Progetto interdisciplinare di formazione informatica. Unità-2 per manager

Nella prima fase della gestione di quanto abbiamo (gli asset), sarebbe utile innanzitutto rivelare ed elencare i beni di cui disponiamo. È necessario conoscere ciò che un'istituzione possiede e ciò che non possiede. Poi occorre definirne la proprietà. Nessuna attività o transazione dovrebbe essere lasciata incustodita. Infine, si devono determinare le regole per l'utilizzo di questi beni.

Scopo: identificare gli asset dell'organizzazione e definire le responsabilità di protezione appropriate.

Asset inventory (Inventario dei beni). È necessario identificare i beni relativi alle informazioni e alle strutture di elaborazione delle informazioni e redigere e mantenere un inventario di tali beni.

Guida all'applicazione: Un'organizzazione deve identificare le risorse rilevanti nel ciclo di vita delle informazioni e documentarne l'importanza. Il ciclo di vita delle informazioni deve comprendere la creazione, l'elaborazione, l'archiviazione, la trasmissione, la cancellazione e la distruzione. La documentazione deve essere mantenuta in conformità con gli inventari esistenti o in modo specifico.

Asset inventory. Deve essere aggiornato, coerente, accurato e compatibile con altri inventari.

La proprietà del bene deve essere assegnata per ogni bene identificato e deve essere determinata la sua classe.

Proprietà dei beni. Per tutti i beni in inventario devono essere effettuate le assegnazioni di proprietà.

Guida applicativa. Possono essere designati come proprietari dell'asset gli individui e le altre entità con responsabilità di gestione approvata per il ciclo di vita dell'asset.

Spesso si utilizza un processo per garantire che la proprietà degli asset sia determinata in modo tempestivo. La proprietà deve essere determinata quando le risorse vengono create o trasferite all'organizzazione. Il proprietario dell'asset deve essere responsabile della corretta gestione dell'asset per tutto il suo ciclo di vita.

Il proprietario del bene deve:

a) assicurare la registrazione dell'inventario dei beni,

b) assicurare che le attività siano classificate e protette in modo appropriato,

c) definire e rivedere periodicamente le restrizioni di accesso alle attività significative e la loro classificazione, tenendo conto della politica di controllo degli accessi applicabile,

d) garantire che vengano intraprese azioni appropriate per la cancellazione o la distruzione degli asset.

Uso accettabile delle risorse. Le *regole* relative all'uso accettabile delle informazioni e delle risorse relative alle strutture informatiche e di elaborazione delle informazioni devono essere determinate, documentate e attuate.

Guida all'applicazione: I dipendenti e gli utenti esterni che utilizzano o hanno accesso alle risorse dell'organizzazione devono essere informati dei requisiti di sicurezza delle risorse dell'organizzazione associate alle strutture e alle risorse informatiche e di elaborazione delle informazioni. Questi utenti devono essere responsabili dell'uso di tutte le risorse di elaborazione delle informazioni e di qualsiasi uso che avvenga sotto la loro responsabilità.

Restituzione dei beni. Tutti i dipendenti e gli utenti di soggetti esterni devono restituire tutti i beni aziendali in loro possesso al termine del rapporto di lavoro, del contratto o dell'accordo.

Guida applicativa: Il processo di cessazione deve essere formulato in modo da includere la restituzione della proprietà di tutti i beni fisici ed elettronici dell'organizzazione precedentemente concessi.

Quando un dipendente o un utente esterno acquista o utilizza le apparecchiature dell'organizzazione, vengono seguite procedure per garantire che tutte le informazioni rilevanti vengano trasferite all'organizzazione e cancellate in modo sicuro dalle apparecchiature.

Se un dipendente o un utente esterno dispone di informazioni importanti per le operazioni in corso, queste devono essere documentate e trasferite all'organizzazione.

Valutazione e gestione delle minacce e delle vulnerabilità. Quasi tutte le organizzazioni dispongono di beni sensibili e preziosi che devono essere protetti. Tuttavia, non tutte le organizzazioni dispongono di una strategia completa e ponderata per la protezione di questi beni. Nella cybersecurity, le strategie di gestione delle vulnerabilità sono il fondamento di una difesa forte. In genere, le strategie di gestione delle vulnerabilità sono progettate per aiutare i sistemi, le reti, le applicazioni e così via di un'organizzazione. Queste vulnerabilità vengono quindi identificate, valutate e risolte il prima possibile.

Che cos'è la valutazione delle vulnerabilità? La valutazione delle vulnerabilità è il processo di identificazione, individuazione, classificazione e prioritizzazione delle vulnerabilità nei sistemi informatici, nelle applicazioni e nelle infrastrutture di rete.

Un processo di valutazione delle vulnerabilità mira a identificare le minacce e i rischi che esse comportano. Spesso prevede l'uso di strumenti di test automatizzati, come gli scanner di sicurezza di rete, i cui risultati sono elencati in un rapporto di valutazione delle vulnerabilità.

L'importanza delle valutazioni di vulnerabilità. Per comprendere meglio l'importanza della valutazione della vulnerabilità, consideriamola attraverso gli occhi del proprietario di un immobile. Se possedete un edificio di valore, probabilmente adottate una serie di misure per proteggerlo.

Una valutazione delle vulnerabilità fornisce a un'organizzazione informazioni dettagliate su eventuali punti deboli della sicurezza nel suo ambiente. Fornisce inoltre indicazioni su come valutare i rischi associati a tali punti deboli. Questo processo consente all'organizzazione di comprendere meglio le

proprie risorse, le falle nella sicurezza e il rischio complessivo, riducendo la probabilità che un criminale informatico violi i sistemi e colga l'azienda di sorpresa.

Tipi di valutazione della vulnerabilità.

- Scansione basata sulla rete
- Scansione basata su host
- Scansione della rete wireless
- Scansione di prova sul web
- Scansione del database

Continuità operativa informatica. Quando i cyberattacchi colpiscono, molte giurisdizioni interessate scoprono che i loro piani COOP di base non reggono. Sebbene i piani siano adeguati per la transizione a un luogo di lavoro alternativo, hanno molto meno da offrire quando si tratta di lavorare senza accesso ai sistemi e ai dati di cui il personale ha bisogno per svolgere le proprie funzioni essenziali.

Elemento di configurazione: Un elemento di configurazione è qualsiasi componente che deve essere gestito per fornire un servizio IT. Esempi di elementi di configurazione sono servizi IT, hardware, software, edifici, persone e documentazione formale.

Sistema di gestione della configurazione: Il sistema di gestione della configurazione, abbreviato in CMS, è un insieme di strumenti e database utilizzati per gestire i dati di configurazione di un fornitore di servizi IT. I dati relativi agli elementi di configurazione sono memorizzati in record di configurazione e i record di configurazione sono inclusi nei database del sistema di gestione della configurazione. **Configuration Management Database**: Il database di gestione della configurazione è abbreviato in CMDB. Il CMDB è un database utilizzato per archiviare i record di configurazione durante il loro ciclo di vita.

Valutazione dei rischi per la sicurezza. Il rischio è definito come la combinazione delle probabilità di un evento e del suo esito. La valutazione del rischio, che è una fase della gestione del rischio, è un processo in cui vengono definiti i rischi e vengono determinati gli effetti e le priorità di questi rischi identificati. La gestione del rischio consiste nel determinare un livello di rischio accettabile, nel valutare il rischio attuale, nell'adottare le misure necessarie per ridurlo a un livello accettabile e nel mantenere tale livello.

Configurazione ideale della sicurezza informatica. In primo luogo, la prevenzione.

- Esaminare periodicamente i service pack e gli aggiornamenti del sistema operativo e del software,
- Mantenere i diritti degli utenti al minimo,
- Utilizzare gli scanner di vulnerabilità,

- Utilizzare la firma elettronica,
- Utilizzare uno screen saver protetto da password sul computer.

In secondo luogo, la determinazione. La sicurezza non è solo una questione di prevenzione. Ad esempio, il fatto che un museo sia ben protetto, che sia circondato da recinzioni, che le porte siano chiuse e bloccate, non rende necessario l'uso di guardie notturne in quel museo. Allo stesso modo, aumenta l'uso di metodi per rilevare i tentativi di attacco ai sistemi informatici. La prevenzione consiste nel costruire una barriera che renda gli attacchi più forti (ma non impossibili) o che scoraggi (ma non distrugga) gli aggressori.

Il primo e più elementare passo per il rilevamento è il monitoraggio dell'intero stato e dei movimenti del sistema e la registrazione di queste informazioni. In questo modo, si raccolgono anche dati e prove per l'analisi post-attacco. Firewall, sistemi di rilevamento delle intrusioni, monitor del traffico di rete, scanner di porte, utilizzo di honeypot, strumenti di protezione in tempo reale da virus e spyware, programmi di controllo del checksum dei file e sensori Sniffer di rete sono alcuni dei metodi più comuni utilizzati nel processo di rilevamento.

L'ultima risposta (the last Answerback). Una risposta rapida emerge come elemento essenziale che completa il sistema di sicurezza per respingere questi attacchi. La risposta può essere definita come l'esecuzione di azioni che rispondono immediatamente o il prima possibile ai tentativi di attacco che non possono essere gestiti dal processo di prevenzione e determinati dai processi di rilevamento. I sistemi di rilevamento delle intrusioni possono avere senso se c'è qualcuno o un sistema che risponde a questo rilevamento. Altrimenti la situazione non va oltre il vantaggio di un allarme per auto che nessuno sente e di cui nessuno si preoccupa.