ALLEGATO E

Istituzione del Computer Security Incident Response Team (CSIRT) di Regione Lombardia

Regione Lombardia istituisce il Computer Security Incident Response Team (CSIRT) quale ambito organizzativo (Nucleo) all'interno della Regione stessa, con lo scopo di innalzare il livello di maturità e protezione cyber dei membri della propria Constituency. Oltre a prevenire, rilevare e rispondere agli incidenti di sicurezza informatica, il CSIRT di Regione Lombardia mira a diffondere l'adozione di pratiche consolidate e standard di sicurezza comuni a beneficio di un'azione sinergica in risposta ad uno scenario di minacce cibernetiche in continua evoluzione.

Il CSIRT di Regione Lombardia è integrato nella rete nazionale dei CSIRT, sotto il coordinamento del CSIRT Italia, operante presso l'Agenzia per la Cybersicurezza Nazionale.

La Giunta ha il compito di delineare e governare le strategie per lo sviluppo del CSIRT, di gestire le relazioni con i membri della Constituency e verificare che le attività del CSIRT siano conformi alle migliori pratiche e agli standard di settore.

La Giunta, inoltre, aggiorna il modello organizzativo del CSIRT, monitorandone l'aderenza rispetto agli obiettivi stabiliti dalla Giunta e valutando eventuali proposte di miglioramento.

Constituency

La Constituency del CSIRT di Regione Lombardia comprende attualmente:

- tutti i dipendenti e il patrimonio di Regione Lombardia;
- gli enti locali e sanitari che ne hanno fatto richiesta;
- le istituzioni lombarde che utilizzano i servizi centralizzati forniti da ARIA S.p.A. in qualità di società in house di Regione Lombardia.

La Constituency del CSIRT potrà essere ampliata nel corso del tempo sulla base delle necessità che potrebbero sorgere dal territorio - in termini di prevenzione e protezione cyber - oltre che sulla base degli obiettivi strategici di Regione Lombardia, secondo le modalità di ingaggio e di adesione che saranno definite.

Servizi erogati

I servizi del CSIRT sono erogati attraverso un presidio 5/7giorni e 8/24H, con reperibilità nei giorni festivi e negli altri orari, in caso di incidenti critici.

All'interno del Catalogo Servizi del CSIRT, questi sono suddivisi e classificati con riferimento ai seguenti ambiti operativi:

- Info Security Event Management: monitoraggio e gestione degli eventi di sicurezza relativamente la correlazione e l'analisi degli eventi rilevati dalle sorgenti di dati al fine di identificare potenziali incidenti;
- Info Security Incident Management: gestione degli incidenti di sicurezza relativamente l'analisi, la classificazione e la segnalazione, nonché attività di supporto e indirizzamento degli interventi di contenimento, mitigazione e risoluzione;
- Vulnerability Management: identificazione proattiva e/o reattiva, segnalazione e gestione delle vulnerabilità e delle minacce di sicurezza;

- Situational Awareness: progettazione, configurazione e mantenimento dell'infrastruttura interna di sicurezza per la corretta acquisizione e aggregazione dei dati, in considerazione delle informazioni relative a evoluzioni tecnologiche e scenari internazionali raccolti mediante attività di info sharing;

- Knowledge Transfer: attività erogate per innalzare il livello di sicurezza generale dell'organizzazione e delle persone in termini di awareness e formazione.

Ciascuno dei servizi presenti a Catalogo viene erogato ai membri della constituency sulla base delle esigenze di ciascuno e delle strategie attuate da Regione Lombardia.

Modello Organizzativo

Per svolgere le attività sopra descritte viene costituito il Nucleo CSIRT, organizzato come nel seguito indicato.

Il Direttore della Direzione competente in materia di cybersicurezza è il Responsabile e rappresentante del CSIRT regionale. Esso è chiamato a supervisionare i processi e assicurare l'aderenza delle attività agli obiettivi strategici delineati da Regione.

Nello svolgimento delle sue attività, il Responsabile del CSIRT è coadiuvato dai:
- "Coordinatore CSIRT ambito Sistema Informativo Regionale (Coordinatore CSIRT SIRE)" individuato nel dirigente responsabile della UO Sistemi informativi regionali e Cybersecurity
- "Coordinatore CSIRT ambito Sistema Informativo Socio Sanitario (Coordinatore CSIRT SISS)" individuato nel dirigente responsabile della UO Sistemi informativi e Sanità digitale;

Nello specifico, afferiscono al Responsabile del CSIRT:

- la rappresentanza del CSIRT nelle relazioni istituzionali fungendo da punto di contatto ufficiale per le questioni di sicurezza informatica all'interno e all'esterno di Regione;
- l'approvazione le strategie del CSIRT in accordo ai piani di sicurezza di Regione, anche analizzando e validando le proposte di miglioramento presentate dai Coordinatori CSIRT SIRE e SISS;
- la responsabilità organizzativa del CSIRT assicurandosi che la struttura e i servizi di sicurezza del CSIRT siano progettati in modo da rispondere efficacemente agli obiettivi strategici definiti dalla Giunta;
- la definizione in sede di bilancio della proposta di budget complessivo necessario a garantire l'operatività del CSIRT ed eventuali investimenti volti al continuo miglioramento.

Al "Coordinatori CSIRT" e ciascuno per l'area di propria competenza, è affidato:
- il coordinamento, ciascuno nel proprio ambito, delle iniziative operative in raccordo con gli altri membri della constituency del proprio ambito;
- la valutazione periodica degli eventi registrati e l'individuazione di azioni di mitigazione del rischio con ARIA spa e gli Enti coinvolti;
- il monitoraggio delle performance dei servizi erogati dal CSIRT, ciascuno rispetto ai membri della constituency di proprio interesse per area di competenza;
- la partecipazione, in raccordo con il Responsabile del CSIRT e ARIA spa, nella gestione di incidenti critici con particolare riguardo alla gestione dei rapporti sia interni che esterni a Regione;
- la predisposizione per la propria area di competenza, della proposta di budget per le attività del CSIRT da sottoporre annualmente al Responsabile del CSIRT.

Il CSIRT regionale opera in stretto raccordo e coordinamento coi referenti sulla cybersicurezza identificati attraverso l'art. 8 della legge 90/2024.

ARIA S.p.A., in qualità di centrale di committenza, garantisce l'acquisizione e il coordinamento dei servizi necessari all'operatività del CSIRT di Regione Lombardia, nonché l'erogazione dei servizi e le capacità di

prevenzione e protezione dagli attacchi informatici attraverso l'esperimento di procedure di gara comprese nelle deliberazioni di programmazione degli acquisti e la relativa gestione dei contratti per i servizi e le forniture.

L'operativa erogazione dei servizi viene svolta da ARIA S.p.A. che reperisce e coordina le risorse necessarie sotto il governo e la supervisione di Regione.

ARIA S.p.A. è, quindi, responsabile della gestione operativa del CSIRT. Tra i suoi compiti rientrano la progettazione, configurazione e gestione dell'infrastruttura di sicurezza interna, il monitoraggio costante degli eventi di sicurezza, la segnalazione tempestiva di incidenti e l'assistenza nella gestione di eventuali minacce alla sicurezza informatica, oltre che lo svolgimento di attività specifiche volte ad innalzare il livello di protezione informatica.
Le responsabilità in carico di ARIA S.p.A. includono:

- la gestione operativa e l'erogazione dei servizi di sicurezza informatica;
- il supporto a Regione nella valutazione dello scenario cyber, per individuare strategie di protezione e servizi sempre in linea all'evoluzione tecnologica;
- l'adozione di modelli e processi in linea a best practice e standard di settore quali le "Linee guida per la realizzazione di CSIRT" pubblicate dall'Agenzia per la cybersicurezza nazionale;
- la valutazione della maturità del CSIRT sulla base di modelli di settore (es. framework SIM3) e la garanzia del rispetto del livello target definito da Regione;
- il supporto ai membri della constituency del CSIRT nella prevenzione, risposta e gestione degli incidenti di sicurezza;
- il mantenimento e l'aggiornamento delle tecnologie a supporto dell'erogazione dei servizi del CSIRT;
- la formazione e l'aggiornamento continuo del personale del CSIRT.

Al Chief Information Security Officer di ARIA S.p.A. è affidato il ruolo di responsabile operativo del CSIRT. Esso gestisce le attività operative assicurando che le procedure di prevenzione e risposta agli incidenti di sicurezza informatica siano eseguite efficacemente e in conformità con le politiche stabilite.

Rientrano tra i suoi compiti:

- la rilevazione continua dei fenomeni e la tempestiva comunicazione dei possibili incidenti ai referenti dei membri della constituency coinvolti;
- il supporto nella gestione degli incidenti di sicurezza, con particolare riferimento alla gestione delle comunicazioni con i membri della constituency interessati e Regione;
- la verifica che le tecnologie e le procedure utilizzate dal CSIRT siano sempre aggiornate e all'avanguardia per garantire la massima efficacia nell'erogazione dei servizi;
- la partecipazione a momenti periodici di allineamento con Regione Lombardia a garanzia di un costante allineamento tra le parti;
- la gestione delle risorse a disposizione del CSIRT.

Ambienti operativi dedicati e strumenti necessari per le attività del CSIRT in Regione

Regione mette a disposizione uno spazio dedicato al lavoro degli analisti del CSIRT all'interno di una propria sede. Questo spazio è attrezzato con l'equipaggiamento essenziale per fornire i servizi e per le operazioni quotidiane, soddisfacendo i requisiti minimi per il lavoro di un numero limitato di risorse.