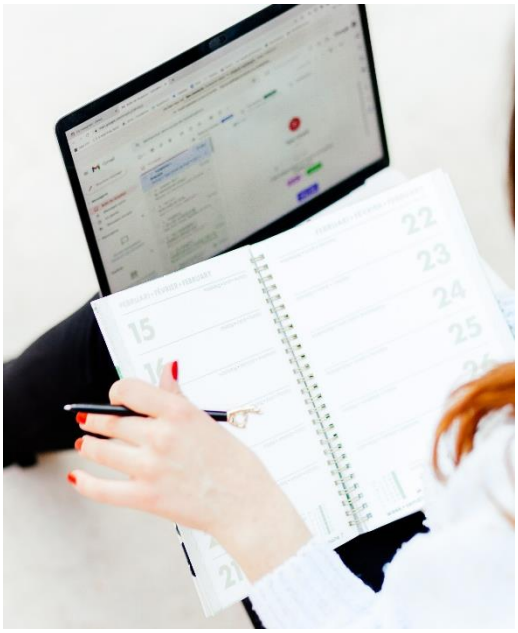
SURFTECH
SICUREZZA SERVER DI POSTA

La Posta Elettronica è un servizio fondamentale e di Business per ogni Azienda. Le e-mail che si ricevono e quelle che si spediscono devono essere sicure e vere. Sai quali sono i danni economici se il tuo servizio di posta viene compromesso?

Il Servizio di Posta Elettronica è diventato uno strumento di Business e di produttività irrinunciabile per qualsiasi azienda. Gli utenti, ad ogni livello, devono poter essere sicuri che le email che ricevono siano "vere" (non alterate) e che quelle che spediscono non possano essere intercettate e modificate. La Sicurezza dei Server di Posta diventa un fattore irrinunciabile a cui dare la massima priorità ed importanza a garanzia della continuità delle attività aziendali.

Certezza di Autenticità di una e-mail e della sua provenienza
Protezione dal furto e frode dei propri indirizzi di posta
Protezione dalle responsabilità legali per e-mail falsificate
Aumenta l'affidabilità del contenuto delle e-mail aziendali
Contribuisce ad innalzare la Sicurezza Informatica aziendale
Conformità ai Controlli CIS e Framework internazionali

La Soluzione **Sicurezza Server di Posta** ha lo scopo di garantire la **certezza dell'Autenticità di una e-mail** e della sua **provenienza**. Inoltre, impedisce che malintenzionati possano inviare delle e-mail false utilizzando un indirizzo di posta aziendale oppure **mascherando la provenienza**. Questo è ancora più importante quando l'e-mail ha un valore giuridico e quindi **l'Azienda è corresponsabile** se non dimostra di aver svolto tutte le attività necessarie per impedire che la propria e-mail possa essere utilizzata con finalità criminali. In definitiva è di fondamentale importanza per innalzare complessivamente le Difese Informatiche e per essere il più possibile conformi alle Raccomandazioni Internazionali.



SICUREZZA SERVER DI POSTA

un Servizio Surftech per innalzare le difese Aziendali

Il servizio è costituito da attività sistemistiche che si concentrano soprattutto su SPF, KDIM e Dmarc utilizzando **specifiche metodologie e avvalendosi di appositi tools** software. Le varie attività sistemistiche posso essere realizzate sia “on site” che “da remoto” in base alle necessità ed esigenze del cliente. Tutto ciò **comporta un impegno minimo da parte del cliente e solitamente si realizza in pochi giorni** e con tempi molto brevi a meno che non si debba operare in ambienti molto complessi e con molteplici Server di Posta.

I **punti chiave della Soluzione** sono i seguenti:

- Verifica della **configurazione SPF** (**S**ender **P**olicy **F**ramework)
- **Impostazione** del **DKIM** (**D**omain**K**eys **I**dentified **M**ail) e sua corretta configurazione
- **Configurazione** con **DMARC** (**D**omain-based **M**essage **A**uthentication **R**eporting and **C**onformance) in monitoring e osservazione per almeno sei mesi **utilizzando appositi tools forniti da Surftech**
- **Controllo** per almeno sei mesi delle **analisi e dei vari report**
- Al completamento delle varie analisi e dei report, **verifica delle opportune impostazioni** del DMARC

In aggiunta, solo per chi utilizza **Microsoft 365 come servizio di posta**:

- Attivazione della segnalazione della provenienza dell’e-mail con la dicitura **EXTERNAL** se ricevuto da un indirizzo di posta esterno all’azienda.

CIS Center for Internet Security®

CIS Controls®

Questa Soluzione “Sicurezza dei Server di Posta” è realizzata in conformità alle “raccomandazioni” CIS Controls V.8.0 e pertanto contribuisce a rendere complessivamente più sicuro tutto l’ambiente informatico aziendale in conformità agli Standard e Framework internazionali.

SURFTECH
YOUR EXPERIENCE MATTERS

Via Montecchi 8/2 – 37031 Illasi (VR) – Tel 045.5117703
Info@surftech.it - www.surftech.it