



IL DILEMMA DELLA FIDUCIA DIGITALE

Cosa sono i **Remote Services** e come costruire una relazione sicura con il tuo fornitore

INDICE

Capitolo 1: *Introduzione ai Remote Services*

- Definizione e evoluzione dei remote services
- Tipologie principali (assistenza remota, monitoraggio, gestione sistemi)
- Vantaggi chiave per le aziende (riduzione costi, efficienza, scalabilità)
- Sfide comuni nell'adozione (sicurezza, resistenza al cambiamento)

Capitolo 2: *Implementazione pratica dei Remote Services*

- Valutazione delle esigenze aziendali e selezione dei servizi appropriati
- Infrastruttura necessaria e integrazione con i sistemi esistenti
- Best practices per l'implementazione
- Formazione del personale e gestione del cambiamento organizzativo

Capitolo 3: *Sicurezza e conformità*

- Protocolli di sicurezza essenziali (crittografia, autenticazione multifattore)
- Strategie per la protezione dei dati e gestione degli accessi
- Conformità alle normative rilevanti (GDPR, HIPAA, ecc.)
- Bilanciamento tra accesso remoto e controllo aziendale

Capitolo 4: *Costruire fiducia e gestire i fornitori*

- Il concetto di fiducia nel contesto dei remote services
- Criteri per la valutazione e selezione dei fornitori affidabili
- Negoziazione di contratti e SLA (Service Level Agreements)
- Stabilire una comunicazione efficace e monitorare le prestazioni

Capitolo 5: *Massimizzare il valore e prepararsi al futuro*

- Strategie per ottimizzare il ROI dei remote services
- Metriche chiave per monitorare l'efficacia dei remote services
- Tendenze emergenti nei remote services (AI, IoT, edge computing)
- Preparazione per l'evoluzione tecnologica e adattamento ai cambiamenti del mercato

Capitolo 6: *Casi di studio e best practices*

- Esempi reali di implementazioni di successo di remote services
 - Nice Footwear
 - Cabrellon srl
 - Officine Zoppelletto srl

Capitolo 1

INTRODUZIONE AI REMOTE SERVICES

1.1 Definizione ed evoluzione dei Remote Services

I Remote Services sono soluzioni che permettono la gestione, il monitoraggio e il supporto di sistemi IT a distanza, senza la necessità di interventi fisici sul posto. Inizialmente utilizzati principalmente per fornire assistenza tecnica da remoto, oggi coprono un ampio spettro di funzionalità, grazie alla crescente connettività e alle tecnologie digitali. L'evoluzione di strumenti come il cloud computing, le reti VPN sicure e le soluzioni di monitoraggio in tempo reale ha consentito di trasformare i servizi remoti in una componente essenziale per le aziende moderne.

La storia dei Remote Services è affascinante quanto la tecnologia stessa.

- **Era Pre-Internet (1980-1995):** quando i personal computer iniziavano a diffondersi nelle aziende, il supporto tecnico richiedeva inevitabilmente la presenza fisica di un tecnico.
- **Era Internet (1995-2010):** L'avvento di Internet ha segnato il primo grande cambiamento: improvvisamente, i tecnici potevano collegarsi ai sistemi aziendali attraverso connessioni remote, diagnosticare problemi e spesso risolverli in tempo reale.
- **Era Cloud (2010-presente):** La vera rivoluzione è arrivata con l'era del cloud computing. La possibilità di accedere a risorse computazionali praticamente illimitate attraverso Internet ha trasformato i Remote Services da semplici strumenti di supporto a complesse piattaforme di gestione integrata.

Oggi, grazie all'intelligenza artificiale e all'automazione, questi servizi non si limitano a risolvere problemi: li prevengono, ottimizzano le prestazioni dei sistemi e contribuiscono attivamente alla strategia digitale delle aziende.



1.2 Tipologie principali

Nel variegato ecosistema dei Remote Services, possiamo identificare tre macro-categorie che rispondono a diverse esigenze aziendali.

1. Assistenza Remota

- Help Desk virtuale: supporto tecnico in tempo reale
- Troubleshooting remoto: diagnosi e risoluzione problemi a distanza
- Assistenza proattiva: identificazione preventiva delle problematiche

2. Monitoraggio

- Performance Monitoring: controllo continuo delle prestazioni
- Security Monitoring: sorveglianza della sicurezza informatica
- Resource Monitoring: gestione delle risorse hardware e software

3. Gestione dei sistemi

- Amministrazione Server: gestione centralizzata dei server
- Network Management: controllo dell'infrastruttura di rete
- Updates & Patches: gestione automatizzata degli aggiornamenti

1.3 Vantaggi chiave per le aziende

1. Riduzione dei costi

- Minimizzazione degli interventi on-site
- Ottimizzazione delle risorse IT
- Riduzione dei tempi di inattività

2. Efficienza Operativa

- Risposta rapida agli incidenti
- Automazione dei processi di routine
- Gestione centralizzata delle risorse

3. Scalabilità

- Facilità di espansione dei servizi
- Adattabilità alle esigenze aziendali
- Flessibilità nell'implementazione



1.4 Sfide comuni nell'adozione

Nonostante i numerosi vantaggi, l'implementazione dei Remote Services non è priva di ostacoli.

1. Sicurezza

- Protezione degli accessi remoti
- Salvaguardia dei dati sensibili
- Gestione delle vulnerabilità

2. Resistenza al cambiamento

- Barriere organizzative
- Cultura aziendale tradizionale
- Timore della perdita di controllo
- Resistenza del personale

3. Sfide Tecniche

- Integrazione con sistemi legacy
- Requisiti di connettività
- Complessità dell'implementazione

Capitolo 2

IMPLEMENTAZIONE PRATICA DEI REMOTE SERVICES

2.1 Valutazione delle esigenze aziendali e selezione dei servizi appropriati

Per implementare efficacemente i Remote Services, la prima fase consiste in una valutazione approfondita delle necessità aziendali.

Ogni azienda ha, infatti, specifiche esigenze di supporto, monitoraggio e gestione remota che possono variare in base alla dimensione, al settore e alla maturità digitale dell'organizzazione.

- **Identificazione degli obiettivi:** è cruciale comprendere quali processi o sistemi necessitano di monitoraggio e supporto remoto. Ad esempio, per un'azienda in rapida crescita, la scalabilità e l'efficienza operativa potrebbero rappresentare priorità centrali.
- **Analisi costi-benefici:** è importante analizzare i costi dei servizi remoti rispetto ai benefici attesi, come la riduzione dei tempi di inattività e dei costi operativi.
- **Personalizzazione del servizio:** a seconda delle esigenze, sarà necessario scegliere tra diverse opzioni, come assistenza remota personalizzata o pacchetti standardizzati di monitoraggio.



2.2 Infrastruttura necessaria e integrazione con i sistemi esistenti

- **Reti e sicurezza:** è essenziale disporre di una rete affidabile e sicura, che permetta connessioni remote protette. Strumenti come VPN, firewall avanzati e segmentazione della rete aiutano a proteggere i dati e le comunicazioni.
 - **Compatibilità e interoperabilità:** spesso, le aziende hanno sistemi legacy che devono essere integrati con le nuove piattaforme di Remote Services. Questa fase richiede una valutazione tecnica per assicurarsi che i nuovi servizi possano funzionare senza problemi insieme ai sistemi preesistenti.
 - **Scalabilità e flessibilità:** la scelta dell'infrastruttura dovrebbe permettere una facile espansione dei servizi, in linea con la crescita futura dell'azienda.
-

2.3 Best Practices per l'implementazione

- **Pianificazione graduale:** iniziare con un progetto pilota consente di valutare il funzionamento del servizio e di risolvere eventuali problemi prima di un'implementazione su larga scala.
 - **Monitoraggio continuo:** stabilire un sistema di monitoraggio costante durante la fase di implementazione aiuta a individuare eventuali criticità e a ottimizzare il servizio in tempo reale.
 - **Gestione delle responsabilità:** definire chiaramente le responsabilità tra i fornitori di servizi e il team IT interno per evitare confusione e garantire che ogni aspetto dell'implementazione sia adeguatamente seguito.
-

2.4 Formazione del personale e gestione del cambiamento organizzativo

- **Formazione continua:** il personale IT e i dipendenti coinvolti devono essere addestrati per utilizzare correttamente le nuove tecnologie. La formazione dovrebbe includere sia aspetti tecnici che operativi, affinché tutti comprendano i vantaggi e le funzionalità del sistema.
- **Promuovere la cultura del cambiamento:** integrare i Remote Services richiede un cambiamento nella mentalità aziendale. È utile comunicare chiaramente i vantaggi e fornire supporto ai dipendenti per facilitare l'adozione delle nuove pratiche.
- **Supporto post-implementazione:** dopo l'implementazione, è fondamentale continuare a monitorare e ottimizzare il sistema. Inoltre, il feedback del personale può rivelarsi prezioso per apportare ulteriori miglioramenti.

Capitolo 3

SICUREZZA E CONFORMITÀ

3.1 Protocolli di sicurezza essenziali

Nel contesto dei remote services, la sicurezza dei dati aziendali è di importanza primaria. Ecco alcuni dei protocolli fondamentali per garantire la protezione durante le interazioni a distanza:

- **Crittografia:** è essenziale per proteggere i dati trasmessi attraverso connessioni remote. Utilizzando standard come l'Advanced Encryption Standard (AES), le informazioni sensibili sono cifrate sia durante la trasmissione che nel caso in cui siano archiviate temporaneamente.
- **Autenticazione multifattore (MFA):** questo sistema richiede un secondo livello di verifica per accedere ai sistemi, rendendo l'accesso molto più sicuro. L'implementazione moderna dell'MFA include:
 - **Qualcosa che si conosce:** questo primo fattore è una conoscenza dell'utente, come una password o un PIN, che è noto solo all'utente.
 - **Qualcosa che si possiede:** il secondo fattore è qualcosa di fisico in possesso dell'utente, come uno smartphone (per ricevere un codice via SMS o app di autenticazione) o un token hardware.
 - **Qualcosa che si è:** questo fattore si riferisce a caratteristiche biometriche dell'utente, come impronte digitali, riconoscimento facciale o scansione dell'iride.

Usati in combinazione, questi fattori aumentano la sicurezza poiché anche se uno venisse compromesso, gli altri due sarebbero ancora in grado di proteggere l'accesso.



3.2 Strategie per la protezione dei dati e la gestione degli accessi

Gestione granulare degli accessi

Il principio del privilegio minimo (Least Privilege Access) deve guidare ogni aspetto della gestione degli accessi remoti:

1. **Controllo degli accessi basato su ruoli (RBAC):** definire ruoli specifici per ogni utente consente di limitare l'accesso ai dati solo al personale che ne ha effettivamente bisogno, riducendo la possibilità di errori o accessi malevoli.
2. **Segmentazione delle reti:** la suddivisione dell'infrastruttura in zone isolate riduce la superficie d'attacco e limita potenziali danni in caso di violazione.
3. **Monitoraggio continuo:** implementazione di sistemi SIEM (Security Information and Event Management) per:
 - Tracciamento in tempo reale delle attività
 - Identificazione di pattern sospetti
 - Risposta automatizzata alle minacce
4. **Logging e audit:** tenere traccia delle attività svolte dai fornitori tramite logging accurato e audit periodici è fondamentale per verificare la conformità agli standard di sicurezza.

Protezione dell'endpoint

Anche la sicurezza dei dispositivi che accedono ai sistemi remoti è cruciale:

- Implementazione di soluzioni EDR (Endpoint Detection and Response)
- Gestione centralizzata degli aggiornamenti di sicurezza
- Politiche di ****hardening** dei sistemi

*** indica l'insieme di operazioni specifiche di configurazione di un dato sistema informatico (e dei suoi relativi componenti) che mirano a minimizzare l'impatto di possibili attacchi informatici*



3.3 Conformità alle normative rilevanti

Oltre alla protezione tecnica, i remote services devono essere conformi alle normative locali e internazionali, in particolare quelle che regolano la privacy dei dati. I principali framework da considerare sono:

GDPR: per le aziende in Europa, il General Data Protection Regulation richiede di proteggere i dati personali e gestire i flussi di informazioni tra azienda e fornitore in modo trasparente e sicuro.

ISO/IEC 27001: questa norma internazionale stabilisce i requisiti per un sistema di gestione della sicurezza delle informazioni, includendo le misure per l'accesso remoto e la protezione dei dati.

HIPAA: per le aziende che operano nel settore sanitario, il Health Insurance Portability and Accountability Act impone severe restrizioni su come le informazioni sanitarie devono essere trattate e protette.

NIST (National Institute of Standards and Technology): linee guida di riferimento dagli USA per best practices di cybersecurity, adottate anche in settori privati e pubblici a livello globale come supporto alla conformità normativa e alla protezione dei dati.

3.4 Bilanciamento tra accesso remoto e controllo aziendale

Per ottenere il massimo vantaggio dai remote services senza compromettere la sicurezza, è importante trovare un equilibrio tra la necessità di accesso dei fornitori e il controllo dell'azienda sui propri sistemi. Come?

1. **Verifica e autorizzazione preventiva:** prima di consentire accessi remoti, l'azienda può implementare processi di autorizzazione che richiedano una conferma da parte di un responsabile interno.
2. **Definizione di politiche di accesso e Service Level Agreement (SLA):** stabilire chiaramente nei contratti le regole di accesso e sicurezza, definendo un SLA che includa l'adozione di pratiche di sicurezza come quelle sopra indicate, assicurando trasparenza e controllo reciproco tra le parti.
3. **Politiche di revoca immediata:** in caso di necessità, le aziende devono essere in grado di revocare immediatamente l'accesso ai fornitori, ad esempio in caso di cambiamenti contrattuali o sospetti di sicurezza.

Capitolo 4

COSTRUIRE FIDUCIA E GESTIRE I FORNITORI

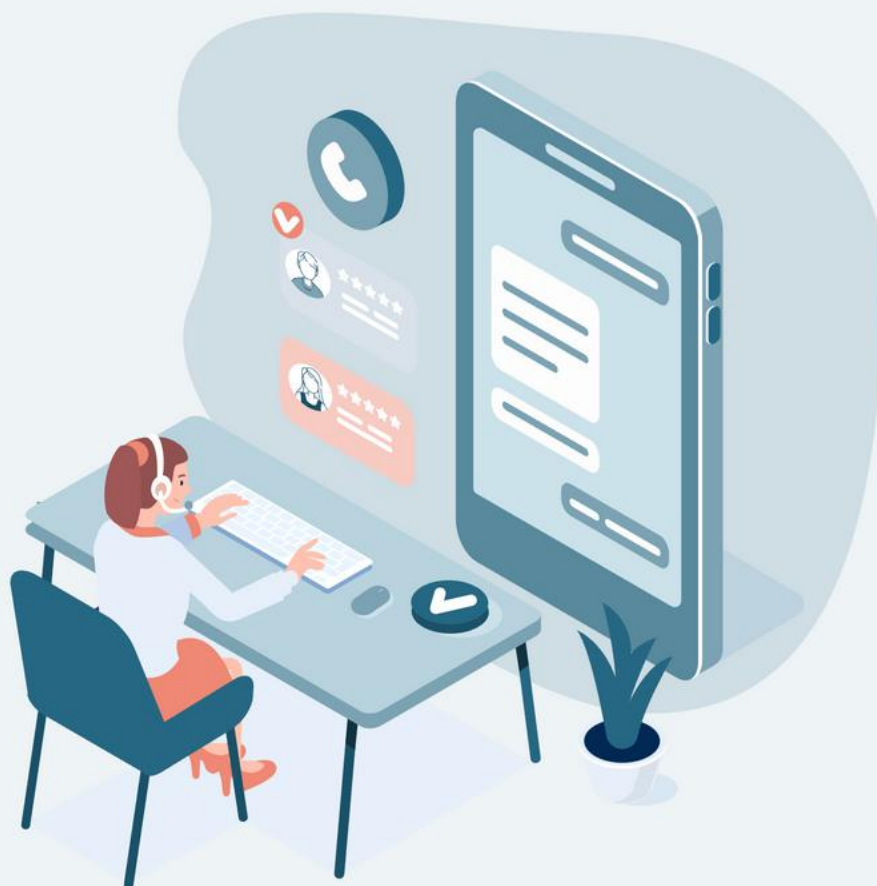
4.1 Il concetto di fiducia nel contesto dei remote services

La fiducia è l'ingrediente chiave per una relazione di successo tra un'azienda e il fornitore dei suoi servizi remoti. Quando si affida a terzi la gestione di componenti critiche della propria infrastruttura IT, l'organizzazione deve poter contare sulla dedizione, l'affidabilità e la competenza del partner.

In questo contesto, **la fiducia non è solo una questione di reputazione, ma si basa sulla trasparenza delle operazioni**, la capacità del fornitore di rispettare protocolli di sicurezza e l'attenzione per la riservatezza delle informazioni aziendali.

Le aziende, in particolare le PMI, affrontano sfide specifiche nell'affidarsi ai fornitori di remote services e devono adottare un approccio strategico per selezionare e mantenere un rapporto sicuro e vantaggioso con questi partner.





4.2 Criteri per la valutazione e selezione dei fornitori affidabili

La scelta del fornitore di servizi remoti è una decisione strategica che richiede un'attenta due diligence. Tra i principali fattori di valutazione troviamo:

1. **Competenze tecniche:** valutare il background, le certificazioni e le referenze del fornitore per verificare che disponga del know-how necessario a gestire in modo sicuro e performante l'infrastruttura IT.
2. **Esperienza nel settore:** preferire fornitori con una comprovata esperienza nella fornitura di remote services, in particolare nell'ambito del settore in cui opera l'azienda cliente.
3. **Compliance e certificazioni:** verificare che rispetti le normative di settore e sia in possesso di certificazioni rilevanti per la sicurezza delle informazioni.
4. **Flessibilità:** preferire provider in grado di adattarsi rapidamente ai cambiamenti e di proporre soluzioni innovative per massimizzare il valore dei remote services.
5. **Capacità di risposta e supporto:** valutare il livello di assistenza offerta, inclusa la disponibilità di supporto 24/7 in caso di necessità critiche.
6. **Feedback di altri clienti:** analizzare recensioni e testimonianze di clienti passati, chiedendo riferimenti diretti per comprendere meglio l'affidabilità del fornitore.

4.3 Negoziazione di contratti e SLA (Service Level Agreements)

Una volta identificato il fornitore più idoneo, la fase successiva è la definizione di un contratto che tuteli adeguatamente gli interessi di entrambe le parti. Gli elementi chiave da includere sono:

1. **Descrizione dettagliata dei servizi:** elencare in modo chiaro e preciso tutte le attività e i livelli di servizio garantiti dal fornitore, nonché gli standard di performance attesi. Stabilire metriche, obiettivi e penali per garantire il rispetto degli impegni assunti dal fornitore in termini di disponibilità, prestazioni, tempi di risposta, ecc.
2. **Gestione della sicurezza e della conformità:** definire in dettaglio le responsabilità del fornitore in ambito sicurezza informatica e conformità normativa, inclusi audit e reportistica periodica.
3. **Clausole di riservatezza e proprietà intellettuale:** tutelare adeguatamente i dati aziendali e l'ownership delle soluzioni sviluppate.
4. **Processi di revisione e aggiornamento:** inserire nel contratto la possibilità di revisionare e aggiornare i termini di servizio periodicamente, così da adattarli a nuove esigenze o cambiamenti nelle normative.
5. **Termini di recesso e rinnovo:** stabilire condizioni chiare per la rescissione del contratto e per il suo eventuale rinnovo.

4.4 Stabilire una comunicazione efficace e monitorare le prestazioni

Per mantenere una relazione di fiducia con il fornitore, è fondamentale instaurare canali di comunicazione aperti e trasparenti e monitorare costantemente le prestazioni del servizio.

1. **Reportistica dettagliata:** richiedere al fornitore una reportistica regolare e dettagliata che copra gli aspetti operativi, di sicurezza e di conformità. I report possono includere KPI (Key Performance Indicators) come tempi di risposta, incidenti gestiti e feedback dell'azienda cliente.
2. **Implementare strumenti di monitoraggio delle prestazioni in tempo reale:** utilizzare dashboard o piattaforme condivise che consentano di monitorare in tempo reale le attività del fornitore, agevolando l'identificazione tempestiva di potenziali criticità.
3. **Sistema di ticketing e incident management:** implementare procedure chiare per la gestione di incidenti e richieste di assistenza.

Capitolo 5

MASSIMIZZARE IL VALORE E PREPARARSI AL FUTURO

5.1 Strategie per ottimizzare il ROI dei remote services

Massimizzare il ritorno sull'investimento (ROI) dei remote services richiede l'adozione di strategie che permettano all'azienda di sfruttare pienamente i benefici di queste tecnologie.

L'ottimizzazione del ROI non significa, infatti, solo ridurre i costi, ma anche aumentare l'efficienza e migliorare la qualità dei servizi.

- **Monitorare le prestazioni:** definire metriche chiare per misurare l'efficacia dei servizi remoti aiuta a identificare le aree da migliorare e ottimizzare l'allocazione delle risorse.
- **Automatizzare i processi ricorrenti:** ridurre il carico di lavoro manuale nelle attività di routine libera risorse da destinare a progetti strategici, aumentando così la produttività.
- **Integrare i dati aziendali:** collegare i remote services agli altri sistemi aziendali centralizza le informazioni e facilita analisi più complete e decisioni più rapide.



5.2 Metriche chiave per monitorare l'efficacia dei remote services

1. **Tempo di Uptime:** la disponibilità continua dei sistemi è uno degli indicatori principali del successo dei remote services. Un alto tempo di uptime significa che i sistemi sono operativi e i servizi vengono erogati senza interruzioni.
2. **Tempo di Risoluzione (MTTR - Mean Time to Repair):** misura il tempo medio necessario per risolvere un problema tecnico. Una risposta rapida è cruciale per mantenere l'efficienza operativa.
3. **Tempo di Risposta:** indica la rapidità con cui il team di supporto remoto risponde ai problemi rilevati nei sistemi. Un tempo di risposta rapido aumenta la soddisfazione del cliente e riduce il rischio di interruzioni.
4. **Soddisfazione del Cliente (CSAT - Customer Satisfaction):** misurare la soddisfazione degli utenti attraverso sondaggi o feedback è essenziale per comprendere la qualità del servizio remoto offerto e identificare aree di miglioramento.
5. **Tasso di Risoluzione al Primo Contatto (FCR - First Contact Resolution):** misura la percentuale di problemi risolti al primo contatto con il supporto remoto. Un tasso elevato di FCR è segno di un servizio efficiente e ben organizzato.
6. **Tasso di Adesione alla SLA (Service Level Agreement):** Rappresenta la percentuale di volte in cui il servizio remoto rispetta gli accordi definiti nelle SLA. Un buon livello di conformità alle SLA indica un servizio affidabile e ben gestito.
7. **Numero di incidenti / Eventi di sicurezza:** monitorare la frequenza degli incidenti di sicurezza, come violazioni dei dati o attacchi informatici, aiuta a capire se i remote services sono abbastanza sicuri e protetti.
8. **Costi di gestione e manutenzione:** analizzare i costi associati è fondamentale per determinare l'efficienza economica dei servizi e per ottimizzare i costi operativi.



5.3 Tendenze emergenti nei remote services

Il settore dei remote services è in continua trasformazione, spinto da tecnologie come l'intelligenza artificiale, l'Internet of Things (IoT) e l'edge computing, che stanno ridefinendo i confini del possibile.

- **AI:** l'intelligenza artificiale permette di anticipare problemi grazie all'analisi predittiva, ottimizzando i servizi con un supporto sempre più proattivo.
- **IoT ed edge computing:** l'IoT amplifica le capacità di monitoraggio in tempo reale, mentre l'edge computing permette di elaborare i dati direttamente sul campo, riducendo la latenza e migliorando la sicurezza.

5.4 Prepararsi all'evoluzione tecnologica e adattarsi al cambiamento

Per restare competitive, le aziende devono essere pronte ad evolversi in risposta ai cambiamenti del mercato e all'avanzamento tecnologico. Un approccio flessibile permette di integrare rapidamente le novità e rispondere alle nuove esigenze in modo agile.

- **Aggiornamenti continui:** monitorare regolarmente le nuove tecnologie consente di adottare tempestivamente soluzioni più avanzate, mantenendo la propria infrastruttura all'avanguardia.
- **Formazione del personale:** preparare i team all'uso delle nuove tecnologie è fondamentale per assicurare una transizione fluida e senza intoppi.
- **Pianificazione a lungo termine:** stabilire una roadmap tecnologica aiuta a pianificare gli investimenti futuri, mantenendo l'infrastruttura aziendale in linea con gli obiettivi e le priorità strategiche.

Capitolo 6

CASI DI STUDIO E BEST PRACTICES

Esempi reali di implementazioni di successo
di remote services

NICE FOOTWEAR

Il Gruppo **Nice Footwear**, con sede a Padova, dal 2016 si occupa di creazione, sviluppo, produzione e distribuzione di calzature. Con passione, creatività e determinazione, gli “Shoe Trends Architects” dell’azienda contribuiscono a plasmare la moda e le sue tendenze, con un’impronta innovativa e all’avanguardia, riflessa nell’unicità dei loro prodotti. Dal 2021, con l’acquisizione di importanti eccellenze nella produzione di calzature ed accessori alto di gamma, sta perseguendo il proprio piano di sviluppo come aggregatore veneto di imprese manifatturiere.

*“La nostra partnership è stata
trasformativa.*

*La **modernizzazione** della
nostra infrastruttura IT non
solo ha **semplificato** le nostre
operazioni, ma ha anche
rafforzato il nostro impegno
verso la sostenibilità. La loro
competenza e **dedizione** sono
state cruciali per raggiungere
i nostri obiettivi.”*

CEO, Bruno Conterno



SFIDA

L'obiettivo dell'azienda era quello di migliorare i processi e la gestione della propria infrastruttura IT, in particolare riguardo a una serie di aspetti critici:

1. **Sistemi obsoleti:** sistemi IT datati causavano ritardi nello sviluppo e nella distribuzione dei prodotti.
2. **Dati isolati:** la mancanza di integrazione tra i dipartimenti ostacolava la collaborazione e le decisioni in tempo reale.
3. **Problemi di scalabilità:** la rapida crescita richiedeva soluzioni IT scalabili per supportare l'aumento delle operazioni e delle richieste dei clienti.
4. **Obiettivi di sostenibilità:** necessità di soluzioni IT in linea con le iniziative di sostenibilità, quali la riduzione del consumo energetico e la minimizzazione degli sprechi.

SOLUZIONE

Per raggiungere gli obiettivi, abbiamo avviato con il cliente una collaborazione che dura da diversi anni, adottando una strategia che si è concentrata su:

1. **Modernizzazione dell'infrastruttura IT**
2. **Integrazione dei sistemi**
3. **Soluzioni IT green**
4. **Supporto e manutenzione continuativi**

In dettaglio abbiamo fornito:

1. **Supporto al Cloud:** abbiamo implementato un'infrastruttura on-prem e cloud-based per sostituire i sistemi obsoleti e collegamenti sicuri alla piattaforma cloud, consentendo l'accesso remoto, l'analisi dei dati in tempo reale e una scalabilità conveniente.
2. **Applicazioni personalizzate:** abbiamo sviluppato soluzioni software su misura per il "Data Collaboration" integrate con il sistema ERP aziendale, per unificare le operazioni e migliorare il flusso di dati tra i dipartimenti, con soluzioni di file-sharing.
3. **Iniziative di sostenibilità:** utilizzo di hardware a basso consumo energetico e implementazione di programmi di ricambio tecnologico per le apparecchiature obsolete. Abbiamo introdotto server virtualizzati, riducendo la necessità di hardware fisico e il consumo energetico del 40%.
4. **Miglioramenti alla cybersecurity e supporto continuo:** abbiamo implementato soluzioni e protocolli di sicurezza Mamacloud tra i quali: Firewall con Total security suite, soluzione di Vulnerability Assessment e Penetration Testing, sistema di Disaster Recovery e Business Continuity, il tutto per proteggere i dati sensibili aziendali, dei clienti e dei prodotti. Attraverso la fornitura di supporto IT continuativo abbiamo garantito operazioni senza interruzioni.

RISULTATI

Grazie alle nostre soluzioni integrate, Nice Footwear può vantare il raggiungimento di importanti traguardi:

1. **Maggiore efficienza:** i cicli di sviluppo dei prodotti sono stati ridotti del 30%, consentendo un time-to-market più rapido.
2. **Collaborazione migliorata:** i sistemi integrati hanno facilitato una migliore comunicazione e coordinazione tra i dipartimenti.
3. **Scalabilità:** l'infrastruttura IT supporta ora la loro crescita, accogliendo un aumento del 50% delle operazioni.
4. **Risparmio sui costi:** l'ottimizzazione dei processi IT ha portato a una riduzione del 25% dei costi operativi.

CABRELLON SRL

Cabrellon srl, azienda vicentina fondata nel 1966 come officina artigianale, è oggi riconosciuta come leader mondiale nella produzione di stampi in policarbonato per il cioccolato.

Con oltre 55 anni di esperienza, l'azienda vanta una presenza internazionale e una reputazione consolidata per l'eccellenza dei suoi prodotti.

*“Grazie alla partnership con **CASH SRL-MAMACLOUD**, abbiamo **trasformato la nostra infrastruttura tecnologica** e reso la sicurezza informatica una priorità assoluta. Questo ci ha permesso di **mantenere il nostro vantaggio competitivo** e garantire ai nostri clienti standard qualitativi e di sicurezza eccellenti.”*

CFO, Patrizia Cabrellon



SFIDA

Con la crescita esponenziale del business e l'espansione verso mercati globali, l'azienda si è trovata di fronte a diverse sfide in ambito tecnologico:

- **Modernizzazione IT:** aggiornare infrastrutture obsolete per supportare le crescenti esigenze produttive e logistiche.
- **Cybersecurity:** proteggere dati sensibili relativi a clienti, fornitori e progetti di ricerca e sviluppo.
- **Continuità operativa:** garantire la massima operatività in un settore altamente competitivo e sensibile a eventuali interruzioni.

SOLUZIONE

Dopo una collaborazione lavorativa pluridecennale, dal 2017 abbiamo instaurato una partnership strategica con l'azienda per fornire soluzioni IT avanzate e servizi di cybersecurity. Le principali azioni intraprese includono:

1. **Assessment iniziale e piano di intervento**

- Analisi approfondita delle infrastrutture IT e dei sistemi di sicurezza esistenti.
- Progettazione di un piano di evoluzione tecnologica in linea con le esigenze aziendali.

2. **Modernizzazione dell'infrastruttura IT**

- Implementazione di server ad alte prestazioni per supportare i sistemi di progettazione CAD/CAM.
- Virtualizzazione delle risorse per ottimizzare la gestione dei carichi di lavoro.
- Aggiornamento delle reti aziendali per garantire una connessione stabile e veloce tra gli impianti di produzione e i restanti reparti/uffici.
- Adozione di un sistema telefonico e di comunicazione VoIP all'avanguardia

3. **Cybersecurity**

- Installazione di firewall di nuova generazione e sistemi avanzati di rilevamento delle intrusioni (IDS/IPS).
- Adozione di soluzioni di e-mail security e password management per tutti i dispositivi aziendali.
- Implementazione di backup criptati e piani di disaster recovery per garantire la resilienza contro eventuali attacchi ransomware.

4. **Formazione e sensibilizzazione del personale**

- Organizzazione di sessioni formative periodiche per aumentare la consapevolezza sui rischi informatici.

RISULTATI

Nel corso della nostra partnership pluriennale, l'azienda ha raggiunto importanti traguardi:

- **Riduzione dell'80%** degli incidenti legati alla sicurezza informatica.
- **Incremento del 50%** delle performance dei sistemi IT, con un impatto positivo sulla produttività.
- **Zero interruzioni** significative delle attività produttive grazie ai sistemi di continuità operativa implementati.

OFFICINE ZOPPELLETTO SRL

Officine Zoppelletto Srl è una storica realtà imprenditoriale del Vicentino, attiva nel settore della lavorazione della lamiera dal 1953. Con un complesso produttivo di 12.000 metri quadrati, l'azienda è dotata delle più avanzate tecnologie e di macchinari all'avanguardia per il taglio e la piegatura della lamiera. Il tratto distintivo è la capacità di garantire lavorazioni caratterizzate da elevata qualità e precisione, garantendo tempi di consegna rapidi.

Negli ultimi anni, Officine Zoppelletto ha registrato una significativa crescita, investendo in soluzioni tecnologiche 4.0, sia nel dipartimento di taglio che in quello di piegatura della lamiera. Questo progresso tecnologico, unito all'evoluzione delle minacce informatiche, ha reso necessario un aggiornamento delle infrastrutture IT e l'adozione di soluzioni avanzate di Cybersecurity. La nostra azienda è stata selezionata per soddisfare queste nuove esigenze, supportando Officine Zoppelletto nel rafforzamento della propria sicurezza digitale.

*"L'intervento del team di **Cash S.r.l** sulla cybersecurity è stato cruciale per il **rafforzamento della nostra infrastruttura IT** e per garantire la massima protezione dei nostri sistemi. Grazie alle soluzioni avanzate che hanno implementato, oggi possiamo operare consapevoli che i nostri dati e le nostre operazioni sono protetti da elevati standard di sicurezza. Questo **ci permette anche di essere più competitivi sul mercato**, in quanto molti dei nostri clienti, in particolare grandi aziende soggette alla Direttiva NIS 2, richiedono la piena compliance da parte dei loro subfornitori. Abbiamo scelto di investire in questo ambito non solo perché crediamo nell'**importanza della sicurezza**, ma anche perché ci consente di posizionarci come partner strategici, in grado di affrontare con successo progetti di qualsiasi dimensione. La competenza, l'approccio proattivo e la disponibilità di Cash S.r.l sono stati fondamentali per il successo di questo ambizioso progetto."*

CEO, Flavia Turco



**Officine
Zoppelletto**
Qualità d'acciaio



SFIDA

L'azienda aveva bisogno di:

- **Ottimizzare l'infrastruttura IT** per garantire una gestione fluida delle operazioni.
- **Proteggere** i dati sensibili e i sistemi produttivi da minacce informatiche sempre più sofisticate.
- **Integrare nuove tecnologie** senza interrompere la produzione e mantenendo alti standard di efficienza.
- **Adeguarsi** alla nuova Direttiva NIS 2 (Network and Information Systems 2) sulla cybersecurity.

SOLUZIONE

Abbiamo sviluppato un piano strategico personalizzato, che comprendeva:

1. Audit e analisi dell'infrastruttura esistente

- Identificazione dei punti deboli e le opportunità di miglioramento.
- Valutazione delle esigenze specifiche del cliente per mantenere alti livelli di sicurezza.

2. Aggiornamento e ottimizzazione IT

- Implementazione di un sistema di remote management (RS) per garantire un controllo ottimale dell'infrastruttura IT.
- Migrazione a soluzioni ridondate (clustering) per migliorare la scalabilità e la resilienza dei dati.

3. Cybersecurity avanzata

- Implementazione di firewall di nuova generazione e soluzioni di rilevamento e prevenzione delle intrusioni (IDS/IPS).
- Introduzione di un sistema di Vulnerability Assessment e Penetration Testing per monitorare, analizzare e rispondere in tempo reale agli eventi di sicurezza.
- Sistemi di backup automatizzati e crittografia end-to-end per proteggere i dati sensibili e garantirne la disponibilità in caso di incidente.
- Applicazione di piattaforme di sicurezza e filtraggio della posta elettronica.
- Formazione continua del personale sulla sicurezza informatica, inclusi corsi specifici per affrontare le minacce emergenti.

4. Monitoraggio e manutenzione proattiva

- Servizi di monitoraggio continuo per identificare e neutralizzare le minacce in tempo reale.
- Aggiornamenti regolari e manutenzione preventiva per garantire la massima efficienza del sistema.

RISULTATI

Grazie al nostro intervento, l'azienda ha ottenuto:

- **Maggiore efficienza operativa:** i processi produttivi sono stati integrati con le nuove tecnologie, riducendo i tempi di inattività e migliorando la gestione delle risorse.
- **Protezione avanzata:** i sistemi informatici sono ora protetti da minacce interne ed esterne secondo i requisiti della Direttiva NIS 2, con un rischio notevolmente ridotto di attacchi informatici.
- **Resilienza operativa:** grazie ai sistemi di backup avanzati e alle soluzioni di monitoraggio, l'azienda può continuare a operare anche in caso di incidenti informatici.
- **Supporto continuativo:** i servizi di monitoraggio e manutenzione garantiscono protezione costante e assistenza dedicata.



Viale Trieste, 429
36100 Vicenza
presso Cash s.r.l.

info@mamacloud.it
+39 0444 50.71.55
www.mamacloud.it

