



Press Release

Cisco pubblica il suo primo report sul panorama mondiale della sicurezza

L'edizione 2007 prende in esame le minacce di sicurezza relativamente a sette categorie di rischio, include previsioni per il 2008 e presenta linee guida formulate dai principali esperti di sicurezza dell'azienda

Milano, 7 gennaio 2008 – Con l'obiettivo di fare luce sulle principali tendenze in tema di security, Cisco ha recentemente diffuso il suo primo report annuale sulla situazione globale della sicurezza. Il documento evidenzia i crescenti rischi e le sfide che aziende, governi e consumatori devono affrontare e propone suggerimenti per difendersi.

Il Cisco Annual Security Report 2007, diffuso contemporaneamente al lancio della versione aggiornata del sito Cisco Security Center (www.cisco.com/security), passa in rassegna le tematiche di sicurezza che hanno tenuto banco nello scorso anno; inoltre include previsioni per l'anno 2008 e raccomandazioni formulate dai più importanti esperti Cisco in materia di security, quali John Stewart, Chief Security Officer dell'azienda, e Dave Goddard, che ricopre il ruolo di Vice President Customer Assurance and Security Programs.

A differenza dei tanti report di fine anno in questo settore, che sono focalizzati sulle minacce alla sicurezza dei contenuti (virus, worm, trojan, spam e phishing), il report Cisco amplia l'ambito della discussione includendovi sette categorie di risk management, andando quindi ben oltre le singole criticità relative alla sicurezza dei contenuti. Le categorie in questione sono la vulnerabilità, la sicurezza fisica, il cybercrime, la minaccia interna, l'identità, l'errore umano e il rischio geopolitico; nell'insieme, esse riguardano requisiti di sicurezza quali la protezione dal malware, la protezione dalla fuoriuscita non autorizzata di dati, la gestione del rischio a livello d'impresa, il disaster planning e molto altro ancora.

I contenuti del report Cisco confermano ulteriormente il fatto che le minacce e gli attacchi informatici hanno ormai assunto una dimensione globale ed assai più sofisticata che in passato. La crescente diffusione di applicazioni, strumenti e metodi di comunicazione basati su IP crea infatti le condizioni per sferrare un maggior numero di attacchi; si sta così aprendo un nuovo capitolo nella storia delle minacce alla sicurezza e nelle metodologie di assalto.

Anni fa, virus e worm (ad esempio Code Red, Nimbda ed altri) infettavano i sistemi informatici allo scopo di far danno e di dare notorietà ai loro creatori. Con la diffusione dell'uso di Internet e dell'e-commerce, sono nate nuove minacce miste

(attacchi di phishing realizzati con l'invio di spam, botnet ecc.) create allo scopo di sottrarre informazioni personali e denaro. Questo approccio "stealth-and-wealth" si è poi ulteriormente evoluto, assumendo dimensioni globali e caratteristiche tali da riguardare di frequente e contestualmente più di una delle sette categorie di rischio elencate nel report.

Secondo Stewart, la sicurezza delle informazioni non è più semplicemente una battaglia contro un virus o un attacco spam. Spesso sono in gioco anche fattori di tipo legale, di identità e geopolitici. Stewart fa riferimento, ad esempio, ai furti di identità realizzati ai danni delle grandi catene commerciali, e ad un recente attacco di distributed denial-of-service avvenuto la scorsa primavera, che sembra sia stato lanciato da hacker russi contro la vicina Estonia con motivazioni di tipo politico. Secondo le notizie disponibili, l'attacco sarebbe stato una reazione alla decisione delle autorità estoni di rimuovere un monumento di guerra dell'era sovietica da un parco; il risultato è stato il blocco completo di numerosi siti web governativi del paese.

“Il crimine informatico sta cambiando pelle sotto i nostri occhi, e spesso si serve di tecniche ben note, ma che in precedenza erano utilizzate solo tramite mezzi elettronici” spiega Stewart. “Non ci si può permettere di affrontare le minacce alla sicurezza delle informazioni come se si trattasse di battersi solamente contro un virus, o un attacco di phishing; le minacce implicano tecniche di social engineering e tecnologia, così come il riconoscimento della fiducia e dell'uso pervasivo della Rete. Oggi, lo sforzo per mantenere al sicuro le aziende, i paesi e l'identità delle persone richiede un elevato livello di coordinamento fra attori che, tradizionalmente, non collaboravano tanto strettamente quanto sarà loro necessario in futuro. I team che si occupano della sicurezza IT, le aziende, i governi, le forze dell'ordine, i consumatori, i cittadini: sono tutti potenziali obiettivi di attacco, ma anche tutti potenziali alleati. L'efficacia della sicurezza a livello nazionale, aziendale e personale dipenderà dalla collaborazione e dalla comunicazione fra tutti questi soggetti”.

Secondo Stewart e Goddard, alla base del successo di questa collaborazione c'è una azione educativa. Il report Cisco propone numerose linee guida per ognuna delle sette categorie di risk management individuate. Ecco alcune delle più importanti.

- Condurre su base regolare verifiche all'interno delle organizzazioni che possono costituire un target interessante per il crimine informatico e valutare le possibili modalità con cui esse possono essere attaccate. “Gli attacchi spesso finiscono per avere successo perché non si sono seguiti i principi base della sicurezza: prevenzione delle intrusioni a livello di host, aggiornamento dei sistemi con le patch e gli upgrade che risolvono problemi di sicurezza, e verifiche regolari” afferma Stewart.
- Tenere ben presente il fatto che le minacce agiscono in parallelo con le modalità di utilizzo dei sistemi “Gli hacker vanno dove vanno i più” spiega Goddard. “Ed ogni volta che si inserisce una nuova applicazione o un nuovo dispositivo, emergono nuove minacce”.

- Cambiare la mentalità dei dipendenti, dei consumatori e dei cittadini, che tendono a considerarsi semplici spettatori, dando loro la possibilità di diventare attori influenti, condividendo la responsabilità della sicurezza. I team IT dovrebbero guidare questo cambiamento, ma non è un compito di loro esclusiva pertinenza.
- Dare priorità all'educazione in materia di sicurezza. Le aziende, i vendor del settore security e gli enti governativi devono investire per educare e creare consapevolezza del problema. Questa azione dovrebbe prevedere anche una collaborazione a livello di settore fra partner e fra concorrenti.
- Istituzionalizzare la formazione nel campo della sicurezza IT includendola nei curriculum scolastici e accademici.
- Quando si costruisce una rete sicura, non tenere in considerazione solamente le prestazioni; concentrarsi piuttosto sulla capacità della rete di collaborare, analizzare, adattarsi e risolvere i problemi di sicurezza globalmente, a partire da gateway e server fino ai desktop e ai dispositivi mobili.
- I fornitori di sicurezza devono offrire soluzioni omnicomprensive, che coprano tutta l'infrastruttura di rete, l'insieme delle applicazioni attive su di essa e i dati stessi.

Il report è disponibile per la consultazione all'indirizzo:

http://www.cisco.com/web/about/security/cspo/docs/Cisco2007Annual_Security_Report.pdf

#

Cisco

Cisco (NASDAQ:CSCO) è leader mondiale nella fornitura di soluzioni di rete che trasformano il modo con cui le persone comunicano e collaborano. Notizie e informazioni relative alla società e ai prodotti sono disponibili all'indirizzo <http://www.cisco.com/it>. Le apparecchiature di Cisco Systems sono fornite in Europa da Cisco Systems International BV, una consociata interamente controllata da Cisco Systems, Inc.

###

Ufficio Stampa
Cisco Systems
Cristina Marcolin

Tel: 039/62951
email: pressit@external.cisco.com

Prima Pagina Comunicazione
Benedetta Campana
Caterina Ferrara
Vilma Bosticco
Tel: 02/76.11.83.01
email: ciscotech@primapagina.it