CSIRT-RER
Modello organizzativo - Accreditamento - Servizi

Alessandro Landi
Settore Innovazione Digitale, Dati, Tecnologia e Polo Archivistico Regione Emilia-Romagna

Stefano Giannandrea
Direttore Divisione Sicurezza, Ambiente & Emergenza
Lepida ScpA

Bologna, 21/07/2023

Modello organizzativo

Il Computer Security Incident Response Team della Regione Emilia-Romagna (CSIRT-RER) è una struttura istituita con delibera n. 663 del 28/04/2022, al fine di contribuire all'innalzamento dei livelli di sicurezza della propria consituency conducendola verso uno stato di "readiness" in tema di cyber security.

Con determina n. 7236/2023 Regione ne ha definito il modello organizzativo e delineato le tipologie di servizi (suddivisi tra reattivi, proattivi e di governance) la cui erogazione è affidata alla società Lepida scpa. In tale atto è definito che:

- La constituency del CSIRT-RER è composta da:
  - strutture della Giunta regionale e dell'Assemblea Legislativa;
  - AGREA (Agenzia Regionale per le Erogazioni in Agricoltura);
  - Agenzia Regionale per la Sicurezza Territoriale e la Protezione Civile;
  - INTERCENT-ER (Agenzia per lo sviluppo di mercati telematici);
  - Agenzia Regionale per il Lavoro;
  - Enti della Community Network Emilia-Romagna (CNER).

- Il suo modello organizzativo prevede:
  - DGREII (CSIRT Director);
  - Lepida ScpA (soggetto attuatore e CSIRT Manager);
  - Board Scientifico;
  - Comitato Tecnico della CNER.

La constituency

Tutti gli Enti della CNER entrano di diritto a far parte della Constituency del CSIRT regionale; ciò in virtù della gestione transitoria del rinnovo della convenzione CN-ER (delibera nr. 1130 del 03/07/2023).

I servizi sono erogati da Lepida Scpa sulla base del CdS con RER ed i relativi costi sono sostenuti in parte con fondi PNRR di RER ed in parte saranno a carico degli enti (per i servizi acquistabili da listino).

Per poter iniziare a fruire dei servizi erogati dal CSIRT-RER ciascun Ente dovrà essere accreditato secondo il processo descritto nella slide successiva.

Una volta accreditati, gli Enti avranno a disposizione un set di servizi gratuiti e avranno la possibilità di acquistare ulteriori servizi da un listino che verrà messo a disposizione da Lepida.

L'elenco dei servizi, nonché la relativa erogazione in modalità gratuita o a pagamento, nel corso del tempo potranno subire modifiche sulla base:

- delle risorse economiche messe a disposizione dalla Regione Emilia-Romagna
- delle valutazioni tecniche effettuate da Lepida
- dei pareri del Board scientifico in ordine alla progettazione dei servizi da erogare, con specifico riguardo all'adeguatezza rispetto agli obiettivi assegnati dalla Giunta Regionale
- delle esigenze della constituency raccolte dal Comitato tecnico della RER in ordine alla definizione dei servizi erogabili

Accreditamento

Il processo di accreditamento degli Enti al CSIRT-RER avrà inizio a settembre 2023 e prevederà le seguenti fasi:

- il Referente per la Sicurezza Informatica dell'Ente invia la richiesta di accreditamento a Lepida tramite apposito modulo
- Lepida fornisce al Referente per la Sicurezza Informatica dell'Ente un modulo di "assessment della postura di sicurezza" e un ulteriore modulo di "raccolta informazioni" da compilare
- Lepida fornisce supporto all'Ente per la compilazione dei moduli tramite un corso pubblicato sulla piattaforma di e-learning regionale SELF e sessioni online collettive
- il Referente per la Sicurezza Informatica dell'Ente compila i due moduli e li trasmette a Lepida secondo le modalità comunicate dalla stessa
- Lepida verifica che i due moduli trasmessi siano stati correttamente compilati in tutte le loro parti, predispone un report in cui vengono descritti il livello di maturità dell'Ente, i punti deboli riscontrati e le azioni migliorative suggerite, e trasmette il report al Referente per la Sicurezza Informatica dell'Ente, comunicando l'avvenuto accreditamento

Servizi gratuiti

Una volta accreditati, gli Enti avranno a disposizione i seguenti servizi gratuiti a partire da fine settembre / ottobre 2023.

- **Portale WEB del CSIRT-RER**
  Il CSIRT-RER mette a disposizione un portale web ad accesso pubblico utilizzato per: comunicare le proprie iniziative, descrivere i servizi erogati, pubblicare policy, linee guida e altri documenti prodotti a beneficio della Constituency, emanare alert e bollettini di sicurezza.
  In una seconda fase sarà realizzata un'area ad accesso riservato per: scambio di documenti tra CSIRT-RER e singolo Ente, invio di segnalazioni al CSIRT-RER da parte dell'Ente.

- **Eventi di training e awareness**
  Il CSIRT-RER organizza eventi, online o in presenza, per finalità di formazione e sensibilizzazione su vari ambiti della sicurezza informatica rivolti al personale degli Enti.

- **Training su piattaforma SELF**
  Il CSIRT-RER mette a disposizione una serie di corsi di formazione rivolti al personale IT e a quello con responsabilità dirigenziali degli Enti, fruibili attraverso la piattaforma regionale di e-learning SELF.
  Per poter fruire dei corsi il Referente della Sicurezza Informatica dell'Ente deve censire il personale interessato all'interno del proprio Ente e comunicare a Lepida, per ciascuna persona, nome, cognome, codice fiscale e indirizzo e-mail, al fine di consentirne la profilazione all'interno della piattaforma SELF.

Servizi gratuiti

- **Report e alert di cyber threat intelligence**
  Il CSIRT-RER fornisce report mensili e alert tempestivi (in caso di eventi che richiedono un trattamento immediato), contenenti informazioni ottenute tramite attività di cyber threat intelligence, ovvero di ricognizione passiva su clear e dark web per lo studio di minacce e attaccanti. Le informazioni possono riguardare ad esempio vulnerabilità note su tecnologie, mappatura del perimetro esposto su Internet e relative vulnerabilità, campagne di phishing, credenziali rubate, ecc… e sono utili per prevenire o mitigare attacchi informatici. Il servizio viene offerto su un numero limitato di asset per ciascun Ente (indicativamente 1 dominio e 1 subnet di indirizzi IP pubblici).
  Per poter fruire del servizio il Referente della Sicurezza Informatica dell'Ente deve comunicare a Lepida gli asset su cui attivare il servizio.

- **Cyber threat intelligence sharing**
  Il CSIRT-RER dispone di una propria piattaforma di cyber threat intelligence (MISP), che raccoglie e correla feed ricevuti da fonti aperte, commerciali e istituzionali (accordo con Polizia Postale), nonchè eventi identificati durante le proprie attività di monitoraggio. Il CSIRT-RER offre agli Enti la possibilità di accedere a tali informazioni in due differenti modalità:
  - tramite interfaccia web: è possibile effettuare ricerche basate su keyword ed esportare liste di IoC;
  - tramite federazione di istanze MISP (nel caso in cui l'Ente abbia attivato una propria istanza): è possibile ricevere gli eventi raccolti dall'istanza del CSIRT-RER e, su base volontaria, condividere con il CSIRT-RER gli eventi censiti sulla propria istanza.

  Tale servizio consente agli Enti di ottenere informazioni di dettaglio sugli eventi segnalati nei report di threat intelligence e di disporre di liste di IoC da utilizzare sui propri strumenti di sicurezza (es. firewall, EDR, web proxy).
  Per poter fruire del servizio il Referente della Sicurezza Informatica dell'Ente deve comunicare a Lepida la modalità che intende utilizzare.

Servizi acquistabili a listino

Gli Enti avranno la possibilità di acquistare ulteriori servizi da un listino che verrà messo a disposizione da Lepida. Si prevede la progressiva attivazione tra la fine del 2023 e il 2024 dei seguenti servizi:

- Campagne di phishing simulato
- Training dedicati
- Assessment
- Esercitazioni cyber
- Vulnerability assessment e penetration test
- Monitoraggio della superficie di attacco esterna
- Monitoraggio e rilevazione degli incidenti di sicurezza
- Risposta agli incidenti di sicurezza