PROTEZIONE

La protezione in ambito cybersecurity copre diversi aspetti fondamentali. I cinque criteri di questa sezione definiscono le aree chiave che le PMI devono considerare per accrescere la loro cyber-resilienza. Questi includono: aggiornamento dei sistemi operativi, applicativi e librerie; gestione IT da parte del personale; crittografia delle informazioni; politiche di backup e sicurezza di rete tramite firewall, IDS, NIDS, Antivirus, EDR e SIEM.

AGGIORNAMENTO SOFTWARE

L'aggiornamento dei sistemi operativi, applicativi e librerie software è essenziale per garantire un livello adeguato di sicurezza. Le procedure centralizzate semplificano la gestione IT e migliorano l'efficacia degli aggiornamenti.

Come vengono gestiti gli aggiornamenti software nella vostra azienda?

- ☐ A: L'IT interno aggiorna manualmente i software e dispositivi OT su base periodica, con policy formalizzate.
- ☐ B: Gli aggiornamenti sono centralizzati, ma non si ricevono notifiche automatizzate dai produttori.
- ☐ C: Gli aggiornamenti software sono demandati ai singoli utenti, mentre l'IT aggiorna i dispositivi OT su segnalazione.
- ☐ D: Gli aggiornamenti sono centralizzati e automatizzati, con notifiche ricevute dal produttore.
- ☐ E: Gli aggiornamenti vengono effettuati manualmente senza policy definite, raramente sui dispositivi OT.

POLICY DI SICUREZZA

Le policy di sicurezza regolano l'uso delle apparecchiature IT e dovrebbero essere comprese e sottoscritte dai dipendenti.

Quali policy di sicurezza sono presenti in azienda?

- ☐ A: Policy formalizzate con controllo centralizzato, accesso ospiti limitato alla rete guest.
- ☐ B: Il personale non può collegare dispositivi personali alla rete aziendale.
- ☐ C: Policy formalizzate vietano l'uso di dispositivi personali per accedere ai dati aziendali.
- ☐ D: Policy formalizzate regolano la gestione dei dispositivi aziendali e prevedono formazione ai dipendenti.
- ☐ E: Nessuna policy di sicurezza, i dipendenti possono connettere dispositivi personali.

CRITTOGRAFIA

La crittografia protegge i dati rendendoli inaccessibili ai non autorizzati. La gestione sicura delle chiavi crittografiche è essenziale per evitare perdite di dati.

Qual è l'approccio dell'azienda nei confronti della crittografia?

- ☐ A: Nessuna crittografia è utilizzata.
- ☐ B: Cifratura usata solo per alcuni dati sensibili.
- ☐ C: Crittografia applicata solo a specifici processi o dispositivi.
- ☐ D: Crittografia ampiamente usata, con chiavi protette da sistemi di sicurezza fisici e informatici.
- ☐ E: Crittografia utilizzata su tutti i dispositivi fisici (PC, mobili e memorie rimovibili).

BACKUP

Il backup dei dati è essenziale per il ripristino in caso di perdita. La pratica di disaster recovery consente di ripristinare i dati in situazioni critiche.

Come vengono gestiti i backup nella vostra azienda?

- ☐ A: Backup eseguiti regolarmente senza procedure formalizzate.
- ☐ B: Backup automatici con ripristini periodici per verificarne l'efficacia.
- ☐ C: Backup regolari con procedure formalizzate e test di ripristino effettuati.
- ☐ D: Backup eseguiti centralmente, ma senza procedure formalizzate.
- ☐ E: Backup effettuati a discrezione degli utenti o non eseguiti.

SICUREZZA DELLA RETE

Una protezione adeguata della rete aziendale è garantita dall'uso di dispositivi hardware e software specifici. Ogni azienda dovrebbe valutare i rischi e destinare budget alla manutenzione e all'acquisto di soluzioni di cybersecurity.

Qual è lo stato della sicurezza della rete nella vostra azienda?

- ☐ A: Implementati firewall, EDR, logger, con un piano formalizzato per la gestione della cybersecurity e un budget destinato a miglioramenti futuri.
- ☐ B: Valutazione dei rischi effettuata, con un piano formalizzato e sistemi come EDR per la gestione delle minacce interne.
- ☐ C: Non sono presenti dispositivi hardware o software per la sicurezza della rete, ma si stanno valutando future implementazioni.
- ☐ D: Implementati firewall e altri sistemi con un piano formalizzato per la cybersecurity, con ulteriori implementazioni previste a seconda del budget.
- ☐ E: Sono presenti solo firewall, senza un piano formalizzato per la gestione della sicurezza informatica e senza previsione di nuovi strumenti.

GESTIONE E TECNOLOGIE

L'uso crescente di strumenti cloud richiede una valutazione sulla loro affidabilità e conformità al GDPR. È essenziale dotarsi di un inventario aggiornato di hardware e software e gestire correttamente i diritti di amministrazione.

STRUMENTI CLOUD

Gli strumenti cloud sono sempre più diffusi nel tessuto imprenditoriale e possono avere diverse forme (per esempio, suite di ufficio, macchine controllabili da remoto, spazio di archiviazione, applicazioni) e generalmente sono accessibili via browser. Questa tipologia di servizi non è intrinsecamente più sicura di quelli on premise (ospitati nella rete aziendale), ma può avere delle modalità differenti per la sua protezione. È frequente che un livello di protezione adeguato per questa tipologia di servizi debba essere messo in piedi dai responsabili della sicurezza o debba essere acquistato come servizio aggiuntivo al provider.

Come si colloca la vostra azienda rispetto all'uso di tecnologie cloud e alla gestione IT?

- ☐ A: L'azienda utilizza servizi cloud privi di feature di sicurezza (es. protezione DDoS o backup).
- ☐ B: L'azienda non utilizza servizi cloud.
- ☐ C: I servizi cloud utilizzati offrono feature di sicurezza di base garantite dal fornitore.
- ☐ D: I servizi cloud offrono solo protezioni minime e non sono state adottate ulteriori misure di sicurezza.
- ☐ E: Oltre alle protezioni di base del cloud, sono stati acquisiti pacchetti aggiuntivi di cybersecurity o servizi di monitoraggio da terze parti.

VA E PT (Vulnerability Assessment e Penetration Test)

Per garantire la sicurezza della rete e delle applicazioni web, le aziende dovrebbero eseguire controlli periodici come il Vulnerability Assessment (VA) e il Penetration Test (PT).

L'azienda ha previsto o svolto attività di VA e PT?

- ☐ A: L'azienda non ha previsto servizi di questo tipo.
- ☐ B: L'azienda ha pianificato VA o PT, ma non li ha ancora eseguiti.
- ☐ C: Sono stati eseguiti controlli sulla sicurezza di applicazioni web e siti, con valutazioni periodiche.
- ☐ D: Penetration test vengono effettuati mensilmente o in modo automatico su tutte le applicazioni e servizi cloud.
- ☐ E: Sono stati eseguiti controlli occasionali su siti e applicazioni web.

INVENTARIO

Avere un inventario aggiornato di hardware e software aziendali è fondamentale per la sicurezza e la conformità alle normative.

È presente un inventario per hardware e software in azienda?

- ☐ A: Non esiste un inventario per hardware e software.
- ☐ B: L'inventario esiste, ma viene aggiornato manualmente e non sempre tracciato.
- ☐ C: L'inventario include anche software gratuiti, aggiornato manualmente e collegato ai processi di acquisto.
- ☐ D: L'inventario viene aggiornato tramite strumenti automatici che monitorano la rete e rilevano nuovi dispositivi.
- ☐ E: È presente solo un inventario hardware, ma non software.

GESTIONE APPLICATIVI

Le aziende devono stabilire regole per gestire e configurare gli applicativi, soprattutto per quelli legati alla sicurezza informatica.

Come sono gestiti e configurati gli applicativi nella vostra azienda?

- ☐ A: Esistono procedure informali, ma non applicabili a tutti i software.
- ☐ B: Alcune procedure sono formalizzate per la gestione degli applicativi.
- ☐ C: Procedure definite per la gestione degli applicativi, ma non formalizzate.
- ☐ D: Procedure formalizzate per gestire tutti gli applicativi, inclusi quelli per la sicurezza.
- ☐ E: Non esistono procedure per la gestione degli applicativi.

AMMINISTRATORI DI SISTEMA

Solo utenti con privilegi amministrativi possono installare e configurare alcuni software. È importante che i permessi siano gestiti correttamente.

Quali sono le politiche sui privilegi di amministrazione nella vostra azienda?

- ☐ A: Gli utenti hanno privilegi di amministratore e la configurazione è gestita dal responsabile di rete o da un'azienda esterna senza contratto continuativo.
- ☐ B: Gli utenti hanno privilegi di amministratore, ma la configurazione è gestita dal reparto IT o da un'azienda esterna con contratto continuativo.
- ☐ C: Gli utenti hanno privilegi di amministratore e gestiscono in autonomia la configurazione degli applicativi.
- ☐ D: Gli utenti non hanno privilegi di amministratore e la configurazione è gestita dal reparto IT o da un'azienda esterna con contratto continuativo.
- ☐ E: Gli utenti non hanno privilegi di amministratore e la configurazione è gestita da una figura interna o da un'azienda esterna senza contratto continuativo.

ORGANIZZAZIONE E PROCESSI

Una gestione chiara e strutturata della cybersecurity è il primo passo per rendere un'azienda cyber-resiliente. Tra gli aspetti fondamentali ci sono la manutenzione IT, un piano di rientro (Disaster Recovery Plan) e una corretta gestione delle autenticazioni e degli strumenti di sicurezza.

MANUTENZIONE IT

La manutenzione dell'IT aziendale è un aspetto fondamentale per garantire un corretto livello di sicurezza della rete e dei dispositivi aziendali. Avere del personale dedicato consente anche di avere dei tempi di reazione minori in caso di incidenti di sicurezza o malfunzionamenti in genere che potrebbero portare a indisponibilità dei dati o a blocchi del flusso lavorativo.

Chi gestisce la manutenzione e la sicurezza IT nella vostra azienda?

- ☐ A: Un'azienda esterna senza contratto formale, attivata solo in caso di problemi.
- ☐ B: Non esiste una gestione formalizzata.
- ☐ C: Un'azienda esterna con contratto continuativo si occupa della manutenzione IT.
- ☐ D: Un'azienda esterna con contratto e/o personale interno dedicato si occupa della manutenzione.
- ☐ E: La manutenzione è gestita da dipendenti che ricoprono anche altri ruoli.

PIANO DI RIENTRO (Disaster Recovery)

Il processo di gestione degli incidenti è cruciale per garantire la continuità operativa dell'azienda. Un Disaster Recovery Plan (DRP) permette di ripristinare l'infrastruttura IT in seguito a disastri o interruzioni non pianificate.

Qual è la situazione della vostra azienda in merito al Disaster Recovery Plan?

- ☐ A: Non esiste un piano di rientro.
- ☐ B: Esiste un DRP basato su un'analisi dell'impatto aziendale (BIA), con un gruppo specializzato incaricato della sua gestione.
- ☐ C: L'azienda ha un Business Continuity Plan (BCP) che include il DRP, con un gruppo incaricato della sua gestione e dell'aggiornamento delle procedure.
- ☐ D: È presente un DRP gestito dal reparto IT, che viene attivato in caso di problemi.
- ☐ E: Esiste un DRP con test periodici, integrato con la procedura di gestione dei data breach.

AUTENTICAZIONE

Le password rappresentano un elemento fondamentale per la sicurezza informatica. È essenziale implementare policies formali per la gestione delle password e, ove possibile, integrare metodi di autenticazione avanzata, come le OTP (One Time Password) o l'autenticazione biometrica.

Come viene gestita l'autenticazione ai sistemi aziendali?

- ☐ A: Non ci sono policies per la gestione delle password.
- ☐ B: Esistono policies per la gestione delle password, ma non sono formalizzate.
- ☐ C: Le policies per la gestione delle password sono precise e formalizzate.
- ☐ D: Policies formalizzate impongono l'uso di password sicure e lunghe, con sistemi automatizzati di verifica della complessità.
- ☐ E: Oltre a policies formalizzate, vengono utilizzati ulteriori fattori di autenticazione, come OTP o autenticazione biometrica.

SEGREGAZIONE DELLA RETE

La segregazione della rete consente di isolare diverse aree operative e ridurre la possibilità di contaminazioni incrociate o movimenti laterali in caso di attacco informatico.

Qual è la situazione della vostra azienda in merito alla segregazione delle reti?

- ☐ A: La rete operativa e quella per gli ospiti sono segregate.
- ☐ B: Ogni area operativa ha una VLAN dedicata, ma i dispositivi IoT e OT sono connessi alla stessa rete degli altri endpoint.
- ☐ C: Non è stata applicata alcuna segregazione delle reti.
- ☐ D: Ogni area operativa ha una VLAN dedicata e i dispositivi IoT sono separati dagli altri endpoint. È stata effettuata una valutazione dei rischi relativi alla sicurezza dei dispositivi.
- ☐ E: La rete degli endpoint è segregata da quella a cui è connesso l'OT.

ACQUISIZIONE DI STRUMENTI DI SICUREZZA

È fondamentale acquisire strumenti di sicurezza informatica come antivirus di nuova generazione, firewall avanzati e sistemi SIEM per garantire un buon livello di protezione.

Come sono gestiti gli strumenti di sicurezza nella vostra azienda?

- ☐ A: Il livello di sicurezza è molto elevato e può influire sulle operazioni aziendali, con blocchi frequenti di siti e programmi.
- ☐ B: Gli strumenti di sicurezza sono configurati, con blocchi di siti web e rallentamenti, e richiedono credenziali multiple per accedere ai sistemi.
- ☐ C: Ogni attività tiene conto della sicurezza, seguendo il principio di "cybersecurity by default".
- ☐ D: Gli strumenti di sicurezza sono configurati con pochi blocchi, senza rallentamenti significativi.
- ☐ E: Sono presenti strumenti di sicurezza di base (antivirus, firewall) con configurazioni standard e nessun impatto operativo significativo.

COMPLIANCE E NORMATIVE
La conformità alle normative, come il GDPR, è cruciale per la protezione dei dati personali. Le aziende dovrebbero anche considerare l'implementazione di standard come la ISO/IEC 27001 per migliorare la gestione della sicurezza delle informazioni.

La vostra azienda si è adeguata al GDPR?

- ☐ A: L'azienda non si è ancora adeguata alla normativa GDPR.
- ☐ B: L'azienda si è adeguata al GDPR, ma le informative non sono aggiornate alle ultime modifiche.
- ☐ C: Un gruppo dedicato, supportato da consulenti esterni, si occupa della gestione dei dati e del rispetto del GDPR.
- ☐ D: L'azienda si è adeguata alla normativa e mantiene aggiornate le informative.
- ☐ E: Non sono sicuro se l'azienda si sia adeguata al GDPR.

MONITORAGGIO NORMATIVA
È importante monitorare le normative, sia generali che specifiche per il settore aziendale, per garantire la conformità e ridurre i rischi legali.

Come viene gestito il monitoraggio delle normative nella vostra azienda?

- ☐ A: Non esiste una funzione dedicata al monitoraggio delle normative.
- ☐ B: Il monitoraggio è gestito da uno studio di consulenza esterno.
- ☐ C: È stato creato un ufficio apposito per monitorare le normative.
- ☐ D: È stato istituito un ente interno che collabora con uno studio di consulenza esterno.
- ☐ E: Prevediamo di inserire a breve una figura dedicata al monitoraggio delle normative.

CONFORMITÀ ISO/IEC 27001
La norma ISO/IEC 27001 è uno standard internazionale che aiuta le aziende a proteggere le informazioni all'interno dei processi aziendali. La certificazione può migliorare la compliance e la gestione della sicurezza.

La vostra azienda ha implementato un sistema di gestione conforme alla norma ISO/IEC 27001?

- ☐ A: Al momento no.
- ☐ B: Abbiamo definito l'ambito e stiamo per certificare il sistema.
- ☐ C: Abbiamo iniziato a lavorare sulle procedure per implementare il sistema.
- ☐ D: Stiamo implementando alcuni punti di controllo previsti dalla norma.
- ☐ E: Abbiamo un sistema di gestione certificato e sottoposto a audit.

VALUTAZIONE DEL RISCHIO
Le norme prevedono la valutazione del rischio in alcuni ambiti, come la sicurezza fisica e la privacy. È importante verificare la compliance anche in ambiti non obbligatori.

Qual è la situazione attuale della vostra azienda riguardo la valutazione dei rischi?

- ☐ A: Non saprei.
- ☐ B: Viene monitorato solo il rischio legato agli obblighi di legge.
- ☐ C: Stiamo iniziando a valutare anche rischi non legati agli obblighi di legge.
- ☐ D: Sono state fatte alcune analisi di rischio, ma non regolarmente.
- ☐ E: Abbiamo procedure definite per la valutazione periodica dei rischi, anche oltre quelli obbligatori.

ESECUZIONE AUDIT

Gli audit interni ed esterni sono fondamentali per verificare che le misure di sicurezza siano adeguate e rispettino le normative e gli standard ISO.

Sono previsti audit periodici nella vostra azienda?

- ☐ A: Sono previsti audit interni periodici e continuativi.
- ☐ B: Non sono previsti audit.
- ☐ C: Sono previsti audit interni su richiesta di clienti esterni.
- ☐ D: Sono previsti audit interni, oltre a quelli degli enti di certificazione ISO.
- ☐ E: L'azienda è certificata ISO e sono previsti audit anche per i fornitori.

FATTORE UMANO

La cultura aziendale in materia di cybersecurity è essenziale. La formazione e la sensibilizzazione dei dipendenti aiutano a ridurre il rischio di errori umani.

FORMAZIONE E SENSIBILIZZAZIONE

La formazione è fondamentale perché il personale abbia le competenze per acquisire, configurare, mantenere, usare e dismettere gli strumenti di sicurezza. Formazione e sensibilizzazione servono affinché il personale conosca le procedure da seguire, incluse quelle per il corretto uso degli strumenti di sicurezza e quelle relative ai processi (p.e. di gestione delle autorizzazione e di gestione degli incidenti). La le attività di sensibilizzazione hanno l'obiettivo di convincere il personale della necessità di assicurare la sicurezza delle informazioni e degli strumenti informatici, affinché la loro attenzione sia sempre elevata e non commettano errori (per es., fornire la password a estranei).

Come viene gestita la formazione e sensibilizzazione sulla sicurezza informatica nella vostra azienda?

- ☐ A: Non sono previste attività di formazione o sensibilizzazione.
- ☐ B: È prevista una presentazione delle procedure di sicurezza al momento dell'assunzione.
- ☐ C: È sviluppato un piano di formazione per il personale tecnico, con verifica delle certificazioni.
- ☐ D: È sviluppato e aggiornato periodicamente un piano di formazione personalizzato per ogni ruolo.
- ☐ E: Sono previste attività di sensibilizzazione continue e verifiche periodiche del rispetto delle regole di sicurezza.

RUOLI E RESPONSABILITÀ

Un’organizzazione chiara e ben definita dei ruoli in tema di sicurezza è fondamentale per evitare conflitti di interesse e garantire l'efficienza dei processi.

Sono stati formalmente assegnati i ruoli e le responsabilità legati alla sicurezza informatica nella vostra azienda?

- ☐ A: Le responsabilità sono state formalmente assegnate al responsabile IT.
- ☐ B: Le responsabilità non sono ancora pienamente stabilite.
- ☐ C: Le responsabilità sono state assegnate informalmente a una o più persone.
- ☐ D: Le responsabilità sono state assegnate a più persone, oltre al responsabile IT.
- ☐ E: Oltre a quanto sopra, è presente una figura indipendente dall'IT incaricata di monitorare le misure di sicurezza.

GESTIONE REGOLE

Per garantire la sicurezza delle informazioni vanno fornite al personale regole e istruzioni su come comportarsi, come trattare le informazioni e come gestire gli strumenti in uso.

Questo è importante soprattutto quando le attività:

- ☐ a) sono svolte da più persone;
- ☐ b) sono svolte raramente e, pertanto, il modo di procedere potrebbe essere dimenticato;
- ☐ c) sono nuove e il personale necessita supporto per svolgerle in modo corretto.

Tali regole e istruzioni potrebbero essere date in forma orale. Questo però non ne garantirebbe la corretta comprensione, l'omogenea attuazione e il sistematico riesame periodico; e quindi necessario prevedere alcuni documenti scritti.

Nella tua azienda sono presenti regole di sicurezza informatica? Come sono distribuite e aggiornate?

- ☐ A Sono presenti regole comportamentali per tutto il personale e sono descritti i processi di sicurezza coordinati tra loro. La distribuzione avviene a tutto il personale. È prevista una verifica periodica dei documenti
- ☐ B Sono presenti regole comportamentali per il personale e sono descritti alcuni processi di sicurezza (per es., gestione degli incidenti, sviluppo applicazioni), ma non coordinati tra loro. Non è presente una distribuzione controllata dei documenti a tutto
- ☐ C Ci sono alcune regole scritte, ma non coordinate tra loro e senza una distribuzione controllata a tutto il personale e una verifica periodica per assicurarne l'aggiornamento.
- ☐ D Non ci sono regole scritte.
- ☐ E Sono presenti regole comportamentali per il personale e sono descritti alcuni processi di sicurezza, ma non coordinati tra loro. il personale e verifiche periodiche.

GESTIONE AUTORIZZAZIONI

La corretta gestione delle autorizzazioni è cruciale per limitare l'accesso a informazioni sensibili e sistemi aziendali solo a chi ne ha necessità.

Come vengono assegnate le autorizzazioni nella vostra azienda?

- ☐ A: Le autorizzazioni sono assegnate tramite un processo informale.
- ☐ B: Le autorizzazioni sono assegnate dall'IT senza un controllo formale da parte delle HR.
- ☐ C: I sistemi sono censiti e sono identificati i responsabili per le richieste di accesso.
- ☐ D: Le HR comunicano tempestivamente gli ingressi e le uscite del personale per attivare o disabilitare le autorizzazioni.
- ☐ E: È previsto un riesame periodico delle autorizzazioni, con scadenze precise per il personale esterno.

PARTECIPAZIONE AD ASSOCIAZIONI

Il personale tecnico deve mantenersi aggiornato anche partecipando ad associazioni e gruppi di interesse (p.e. Clusit, AIEA, ISACA, AIPSI, ISC2), che mettono a disposizione newsletter, riviste e siti web e organizzano convegni ed eventi finalizzati all'aggiornamento tecnico e professionale.

L'azienda dovrebbe incentivare queste iniziative, provvedendo direttamente al pagamento degli esami per ottenere i certificati, degli abbonamenti, delle iscrizioni ai corsi di formazione e alle associazioni professionali e degli eventuali viaggi.

La tua azienda partecipa a qualcuno di questi enti e/o prende parte a eventi/convegni da loro organizzati?

- ☐ A Il personale è invitato a partecipare a convegni ed eventi di sicurezza a livello personale e l'azienda non ha stabilito un budget per queste iniziative.
- ☐ B L'azienda è iscritta ad associazioni che si occupano di sicurezza e il personale partecipa alle iniziative a nome dell'azienda stessa. L'azienda ha stabilito un budget per queste iniziative.
- ☐ C L'azienda è iscritta ad associazioni che si occupano di sicurezza e il personale partecipa alle iniziative a nome dell'azienda stessa. L'azienda ha stabilito un budget per queste iniziative; inoltre l'azienda partecipa attivamente alle attività ricerca.
- ☐ D Il personale è invitato a partecipare a convegni ed eventi di sicurezza a livello personale, con supporto economico da parte dell'azienda.
- ☐ E Non è previsto alcun contatto con associazioni e gruppi di interesse.