PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5488 di Lunedì 23 ottobre 2023

Un prezioso e gratuito manuale sulla sicurezza informatica

L'esperienza del GAO è indiscutibile ed ecco il motivo per cui riteniamo che i lettori debbano fare tesoro di questo prezioso documento che illustra il programma di audit delle misure di sicurezza informatica del sistema aziendale.

Ormai i lettori conoscono bene il General accounting Office (GAO), che è l'ufficio americano, che effettua verifiche di sicurezza su tutte le attività federali del governo degli Stati Uniti.

Questa linea guida, messa a disposizione di tutti gli enti federali, deve essere usata per svolgere degli audit di efficienza ed efficacia della sicurezza informatica aziendale. L'obiettivo della guida è quello di mettere a disposizione degli auditor una serie di metodologie, tecniche e procedure di audit, che permettano di valutare tutte le componenti del programma di sicurezza informatica.

Ecco quali sono i sei componenti primari di questa guida.

Lo sviluppo di un'analisi dei beni coinvolti e della gestione del rischio

Grazie a questo passo, si può avere a disposizione un quadro organico di tutte le attività che devono essere messe sotto controllo, a livello di beni, sistemi, informazioni trattate e capacità operative

Gestione della configurazione

Questo passo permette di identificare e gestire le caratteristiche di sicurezza dell'hardware e del software e di tenere sotto controllo le modifiche della configurazione operativa.

Gestione delle identità e degli accessi

Nessuno può dubitare del fatto che la protezione delle risorse computerizzate da possibili attacchi, da parte di soggetti non autorizzati, che possono portare a modifica, perdita e rivelazione di dati, rappresenti un rischio di elevato livello. Ecco perché la gestione dei profili di accesso dell'identità di coloro che accedono al sistema informatico rappresenta un'area critica dell'intera

attività di controllo della sicurezza informatica.

Monitoraggio continuo della sicurezza informatica

È indispensabile mantenere una costante attenzione alle vulnerabilità legate all'informatica e alla evoluzione delle minacce, che possono coinvolgere i sistemi utilizzati dall'organizzazione sotto audit.

La risposta agli incidenti

Occorre avere sempre disponibili ed aggiornato un piano efficiente ed efficace per fronteggiare possibili incidenti, sia di natura accidentale, sia di natura dolosa. Una fase di simulazione rappresenta un aspetto fondamentale per verificare l'efficienza del piano di risposta.

Pianificazione delle emergenze e ripristino della funzionalità

Durante l'audit vengono verificati i piani che permettono di fronteggiare l'evento e riprendere al più presto la piena funzionalità dei sistemi da proteggere

Per ognuno dei componenti sopra illustrati, il GAO mette a disposizione da quattro a sei pratiche specifiche. Per ognuna di queste pratiche, vengono inoltre forniti ulteriori obiettivi di controllo, criteri di applicabilità e possibili procedure di audit.

Come i lettori possono ben vedere, si tratta di un prezioso manuale, emesso da un soggetto oltremodo autorevole, che potrà aiutare ogni lettore, coinvolto nella verifica dell'efficienza e della efficacia dei sistemi informatici, nel compiere al meglio la sua preziosa attività di monitoraggio e prevenzione.

GAO - CYBERSECURITY PROGRAM AUDIT GUIDE (PDF, 10.5 MB)

Adalberto Biaasiotti

www.puntosicuro.it