



REPORT THETA

W W W . D A T A S H I E L D S . T E C H



ABOUT US

Fondata nel 2010 da un gruppo di appassionati di tecnologia con una profonda conoscenza delle sfide legate alla sicurezza informatica, DataShields è cresciuta da una piccola startup a una rinomata azienda di riferimento nel settore della sicurezza digitale. La nostra avventura è iniziata con un obiettivo chiaro: rendere il mondo digitale un luogo più sicuro per tutti. Inizialmente, ci siamo concentrati sul fornire soluzioni di sicurezza per piccole e medie imprese, aiutandole a proteggere le loro risorse digitali da minacce sempre più sofisticate.



LA NOSTRA VISIONE

La nostra visione è di creare un mondo in cui la sicurezza informatica non sia solo una necessità, ma un pilastro fondamentale della fiducia e della crescita aziendale. Puntiamo a essere riconosciuti come i leader nel fornire soluzioni di sicurezza innovative e affidabili, contribuendo a costruire un ambiente digitale sicuro per tutti.

LA NOSTRA MISSIONE

In un mondo sempre più connesso e vulnerabile alle minacce informatiche, la nostra missione è chiara: proteggere i dati dei nostri clienti e salvaguardare la loro integrità digitale. DataShield si impegna a fornire soluzioni avanzate e personalizzate per affrontare le sfide di sicurezza più complesse, garantendo che le informazioni sensibili rimangano sicure e protette.





PERFORMANCE

**Sicurezza rete
con DataShield**

100%

**Sicurezza rete
Senza DataShield**

15%

Senza adeguate misure di sicurezza informatica , l'azienda è vulnerabile a una vasta gamma di minacce , tra cui attacchi hacker , malware, phishing e furti di dati che possono portare a gravi perdite finanziarie e danni reputazionali

INTRODUZIONE

Nel contesto odierno di crescenti minacce informatiche, garantire la sicurezza della rete aziendale è di fondamentale importanza: per ottimizzare questo processo e assicurare la qualità di vita online e offline presentiamo questo business plan di rete. DataShield è un'azienda leader nella consulenza e implementazione di soluzioni di sicurezza informatica. La nostra esperienza consolidata ci consente di affrontare le sfide più complesse, fornendo soluzioni su misura che garantiscono la protezione dei dati e l'integrità delle comunicazioni aziendali. Per il nostro illustre cliente Theta proponiamo una serie di soluzioni presentando esempi illustrativi e preventivi dell'intero progetto, esponendo la topologia di rete proposta, descrivendo dettagliatamente gli elementi utilizzati e le loro funzionalità. La progettazione tiene conto di una combinazione di firewall, sistemi di prevenzione delle intrusioni (IPS), segmentazione della rete e altre tecnologie avanzate per garantire un ambiente sicuro e affidabile.

OBIETTIVI

La nostra analisi iniziale ha identificato una serie di requisiti specifici e obbligatori per la rete di Theta, che includono i seguenti punti:

- **Protezione dei dati sensibili:** Implementazione di misure di sicurezza per garantire che i dati aziendali siano protetti da accessi non autorizzati.
- **Continuità operativa:** Progettazione di una rete resiliente che possa mantenere operatività anche in caso di guasti o attacchi.
- **Scalabilità:** Una topologia che possa crescere insieme all'azienda, senza compromettere la sicurezza
- **Gestione centralizzata:** Strumenti e procedure per la gestione centralizzata della rete, semplificando il monitoraggio e la risposta agli incidenti.

ANALISI

Questo report descrive i risultati riguardo la ricerca di eventuali vulnerabilità per l'azienda Theta, concentrando sui servizi web. Durante la nostra approfondita valutazione, abbiamo identificato diverse vulnerabilità critiche all'interno dell'infrastruttura IT di Theta. Queste vulnerabilità rappresentano significativi rischi di sicurezza, inclusi potenziali accessi non autorizzati e violazioni di dati (**per maggiori info fare riferimento alla report tecnico allegato**).

Tuttavia, abbiamo sviluppato soluzioni efficaci per affrontare ciascuno dei problemi identificati. Le nostre raccomandazioni includono passaggi specifici per la correzione, il miglioramento dei protocolli di sicurezza e l'implementazione di misure preventive per rafforzare il sistema contro future minacce. Questo approccio aiuterà a garantire l'integrità e la sicurezza dei beni digitali di Theta.





SEGMENTAZIONE DI RETE

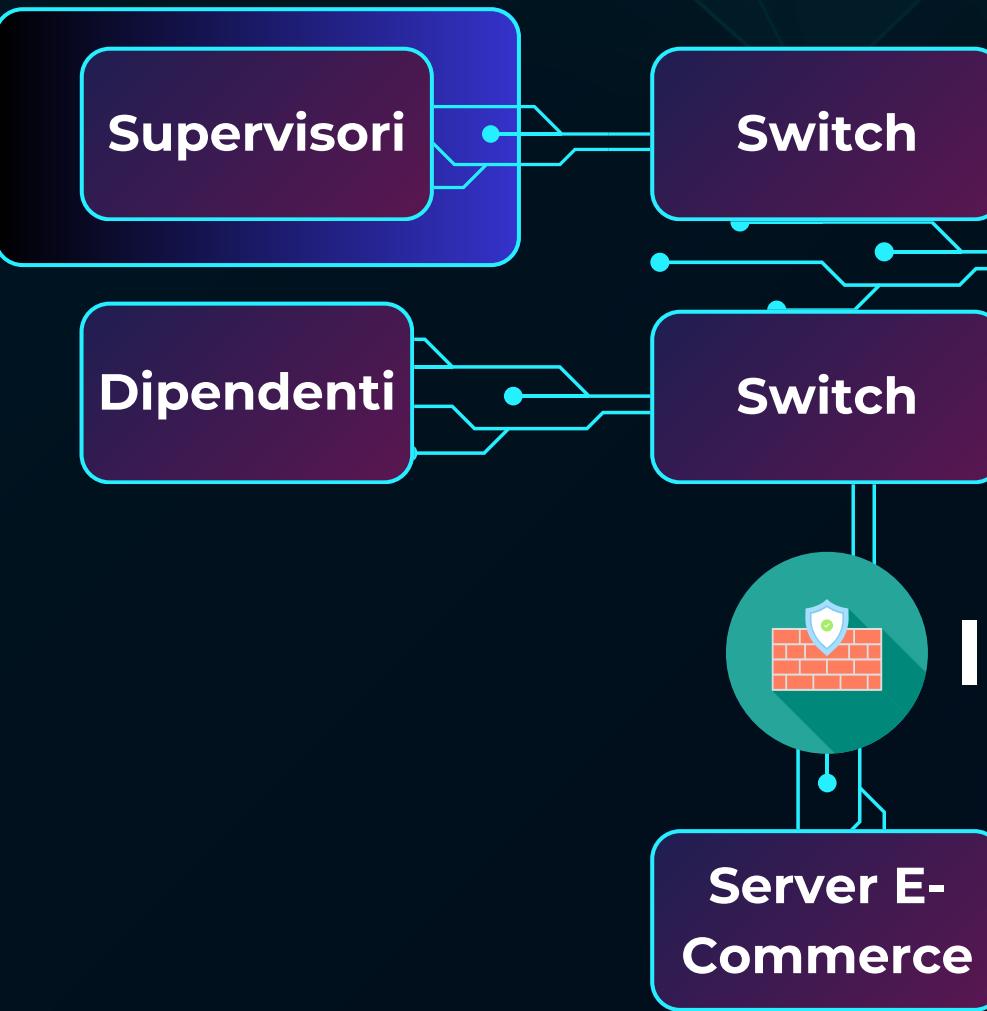
In primo luogo, per mantenere la riservatezza dei dati sensibili dell'azienda sia verso l'esterno che verso l'interno, riteniamo sia fondamentale segmentare la rete (zoning). Questi segmenti sono basati su livelli di sicurezza e funzionalità in modo da permettere l'accesso solamente a chi ne ha i diritti. Di fatti il modello da noi consigliato pone le risorse critiche in zone altamente protette con controlli di sicurezza avanzati, la protezione degli asset critici è fondamentale per prevenire interruzioni operative e perdite di dati sensibili e le difese sono progettate per rilevare e bloccare tentativi di accesso non autorizzato.



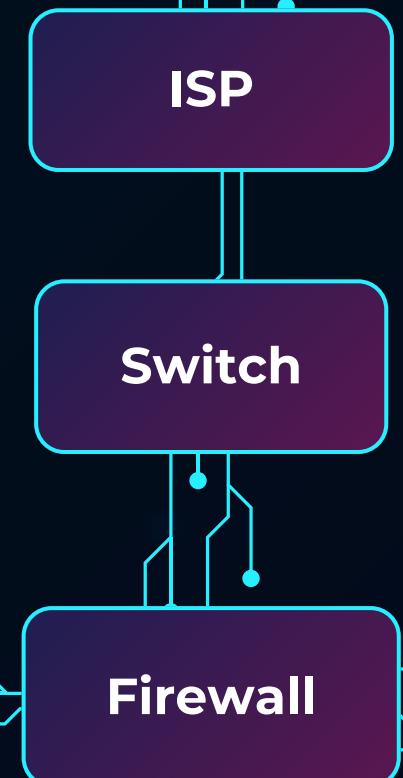


TOPLOGIA DI RETE

VLAN



Internet





REVERSE PROXY E DMZ

Per aumentare la protezione l'ideale è di inserire un reverse proxy per gestire le richieste di ingresso dei client esterni verso i server interni, nella zona DMZ (il segmento che espone i vostri servizi verso l'esterno, quindi raggiungibili da internet), in modo da mascherare i server interni e filtrare il traffico malevolo prima che raggiunga il server. Quando i server rispondono, il reverse proxy reindirizza le risposte agli utenti. Questa scelta è basata sui seguenti vantaggi:

- **Efficienza:** il reverse proxy ascolta su determinate porte e inoltra le richieste a diversi server interni con differenti IP riducendo i disservizi di rete.
- **Sicurezza:** funziona come un filtro in entrata, proteggendo i server interni dagli attacchi esterni. Gli utenti esterni non interagiscono direttamente con i server interni, ma solo con il reverse proxy e questo aiuta a nascondere l'infrastruttura interna e a ridurre il rischio di attacchi diretti ai server.
- **Bilanciamento del carico:** può distribuire il carico tra diversi server interni (back-end). Questa funzionalità migliora le prestazioni, la disponibilità e l'affidabilità del sistema, distribuendo le richieste tra più server per evitare sovraccarichi. Il nostro consiglio è quello di considerare le opzioni future per server aggiuntivi, per i quali sarà utile questa funzionalità.



FIREWALL

In aggiunta al reverse proxy, è stato implementato un Firewall che garantisce una maggiore granularità nel management delle porte. Come hardware proponiamo un Firewall di ultima generazione targato Cisco (ASA 5585-X) , in grado di formare un perimetro di difesa tra la rete interna ed internet (o altre non fidate).

In aggiunta , il Firewall è stato configurato con delle policy conformi alle necessità attuali dell'azienda, in modo tale da rispettare le richieste del cliente.

I Firewall Cisco ASA-5585-X offrono numerosi vantaggi per la protezione delle reti aziendali:

- forniscono alta sicurezza contro minacce come virus e malware garantendo la protezione dei dati aziendali
- Garantiscono affidabilità e assicurano che la rete rimanga operativa senza interruzioni .
- Gestiscono un grande volume di traffico di rete senza rallentamenti mantenendo la velocità delle operazioni aziendali.
- Offrono strumenti intuitivi per la configurazione e la gestione facilitando il lavoro degli amministratori IT.
- Sono progettati per crescere con l'azienda permettendo di aggiungere capacità e funzionalità man mano che le esigenze aumentano





IPS



Successivamente per mettere un livello di difesa addizionale suggeriamo la disposizione di un IPS (Intrusion Prevention System) a difesa del server interno, offre protezione in tempo reale bloccando le minacce, monitora costantemente la rete per rilevare possibili incidenti dannosi e acquisire informazioni in merito.

Il vantaggio nell'utilizzo di un IPS rispetto ad un IDS (Intrusion Detection System) sta nell'azione immediata del primo rispetto al secondo che si limita a rilevare le minacce senza intervenire direttamente. Il nostro obiettivo principale è impedire che gli attacchi danneggino il sistema, per questo la migliore opzione è un IPS che li blocca a monte.



VLAN

Assegnare permessi differenti tra dipendenti e amministratori è cruciale per proteggere le risorse aziendali sensibili. I dipendenti possono essere limitati all'accesso solo alle risorse necessarie per svolgere il loro lavoro quotidiano, mentre gli amministratori possono avere accesso completo per gestire e mantenere l'infrastruttura IT. Questa separazione dei privilegi minimizza il rischio di accessi non autorizzati a dati critici e riduce il potenziale impatto di errori o comportamenti malevoli. Inoltre, le VLAN migliorano la gestione del traffico di rete, poiché consentono di applicare politiche di sicurezza e gestione del traffico specifiche per ogni segmento. Ciò significa che il traffico può essere prioritizzato, monitorato e controllato in modo più efficace, garantendo che le risorse di rete siano utilizzate in modo ottimale.



MISURE DI SICUREZZA FISICHE

- Telecamere di Sicurezza: Monitoraggio continuo delle aree sensibili per rilevare e registrare accessi non autorizzati.
- Controllo degli Accessi Fisici: Utilizzo di badge, lettori di impronte digitali o sistemi di riconoscimento facciale per limitare l'accesso ai server ai soli dipendenti autorizzati.
- Crittografia dei Dati: Protezione dei dati memorizzati sui server tramite tecniche di crittografia per prevenire accessi non autorizzati anche in caso di furto fisico.
- Barriere Fisiche: Utilizzo di porte e recinzioni robuste, eventualmente con serrature elettroniche, per proteggere le sale server.
- Sistemi di Allarme: Allarmi sonori e visivi per notificare tentativi di intrusione o accesso non autorizzato.
- Controllo Ambientale: Sistemi di rilevazione di fumo e calore per prevenire incendi, oltre a sistemi di raffreddamento per mantenere la temperatura ottimale dei server.
- Backup e Ridondanza: Implementazione di sistemi di backup dei dati e ridondanza dell'infrastruttura per garantire la continuità operativa in caso di guasti

SISTEMI DI RIDONDANZA

Inoltre sarebbe opportuno utilizzare eventuali sistemi di ridondanza. Questi sistemi e i NAS (Network Attached Storage) sono essenziali per garantire la sicurezza e l'affidabilità dei dati in un'azienda. La ridondanza consiste nell'implementare duplicati di componenti critici, come server o dischi rigidi, per assicurare che un guasto hardware non comprometta la continuità operativa. I NAS, d'altra parte, offrono una soluzione centralizzata per la gestione e l'archiviazione dei dati, permettendo un accesso rapido e sicuro a file condivisi attraverso la rete aziendale. Integrando i NAS con tecnologie di ridondanza, le aziende possono proteggere i propri dati da perdite accidentali o attacchi informatici, garantendo al contempo la disponibilità continua delle risorse informative. Questo approccio è particolarmente utile per la gestione di backup automatici e la sincronizzazione dei dati in tempo reale, migliorando l'efficienza operativa e la resilienza complessiva dell'infrastruttura IT aziendale.



CONCLUSIONI

L'azienda Theta deve affrontare una serie di sfide significative per migliorare la propria postura di sicurezza informatica. È essenziale che venga intrapresa un'azione immediata per colmare le lacune identificate e ridurre il rischio complessivo di compromissione. Investire in tecnologie di sicurezza avanzate e promuovere una cultura della sicurezza tra i dipendenti sarà cruciale per proteggere le risorse aziendali e garantire la continuità operativa in un panorama di minacce in continua evoluzione.

L'attuazione delle raccomandazioni fornite consentirà all'azienda Theta di rafforzare la propria sicurezza e di posizionarsi meglio per affrontare le sfide future in ambito di cybersecurity.



CONTATTI



02697161



www.datashields.tech



info@datashields.tech



Via Della Sicurezza 20, Roma 20159



GRAZIE

W W W . D A T A S H I E L D S . T E C H