazioni di compromissione di sistemi per analizzarne il comportamento e valutare possibili contromisure. La segregazione di tale rete è essenziale per la protezione dei dati custoditi dal CERT e per preservare l'operatività e l'integrità di tutti i servizi offerti. L'ambiente di test, infine, deve poter essere ripulito e ripristinato rapidamente dopo un'investigazione.

Il CERT deve disporre di una connessione Internet per erogare i propri servizi pubblici (web, mail, etc.). È auspicabile che il collegamento Internet avvenga tramite due ISP (Internet Service Provider) differenti così da garantire continuità

operativa nel caso di guasto sulla linea principale. La presenza di una linea telefonica dedicata, fissa e/o mobile, consente di rendere raggiungibile il CERT anche tramite chiamata o fax: tale alternativa permette di avere comunicazioni in caso di emergenza, ad esempio, qualora vi sia un'assenza di connettività dalla rete Intenet di un membro della constituency o del CERT stesso.

I server utilizzati dal CERT sia per i servizi interni che esterni possono essere fisicamente separati o rappresentati tramite un unico cluster virtuale per ottimizzare le risorse disponibili ed aumentare la tolleranza ai guasti.

La figura seguente mostra una possibile configurazione dell'architettura di rete come precedentemente illustrato:

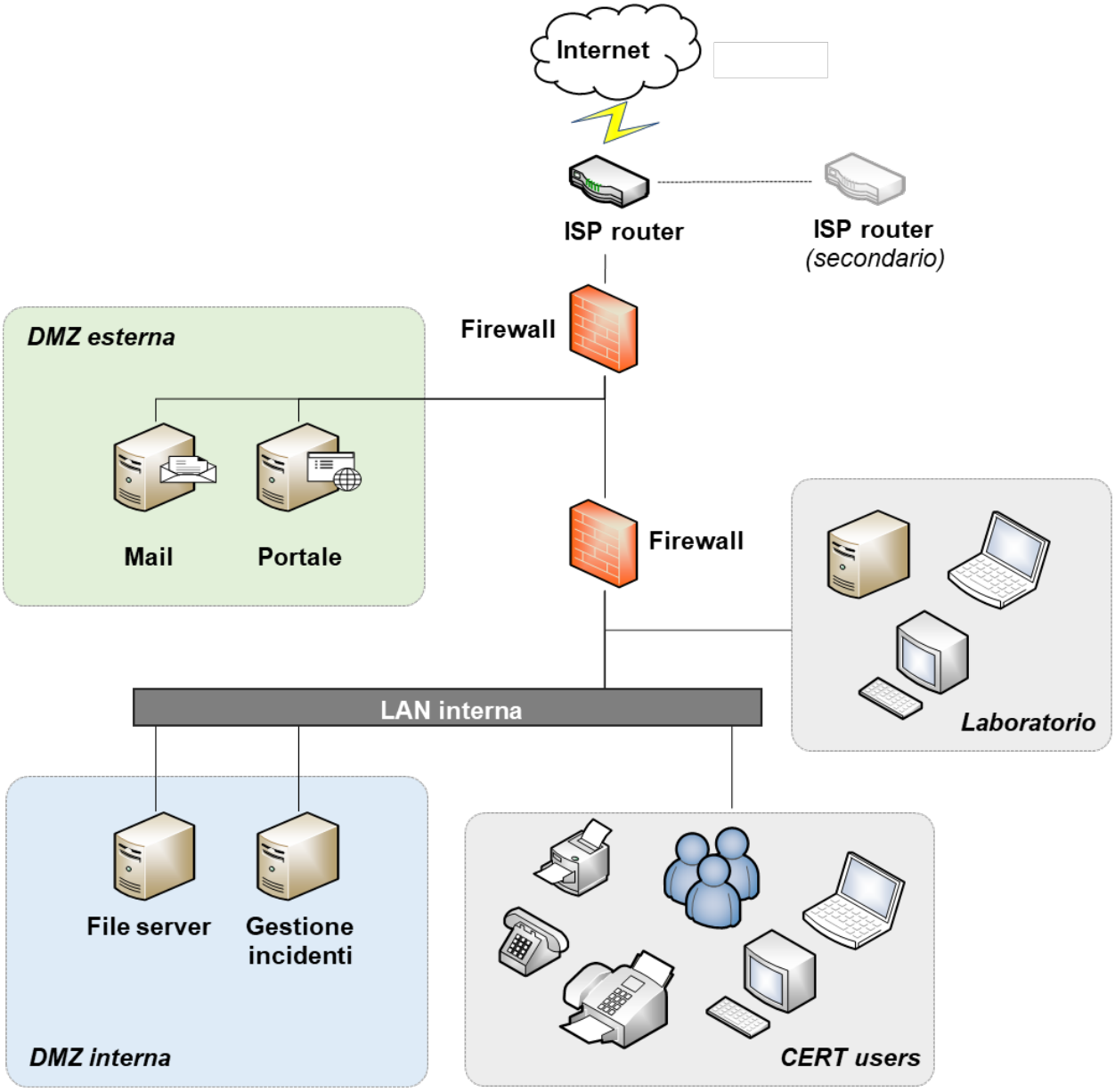

Fig. 10.3: Infrastruttura di rete

10.3.2 Strumenti

I servizi erogati dal CERT verso la propria constituency dovranno essere supportati da strumenti specializzati per area di servizio, che possono tuttavia essere impiegati anche per più aree funzionali:

- *Strumenti di correlazione* (crawling/mining/correlation), ovvero tecnologie che abilitano attività di threat intelligence in termini di raccolta, ricerca ed analisi dei dati su minacce, violazioni, ecc.
- *Piattaforme per l'information sharing*, ovvero tecnologie dedicate all'acquisizione ed allo scambio di informazioni ed alla relativa trasmissione alle soluzioni di sicurezza per la prevenzione e il monitoraggio.
- *Strumenti per l'analisi malware*, volti all'esecuzione di analisi statica e dinamica di codice eseguibile
- *Strumenti per l'investigazione e l'analisi forense*, strumenti volti all'acquisizione ed analisi di tutti i dati necessari che riguardano un attacco subìto da sistemi.
- *Strumenti di comunicazione sicura*, per coordinare e consentire lo scambio di informazioni con la constituency e la comunità di riferimento sulla base dei livelli di protezione e sicurezza richiesti (es. meccanismi di autenticazione, cifratura delle comunicazioni).
- *Knowledge Base*, ovvero un ambiente volto a facilitare la raccolta, l'organizzazione e la distribuzione della conoscenza sulle modalità di analisi e risoluzione degli incidenti con l'obiettivo di favorire la definizione di modus operandi standardizzati.
- *Strumenti di ticketing*, ovvero tecnologie per favorire l'automazione dei workflow autorizzativi e la tracciatura delle attività effettuate per l'analisi e la risoluzione degli incidenti.
- *Strumenti per la conduzione di simulazioni/formazione*, che comprendono le piattaforme applicative di e-learning (*Learning Management System*) che permettono l'erogazione dei corsi online e quelle destinate alla progettazione di scenari simulati per la conduzione di esercitazioni.

Strumenti di correlazione

Tali tecnologie abilitano la raccolta, l'analisi e la correlazione di informazioni da molteplici fonti su minacce, violazioni, ecc., costituendo di fatto un input per il processo di Incident Response. In particolare, favoriscono la conduzione di analisi su specifiche minacce e dunque l'individuazione di linee guida ed indicazioni per le successive attività investigative e rendendo possibile la condivisione con gli altri soggetti coinvolti per le azioni di prevenzione e monitoraggio.

Le principali funzionalità correlate a tali tecnologie sono:

- raccolta dati su host, domini, siti web compromessi ed indirizzi IP associati ad attività malevole;
- capacità di collezionare e aggregare più dati da diverse sorgenti in formati differenti;
- capacità di correlare i dati raccolti;
- supporto alle attività di analisi dei contenuti degli indicatori di minaccia e delle relative relazioni tra i contenuti.

---

example

IntelMQ

IntelMQ (https://github.com/certtools/intelmq) è una soluzione sviluppata con la collaborazione di ENISA, e di diversi CERT della Comunità Europea, per i CERT per la raccolta e il trattamento delle informazioni provenienti da diverse fonti, come security feeds, pastebins e tweets utilizzando un protocollo di tipo message queue.

Obiettivo principale è dare uno strumento semplice agli incident responders per raccogliere ed elaborare informazioni di threat intelligence, migliorando i processi di gestione degli incidenti nei CERT. È stato ideato seguendo delle linee guida volte a sviluppare un software semplice da utilizzare e minimale nelle sue funzionalità evitando quindi inutili complessità. Il risultato è quindi un prodotto volto a:

- ridurre la complessità per l'amministrazione del sistema;
- ridurre la complessità di scrivere di nuovi bots (moduli aggiuntivi) per nuovi feed di dati;
- ridurre la probabilità di perdita di informazioni con funzionalità di persistenza (anche crash di sistema);
- usare e migliorare l'esistente Data Harmonization Ontology;
- usare il formato JSON per tutti i messaggi;
- integrazione dei tool esistenti (AbuseHelper, CIF);
- fornire un modo semplice per archiviare i dati in collettori di log commerciali o database (e.g. PostgreSQL);
- fornire un modo semplice per creare le proprie black-list;
- fornire una facile comunicazione con altri sistemi tramite l'utilizzo di HTTP RESTFUL API.

example

The Hive

The Hive (https://thehive-project.org/) è una piattaforma di risposta agli incidenti di sicurezza scalabile, open source e gratuita, progettata per agevolare le operazioni dei gruppi di sicurezza nel corso delle relative analisi.

Consente la collaborazione da parte di più analisti simultaneamente sulle stesse indagini, sfruttando funzionalità come lo "streaming live" integrato, che rende accessibile in tempo reale a tutti i membri del team le informazioni relative a casi nuovi o esistenti, attività, osservabili e IOC. Permette inoltre di automatizzare alcune operazioni di analisi e investigazione.

Può essere facilmente integrata con altre piattaforme quali MISP (vedere successivamente), da cui è possibile importare direttamente gli oggetti da analizzare come IP e indirizzi e-mail, URL, file o hash, e Cortex, che permette di analizzare tali oggetti utilizzando un'unica interfaccia (in alternativa ad una pluralità di strumenti).

Strumenti di comunicazione sicura

I CERT come si è visto devono proteggere sistematicamente i dati trattati durante le proprie operazioni. Ciò implica l'adozione di strumenti di comunicazione sicura nei casi in cui i dati sono raccolti da altre fonti o condivisi e scambiati con altre entità.

In linea generale la comunicazione verso l'esterno può avvenire tramite le seguenti tecnologie:

- VoIP – Voice over IP è un sistema di comunicazione che rende possibile chiamate audio-video (videochiamata, videoconferenza, etc.) sfruttando una connessione Internet;
- e-mail – electronic mail è un servizio Internet per lo scambio di messaggi tra utenti aventi un proprio indirizzo di posta elettronica registrato presso un provider del servizio;
- web – diminutivo di World Wide Web, è il principale servizio pubblico di scambio informazioni attraverso la rete Internet.

Esistono diverse modalità per permettere scambi di informazioni in modalità sicura. Le principali sono:

- cifratura dei canali di comunicazione (Instant Messaging, Chiamate, Video Chiamate, Video Conferenze, Email);
- cifratura dei contenuti allegati;
- sistemi di condivisione di documentazione.

L'utilizzo di cifratura a chiave pubblica (es. PGP, GPG), di certificati digitali (X.509) e di protocolli di comunicazione sicura (es. HTTPS), risulta indispensabile per mitigare il rischio di attacchi di tipo man-in-the-middle e spoofing e per garantire adeguati livelli di sicurezza (es. comunicazioni autenticate/cifrate) sui canali di scambio.

---

example

GnuPG

GnuPG (Privacy Guard) (https://www.gnupg.org/) è un'implementazione open source che segue lo standard RFC4880, ovvero il formato per lo scambio di messaggi OpenPGP.

GnuPG permette di criptare e firmare i dati e le comunicazioni. Inoltre è dotato di un versatile sistema di gestione delle chiavi e moduli di accesso per potersi collegare a tutti i tipi di directory di chiavi pubbliche, ovvero i repository pubblici dove scambiare le informazioni di verifica degli utenti.

GnuPG, noto anche come GPG, è uno strumento nato per i sistemi operativi open source utilizzando solo la linea di comando con tutta una serie di funzionalità per una facile integrazione con altre applicazioni. Attualmente sono disponibili numerose applicazioni e librerie per l'utente finale. GnuPG fornisce anche supporto per S/MIME e Secure Shell (SSH). Per i sistemi operativi Windows è possibile utilizzare l'applicativo Gpg4win, un software open source per il trasferimento di messaggi digitalmente firmati e cifrati nonché contenente un plugin per Outlook in grado di mandare e ricevere email con formato di cifratura sicuro PGP/MIME.

Piattaforme di info-sharing

Tali strumenti consentono la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di compromissione e minacce relative all'analisi degli incidenti di sicurezza informatica e all'analisi di malware. Attraverso l'utilizzo di tali piattaforme è possibile condividere informazioni in forma strutturata all'interno della propria comunità o anche all'esterno, favorendo l'adozione di approcci comuni per la risoluzione degli incidenti. Questo processo permette infatti agli stakeholder lo scambio di informazioni delicate e privilegiate mantenendo la confidenzialità e la fiducia nella comunicazione e mantenendo la sicurezza delle informazioni.

---

example

MISP (Malware Information Sharing Platform)

MISP (https://www.misp-project.org/), è una soluzione software open source per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di compromissione e minacce relative all'analisi degli incidenti di sicurezza informatica e all'analisi di malware. MISP è progettato da e per analisti di incidenti, professionisti della sicurezza e delle ICT come piattaforma per la condivisione di informazioni in modo efficiente.

L'obiettivo di MISP è favorire la condivisione di informazioni in forma strutturata all'interno della propria comunità o anche all'esterno. MISP fornisce funzionalità per supportare lo scambio di informazioni ma anche il consumo delle informazioni da parte di Intrusion Detection System (IDS) sia a livello di rete che di sistema, inoltre viene anche utilizzato dagli strumenti di analisi dei log e correlazione di log quali i SIEM.

Tra le sue caratteristiche principali troviamo:

- un efficiente database di IoC che consente di archiviare informazioni tecniche e non tecniche riguardo malware, incidenti e altri temi di cyber intelligence;
- correlazione automatica volta a rilevare relazioni tra attributi e indicatori di malware, attacchi registrati o analisi;
- un modello di dati flessibile in cui oggetti complessi possono essere espressi e collegati tra loro per esprimere threat intelligence, incidenti o elementi connessi;

- funzionalità di sharing integrate per facilitare la condivisione dei dati utilizzando diversi modelli di distribuzione. MISP può sincronizzare automaticamente eventi e attributi tra diversi MISP. Funzionalità di filtro avanzate possono essere utilizzate per soddisfare ogni politica di condivisione dell'organizzazione;
- un'intuitiva interfaccia utente per creare, aggiornare e collaborare su eventi e attributi / indicatori. Un'interfaccia grafica per navigare senza problemi tra gli eventi e le loro correlazioni. Funzionalità di filtro avanzate e lista di avvisi per aiutare gli analisti a contribuire con eventi e attributi;
- memorizzazione dei dati in un formato strutturato (che consente l'uso automatizzato del database per vari scopi) con un ampio supporto degli indicatori per la cyber security, ad esempio utilizza indicatori di frode specifici per il settore finanziario;
- esportazione: generazione di IDS (i pricipali vendor sono supportati nativamente), OpenIOC, file di testo, CSV, MISP XML e JSON per l'integrazione con altri sistemi;
- importazione: supporto operazioni quali bulk-import e batch-import per l'importazione da OpenIOC, GFI sandbox, ThreatConnect CSV e MISP, inoltre permette l'importazione di testo libero per semplificare l'integrazione di report non strutturati. Integra infine uno strumento flessibile per importare, oltre i feed MISP, qualsiasi feed da fonti commerciali ed open source, di cui molte configurazioni predefinite sono incluse nell'installazione standard di MISP;
- consente agli utenti di MISP di proporre modifiche o aggiornamenti di attributi / indicatori;
- condivisione dei dati: scambio automatico e sincronizzazione con altre parti e gruppi che utilizzano MISP;
- delega della condivisione: consente, tramite un semplice meccanismo pseudo-anonimizzante, di delegare la pubblicazione di eventi / indicatori a un'altra organizzazione;
- espone API flessibili per integrare MISP con la propria soluzione;
- tassonomia personalizzabile per classificare e ed assegnare tag agli eventi seguendo i propri schemi di classificazione o tassonomie già esistenti. La tassonomia può essere locale o condivisibile tra diversi gruppi MISP. Viene fornita inoltre una serie predefinita di tassonomie e schemi di classificazione ben noti per supportare la classificazione standard utilizzata da ENISA, Europol, DHS, CSIRT ed altre ancora;
- un set di vocabolari di intelligence pre-esistenti con attaccanti, malware, RAT, ransomware, etc., attualmente presenti nel panorama della sicurezza cibernetica e che possono essere facilmente collegati agli eventi in MISP;
- moduli di espansione in Python per interconnettere MISP ai propri servizi;
- supporto di notifica per ottenere avvisi da organizzazioni relative a modifiche di indicatori e attributi condivisi. Tali avvisi possono essere forniti tramite l'interfaccia utente MISP o le API messe a disposizione;
- supporto STIX: esportazione dei dati nel formato STIX (XML e JSON) compresa l'ultima versione STIX 2.0;
- crittografia e firma integrate delle notifiche tramite PGP e/o S/MIME.

example

MineMeld

Molte organizzazioni raccolgono indicatori di compromissione (IoC) da vari fornitori di informazioni sulle minacce con l'intento di creare nuovi controlli per i dispositivi di sicurezza. Gli approcci tradizionali impiegati per l'aggregazione e l'applicazione sono di natura strettamente manuale, portando alla creazione di flussi di lavoro estremamente complessi e allungando i tempi necessari per identificare e convalidare quali IoC dovrebbero essere bloccati.

Il tool open-source MineMeld (https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld) semplifica le operazioni di aggregazione, applicazione e condivisione delle informazioni sulle minacce. MineMeld supporta una varietà di casi d'uso, quali:

- aggregazione e correlazione di feed di informazioni sulle minacce, raccolte da fonti di intelligence pubbliche, private e commerciali;
- applicazione di nuovi controlli di prevenzione, comprese le blacklist su indirizzi IP;
- condivisione degli IoC con peer di fiducia;
- possibilità di integrazione con altre piattaforme di sicurezza per un'applicazione automatizzata dei controlli basati sulla prevenzione

L'architettura modulare scalabile consente inoltre di aggiungere funzionalità MineMeld aggiungendo codice al repository open-source.

Knowledge Base

Si tratta di tecnologie che supportano la creazione di repository che contengano informazioni su minacce, incidenti e relative soluzioni adottate, rendendo di fatto più agevole la ricerca di informazioni e più efficaci le attività di analisi e correlazione con i dati storici e, consentendo, in ultima analisi, la definizione di un modus operandi standard.

Le principali funzionalità correlate a tali tecnologie sono:

- accesso ai contenuti basato su ruoli e su principi di "need-to-know" e "least-privilege";
- elevata facilità di ricerca dei contenuti;
- contenuto "ready-to-use";
- guida su istruzioni operative per gestire gli incidenti;
- tracciamento di tecniche, soluzioni e procedure di risoluzione.

example

Alfresco

Alfresco (https://www.alfresco.com/it/piattaforma) è uno strumento di Enterprise Content Management per Microsoft Windows e per sistemi Unix-like. Oltre ad una versione proprietaria con supporto commerciale (Enterprise Edition) è disponibile anche una pubblicata sotto licenza GNU GPL (Community Edition). È basata su un'architettura open source e supporta gli standard aperti, per facilitarne l'integrazione, l'estensione e la personalizzazione della stessa.

È una piattaforma per la gestione di documenti e per forme di collaboration interne ed è una soluzione molto diffusa per la gestione dei contenuti non strutturati all'interno di un'organizzazione. Offre funzionalità di Enterprise Content Management (ECM) aperte, flessibili e altamente scalabili. I contenuti sono accessibili ovunque siano necessari, nella modalità preferita dall'utente, e si integrano facilmente con le altre applicazioni utilizzate all'interno dell'organizzazione. Alfresco permette infatti di accedere in modo rapido e sicuro ai contenuti rendendo possibile per gli utenti una facile individuazione e condivisione degli stessi, anche grazie a funzioni di ricerca, flussi di lavoro e metadati avanzati, quali a titolo esemplificativo:

- utilizzo di «smart folder» per la ricerca dinamica con suggerimenti automatici, filtri e anteprima dei contenuti velocizzano il recupero dei contenuti richiesti;
- funzioni di collaborazione evolute quali siti per team, controllo delle versioni, thread di discussione, wiki, elenchi di task e feed delle attività.

La piattaforma fornisce inoltre estese funzionalità di information governance, consentendo una completa automatizzazione della gestione del ciclo di vita dell'informazione, dall'acquisizione alla conservazione fino alla rimozione finale, compresa la gestione dei livelli di autorizzazione necessari a controllare in modo granulare gli aspetti legati alla sicurezza degli accessi all'informazione.

Sistema di gestione dei ticket (Workflow Automation)

Tali tecnologie favoriscono l'automazione e la tracciatura delle attività di Incident Response. In particolare, consentono di gestire il processo di risoluzione dell'incidente in maniera automatizzata, dalla registrazione della segnalazione fino alla soluzione. In questo modo, è possibile avere una visione completa del processo seguito, visualizzando l'avanzamento della soluzione passo dopo passo e con la possibilità di allegare, ed utilizzare successivamente, ampia documentazione correlata all'evento.

Le principali funzionalità correlate a tali tecnologie sono:

- supporto per l'automatizzazione di workflow di processo, attori e task;
- template per la gestione di incidenti noti sulla base di occorrenze pregresse;
- supporto per la definizione di playbook personalizzati per le attività di risposta agli incidenti;
- integrazione con soluzioni di threat intelligence, indagine forense e di monitoraggio degli eventi di sicurezza;
- storicizzazione degli eventi.

---

example

RTIR

Request Tracker for Incident Response (RTIR) (https://bestpractical.com/rtir/) è una piattaforma web, basata sul sistema di ticketing RT, orientata alla gestione degli incidenti da parte di un CERT.

RTIR dispone di strumenti per correlare informazioni chiave sui rapporti degli incidenti, con funzionalità automatiche e ricerche manuali: trova ad esempio schemi comuni e collega i rapporti sugli incidenti aventi causa comune. Può essere utilizzato per gestire la comunicazione a più parti interessate che collaborano alle risposte e possibili altri team interni.

Tra le sue caratteristiche principali:

- disponibilità di una dashboard dedicata agli incidenti con elenchi predefiniti delle richieste più frequenti. Può essere modificata per mostrare subito i ticket ritenuti più importanti;
- gli eventi possono essere classificati usando numerosi campi predefiniti o aggiungendo eventuali campi personalizzati;
- vengono indicizzati tutti i campi per una ricerca rapita ed efficace nel database;
- possono essere generati report delle attività svolte in formato HTML, testo o foglio di calcolo;
- consente una gestione semplice dei collegamenti tra diverse richieste afferenti lo stesso incidente, vengono inoltre mostrati tutti i collegamenti tra rapporti sugli incidenti, indagini, e contromisure insieme allo stato corrente di ciascuno;
- supporto bulk operation;
- espone API RT per accettare automaticamente feed da sistemi esterni commerciali;
- crea diverse code per la gestione degli incidenti e per separare nuove richieste in arrivo;
- integra ed estende tutte le funzionalità native di RT.

Strumenti per la conduzione di formazione/simulazione

Tali tecnologie sono volte ad arricchire i processi di apprendimento classici offrendo strumenti di tipo digitale. In linea generale, tali sistemi offrono le seguenti funzionalità di base:

- essere accessibili online e da remoto;

- prevedere percorsi di apprendimento basati su materiale multimediale di tipo testuale, audio, video;
- consentire e un monitoraggio continuo delle attività compiute dai soggetti coinvolti nell'attività formativa;
- presentare test di valutazione del livello di apprendimento;
- consentire l'interazione tra i partecipanti tramite scambio di messaggi/ sistemi di videoconferenza.

Tali tecnologie comprendono un ampio spettro di strumenti, dalle tradizionali piattaforme di e-Learning (*Learning Management System*) fino a piattaforme più evolute di apprendimento/simulazione online, che consentono la conduzione di esercitazioni pratiche su vari argomenti di cyber security, anche in stile «Capture the Flag" e impiegando sistemi reali ed interattivi da attaccare.

10.4 Facilities

Le facilities sono un sottoinsieme del patrimonio fisico dell'organizzazione che viene utilizzato per eseguire i servizi. Sono centri di attività in cui si intersecano molti servizi dell'organizzazione, come edifici per uffici e locali tecnici. Possono essere di proprietà dell'organizzazione ma spesso vengono noleggiate da un fornitore esterno. Le persone, le informazioni e le risorse tecnologiche «vivono» all'interno delle facilities: forniscono lo spazio fisico per le azioni delle persone (le persone lavorano negli uffici), l'uso e la memorizzazione delle informazioni (file, server) e l'operazione di componenti tecnologici (come nei data center e nelle server farm). Proprio per tale ragione è cruciale l'adozione di requisiti di sicurezza fisica ed ambientale idonei a consentire la protezione delle informazioni (si veda il Cap. 12).

CAPITOLO 11

Sicurezza

11.1 Sicurezza fisica

La gestione della sicurezza fisica concerne l'identificazione e l'adozione di tutte le misure necessarie per proteggere le aree, i sistemi e le persone che operano sui sistemi informativi e le informazioni (riservate, sensibili, ecc.) da questi raccolte, trattate e conservate.

La sicurezza fisica degli ambienti del CERT deve essere progettata in modo tale da garantire dei livelli appropriati di protezione delle informazioni gestite. Alcuni aspetti più immediati da considerare sono la disponibilità di aree dedicate per ogni rappresentanza all'interno del CERT, aree sicure per tutti i server e le repository di dati del CERT, così come casseforti o armadi blindati per le informazioni e i dati non elettronici, e la disponibilità di linee cifrate e sicure di comunicazione interna ed esterna (telefoni, fax, email, schemi crittografici), al fine di impedire accessi non autorizzai, danni o interferenze.

La sicurezza delle aree concerne la protezione degli ambienti che ospitano le persone e i sistemi, impedendo accessi non autorizzati, danni e interferenze, danneggiamento delle informazioni e impedimento allo svolgimento dei servizi e dei processi informatici.

È importante osservare che l'adozione di alcune misure minime di sicurezza fisica delle strutture che ospitano i CERT deve essere assicurata per poter soddisfare i requisiti di accreditamento ed affiliazione richiesti da organizzazioni ed associazioni di riferimento quali ENISA, Carnegie Mellon, FIRST, Trusted Introducer.

In particolare sono di seguito riportate alcune delle misure minime da implementare, ovvero:

- Stabilire un luogo specifico per ogni locale del CERT, con in aggiunta una struttura protetta per le riunioni (war room).
- Assicurare la chiusura delle porte di accesso ai locali del CERT.
- Rafforzare i controlli fisici di accesso (badge, chiavi) al fine di impedire accessi non autorizzati alle strutture del CERT.
- Rendere disponibile in ogni locale del CERT un deposito sicuro (armadio chiuso a chiave, cassaforte) per archiviare la documentazione riservata ed il disco di backup.
- Dotare i locali di distruggi documenti.

- Adottare, in conformità con i termini di legge, sistemi di videosorveglianza per proteggere i perimetri esterni e registrare gli accessi alle aree riservate.
- Attivare all'interno dei locali sistemi di allarme con sensori di movimento quando personale del CERT o altro personale autorizzato (vigilanza, servizi di pulizia, ecc.) non sono presenti.
- Adottare le dovute contromisure per proteggere le conversazioni telefoniche confidenziali, per non renderle accessibili a terzi non autorizzati.

Altre misure, per quanto raccomandabili al fine garantire il raggiungimento di livelli di sicurezza superiori, possono ritenersi opzionali, anche in considerazione della relativa complessità e dei costi implementativi.

Un'ulteriore area di sicurezza fisica da considerare concerne quella delle apparecchiature, ovvero l'insieme delle misure in grado di assicurare la protezione delle risorse ICT e dei supporti da danneggiamenti accidentali o intenzionali e la sicurezza ambientale demandata principalmente agli impianti di alimentazione e di condizionamento. Tali misure sono da valutare ed implementare quando il CERT ha in gestione esclusiva anche la componente di data center e delle apparecchiature informatica. I fattori da tenere in considerazione in questi casi sono:

- *Posizionamento delle apparecchiature*: le apparecchiature devono essere disposte su pavimenti flottanti, a distanza da condutture di liquidi. I server e gli apparati di rete devono essere posti in appositi armadi (rack).
- *Sistemi di climatizzazione*: deve essere implementato un sistema di controllo del livello di temperatura ambientale e di umidità, almeno nelle aree che ospitano i server, al fine di garantire le condizioni ambientali volute.
- *Sistema rilevamento allarmi ambientali*: comprendono i sistemi di rivelazione fumo e sistemi antincendio, con attivazione dei relativi impianti di spegnimento degli incendi, progettati in conformità con le normative di settore al fine di non mettere a rischio la sicurezza delle persone né danneggiare i sistemi, e impianti di allarme anti-allagamento da posizionare al di sotto del pavimento flottante.
- *Impianti di alimentazione elettrica*: deve essere garantita l'alimentazione elettrica delle apparecchiature e degli impianti. Ciò può avvenire configurando le linee di alimentazione elettrica in modo che provengano da sorgenti separate, attraverso l'uso di UPS (Uninterruptible Power Supply) e batterie tampone (per protezione da brevi black-out o discontinuità elettriche) e di gruppi elettrogeni (per protezione in caso di lunghi black-out, purché sia garantita la disponibilità di combustibile per alimentarli). UPS, batterie e generatori devono avere la potenza necessaria per sostenere tutte le apparecchiature ad essi collegate durante il periodo di indisponibilità dell'alimentazione elettrica.
- *Cablaggi*: i cavi di alimentazione elettrica e di telecomunicazione devono essere disposti in canaline sotto un pavimento flottante o aeree per evitare danneggiamenti involontari. Tali canaline devono essere opportunamente distinte tra i cablaggi di alimentazione e quelli di telecomunicazione, per evitare interferenze reciproche, ed etichettate all'inizio e alla fine per consentirne rapidamente il riconoscimento della funzione. Ove possibile, è auspicabile corazzare le canaline se transitano fuori dalla sede (per evitare manomissioni volontarie o danneggiamenti durante interventi ordinari e straordinari sulle aree esterne (es. scavi).

11.1.1 Archivi fisici

Gli archivi fisici possono essere utilizzati per conservare documenti su supporto non digitale (carta, fotografie, ecc.) o digitale (hard disk, nastri, CD, DVD, ecc.). L'accesso agli archivi fisici deve essere regolamentato attraverso l'assegnazione di opportune autorizzazioni e meccanismi di controllo degli accessi condivisi, come chiavi tradizionali o combinazioni, oppure personali, spesso basati sulla lettura di tessere magnetiche, smart card o caratteristiche biometriche. Per evitare che i documenti o i supporti siano danneggiati, devono essere controllati costantemente da controllare temperatura e umidità degli archivi.

All'intero degli uffici e delle aree critiche tutti i documenti devono essere conservati negli archivi e sulla scrivania essere presenti solo quelli strettamente indispensabili per evitare che persone non autorizzate le possano leggere (clear desk policy).

11.2 Sicurezza logica

Se da un lato la sicurezza fisica rappresenta un primo livello di protezione dei dati, dall'altro la sicurezza logica costituisce uno strato indispensabile per la difesa di sistemi e reti informatiche. Infatti, in ragione della natura delle informazioni trattate dal CERT in caso di vulnerabilità ed incidenti, oltre alle misure di sicurezza per i canali di comunicazione, dovrebbero essere implementati controlli logici di sicurezza per proteggere la riservatezza e l'integrità delle informazioni.

Una base di partenza può essere validamente rappresentata, nel contesto nazionale italiano, dalle Misure minime di Sicurezza ICT per la PA[76], ovvero quell'insieme di controlli volti a garantire una sicurezza di base a tutte le organizzazioni esposte alle minacce di tipo cyber.

I suddetti controlli possono essere raccolti nei seguenti ambiti di sicurezza:

- *Inventario dispositivi e software*: individuare i sistemi (hardware, software), i servizi e le risorse che gestiscono i dati informatici trattati da proteggere.
- *Governance*: identificare e rispettare le leggi e/o i regolamenti con rilevanza in tema di cyber security applicabili al contesto.
- *Protezione da malware*: i dispositivi in perimetro quando possibile devono utilizzare software di protezione, ad esempio antivirus / anti-malware, regolarmente aggiornato.
- *Gestione password e account*: assicurare una complessità adeguata delle password e gestire le utenze secondo i principi di *need to know* e *least privilege*.
- *Formazione e consapevolezza*: sensibilizzare il personale sui rischi di cyber security e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali.
- *Protezione dei dati*: i sistemi devono essere configurati tramite procedure di hardening e backup periodici devono essere effettuati.
- *Protezione delle reti*: le reti e i sistemi devono essere protetti da accessi non autorizzati attraverso componenti hardware / software.
- *Prevenzione e mitigazione*: i software utilizzati vanno mantenuti aggiornati o dismessi in caso risultino obsoleti e non più aggiornabili. Nel caso di un incidente informatico devono essere informati i responsabili di sicurezza che seguiranno il processo di gestione degli incidenti interno.

[76] AGID "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*" (2017).

CAPITOLO 12

Modelli di analisi e valutazione dei risultati raggiunti

Disporre di metriche ben definite è essenziale per poter valutare i risultati delle attività di un CERT e dell'azione complessiva verso la propria constituency. Tali prestazioni devono essere valutate sia in termini di robustezza dei risultati (efficacia) che di tempestività nel raggiungimento (efficienza).

Tali misure forniscono informazioni fondamentali per il management del CERT al fine di migliorare le prestazioni dell'organizzazione e determinare il livello target di efficacia delle pratiche e processi di sicurezza implementati in favore della propria constituency.

Esistono diverse modalità per misurare i risultati delle attività di un CERT. Nell'ambito di questo documento, si propongono alcune metriche organizzate rispetto a tre differenti categorie:

- indicatori sulla qualità della risposta degli incidenti;
- indicatori sulla qualità della prevenzione degli incidenti;
- indicatori sulle capacità generali del CERT, utilizzate per valutare – anche indirettamente - l""impatto" della mission del CERT.

12.1 Indicatori sulla qualità della risposta agli incidenti

- Numero di incidenti segnalati
- Numero di incidenti gestiti
- Numero di incidenti ricorrenti già gestiti in passato
- Tempo medio di risoluzione di un incidente (espresso ad esempio rispetto al tipo di incidente, al livello di gravità, alle risorse critiche coinvolte)
- Definizione di processi con fasi chiaramente identificate, ruoli e responsabilità e meccanismi di escalation
- Disponibilità di strumenti e standard condivisi
- Livello di consapevolezza raggiunto dalle diverse parti interessate (come indicatore delle capacità di comunicazione del CERT)

- Tempo medio per il contenimento iniziale di un incidente cyber
- Tempo medio tra il momento in cui l'incidente è rilevato e il momento in cui è assegnato a un gruppo di lavoro
- Capacità di identificare la natura dell'incidente e/o delle caratteristiche dell'attacco (vulnerabilità sfruttata, attaccante, motivazione)
- Percentuale di incidenti di sicurezza gestiti in conformità con le politiche, le procedure e i processi stabiliti
- Capacità di rimuovere la minaccia dal target attaccato
- Capacità di collaborare con altri team CERT a supporto di indagini e procedimenti giudiziari (ad es. espressa come numero di organizzazioni/CERT con cui sono stati sottoscritti accordi di reciproco data-sharing)
- Livello di precisione delle stime effettuate dal CERT durante la gestione dell'incidente rispetto a quelle convalidate durante l'analisi post-incidente (ciò può fornire indicazioni utili sull'efficacia della capacità decisionale del CERT in condizioni di incertezza)
- Capacità del CERT di adattarsi rapidamente all'evoluzione delle circostanze dell'incidente, mantenendo i livelli di servizio e qualità attesi

12.2 Indicatori sulla qualità della prevenzione degli incidenti

- Percentuale di incidenti cyber che hanno sfruttano vulnerabilità esistenti con soluzioni, patch o workaround
- Percentuale di incidenti cyber che hanno sfruttato vulnerabilità non note (es. Zero-day attacks)
- Tempi medi che intercorrono tra gli incidenti
- Numero di exploit di vulnerabilità per organizzazioni e/o individui appartenenti alla constituency del CERT
- Percentuale di sistemi con risorse o funzioni critiche che sono stati oggetto di attività di vulnerability assessment
- Trend di rilevamento per famiglie di malware rilevanti
- Accesso a feed di dati su minacce e attacchi
- Livello di supporto per capacità di threat intelligence e relativi risultati (sia dal punto di vista della data collection che degli analytics)
- Traduzione in informazioni per la distribuzione alla comunità degli stakeholder
- Traduzione di informazioni utilizzabili per la risposta agli incidenti

12.3 Indicatori sulle capacità generali

- Volume di informazioni prodotte dal CERT (avvisi, bollettini, rapporti)
- Numero di accessi alle informazioni fornite dal CERT
- Numero di richieste raccolte dalla constituency
- Quantità di informazioni presentate alla propria constituency su tematiche di cyber security o sulle attività in corso
- Perdite monetarie totali derivanti da attacchi cyber subite dalla constituency servita dal CERT (normalizzate rispetto alle dimensioni della constituency)
- Capacità di offrire servizi in termini di numero e/o qualità rispetto ai propri peer (ciò può essere misurato sia effettuando la valutazione rispetto a standard o best practice di settore, sia effettuando una misurazione comparativa dei risultati dei peer in situazioni analoghe)

- Disponibilità di finanziamenti sufficienti
- Numero totale di membri dello staff
- Assegnazione tra i membri dello staff di esperti legali e di comunicazione specializzati
- Assegnazione di personale specializzato in discipline tecniche (analisi del codice, analisi forense, ecc.)
- Livelli di istruzione / formazione dei membri dello staff
- Frequenza e qualità della formazione interna su aspetti tecnici specialistici
- Numero di esercitazioni cyber condotte dal CERT internamente
- Livello di conformità dei processi e delle procedure del CERT a standard e specifiche normative (può essere determinato attraverso l'ottenimento di certificazioni o attività di audit)
- Capacità di proteggere la confidenzialità dei dati e delle informazioni durante le proprie operazioni (ad esempio durante il processo di gestione di un incidente)
- Livello di utilizzo delle risorse del CERT rispetto alla sua effettiva capacità (si noti come un elevato utilizzo delle risorse possa portare da un lato a tempi di risposta migliori e/o indicare una migliore allocazione, mentre dall'altro il pieno utilizzo potrebbe essere un indicatore del raggiungimento della capacità massima con possibili ripercussioni nella capacità di erogare altri servizi)
- Capacità del CERT di stabilire canali di comunicazione che permettono una trasmissione efficiente dei dati e delle informazioni (sia verso l'interno che verso l'esterno)
- Livello di soddisfazione della constituency (customer satisfaction), determinabile attraverso survey e questionari
- Capacità del CERT di effettuare le proprie operazioni senza necessità di supporto esterno (un eccessivo ricorso a capacità esterne potrebbe essere un indicatore di risorse inadeguate o insufficienti a supporto dei servizi)

CAPITOLO 13

Modelli di finanziamento

Un elemento chiave nell'analisi di fattibilità di un CERT regionale è rappresentato dall'individuazione del modello da attuare per la copertura finanziaria degli investimenti e dei costi riconducibili alle fasi di attivazione (investimento iniziale) e di gestione ordinaria dei servizi.

Con riferimento agli investimenti iniziali necessari all'attivazione del CERT regionale, così come suggerito anche da ENISA, potrebbe essere valutata l'eventualità di ricevere finanziamenti di tipo governativo a livello nazionale e/o o comunitario. Grazie all'adozione della Strategia dell'Unione Europea per la Cyber Security del 2013, rivista ed ampliata nel 2017, la Commissione Europea ha infatti intensificato gli sforzi per migliorare e rafforzare le misure di protezione per i cittadini e le imprese, stanziando importanti fondi per gli investimenti rivolti alla ricerca e l'innovazione per iniziative in ambito di cyber security.

Per l'Unione Europea è diventato prioritario individuare ed assegnare competenze e definire gli strumenti per prevenire gli incidenti che possono verificarsi in quest'ambito e, parallelamente, per sviluppare capacità di risposta in caso di avvenuto incidente. Più nello specifico, la Commissione sta promuovendo l'avvio di iniziative che possano favorire sia il settore pubblico che il settore privato nel raggiungimento dei seguenti obiettivi:

- aumentare le capacità e la cooperazione in materia di cyber security, cercando di uniformare il livello di maturità in tutti gli Stati membri dell'UE e garantendo che gli scambi di informazioni e la cooperazione siano efficaci, anche a livello transfrontaliero;
- consentire ai cittadini, alle imprese (di qualsiasi dimensione) ed alle amministrazioni pubbliche dell'Unione Europea di accedere alle più recenti tecnologie per la sicurezza digitale;
- rendere la cyber security parte integrante delle future iniziative politiche dell'Unione Europea, in particolare per quanto riguarda le nuove tecnologie ed i settori emergenti.

Tali interventi poggiano su un impianto programmatorio pluriennale e possono essere suddivisi in due tipologie:

- *fondi a gestione diretta*, ovvero erogati direttamente dalla Commissione Europea agli utilizzatori finali attraverso la partecipazione a bandi rivolti alla presentazione di iniziative di ricerca e innovazione;
- *fondi strutturali* (o a gestione indiretta), ovvero gestiti dagli Stati membri che, sulla base di programmi operativi e attraverso le proprie amministrazioni centrali e locali, ne dispongono l'assegnazione ai beneficiari finali e ne rendicontano l'utilizzo alla Commissione Europea.

Sono illustrati a seguire i principali programmi di finanziamento avviati negli ultimi anni e finalizzati a promuovere iniziative in ambito di cyber security.

13.1 Fondi a gestione diretta

Fondi strutturali e di investimento europei (European Structural and Investment Funds)

Con un bilancio pari a 454 miliardi di EUR per il periodo 2014-2020, i Fondi strutturali e di investimento europei (fondi SIE) rappresentano il principale strumento della politica di investimento dell'Unione Europea. Per il periodo in esame, prevedono un contributo fino a 400 milioni di euro per investimenti in ambito cyber security e protezione dei dati, volti a migliorare interoperabilità e interconnessione delle infrastrutture digitali, i sistemi di identità digitale, la privacy e i trust services.

Trattandosi di una gestione concorrente dei finanziamenti, per accedere alle relative risorse, le autorità competenti (nel caso dell'Italia, le Regioni, i Ministeri e le Agenzie ministeriali) devono redigere – ed ottenere l'approvazione dalla Commissione Europea – i relativi programmi operativi, ovvero documenti che specificano come saranno impiegati i fondi strutturali.

In Italia esistono in particolare due tipologie di programmi operativi:

- Programmi Operativi Nazionali (PON)
- Programmi Operativi Regionali (POR)

A questo proposito, l'individuazione di tali finanziamenti deve essere effettuata non solo a partire dall'analisi dei programmi pubblicati dalla Commissione Europea, ma anche, e soprattutto, di quelli che sono stati effettivamente lanciati dalle autorità nazionali o regionali, per quanto riguarda le relative modalità di partecipazione e le scadenze.

Per accedere alle possibilità di fondi e finanziamenti è necessario collegarsi ai portali dei vari programmi o delle Agenzie che coordinano i progetti (a livello nazionale e locale), controllare le relative sezioni in cui sono pubblicati avvisi e bandi, dove sono raccolte le call disponibili. Nella documentazione di riferimento della singola opportunità sono dettagliati i criteri di idoneità ed ammissibilità, le modalità di presentazione delle proposte e le relative tempistiche.

13.1.1 Programmi Operativi Nazionali (PON)

Dei quattordici PON italiani per il periodo di programmazione 2014-2020, i seguenti risultano rilevanti per supportare eventuali iniziative da avviare in ambito cyber security[77].

I PON di interesse in tal senso sono:

PON Governance e Capacità Istituzionale[78]

Gestito dall'Agenzia della Coesione Territoriale, è il programma volto a sostenere il Paese nello sviluppo, nel miglioramento e nel rafforzamento della capacità amministrativa e istituzionale, in linea con obiettivi della Strategia Europa 2020 (crescita intelligente, inclusiva e sostenibile). I progetti finanziati sono rivolti in particolare ad amministrazioni pubbliche centrali, regionali, locali, enti pubblici, strutture periferiche dello Stato; azioni specifiche potranno essere rivolte ad associazioni della società civile, università e centri di ricerca. Il programma è articolato su quattro assi prioritari, dei quali il secondo "*Sviluppo dell'e-government, dell'interoperabilità e supporto all'attuazione dell'Agenda Digitale*"supporta la realizzazione di infrastrutture digitali funzionali agli interventi di modernizzazione delle Pubbliche Amministrazioni italiane

Le opportunità di finanziamento e le informazioni relative ai bandi di gara e di concorso sono presentate e periodicamente aggiornate su un apposito portale, nell'area "Opportunità".

PON Per la Scuola- competenze e ambienti per l'apprendimento[79]

Il PON "Per la Scuola - competenze e ambienti per l'apprendimento"contribuisce all'attuazione della Strategia UE 2020 ed interviene sul contrasto alla dispersione scolastica, sul miglioramento della qualità del sistema di istruzione e

[77] http://www.guidaeuroprogettazione.eu/guida/guida-europrogettazione/fondi-strutturali/programmi-operativi-nazionali-pon/
[78] Per ulteriori informazioni consultare la pagina: http://www.pongovernance1420.gov.it/it/
[79] Per ulteriori informazioni consultare la pagina: http://www.istruzione.it/pon/index.html

dell'attrattività degli istituti scolastici, potenziando gli ambienti per l'apprendimento, favorendo la diffusione di competenze specifiche e sostenendo il processo di innovazione e digitalizzazione della scuola. Il Programma si sviluppa attraverso quattro assi prioritari d'intervento, dei quali il secondo "*Infrastrutture per l'istruzione*" ha tra gli obiettivi anche quello di potenziamento delle dotazioni tecnologiche.

Per accedere ai fondi specifici per ogni sezione e per altri finanziamenti consultare la sezione "Avvisi" sul portale del Programma.

13.1.2 Programmi Operativi Regionali (POR)

In Italia i POR sono multisettoriali, si sviluppano sull'intero territorio delle singole regioni e vengono finanziati con Fondi Strutturali europei attraverso la gestione delle Amministrazioni Regionali[80].

I POR rilevanti ai fini del miglioramento dei livelli di cyber security sono quelli che dispongono di opportunità di fondi e finanziamenti rispetto la realizzazione dell'Agenda Digitale, la promozione di Ricerca e Innovazione, lo sviluppo tecnologico, la diffusione dei servizi digitali e l'e-governance, ed il miglioramento e la sicurezza delle Tecnologie dell'Informazione e delle Comunicazioni (TIC).

Le Regioni interessate in tal senso sono:

- Abruzzo (http://www.regione.abruzzo.it/)
- Bolzano (http://www.provincia.bz.it/it/)
- Calabria (http://www.regione.calabria.it/website/)
- Campania (http://www.regione.campania.it/)
- Emilia Romagna (http://www.regione.emilia-romagna.it/)
- Friuli Venezia Giulia (http://www.regione.fvg.it/rafvg/cms/RAFVG/)
- Lazio (http://www.regione.lazio.it/rl_main/)
- Liguria (https://www.regione.liguria.it/)
- Marche (http://www.regione.marche.it/)
- Molise (http://www3.regione.molise.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/1)
- Puglia (http://www.regione.puglia.it/)
- Sardegna (http://www.regione.sardegna.it/)
- Toscana (http://www.regione.toscana.it/)
- Trentino Alto Adige (http://www.regione.taa.it/)
- Trento (http://www.comune.trento.it/)
- Valle d'Aosta (http://www.regione.vda.it/)
- Veneto (http://www.regione.veneto.it/web/guest/home)

Per accedere alle possibilità di fondi e finanziamenti è necessario collegarsi al portale della Regione interessata e controllare la sezione"Avvisi e Bandi" dove sono raccolte le proposte di fondi e finanziamenti disponibili. Nella documentazione di riferimento sono dettagliati i criteri di idoneità ed ammissibilità, le modalità di presentazione delle proposte e le relative tempistiche.

[80] http://www.guidaeuroprogettazione.eu/guida/guida-europrogettazione/fondi-strutturali/programmi-operativi-regionali-por/

13.2 Fondi a gestione indiretta

13.2.1 Horizon 2020 Research and Innovation Framework Programme

Horizon 2020 (H2020)[81] è il programma europeo destinato alla ricerca e all'innovazione nel periodo 2014-2020, dotato di un budget totale di circa 80 miliardi di euro. H2020 persegue gli obiettivi della "Strategia Europa 2020", ovvero una crescita intelligente, inclusiva e sostenibile, volta a incrementare la competitività globale dell'Europa. Lo scopo di H2020 è favorire lo sviluppo della ricerca scientifica di alto livello rimuovendo le barriere all'innovazione ed incoraggiando la costituzione di partnership fra i settori pubblico e privato ed il mondo accademico[82].

Sostenendo la ricerca e l'innovazione, H2020 si struttura su tre priorità:

- eccellenza scientifica (*Excellent Science*), per consolidare ed estendere il sistema di ricerca e innovazione in Europa favorendone la competitività su scala globale, attraverso il rafforzamento dell'Area Europea di Ricerca;
- leadership industriale (*Industrial Leadership*), azioni volte a rafforzare le capacità di sviluppo industriale e di business per le imprese così come le innovazioni ad alto potenziale di sviluppo tecnologico (*Key Enabling Technologies*) e le tecnologie dell'informazione e della comunicazione in generale;
- sfide della società (*Societal Challenges*), come il filone delle "Società sicure", per proteggere la libertà e la sicurezza dell'Europa e dei suoi cittadini.

Durante il periodo 2014-2016, l'Unione Europea ha investito circa 160 milioni di euro in progetti di ricerca e innovazione in materia di cyber security[83] nell'ambito del Programma. Sono stati finanziati in particolare progetti in ambito di Crittografia e Security by Design, iniziative volte ad incorporare la sicurezza tra i requisiti per lo sviluppo delle nuove tecnologie (IoT, 5G, ecc.) e programmi di contrasto al crimine organizzato ed al terrorismo. Per il periodo 2017-2020 sono stati messi a disposizione fino a 450 milioni di Euro dei fondi stanziati per l'intero Programma sui temi di Cyber Security e Privacy[84].

Le attività del programma H2020 e le opportunità di finanziamento sono delineate in programmi di lavoro (*work programme*) pluriennali predisposti dalla Commissione Europea all'interno del quadro legislativo di H2020 e gestiti dalla Direzione Generale per la Ricerca e l'Innovazione. I programmi di lavoro riportano, in allegato, gli obiettivi, le condizioni di partecipazione, i criteri di valutazione e di selezione per i bandi nel periodo di riferimento. Le proposte progettuali devono essere presentate tramite un apposito portale (*Portale dei Partecipanti*), dove gli inviti a presentare proposte (*calls*) sono suddivisi in tematiche più specifiche (*topics*).

La procedura di presentazione della proposta può prevedere una o due fasi. Nel secondo caso i partecipanti devono inviare un primo schema di proposta (generalmente un abstract di 5-6 pagine) che viene valutata da un panel di esperti suddivisi per settore e area di esperienza. Solo in caso di esito positivo, viene richiesto ai partecipanti di inviare una proposta completa.

Il Programma è aperto ad una pluralità di beneficiari, purché attivi nell'ambito della ricerca (in ogni campo), della scienza e dello sviluppo. Generalmente, sono ammesse proposte da organizzazioni avente sede nei paesi membri e nei paesi associati, con un consorzio di almeno tre persone giuridiche. Tra i soggetti ammissibili: enti di ricerca, università, organizzazioni non governative, imprese (incluse PMI). Poiché l'invio delle domande di finanziamento avviene solo attraverso il Portale dei partecipanti, tutti i beneficiari devono registrarsi ed avere un PIC (*Participant Identification Code* – codice identificativo dei partecipanti). Le Agenzie Nazionali, ma anche enti diversi come le

[81] Per ulteriori informazioni consultare i siti: http://ec.europa.eu/programmes/horizon2020/ e http://www.guidaeuroprogettazione.eu/guida/guida-europrogettazione/programmi-comunitari/horizon2020/

[82] A maggio 2018, la Commissione ha rinnovato l'impegno sul fronte Ricerca ed Innovazione lanciando il programma Horizon Europe (2020-2027) che avrà un budget di 114,8 milioni di euro e sarà fondato su tre pilastri, tra cui l'*Open Innovation Pillar* rafforzato dalla nascita del Consiglio Europeo sull'Innovazione (*European Innovation Council*). Inoltre, grazie a questo nuovo programma, ci sarà un incremento fino a 9,2 milioni destinati al Digital Europe Programme (https://ec.europa.eu/commission/sites/beta-political/files/budget-proposals-research-innovation-may2018_en.pdf)

[83] http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

[84] Nell'ambito degli stream "*Secure societies – Protecting freedom and security of Europe and its citizens*" (filoni *Digital Security* e *Fighting crime and terrorism*) e "*Leadership in enabling and industrial technologies*".

Camere di Commercio, possono offrire consulenze e sostegno nella creazione di partenariati e presentazione delle proposte.

Per quanto concerne i finanziamenti, in H2020 è previsto un unico tasso di finanziamento per tutti i beneficiari e tutte le attività: i finanziamenti comunitari coprono fino al 100 % di tutti i costi ammissibili per le azioni di ricerca e innovazione (ovvero per la ricerca ad ampio raggio), mentre il finanziamento copre generalmente il 70 % dei costi ammissibili per le azioni di innovazione (ovvero per la ricerca più vicina al mercato; la quota può raggiungere il 100 % per le organizzazioni senza scopo di lucro). Oltre ai costi diretti ammissibili (rimborsati sulla base della rendicontazione) viene rimborsata una quota fissa aggiuntiva forfettaria di "costi indiretti" (spese generali dell'organizzazione) corrispondente al 25 % dei costi diretti ammissibili.

13.2.2 Programma CEF Telecom

L'Agenzia Esecutiva INEA (*Innovation And Networks Executive Agency*) della Commissione Europea, mediante il Programma CEF Telecom Call[85] (*Connecting Europe Facility*, progetto per lo sviluppo, la costruzione e l'ammodernamento delle reti di telecomunicazione) finanzia progetti di interesse comune che contribuiscono ad aumentare l'interoperabilità, la connessione e lo sviluppo di infrastrutture digitali trans-europee che migliorino la qualità della vita dei cittadini, delle imprese e delle pubbliche amministrazioni, con l'obiettivo di promuovere il Mercato Unico Digitale.

Il Programma CEF Telecom Call fa parte di un set di inviti coordinati che coprono, oltre al settore delle telecomunicazioni, quello dei trasporti (*CEF Transport*) e dell'energia (*CEF Energy*).

La Cyber Security è una delle aree supportate dal Programma, con uno stanziamento allocato nel 2018 di circa 13 milioni di Euro[86], per creare, mantenere o ampliare le capacità nazionali di svolgere una serie di servizi di sicurezza informatica, al fine di consentire agli Stati membri di partecipare in condizioni di parità ai meccanismi di cooperazione.

All'interno dell'area Cyber Security, uno degli obiettivi definiti riguarda iniziative volte lo sviluppo delle capacità dei CSIRT) nazionali designate dagli stati membri dell'Unione Europea in conformità con quanto stabilito dalla Direttiva NIS. In particolare, sono finanziate in tale ambito le proposte finalizzate a rafforzare le competenze e le *capabilities* dei CSIRT governativi e/o settoriali, sia a livello tecnologico che organizzativo (es. le esercitazioni in ambito cyber).

Anche in questo caso le opportunità di finanziamento sono presentate tramite un apposito portale, all'interno del sito della Commissione Europea (sezione *Connecting European Facilities*), e gli inviti sono suddivisi per settore (tra cui quello delle telecomunicazioni) e declinati in base ai singoli obiettivi definiti (*Objectives*). Nei work programme di riferimento sono dettagliati i criteri di idoneità ed ammissibilità, le modalità di presentazione delle proposte e le relative tempistiche.

Con riferimento ai finanziamenti ottenibili, può essere stanziato dalla Commissione un contributo non superiore al 75% dei costi totali presentati per il progetto, che dovranno essere successivamente rendicontati su base periodica.

[85] Ulteriori indicazioni utili sulle modalità con cui presentare le candidature sono illustrate alla pagina: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2018-cyber-security

[86] Nel 2014-2016, l'UE ha investito circa 20 milioni di euro in tali progetti; nel 2017 sono stati stanziati fondi per 12 milioni di euro.

CAPITOLO 14

Ipotesi di piano di attuazione

In questa sezione del documento viene rappresentato un possibile piano di attuazione di un CERT regionale, fornendo indicazione delle fasi da seguire, le macro-azioni necessarie e un'ipotesi di tempistiche. Tale piano è da ritenersi puramente indicativo e basato sull'esperienza pregressa di AGID e sul confronto con analoghe organizzazione. In tal senso, deve essere considerato come un'ipotesi a partire dalla quale costruire un piano di attuazione effettivo basato su una puntuale analisi del contesto in cui agirà il CERT regionale e degli specifici fabbisogni della constituency e degli ulteriori stakeholder.

Pianificazione

Fase 1: Identificazione degli stakeholder e degli attori coinvolti nel piano

- Stabilire quali soggetti/entità devono essere coinvolte nelle diverse fasi di pianificazione, disegno, implementazione ed esercizio
- Identificare la constituency del CERT regionale
- Identificare soggetti/interni ed esterni con cui il CERT dovrà interagire
- Individuare uno sponsor per l'attuazione dell'iniziativa ed ottenerne il supporto

Fase 2: Ottenere la sponsorship dell'iniziativa

- Individuare uno sponsor per l'attuazione dell'iniziativa
- Definire un business case sui benefici derivanti dall'avvio del CERT regionale
- Presentare il business case allo sponsor dell'iniziativa ed ottenerne il supporto

Fase 3: Sviluppare il piano di progetto operativo

- Definire il team di progetto
- Assegnare ruoli e responsabilità
- Definire il macro-piano di progetto
- Definire il piano di progetto di dettaglio, incluso il piano di comunicazione finale

Progettazione

Fase 4: Definizione della constituency

- Raccogliere informazioni sul contesto (operativo, tecnologico, normativo, ecc.) in cui agisce la constituency
- Identificare le aspettative della constituency e degli altri stakeholder
- Definire l'approccio comunicativo verso la constituency
- Determinare la constituency (iniziale) di riferimento per il CERT regionale

Fase 5: Dichiarare la missione del CERT regionale

- Definire la missione del CERT regionale, ovvero la sua funzione di base
- Comunicare la missione alla constituency e al resto della community di riferimento

Fase 6: Determinare il modello finanziario

- Definire il modello dei costi di avvio ed esercizio
- Determinare il modello di finanziamento/ricavo
- Ottenere il finanziamento iniziale

Fase 7: Definizione del catalogo dei servizi

- Identificare quali servizi offrire ai vari componenti della constituency di riferimento (effettuare uno studio di fattibilità iniziale basato su analisi costi/benefici)
- Determinare le modalità di erogazione dei servizi ai membri della constituency
- Definire i livelli di servizio

Fase 8: Definizione del modello organizzativo

- Determinare i livelli di autorità e la struttura di reporting
- Determinare la struttura amministrativa
- Determinare l'assetto organizzativo e il sistema di ruoli e reponsabilità

Fase 9: Definizione dei fabbisogni (personale, tecnologie, facilities)

- Determinare il fabbisogno di risorse:
  - Personale: definire le job description
  - Tecnologie: definire l'infrastruttura di rete ed e le applicazioni a supporto dei servizi
  - Facilities: individuare gli spazi fisici (uffici, data center, ecc.)

Fase 10: Definire il modello di information sharing con la constituency

- Definizione dei livelli di interazione e le interfacce con i diversi membri della constituency e gli altri stakeholder interni/esterni
- Definire i flussi informativi da gestire e i metodi di collaborazione e comunicazione con tutte le parti coinvolte

Fase 11: Definire policy, processi e procedure

- Formalizzare le policy interne al CERT
- Documentare i flussi di lavoro e relativi ruoli e responsabilità
- Formalizzare le procedure operative a supporto dei processi

Fase 12: Definizione dei modelli di valutazione delle prestazioni del CERT

- Individuare metriche per misurare le prestazioni
- Definire i livelli target/obiettivo
- Costruire gli indicatori

- Definire modalità di rilevazione e misurazione

Implementazione

Fase 13: Avviare il processo di acquisizione/potenziamento delle risorse individuate

- Acquisire le risorse identificate
  - Personale: avviare i processi di selezione interni/esterni
  - Tecnologie: acquisire le componenti infrastrutturali e applicative
  - Facilities: installare gli equipaggiamenti presso gli spazi fisici individuati

Fase 14: Rendere operativo il CERT regionale

- Creare operativamente i flussi di lavoro
- Formare il personale
- Implementare gli strumenti tecnologici presso i locali del CERT

Fase 15: Promuovere l'operatività del CERT presso la community

- Attuare il piano di comunicazione per l'avvio del CERT (promozione online, organizzazione di eventi, workshop, ecc.)

CAPITOLO 15

Glossario

15.1 A

Alert Una breve notifica di tipo tecnico, di solito leggibile dall'uomo, relativa a vulnerabilità, exploit e altri problemi di sicurezza correnti. Spesso noto anche avviso, bollettino o nota di vulnerabilità.

APT (Advanced Persistent Threat) Minaccia consistente in un attacco mirato, volto ad installare una serie di malware all'interno delle reti del bersaglio al fine di riuscire a mantenere attivi dei canali che servono a far uscire informazioni di valore dalle reti dell'ente obiettivo.

Audit di sicurezza Riesame di un sistema finalizzato a valutarne il livello di sicurezza. Tipicamente, ci si riferisce con questo termine sia al riesame del codice che dei log di audit.

Autenticazione Garanzia che una caratteristica rivendicata di un'entità sia corretta.

Autorizzazione Processo per determinare, mediante una valutazione dei criteri di controllo sugli accessi applicabili, se un soggetto può ottenere i tipi richiesti di accesso a una particolare risorsa.

15.2 B

Backdoor Letteralmente, «porta posteriore» o «porta di servizio». In informatica indica una procedura o canale di accesso, per lo più nascosto e non noto all'utente, che consente di aggirare in parte o in tutto i meccanismi di sicurezza di un sistema informatico o di un programma per computer.

Backup Copia di file e programmi creata per facilitare il recupero degli stessi se necessario.

Biometria Una tecnica di sicurezza che verifica l'identità di una persona analizzando un attributo fisico univoco, come un'impronta digitale.

Botnet Letteralmente "rete di robot". Indica un insieme di computer o dispositivi che, precedentemente compromessi da parte di un malware, permette a un soggetto terzo di impartire istruzioni da remoto. Una botnet può essere controllata da un malware specializzato, arrivando a manipolare un gran numero di computer o perfino milioni di dispositivi.

Brute force Letteralmente, «attacco a forza bruta». Indica generalmente il metodo utilizzato da un attaccante per individuare una password di accesso ad un sistema provando in maniera esaustiva tutte le possibili combinazioni di caratteri ammesse e tutte le lunghezze di stringa ammesse dal particolare sistema.

Buffer overflow Condizione di errore che si verifica quando in un programma informatico si tenta di immagazzinare un dato in una zona di memoria preallocata (*buffer*), la cui dimensione è inferiore a quella necessaria per ospitare il dato per intero. Ciò comporta la sovrascrittura di parti di memoria circostanti al buffer che sono necessarie all'esecuzione del codice del programma stesso, causando gravi malfunzionamenti che possono anche tradursi in potenziali vulnerabilità di sicurezza.

Business Continuity (o Continuità operativa) Capacità di un'organizzazione di continuare a erogare prodotti o servizi a livelli predefiniti accettabili a seguito di un incidente destabilizzante.

15.3 C

Campagna hacker (o hacking) Accesso intenzionale ad un sistema informatico senza l'autorizzazione dell'utente o del proprietario.

CAPEC (Common Attack Pattern Enumeration and Classification) Dizionario completo dei pattern di attacco noti utilizzati dagli attaccanti per sfruttare le vulnerabilità note nelle funzionalità informatiche.

CED (Centro Elaborazione Dati) Anche indicati con il termine inglese «Data Center», si intende una struttura fisica, normalmente un edificio compartimentato, unitamente a tutti gli impianti elettrici, di condizionamento, di attestazioni di rete, di cablaggi, ecc. e a sistemi di sicurezza fisica e logica, che in tale edificio sono presenti, progettato e allestito per ospitare e gestire un numero elevato di apparecchiature e infrastrutture informatiche e i dati ivi contenuti, allo scopo di garantirne la sicurezza fisica e gestionale.

Cloud computing Modello per abilitare, tramite la rete, l'accesso diffuso, agevole e a richiesta, ad un insieme condiviso e configurabile di risorse di elaborazione (ad esempio reti, server, memoria, applicazioni e servizi) che possono essere acquisite e rilasciate rapidamente e con minimo sforzo di gestione o di interazione con il fornitore di servizi.

Codifica base 64 Sistema di codifica che consente la traduzione di dati binari in stringhe di testo ASCII, rappresentando i dati sulla base di 64 caratteri ASCII diversi.

Community Rete di individui che interagiscono attraverso specifici canali fisici e/o virtuali, potenzialmente superando i confini geografici e politici al fine di perseguire interessi o obiettivi comuni.

Confidenzialità Proprietà di un'informazione di non poter essere resa disponibile o divulgata ad individui, entità o processi non autorizzati.

Constituency Insieme di utenti, clienti ed organizzazioni che costituiscono la comunità di riferimento di un CSIRT/CERT/CIRT.

Controllo / Contromisura Mezzi e modalità per gestire il rischio, comprese politiche, procedure, linee guida, pratiche o strutture organizzative, che possono essere di natura amministrativa, tecnica, gestionale o legale.

Cookie I cookie sono informazioni immesse sul browser quando viene visitato un sito web o utilizzato un social network con un pc, smartphone o tablet. Ogni cookie contiene diversi dati come, ad esempio, il nome del server da cui proviene, un identificatore numerico, ecc. I cookie possono rimanere nel sistema per la durata di una sessione (cioè fino a che non si chiude il browser utilizzato per la navigazione sul web) o per lunghi periodi e possono contenere un codice identificativo unico.

CSIRT/CERT/CIRT/IRT/SERT Con tali termini si indica genericamente un gruppo di gestione degli incidenti di sicurezza informatica, con compiti di prevenzione e coordinamento della risposta ad eventi cibernetici. Il termine CSIRT viene usato prevalentemente in Europa per il termine protetto CERT, che è registrato negli Stati Uniti dal CERT Coordination Center (CERT/CC). A seguire si riportano le varie abbreviazioni usate per lo stesso genere di gruppi: - CERT o CERT/CC (Computer Emergency Response Team / Coordination Center) - CSIRT

(Computer Security Incident Response Team) - IRT (Incident Response Team) - CIRT (Computer Incident Response Team) - SERT (Security Emergency Response Team)

CVE (Common Vulnerabilities and Exposures) Elenco di voci relative a vulnerabilità di sicurezza informatica note pubblicamente, ciascuna contenente un numero di identificazione, una descrizione e almeno un riferimento pubblico.

CWE (Common Weaknesses Enumeration) Elenco sviluppato dalla comunità professionale nel campo della sicurezza sulle tipiche debolezze di sicurezza dei software. Rappresenta un linguaggio comune, un mezzo di confronto per gli strumenti di sicurezza del software e una base per l'identificazione delle debolezze, la loro mitigazione e le azioni di prevenzione.

Cyber Relativo ad un'interazione, più o meno avanzata, tra uomo e computer.

Cyber Event Qualsiasi evento osservabile in un sistema informativo. Gli eventi possono fornire l'indicazione che si sta verificando un incidente cibernetico.

Cyber Incident Azione intrapresa attraverso l'utilizzo di reti informatiche che determina un effetto negativo reale o potenziale su un sistema informativo e/o sulle informazioni che vi risiedono.

Cyber Risk Combinazione della probabilità che si verifichi un evento cibernetico e delle sue conseguenze.

Cyber Security Pratica che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri asset fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space.

Cyber Threat Qualsiasi circostanza o evento potenzialmente in grado di influenzare negativamente le attività di un'organizzazione (incluse la missione, le funzioni, l'immagine o la reputazione), le risorse organizzative, le persone fisiche, altre organizzazioni attraverso l'accesso non autorizzato, la distruzione, la divulgazione o la modifica di informazioni e/o il rifiuto del servizio (DoS) di un sistema di informazioni.

Cyber Threat Intelligence Informazioni sulle minacce che sono state aggregate, trasformate, analizzate, interpretate o arricchite per fornire il contesto necessario a supporto dei processi decisionali.

Cyber warfare Letteralmente "guerra cibernetica", indica l'insieme delle attività di preparazione e conduzione di operazioni di contrasto nello spazio cibernetico. Si può tradurre nell'intercettazione, nell'alterazione e nella distruzione dell'informazione e dei sistemi di comunicazione nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione e contempla diverse tipologie di attacco, quali: attacco a infrastrutture critiche; vandalismo web; intralcio alle apparecchiature; raccolta di informazioni riservate, rendendo possibile lo spionaggio; propaganda di messaggi politici.

15.4 D

Data breach Incidente di sicurezza in cui dati sensibili, riservati, protetti vengono consultati, copiati, trasmessi, rubati o utilizzati da soggetti non autorizzati. Solitamente si realizza attraverso una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezza (come ad esempio il web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a perdita accidentale, furto, infedeltà aziendale, accesso abusivo. Ai sensi del GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

Dati personali Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati sensibili Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DCOM (Distributed Component Object Model) Tecnologia informatica proprietaria di Microsoft che permette di effettuare chiamate di procedure remote attraverso una rete, occupandosi di tutte le mediazioni necessarie, in maniera indipendente dal linguaggio.

Deep/Dark Web Surface web, Deep web e Dark web possono essere definite come tre modalità d'accesso diverse a contenuti online che possono essere sicuri o pericolosi, legali o illegali, morali o immorali. Al primo livello si trova il "surface web" (web in "chiaro»), cui appartengono tutti i siti e in generale gli indirizzi indicizzati dalla maggior parte dei motori di ricerca. Sotto la superfice del "surface web" troviamo il "deep web" ("Invisible Web"), ossia quella parte di WWW non indicizzata dai motori di ricerca, ma accessibile tramite i normali browser a patto di conoscerne l'indirizzo (es. papers accademici e scientifici, documenti legali, cartelle mediche, risorse contenute in database governativi o nei repository di aziende private). Al livello più basso troviamo il «dark web», quella parte del WWW che utilizza le cosiddette reti darknet, ossia reti che si appoggiano all'Internet pubblico, ma che sono accessibili solo tramite particolari software (es. TOR). Il termine "dark" descrive sia le caratteristiche di "non- visibilità" delle informazioni sia il fatto che questo livello della rete è spesso utilizzato per attività criminali, pornografia, traffici illeciti e transazioni illegali.

Defacement Modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne. Questo tipo di attacco, viene eseguito all'insaputa di chi gestisce il sito ed è illegale in tutti i paesi del mondo.

Disaster Recovery Insieme delle misure tecniche e organizzative adottate per assicurare all'organizzazione il funzionamento del centro elaborazione dati e delle procedure e applicazioni informatiche dell'organizzazione stessa, in siti alternativi a quelli primari/di produzione, a fronte di eventi che provochino, o possano provocare, indisponibilità prolungate.

Disponibilità Proprietà di un'informazione di poter essere accessibile e utilizzabile su richiesta da un'entità autorizzata.

DMZ (Demilitarized zone) Letteralmente «zona demilitarizzata», indica una sottorete isolata, fisica o logica, che contiene dei servizi informatici offerti da un'organizzazione, accessibili sia da reti esterne non protette, che da workstation interne alla stessa organizzazione (intranet) e il cui scopo è quello di far usufruire questi servizi nella maniera più sicura possibile, senza compromettere la sicurezza della rete dell'organizzazione.

DNS (Domain Name System) Sistema di denominazione del dominio consistente in un database distribuito che converte in automatico un indirizzo web in un codice numerico di protocollo internet (indirizzo IP) che identifica il server web che ospita il sito.

Domain Name Serie di stringhe separate da punti, che identifica il dominio dell'autonomia amministrativa, dell'autorità o del controllo all'interno di internet. Sono formati dalle regole e dalle procedure del Domain Name System (DNS). Qualsiasi nome registrato nel DNS è un nome di dominio. Essi vengono utilizzati in diversi contesti di rete e in ambito specifico per la denominazione o l'indirizzamento.

DoS (Denial of Service) Malfunzionamento dovuto ad un attacco informatico che causa la saturazione deliberata delle risorse di un sistema informatico, ad esempio un sito web su un web server, fino a renderlo non più in grado di erogare il servizio. Un attacco DoS può essere anche di tipo distribuito (DDoS – Distributed Denial of Service). Il DDoS mantiene gli stessi scopi del DoS, ma in questo caso il traffico che colpisce la vittima proviene da molteplici fonti distribuite anche geograficamente e, per tale motivo, avrà bisogno di un lasso di tempo minore per avere successo.

15.5 E

Escalation Casistiche e modalità con cui, nell'ambito di un'iniziativa, di un progetto o di un processo, vengono trasferite gerarchicamente verso l'alto le responsabilità di una certa decisione.

Esfiltrazione Azione di compromissione di un computer alla ricerca di dati specifici, che abbiano valore per l'attaccante.

Exploit Codice che sfrutta un bug o una vulnerabilità di un codice informatico.

Exploit Letteralmente «sfruttare". Identifica una tipologia di script, virus, worm o binario in grado di sfruttare una specifica vulnerabilità presente in un software o sistema informatico. Di solito un exploit permette l'esecuzione di codice malevolo con lo scopo di far ottenere all'attaccante l'acquisizione dei privilegi amministrativi.

15.6 F

Falso negativo Attacco reale che non genera una segnalazione.

Falso positivo Segnalazioni di anomalie non dovute ad attacchi ma ad effettivi schemi di traffico benigni ma inusuali.

Firewall Un sistema o una combinazione di sistemi che definisce un confine tra due o più reti, formando tipicamente una barriera tra un ambiente sicuro e un ambiente aperto (es. Internet).

15.7 H

Hacker Studioso dei sistemi informatici, che tenta di violare per saggiarne i limiti e la sicurezza senza provocare danni. L'hacker deve essere distinto dal *cracker*, ossia colui che agisce allo scopo di violare sistemi informatici, per acquisire informazioni riservate o per puro vandalismo.

Hash Algoritmo che mappa o traduce un insieme di bit in un altro (generalmente più piccolo) in modo che un messaggio restituisca lo stesso risultato ogni volta che l'algoritmo viene eseguito utilizzando lo stesso messaggio di input.

Hosting Concessione, tipicamente a fronte del pagamento di un canone, di un'infrastruttura formata da server, storage, switch, firewall, ecc. Per poter accedere ai servizi il cliente deve unicamente interfacciarsi con i client all'infrastruttura in hosting. Tutte le attività sistemistiche così come l'assistenza, le metodologie di sicurezza, la protezione e conservazione dei dati, fanno parte integrante del servizio offerto dal fornitore.

Housing Concessione in locazione ad un utente o ad un'organizzazione di uno spazio fisico, generalmente all'interno di appositi armadi detti rack, dove inserire il server, di proprietà del cliente. Tipicamente i server vengono ospitati in Data Center in cui il fornitore garantisce la gestione degli aspetti hardware, software ed infrastrutturali. In pratica, il proprietario della macchina fisica (compreso il relativo storage) trasferisce fisicamente questa presso il fornitore che svolgerà le attività sistemistiche facenti parte del servizio di locazione dell'infrastruttura (il Data Center).

15.8 I

Identificazione Capacità di identificare in modo univoco un utente di un sistema o un'applicazione in esecuzione nel sistema.

Identità digitale Insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore, nell'ambito di un processo di identificazione.

IDS (Intrusion Detection System) Dispositivo software o hardware utilizzato per identificare accessi non autorizzati ai computer o alle reti locali. Tali accessi includono gli attacchi alle reti informatiche tramite lo sfruttamento di servizi vulnerabili, attacchi attraverso l'invio di dati malformati e applicazioni malevole, tentativi di accesso agli host tramite innalzamento illecito dei privilegi degli utenti, accessi non autorizzati a computer e file, e programmi malevoli.

Impersonation Utilizzo di una falsa identità con l'obiettivo di accedere ad aree e informazioni riservate o a sistemi informativi aziendali.

Incident Management Esercizio di un approccio coerente ed efficace alla gestione degli incidenti (di sicurezza delle informazioni)

Incident Management Plan Piano che descrive in dettaglio come un incidente verrà gestito dall'occorrenza al ripristino del normale funzionamento e che fornisce informazioni sulla struttura del team di gestione degli incidenti, i criteri per attivare i processi di continuità operativa e la gestione dell'incidente, i requisiti in termini di risorse, i processi critici e la necessità di eventuali spostamenti necessari del personale.

Incidente Situazione che potrebbe costituire, o potrebbe portare a una interruzione dell'attività, perdita, emergenza o crisi.

Indirizzo IP (Internet Protocol) Etichetta numerica che identifica univocamente un dispositivo (detto host) collegato a una rete informatica che utilizza l'Internet Protocol (IP) come protocollo di rete.

Indirizzo MAC (Media Access Control) Rappresenta l'indirizzo fisico, indirizzo ethernet o indirizzo LAN assegnato in modo univoco dal produttore ad un dispositivo di rete (es. scheda di rete ethernet o wireless) a livello di rete locale.

Information Sharing Scambio di dati, informazioni e/o conoscenza che possono essere utilizzati per gestire i rischi cyber o rispondere agli incidenti informatici.

Infrastruttura critica Infrastruttura, ubicata in uno Stato membro dell'Unione Europea, che è essenziale peril mantenimento delle funzioni vitale della società, della salute, della sicurezza e del benessere economico e sociale della popolazione ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in quello Stato, a causa dell'impossibilità di mantenere tali funzioni.

Integrità Proprietà di un'informazione di essere accurata e completa.

IOA (Indicator of Attack) Evento che potrebbe rivelare un attacco attivo prima che diventino visibili gli IoC. Gli IOA si concentrano sul rilevamento di ciò che un utente malintenzionato sta tentando di realizzare, indipendentemente dal malware o dall'exploit utilizzato in un attacco.

IOC (Indicator of Compromise) Artefatto osservato in una rete o all'interno di un sistema che con un'alta probabilità è correlabile, o indica, un'intrusione. Tipici IOC sono le firme antivirus, un Indirizzo IP[87], un hash MD5[88] con cui si identifica univocamente un file malevolo, una URL[89] e/o un nome di dominio[90] da cui è stato veicolato un attacco o verso cui un malware[91] si connette una volta attivato.

15.9 K

Keylogger Strumento (hardware o, più diffusamente, software) che realizza uno sniffing monitorando e/o registrando quello che un utente digita sulla tastiera del computer. Può essere utilizzato per l'assistenza tecnica o come malware per sottrarre credenziali di accesso, numeri di carte di credito o altri dati sensibili.

15.10 L

Livelli di servizio Livelli che caratterizzano le attività di forniture nei contratti e/o negli accordi di servizio, e che consentono di misurare il raggiungimento degli obiettivi concordati tra Fornitore e committente

[87] https://it.wikipedia.org/wiki/Indirizzo_IP
[88] https://it.wikipedia.org/wiki/MD5
[89] https://it.wikipedia.org/wiki/URL
[90] https://it.wikipedia.org/wiki/Nome_di_dominio
[91] https://it.wikipedia.org/wiki/Malware

Log Registrazione dei dettagli di informazioni o eventi in un sistema di conservazione organizzato (registro), solitamente sequenziati nell'ordine in cui si sono verificati.

15.11 M

Malspam (Malware Spam) Identifica il malware che viene fornito tramite messaggi di posta elettronica.

Malware In italiano «codice malevolo», è un software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole malicious e software e significa "programma malvagio" e comprende adware, bot, keylogger, spyware, trojan, virus e worm.

MD5 Funzione hash crittografica unidirezionale che prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit.

Minimo Privilegio Principio generale sviluppato nella gestione dei sistemi di sicurezza secondo il quale un processo, un programma o un utente abbia visibilità delle sole risorse/informazioni immediatamente necessarie al suo funzionamento.

MiTM (Man in The Middle) È una tipologia di attacco informatico in cui l'attaccante si introduce nella comunicazione tra la vittima e il server con il quale quest'ultima sta cercando di dialogare. Lo scopo è quello di carpire o alterare le informazioni trasmesse.

Modello di maturità In ambito cyber, è una misura della capacità di un'organizzazione di migliorare continuamente il suo approccio alla cyber security. Maggiore è la maturità, maggiori saranno le probabilità che incidenti o errori porteranno a miglioramenti nella qualità o nell'uso delle risorse implementate dall'organizzazione. I modelli di maturità cyber valutano qualitativamente persone, processi, strutture e tecnologie riguardanti la cyber security.

Monitoring Insieme delle regole che definiscono le modalità in cui le informazioni sull'uso di computer, reti, applicazioni e informazioni sono raccolte ed interpretate.

15.12 N

NAT (Network Address Translation) Metodologia per modificare gli indirizzi IP contenuti negli header dei pacchetti in transito su un sistema che agisce da router all'interno di una comunicazione tra due o più host.

Need to know Principio generale sviluppato nella gestione dei sistemi di sicurezza secondo il quale i soggetti che devono compiere attività di trattamento di informazioni sono autorizzati a trattare i soli dati essenziali allo svolgimento del mansionario loro attribuito

NTLM (NT LAN Manager) Protocollo di autenticazione NTLM utilizzato su diverse reti Microsoft, che consente di impostare la periferica in modo che un utente possa effettuare l'autenticazione tramite il pannello di controllo con le proprie credenziali di rete Microsoft.

15.13 O

OLE (Object Linking and Embedding) Tecnologia di transclusione per la creazione di documenti composti (*compound document*) sviluppata da Microsoft.

One-time password Password valida solo per una singola sessione di accesso o una transazione

OSINT/CLOSINT Con il termine OSINT, acronimo di Open Source Intelligence, si fa riferimento al processo di raccolta d'informazioni attraverso la consultazione di fonti di pubblico dominio definite anche "fonti aperte". Fare OSINT significa descrivere l'informazione disponibile e aperta al pubblico (mezzi di comunicazione, motori di ricerca, social network, forum, blog, ecc.), attraverso un processo di ricerca, selezione, vaglio e reportizzazione verso uno specifico destinatario al fine di soddisfare una necessità informativa. Si distingue dalla semplice ricerca d'informazioni perché applica un processo di gestione delle informazioni con lo scopo di creare una specifica conoscenza in un determinato ambito/contesto. Con il termine CLOSINT si fa invece riferimento alla Close Source Intelligence, cioè al processo di raccolta d'informazioni attraverso consultazione di "fonti chiuse", non accessibili al pubblico.

15.14 P

Pacchetto di rete Indica ciascuna sequenza finita e distinta di dati trasmessa su una rete o in generale su un canale o linea di comunicazione che utilizzi il modo di trasferimento a commutazione di pacchetto. Le reti che utilizzano tale modalità di trasmissione sono dette reti di trasmissione a pacchetto. Tipicamente un pacchetto si compone delle seguenti tre parti: i) header (intestazione): contiene tutte le informazioni di overhead necessarie alla trasmissione, quali l'indirizzo del trasmettitore, quello del ricevitore, la vita del pacchetto, i dati che riguardano l'assemblaggio con gli altri pacchetti e così via; ii) data: contiene i dati utili trasmessi; iii) checksum: un codice di controllo utilizzato per controllare la corretta ricezione dei dati ovvero l'eventuale presenza di errori.

Password Stringa di caratteri protetta, generalmente cifrata, che autentica un utente su un sistema informatico.

Patch Porzione di software progettata per risolvere/correggere errori di programmazione e vulnerabilità.

Payload Sezione del software (malevolo) contenente il codice e/o i dati dannosi.

PE (Portable Executable) Formato di file per file eseguibili, file oggetto, librerie condivise e device drivers, usato nelle versioni a 32-bit e 64-bit del sistema operativo Microsoft Windows. Il termine «portable» si riferisce alla versatilità del formato per numerose architetture differenti. Il formato PE è praticamente una struttura dati che incapsula le informazioni necessarie al loader di Windows per gestire il codice eseguibile.

Penetration Test Processo operativo di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato. L'analisi comprende più fasi ed ha come obiettivo evidenziare le debolezze del sistema, sfruttando le vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere indebitamente allo stesso.

Phishing Frode informatica, realizzata attraverso l'invio di e-mail contraffatte, finalizzata all'acquisizione, per scopi illegali, di dati riservati oppure a far compiere alla vittima determinate operazioni/azioni. I malintenzionati che si avvalgono delle tecniche di phishing usano tecniche di social engineering, attraverso le quali vengono studiate ed analizzate le abitudini delle persone, cioè delle potenziali vittime, al fine di carpirne potenziali informazioni utili.

Policy Intenzioni e direzione di un'organizzazione, come espresse formalmente dalla direzione.

Porta di rete Porta virtuale o logica che identifica e discrimina il traffico dati di una connessione da quello di un'altra in una rete.

Privacy Diritto alla riservatezza delle informazioni personali e della propria vita privata, cioè strumento posto a salvaguardia e a tutela della sfera privata del singolo individuo, da intendere come la facoltà di impedire che le informazioni riguardanti tale sfera personale siano divulgate in assenza dell'autorizzazione dell'interessato, od anche il diritto alla non intromissione nella sfera privata da parte di terzi.

Privilege escalation Sfruttamento di una vulnerabilità, di un errore di progettazione o di configurazione di un software applicativo e/o sistema operativo al fine di acquisire il controllo delle risorse della macchina normalmente precluse.

15.15 R

Ransomware Malware che limita l'accesso al sistema informatico infettato e richiede il pagamento di un riscatto per la rimozione del blocco. Alcune forme di questo malware crittografano i file sul disco del sistema mentre altre bloccano il sistema visualizzando messaggi che inducono l'utente a pagare.

RAT (Remote Access Trojan) Malware che contiene una backdoor che consente ad un utente non autorizzato il controllo amministrativo da remoto del computer su cui è installato. I RAT vengono generalmente scaricati da Internet e installati all'insaputa dell'utente, ad esempio mascherati come un'applicazione apparentemente innocua, come un gioco o un'utility, o inviati come allegati ad Email malevole. Una volta che il sistema è compromesso, il RAT fornisce una porta attraverso la quale un'attaccante può inviare comandi al malware. Poiché un RAT viene eseguito con i privilegi di amministratore, chi lo controlla può compiere qualsiasi tipo di azione malevola.

RBAC (Role-Based Access Control) Letteralmente "*controllo degli accessi basato sui ruoli*", indica una tecnica di accesso a sistemi ristretto per utenti autorizzati. Si basa sui concetti di ruolo e privilegio e sulle seguenti regole: i) Assegnazione dei ruoli: un soggetto può eseguire una transazione solo se il soggetto ha selezionato o è stato assegnato ad un ruolo; ii) Autorizzazione dei ruoli: un ruolo attivo per un soggetto deve essere stato autorizzato per il soggetto; iii) Autorizzazione alla transazione: un soggetto può eseguire una transazione solo se la transazione è autorizzata per il ruolo attivo del soggetto.

Registro (*in ambiente Windows*) Il registro nei sistemi operativi Windows in cui risiedono le impostazioni a livello centrale e informazioni necessarie per eseguire le operazioni.

Reverse engineering Analisi volta a comprendere i lfunzionamento di prodotti hardware e software al fine di reingegnerizzarli, ad esempio, per migliorarne il funzionamento o per impiegarli per fini diversi e ulteriori rispetto a quelli originari.

Rischio Effetto dell'incertezza sugli obiettivi.

Risk appetite La quantità e il tipo di rischio che un'organizzazione è disposta ad assumere per raggiungere i propri obiettivi strategici.

Rootkit Software creato per prendere il controllo di un sistema senza bisogno di autorizzazione da parte di un utente o di un amministratore.

15.16 S

Sessione Una sessione è una connessione virtuale tra due host tramite cui viene trasmesso il traffico di rete.

SHA (Secure Hash Algorithm) Famiglia di diverse funzioni crittografiche di hash sviluppate a partire dal 1993 dalla National Security Agency (NSA) e pubblicate dal NIST come standard federale dal governo degli USA (FIPS PUB 180-4). Come ogni algoritmo di hash, l'SHA produce un message digest, o «impronta del messaggio», di lunghezza fissa partendo da un messaggio di lunghezza variabile. La sicurezza di un algoritmo di hash risiede nel fatto che la funzione non sia reversibile (non sia cioè possibile risalire al messaggio originale conoscendo solo questo dato) e che non deve essere mai possibile creare intenzionalmente due messaggi diversi con lo stesso digest. Gli algoritmi della famiglia sono denominati SHA-1, SHA-224, SHA-256, SHA-384 e SHA-512. SHA-1, il più diffuso ma ritenuto oggi poco sicuro, produce un digest del messaggio di soli 160 bit, mentre gli altri producono digest di lunghezza in bit pari al numero indicato nella loro sigla (SHA-256 produce un digest di 256 bit).

SIEM (Security information and event management) Tecnologia che supporta il rilevamento di minacce e la risposta agli incidenti di sicurezza, attraverso la raccolta in tempo reale, l'analisi storica e la correlazione delle informazioni su eventi di sicurezza da un'ampia varietà di fonti dati.

Sinkhole Server verso il quale viene reindirizzato traffico potenzialmente malevolo, impedendo che raggiunga la sua destinazione originaria (tecnica del «*sinkholing*»). Più comunemente, la tecnica di sinkholing viene utilizzata

dai ricercatori di sicurezza per reindirizzare il traffico di una botnet verso macchine specifiche allo scopo di acquisire dati utili alla loro analisi e contrasto.

Sistema Informativo Insieme di applicazioni, servizi, risorse informatiche o altri componenti di gestione delle informazioni.

SLA (Service Level Agreement) Accordo documentato tra il fornitore del servizio e il cliente che identifica i servizi e i traguardi per il servizio.

Sniffer Software che osserva e registra il traffico di rete.

Social engineering Letteralmente indica lo studio del comportamento di un individuo con l'obiettivo finale di ricavarne informazioni utili per perpetrare un successivo attacco nei suoi confronti.

Spam Invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati (generalmente commerciali o offensivi), e noto anche come posta spazzatura (in inglese «*junk mail*»). Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board, forum, Facebook e altri servizi di rete sociale.

Spear phishing Indica un tipo particolare di phishing realizzato mediante l'invio di Email fraudolente ad una specifica organizzazione o persona. Lo scopo di questi attacchi è tipicamente quello di ottenere accesso ad informazioni riservate di tipo finanziario, a segreti industriali, di stato o militari.

Spoofing Tipologia di attacco informatico comunemente utilizzata insieme al Social Engineering per falsificare l'identità di un utente, di un dispositivo all'interno di una rete, il mittente di un messaggio di posta elettronica o un certificato.

SQL injection Vulnerabilità che permette a terzi di alterare le basi dati utilizzate da un sito web.

15.17 T

Ticket Richiesta di assistenza, tracciata da un sistema informatico di gestione durante l'intero ciclo di risoluzione.

TLP (Traffic Light Protocol) Protocollo utilizzato per lo scambio di informazioni al fine di garantire la diffusione delle stesse in modo controllato. Sono definiti quattro livelli di criticità crescenti associati a diversi *tag* cromatici: bianco, verde, ambra, rosso (in ordine di crescente criticità).

Triage Il triage (o categorizzazione) è un elemento essenziale di qualunque funzione di gestione degli incidenti, in particolare per qualsiasi CSIRT costituito. Il triage si inserisce nel percorso critico per comprendere cosa viene segnalato attraverso tutta l'organizzazione. Esso funge da veicolo tramite il quale tutte le informazioni confluiscono verso un unico punto di contatto, rendendo possibile una visione aziendale dell'attività in corso e una correlazione completa di tutti i dati segnalati. Il triage consente una valutazione iniziale di un rapporto in entrata, aiutando ad individuare i problemi potenziali di sicurezza e a stabilire le priorità nel carico di lavoro.

Trojan (horse) Particolare categoria di malware le cui funzionalità sono nascoste all'interno di un software apparentemente legittimo facendo sì che l'installazione avvenga in modo inconsapevole da parte dell'utente permettendo in questo modo il controllo da remoto del computer. A causa della specifica modalità di contagio, il malware non è in grado di diffondersi in modo autonomo.

15.18 U

URL (Uniform Resource Locator) La stringa di caratteri che forma un indirizzo web.

15.19 V

Virus Particolare malware che, se legato ad un eseguibile, è in grado di riprodursi e propagarsi autonomamente allo scopo di infettare file, programmi e computer. Alcuni particolari virus sono in grado di danneggiare, oltre ai dati, anche i componenti hardware del computer.

VPN (Virtual Private Network) Rete privata protetta che utilizza l'infrastruttura di telecomunicazioni pubblica per trasmettere dati.

Vulnerability Una debolezza, suscettibilità o difetto di un asset o controllo che può essere sfruttato da una o più minacce.

Vulnerability Assessment Insieme di attività volte ad identificare, e successivamente correggere, le vulnerabilità presenti sui sistemi prima che vengano rilasciati in esercizio oppure controllare con continuità quelle presenti su sistemi già rilasciati.

15.20 W

Worm Particolare categoria di malware capace di autoreplicarsi ma che, a differenza di un virus, non ha bisogno di legarsi ad un eseguibile per diffondersi in quanto modifica direttamente il sistema operativo del computer che lo ospita ed utilizza le connessioni internet.

15.21 X

XSS (Cross Site Scripting) Vulnerabilità che permette a terzi di alterare le funzionalità di un sito web.

15.22 Z

Zero-day (vulnerabilità o attacco zero-day) Indica qualsiasi vulnerabilità di sicurezza informatica non pubblicamente nota e definisce anche il programma - detto "exploit" - che sfrutta questa vulnerabilità per eseguire azioni non normalmente permesse nel sistema in questione. Vengono chiamati zero-day proprio perché lo sviluppatore ha "zero giorni" per riparare la falla nel programma prima che qualcuno la possa sfruttare. Nel momento in cui il bug viene risolto, lo zero-day perde la sua importanza perché non può più essere usato contro quel sistema.

Zombie (computer) Computer contenente software nascosto che consente di controllare la macchina da remoto, in genere per eseguire un attacco su un altro computer.

Le definizioni precedentemente fornite sono state individuate a partire dall'analisi delle seguenti fonti:

- AGID, Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni
- AGID, Linee Guida per la razionalizzazione dei CED delle Pubbliche Amministrazioni
- AGID, Linee Guida sulla qualità dei beni e dei servizi ICT per la definizione ed il governo dei contratti della Pubblica Amministrazione
- Codice in materia di protezione dei dati personali (Codice «Privacy»)
- Codice in materia di protezione dei dati personali (Codice «Privacy»), Allegato «B»
- Cyber Security Report La Sapienza
- ENISA, Un approccio graduale alla creazione di un CSIRT, Documento WP2006/5.1(CERT-D1/D2)
- FIRST

- Garante per la protezione dei dati personali
- Glossario CERT-Nazionale
- Glossario CERT-PA
- Glossario ENISA
- Glossario OWASP
- ISACA, Cybersecurity Fundamentals Glossary
- ISO 22300:2012, Security and resilience – Vocabulary
- ISO 31000:2018, Risk management – Guidelines
- ISO/IEC 20000-1:2011, Part 1: Service management system requirements
- ISO/IEC 27000:2018, Information security management systems – Overview and vocabulary
- ISO/IEC 27032:2012, Guidelines for cybersecurity
- ISO/IEC 27035-1:2016, Information security incident management – Part 1: Principles of incident management
- NIST SP 800-145, The NIST Definition of Cloud Computing
- NIST SP 800-150, Guide to cyber threat information sharing
- NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems
- NISTIR 7298 Revision 2, Glossary of Key Information Security Terms
- Quadro strategico nazionale per la sicurezza dello spazio cibernetico
- Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR)
- SANS Glossary of Security Terms
- The Institute of Risk Management
- The MITRE Corporation
- US Department of Homeland Security, NICCS - National Initiative for Cybersecurity Careers and Studies

Indice