1. Ultimo aggiornamento

Questa è la versione 1.0, pubblicata l'31/12/2024.

2. Informazioni di contatto

2.1 Nome del team

CSIRT Basilicata: Computer Security Incident Response Team Basilicata

2.2 Indirizzo

PRESIDENZA GIUNTA REGIONALE, UFFICI SPECIALI DI PRESIDENZA, UFFICIO AMMINISTRAZIONE DIGITALE Via Vincenzo Verrastro, 6 – 85100, Potenza (PZ)

2.3 Fuso Orario

Europa Centrale (GMT+1, e GMT+2 dall'ultima domenica di marzo all'ultima domenica di ottobre)

2.4 Numero di telefono

Non divulgato

2.5 Numero di fax

Non divulgato

2.6 Altre comunicazioni

I soggetti appartenenti alla Constituency del CSIRT Basilicata devono comunicare con i membri del team tramite il modulo citato nella sezione 6 o via email all'indirizzo di seguito.

2.7 Indirizzo email

csirt[at]regione[.]basilicata[.]it Si tratta di un alias di posta elettronica che inoltra le email agli operatori di turno del CSIRT Basilicata.

2.8 Chiavi pubbliche e altre informazioni di crittografia

Il CSIRT Basilicata supporta la crittografia PGP/GPG.
La chiave pubblica PGP/GPG è disponibile sul sito ufficiale del CSIRT Basilicata

2.9 Membri del team

Il team del CSIRT Basilicata è composto da Analisti della sicurezza informatica, Analisti delle minacce, formatori tecnici e divulgatori per la sensibilizzazione alle tematiche di cybersecurity e Responsabili della risposta agli incidenti.

3. Statuto

3.1 Dichiarazione di missione

La missione del CSIRT Basilicata è quella di supportare le entità incluse nella Constituency attraverso l'erogazione di un set di servizi a catalogo di natura proattiva e reattiva.
Di conseguenza il CSIRT Basilicata è stato progettato per:
- offrire supporto per la progettazione e l'integrazione dei sistemi di monitoraggio sati dai SOC nella Constituency e quelli di risposta agli incidenti del CSIRT e supportare il miglioramento continuo delle loro capacità di detection degli eventi di sicurezza;
- progettare e condividere con la Constituency playbook di risposta agli incidenti fornendo personale esperto nelle fasi di contenimento, eradicazione delle minacce e recupero dei sistemi;
- pianificare ed eseguire scansioni automatiche dei sistemi infrastrutturali e applicativi volte all'identificazione delle vulnerabilità note e definire apposite strategie di rimedio;
- pianificare ed eseguire attività di audit interni e assessment tecnologici all'interno della Constituency e sui fornitori chiave per la sicurezza delle informazioni;
- raccogliere e disseminare dati di intelligence rilevanti per i soggetti che compongono la Constituency assicurando una puntuale valutazione dei rischi e migliorando continuamente la postura di sicurezza;
- trasferire conoscenze e competenze in ambito di cybersecurity per assicurare il miglioramento della cultura associata alla sicurezza delle informazioni ed un ecosistema tecnologico IT e OT, a supporto dei servizi erogati dei soggetti inclusi nella Constituency, adeguatamente configurato;
- sviluppare, condividere e supportare l'attuazione, all'interno della Constituency, di politiche, processi e procedure ilevanti per l'organizzazione delle attività di sicurezza delle informazioni;
- garantire un canale di comunicazione sicuro e resiliente tra le diverse entità e le autorità nazionali che potrebbero dover essere coinvolte in caso di crisi.

3.2 Constituency

Il CSIRT Basilicata offre i propri servizi ad aziende pubbliche ed infrastrutture critiche operanti nel territorio della Regione Basilicata inclusi:
- Enti di pubblica amministrazione regionale;
- Enti sub-regionali;
- Enti operanti nel settore sanitario regionale;
- Enti che erogano servizi essenziali ai cittadini regionali;
- infrastrutture critiche ed aziende censite nel Perimetro di Sicurezza ACN.

Gli enti per essere inclusi nella constituency sono sottoposti ad un processo di presa in carico volto a definire il campo d'applicazione dei servizi ricevuti dallo CSIRT Basilicata. La lista degli enti appartenenti alla Constituency è consultabile all'interno della sezione sicurezza del sito istituzionale della Regione.

3.3 Affiliazione

Il CSIRT Basilicata è affiliato con CSIRT Italia che fa parte dell'Agenzia per la Cybersicurezza Nazionale (ACN), in cui è istituito anche il Comitato Nazionale per la Gestione della Cybersicurezza (NSC) che supporta il Presidente del Consiglio dei Ministri italiano e il Comitato Interministeriale per la Cybersicurezza (CIC) nelle attività di prevenzione, preparazione, risposta e ripresa relative alla gestione delle crisi nazionali di cybersicurezza.

3.4 Autorità

In considerazione degli obiettivi identificati nel documento di Mandato, delle caratteristiche e delle necessità degli Enti che appartengono alla Constituency, CSIRT Basilicata opera in un regime di Autorità Condivisa. In virtù di tale regime, CSIRT Basilicata collabora con i singoli Enti influenzando il processo decisionale circa le azioni che dovrebbero essere intraprese in merito alla sicurezza informatica, senza tuttavia poterle imporre.
In tal senso, il CSIRT Basilicata espleta il suo mandato nell'abito della Constituency con il riconoscimento della propria funzione da parte di:

- Ufficio per l'amministrazione digitale Regione Basilicata.

4. Policies

I servizi del CSIRT Basilicata sono progettati per adattarsi ad un ampliamento progressivo della Constituency, prevedendo che nuovi membri possano essere integrati con i processi del CSIRT in maniera scalabile e modulare. Il CSIRT Basilicata, infatti, adatta i propri servizi al contesto degli Enti e alle prestazioni associate alle tecnologie di sicurezza implementate con l’obiettivo di supportare, reattivamente e proattivamente, la risposta agli incidenti di sicurezza informatica che si verificano all'interno della sua Constituency.
Il CSIRT Basilicata condivide con altre parti interessate le informazioni che riceve, se possibile in forma anonima, al fine di risolvere o prevenire incidenti di sicurezza e/o gestire specifiche questioni di sicurezza delle informazioni.
Il CSIRT Basilicata riceve e condivide informazioni utili per mitigare e risolvere gli incidenti e/o coordina la risposta tra le controparti tecniche regionali e nazionali. Inoltre, si impegna a mantenere aggiornata la sua Constituency sulle potenziali vulnerabilità, possibilmente prima che possano essere sfruttate.
Il CSIRT Basilicata opera entro i limiti imposti dal suo mandato e protegge le informazioni sensibili in conformità con le normative e le politiche pertinenti all'interno dell'Italia e dell'UE. In particolare, il CSIRT Basilicata garantisce la riservatezza delle fonti nella massima misura possibile.
Per le comunicazioni verso CSIRT Basilicata il metodo raccomandato, se non diversamente accordato al momento dell’ingresso nella Constituency è l’invio di email a csirt[@]regione[.]basilicata[.]it assicurando la cifratura di dati sensibili.
I servizi CSIRT non prevedono alcun supporto diretto agli utenti finali, in caso gli utenti degli Enti rilevassero anomalie o indicazioni associate a potenziali incidenti di sicurezza, questi ultimi devono ingaggiare i referenti incaricati dall’Ente per il monitoraggio e rilevamento degli eventi di sicurezza.

4.1 Politica Per La Classificazione Degli Asset Informatici

Il CSIRT Basilicata ritiene fondamentale la cooperazione tecnica e la condivisione delle informazioni con il CSIRT Italia ed altri soggetti rilevanti per

raggiungimento dei propri obiettivi definiti nel mandato.
CSIRT Basilicata assicura che le informazioni relative alle attività proattive e reattive trattate nell'ambito dei propri servizi come nomi e dettagli tecnici, non vengono pubblicate senza accordi formalmente approvati tra le parti.
CSIRT Basilicata per la classificazione delle informazioni e degli asset informatici utilizza, promuove e sensibilizza la Constituency all'utilizzo del TLP.

4.2 Politica Per La Classificazione Degli Incidenti Informatici

Il CSIRT Basilicata utilizza la tassonomia cyber dell'ACN per classificare gli incidenti di sicurezza informatica ed esegue formazione continua per assicurare l'adeguato utilizzo di tale tassonomia da parte dei principali stakeholders.
Nell'ambito del processo di monitoraggio ed identificazione degli eventi di sicurezza utilizza la seguente classificazione di priorità per la gestione della comunicazione da e verso il CSIRT Basilicata:
A basso impatto – evento che riporta informazioni relative ai sistemi di sicurezza, per i quali non è necessario un intervento specifico (ad esempio, durante la normale operatività, log-in fallito di un utente autorizzato a una risorsa). Solitamente tale tipologia di eventi è registrata a fini statistici e senza ulteriori correlazioni non si configura come un evento per il quale è richiesto un approfondimento;
Significativo – evento che indica attività che hanno luogo al di fuori del normale funzionamento di una risorsa o di un servizio IT. Questo tipo di evento è solitamente generato da applicazioni o da strumenti di monitoraggio quando è probabile che il protrarsi dell'utilizzo di una determinata risorsa superi la soglia di performance della stessa e causi un malfunzionamento o un'interruzione;
Critico – evento che indica potenziale violazione delle politiche di sicurezza ICT, errori, importanti degradazioni delle performance, malfunzionamenti o perdita di funzionalità di un servizio o una risorsa tecnologica (ad esempio, attacco DDoS).
Il CSIRT promuove ove configurabili sistemi di automazione per la gestione degli incidenti di sicurezza informatica che ottimizzano la classificazione degli stessi. Per tale finalità e per assicurare una più ampia cooperazione internazionale è predisposto per l'utilizzo delle tassonomie riconosciute al livello internazionale.

4.3 Politica Per Lo Sviluppo Sicuro

CSIRT Basilicata promuove l'adozione di un ciclo di vita sicuro del software, ovvero un approccio alla sicurezza del codice che inizi nelle fasi embrionali dei progetti, assicurando che siano considerati ed implementati i principi di privacy by design e mitigazione dei rischi ritenuti non accettabili.

Per prevenire che nell'ambito della Constituency siano erogati servizi supportati da software vulnerabili e/o non correttamente configurati il CSIRT fornisce supporto attraverso servizi consulenziali nelle seguenti fasi del ciclo di vita del software:

Fase 1: Pianificazione e progettazione – con l'obiettivo di identificare i requisiti di sicurezza tenendo in considerazione il contesto in cui l'applicazione è utilizzata, i dati che essa tratta, le possibili minacce a cui è esposta e le vulnerabilità di sicurezza afferenti al design e all'architettura, al fine di

identificare le opportune contromisure da implementare;
Fase 2: Sviluppo – con l'obiettivo di sviluppare l'applicazione seguendo le linee guida di sviluppo sicuro per evitare di introdurre vulnerabilità di sicurezza. Tali linee guida sono ereditate dai maggiori standard di settore;
Fase 3: Test – con l'obiettivo di eseguire test di sicurezza sul codice, su ambienti appositamente predisposti ed isolati, e sull'infrastruttura ICT ove sarà rilasciato in produzione al fine di rilevare vulnerabilità note o configurazioni non ritenute sicure. Di seguito viene riportata una lista esemplificativa e non esaustiva di possibili test da effettuare in diverse fasi del ciclo di vita del software :

Static Application Security Testing (SAST): scansioni effettuate direttamente sul codice sorgente e sull'applicazione eseguita in tempo reale per identificare possibili sfruttamenti malevoli;

Vulnerability Assessment (VA): verifica delle vulnerabilità dell'infrastruttura ICT su cui poggia l'applicazione in oggetto mediante scansioni dedicate;

Dynamic Application Security Test (DAST) : fase in cui l'intera applicazione viene sottoposta a verifiche di intrusione di tipo manuale per verificare accuratamente l'effettiva possibilità di sfruttamento delle vulnerabilità di sicurezza.

Fase 4: Rilascio e distribuzione – con l'obiettivo di garantire che l'applicazione venga implementata e messa in produzione in un ambiente che preveda gli idonei presidi di sicurezza, riducendo al minimo i rischi di vulnerabilità e attacchi.

4.4 Politica Per L'Accesso ai Sistemi

Il team del CSIRT Basilicata ha accesso ai sistemi dei soggetti in modalità privilegiata solo in presenza di approvazione e in conformità con le leggi applicabili vigenti. L'accesso ai sistemi informatici in modalità privilegiata è concesso alle risorse di CSIRT Basilicata previa formalizzazione di atto di nomina da amministratore di sistema e solo per le finalità del mandato e per i servizi attivati.

4.5 Politica Per L'indipendenza Ed Imparzialità Delle Valutazioni

CSIRT Basilicata assicura inoltre che tutte le valutazioni eseguite nell'abito dell'espletamento del proprio mandato siano svolte in modo oggettivo, senza influenze esterne, e che i risultati riflettano accuratamente la situazione analizzata.

4.6 Politica Per Le Comunicazioni Sui Media Pubblici

Il CSIRT Basilicata comunica esclusivamente tramite canali ufficiali. L'utilizzo dei media pubblici è autorizzato solo nel perimetro normato all'interno dei processi del Framework Operativo del CSIRT. Eventi non prevedibili che potrebbero richiedere l'utilizzo dei media pubblici al di fuori di tali processi saranno gestiti secondo l'approvazione del leader del CSIRT Basilicata. Le risorse del CSIRT possono utilizzare canali media privati per finalità personali non facendo fraintendere quindi che l'utilizzo sia eseguito per conto del CSIRT Basilicata.

5. Servizi

5.1 Risposta agli Incidenti

CSIRT Basilicata, nell'ambito delle fasi di containment, eradication e recovery di incidenti di sicurezza informatica supporta gli Enti della sua Constituency erogando diverse tipologie di servizi:

- supporto all'analisi delle cause dell'incidente;
- coordinamento dei team convolti nella risposta all'incidente;
- supporto alla classificazione dell'incidente ed alla disseminazione nella Constituency degli IoC;
- gestione delle attività di escalation verso CSIRT Italia ed altre autorità competenti.

5.2 Servizi Proattivi

Lo CSIRT Basilicata fornisce alla sua Constituency i seguenti servizi di preparazione alla risposta agli incidenti:

- condivisione dei dati relativi a diverse fonti di threat intelligence;
- audit sulla postura di sicurezza o assessment dei sistemi di monitoraggio degli incidenti;
- sensibilizzazione della propria Constituency relativamente le principali minacce informatiche;
- identificazione e classificazione delle vulnerabilità;
- formazione tecnica rivolta al personale operativo dei SOC degli Enti presenti nella Constituency;
- definizione di azioni correttive basate sulle cause alla radice degli incidenti gestiti.

5.3 Reactive Activities

Lo CSIRT Basilicata fornisce alla sua Constituency i seguenti servizi reattivi.

- analisi degli incidenti;
- supporto nella risposta agli incidenti;
- coordinamento delle attività di risposta agli incidenti;
- coordinamento alla gestione delle vulnerabilità tecniche;
- definizione delle strategie di contenimento ed eradicazione delle minacce informatiche.

6. Incident Reporting Forms

La condivisione dei report associati ad incidenti presi in carico dai SOC degli enti all'interno della Constituency deve avvenire tramite posta elettronica certificata di CSIRT Basilicata utilizzando l'apposito modulo messo a disposizione della Constituency. Le richieste di servizio e di supporto per la risposta agli incidenti devono essere inviate ai contatti indicati al punto 2.

7. Disclaimers

The CSIRT Basilicata non è responsabile per l'utilizzo improprio degli strumenti messi a disposizione della constituency nell'ambito dei servizi erogati.