



Netsecurity Platform

la piattaforma per la sicurezza gestita

**"una sola sicurezza,
quella di avere un buon partner"**

I suoi indefinibili confini hanno reso Internet la base dei progetti di business sviluppati dalle aziende per guadagnare efficienza e competitività.

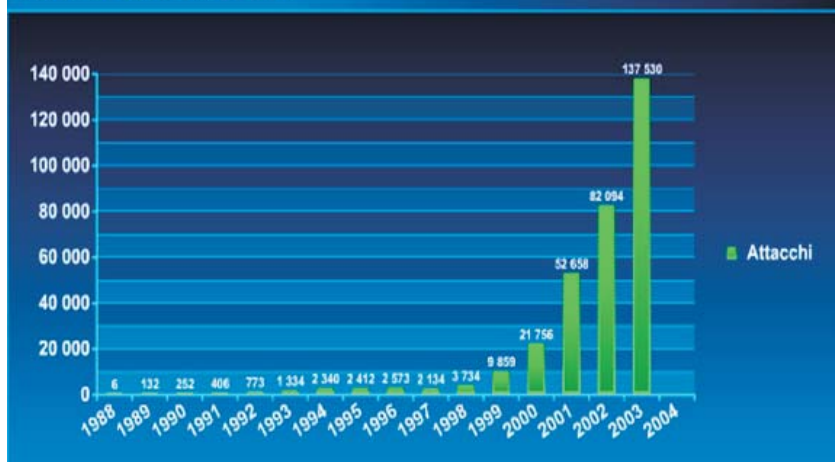
I Network aziendali non veicolano più solo dati propri, ma amministrano e governano le soluzioni più avanzate di E-Commerce, Customer Care, E-Learning, IP Telephony e molte altre, allo scopo di comunicare, gestire, individuare, aggregare la più ampia comunità oggi esistente.

Questo ha reso la gestione delle reti informatiche di rilevanza strategica, inquanto strumento d'accesso e condivisione dei dati e delle applicazioni per utenti interni ed esterni.

La progressiva adozione di Internet ha amplificato le minacce verso i sistemi informatici connessi in rete ed elevato in maniera esponenziale le problematiche connesse alla gestione dei dati, al loro reperimento ed al mantenimento degli stessi in sicurezza.

I rischi di ieri si sono tramutati, oggi, in esigenze e adempimenti di legge.

Statistiche attacchi



La progressiva diffusione di Internet ha elevato in misura proporzionale gli attacchi e le intrusioni ai sistemi informatici aziendali.

Profilo dei nemici, complessità degli attacchi, e criticità degli obiettivi, sono aumentati in funzione del crescente business veicolato sulla rete.

(Dati rilevati da CERT Coordination Center)

B-PRESS SRL GRUPPO MSOFT

Piazzale Lombardia 4 28100 NOVARA - Italy
Tel +39 0321 499508 Fax +39 0321 492974
Partita IVA IT01697420030



Netsecurity Platform

la piattaforma per la sicurezza gestita

Quando un attacco compromette la disponibilità di un sistema o di un'applicazione, o viola la riservatezza dei dati, le conseguenze non sono sempre quantificabili nell'immediato ed in alcuni casi possono essere non "stimabili". Oltre al danno indotto dall'attacco, infatti, l'azienda si trova spesso a dover fronteggiare conseguenze legali derivanti dai danni arrecati per la sospensione di un servizio, la violazione della privacy altrui o una conseguente perdita di credibilità ed immagine nei confronti del mercato.

Profilo Nemici

- **Hackers** - professionisti della pirateria informatiche che prendono possesso di accessi aziendali per danneggiare dati o farne uso improprio per altri attacchi
- **Insider** - ex collaboratori o collaboratori scontenti o inefficienti che asportano dati dall'azienda o li danneggiano, o fanno un uso improprio di internet.
- **Esploratori** - clienti, colleghi, amici, visitatori che per curiosità trafugano dati o informazioni d'accesso

Attacchi

- **Virus** - sono i più pericolosi. Si propagano sulla rete e cancellano file e inibiscono l'uso dei sistemi.
- **Trojans** - mascherati da software spesso scaricati dalla rete sono veicoli per distribuire codice distruttivo o inviare mail con copie di propri file.
- **Vandals** - Applicazione contenente istruzioni di distruzione file o porzioni di sistema.
- **Attacchi di ricognizione** - vengono utilizzati per raccogliere informazioni e testare il sistema di sicurezza della rete al fine di architettare un attacco. Ottenuto con software come sniffer, scanner o programmi di decifrazione password.
- **Attacchi di accesso** - sono indirizzati verso il sistema di autenticazione degli accessi per poter accedere a dati riservati
- **Attacchi DoS** - invio di una mole consistente di dati verso un sistema od un sito al fine di inibirne le funzionalità.
- **Attacchi DdoS** - si diffonde attraverso software "agenti" diffusi su più Pc, in grado di sferrare un unico attacco verso un unico obiettivo.
- **Spam** - mail indesiderate che saturano memoria, banda e inducono perdite di tempo.

Abusi

Riguardano l'uso improprio, da parte di un collaboratore, dell'uso di Internet e della posta elettronica. Tale attività invade e viola i diritti di privacy ed in taluni casi è volta a carpire informazioni riservate dell'azienda.

Danni ed effetti

- **Danni economici** - Il danno economico può derivare da molteplici effetti dell'attacco : distruzione o evasione di informazioni riservate, interruzione di servizio e perdita di business, spese legali derivanti da danni generati a terzi, necessità di bonifica del sistema e rafforzamento delle misure di sicurezza ecc..
- **Danni legali** - Causati da rivalsa di terzi per danni concatenati all'attacco subito, rivalsa di terzi per violazione della privacy su dati personali persi o danneggiati (lg 196/2003)
- **Danni d'immagine** - Per servizi erogati a terzi e resi in affidabili da attacchi portati con successo, senso di fragilità trasmesso da un sistema che non garantisce adeguata sicurezza, invio improprio di mail o dati riservati a terzi.



Netsecurity Platform

la piattaforma per la sicurezza gestita

Il crescente pericolo cui sono sottoposti i network aziendali, ed il valore del “danno procurato” alle attività economiche in seguito all’aumento degli attacchi e degli incidenti, interni ed esterni, ha sviluppato in maniera esponenziale, nelle aziende, l’interesse verso le politiche di sicurezza, nella consapevolezza che la Rete è ormai uno strumento di lavoro indispensabile. Tuttavia, la soluzione ad un problema “nuovo”, complesso e variegato, come la protezione dei sistemi, comporta spesso scelte che non danno definitive garanzie a fronte di costi spesso non valutabili.

Se il crescere di abusi ed eventi intrusivi sta maturando la convinzione che non sia più sufficiente acquistare ed installare qualche apparato per poter garantire integrità, riservatezza e disponibilità delle informazioni, la risoluzione del problema spesso impone quesiti e scelte complesse che si traducono in costi che raramente trovano giusto riscontro in benefici ed efficienza.

<u>Infrastruttura</u>	E’ il primo intervento che viene operato. L’investimento necessario è spesso rilevante poichè più sensibile alle esigenze dell’azienda che al dimensionamento della sua rete o del suo business.
<u>Software</u>	Quello disponibile non soddisfa esigenze specifiche e non è scalabile in funzione di esse. Oltremodo comporta sempre qualche compromesso in ordine alle possibilità di governance del sistema e degli strumenti di reporting e alerting.
<u>Risorse</u>	L’adozione di politiche di sicurezza informatica e l’implementazione allo scopo di un network, impongono sempre l’assegnazione di una risorsa umana.
<u>Competenze e Aggiornamento</u>	La velocità con cui devono essere aggiornati i sistemi, con le patch rilasciate dai produttori, sia in funzione delle mutevoli esigenze aziendali, sia per la molteplicità dei pericoli, impongono un’applicazione continua e la destinazione di risorse economiche finalizzate al mantenimento delle competenze del personale adibito (IT Manager).

**Netsecurity Platform***la piattaforma per la sicurezza gestita*

"perchè *outsourcing*?"

La salvaguardia della sicurezza delle informazioni e della continuità delle funzioni aziendali non può prescindere dalle valutazioni economiche che l'obiettivo impone.

La scelta di gestire in outsourcing i sistemi diviene, sempre più, un passaggio obbligato e consigliato, soprattutto per il segmento delle PMI, che attraverso tale strategia raggiungono performance di massima efficienza ed efficacia senza gravare le aziende di investimenti privi di un tangibile ritorno.

È infatti ormai maturata la consapevolezza che nell'ambito dell' *information security* l'impegno e l'applicazione debbano essere continui nel tempo.

benefici dell' outsourcing

Economici

- Definizione di un canone/costo fisso.
- Alleggerimento dei costi derivanti da mantenimento ed aggiornamento.

Efficienza

- L'analisi del rischio sugli asset informativi viene effettuato con personale esperto e competente.
- Recupero di risorse (tempo) altrimenti impiegate ad attività di monitoring.
- Aggiornamento costante degli apparati e del software.

Efficacia

- Assenza di problemi di integrazione con applicazioni esistenti.
- Soddisfazione dei principali parametri imposti dalla legge 196/2003 anche in ordine alla definizione ed aggiornamento delle credenziali di accesso ai dati da parte degli utenti (identity management), alla manutenzione degli appliance hardware (router, pix ecc..) ed all'aggiornamento delle patch.
- Sistemi di controllo proattivi, flessibili e personalizzati gestibili senza modificare la struttura esistente.
- Garanzie di Business Continuity.



Netsecurity Platform

la piattaforma per la sicurezza gestita

"information security visibilità sul mercato"

Il comparto della sicurezza informatica si propone certamente come uno di quelli a più alto tasso di crescita tra quelli facenti parte del mercato informatico. La crescente sensibilità rispetto ai rischi legati al problema della sicurezza e la consapevolezza del loro forte legame con la competitività delle imprese ha reso più mature le stesse verso necessità fino ad oggi sottovalutate. Tale condizione è stata rilevata anche dallo studio annuale (Global Information Security Survey) promosso da Ernst & Young che denuncia, tuttavia, una persistente resistenza delle aziende ad intraprendere azioni preventive.

Se il 59% (dati italia) delle aziende rilevate dichiara la **sicurezza IT** determinante per raggiungere gli obiettivi di business dell'azienda, solo il 14% di queste (8% sul totale) fornisce abitualmente, per mezzo del personale preposto, reporting sullo stato della sicurezza ed il 32% (19% sul totale) traccia gli stessi dati solo su specifica richiesta.

Minacce - Dallo stesso studio emerge che le imprese sono molto più sensibili e consapevoli delle minacce esterne (azioni invasive), derivanti principalmente dai virus, e tendono a sottovalutare i pericoli derivanti dall'interno dell'organizzazione (abusi). Ciò induce le stesse a concentrarsi su investimenti mirati all'acquisto di firewall e antivirus, ma non dedicano risorse allo sviluppo di strategie più complesse di governo e non operano formazione del personale.

I dati raccolti da Ernst & Young rilevano che il 73% delle aziende intervistate individuano nelle costrizioni di budget i maggiori limiti per l'applicazione di azioni efficaci, ed il 57% del totale intervistati afferma l'intenzione di destinare maggiori risorse alla sicurezza per 2005.

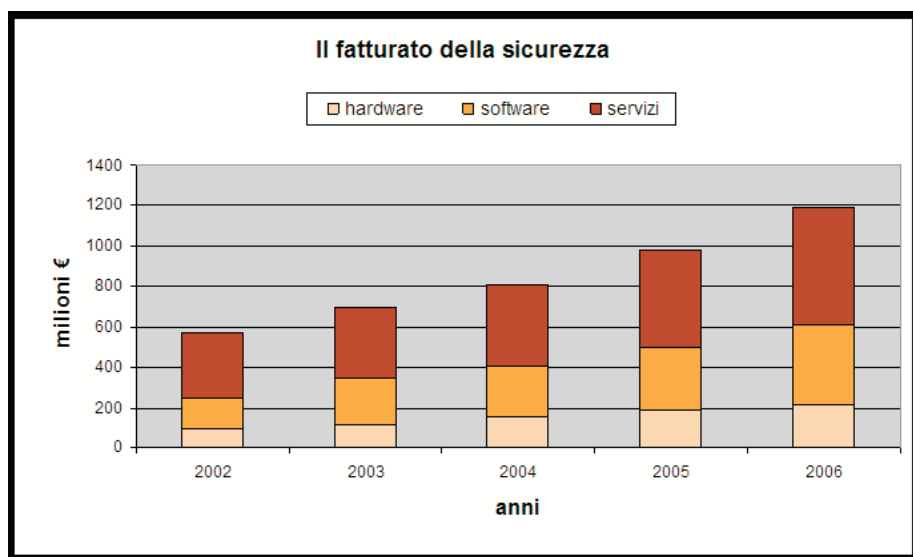
La spesa per la sicurezza informatica in Italia nel 2004 supererà di poco gli 800 milioni di euro, segnando un incremento dell'11% rispetto all'anno precedente, ma secondo Sirmi, che ha condotto uno studio sul fenomeno, tale cifra è destinata a crescere con percentuali molto superiori rispetto gli altri comparti IT.

Anche IDC rileva lo stesso trend di crescita e prevede per i due esercizi futuri in incremento del 20% per ogni anno, con particolare benefici per i servizi erogati in outsourcing.

Uno studio condotto dall'osservatorio Storage Index su 690 aziende rileva che alcuni aspetti della sicurezza rappresentano, per l'81% degli intervistati la priorità più alta per i futuri investimenti.

In Italia l'esigenza di adeguarsi alle nuove normative è strategica solo per il 38% (al 30/09/2004), anche se è da segnalare l'incremento del 6% rispetto agli ultimi 3 mesi (30/06/2004)

Il 69% degli IT Manager italiani percepiscono come priorità la continuità operativa (business continuity) da garantire con un budget limitato.





Netsecurity Platform

la piattaforma per la sicurezza gestita

"information security il punto"

Tutti i dati riportati si possono tradurre in bisogni di sicurezza e continuità che le PMI devono soddisfare, incalzati da esigenze di competitività ed efficienza ma anche dall'adempimento di nuove normative, facendo i conti con budget limitati e con risorse inadeguate alla complessità delle problematiche.

Riteniamo che rispondere a questi bisogni proponendo pacchetti software ed apparati hardware sia anacronistico e spesso inefficace nel tempo.

Crediamo che l'approccio vincente sia quello di soddisfare i medesimi bisogni fornendo un servizio che inglobi il valore aggiunto della competenza e dell'esperienza nel settore, che sgravi le aziende da investimenti non remunerativi ed elevati costi di gestione, che eviti modifiche alle infrastrutture esistenti de-localizzando la gestione su un *security center* protetto, evoluto e performante. Un servizio che massimizzi il rapporto efficacia/spesa attraverso la modularità di soluzioni dal costo accessibile, vigilate, assistite ed aggiornate in ogni istante di ogni giorno di un anno.

Il servizio *Net Security* di **Msoft** è una risposta a molti problemi, questa è l'unica *sicurezza*.