Sicurezza Informatica Aziendale

Viviamo in un'epoca in cui la sicurezza informatica è diventata una delle principali preoccupazioni, un aspetto critico che coinvolge individui, aziende e governi. La crescente interconnessione e la dipendenza dalle tecnologie hanno portato alla necessità di proteggere i dati personali e sensibili in modi sempre più sofisticati.

In un ambiente digitale in costante mutamento, una delle minacce più gravi consiste negli attacchi ransomware. Queste attività dannose non si limitano a colpire solo le organizzazioni, ma coinvolgono anche gli individui. Questo comporta effettivamente una compromissione dei dati, un fenomeno che mette a rischio informazioni personali, finanziarie e aziendali. Le conseguenze di tali violazioni variano dal furto di identità alle perdite finanziarie e ai danni irreparabili alla reputazione delle aziende.

Gli individui rappresentano il punto critico della catena, e le tattiche di manipolazione psicologica si stanno evolvendo in modo sempre più sofisticato. Email apparentemente autentiche o messaggi convincenti possono indurre le persone a divulgare informazioni sensibili, evidenziando l'importanza di potenziare la consapevolezza e la formazione degli utenti per contrastare tali minacce.

Anche l’avvento dell'Internet delle Cose (IoT) ha introdotto nuovi rischi. Dispositivi come telecamere di sicurezza e termostati intelligenti, se non adeguatamente protetti, possono costituire punti deboli nella rete di sicurezza complessiva.

Quali strategie possiamo adottare per difenderci efficacemente da queste crescenti minacce?

Attraverso la collaborazione con DOS Group, è possibile implementare strategie per proteggere i dati aziendali. Il team DOS ha la capacità di analizzare e rendere più sicuri i sistemi informatici aziendali da minacce informatiche, mantenendo alti i livelli di sicurezza nelle attività quotidiane mediante l'uso di antivirus e firewall all'avanguardia, oltre che soluzioni e servizi per una protezione completa e continuativa.

La difesa dei dati e dei sistemi IT dalle minacce informatiche per la **sicurezza delle operazioni quotidiane** grazie a servizi e sistemi all'avanguardia.

Azioni mirate per prevenire attacchi informatici e mantenere i dati al sicuro

VULNERABILITY ASSESSMENT

Processo che ha la scopo di fornire una panoramica globlale della propria infrastruttura

- **produce una valutazione complessiva dello stato di salute dell'ambiente**
- **fornisce raccomandazioni per eseguire nuove implentazioni**
- **guida alla correzioni di eventuali criticità per una gestione ottimale**

REMEDIATION PLAN

Piano di rimedio progettato per:

- **mitigare o eliminare le minacce e le vulnerabilità del sistema**
- **garantire una risposta efficace agli incidenti di sicurezza**
- **migliorare la sicurezza complessiva aziendale**

BACKUP ENCRYPTION

Processo di applicazione di tecniche di crittografia ai dati di backup che

- **permette protezione delle informazioni in caso di perdita o furto dei dati di backup**
- **permette ai dati di rimanere al sicuro in caso di violazioni o accessi non autorizzati**
- **per alcune realtà, permette di rispettare una conformità normativa**

BACKUP IMMUTABILITY

E' una pratica che permette sicurezza l'integrità dei dati di backup il quale non puo' essere eliminato o alterato.

La caratteristica immutabile fornisce una **garanzia** aggiuntiva sull'integrità dei dati; grazie a questa pratica è possibile **prevenire errori** umani, **attacchi** malevoli, proteggere i dati backup da attacchi ransomware e da **minacce interne e esterne**.

FIREWALL SECURITY

Un firewall è progettato per controllare e monitorare il traffico di rete con la funzionalità di stabilire regole e filtri per consentire o bloccare il flusso di dati in base a criteri specifici.
Un firewall permette:

- **il controllo degli accessi**
- **aggiornamenti regolari**
- **regole personalizzate**
- **rilevamento e prevenzione delle intrusioni**
- **registrazione delle attivtà di rete**

EMAIL SECURITY

La sicurezza delle mail è essenziale per la protezione globale aziendale e/o privata.
Per questo è necessario valutare diverse pratiche di sicurezza come:

- **implementazione di filtri antispam**
- **protezione da phising, malware o virus**
- **ottimizzare l'efficenza delle risorse di rete**

ENDPOINT SECURITY

La salvaguardia dei dispositivi finali (telefoni, computer ecc.) è fondamentale per la sicurezza e l'integrità dell'infrastruttura IT di un'azienda; questo è possibile attraverso

- **implementazioni di soluzioni di rilevamento delle minacce**
- **applicazione dei controlli di accesso**
- **crittografia per proteggere i dati**