PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5820 di Lunedì 31 marzo 2025

Un prezioso manuale per la gestione degli incidenti informatici

Gli incidenti informatici sono sempre più frequenti e coinvolgono i responsabili della sicurezza informatica. L'unione europea ha quindi sviluppato un manuale con preziose indicazioni sulla gestione di un incidente informatico: il contenuto del manuale.

Il manuale inizia mettendo in evidenza come le strategie di risposta ad un incidente informatico devono essere adattate alla tipologia specifica di incidenti. Ad esempio, di queste varie tipologie si illustrano le seguenti:

- accesso non autorizzato al sistema ed ai dati,
- minacce dall'interno,
- attacchi per DoS- denial of service
- attacchi alle password
- attacchi al sito Web
- e via dicendo.

Al proposito, può essere utile ricordare ai lettori come la gran parte degli attacchi portati ai sistemi informatici pubblici in Italia, nel mese di febbraio 2025, da parte di un attaccante russo, consistevano essenzialmente in attacchi di tipo DoS. Questa tipologia di attacchi crea un serie di problemi alle utenze, ma almeno non comporta il furto o l'alterazione dei dati presenti nel sistema informativo. Questa tipologia di attacco infatti rallenta in misura significativa la possibilità di accesso al sistema da parte di utenti legittimi.

Il manuale continua indicando le modalità con cui deve essere impostato e sviluppato un piano di risposta ad un incidente informatico. Per sviluppare questo piano bisogna rispondere alle ormai famose quattro domande:

- che cosa è successo,
- chi potrebbe essere responsabile dell'attacco,
- quando l'attacco si è verificato,
- come l'attacco si è sviluppato.

Come al solito, un aspetto fondamentale per sviluppare un piano di risposta ad un incidente informatico inizia con una decisione dell'alta direzione, che definisca una policy di messa sotto controllo dell'evento.

Pubblicità

Successivamente occorre mettere a punto una squadra di pronto intervento, che, a sua volta, deve mettere a punto, anche mediante simulazioni, i successivi interventi.

La messa punto di un piano di comunicazione, che permetta di raggiungere e tenere allineati tutti i soggetti coinvolti, rappresenta un aspetto fondamentale per la distribuzione di informazioni aggiornate.

Per quanto riguarda le squadre di pronto intervento, il manuale ne identifica tre, rispettivamente:

- Computer security Incident response Team- CSIRT
- computer Incident response Team- CIRT
- computer Emergency response Team ? CERT

Al proposito, si fa presente che l'ultimo acronimo è stato depositato dall'università Carnegie Mellon e quindi per utilizzarlo bisogna chiedere una specifica autorizzazione.

Il luogo dove tutte le attività vengono coordinate viene spesso chiamato security operations Center- SOC.

I componenti delle varie squadre di pronto intervento sono evidentemente scelti fra soggetti con competenze tecniche, dirigenziali, di comunicazione ed anche soggetti terzi, come ad esempio consulenti per settori specializzati o consulenti legali.

Il manuale dedica poi uno specifico capitolo al fatto che l'incidente si sia verificato nel cloud e quindi richieda particolari accorgimenti per la messa sotto controllo.

Il manuale mette in evidenza come le squadre di pronto intervento debbano avere a disposizione tutta una serie di tecnologie, che permettano di mettere sotto controllo rapidamente le aree del sistema informativo, che sono state compromesse.

Un interessante paragrafo è dedicato all'opportunità o meno di coinvolgere soggetti terzi specializzati. È una decisione non facile, che va attentamente studiata dalla direzione.

Il manuale si chiude con una viva raccomandazione all'essere preparati a questi eventi, citando un'ormai famosa frase di Benjamin Franklin.

Nella seconda parte di questo articolo, metteremo a disposizione, in formato Word, un modulo descrittivo di un tipico incidente informatico.

ENISA - Good Practice Guide for Incident Management - Guida alle buone pratiche per la gestione degli incidenti di sicurezza di rete e delle informazioni (pdf)

Adalberto Biasiotti

 Licenza Creative Commons

---

www.puntosicuro.it