Lo stack TCP/IP di Windows 2000 e i parametri di sicurezza

Lo stack TCP/IP implementato da Microsoft nei sistemi operativi della famiglia Windows 2000 introduce, rispetto alle precedenti implementazioni, alcuni miglioramenti quali:

- l'aumento delle dimensioni di default delle finestre TCP e l'introduzione di nuovi algoritmi diretti a migliorare i collegamenti ad alta congestione e ritardo nonchè le prestazioni complessive dello stack;
- il pieno supporto per la RFC 1323 per quanto riguarda le dimensioni delle finestre TCP scalabili;
- il pieno supporto per il meccanismo delle conferme selettive (SACK - Selective Acknowledgments);
- un meccanismo veloce di ritrasmissione dei pacchetti TCP;
- miglioramenti negli algoritmi per il calcolo del Round Trip Time (RTT) e del Retransmission Timeout (RTO);
- miglioramenti nella gestione di un elevato numero di connessioni;

Inoltre è stato garantito il supporto per altre caratteristiche come IPSEC (Internet Protocol Security), NAT (Network Address Translation), QoS (Quality of Service), L2TP (Layer Tunneling Protocol) e così via.

Parametri di sicurezza dello stack

La suite di protocolli TCP/IP di Windows 2000 ricava tutte le informazioni per il suo corretto funzionamento dal Registro di sistema dove esse vengono scritte dal programma di installazione ed, in alcuni casi, dal servizio client DHCP qualora esso venga utilizzato.
Generalmente le impostazioni di default si rivelano sufficienti per una grande varietà di ambienti tuttavia in alcune circostanze (come ad es. nel caso di un Web Server) può essere opportuno riconfigurare manualmente alcuni parametri in modo tale da migliorare la robustezza dello stack TCP/IP ed il livello generale di sicurezza.
Attenzione: le modifiche manuali apportate al registro possono rendere instabile l'intero sistema. Pertanto prima di compiere qualsiasi operazione si raccomanda di effettuare un backup dei dati e dello stesso registro di configurazione. Inoltre è fortemente consigliata una fase di verifica circa il corretto funzionamento delle nuove impostazioni su sistemi di test prima di replicare qualsiasi modifica su un sistema in produzione.
Grazie alla esperienza maturata nella gestione dei laboratori di **Win2000test.com** la Microsoft è riuscita ad aggiungere al registro di configurazione un set di chiavi che possono essere impostate con valori "tarati" in modo tale da accrescere la resistenza del sistema soprattutto nei confronti di certe tipologie di attacco (vedi gli attacchi di tipo Denial of Service).

I parametri in questione si trovano sotto la chiave di registro **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpipParameters** e sono i seguenti:

- **SynAttackProtect (REG_DWORD - valori validi: 0,1,2)**: la corretta impostazione di questa chiave comporta una riduzione dei tentativi di ritrasmissione dei segnali SYN-ACK, riducendo di fatto il tempo in cui le risorse associate alle connessioni devono rimanere allocate. Peraltro affinchè questo meccanismo di protezione operi effettivamente occorre che i valori massimi impostati per le chiavi **TcpMaxHalfOpen** e **TcpMaxHalfOpenRetried** siano superati. Il valore di default della chiave è 0 (nessuna protezione) ma un valore di 2 viene in genere raccomandato. Quest'ultimo offre naturalmente la migliore protezione poichè l'allocazione delle risorse viene di fatto ritardata fino al momento in cui il three-way handshake è stato completato; tuttavia la stessa impostazione può a volte determinare l'insorgere di problemi di connettività soprattutto per gli utenti che fanno uso di connessione remote caratterizzate da tempi di risposta lunghi. Inoltre è opportuno ricordare che quando la chiave assume il valore di 2 alcune funzionalità dello stack non sono utilizzabili (in particolare il meccanismo delle finestre scalabili, la dimensione delle finestre e il Round Trip Time iniziale);
- **TcpMaxHalfOpen (REG_DWORD - valori validi: 100 - 0xFFFF):** questo valore fissa il numero massimo di connessioni che si trovano in stato SYN_RCVD permesso prima che la protezione della chiave **SynAttackProtect** cominci ad operare (il valore di default è 100 per i sistemi Windows 2000 Professional e Server e 500 per quelli Advanced Served). La determinazione del valore più opportuno dipende dall'ambiente ma soprattutto dal volume di traffico che il server deve normalmente sostenere;
- **TcpMaxHalfOpenRetried (REG_DWORD - valori validi: 80 - 0xFFFF):** questo valore fissa il numero massimo di connessioni in stato SYN_RCVD per le quali vi sia già stata la ritrasmissione di un segnale di SYN permesso prima che la protezione della chiave **SynAttackProtect** cominci ad operare (il valore di default è 80 per i sistemi Windows 2000 Profesional e Server e 400 per quelli Advanced Server). Anche per questa chiave la determinazione del valore più opportuno dipende dall'ambiente ma soprattutto dal traffico che normalmente il server deve sostenere;
- **EnablePMTUDiscovery (REG_DWORD - Boolean - valori validi: 0,1):** questo parametro influenza il comportamento dello stack TCP/IP nella determinazione del valore della MTU cioè della dimensione massima dei pacchetti di rete. Un valore di default pari ad 1 comporta una limitazione di questa dimensione in modo tale che essa si adatti ad un valore precedentemente individuato. Questo si traduce in una minore probabilità che il pacchetto subisca una frammentazione da parte dei routers con MTU inferiore posti lungo il percorso di instradamento. A dispetto dei vantaggi derivanti da una impostazione di questo tipo viene comunque raccomandato un valore di 0 (false) poichè così facendo viene utilizzato un valore fisso di 576 byte per tutte le connessioni non dirette agli host della rete locale con conseguente impedimento di tutti quei tentativi di forzare la MTU a valori bassi nel tentativo di sovraccaricare lo stack;
- **EnableDeadGWDetect (REG_DWORD - Boolean - valori validi: 0,1):** quando questo parametro assume il valore di 1 (default) allora lo stack TCP è in grado di sfruttare le funzionalità di riconoscimento dei cd. "dead gateway". In base a questo meccanismo quando una connessione instradata tramite il default gateway invia un pacchetto TCP senza ricevere risposta da parte del target per un certo numero di volte (pari alla metà del valore impostato per la chiave **TcpMaxDataRetransmission)** allora la cache dei percorsi di routing viene sovrascritta in modo da impostare per questa connessione un gateway secondario purchè esso sia stato definito nelle impostazioni di rete. Il valore consigliato per la chiave è 0 perchè di fatto esso impedisce ad un eventuale aggressore di forzare il passaggio delle connessioni verso gateway non desiderati;
- **KeepAliveTime (REG_DWORD - valori validi: 1 - 0xFFFFFFFF):** questo parametro indica la frequenza (millisecondi) dei tentativi con i quali lo stack verifica che una connessione inattiva sia ancora integra tramite l'invio di un pacchetto keep-alive. Il valore di default è di 7.200.000 millisecondi (pari a due ore) ma viene consigliato un valore di 300.000, corrispondente a 5 minuti;

In aggiunta a quella già menzionate esistono inoltre altre due chiavi del registro di sistema che possono influenzare la sicurezza di rete: una è situata nel percorso **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ TcpipParametersInterfaces<nr. interfaccia>** :

- **PerformRouterDiscovery (REG_DWORD - valori validi: 0,1,2):** questo parametro controlla se il sistema operativo tenta di effettuare la scoperta del router in applicazione della RFC 1256. Il valore consigliato è 0 poichè esso previene i tentativi di un attacco tramite contraffazione di router che un eventuale aggressore può porre in essere. Il valore di default in genere è 2 nel caso di utilizzo del servizio DHCP oppure 0;

mentre l'altra è localizzata sotto **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ NetBTParametersInterfaces<nr. interfaccia>:**

- **NoNameReleaseOnDemand (REG_DWORD - Boolean - valori validi: 0,1):** questa parametro specifica se il sistema rilascia il suo nome NetBIOS quando riceve una richiesta di tipo Name-Release dalla rete. Il valore di default è 0 mentre viene consigliato un valore di 1 poichè esso protegge contro gli attacchi che provocano il rilascio del nome (Microsoft Security Bullettin MS00-047). Tuttavia è anche opportuno ricordare che questa impostazione potrebbe non avere alcun effetto per una interfaccia di rete per la quale siano stati disabilitati i servizi NetBIOS/SMB/CIFS (come effettivamente dovrebbe essere per l'interfaccia di rete esterna di un server Web);