Cleis Security s.r.l.

Cleis Security nasce:

- Dall'Istituto di Elettronica ed Ingegneria dell'Informazione e delle Telecomunicazioni (IEIIT) organo del Consiglio Nazionale delle Ricerche (CNR), la cui mission è studiare ed innovare i processi per la sicurezza informatica.

- Dall'esperienza di Cleis Tech, Advanced Business Partner IBM ed operante dal 1992 nel campo della fornitura di infrastrutture e servizi IT ad alta specializzazione.

Cleis Security vuole rispondere e soddisfare le sempre più incalzanti esigenze di sicurezza informatica delle Aziende di qualunque dimensione e categoria merceologica, portando nell'industria l'innovazione tecnologica che nel mondo della ricerca ha raggiunto uno stato maturo.

Lo stretto collegamento con il mondo della Ricerca e dell'Università rendono il Personale di Cleis Security sempre aggiornato sullo stato dell'arte della sicurezza informatica.

NETWORKING

La progettazione di reti LAN, WLAN e distribuite, l'ottimizzazione del traffico attraverso l'analisi delle prestazioni di rete sono i punti cardine dell'attività di Cleis Security. Con l'analisi dei protocolli e delle applicazioni TCP/IP si migliora la fluidità dei sistemi e la gestione dei servizi Aziendali.

Le competenze e l'esperienza di Cleis Security permettono di implementare le reti a misura delle esigenze dei Clienti soprattutto in termini di sicurezza e velocità.

NETWORKING

I servizi forniti non coprono solo le esigenze standard di gestione ma si elevano a soddisfare le necessità emergenti dal costante sviluppo tecnologico.

Il controllo del traffico e dei server per tipologia di dati permette di ricavare: la natura della propria rete, individuare utilizzi illeciti, diminuire gli sprechi ed ottimizzare le risorse, bloccare le operazioni non consentite dalle politiche Aziendali ed eventualmente individuarne i responsabili.

WIRED & WIRELESS SECURITY

- Spam La posta indesiderata influisce sulla produttività ed infastidisce gli utenti. Si sottolinea che un sistema anti-spam non preciso, può far perdere e-mail importanti.

- Worm/Virus Occupano risorse sui PC e sulla rete locale fino a causare imponenti fermi, trasformano i computer Aziendali in “zombie” o “time bomb” pronti ad eseguire operazioni indesiderate a comando.

WIRED & WIRELESS SECURITY

- Intrusioni Virus giunti da Internet o da chiavette USB creano porte d'accesso sui PC Aziendali da cui possono consentire l'entrata nella rete Aziendale di malintenzionati o la fuoriuscita di dati importanti (info leakage).

- Sabotaggi Danni causati da attacchi diretti a Terzi (es. Stuxnet).

- Furti Intrusioni su commissione, social engineering, spionaggio industriale, acquisizioni di dati sensibili e/o personali.

WIRED & WIRELESS SECURITY

I servizi di Cleis Security sono orientati ad evitare ognuno di questi eventi attraverso l'implementazione di soluzioni perimetrali di ultima generazione per proteggere gli "ingressi" informatici dell'Azienda senza però ingessarne l'operatività.

In particolare, si fa riferimento alla definizione e messa in opera di procedure operative per la gestione delle connessioni: ad Internet, alla rete wireless, alle periferiche di PC e notebook.

WIRED & WIRELESS SECURITY

Implementazione di soluzioni “interne” per il controllo e la protezione da azioni accidentali o volute, volte al furto di dati (white collar crime), alla regolamentazione degli accessi ai sistemi informatici coerentemente agli accessi fisici alla sede Aziendale.

La soluzione vincente, in questi casi, è l'affiancamento al Cliente nell'ottica di una partnership tecnologica e la cura delle diverse esigenze del Cliente e del suo core business.

SYSTEM INTEGRATION

Presa in carico di infrastrutture informatiche pre-esistenti, nell'ottica del mantenimento o del miglioramento di tale infrastruttura.

Integrazione fra sistemi esistenti o in fase di introduzione in Azienda: sistemi Blade, virtuali, open-source, posta elettronica, storage.

Cleis Security propone soluzioni chiavi in mano per precise esigenze Aziendali di innovazione o gestione.

FRINGE SECURITY

Le esigenze di security "di frontiera" comprendono tutti quei servizi non citati fin'ora e che riguardano quelle attività di hacking legali svolte per Clienti con particolari esigenze di sicurezza dei dati e delle reti (risk assessment, simulazione di disastro, hacking offensivo).

Inoltre, si considera sicurezza di frontiera anche il tentativo di accesso a propri sistemi di cui non si dispongono più le credenziali, le analisi forensi e le consulenze per Procure e Forze dell'Ordine.