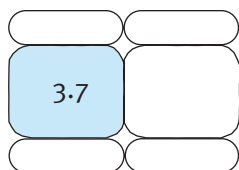




SICUREZZA E BUSINESS IN RETE

Marco Mezzalama
Edoardo Calia



La sicurezza è oggi percepita dal mondo occidentale come esigenza fondamentale. Questo senso di incertezza è avvertito anche nel settore informatico e delle TLC. Oggi i sistemi informativi costituiscono il cuore dei processi aziendali e la loro sicurezza fisica e logica diventa un elemento determinante. Se si considera che un sistema informativo odierno non può prescindere dall'infrastruttura di rete si comprende come la sicurezza della rete informatica sia condizione necessaria per la sicurezza del sistema e del patrimonio aziendale.

1. LO SCENARIO

Non molto tempo fa il noto settimanale americano Newsweek indicava come “la sicurezza informatica fosse il fattore abilitante per un reale uso commerciale di Internet”. Affermazione suffragata da una recente indagine sugli utilizzatori di Internet che indica in circa l'80% la quota di coloro che non utilizzavano ambienti di *e-commerce B2C (Business to Commerce)* a causa di presunti rischi di sicurezza sulla rete.

Una rete è essenzialmente un'infrastruttura costituita da connessioni e apparati che collega calcolatori (*host*) al fine di far interoperare questi ultimi e di realizzare servizi applicativi. Ma la rete e i servizi applicativi che su essa si appoggiano risultano veramente insicuri, e se sì dove sono le cause e quali i rimedi?

Ebbene se si considera l'ultima edizione dello studio condotto da CSI (*Computer Security Institute*) in collaborazione con l'FBI di San Francisco nel 2002 e si valutano le prime 20 criticità rilevate su sistemi in rete,

ci si accorge che ben 17 riguardano “debolezze” proprie degli *host*, e in particolare dei loro sistemi operativi. Un esempio per tutti è lo sfruttamento del cosiddetto *buffer overflow*, tecnica che satura di messaggi opportuni i buffer del sistema operativo, permettendo in tal modo di acquisire il controllo totale o parziale del sistema. Pertanto, nel valutare le problematiche di sicurezza verranno prese in considerazione le azioni, le minacce e le vulnerabilità che riguardano sia la rete come infrastruttura (protocolli e apparati di rete) sia i calcolatori a essa connessi e che realizzano servizi di rete, quali *e-mail* o *web server*.

Per semplicità di esposizione verranno suddivise le criticità in tre aree distinte: quelle che fanno riferimento ai protocolli e agli apparati di rete, quelle che interessano i sistemi operativi e i *data base* e, infine, quelle che riguardano le applicazioni.

Ci si soffermerà soprattutto sulle prime, pur considerando anche il secondo ambito essendo sovente strettamente interdipendente dal primo.

1.1. Attacchi alla sicurezza: tipi ed evoluzione

Il fatto che negli ultimi anni le minacce e gli attacchi ai sistemi in rete siano notevolmente cresciuti è un dato reale. I dati indicati dal CERT (*Computer Emergency Report Team*) relativi a incidenti accertati di intrusione indicano, come illustrato in figura 1, un tasso di crescita esponenziale che negli ultimi anni può essere semplificato indicando un fattore di crescita pari a circa 2,5/anno. Ancora più significativo appare il dato che evidenzia il crescere di nuove tipologie di vulnerabilità, denotando come, al crescere della complessità dei sistemi, protocolli e apparati, cresca di concerto quella delle tecniche di attacco: si passa da circa 300 tipi di tecniche di attacco nel 1997, a 1090 nel 2000, a 3750 nel 2002.

Nella definizione di questo quadro è opportuno citare il rapporto annuale "Computer Security Issues&Trends" del CSI/FBI. Esso si basa su una puntuale analisi condotta su un campione di circa 500 aziende americane rappresentative del contesto industriale e dei servizi. Tra i vari dati ottenibili dal report, direttamente scaricabile dalla rete, appare interessante citare i seguenti:

- il 90% del campione ha subito attacchi diretti al sistema IT (*Information Technology*);
- l'80% ha rilevato perdite finanziarie, con valor medio pari a circa 7.000.000 di dollari in crescita significativa rispetto agli anni passati (un fattore 3 rispetto all'anno precedente);
- le perdite più significative riguardano il furto di informazioni o le frodi finanziarie;
- l'85% hanno subito un attacco da *virus* o *worm*;
- il 38% hanno rilevato accessi non autorizzati al proprio sito web.

Per definire un quadro completo delle criticità cui può essere assoggettato un sistema informatico, è importante conoscere da dove proviene l'attacco e da chi. Anche a queste domande si può rispondere facendo riferimento al già citato rapporto CSI/FBI.

Nella figura 2 è illustrato, nel corso degli ultimi tre anni, quale sia il punto di partenza di un attacco: si noti come sia preponderante la provenienza dalla rete Internet, sebbene risulti notevole ancora la percentuale di minacce portate dall'interno dell'azienda.

Questa lettura, che stempera abbastanza il

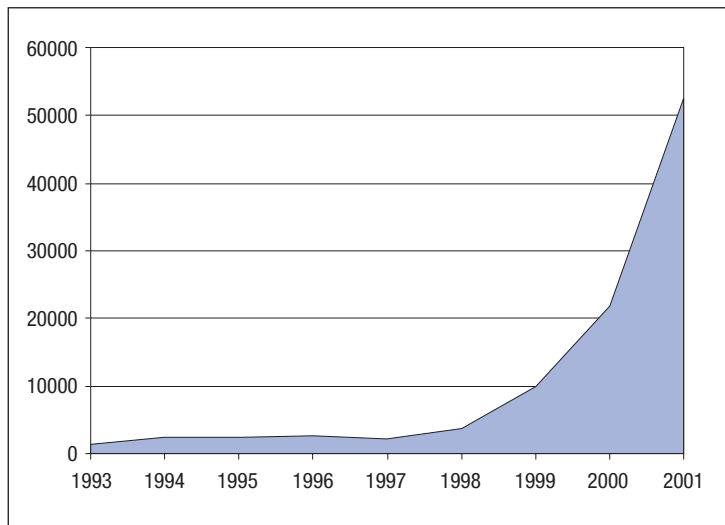


FIGURA 1

Numero di incidenti segnalati dal 1993 al 2001

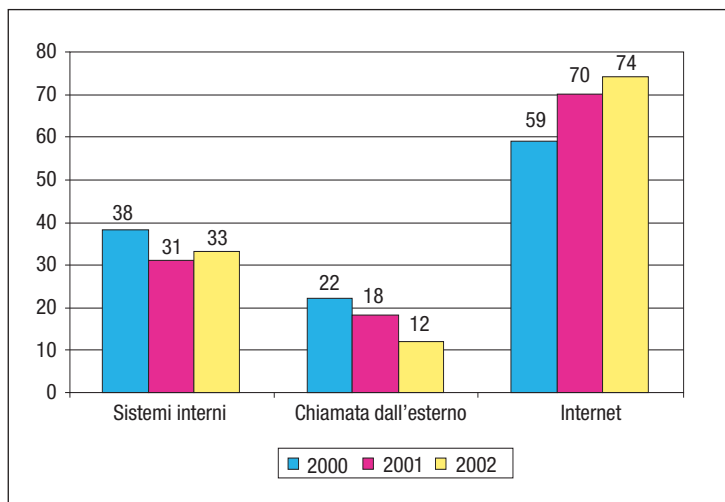


FIGURA 2

Provenienza degli attacchi
(Fonte: CSI/FBI 2002)

mito che gli attacchi al sistema aziendale derivino principalmente dall'esterno, è rafforzata dai dati relativi ai soggetti che mettono in atto un attacco riportati in figura 3. Si evince come il rischio "interno" risulti significativo e come, pertanto, una saggia politica di sicurezza debba guardare con attenzione non solo "fuori ma anche dentro le mura".

Un'ultima considerazione in questo scenario preliminare, riguarda i danni economici subiti per attacchi informatici. Il Club Sicurezza Informatica ipotizzava nel 1999, in Italia, una perdita generica dovuta ad attacchi e malfunzionamenti valutabile in circa 1.500 milioni di euro. Sempre dal rapporto CSI/FBI sono, inoltre, desumibili non i valori assoluti delle perdite, bensì quelli relativi per classe

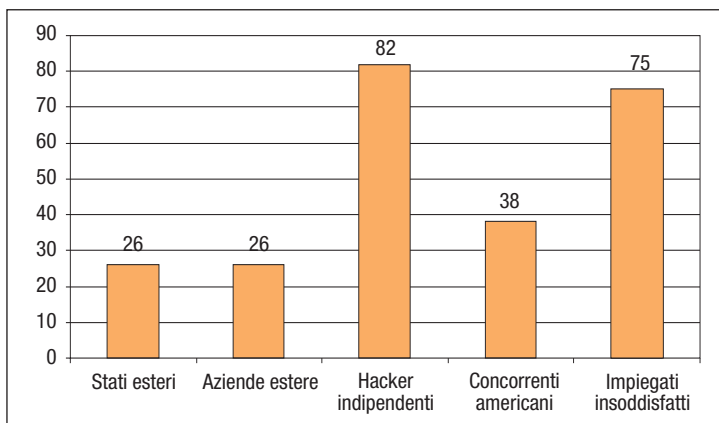


FIGURA 3
Attuatori degli attacchi
(Fonte: CSI/FBI 2002)

di vulnerabilità. Normalizzando a 100 le perdite dovute a furti di informazioni riservate, che come si è detto, costituiscono la classe con il valore assoluto più elevato, si ottengono i valori relativi riportati nella tabella 1.

In generale, i dati precisi sulle perdite economiche dovute a intrusioni, minacce e vulnerabilità varie sono difficili da ottenere per problemi sia di riservatezza (l'80% degli attacchi con o senza danni non viene denunciato o, comunque, reso esplicito) sia di valutazione tra costi diretti e indiretti.

È possibile, tuttavia, disporre di alcuni dati attendibili, ad esempio sui costi dei danni prodotti da virus e worm. Nel 1999, si stima che siano stati persi globalmente circa 8 miliardi di dollari per worm di rete, di cui una parte consistente dovuti al worm *Melissa*. Nel 2001, il worm *Red Code*, che in poco meno di 9 min ha compromesso 250.000 computer, si stima abbia provocato danni per 2,6 milioni di dollari. Una cifra assai significativa se si pensa che il danno complessivo alle strutture IT in occasione dell'attacco terroristico dell'11 settembre è stimato pari a circa 12 milioni di dollari.

TABELLA 1
Perdite dovute ad attacchi informatici per classi di vulnerabilità

DOS (<i>Denial of Service</i>)	13
Virus/worm	30
Accessi dall'esterno non autorizzati	11
Furti di informazioni riservate	100
Frodi finanziarie	68
Sabotaggi	9
Abuso nell'uso delle reti interne	29

2. SICUREZZA DELLE RETI

L'insieme delle comunicazioni fisse e mobili si sta oggi muovendo verso un significativo punto di aggregazione costituito dall'adozione del paradigma dei **protocolli Internet**. In particolare, le reti basate su *Transmission Control Protocol (TCP)* e *Internet Protocol (IP)* costituiscono, ormai, la quasi totalità delle reti orientate ai dati e stanno diventando predominanti anche per reti orientate ad altri flussi informativi, quali la voce e il video. Ne deriva che la trattazione che verrà fatta in questo articolo si orienterà esclusivamente alle reti di tipo TCP/IP.

Va subito osservato che la genesi dei protocolli Internet, realizzati sostanzialmente negli anni '70 e '80, ha tenuto conto, in modo assai marginale, dei problemi di sicurezza derivanti dall'uso intensivo di tali protocolli in un contesto pubblico, assai complesso, e ancor meno dei servizi applicativi che imponevano vincoli di sicurezza stringenti, si pensi alle transazioni economiche via web. Ciò ha determinato una serie di vulnerabilità, ancora oggi presenti, che costituiscono la base su cui varie minacce, quali virus, worm, attacchi alla disponibilità dei sistemi, si basano. Come per altro già affermato, la vulnerabilità dei protocolli di rete deve essere associata alla vulnerabilità degli ambienti *software* sugli host.

In sintesi, i problemi di sicurezza nascono, *in primis*, dai seguenti fatti:

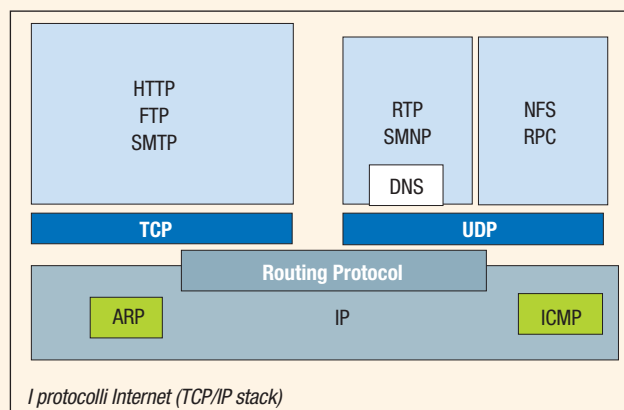
■ Le reti e i relativi protocolli di base sono per loro natura strutture insicure: per esempio, in assenza di specifiche misure, la trasmissione dell'informazione avviene sempre in chiaro, *password* comprese; le reti, specie quelle locali, operano in modalità *broadcast*; la disponibilità agevole di strumenti di gestione per l'intercettazione, la modifica di pacchetti di rete, i cosiddetti *sniffer software*;

■ gli ambienti software di sistema (sistema operativo) o applicativi contengono errori e criticità sfruttabili a fini di realizzare minacce: è il caso di errori di codifica o configurazione quali il già citato *buffer overflow*, o la presenza di *backdoor*;

■ i dati sono sempre più condivisi tra utenti e applicazioni, e ciò in assenza di politiche forti di protezione o di protocolli di negoziazione

I **protocolli** su cui si basa **Internet** si rifanno allo schema concettuale ISO-OSI, che prevede una serie di livelli logici separati di protocollo, ciascuno con funzionalità ben definite e con interfacce standard verso il livello superiore o inferiore. I protocolli della *suite* Internet possono essere classificati in tre livelli distinti, definiti come livello di rete o di *internetworking*, livello di trasporto e livello di applicazione. Si veda, a tal proposito la figura. Il livello di rete si appoggia sul livello *data-link* che non è considerato nella suite Internet e riguarda più propriamente i tipici protocolli delle reti locali (per esempio, Ethernet) oppure il protocollo punto-punto per le reti geografiche (per esempio, HDLC, PPP). Il livello di rete è caratterizzato dal protocollo IP, responsabile dell'instradamento dei pacchetti tra sottoreti anche disomogenee. Il livello di trasporto prevede due fondamentali protocolli che garantiscono una connessione diretta end-to-end di tipo affidabile o connesso (TCP) o di tipo non connesso. Il livello di applicazione riguarda, invece, un insieme di protocolli ognuno dei quali orientato a un particolare servizio Internet, tra cui il protocollo SMTP per i servizi di posta elettronica e il protocollo HTTP per la navigazione web. Va infine ricordato che, in aggiunta ai classici citati protocolli, esistono molti altri protocolli dell'architettura Internet che hanno rilevanza ai fini dell'operatività di Internet stessa. Alcuni sono protocolli relativi a servizi, altri protocolli che realizzano funzioni di controllo. Alcuni di questi ultimi rivestono particolare importanza ai fini della sicurezza. Tra questi si citano:

- il protocollo ICMP (*Internet Control and Management Protocol*), usato per scambiare informazioni sullo stato dei nodi della rete;
- i protocolli di routing (RIP, OSF, BGP ecc.), impiegati dai router per lo scambio di informazioni di instradamento;
- il protocollo DNS (*Domain Name System*) utilizzato per lo scambio di informazioni tra speciali server di rete (DNS server) che effettuano la traduzione tra indirizzi logici (per esempio www.polito.it) e indirizzi binari di rete (per esempio, 130.192.23.13).



idonei a livello di data base, tali da permettere accessi controllati e autenticati ai dati.

In questo contesto, si realizzano un'ampia serie di minacce ai fondamenti della sicurezza. Questi devono garantire la *riservatezza* e *l'integrità* dei dati, *l'autenticazione* del mittente e del destinatario, la *disponibilità* di dati e risorse e il *non ripudio*, ossia la proprietà per cui non sia possibile negare la generazione e/o la trasmissione di informazioni.

Introdurre qui una completa tassonomia dei possibili tipi di attacco o di vulnerabilità risulterebbe assai dispendioso. Si preferisce riassumere in breve le minacce che risultano quantitativamente e qualitativamente più rilevanti.

❑ **Sniffing (snooping)** È l'insieme di tecniche mirate a catturare i pacchetti che transitano sulla rete al fine di leggerne i contenuti, siano essi gli indirizzi di partenza o di arrivo, oppure il contenuto vero e proprio del pacchetto, il cosiddetto *payload*. Si tratta, pertanto, di un attacco alla riservatezza dei dati reso assai agevole da alcune tecnologie di rete, come quelle LAN (*Local Area Network*), dove l'infor-

mazione viene inviata in modalità broadcast a tutti i nodi. Nel caso di reti punto-punto, è, invece, necessario acquisire il controllo di una delle apparecchiature che costituiscono la rete, per esempio i *router*. Ci si può proteggere da attacchi di tipo *sniffing* sui dati attraverso l'impiego di opportune tecniche crittografiche, come realizzato nelle VPN (*Virtual Private Network*) sicure descritte nel seguito.

❑ **Address spoofing** Con questo termine si indicano le tecniche di attacco basate sulla generazione di pacchetti di rete contenenti l'indicazione di un falso mittente. Quando questa modifica riguarda l'indirizzo IP di un pacchetto si parla di *IP spoofing*. Si tenga presente che la manipolazione degli indirizzi di rete di un pacchetto risulta, in genere, assai semplice poiché la maggior parte dei protocolli di rete non ammettono protezioni su tali valori. Falsificando l'indirizzo del mittente si inganna il nodo destinatario con lo scopo di superare alcune protezioni di accesso, se queste sono basate sull'indirizzo del mittente, o di dirottare verso altri nodi le risposte attese o ancora di attribuire, a terzi, azioni richieste o attivate

dal pacchetto modificato, come nel caso di **attacchi DOS** (*Denial of service*) per far ricadere l'origine dell'attacco su altri nodi.

❑ **Denial of service (DOS)** Questi tipi di attacchi compromettono la disponibilità di servizi o elaboratori tenendoli impegnati in una serie di operazioni inutili o bloccando totalmente l'attività. Quando l'attacco proviene da diverse stazioni contemporaneamente, al fine di rendere molto più incisiva l'efficacia dell'attacco, si parla di *distributed DOS*, o DDOS. Gli attacchi DOS sfruttano, in genere, un'intrinseca debolezza di un protocollo di rete o una sua non idonea configurazione o implementazione. Esempi ampiamente diffusi sono gli attacchi basati sul protocollo TCP (*TCP/SYN flooding*) e ICMP (*Internet Control Message Protocol smurfing*). Tali attacchi possono essere indirizzati sia a servizi, quali i siti *www*, compromettendo in tal caso le funzionalità del servizio (l'accesso al sito per esempio o a elaboratori di rete come i router o i *server DNS*) determinando notevoli criticità all'operatività complessiva della rete.

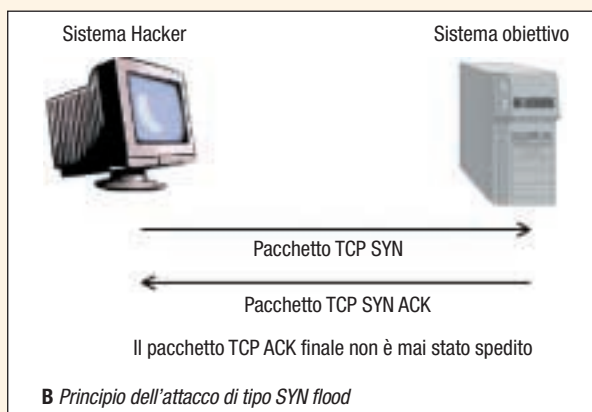
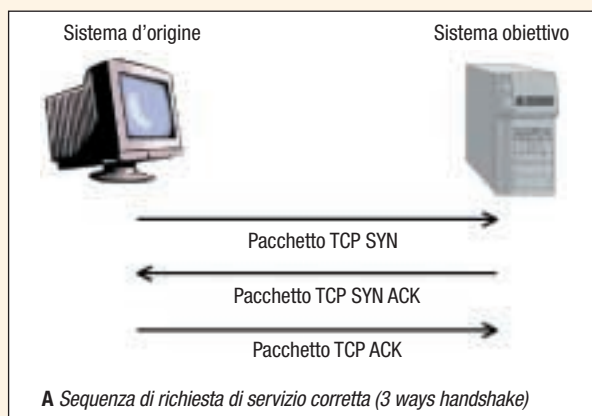
In aggiunta ai tre tipi di attacco in precedenza descritti, debbono essere ricordati ancora due fondamentali elementi che concorrono alla realizzazione di minacce per sistemi. Essi riguardano più gli host che non la rete o i suoi protocolli in senso stretto. Si tratta delle tecniche definite come *Trojan* (cavallo di Troia) e *backdoor*.

❑ **Trojan** Un Trojan (o *Trojan Horse*) è una porzione di codice, o più genericamente, un programma che realizza azioni indesiderate o non note all'utilizzatore. Tali programmi possono essere inseriti all'interno di programmi o procedure tradizionali che svolgono, apparentemente, normali funzioni applicative o di sistema. La concezione di virus informatico si basa fundamentalmente sull'impiego di programmi Trojan. Tutti i virus più famosi, da *Nimba* a *Melissa* a *I loveYou*, contenevano un "cavallo di troia", nascondevano cioè il proprio codice virale in *file* eseguibili apparentemente innocui o di sistema.

❑ **Backdoor** Con questo termine si indica un meccanismo, in generale non noto diffusa-

Per comprendere il meccanismo di un **attacco di tipo DOS** della categoria *SYN flood* è necessario tener presente che l'apertura di una normale connessione TCP si realizza inviando da parte del sistema che vuole attivare il collegamento (*source system*) un pacchetto TCP di richiesta di apertura di connessione, denominato SYN. Il sistema destinazione (*target system*) quando riceve il pacchetto SYN, pone la richiesta di connessione in una apposita lista o buffer contenenti le richieste di connessione e risponde con un pacchetto di accettazione della connessione denominato SYN ACK. Il sistema target si pone, quindi, in attesa di un'ulteriore conferma da parte del sistema *source*, conferma che si realizza mediante l'invio di un pacchetto di conferma di tipo ACK. Quando questo giunge al sistema target esso stabilisce definitivamente la connessione rimuovendo dalla lista la richiesta pendente di connessione. La sequenza delle operazioni è illustrata nella figura A.

Nel caso, invece, di un attacco di tipo Syn flood, il programma di attacco residente sul sistema source (*Hacker system* in figura B) ignora deliberatamente il pacchetto di conferma SYN ACK proveniente dal sistema target e invia in brevissimo tempo una ulteriore richiesta di connessione tramite il pacchetto di SYN. Il sistema target riceverà così in brevissimo tempo molte richieste di connessione saturando in breve la lista delle richieste pendenti. A questo punto il sistema non sarà più in grado di ricevere alcuna ulteriore legittima richiesta di connessione e, pertanto, risulterà di fatto scollegato dalla rete. Ovviamente, se durante l'attacco di tipo Syn flood il sistema source non maschera il proprio indirizzo nel pacchetto TCP, risulta relativamente semplice rilevare l'attacco, attraverso l'analisi degli "indirizzi mittente" dei pacchetti giunti al sistema target, e bloccarlo. Se, invece, il codice di attacco presente sul hacker system modifica l'indirizzo mittente, mediante la citata tecnica di spoofing, introducendo nel pacchetto al posto del reale indirizzo del sistema source indirizzi inesistenti o fasulli, l'identificazione risulta assai ardua e l'attacco difficile da rigettare.



mente, che permette di “entrare” in un ambiente o programma superando le normali barriere poste per accedervi. Tali percorsi possono essere stati progettati volutamente per garantire un accesso diretto durante le fasi di sviluppo e/o manutenzione del codice, oppure possono derivare da errori di progettazione o di codifica del codice. L'importanza delle backdoor deriva dal fatto che gli *hacker* per iniziare un attacco devono penetrare un sistema sul quale installare il codice di attacco. E ciò di norma è realizzato attraverso lo sfruttamento di backdoor. Lo stesso vale per la realizzazione di meccanismi di propagazione per virus e worm. Per esempio, il recente *worm Sapphire* o *sq hell* che ha generato notevoli danni all'inizio di questo anno sfruttava una tecnica di backdoor per acquisire privilegi di sistema.

Sniffing, spoofing, DOS, Trojan e backdoor costituiscono le tecniche di base per realizzare attacchi in rete molto articolati e complessi. Mediante queste tecniche si realizzano le intrusioni informatiche per realizzare furti di informazioni o danneggiamenti, o si creano virus e worm oppure si attaccano apparati o server di rete.

Per esempio, per compromettere il funzionamento e le prestazioni della rete Internet, o di una sua porzione oppure di una rete aziendale basata su tecnologia Intranet, possono essere attaccati router e DNS (*Data Source Name*) server. Si consideri, a titolo esplicativo, quest'ultimo caso.

Si ricorda che la funzione fondamentale di un server DNS è quella di tradurre gli indirizzi logici della rete (per esempio, www.polito.it) nei corrispondenti indirizzi binari o indirizzi IP (per esempio, 130.192.23.13). Il protocollo DNS, permette a ogni nodo della rete di richiedere a un server DNS questa traduzione: viene inviato l'indirizzo logico e si ottiene in risposta quello IP. Gli attacchi ai servizi erogati dai DNS server possono riguardare l'integrità dei dati contenuti nel server o la disponibilità dei servizi. Un server DNS può essere compromesso mediante un attacco DOS, nel qual caso risulta non più accessibile dai nodi di rete. Un risultato analogo può essere ottenuto intercettando le richieste dei vari nodi (*sniffing*) e inviando indietro falsi pacchetti di risposta (*spoofing*) o re-indirizzando i pacchetti di ri-

chiesta a server senza funzioni DNS. Si otterrà in tutti i casi che i nodi mittenti non otterranno risposta. Un server DNS può essere, inoltre, compromesso attraverso tecniche di backdoor che implicano l'acquisizione del controllo del sistema, potendo in tal caso svolgere funzioni mirate a corrompere il data base di corrispondenza tra indirizzi logici e binari. Queste tabelle di corrispondenza possono essere, infine, corrotte attraverso l'invio di dati di aggiornamento falsi, sfruttando in modo anomalo certe funzioni del protocollo DNS. Per esempio, a un dato indirizzo logico può essere associato l'indirizzo IP non del vero sito web ma di un sito clonato o diverso (*shadow web server*), con evidenti criticità sul piano dell'immagine e del business. Si noti che le funzioni DNS sono tra quelle fondamentali nel funzionamento di Internet: la loro compromissione determina, pertanto, gravi e significativi problemi al funzionamento della rete, tanto è che lo IETF ha introdotto una versione sicura del protocollo DNS, denominata DNSSEC.

Nel concludere questa breve rassegna sulle tecniche di attacco e sulle vulnerabilità presenti nei sistemi di rete odierni, non possono non essere citati i worm. Questi, come noto, sono programmi dotati della caratteristica di auto replicarsi, come i tradizionali virus, e di auto propagarsi in rete. È quest'ultima caratteristica che, almeno sul piano formale, li distingue dai virus, anche se oggi le differenze diventano sempre più labili. Oggi i worm sfruttano tecniche di diffusione assai sofisticate e molto veloci, tali da rendere le contromisure inefficaci se non nel medio termine. Si consideri che il worm *Sapphire*, attivatosi il 25 gennaio scorso generando notevoli danni nel nostro Paese, ha realizzato una velocità di diffusione, dovuta a tecniche sofisticate di scansione del codice virale, che portava al raddoppio dei calcolatori infettati ogni 8,5 s, contro i 37 min del già citato worm *Red Code*, considerato a suo tempo il più veloce worm della storia. *Sapphire* ha infettato più del 90% degli host vulnerabili in circa 15 min, con un numero di host compromessi complessivamente superiore a 100.000. Il maggior danno di questi worm, al di là dei potenziali effetti distruttivi di file eventualmente contenuti, a scadenza, nel codice virale, deriva dalla saturazione della rete che si realizza durante la propagazione

0

0

1

0

1

0

1

0

42

produciendo un effetto di DOS su server e apparati di rete, ivi comprese le reti locali soggette alla diffusione del codice virale.

3. COME DIFENDERSI

La necessità di realizzare reti sicure è, come detto, un'esigenza imprescindibile per le applicazioni business. Essa, pur in presenza delle citate vulnerabilità, può essere ottenuta attraverso una idonea politica di sicurezza che si poggia su corrette scelte tecnologiche e su adeguate strategie organizzative. Soffermandosi, per ragioni di brevità, unicamente sulle prime senza per altro trascurare l'importanza fondamentale delle seconde, si può affermare che il raggiungimento di accettabili livelli di sicurezza si ottiene impiegando tecnologie mirate a realizzare le funzioni di segretezza, di autenticazione, di autorizzazione e di *auditing*. Tali funzioni si basano, essenzialmente, sull'impiego di tecniche crittografiche descritte brevemente nel seguito. La realizzazione delle sopra citate funzioni di sicurezza può essere realizzata con modalità tecnologiche diverse in funzione dei contesti architeturali e dei servizi di cui si vuole disporre. A un primo livello di approssimazione, è possibile suddividere le tecniche per rendere sicuro un sistema in rete in due grandi categorie: le tecniche che operano sui protocolli di rete, modificando quelli tradizionali al fine di introdurre prestazioni di sicurezza (sottoparagrafo 3.4), e quelle di tipo architeturale che mirano a rendere sicuro un sistema introducendo appositi apparati, per esempio *firewall*, e/o modificando la struttura stessa della rete riducendo le vulnerabilità esistenti (sottoparagrafo 3.5).

Prima di poter esaminare, in dettaglio, alcune delle possibili soluzioni atte a rendere sicura una rete aziendale e i suoi servizi, sembra utile riassumere i fondamentali concetti di crittografia, che come noto è la base concettuale per realizzare le fondamentali proprietà della sicurezza: segretezza, autenticazione, non ripudio.

3.1. Cenni di crittografia

Affinché due nodi possano comunicare tra loro in modo sicuro è necessario che il canale che li collega goda delle proprietà di segretezza

e autenticazione. Queste vengono realizzate mediante tecniche e algoritmi crittografici. In generale, nella fase più propriamente detta di cifratura, un testo in chiaro (*plaintext*) viene trasformato nel corrispondente testo cifrato (*ciphertext*) mediante l'uso di una chiave predefinita. Un procedimento analogo si realizza nella fase di decifratura che garantisce il passaggio dal testo cifrato a quello originale. La chiave e gli algoritmi utilizzati nella cifratura non necessariamente coincidono con quelli impiegati durante la decifratura.

Esistono due principali categorie di algoritmi utilizzati per la cifratura delle informazioni: quelli che fanno uso di chiavi simmetriche (dove la stessa chiave serve sia per la cifratura dei dati sia per la loro decodifica) e quelli a chiavi asimmetriche, dove le due chiavi sono diverse e intercambiabili: ciascuna di esse può essere utilizzata per cifrare le informazioni, ma solo l'altra può essere usata per decifrarle. In generale, della coppia di chiavi una, detta privata, viene tenuta segreta, l'altra detta pubblica viene, invece, resa disponibile a tutti. In pratica a ciascun soggetto è associata una coppia di chiavi (chiave pubblica e chiave privata). L'associazione tra la chiave pubblica e il soggetto a cui essa è associata, è realizzata mediante un certificato a chiave pubblica, cioè una tabella informatica che contiene gli estremi del soggetto e la chiave pubblica associata. Tale certificato è di norma rilasciato da un apposito ente indicato come autorità di certificazione o CA (*Certification Authority*).

Gli algoritmi basati su chiave simmetrica sono più semplici e, quindi, meno pesanti dal punto di vista computazionale rispetto agli algoritmi a chiave asimmetrica. Esempi di algoritmi simmetrici sono: DES, triplo DES, AES, RC4. Il problema intrinseco degli algoritmi simmetrici risiede nella distribuzione della chiave in modo affidabile e segreto. Se questa non è distribuita in modo sicuro, e qualcuno ne viene a conoscenza, tutto il sistema risulta compromesso. Da qui, l'uso di definire gli algoritmi simmetrici anche come algoritmi a chiave segreta. La distribuzione della chiave segreta ai soli soggetti suoi depositari può essere realizzato in vari modi, tra cui quello di impiegare la crittografia asimmetrica.

Mentre gli algoritmi simmetrici sono impiegati principalmente per realizzare la funzione

di segretezza, quelli a chiave asimmetrica permettono di realizzare sia la *segretezza* sia l'*autenticazione*.

La funzionalità di *segretezza* si ottiene utilizzando la chiave pubblica per cifrare le informazioni da inviare al soggetto cui la chiave stessa è associata. Solo l'interessato possiede la chiave privata, e pertanto è in grado di decodificare le informazioni.

La funzionalità di *autenticazione del mittente* (ovvero, la certificazione dell'identità del mittente) è ottenuta facendo sì che l'originatore cifri i dati con la propria chiave privata prima di inviarli. Chiunque sia in possesso della chiave pubblica può utilizzarla per decodificare le informazioni ricevute e avere, quindi, la certezza che esse siano state cifrate con la chiave privata del soggetto in questione.

Gli algoritmi a chiave asimmetrica ricoprono anche un ruolo fondamentale nel garantire la corretta distribuzione di chiavi simmetriche. Esempi di algoritmi asimmetrici sono RSA, DSA e *Diffie-Hellman*, per la distribuzione di chiavi segrete.

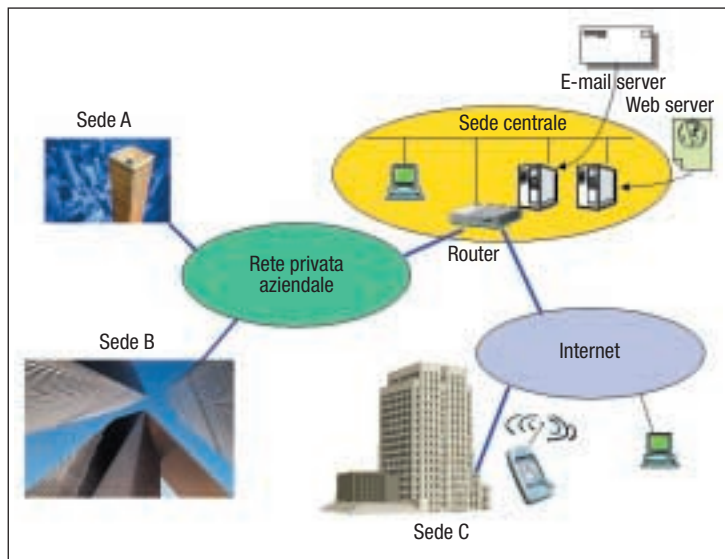
3.2. Reti aziendali e sicurezza

Nel caso più generale, una rete aziendale è costituita da un insieme di reti locali, ciascuna corrispondente a una specifica sede dell'azienda, connesse fra loro da collegamenti che possono essere realizzati con un'infrastruttura privata oppure utilizzando una rete pubblica (ad esempio, Internet) come illustrato in figura 4.

In relazione agli aspetti di sicurezza risulta opportuno definire i seguenti tre sottosistemi:

La rete locale (una per ogni sede). Renderla sicura significa introdurre meccanismi di riservatezza delle informazioni trasmesse, oltre a sistemi che "osservano" il traffico al fine di identificare comportamenti o eventi anomali. La rete locale può prevedere zone che richiedono livelli di protezione diversi, come sarà illustrato nel seguito trattando le soluzioni di tipo firewall.

La zona di frontiera (una per ogni sede). È il punto di contatto tra la rete locale e la rete "pubblica" utilizzata per le comunicazioni con il resto del mondo (tipicamente la rete Internet). In tale area è generalmente presente un router che collega a un fornitore di servizi di connettività (per esempio, un *Internet Service Provider*, ISP). Rendere sicura questa zo-



na implica attivare, per esempio, sul router di frontiera meccanismi di ispezione dei pacchetti in transito al fine di verificare traffico anomalo in ingresso verso la rete locale o in uscita da essa.

La rete esterna utilizzata per realizzare le connessioni tra le varie sedi aziendali. Trattandosi nel caso più comune di una rete pubblica (Internet), questa zona dovrà essere sempre considerata insicura, e nel caso si vogliono proteggere le comunicazioni che su essa hanno luogo occorrerà introdurre meccanismi che rendano indecifrabile il traffico tra le diverse sedi dell'azienda.

3.3. Le politiche aziendali per la sicurezza

La messa in atto di meccanismi che rendano sicura una rete aziendale possono essere definiti con precisione solo a seguito di una pianificazione delle politiche di sicurezza dell'azienda, in generale contenute nel documento fondamentale della sicurezza aziendale, il "piano di sicurezza". In esso, tra l'altro, si descrivono le funzionalità di rete che si vogliono concedere e le relative modalità, così come le funzionalità che si decide di proibire.

Esempi di aree interessate dalla definizione delle politiche di sicurezza aziendale sono:

La possibilità di concedere comunicazione diretta tra i nodi della rete (PC degli utenti) e la rete Internet per scopi di navigazione. Qualora si stabilisca di non voler concedere tale diritto, occorrerà, per esempio, prevedere un nodo *proxy web* (o *web cache*) attraverso il quale gli

FIGURA 4
Rete aziendale

utenti che vogliono consultare il mondo web siano costretti a passare (quindi, parallelamente bloccando il passaggio diretto dei pacchetti tra i PC degli utenti e il mondo esterno).

■ La presenza di un sistema centralizzato di antivirus in grado di “intercettare” ed esaminare il grado di sicurezza dei messaggi di posta elettronica, delle pagine web e delle eventuali porzioni di codice (per esempio, *Java applet*) in esse presenti.

■ La presenza di un sistema che analizza periodicamente il traffico presente sulla rete locale, configurato per riconoscere sequenze di attacco e identificare, quindi, tentativi di forzatura originati all’interno della LAN aziendale.

■ La presenza di un sistema analogo al precedente, ma installato in posizione tale da permettergli di analizzare il traffico da e verso il mondo esterno (al fine di identificare attacchi provenienti dall’esterno e diretti alla LAN aziendale o viceversa).

■ La presenza di un sistema in grado di eseguire autenticazione di utenti aziendali che si trovano all’esterno dell’azienda e che, in caso di riconoscimento di personale autorizzato, conceda l’accesso sicuro alle risorse aziendali con le stesse modalità disponibili per gli utenti interni.

3.4. Sicurezza nelle applicazioni e nei protocolli di rete

La necessità di introdurre sicurezza nel software di comunicazione mediante impiego di applicazioni o protocolli di rete resi sicuri nasce dalla assunzione fondamentale di non avere garanzie di sicurezza offerte dalla rete. Partendo cioè dal presupposto di avere

una rete non sicura (alla quale, pertanto, si assume siano connessi soggetti intenzionati a osservare il traffico al fine di carpire informazioni e successivamente perpetrare attacchi), due elaboratori che intendono scambiarsi informazioni devono utilizzare accorgimenti che impediscono l’intercettazione e la manipolazione delle informazioni stesse, nonché la certezza dell’autenticità del mittente e/o destinatario delle informazioni.

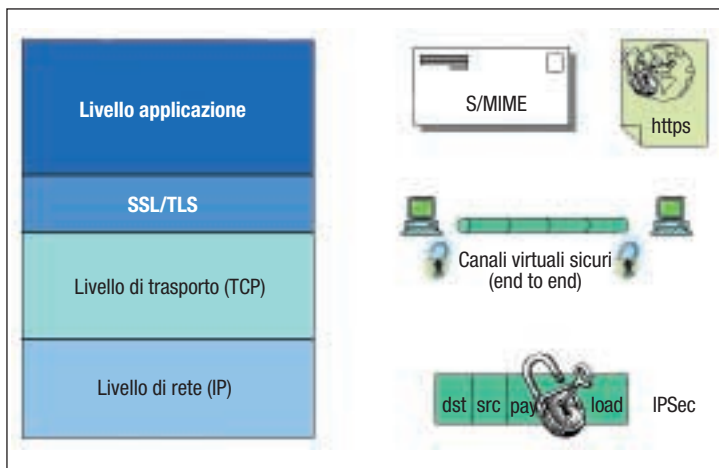
Come specificato nel riquadro sui protocolli Internet, il software di comunicazione di rete viene convenzionalmente organizzato e sviluppato in modo stratificato, identificando diversi “livelli” per ciascuno dei quali sono definite funzionalità e modalità di comunicazione verso i livelli superiore e inferiore (interfacce). L’indipendenza (tipica di questa architettura e suo principio fondamentale) di ciascuno dei livelli rispetto agli altri offre la possibilità di modificare il software che costituisce un livello senza dover intervenire su quelli superiori o inferiori.

Le funzionalità di comunicazione sicura possono, quindi, essere introdotte in diversi punti della “pila”, ottenendo soluzioni di sicurezza con caratteristiche diverse. Si considerano ora le diverse soluzioni adottabili ai diversi livelli di protocollo, rappresentate in modo sintetico in figura 5.

3.4.1. SICUREZZA A LIVELLO DI APPLICAZIONE

Introdurre funzionalità di sicurezza a livello applicativo significa modificare l’applicazione che si vuole rendere sicura aggiungendo, ad esempio, la crittografia dei dati: le informazioni vengono rese indecifrabili a bordo dell’elaboratore che le genera, e nessuna altra applicazione risente dell’effetto di questa operazione. I dati generati dall’applicazione sicura vengono inviati utilizzando normali pacchetti di rete, ai quali non è applicata alcuna operazione di cifratura (per la rete tali dati sono “in chiaro”, ma sono di fatto indecifrabili in quanto sono stati cifrati alla fonte). Molto comune è, per esempio, l’impiego di posta elettronica cifrata (per esempio, in conformità con le specifiche S/MIME), che prevede che solo l’applicazione che compone il messaggio e quella che lo riceve rilevino l’uso di crittografia. Ne deriva che lo scambio di chiavi crittografiche riguarda ciascuna applicazione e la sicurezza

FIGURA 5
Sicurezza a diversi livelli





si limita alla singola applicazione, per esempio la posta elettronica ma non il web.

3.4.2. SICUREZZA A LIVELLO DI SESSIONE

Introdurre sicurezza a livello di sessione significa creare un canale virtuale sicuro sul quale far transitare una specifica transazione o sessione di comunicazione. Le applicazioni coinvolte, in questo caso, generano e ricevono informazioni senza cifrarle (e, quindi, potrebbero anche ignorare l'esistenza della sicurezza e della crittografia). Ne deriva che più applicazioni possono avvalersi del canale sicuro. Le informazioni vengono "intercettate" prima di lasciare l'elaboratore che le ha generate per essere cifrate e inviate al nodo destinatario. Presso il nodo destinatario è attivo un procedimento speculare che prevede la ricezione delle informazioni stesse, la loro decodifica e il passaggio (in chiaro) alla applicazione che le deve ricevere. Le applicazioni coinvolte non sono al corrente delle operazioni di crittografia. Un caso molto diffuso di questo tipo di soluzione è rappresentato dal protocollo SSL (*Secure Socket Layer*), alla base delle comunicazioni web sicure. Nel caso del trasferimento di pagine web mediante SSL, le pagine stesse non sono crittografate, e possono essere consultate in modo sicuro utilizzando il protocollo HTTP inviato su un canale con protocollo SSL (a sua volta costruito sul TCP) che garantisce l'autenticazione del server e del client e la cifratura di tutti i dati che transitano sul canale.

È importante osservare come la possibilità di stabilire un canale di comunicazione sicuro permetta l'utilizzo di questa soluzione a un numero arbitrario di applicazioni, senza modificare il codice relativo alla applicazione stessa. Nel caso precedente (sicurezza a livello applicativo) viene, invece, risolto il problema della sicurezza solo per l'applicazione che viene modificata per renderla sicura. Il protocollo SSL, introdotto da Netscape, è stato standardizzato con lievi modifiche da IETF ed è denominato TLS (*Transport Layer Security*).

3.4.3. SICUREZZA A LIVELLO NETWORK: IPSEC

La costruzione di un canale di comunicazione sicuro mediante SSL implica la realizzazione di un canale virtuale *end-to-end*, cioè tra mittente e destinatario, che rende sicuro tutto il

traffico esistente tra i due nodi mittente e destinatario e che utilizza come protocollo il TCP. Di fatto, SSL può essere visto come uno strato aggiuntivo collocato nella architettura TCP/IP al di sopra del livello TCP. Di conseguenza, non tutto il traffico è associato a canali virtuali realizzati mediante TCP (per esempio, il traffico che impiega il protocollo UDP (*User Datagram Protocol*)).

È possibile, tuttavia, introdurre sicurezza anche a livello più basso del trasporto, agendo, ad esempio, direttamente sui singoli pacchetti IP. Una soluzione molto diffusa che fa uso di questa strategia è l'architettura IPsec (*Secure Internet Protocol*), che prevede di eseguire cifratura e autenticazione a livello dei singoli pacchetti IP.

Questa caratteristica svincola questa soluzione dal dover essere messa in atto sul nodo origine del traffico (come, invece, avviene nei due casi precedenti). La cifratura del traffico IP può, infatti, essere effettuata tra due nodi qualsiasi esistenti tra il nodo sorgente e quello destinatario e riguarda tutti i pacchetti IP in transito indipendentemente dai protocolli superiori impiegati, TCP o UDP. Il protocollo IPsec agisce in sostanza tra due nodi qualunque della rete, in genere costituiti da router. È evidente che non è richiesto che il nodo mittente o quello destinatario siano informati dell'esistenza di un canale IPsec lungo il percorso che li unisce. Il nodo mittente immette traffico "in chiaro" sulla rete, quello destinatario riceve traffico "in chiaro". Tecniche quali IPsec trovano frequente impiego nella realizzazione di reti private virtuali o VPN, grazie alle quali diverse sedi possono essere messe tra loro in comunicazione senza utilizzare un'infrastruttura dedicata, ma costruendo canali sicuri su una struttura intrinsecamente insicura. Nella figura 6 è riportata la stessa struttura logica precedentemente illustrata (Figura 4), ma nella quale la rete privata di connessione tra le sedi è stata sostituita da canali virtuali costruiti su Internet. Non tutte le sedi aziendali sono obbligate a essere connesse utilizzando canali virtuali sicuri: nella figura, la sede C, che precedentemente era connessa alla sede centrale utilizzando la rete Internet, continua a essere partecipe della rete aziendale nella stessa modalità.

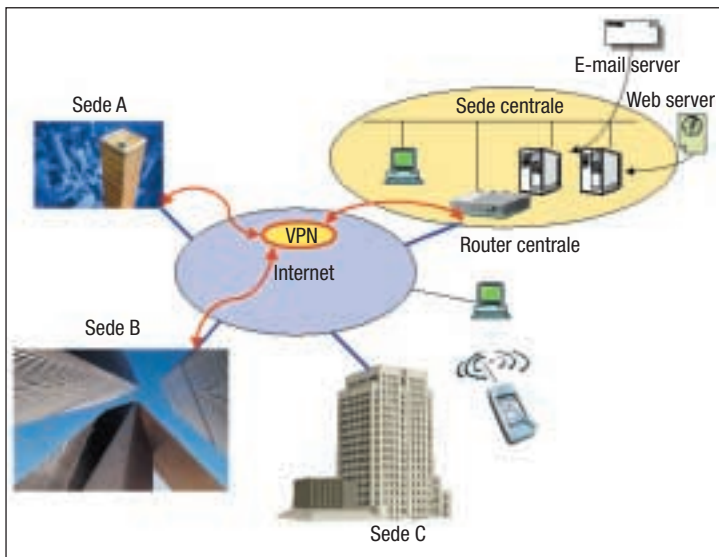


FIGURA 6

Rete aziendale con VPN (Virtual Private Network)

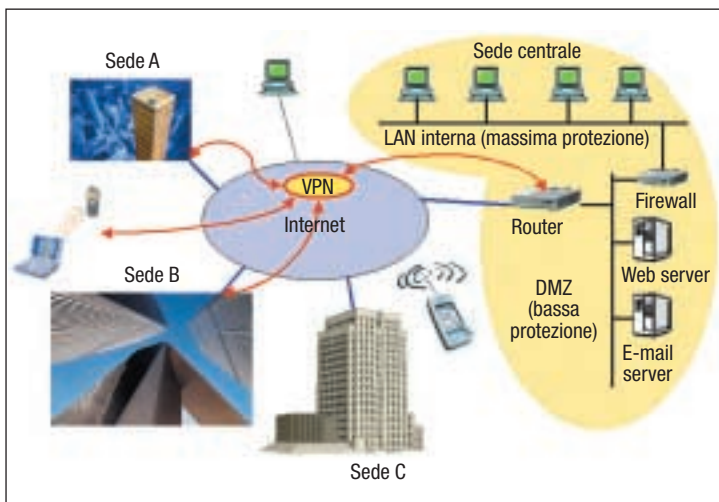


FIGURA 7 3.5. Introdurre sicurezza nell'architettura di rete

Rete aziendale protetta mediante firewall

Le soluzioni sopra citate permettono di ottenere comunicazioni sicure su un'infrastruttura non sicura. Esse, tuttavia, non tutelano nei confronti di attacchi che non hanno come oggetto l'informazione in transito ma le funzionalità della stessa rete, quali ad esempio gli attacchi di tipo DOS (già descritti in precedenza), o la forzatura (*hacking*) di sistemi per ottenerne il controllo.

Molte di queste minacce possono essere vanificate mediante l'introduzione, nell'architettura della rete, di componenti che hanno il compito di "osservare" tutto il traffico e riconoscere situazioni anomale, a seguito delle

quali prendere provvedimenti atti a bloccare l'attacco in corso.

Tra i componenti più frequentemente introdotti a tale scopo all'interno delle reti aziendali figurano i firewall, le reti private virtuali o VPN, i sistemi di rilevamento di intrusioni o IDS (*Intrusion Detection Systems*) e i sistemi antivirus.

Nella figura 7, è rappresentata l'architettura di rete aziendale già descritta in precedenza, ulteriormente ampliata introducendo alcune soluzioni mirate alla messa in sicurezza. Per brevità sono state raffigurate solo le soluzioni VPN e firewall. Si osservi come, in questo caso, partecipa alla VPN anche un utente mobile (PC portatile connesso a un telefono cellulare).

3.5.1. VPN

Le reti private virtuali o VPN (*Virtual Private Network*) costituiscono un'applicazione che integra l'uso di protocolli di rete sicuri e tecniche di autenticazione dell'utente. Il servizio di VPN è un meccanismo che permette di stabilire, tra due sedi, comunicazioni sicure e autenticate, permettendo (attraverso una rete pubblica non sicura) lo scambio di informazioni e l'accesso alle risorse aziendali con le stesse caratteristiche di riservatezza e le stesse autorizzazioni garantite agli utenti fisicamente connessi alla rete aziendale.

Due sono i principali ambiti di impiego delle VPN:

- VPN "permanenti" per connessione reciproca di sedi aziendali;
- VPN temporanee per la connessione da remoto di utenti con caratteristiche di nomadicità.

Le VPN permanenti si costruiscono identificando coppie di sedi che devono essere tra loro connesse, e installando in ciascuna di esse un apparato (o un elaboratore che svolge le stesse funzioni) detto terminatore di VPN. Ciascuno dei due terminatori di un circuito virtuale si preoccupa di cifrare il traffico ricevuto dalla propria LAN e di inviarlo al terminatore di VPN presente nell'altra sede. Il traffico, cifrato, può tranquillamente essere trasportato a questo fine su una rete insicura quale la rete Internet senza che questo rappresenti una minaccia per la sicurezza. Solo i due apparati terminatori del canale VPN conoscono le chiavi per eseguire codifica e decodifica dei pac-

chetti. Di fatto, i pacchetti originali sono prima cifrati e poi imbustati in nuovi pacchetti che viaggiano tra i due soli terminatori della VPN. Come è semplice intuire, questa soluzione può essere applicata facilmente anche al caso in cui uno dei due terminatori di canale VPN sia su un elaboratore di un utente (per esempio, un PC portatile). Risulta, pertanto, possibile, mediante installazione di opportuno software sull'elaboratore dell'utente, concedere accesso sicuro alle risorse aziendali anche a personale autorizzato che si trovi fuori sede e sia connesso a un comune Internet Service Provider. In quest'ultimo caso è anche evidente la temporaneità del canale virtuale, che viene creato quando l'utente desidera connettersi e cancellato al termine della sessione di lavoro.

3.5.2. FIREWALL

La posizione di frontiera tra la rete aziendale (che si vuole mantenere sicura) e quella pubblica, è la sede ideale nella quale installare apparati (spesso denominati *firewall*) dedicati a svolgere funzioni di "filtro" del traffico di rete, al fine di impedire il transito di tutto il traffico che non rientra nelle politiche aziendali.

Le funzioni di firewall possono essere anche integrate (nei casi più semplici) all'interno di router esistenti (in particolare, il router principale di connessione verso l'esterno). Anche i router, infatti, sono in grado di eseguire un'analisi (sebbene solo macroscopica) del traffico, e di prendere i primi provvedimenti ove necessario.

Per esempio un router è facilmente in grado di identificare (e bloccare se questo è previsto) traffico di posta elettronica entrante in azienda ma non diretto al server mail aziendale, oppure traffico di navigazione uscente verso il mondo Internet, o altre richieste di connessione provenienti dall'esterno alle quali si sceglie di non voler concedere autorizzazione.

Un router non è, invece, generalmente in grado di identificare pattern di traffico sofisticati quali *port scanning* o TCP SYN attack, così come non è in grado di eseguire sul traffico analisi sofisticate che richiedono la ricostruzione di file di grandi dimensioni quali messaggi di posta elettronica o di intere pagine Web (per esempio per effettuare scansione antivirus). Vista la sua posizione centrale nell'architettura di rete locale dell'azienda, il firewall vie-

ne anche utilizzato per suddividere la LAN in aree a diverso livello di sicurezza, come accennato in precedenza (sottoparagrafo 3.2). Viene a tal fine spesso identificata una zona detta "demilitarizzata" (DMZ) sulla quale vengono rilasciati alcuni dei vincoli che proteggono la rete interna dell'azienda. Sulla DMZ, accessibile più facilmente dal mondo esterno, si trovano elaboratori quali il mail server e il web server aziendali.

4. UN ESEMPIO APPLICATIVO: HOME BANKING

Nei paragrafi precedenti sono state descritte, in modo conciso, le tecnologie disponibili per rendere sicure reti e comunicazioni. Al fine di dare concretezza a tali concetti si ritiene utile descrivere applicazioni di business che si avvalgono di queste tecnologie per realizzare servizi applicativi sicuri.

Tra le varie applicazioni si descrive quella più nota e diffusa: *home* o *Internet banking*. Questa risulta particolarmente interessante in quanto è percepita come estremamente critica dal punto di vista della protezione e riservatezza delle informazioni. Essendo essa basata su una tecnologia ampiamente utilizzata nel mondo Internet (la tecnologia web), permette di evidenziare come, anche in una situazione in cui la sicurezza della rete di comunicazione non è sicura, sia possibile creare una infrastruttura virtuale estremamente affidabile.

In estrema sintesi, il problema dell'Internet banking si riconduce a quello di proteggere la comunicazione tra due nodi connessi alla rete Internet: il *client* utilizzato dall'utente (*browser web*) e il server messo a disposizione dalla banca (web server che svolge funzioni di *front end* verso il sistema informativo bancario).

Condizione essenziale per garantire la sicurezza in questo caso è provvedere alla indecifrabilità delle informazioni trasmesse tra i due elaboratori interessati, mediante tecniche crittografiche (per una descrizione delle quali si rimanda al sottoparagrafo 3.1).

Come precedentemente citato, la creazione di un canale sicuro di comunicazione richiede la condivisione di informazioni segrete (chiavi) tra i due nodi interessati a rendere indecifrabile una specifica sessione di scambio di dati.

Nel caso dello home banking si rende necessaria la generazione di chiavi temporanee che abbiano validità limitata alla sessione di comunicazione di interesse (chiavi di sessione). Parallelamente, occorre un meccanismo grazie al quale due elaboratori che si apprestano a iniziare una comunicazione sicura riescano come azione preliminare a scambiarsi in modo sicuro le chiavi di sessione.

A causa della minore complessità computazionale associata agli algoritmi a chiave simmetrica, questi rappresentano la soluzione preferita per cifrare le informazioni scambiate tra due nodi, i quali devono, quindi, preventivamente condividere un solo segreto (la chiave di sessione, che in questo caso è unica).

La costituzione di un canale sicuro di comunicazione tramite SSL richiede, quindi, due azioni preliminari:

- la generazione della chiave di sessione da parte di uno degli interlocutori;

- la trasmissione della chiave di sessione all'altro interlocutore, *in modo sicuro*.

La *generazione* di chiavi crittografiche, siano esse simmetriche o asimmetriche, è un problema oggi ampiamente risolto mediante opportuni algoritmi, basati su generatori di numeri pseudo casuali, in grado di generare idonee sequenze di *bit* cui le chiavi vengono fatte corrispondere.

Il problema maggiore consiste, invece, nella *trasmissione sicura* di questa chiave dal nodo che la ha generata al suo interlocutore. Ovviamente, tale chiave non può essere trasmessa "in chiaro" prima di iniziare la sessione sicura, perché la sua intercettazione permetterebbe di decifrare tutto il traffico della sessione stessa. Ci si trova, quindi, in presenza di un apparente paradosso: occorre un canale sicuro per trasmettere l'informazione necessaria a creare un canale sicuro di comunicazione.

Il problema della trasmissione della chiave di sessione da un nodo all'altro trova una facile soluzione nell'impiego di una coppia di chiavi asimmetriche. In particolare, le operazioni svolte per trasmettere in modo sicuro la chiave di sessione vengono chiarite nel seguito.

Nel caso dell'applicazione in esame (home banking) il nodo client (utente del servizio) e il nodo server mettono in atto una sessione di comunicazione sicura tra loro mediante la seguente sequenza di operazioni:

1. Il client invia al server una richiesta di creazione di un canale di comunicazione sicuro temporaneo;

2. Il server della banca, che possiede una coppia di chiavi asimmetriche (AK₁, AK₂, con AK₁ chiave pubblica e AK₂ privata) invia la chiave pubblica AK₁ al nodo client (browser dell'utente);

3. Il nodo client genera la chiave di sessione SK (chiave simmetrica), la crittografa utilizzando la chiave pubblica AK₁, e invia il risultato di tale operazione al server bancario. Siccome per decifrare le informazioni è necessaria la chiave privata AK₂, solo il server stesso è in grado di decodificare la chiave di sessione (si noti, infatti, che la chiave AK₂ non ha mai lasciato l'elaboratore server). La eventuale intercettazione della chiave AK₁ non è di nessuna utilità per un eventuale malintenzionato che fosse in ascolto sulla rete.

A questo punto, i due elaboratori condividono il segreto (la chiave di sessione simmetrica SK), e possono iniziare a comunicare in modo sicuro mediante algoritmi simmetrici veloci, trasmettendo le varie informazioni: password, dati finanziari ecc..

Questa sequenza di operazioni è alla base della tecnologia detta SSL (*Secure Socket Layer*) utilizzata per stabilire comunicazioni sicure tra browser e web server. Sul canale SSL (che a questo punto è cifrato e, quindi, sicuro) vengono successivamente inviate le informazioni di autenticazione (username e password nel più comune dei casi). Se la fase di autenticazione viene superata con successo, la banca acquisisce fiducia circa l'identità del cliente e gli rende disponibili i servizi e le informazioni alle quali ha diritto di accedere. Vista la criticità di questa categoria di applicazioni, misure aggiuntive di sicurezza vengono, generalmente, messe in atto oltre alla creazione di un canale di comunicazione cifrato. Tra queste è possibile citare:

- Scadenza della sessione sicura: qualora l'utente, una volta autenticato, non esegua operazioni di navigazione sul sito per un certo tempo, la sessione "scade" e per continuare le operazioni sarà necessaria una ripetizione delle operazioni di autenticazione.

- Alcune operazioni particolarmente critiche (trasferimento di somme di denaro consistenti) richiedono una ulteriore autenticazio-

ne, spesso basata su tecniche quali *one time password* o similari: per poter portare a termine tali operazioni viene cioè richiesta una informazione aggiuntiva a ulteriore garanzia della identità del cliente.

5. SICUREZZA E TECNOLOGIE WIRELESS

Per completare la rapida panoramica delle architetture di rete aziendale e delle relative tecniche di messa in sicurezza occorre citare la categoria delle soluzioni basate su tecnologie wireless, introdotte diversi anni fa ma per le quali solo in questi anni si sta assistendo a una diffusione consistente sul mercato. Il principio di base della connettività IP fruibile anche da dispositivi non connessi fisicamente a una rete rende possibile un'ampia gamma di applicazioni. Queste sono in parte semplici estensioni di quelle tradizionalmente fruibili tramite connettività fissa (navigazione su Internet, posta elettronica ecc.), e in parte specifiche del contesto mobile in quanto si basano per esempio su informazioni come la localizzazione fisica dell'utente (telematica per il veicolo, informazioni turistiche ecc.).

La fruibilità delle applicazioni basate su IP da terminali mobili ha visto evolversi parallelamente due settori tecnologici: quello della connettività IP per terminali di tipo telefonico cellulare (quindi connessi alla rete tramite tecnologie quali GSM o GPRS, e WAP per la navigazione Internet), e quello della connettività IP vista come estensione delle reti locali fisse (per terminali connessi alla rete mediante tecnologia Wireless LAN (WLAN), che utilizzano le stesse tecnologie e protocolli tipici delle reti fisse a partire dal livello *network*).

La connettività IP in condizioni di mobilità, e la conseguente trasmissione in aria libera dei dati scambiati tra coppie di elaboratori costituiscono uno scenario nel quale sono ancora più evidenti le problematiche di sicurezza. L'ascolto delle comunicazioni risulta tecnicamente più semplice in ambienti dove queste avvengono via radio rispetto a quanto avviene su rete fissa, dove l'interessato deve almeno trovare un punto di connessione fisica alla rete stessa per avere accesso al flusso di dati. L'uso di tecnologie crittografiche sul canale radio è, quindi, praticamente obbligatorio,

sebbene spesso questo aspetto sia effettivamente trascurato. La tecnologia in questo settore è tuttavia già disponibile. Lo scarso successo riscontrato dal protocollo WEP (*Wireless Encryption Protocol*) a seguito della provata possibilità di risalire senza eccessiva difficoltà alla chiave utilizzata per cifrare le informazioni ha incentivato la ricerca di soluzioni alternative quali WPA (*Wi-Fi Protected Access*) o il più generale EAP-TLS (*Extensible Authentication Protocol – Transport Layer Security*), che sono in grado di garantire all'utente la necessaria riservatezza nel dialogo in rete. Per le tecnologie WLAN basate sui protocolli della classe 802.11 sono stati introdotti criteri di elevata sicurezza utilizzando il *framework* di autenticazione fornito dallo standard 802.1x.

Bibliografia

- [1] CERT: www.cert.org
- [2] CSI/FBI annual report 2002: *Computer security issues & trends*. www.gocsi.com
- [3] Mezzalama M, Lioy A: La sicurezza dei sistemi informativi. In *Sistemi Informativi*, Vol. V, Franco Angeli, 2001.
- [4] Stallings W: *Cryptography and network security*. 2nd Ed., Prentice Hall, 1999.
- [5] SSL specification: www.netscape.com/eng/ssl3

MARCO MEZZALAMA è Professore ordinario di Sistemi di Elaborazione presso la Facoltà di Ingegneria dell'Informazione del Politecnico di Torino, dove attualmente ricopre la carica di Pro Rettore. Autore di numerose pubblicazioni scientifiche, ha collaborato e coordinato parecchi progetti di ricerca in ambito nazionale ed europeo. La sua attività scientifica si è svolta principalmente nei settori dell'architettura dei sistemi di elaborazione, delle reti di calcolatori e dei sistemi informativi aziendali. Ha fondato il Laboratorio di Sicurezza Informatica del Politecnico di Torino e recentemente l'associazione *Assosecurity*. marco.mezzalama@polito.it

EDOARDO CALIA è direttore dei laboratori di ricerca presso l'Istituto Superiore "Mario Boella" di Torino. Presso il Politecnico di Torino è stato responsabile dei Sistemi Informativi e di Telecomunicazioni tra il 1994 e il 2001, ed è attualmente professore a contratto per la docenza del corso di Reti di Calcolatori. Nel 1992 ha ottenuto presso il Politecnico di Torino il titolo di Dottore di Ricerca. Durante il corso di dottorato ha trascorso un anno presso i Laboratori di Ricerca della Digital Equipment Corporation di Marlboro, MA (USA). calia@ismb.it