Policy di Sicurezza Informatica

L’adozione di una policy di sicurezza informatica definisce le regole e gli standard che dovranno essere seguiti da tutti i dipendenti e collaboratori dell’azienda.

Avere una policy di questo tipo è vantaggioso tanto per l’azienda quanto per gli utenti della stessa; di fatto il suo scopo è quello di ridurre i rischi, velocizzare le risposte in caso di attacco, e nel caso in cui questo si verificasse, chiarirne le responsabilità.

Normativa applicabile

La normativa applicabile è costituita dallo standard ISO/IEC 27001, pubblicato dall’Organizzazione internazionale per la normazione (ISO) e dalla Commissione elettrotecnica internazionale (IEC). Si tratta di una norma internazionale che definisce i requisiti per definire e gestire un Sistema di Gestione della Sicurezza delle Informazioni (SGSI o ISMS dall'inglese Information Security Management System) in merito ad aspetti di sicurezza logica, fisica ed organizzativa. Lo standard fornisce inoltre una serie di linee guida per la valutazione dei rischi, nonché la gestione, la selezione dei controlli e l'audit della sicurezza delle informazioni.

Ottenere una Certificazione ISO/IEC 27001 permette di dimostrare ai propri clienti, ai propri partner commerciali e alle autorità di regolamentazione che è stato adottato un approccio rigoroso e sistematico per garantire la sicurezza delle informazioni.

Policy Asset IT

Responsabilità dell'azienda è quella di definire i criteri di sicurezza fisica e ambientale degli asset IT al fine di impedire e/o limitare perdite di dati e di risorse dovute a vulnerabilità nell'ambito del dominio fisico.

Tutti gli asset tecnologici (hardware, software e risorse di rete) dell'azienda devono essere identificati e registrati in un inventario mantenuto aggiornato.

PROCEDURE IMPLEMENTABILI:

- Controllo e regolazione dell'accesso fisico ai locali. L'acceso ai locali deve essere consentito solo al personale preposto e autorizzato.
- I locali che ospitano gli elaboratori elettronici devono disporre di dispositivi che consentano di:

1. segregare e tracciare gli accessi effettuati dal personale autorizzato;
2. monitorare tentativi di accesso non autorizzato o di effrazione nei locali;
3. monitorare il livello della temperatura e dell'umidità presenti nei locali;
4. contrastare eventi dannosi quali allagamenti e/o incendi attraverso idonei strumenti di environmental control;
5. garantire l'erogazione del servizio in mancanza di energia elettrica primaria attraverso l'implementazione di opportune soluzioni compensative;
6. segnalare ad una centrale operativa eventuali malfunzionamenti.

- Durante le attività di manutenzione o in caso di cambio d'uso, cambio di proprietà e dismissione dovranno essere previsti meccanismi che garantiscano la riservatezza dei dati contenuti all'interno degli asset e, se necessario, dovranno essere previsti meccanismi che ne impediscano il recupero non autorizzato compresa la cancellazione sicura dei dati.
- Tutti gli asset tecnologici (hardware, software e risorse di rete) dell'azienda devono essere identificati e registrati in un inventario mantenuto aggiornato.

Asset IT e Dipendenti:

Personal Computer: costituisce uno strumento di lavoro e dovrà essere custodito con cura adottando ogni precauzione volta ad evitare ogni forma di danneggiamento; ogni utilizzo non conforme potrà potenzialmente costituire una minaccia alla sicurezza.

1. Si consiglia di permettere l'accesso al gruppo Amministratori solo al personale tecnico. Ai singoli dipendenti non sarà consentito né procedere all'installazione di nuovi software, né alla modifica dei software esistenti. Tutte queste operazioni saranno di esclusiva competenza del personale tecnico individuato.
2. Ogni dipendente dovrà prestare la massima attenzione nell'utilizzo di memorie di massa esterne, limitandone l'utilizzo, conservandole in luoghi sicuri e avvertendo immediatamente il personale tecnico nel caso in cui siano rilevati virus o altre problematiche.
3. In caso di allontanamento, anche temporaneo, dalla postazione di lavoro, l'utente non dovrà lasciare il sistema operativo del proprio pc aperto e dovrà provvedere a proteggere lo stesso attraverso la sospensione o il blocco della sessione di lavoro.
4. Il dipendente è responsabile degli asset IT a lui assegnati e dovrà custodirli con diligenza, sia all'interno degli uffici, sia durante gli spostamenti esterni.

Policy dipendenti

Accesso ad internet:

- L'abilitazione dei pc consegnati ai dipendenti alla navigazione in rete dovrà essere regolamentata e dovrebbe essere proibita per motivi diversi da quelli strettamente collegati all'attività lavorativa; l'accesso ad internet dovrebbe intendersi come "strumento di lavoro", quindi il dipendente non dovrebbe utilizzare lo stesso per "fini personali".
- Per evitare l'accesso a siti non pertinenti all'attività lavorativa svolta, l'azienda potrebbe provvedere ad adottare un sistema di Web Filtering che prevenga determinate operazioni, come ad esempio, il file-sharing o l'accesso a determinati siti segnalati come non autorizzati.

Gestione password:

- E' importante effettuare una corretta gestione delle password. Il personale dovrebbe essere formato sulle regole per una corretta creazione e conservazione delle password.
- Regole basilari da stabilire per l'uso di credenziali aziendali:

1. lunghezza minima di 12 caratteri, con regole di complessità adeguata (utilizzo di lettere, numeri ed anche caratteri speciali);
2. sequenze o caratteri ripetuti. Esempi: 12345678, 222222, abcdefg, o lettere adiacenti sulla tastiera (qwerty);
3. utilizzo di informazioni personali o aziendali (nome, compleanno ecc.);
4. divieto di conservare le password su supporti insicuri (post-it, foglietti, file salvati sul desktop ecc.);
5. divieto di comunicare le proprie password a colleghi.

- Al fine di tutelare maggiormente le credenziali aziendali si potrebbe prevedere l'introduzione della "strong authentication" o autenticazione a due o più fattori (MFA). La MFA necessiterà di un dispositivo aggiuntivo che generi il secondo fattore di autenticazione; in genere tale dispositivo è uno smartphone sul quale ricevere il secondo fattore OTP (One Time Password) via SMS, oppure mediante un'app Authenticator installata.

Security Awareness

- Previsione di corsi di Security Awareness al fine di aumentare la consapevolezza di ogni singolo appartenente alla società dei rischi a cui essa stessa, nonché loro come singoli, sono esposti.

→ Tali corsi di formazione necessitano innanzitutto di essere estesi a tutto il personale; i manager sono i primi a dover essere coinvolti, ma anche la partecipazione e il contributo dell'area HR è decisiva. Da tali percorsi non devono essere escluse le figure dirigenziali.

Tali corsi:

1. devono essere svolti su base continuativa, in quanto le minacce cambiano ed evolvono ogni giorno;
2. il loro obiettivo, oltre quello di creare una cultura della sicurezza collettiva, è anche quello di permettere a tutti di sviluppare un bagaglio di conoscenze tale da mettere in atto comportamenti virtuosi e attuare risposte immediate e efficaci in caso di rilevamento di minacce.

L'ambito delle policy di sicurezza è molto ampio e in ambito di sicurezza informatica può ricoprire diverse casistiche e settori.

Si consiglia l'adozione di una policy commisurata alla dimensioni e alle caratteristiche operative e di asset tecnologici dell'impresa. Si consiglia di implementare il più possibile le policy di sicurezza informatica al fine di rendere fruibili a tutti le regole stabilite e di conseguenza le relative sanzioni in caso di non conformità.