

Soluzioni per la Sicurezza Informatica



PREMESSA

I nuovi modelli di business spingono le aziende a dotarsi di mezzi informatici, più o meno sofisticati, per rimanere competitivi nella corsa alla globalizzazione. Adottare tali modelli significa spesso autorizzare l'accesso al Sistema Informativo Aziendale ai propri clienti, fornitori, partner e collaboratori: e-mail, accesso ad Internet, pendrive, possono diventare altrettante fonti di vulnerabilità se non vengono adeguatamente protette.

Le imprese scambiano sulla rete una quantità crescente di documenti ed informazioni: dati che rappresentano un patrimonio strategico e di business importantissimo, che deve essere protetto da tentativi di intrusione degli hacker e di terzi, estranei all'azienda in generale e da un non adeguato utilizzo da parte del personale interno.

Queste sono solo alcune delle criticità da fronteggiare. In più ci sono le indicazioni che riguardano la legge sulla Privacy da seguire tassativamente.

Per questo motivo è indispensabile essere in grado di valutare i rischi legati all'infrastruttura e che venga definita, a livello aziendale, una politica per la sicurezza del Sistema Informativo.

La "**politica di sicurezza**" è la specificazione ad alto livello degli obiettivi di sicurezza (espressi in termini di volontà di salvaguardare la riservatezza, l'integrità e la disponibilità dell'informazione in presenza di minacce) che l'organizzazione si propone di conseguire.

PREVENIRE E' MEGLIO CHE CURARE

Alle minacce provenienti dall'esterno, si affianca la necessità di garantire la protezione, l'integrità e la riservatezza di un sempre maggiore volume di dati all'interno dell'azienda, per cui la Sicurezza si sposta su un altro piano e diventano a questo punto fondamentali soluzioni di Data Protection, di Back Up, di Disaster Recovery e l'implementazione di sistemi di Identity & Access Management, che

aiutino a gestire e preservare i dati e a controllare l'accesso alle applicazioni. Tutto questo a garanzia della continuità del business e dell'ottemperanza alla compliance.

COSA FARE?

Le aziende hanno bisogno di un modo pratico e accessibile per risolvere il problema chiave della sicurezza, di monitorare e analizzare l'enorme volume di eventi di sicurezza in modo efficiente allo scopo di:

- identificare le minacce attuali e prevenire il loro impatto sulle operazioni di business;
- documentare e dimostrare la compliance dell'azienda con i mandati normativi e industriali;
- dimostrare ad auditor e a terze parti che sono stati posti in essere controlli IT efficienti.

Oggi la sicurezza informatica è una priorità assoluta e queste informazioni ti possono davvero essere utili.

SERVIZI DI GESTIONE E MONITORAGGIO

Cos'è un sistema di gestione e protezione delle vulnerabilità?

La gestione e la protezione delle vulnerabilità costituiscono un processo continuo che protegge le preziose informazioni dei clienti, le risorse critiche di rete e la proprietà intellettuale. Identifica rapidamente le vulnerabilità e fornisce soluzioni di correzione e tecniche per bloccare le minacce eseguendo, al tempo stesso, attività di monitoraggio e verifica della riduzione dei rischi.

SCEGLI LE SOLUZIONI PROPOSTE DA SCP

- ✓ **Security Analysis**
- ✓ **Security Presence**
- ✓ **Security Governance**

Soluzioni per la Sicurezza Informatica



SCEGLI LA TUA SOLUZIONE

-  Security Analysis
-  Security Presence
-  Security Governance

SECURITY ANALISYS

Obiettivi da raggiungere

Rapida ricognizione dei computer, server e programmi di base installati al fine di:

- ✓ verifica che il backup dei dati sia installato, configurato e attraverso un'analisi sommaria dei log, che stia funzionando¹;
- ✓ verifica che il software antivirus sia installato, configurato ed attraverso un'analisi sommaria dei log, che sia aggiornato e che stia funzionando²;
- ✓ verifica presenza dei gruppi di continuità, e controllo vetustà dell'apparato.

Caratteristiche della rete:

- ✓ utilizzo di strumento software/hardware automatizzato per la rilevazione delle caratteristiche della rete (vulnerabilità software, presenza degli aggiornamenti ecc.)

Collegamento ad Internet:

- ✓ In presenza di collegamento internet con indirizzo IP pubblico fisso, si effettua una scansione dei servizi aperti.³;

Se è presente il documento sicurezza:

- ✓ verifica della presenza delle password e le loro caratteristiche.

Prodotto della soluzione

Report coi risultati delle scansioni ed analisi generale di quanto è stato rilevato.

Operatività

¹ relativamente ai software più in uso, nel caso di software particolari si deciderà caso per caso quanto tempo impegnare per capire il funzionamento del software in questione.

² Idem come sopra

³ previa autorizzazione scritta da parte del Cliente

Dopo la sottoscrizione di un contratto-liberatoria, viene installato un dispositivo hardware (generalmente un PC) che esegue automaticamente la scansione della rete. Alla fine della scansione il dispositivo viene rimosso. In contemporanea di tale scansione, viene eseguita la rilevazione manuale dei parametri del sistema informatico.

Se convenuto in anticipo viene effettuata la scansione dell'indirizzo IP dai Laboratori di Scp.

Tempistica

La durata dipende dalle dimensioni della rete, dal numero di pc, di server ecc. Si prevede una settimana di scansione al fine di raccogliere una consistente quantità di dati, sufficiente ad elaborare un'analisi pressoché completa, mentre la rilevazione manuale è direttamente proporzionale al numero dei PC.

Strumenti utilizzati

Scp utilizzerà per i servizi sopra elencati la seguente strumentazione software:

- ✓ software Open Source
- ✓ analizzatore di vulnerabilità
- ✓ analizzatore di WiFi
- ✓ software per analisi di protocollo, o packet sniffer.



Risultati

Viene consegnato un report che evidenzia le vulnerabilità rilevate ed i risultati delle verifiche.

Se durante la Security Analysis, vengono evidenziate particolari vulnerabilità e/o problematiche importanti, si propone la stesura di una soluzione progettuale per la messa in sicurezza del sistema (Soluzione Security Response).

Soluzioni per la Sicurezza Informatica

SECURITY PRESENCE

La soluzione comprende tutte le funzioni offerte dalla soluzione Security Analysis, più le seguenti attività:

- ✓ stesura di un manuale di sicurezza di base che riporta le linee guida per la protezione del patrimonio informativo aziendale. Tale manuale viene redatto seguendo le direttive del management e rispettando le normative ISO-17799 (BS-7799), ISO-27001. Il contenuto del manuale evidenzia le regole di accesso ed utilizzo delle informazioni e degli asset aziendali.
- ✓ analisi, progettazione ed eventualmente realizzazione dell'infrastruttura di sicurezza IT.



La soluzione prevede anche il Monitoraggio dell'infrastruttura, mediante l'installazione di dispositivi specializzati e loro configurazione

particolareggiata.

Il Monitoraggio permetterà un controllo di:

- ✓ attività dispositivi (rilevamento intrusioni, attività anomala, ecc.);
- ✓ inventario "dinamico" infrastruttura;
- ✓ attività IDS-IPS;
- ✓ banda di rete.

Schedulazione dell'analisi vulnerabilità: in momenti predefiniti si procede (previa liberatoria) ad un verifica delle eventuali vulnerabilità dell'infrastruttura ed alla loro risoluzione.

Produzione di report periodici (eventualmente riassunti e commentati).

Pronto intervento

SECURITY GOVERNANCE

La soluzione comprende tutte le funzioni offerte dalla Security Presence più le seguenti attività:

- ✓ stesura del Security Plan aziendale e sua implementazione.
- ✓ security Training per la formazione del personale.



MODALITA' DI EROGAZIONE

L'attività prevista dai servizi sopra elencati, ha la finalità di verificare lo stato di salute della gestione delle informazioni all'interno dell'azienda individuando le principali rischiosità.

L'attività prevista da Scp, è basata sui principi guida dello standard ISO27001.

Scp definisce sempre prima le modalità operative con il committente (che è sempre la Direzione generale o la proprietà) che nel contempo rilascia una liberatoria per l'esecuzione di attività di screening e ricerca delle informazioni anche attraverso la simulazione di attività interne o esterne.

Soluzioni per la Sicurezza Informatica

CONCLUSIONI

SCP crede nella sicurezza attraverso il controllo.

SCP offre protezione completa per imprese, enti pubblici, enti scolastici, associazioni, proteggendo da malware noto e sconosciuto, spyware, intrusioni, applicazioni indesiderate, spam, violazione dei criteri di sicurezza e fornendo un ampio controllo dell'accesso di rete (NAC).

Le soluzioni Security di SCP rappresentano un modo semplice per ridurre i costi e la difficoltà di proteggere la vostra impresa dalle minacce.

Protezione multipla dalle minacce con prodotti specialistici.

Supporto tramite web, e-mail e telefono inclusi in tutti i tipi di soluzione, previa attivazione del canone di manutenzione.

Se siete interessati contattate il commerciale di riferimento ai seguenti recapiti:



Pierpaolo De Paris *servizi commerciali*

p.deparis@scponline.it

Mobile: 39 338 5950163

Scp srl

Sede centrale: via Vittorio Veneto 274 - 32100 Belluno tel. 0437 938.444 fax 0437 930.045 e-mail: info@scponline.it

Ufficio di Treviso: viale della Repubblica19/B - 31020 Villorba (TV) tel. 0422 308.803 fax 0422 301.006 e-mail: infotv@scponline.it

www.scponline.it

Reg. Imprese BL - C.F. e P.I. 00524890258

REA 0056750 - Cap. Soc. € 50.000,00 i.v.

Azienda certificata UNI EN ISO 9001