Aspetti di sicurezza per il deployment dell'IPV6

Antonio De Martino

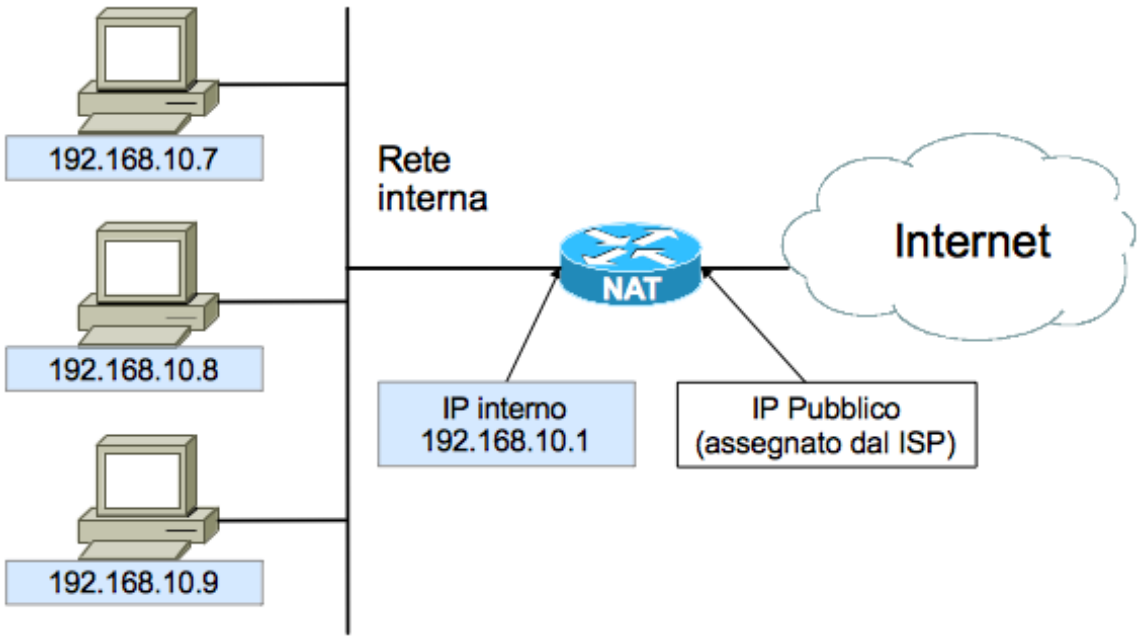
ICT Security Engineer e Project Manager

Il 6 Giugno 2012 numerosi siti web hanno pubblicato la notizia relativa al lancio ufficiale del Internet Protocol versione 6, IPv6, in sostituzione dell'attuale versione IPv4 a causa dell'esaurimento di indirizzi IP pubblici disponibili.

Un indirizzo IP è una sequenza di numeri che identifica univocamente un computer in Internet, per esempio 173.194.35.48, che corrisponde a uno dei sistemi che pubblicano la pagina iniziale di Google.

Inizialmente gli indirizzi IPv4 furono distribuiti ai grandi service provider, alle università e agli enti come l'Internet Assigned Numbers Authority (IANA) preposti all'assegnazione che avevano il compito di garantirne la gestione. Nonostante lo schema IPv4 permettesse il collegamento di svariati milioni di computer, ben presto si capì che era necessario ideare un nuovo metodo di indirizzamento per far fronte alla crescente domanda di indirizzi IP, legata alla diffusione dei computer per uso privato e al commercio elettronico.

Il documento che definisce il protocollo IPv6 è la RFC 2460 del 1998, ma il lancio vero e proprio è avvenuto molti anni più tardi. In questo lasso di tempo infatti i maggiori produttori di dispositivi di rete hanno cercato di sfruttare al massimo le possibilità offerte dall'IPv4, realizzando apparati capaci di implementare tecniche di traduzione degli indirizzi, generalmente conosciute come NAT (Network Address Traslation), per ottimizzarne il consumo.



L'IPv4 offre infatti la possibilità di creare reti locali tramite alcuni classi di indirizzi speciali. Questo significa che le aziende e le organizzazioni possono realizzare la propria rete interna utilizzando la categoria di indirizzi privati che meglio si adatta alle proprie esigenze. La tecnica di NAT permette di tradurre uno qualsiasi degli indirizzi privati della rete locale con un unico indirizzo pubblico appartenente ad Internet, riducendo quindi l'utilizzo degli indirizzi ormai in esaurimento. In altri termini un computer può comunicare con il mondo esterno grazie a un indirizzo ip di un altro dispositivo già connesso a Internet.

Questo metodo fornisce da un lato il vantaggio di “nascondere” gli indirizzi dei computer privati rendendoli non visibili direttamente da Internet, dall’altro porta con se una serie di problematiche legate alla complessità delle configurazioni, al sovraccarico della memoria degli apparati di rete (che devono mantenere una tabella di associazioni per gestire le comunicazioni) ed ha causato non pochi problemi per le implementazioni di alcuni protocolli applicativi.

Il primo vantaggio offerto dall’IPv6 è il notevole aumento dello spazio di indirizzi che passa dai circa 4.294 miliardi (2^{32}) del IPv4 ai circa $3.4x10^{38}$ ovvero 2^{128} indirizzi con IPv6. Per poter comprendere la necessità di un così elevato numero di indirizzi, basti pensare ai moderni dispositivi elettronici come smart-phone, tablet e TV che sono già tutti connessi a Internet e all’opportunità di connetterne di nuovi per fornire molti altri servizi, si pensi infatti a tutti servizi di controllo remoto, telerilevamento ambientale e automazione.
Si prevede una crescita del numero di oggetti collegati alla rete tale da introdurre il concetto di ”Internet delle cose” e in questo scenario la sicurezza ricopre un aspetto fondamentale.

L’IPv6 è un protocollo dotato di sicurezza nativa. Quella che oggi conosciamo come suite di protocolli IPsec (IP Security), funzionalità che si aggiunge ad IPv4 per aumentare la salvaguardia delle comunicazioni, è in realtà una caratteristica intrinseca dell’IPv6. IPsec è infatti obbligatorio nell’implementazione di una rete IPv6.

Tuttavia ci sono non poche preoccupazioni riguardo la realizzazione di una Internet completamente IPv6, principalmente per gli aspetti legati alla sicurezza. L’infrastruttura di rete attuale, infatti, è formata da alcuni strumenti e dispositivi IPv4 che non supportano ancora IPv6, mentre altri che funzionano con IPv6 ma non sono correttamente configurati dai vari amministratori di sistema. Di conseguenza, alcuni firewall e dispositivi per la gestione delle intrusioni, sono in grado di rilevare malware solo su traffico dati IPv4.

In pratica un attaccante potrebbe potenzialmente superare tutti i controlli e i meccanismi di sicurezza con l'invio di malware sfruttando il traffico dati IPv6. Un'altra preoccupazione è rappresentata dalle debolezze specifiche del protocollo, che possono essere utilizzate da un aggressore per condurre un attacco contro il livello rete di IPv6.

Alcuni ricercatori hanno già pubblicato delle guide e messo a disposizione degli strumenti di verifica e di penetration test. Il toolkit di penetration test, pubblicato dal sito The Hacker Choice (www.thc.org), è un buon esempio di strumento attualmente a disposizione.

La migrazione da IPv4 ad IPv6 è necessaria in quanto la nuova versione del protocollo non è compatibile con la precedente. Il processo dovrebbe essere programmato e graduale. Prima di iniziare si dovrebbe semplificare e assestare l’infrastruttura di rete esistente in IPv4 eliminando tutte le funzionalità non più necessarie.

Dato che il passaggio a IPv6 non sarà istantaneo, e che gli apparati IPv4 resteranno in rete per molto tempo ancora mentre la migrazione è in corso, sarà necessario mettere in campo dispositivi dual stack in grado di comunicare con entrambe le versioni del protocollo. Tutti i nuovi dispositivi di rete messi in campo dovrebbero essere certificati da enti esterni che ne garantiscano la piena compatibilità di funzionamento nelle reti IPv6 per evitare inattesi malfunzionamenti.

Una volta che tutti gli apparati IPv6 sono stati correttamente inseriti nel segmento di rete in corso di migrazione, questi dovrebbero essere sottoposti a un rigoroso processo di hardening delle configurazioni prima del collegamento con domini di rete esterni. Il processo di hardening avrebbe non solo il vantaggio di ridurre i rischi legati alle varie dinamiche di attacco ma anche quello di abbassare il carico elaborativo dell'apparato disabilitando i servizi non necessari.

Non è da trascurare inoltre la formazione e l'aggiornamento professionale degli addetti ai lavori. Gli operatori dovranno essere preparati a gestire eventuali problemi di incompatibilità ed avere le conoscenze necessarie per applicare le configurazioni per contrastare gli eventi di sicurezza che potrebbero verificarsi.

Il passaggio a IPv6 sarà un'operazione del tutto trasparente agli utenti e non avrà nessun effetto sull'usabilità della rete, ma il periodo di transizione non sarà affatto breve. I centri di ricerca e le organizzazioni che operano nel settore hanno rilasciato diversi studi e linee guida a supporto della diffusione dell'IPv6. Il NIST, National Institute of Standards and Technology, per esempio ha pubblicato il documento 800-119[1] Guidelines for the Secure Deployment of IPv6.

L'argomento è un tema chiave anche per l'Europa[2]. Il vicepresidente della Commissione Europea, Neelie Kroes, ha infatti incoraggiato tutti gli stakeholder in gioco a procedere velocemente alla migrazione verso IPv6 per evitare un impatto negativo sia sull'innovazione che sui mercati.

L'8 giugno 2011 i grandi service provider come Google, Facebook, Yahoo!, Akamai e Limelight Networks e altri 1000 siti web hanno partecipato a un primo test[3] di 24 ore per la sperimentazione del nuovo IPv6. I risultati ottenuti sono stati molto incoraggianti ed hanno dimostrato su scala globale la fattibilità dell'operazione di migrazione dando una spinta importante al passaggio alla nuova architettura.

L'ing. Antonio DE MARTINO, laureato presso l'Università degli studi di Napoli Federico II in Ingegneria Informatica con specializzazione sull'Enterprise Application Integration, si è occupato di progettazione di infrastrutture ICT sicure, hardening e sicurezza di apparati di rete, di piattaforme per l'identity management ed il controllo degli accessi. Oggi si occupa di project management di architetture di sicurezza informatica, in particolare di soluzioni di accesso controllato alle reti dati.

Riferimenti

http://www.thc.org/thc-ipv6/
http://www.sans.org/reading_room/whitepapers/protocols/security-features-ipv6_380
http://www.sans.org/reading_room/whitepapers/detection/complete-guide-ipv6-attack-defense_33904

1 http://www.nist.gov/itl/csd/ipv6_010511.cfm
2 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/837
3 http://www.wired.co.uk/news/archive/2011-01/14/ipv6-test-day