Approccio ciclico alla governance della sicurezza informatica



In un contesto digitale in continua evoluzione, caratterizzato dall'esplosione dei dati, e dalla crescente sofisticazione delle minacce, la sicurezza informatica non può più essere concepita come un progetto isolato o come un insieme statico di policy da aggiornare saltuariamente. I rischi di cybersecurity esistono in ogni fase del ciclo di vita di un dispositivo, dalle fasi di produzione, distribuzione, implementazione e messa in servizio, fino alla disattivazione. Diventa, invece, imprescindibile adottare un approccio ciclico, capace di integrare la gestione della sicurezza in un processo costante di miglioramento e adattamento.

Governare la sicurezza attraverso cicli ricorsivi consente non solo di rispondere efficacemente alle minacce emergenti, ma anche di anticiparle, costruendo un'infrastruttura resiliente e adattiva. Il cuore di questa filosofia risiede nella capacità di pianificare, agire e correggere costantemente le strategie di sicurezza, secondo principi ormai consolidati in ambito organizzativo e qualitativo.

Il ciclo PDCA (Plan-Do-Check-Act) nella gestione della governance della sicurezza informatica

Il ciclo PDCA rappresenta uno dei modelli più efficaci per strutturare un sistema di governance della sicurezza informatica dinamico e reattivo. Il ciclo di Deming **(PDCA, Plan-Do-Check-Act, Pianificare-Fare-Verificare-Agire)** è un

metodo di gestione utilizzato per il controllo e il miglioramento continuo dei processi e dei prodotti. Nato nell'ambito del Total Quality Management, questo approccio ha trovato una naturale applicazione anche nella gestione della sicurezza.

Questo modello si basa sull'idea che il raggiungimento dei più elevati standard di qualità richieda una continua interazione tra le fasi di ricerca, progettazione, test, produzione e commercializzazione. Nell'ambito dei sistemi di gestione, la sua implementazione risulta ancora più naturale: il metodo, infatti, si integra armoniosamente con il normale ciclo operativo dei sistemi, senza introdurre complessità aggiuntive e, anzi, contribuendo a valorizzarli in maniera semplice ed efficace.

Nella fase di **pianificazione (Plan)**, si analizzano i rischi, si individuano le vulnerabilità più critiche e si stabiliscono obiettivi concreti e misurabili per la sicurezza. Pianificare non significa soltanto elencare controlli tecnici da implementare, ma anche definire strategie di lungo periodo, politiche di compliance normativa e piani di formazione per il personale. È un momento in cui l'analisi del contesto interno ed esterno diventa fondamentale per determinare priorità e allocazione delle risorse.

La fase di **attuazione (Do)** traduce le strategie in azioni concrete: implementazione di firewall, sistemi di protezione endpoint, soluzioni SIEM, configurazione di backup sicuri e procedure operative di sicurezza. L'esecuzione non si limita alla tecnologia; coinvolge anche la gestione delle identità e degli accessi, la sensibilizzazione degli utenti e l'applicazione delle policy aziendali nella pratica quotidiana.

Successivamente, attraverso la fase di **verifica (Check)**, si misura l'efficacia degli interventi adottati. Questa fase implica il monitoraggio ininterrotto degli eventi di

sicurezza, l’analisi dei log, lo svolgimento di audit interni e la conduzione di simulazioni di incidenti per testare la reattività dei sistemi e del personale. Verificare consente di comprendere se le soluzioni implementate rispondono efficacemente alle minacce reali o se occorrono correttivi.

Infine, nella fase di **azione (Act)**, si introducono modifiche correttive e migliorative sulla base delle evidenze raccolte. In questa fase si aggiornano le policy, si ridefiniscono gli standard, si migliorano i sistemi di rilevazione e risposta e si pianificano nuove iniziative di formazione. Il ciclo si chiude, per riaprirsi immediatamente in un’ottica di miglioramento progressivo.

Strategie di governance della sicurezza informatica e valutazione dei rischi

I sistemi di gestione della sicurezza, ispirati a un modello ricorsivo che richiama il ciclo di Deming, sono strutturati con l’obiettivo di promuovere un costante miglioramento delle condizioni di lavoro. Questi sistemi si articolano, generalmente, attraverso alcune componenti fondamentali.

In primo luogo, viene elaborata una politica aziendale che orienta le decisioni in materia di sicurezza e salute sul lavoro (SSL), definendo gli obiettivi strategici principali. Segue una scrupolosa valutazione dei rischi associati all’ambiente di lavoro, alla quale si collega una pianificazione dettagliata delle attività preventive e protettive da adottare.

Vengono poi stabiliti obiettivi specifici, supportati da un programma operativo volto alla loro concreta attuazione. Contestualmente, si definisce una struttura organizzativa chiara, con ruoli, compiti e responsabilità affidati a

personale adeguatamente formato e competente.

Un ulteriore elemento essenziale è rappresentato dalla predisposizione di procedure operative, mirate a gestire le attività che presentano particolari rischi per la sicurezza. Il successo del sistema dipende anche dal coinvolgimento costante dei lavoratori e dei loro rappresentanti, ai quali viene riconosciuto un ruolo attivo.

La fase di controllo prevede il monitoraggio regolare dell'intero sistema, attraverso verifiche ispettive e audit periodici, per valutare il grado di efficacia delle misure adottate. Infine, viene promossa una revisione sistematica dell'intero modello gestionale, allo scopo di correggere eventuali criticità e individuare nuove opportunità di miglioramento.

Applicare il ciclo PDCA alla governance della sicurezza informatica consente alle organizzazioni di non cristallizzarsi su procedure obsolete, ma di mantenere un'attenzione costante sull'efficacia e l'attualità dei propri presidi difensivi.

Valutazione continua delle politiche di sicurezza IT

Uno dei pilastri dell'approccio ciclico è la consapevolezza che le politiche di sicurezza IT non possono essere statiche. Le policy definite in fase di avvio di un progetto o di una nuova infrastruttura tecnologica rischiano di diventare rapidamente obsolete se non sottoposte a una costante attività di revisione critica. Ancora, va detto che le fasi del ciclo PDCA, iterative, sono vitali per controllare e migliorare processi e prodotti in modo costante.

La **valutazione continua delle politiche di sicurezza** impone un'analisi sistematica della loro **adeguatezza rispetto a tre**

vettori principali di cambiamento: l’evoluzione tecnologica, i mutamenti organizzativi e il contesto normativo.

Sul versante tecnologico, l’adozione di architetture **cloud**, l’integrazione di dispositivi **IoT** e la pervasività del **lavoro da remoto** rappresentano esempi concreti di fattori che impongono un ripensamento strutturale delle policy esistenti. Una policy di sicurezza pensata per una rete aziendale chiusa potrebbe risultare del tutto inefficace in un ambiente distribuito su più cloud provider, in cui i confini perimetrali risultano sfumati e i dispositivi di accesso sono molteplici e diversificati.

Dal punto di vista organizzativo, ristrutturazioni aziendali, fusioni, nuove strategie di business o l’introduzione di modelli di lavoro ibridi richiedono aggiornamenti tempestivi delle politiche di sicurezza, pena il rischio di esposizioni incontrollate o lacune procedurali.

Un aspetto critico troppo spesso sottovalutato riguarda la **comprensione** e la **concreta applicazione** delle norme da parte del personale.

A questo scopo, strumenti come i **test di awareness** periodici, i **simulatori di phishing**, le **sessioni di formazione continua** e gli **audit di conformità interni** risultano fondamentali. Essi consentono di misurare il livello di consapevolezza degli utenti, di individuare aree di debolezza e di correggere comportamenti non conformi prima che questi si traducano in violazioni di sicurezza reali.

Parallelamente, l’analisi dei **report di incidenti** e degli eventi anomali fornisce un feedback oggettivo sull’efficacia operativa delle policy: la frequenza, il tipo e l’impatto degli incidenti possono infatti rivelare criticità non emerse nella fase di progettazione normativa.

Un ulteriore livello di complessità nella valutazione continua delle politiche di sicurezza è rappresentato dal **contesto**

normativo. In particolare, l'introduzione di normative come il **GDPR** (General Data Protection Regulation), la direttiva europea **NIS2** sulla sicurezza delle reti e dei sistemi informativi, e le specifiche regolamentazioni settoriali nel campo **sanitario** e **finanziario**, impone un approccio ancora più rigoroso e proattivo.

Non basta infatti adeguare le policy sulla base delle best practice: è necessario **anticipare** i requisiti di compliance, integrando tempestivamente nel proprio framework di governance tutti gli aggiornamenti normativi rilevanti. Questo richiede una costante attività di monitoraggio regolatorio, una collaborazione stretta tra le funzioni IT e legali, e una capacità di adattamento rapido dei sistemi di gestione.

Possiamo concludere affermando che l'adozione di un processo circolare e metodico di revisione delle politiche di sicurezza genera una serie di benefici strategici:

- **Miglioramento della resilienza**: le organizzazioni si dotano di un sistema capace di evolvere insieme alle minacce, riducendo il rischio di incidenti critici.
- **Ottimizzazione della compliance**: il rischio di non conformità normativa e di conseguenti sanzioni viene drasticamente ridotto.
- **Aumento della cultura aziendale della sicurezza**: la sicurezza viene percepita non come un obbligo imposto, ma come una responsabilità condivisa e interiorizzata a tutti i livelli.
- **Protezione della reputazione**: una governance della sicurezza dinamica e trasparente rafforza la fiducia di clienti, partner e investitori.

Adattamento alle nuove minacce

nella governance della sicurezza informatica

La gestione della sicurezza informatica non può prescindere dalla capacità di **adattarsi rapidamente** a un panorama di minacce in continua evoluzione. Gli attaccanti sviluppano tecniche sempre più avanzate: dagli attacchi ransomware-as-a-service alle minacce avanzate persistenti (APT), dai malware polimorfici ai nuovi vettori di attacco sui sistemi di intelligenza artificiale.

In questo scenario, adottare un approccio ciclico significa anche essere costantemente aggiornati sulle nuove vulnerabilità scoperte e sulle tecniche emergenti. L'integrazione di strumenti di threat intelligence all'interno della strategia di governance è oggi un requisito imprescindibile per ottenere una visione aggiornata del rischio.

In un processo ricorsivo, i dati di threat intelligence alimentano le fasi di **pianificazione e verifica** del modello PDCA, consentendo una continua riallocazione delle risorse di sicurezza sulle minacce realmente rilevanti per il contesto specifico dell'organizzazione.

Altrettanto centrale è la capacità di **individuare e correggere tempestivamente le vulnerabilità esistenti** all'interno dell'infrastruttura. Una gestione efficace delle vulnerabilità non può basarsi su interventi occasionali o su analisi una tantum. Deve essere fondata su:

- **vulnerability assessment periodici**, che esplorano l'intero ecosistema IT e OT;
- **patch management strutturato**, con processi agili e trasparenti per l'applicazione degli aggiornamenti;
- **prioritizzazione basata sul rischio**, sfruttando metriche come il CVSS (Common Vulnerability Scoring System), ma

anche considerando il contesto specifico di esposizione e impatto operativo.

In questa ottica, l'automazione gioca un ruolo fondamentale: sistemi di **vulnerability scanning integrati nei pipeline CI/CD**, soluzioni di **patching automatico**, e **dashboard di risk-based prioritization** permettono di trasformare un'attività reattiva in un processo continuo e scalabile.

L'adattamento, tuttavia, non riguarda solo la tecnologia. Il **fattore umano** continua a rappresentare l'anello debole della catena della sicurezza. Phishing, ingegneria sociale, frodi BEC (Business E-mail Compromise) e attacchi su misura puntano a sfruttare comportamenti prevedibili, abitudini consolidate o semplici errori umani.

Per questo motivo, ogni strategia di sicurezza deve includere **programmi di formazione e awareness** personalizzati, aggiornati e, soprattutto, ciclici. Non basta un corso annuale di compliance: servono simulazioni reali, test non annunciati, coinvolgimento attivo e feedback continui per trasformare la consapevolezza in prassi operative.

La cultura della sicurezza, infatti, si costruisce solo nel tempo e attraverso un impegno costante, che coinvolge tutti i livelli aziendali.

In un processo ricorsivo e orientato al miglioramento costante, **gli incidenti di sicurezza non rappresentano solo eventi da contenere**, ma **opportunità preziose di apprendimento e rafforzamento**.

L'analisi post-mortem (o post-incident analysis), condotta attraverso strumenti di forensic analysis e root cause analysis, consente di:

- identificare i **punti di ingresso** e le vulnerabilità sfruttate;
- mappare le **lacune nelle policy o nei controlli**

esistenti;
- riformulare processi, procedure e meccanismi di monitoraggio;
- aggiornare tempestivamente il framework di governance.

In questo modo, ogni attacco respinto o subìto alimenta un circolo virtuoso di **resilienza progressiva**, in cui l'organizzazione diventa progressivamente più capace di fronteggiare anche scenari imprevisti.

Coinvolgimento del top management nel ciclo di governance della sicurezza informatica

Perché la strategia a ciclo continuo alla sicurezza informatica sia veramente efficace, è imprescindibile il **coinvolgimento diretto del top management**. La governance della sicurezza non può essere delegata esclusivamente alle funzioni IT, ma deve diventare una responsabilità condivisa a livello di direzione strategica. I manager prendono **decisioni operative di routine** e gestiscono tutto il lavoro amministrativo che fa funzionare le operazioni.

Il management è praticamente **il collegamento tra la corporate governance e i dirigenti di livello inferiore**. Uno dei compiti fondamentali del management è tradurre e trasmettere in modo efficace le direttive e le aspettative espresse dal Consiglio di amministrazione ai livelli operativi dell'organizzazione.

Per farlo, i dirigenti hanno il compito di declinare tali aspettative in obiettivi concreti, sia di breve che di lungo periodo, assicurandosi che vengano implementati coerentemente lungo tutta la catena operativa fino alla loro piena realizzazione.

Sebbene spetti al Consiglio di amministrazione definire le linee guida e le politiche aziendali, è il management a

detenere la responsabilità della loro attuazione operativa e del controllo sull'adesione da parte dei dipendenti.

Per assolvere efficacemente a questo compito, i manager devono possedere un insieme di competenze specifiche e distintive, che differiscono in modo sostanziale da quelle richieste ai membri del consiglio.

Il supporto del top management si traduce in diversi ambiti concreti: la definizione di una chiara vision di cybersecurity, l'allocazione di budget adeguati, la promozione di una cultura della sicurezza che permei tutta l'organizzazione. È fondamentale che il Consiglio di amministrazione o i comitati di gestione ricevano regolarmente report dettagliati sullo stato della sicurezza, sui principali rischi individuati e sulle misure adottate.

La presenza di figure apicali dedicate, come il Chief Information Security Officer (CISO), che riportano direttamente al top management, rappresenta una best practice sempre più consolidata. Tali figure fungono da trait d'union tra gli aspetti tecnici della sicurezza e la strategia aziendale complessiva, facilitando l'integrazione della cybersecurity negli obiettivi di business.

Inoltre, il coinvolgimento dei vertici è cruciale nei momenti di crisi. In caso di violazioni o incidenti gravi, il top management deve essere pronto a partecipare attivamente alla gestione della crisi, coordinando la comunicazione interna ed esterna e assumendo decisioni rapide ed efficaci.

Tutte le organizzazioni necessitano sia di **funzioni di governance** che di **gestione** e spetta a ciascuna singola organizzazione garantire che entrambe le funzioni siano attive.

In un ciclo di governance maturo, i leader aziendali non sono meri destinatari di report, ma partecipano attivamente alla definizione e revisione delle strategie di sicurezza,

contribuendo a creare un ambiente organizzativo resiliente e reattivo.

Conclusioni

Adottare un **approccio ciclico alla governance della sicurezza informatica** non è più una scelta facoltativa, ma una necessità strategica per ogni organizzazione che voglia prosperare in un ecosistema digitale complesso e in continua evoluzione.

Attraverso l’applicazione rigorosa del ciclo PDCA, la valutazione continua delle politiche di sicurezza, l’adattamento dinamico alle nuove minacce e il coinvolgimento attivo del top management, è possibile costruire un sistema di difesa resiliente, capace non solo di resistere agli attacchi, ma anche di evolversi e migliorare nel tempo.

La sicurezza, in quest’ottica, non è un traguardo, ma un percorso di crescita continua che richiede attenzione, competenza e leadership a ogni livello organizzativo.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/governance-della-sicurezza-informatica/