Manifesto

Comitato CISO Cloud
di
CSA Italy

CSA Italy
Via Cesare Beruto 11
20131 Milano
C.F. 97673120586

www.cloudsecurityalliance.it

PREMESSA

In una società ed economia che gestisce ormai costantemente informazioni "fluide", ovvero digitali, la cyber security sta diventando uno dei più importanti fattori di successo, o insuccesso, per un'azienda. Tra le preoccupazioni dei CEO diventa estremamente importante la protezione delle informazioni strategiche e in generale confidenziali, oltre che personali, e la necessità di non essere influenzati nelle decisioni importanti dalla paura di perdere il controllo dell'informazione, in particolare verso la concorrenza (pensiamo, ad es., ad informazioni su offerte commerciali, Merge & Acquisition, Proprietà Intellettuale, ecc.). I CEO manifestano quindi sempre più la necessità di avere un referente specifico "executive" che possa costantemente assicurarli sulla capacità di gestire la cyber e information security in azienda in modalità trasversale in tutte le attività essenziali (Marketing e Vendite, Ricerca e Sviluppo, Produzione, Risorse Umane, Information Technology, …), in particolare verso potenziali minacce informatiche che possono mettere rapidamente in crisi il proprio business (fino al completo blocco), soprattutto se l'azienda è quotata in borsa (quindi più esposta al rischio di reputazione verso i propri azionisti e clienti).

Il CISO è la figura manageriale emergente nell'ambito delle organizzazioni aziendali che hanno elevato la loro attenzione sui temi della cyber e information security e diviene quindi la naturale risposta alle esigenze dei CEO di avere un punto di contatto unico. Negli ultimi due anni le aziende stanno affrontando da un lato i problemi dell'aumento delle minacce cyber e relativi attacchi ai sistemi informativi da parte della criminalità informatica e dall'altro l'esigenza di conformità a leggi e norme di settore; in quest'ultimo caso alcuni esempi sono il Regolamento Generale per la Protezione dei Dati o GDPR, la Direttiva NIS, il Cybersecurity Act (Regolamento EU n. 881/2019), il Perimetro di Sicurezza Nazionale Cibernetica (Legge 133/2019), le misure minime di sicurezza per la PA di AGID, ed altre normative cyber security nazionali emesse dalle rispettive Agenzie di Sicurezza Informatica Nazionali (ad es. il National Cybersecurity Agency o ANSSI in Francia, la Federal Office for Information Security o BSI in Germania), o similari (ad es. National Cyber Security Center in UK).

Il CISO è pertanto la risposta ad una richiesta aziendale di un forte coordinamento delle attività afferenti alla sicurezza delle informazioni, reti e sistemi sia sul fronte tecnico, sia organizzativo e compliance. Tra i principali compiti citiamo:

- la gestione del sistema di sicurezza delle informazioni (con riferimento alla famiglia di norme ISO/IEC 27000 ed altri controlli specifici di settore e tecnologie) e la correlazione/integrazione con altri sistemi di gestione e norme (Business Continuity, ecc.);
- la definizione e monitoraggio dei requisiti cyber security per i progetti e processi aziendali, in particolare quelli core/critici;
- il monitoraggio (audit) della postura di sicurezza informatica aziendale;
- il coordinamento degli interventi a fronte di incidenti informatici (attraverso i Computer Emergency Response Team – CERT o Computer Security Incident Response Team – CSIRT);
- la definizione di strategie specifiche a supporto del business, della comunicazione e consulenza verso il top management.
- Il supporto nella valutazione dei rischi cyber (e privacy, in supporto al DPO) delle tecnologie e paradigmi emergenti (Cloud Computing, IoT, Machine Learning e Artificial Intelligence).

SCOPO

- Il **Comitato CISO Cloud** (di seguito "CCC") è un tavolo permanente di discussione e condivisione di informazioni ed esperienze dell'associazione no-profit CSA Italy che ha lo scopo di promuovere e perseguire gli obiettivi dell'associazione attraverso lo svolgimento delle seguenti attività:

    1. Promuovere e valorizzare la figura del CISO attraverso diverse iniziative quali: profilazione del ruolo, definizione del percorso formativo (in particolare in

ambito Cloud Security), analisi della sua collocazione nelle organizzazioni aziendali e relativo percorso di crescita, docenze in corsi/master e seminari.

2. approfondire temi inerenti alle ricerche in ambito cloud security effettuate da CSA (ad oggi sono attivi più di 30 gruppi di lavoro a livello internazionale con decine di pubblicazioni per anno),
3. condividere esperienze in ambito cloud security proposte dai singoli CISO,
4. partecipare a tavole rotonde, in presenza o virtuali, nell'ambito di eventi organizzati da CSA (in particolare in Italia ed EMEA),
5. effettuare peer-review su studi prodotti dai gruppi di lavoro CSA Italy.

MEMBRI

- I componenti del CCC vengono scelti e nominati dal Consiglio Direttivo di CSA Italy nell'ambito della categoria professionale dei CISO (Chief Information Security Officer) o equivalenti nei casi in cui questo ruolo sia assimilato in altre cariche apicali quali CIO, CTO ecc. di Enti, Aziende, Associazioni.
- I membri del CCC non possono far parte di Gruppi di Lavoro di CSA Italy o di altre iniziative di ricerca in cui CSA Italy collabora.
- I nomi dei membri del CCC possono apparire nelle comunicazioni istituzionali di CSA Italy (ad es. sito web, presentazioni ecc.).

IMPEGNO

- La qualifica di membro del CCC è a titolo gratuito, ha una durata di un anno solare ed è rinnovabile.
- La partecipazione alle attività del CCC è a titolo personale e viene concordata in tempi e modalità con il Consiglio Direttivo di CSA Italy.

- Tutti i membri del CCC hanno l'obbligo di rispettare il CSA CHAPTER CODE OF ETHICS[1].
- Accordo di Riservatezza - Tutti i membri del CCC si obbligano reciprocamente e garantiscono al Consiglio Direttivo di CSA Italy:
    a. di mantenere riservato qualsiasi tipo di informazione relativo alle reciproche attività e/o alle modalità di lavoro e/o alle soluzioni adottate di cui siano venute a conoscenza in dipendenza delle attività del CCC;
    b. di non divulgare o mettere a disposizione di terze parti, direttamente o indirettamente, le informazioni acquisite nelle attività del CCC senza il consenso degli altri membri del CCC e del Consiglio Direttivo di CSA Italy;
    c. di non utilizzare le informazioni acquisite nelle attività del CCC in alcun modo o per qualsivoglia fine ad eccezione di quanto necessario per eseguire le attività del CCC;
    d. di adottare le misure coerenti con la tutela delle informazioni confidenziali per quanto acquisito nelle attività del CCC per impedire la loro divulgazione o l'accesso non autorizzati.

NOTE FINALI

- Per la risoluzione di questioni riguardanti il CCC il Consiglio Direttivo di CSA Italy decide insindacabilmente, nello spirito dello Statuto associativo.
- Questo manifesto potrà, in qualsiasi momento, essere modificato dal Consiglio Direttivo di CSA Italy previa comunicazione ai membri del CCC.

[1] https://cloudsecurityalliance.it/wp-content/uploads/2020/09/Code-of-Ethics.pdf