

Cybersecurity, scarica la guida alla notifica dei cyber incidenti al CSIRT Italia di ACN

L'Agenzia per la Cybersicurezza Nazionale ha pubblicato una **Guida alla notifica dei cyber incidenti al CSIRT Italia**, un compendio, un "testo unico" delle istruzioni per i diversi soggetti, pubblici e privati, tenuti per legge alla notifica degli incidenti.

La corretta adozione della procedura di notifica degli incidenti cibernetici rappresenta infatti un elemento decisivo per assicurare la **sicurezza** e la **resilienza delle reti**, quella dei **sistemi informativi** e dei **servizi informatici**.

Comunicare al CSIRT l'impatto di un evento dannoso

La prontezza e la precisione delle informazioni fornite nel corso del processo di notifica rivestono un ruolo decisivo per consentire al **CSIRT Italia** (è bene ricordare che nel dicembre scorso è stata pubblicata la graduatoria delle diciannove istanze progettuali che saranno finanziate con oltre 28 milioni di euro messi a disposizione dall'**Investimento 1.5 Cybersecurity** del **PNRR** di cui l'**ACN** è soggetto attuatore) di acquisire una conoscenza completa ed esaustiva dell'incidente occorso finalizzata all'attività di allertamento nonché a fornire ai soggetti impattati il supporto necessario nell'ottica del ripristino dei medesimi servizi.

Il flusso informativo verso il **CSIRT Italia** si sviluppa nelle seguenti fasi:

- **fase preparatoria**, con l'intento di raccogliere le prime informazioni idonee a garantire una sufficiente conoscenza dell'evento;
- **fase di segnalazione del cyber incidente**, che avviene mediante la compilazione di un modulo di segnalazione "Notifica incidente" disponibile sul sito internet del **CSIRT Italia**. Occorre che questa comunicazione venga effettuata al **Computer Security Incident Response Team – Italia** con una tempistica definita nelle linee guida, e diversamente declinata in funzione dell'appartenenza del soggetto ai diversi presidi normativi. La segnalazione è strettamente correlata al principio di immediatezza della conoscenza dell'incidente, inteso nella sua magnitudo e nel suo carattere di impatto sistemico eventuale;
- **fase di gestione della notifica**, ovvero le operazioni di **incident handling**, da parte del personale del **CSIRT Italia**, per dare supporto alla vittima con efficaci azioni di contenimento e di ripristino dei servizi;
- **fase di chiusura dell'incidente**, che conclude il flusso informativo.

Rin saldare la resilienza dell'ecosistema digitale nazionale

L'Agenzia per la Cybersicurezza Nazionale – che, dopo le linee guida sulla conservazione delle password, le funzioni di hash e i codici di autenticazione messaggi, ha pubblicato ulteriori focus sulla crittografia dedicati alla minaccia quantistica – puntualizza che la guida alla notifica dei cyber incidenti si rivolge anche ai soggetti, pubblici e privati, che pur non essendo obbligati alla notifica intendono tuttavia, in maniera volontaria, segnalare l'incidente

allo CSIRT.

Contribuendo a una migliore condivisione della conoscenza del livello e dell'intensità della cyber minaccia, per rafforzare la resilienza dell'ecosistema digitale nazionale. Tutto ciò, rimarcando che il documento è organizzato in sezioni chiave; organizzato per offrire chiarezza e praticità per una corretta adozione del protocollo di comunicazione in funzione del soggetto che effettua la notifica. A vantaggio della comprensione e dell'implementazione del processo.

Per approfondire

Leggi le altre notizie sull'home page di Key4biz

<https://www.key4biz.it/cybersecurity-scarica-la-guida-alla-notifica-dei-cyber-incidenti-al-csirt-italia-di-acn/500793/>