CSIRT

**CSIRT**

(Computer Security Incident Response Team), è un team specializzato nella gestione degli incidenti di sicurezza informatica. Si occupa di rilevare, rispondere e mitigare gli eventi di sicurezza informatica, come attacchi informatici, violazioni della rete e malware.

Inoltre ha il compito di coordinare le attività di risposta agli incidenti, analizzare le minacce, e sviluppare strategie per prevenire futuri attacchi.

**INCIDENT RESPONSE:**

L'Incident Response è come un piano d'azione per gestire situazioni problematiche, come attacchi informatici o violazioni di dati.

Si divide in 4 fasi:

**Preparazione:**

Definizione delle politiche e dei protocolli di sicurezza, formazione del personale e implementazione di strumenti di monitoraggio per rilevare e prevenire incidenti.

**Rilevamento ed analisi:**

Riconoscimento di attività anomale o sospette che potrebbero indicare un incidente di sicurezza.

**Contenimento Rilevazione e Recupero:**

**Contenimento:** Contenimento dell'incidente per evitare ulteriori danni e limitare la sua diffusione

**Eliminazione:** lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell’incidente all’interno della rete o sui sistemi.

**Recupero:** Ripristino dei sistemi e dei dati danneggiati durante l'incidente per ripristinare la normale operatività. Si utilizzano questi due metodi: RECOSTRUTION si usa per recuperare parti affidabili del SO. REBUILDING utilizzato per ricostruire interamente un sistema impattato.

**Attività post-incidente:**

Valutazione dell'incidente per comprendere le cause, migliorare le procedure e prevenire futuri incidenti.

**Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto**

**Segmentazione di Rete:** è possibile dividere la rete in segmenti separati in modo che un incidente in un segmento non possa facilmente diffondersi agli altri (subnetting VLAN).

**Quarantena:** isolare uno o più dispositivi per poterli monitorare

**Isolamento:** isolare un dispositivo con una vulnerabilità e tenerlo scollegato da qualsiais altro in attesa di un aggiornamento che risolva la vulnerabilità

**Rimozione:** Impedire cosi ogni forma di collegamento con qualsiasi altro dispositivo

**Spiegate la differenza tra Purge e Destroy per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi**

**Clear:** il dispositivo viene completamente ripulito dal suo contenuto. Il contenuto viene sovrascritto più e più volte per riportare il dispositivo nello stato iniziale.

**Purge**: la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili.

**Destroy:** si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un danno in termini economici maggiore.