Cyber Security
& Digital Transformation

www.dbi.srl


Digital Transformation
Porta la Tua Azienda nel Futuro. Oggi!
SCOPRI COME
oppure inizia adesso!

Cyber Security e Digital Transformation

La Digital Transformation impone alle Aziende una trasformazione radicale del loro modo di relazionarsi con il mondo esterno.

Digitali e Connesse, le Aziende 4.0 devono aprire i loro Sistemi Informatici per consentire **l'interoperabilità** nello scambio di flussi informativi con i Clienti, Fornitori e Partner.

Devono trattare le informazioni ricorrendo sempre più alla **digitalizzazione dei processi** ed alla dematerializzazione.

Queste sfide impongono un nuovo livello di considerazione della Sicurezza Informatica Aziendale non più limitata alla semplice gestione delle intrusioni oppure alla protezione dai virus informatici o alle copie di sicurezza.

Bisogna **evolvere** il livello di attenzione alla Cyber Security impostando delle strategie di sicurezza più complesse e sofisticate.

Le Strategie Proattive e Reattive

Per evolvere il livello di Sicurezza Informatica dell'Azienda dobbiamo far ricorso ad un approccio programmatico e preventivo che consenta di delineare a priori le strategie di gestione degli incidenti.

Riteniamo importante la fase di valutazione preliminare dei rischi potenziali attraverso la compilazione ed il costante aggiornamento del **Cyber Risk Assessment** che ascriveremo alle azioni **Proattive**.

Non di meno la fase **Reattiva** di gestione dell'eventuale incidente non può essere affrontata dopo l'occorrenza. Bisogne preventivamente pianificarne l'impatto attraverso la compilazione e l'aggiornamento costante del **Cyber Emergency Response Plan**.

Entrambi i documenti sono il punto di arrivo di una serie di valutazioni approfondite frutto di un procedimento cognitivo del management circa le problematiche relative alla Sicurezza Informatica.

Sicurezza Proattiva: Cyber Risk Assessment

Se conosciamo il nostro nemico abbiamo maggiori possibilità di batterlo. Questo è il senso dell'analisi preventiva da effettuare attraverso il Cyber Risk Assessment.

Il documento frutto della fase di identificazione, valutazione e gestione, consentirà di **mappare nel dettaglio** tutte le tipologie di rischio incombenti sull'attività aziendale ed il relativo peso in termini di danno procurato.

Andrà creato un Team qualificato con risorse interne e consulenti esterni per la stesura iniziale mentre il monitoraggio potrà essere effettuato dalle risorse interne con verifiche periodiche.

Dovranno essere **mappati tutti i punti critici** di tutti i sistemi informatici, le modalità di connessione, il livello di danno potenziale ed i cambiamenti necessari per renderli sicuri.

Si procederà alla programmazione degli interventi strutturali necessari per rendere **ragionevolmente** sicuri i Sistemi Informatici.

Sicurezza Reattiva: Cyber Emergency Response Plan

Dopo aver impostato le misure preventive, analizzate le minacce e mappati i rischi, occorre programmare le azioni conseguenti ad eventuali incidenti che, all'occorrenza, possono capitare.

Questa fase che ascriveremo al **Processo Reattivo**, viene definita ed esplicitata nel Cyber Emergency Response Plan.

Il documento prodotto conterrà le azioni da intraprendere in caso di incidente relativo alla Cyber Security.

Esso guiderà l'Azienda nel trattamento di eventuali data breach o intrusioni non autorizzate.

Andrà compilato successivamente al Cyber Risk Assessment e sarà prodotto dallo stesso Team di lavoro.

Entrambi i documenti andranno **sincronizzati** per acquisire contemporaneamente gli eventuali aggiornamenti.

Cyber Security e Cloud Aziendale

Dopo aver soddisfatto la fase preventiva di programmazione della Sicurezza Informatica, andranno valutate le caratteristiche dell'infrastruttura informatica per verificarne la migrazione verso il Cloud Aziendale di parte di essa.

Il Cloud oggi rappresenta una scelta opportuna per acquisire in modo indotto molte delle pratiche efficaci per la sicurezza.

I maggiori provider di Servizi Cloud progettano i loro Data Center in modalità **Secured by Design**; ovvero la Sicurezza Informatica viene progettata dall'inizio e non viene vista come un accessorio alla fine.

Questo consente di delegare a terzi buona parte delle azioni necessarie alla salvaguardia dei dati premettendo una **efficace policy di gestione dell'autenticazione**.

Migrare parte dell'infrastruttura verso il Cloud permette all'Azienda di **concentrarsi sui propri processi** e non sulle pratiche tecnologiche.

Secured by Design: Sviluppo Software Agile

In un efficace piano di gestione della Sicurezza Informatica, inevitabilmente bisognerà mettere mano al software in quanto esso è il gestore delle informazioni.

Molti algoritmi dovranno essere riscritti in quanto risulteranno fallaci nel Cyber Risk Assessment. Occorrerà renderli sicuri dalla progettazione attraverso la modalità Secured by Design.

Ecco che diventa comodol'utilizzo del Processo di Sviluppo Software Agile con **iterazione dedicata**. Essendo un processo iterativo ed incrementale, si può dedicare un ciclo di iterazione solo alla sicurezza.

L'analisi dei Requisiti viene estesa alla sicurezza delle informazioni e l'ultimo ciclo iterativo viene utilizzato solo per le rilevazioni afferenti alla **protezione dei dati** e non solo alla loro manipolazione.

L'approccio Secured by Design nel software aiuta ad eliminare buona parte dei problemi di sicurezza relativi alle violazioni dei dati.

Secure by Design: RESTful APIs e OAuth 2.0

Per i componenti software di interoperabilità e cooperazione applicativa siano essi nel Cloud oppure in locale, sorgono problemi di autenticazione in quanto non possono essere aperti per tutti.

Ecco che può essere interessante l'utilizzo del protocollo OAuth nella sua ultima versione, la 2.0.
OAuth è un protocollo orientato all'autenticazione indotta con garanzia di accesso ma senza condivisione delle informazioni di autenticazione.

In parole semplici l'Azienda autorizza il software del fornitore Alpha ad accedere ai dati Beta senza mandargli il nome utente e password.

Utilizzando anche l'architettura REST - REpresentational State Transfer per i componenti di interoperabilità, otterremo notevoli vantaggi in termini di efficienza applicativa federando i componenti di cooperazione attraverso l'utilizzo di API Gateway.

RESTful APIs e OAuth 2.0 un trinomio **agile ed efficiente** per le esigenze di interoperabilità e cooperazione applicativa.

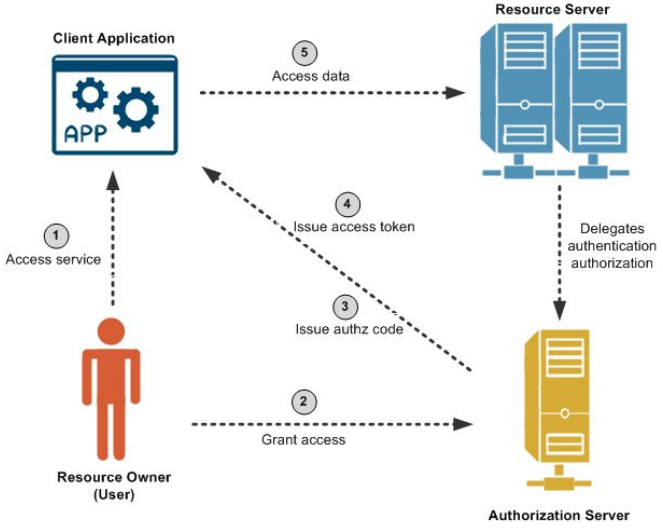

Immagine esemplificativa cortesia di Oracle

La Nostra Startup Innovativa: dbi.srl

Digital Business Innovation Srl in breve D.B.I. Srl è una Startup Innovativa riconosciuta ai sensi del DL 179/2012 Decreto Crescita 2.0, che nasce con delle competenze Multidisciplinari per accompagnare le Aziende nel processo di Digital Transformation con le App Aziendali, il Digital Marketing e la Consulenza Informatica Evolutiva.

www.dbi.srl

Digital Business Innovation Srl
Centro Direzionale is G/2
80143 - Napoli
P.IVA 08280231211
Iscrizione sezione speciale Startup Innovative NA 945395

Numero Verde Commerciale

800.589.889