

# MOBILITÀ AZIENDALE IN SICUREZZA

Il PC portatile è sicuramente l'anello debole del sistema informativo aziendale. Allo scopo di garantire la riservatezza e l'integrità dello scambio di informazioni con i PC itineranti, Arkoon suggerisce autenticazione forte, cifratura adattata alle informazioni scambiate, utilizzazione di VPN (collegamenti IP virtuali privati) e gestione centralizzata delle chiavi e delle regole di sicurezza.



# LE INFORMAZIONI RISERVATE POSSONO USCIRE DALLA RETE AZIENDALE

NON È NECESSARIO FORZARE LE PORTE DELL'AZIENDA PER APPROPRIARSI INDEBITAMENTE DI INFORMAZIONI RISERVATE. ANCHE L'INFORMATICA ITINERANTE E' ESPOSTA AGLI ATTACCHI E RICHIEDE UN'ATTENTISSIMA VIGILANZA.



Attentare alla sicurezza informatica aziendale è relativamente semplice. Gli hacker possono ora colpire ovunque, senza che sia necessario forzare la porta di un ufficio per rubare i documenti cartacei o spiare il disco fisso di un PC portatile. Basta andare in una stazione, un aeroporto o in qualsiasi posto di ristorazione pubblica per collegarsi abusivamente alla rete aziendale tramite il wireless; in altre parole, è possibile rubare informazioni vitali senza neppure scomodarsi a rubare la chiavetta USB o il Pc portatile.

Oltre alle intrusioni durante una sessione, numerosi eventi minacciano i dati contenuti nei PC itineranti. Che si tratti di rischi naturali o di problemi tecnici (rottture, errori umani), quando si verificano provocano più spesso la distruzione dei dati che la loro semplice alterazione.

In termini di sicurezza, la protezione perimetrale della rete aziendale non è più sufficiente per garantire la riservatezza e l'integrità delle informazioni. Dopo aver protetto l'attività all'interno del perimetro aziendale, tramite i firewall, gli antivirus, gli strumenti per la prevenzione delle intrusioni, è necessario completare la fortificazione. In

**LE INFORMAZIONI RISERVATE POSSONO FUORIUSCIRE DALLE POSTAZIONI REMOTE, PC FISSI O ITINERANTI, DAI PALMARI E DAI CELLULARI INTELLIGENTI. LO SCHEMA QUI RIPORTATO DIMOSTRA COME LA MAGGIORANZA DELLE MINACCE NON SIANO VISIBILI AGLI OCCHI DELL'UTENTE, SIA QUEST'ULTIMO ATTIVO O PASSIVO.**

particolare, irrobustendo la sicurezza delle apparecchiature mobili affidate agli itineranti che operano sul campo, siano essi quadri dirigenziali, operatori tecnici o funzionari commerciali.

Insufficientemente protette, tali apparecchiature contengono intrinsecamente un rischio gravissimo: la fuga di informazioni riservate costa ben di più del valore del materiale rubato o smarrito. Per la

sua natura specifica, il furto di informazioni risulta per lo più invisibile (vedi schema qui sotto). La reazione immediata è praticamente impossibile, non rimane altro che una efficace prevenzione. Arkoon, la cui specializzazione è la sicurezza, propone metodi e strumenti per proteggere le informazioni aziendali, ovunque esse si trovino, in modo completo e coerente.

THREATS			SOLUTIONS			
Threat vectors	Active/passive user	Visible/invisible result	Information encryption	Authentication	VPN	Other
Furto del PC portatile	Passivo	Visibile	X			
Intrusione (Man in the middle)	Passivo	Invisibile	X	X	X	
Trasmissione dati in chiaro	Passivo	Invisibile	X			
Condivisione di files	Active	Invisibile	X	X		Configurazione di sistema
Chiavette USB	Active	Invisibile	X	X		Configurazione di sistema
P2P	Active	Invisibile	X			
Infezioni da worms o virus	Passivo	Invisibile				Regole centralizzate Antivirus
Back door	Passivo	Invisibile	X			
Intrusioni	Passivo	Invisibile	X			
Furto d'identità	Passivo	Invisibile	X	X		Rintracciabilità

Il furto di informazioni risulta per lo più invisibile. La reazione immediata è praticamente impossibile, non rimane quindi altro che una efficace prevenzione.

# POLITICA AZIENDALE NELLA MOBILITÀ

**GARANTIRE RISERVATEZZA E INTEGRITÀ DELLE INFORMAZIONI DEGLI ITINERANTI RICHIEDE L'IMPLEMENTAZIONE DI STRUMENTI (FIREWALL, AUTENTICAZIONI, CIFRATURA) ... E COMPORTAMENTI CONSEGUENTI. IL TUTTO SOTTO IL CONTROLLO RIGOROSO DELLA DIREZIONE DEI SERVIZI INFORMATIVI.**

**I** PC portatili e le chiavette USB veicolano informazioni aziendali riservate: la loro protezione è un elemento essenziale della sicurezza informativa dell'azienda. Tuttavia, l'utilizzazione di apparecchiature itineranti pone problemi di incompatibilità e di restituzione delle informazioni, ad esempio nel caso di un utente dimissionario. La generazione e il rinnovo delle chiavi di entrata impongono soluzioni gestionali centralizzate.

Una notissima azienda di consulenza a livello mondiale ha smarrito numerosi PC portatili. Quei PC erano stati utilizzati qualche giorno prima per la dimostrazione di un nuovo sistema di retribuzione di un'azienda leader del settore dell'informatica. Sui dischi fissi dei portatili erano memorizzati, in chiaro, i dati anagrafici dei dipendenti insieme alle informazioni finanziarie che li riguardavano. Questo aneddoto dimostra come i documenti che si trovano all'esterno dell'azienda richiedano protezione assidua e adeguate misure gestionali. Il problema è: come instaurare all'esterno un sistema di controllo sufficiente e coerente con il resto dell'azienda? La risposta risiede nell'interazione coerente di numerosi strumenti di sicurezza: identificazione, autenticazione,

chiavi di cifratura, procedure di cessione delle chiavi (certificati X.509, tokens, chiavette USB, card con microchip integrato...). È quello che normalmente viene definita come infrastruttura fidata di sicurezza.

L'azienda deve elaborare una strategia di sicurezza personalizzata, con regole precise e piani di emergenza adatti a tutte le sue realtà operative. Il parco di apparecchiature mobili, i collegamenti wireless e i livelli di riservatezza e di sicurezza differiscono da azienda a azienda e di conseguenza devono essere personalizzati.

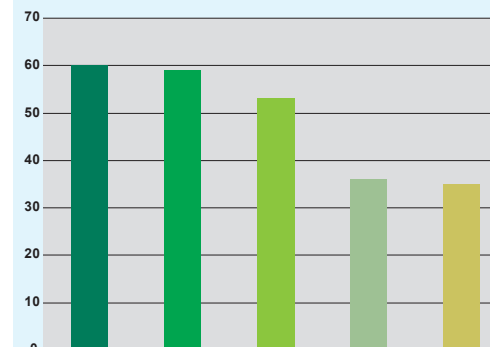
I software di cifratura si distinguono per quanto riguarda la loro trasparenza nei confronti dell'utente e le loro caratteristiche di amministrazione.

La cifratura consiste nel mascherare il contenuto di ciascun file, cartella o volume qualificati come informazione riservata. I molteplici scambi di informazioni con gli itineranti devono tutti essere cifrati: il ricorso a reti private virtuali (VPN SSL o IPSec) rafforza il canale di comunicazione fra i server aziendali e i PC itineranti. La cancellazione dei files deve parimenti essere sicura e irreversibile.

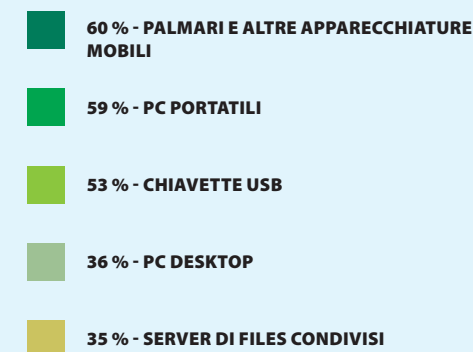
L'accumularsi delle diverse protezioni individuali può risultare piuttosto costosa e per

di più molto pesante in termini gestionali. Conviene allora gestire i collegamenti wireless alla stessa stregua dei collegamenti Internet, cioè considerandoli a rischio, a prescindere. Si tende quindi a proteggere gli accessi remoti con firewall, successivamente si associa a questi un sistema di cifratura per proteggere le informazioni confidenziali memorizzate al di fuori delle sedi aziendali. La soluzione deve essere, per quanto possibile, trasparente e deve corrispondere alle caratteristiche dei potenziali collegamenti. Un'appliance di sicurezza dedicata e centralizzata consentirà di evitare gli interventi tecnici sui PC ogni volta che sia necessario riconfigurarli. Un altro elemento, spesso trascurato, riguarda gli accessi remoti al sistema informativo. Essenziali nel lavoro a distanza o alla gestione centralizzata delle apparecchiature e dei server aziendali, gli accessi remoti consentono all'utente itinerante e agli amministratori di utilizzare in remoto una parte delle risorse informatiche aziendali. Si impone quindi una vigilanza strettissima dei PC remoti, siano questi fissi o itineranti.

## LIVELLI DI RISCHIO DELLE PRINCIPALI APPARECCHIATURE MOBILI



(SOURCE: PONEMON INSTITUTE)



Le apparecchiature mobili (PC portatili, palmari, smartphone) hanno circa 6 probabilità su 10 di memorizzare informazioni non protette. Questa statistica discende da uno studio del Ponemon Institute dell'agosto 2006. Lo stesso studio rivela che più di 8 aziende su 10 hanno subito almeno un furto di PC portatili nell'ultimo anno. Solo il 10% delle persone intervistate dichiarano con certezza di non aver perso alcuna informazione sensibile o riservata memorizzata su un PC portatile nell'ultimo anno, e il 9% preferisce rispondere di non saperlo.

# LA CIFRATURA, PROTEZIONE AZIENDALE NON RAGGIRABILE

LE MINACCE ALLA SICUREZZA INFORMATICA SONO MOLTEPLICI E I CONFINI OPERATIVI DELL'AZIENDA SEMPRE PIÙ LABILI: LA CIFRATURA, LA TRACCIABILITÀ E LA GESTIONE DI REGOLE DI SICUREZZA SONO INDISPENSABILI PER LA SICUREZZA AZIENDALE.

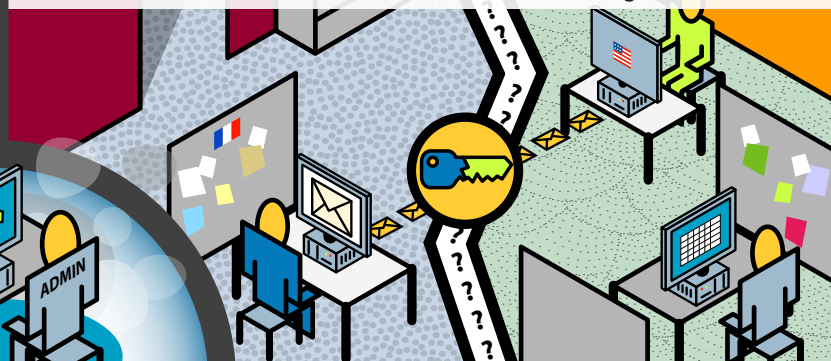
## PREVENIRE IL FURTO

La prima minaccia alle informazioni aziendali: il furto di apparecchiature portatili. Cifrando le informazioni, se ne evita la dispersione.



## CIFRARE I COLLEGAMENTI

La cifratura dei messaggi e dei files riservati permette gli scambi senza rischiare la minima fuga di informazioni



La suite di software Security BOX costringe l'utente a rispettare delle regole di sicurezza aziendale.



Per contrastare le minacce del tipo "man in the middle", si attiva un canale di comunicazione virtuale privata dopo un'autenticazione forte.

## METTERE FUORI GIOCO GLI HACKERS



Il PC aziendale può ospitare applicazioni pericolose. In assenza di autodisciplina, l'unica protezione è la cifratura

## CIRCOSCRIVERE L'UTILIZZAZIONE

# LE TRE FASI FONDAMENTALI PER GARANTIRE SICUREZZA E RISERVATEZZA DELLE INFORMAZIONI

1

## SENSIBILIZZAZIONE UTENTI



Garantire la sicurezza significa gestire la riservatezza delle informazioni, seguire cioè delle procedure di sicurezza precostituite. È necessario prendere coscienza dei rischi “digitali” legati alla mobilità e poi stendere un progetto. Un’azienda non deve essere quotata nelle borse internazionali per avere importanti informazioni da proteggere. La Direzione dell’azienda e un Responsabile da lei nominato devono esaminare ogni aspetto della sicurezza nell’attività operativa dell’azienda. Occorre poi sensibilizzare tutti i collaboratori oppure il progetto per la gestione della sicurezza rischia di fallire in partenza: il progetto coinvolge tutta la struttura aziendale e impatta su ogni suo aspetto organizzativo. È possibile circoscrivere le esigenze e partire da un settore dell’azienda, oppure esaminare il complesso aziendale nella sua totalità: è opportuno stendere un piano d’insieme e metterlo in pratica in funzione delle urgenze specifiche del progetto stesso.

2

## DEFINIZIONE DELLE PROCEDURE

È necessario definire per iscritto le politiche di sicurezza e stabilire “chi fa che cosa e come”, cioè definire le specifiche di comportamento di ognuno, sia all’interno che all’esterno dell’azienda. Dovranno essere definite l’architettura da implementare, le modalità di implementazione e di certificazione. Nella fase di implementazione, l’azienda si avvarrà degli specialisti interni o di consulenti esterni. Sviscerare a priori tutti gli eventuali problemi eviterà di imbattersi in ostacoli tecnici, organizzativi, normativi o legali tenendo conto di quanto in vigore nei vari paesi in cui il piano sarà potenzialmente esteso. Controllare la riservatezza delle informazioni coinvolge numerosi criteri, ivi compreso il livello di fiducia in chi redige materialmente il piano e in chi è preposto ad attuarlo. Tutta la catena deve essere sotto controllo: le specifiche del piano, la politica di attuazione, la scelta degli strumenti e la loro utilizzazione.



3

## GESTIONE DEI CERTIFICATI



Se la cifratura delle email e dei files rappresenta il motore del sistema, la gestione delle chiavi ne è il carburante. Alcune aziende preferiscono mantenere il controllo di tutto ciò che concerne la sicurezza all’interno della loro realtà; altre preferiscono integrare diversi strumenti distinti; altre ancora affidano la gestione dei certificati ad una struttura terza che goda della loro fiducia. Nella fase di creazione delle chiavi, occorre verificare che la soluzione scelta sia compatibile con la PKI prescelta o con quella eventualmente presente in azienda. Nella fase operativa la gestione della soluzione deve restare coerente, nel tempo, con la politica di sicurezza dell’azienda. Le workstation mobili devono sempre collegarsi con l’elenco generale, anch’esso alimentato dalla PKI che assegna chiavi e certificati digitali. Tutti i componenti del sistema devono quindi essere sempre simultaneamente disponibili per assicurare il buon funzionamento dell’insieme.

## MOBILITÀ E MINACCE DIGITALI

Grazie alla disponibilità di reti wireless e computer portatili compatti, potenti ed economici, l’informatica mobile si sviluppa a ritmi sempre più veloci con grande preoccupazione dei responsabili della sicurezza aziendale. In effetti, curiosare nei patrimoni informativi alla ricerca di files riservati, è diventato uno dei passatempi preferiti degli hacker. Il pirata informatico si fa passare per utente abituale o per amministratore, e accede ai files condivisi, indisturbato e all’insaputa di tutti. Colpisce a caso violando i computer portatili in cui si imbatte, approfittando di collegamenti wireless mal protetti. Consulta i files più recenti, copia senza problemi documenti e progetti riservati. A volte vende questi documenti o ne modifica i contenuti prima di renderli pubblici, per puro divertimento o per danneggiare le vittime. Il raggio della vigilanza informatica aziendale deve quindi spingersi fino a raggiungere i collaboratori itineranti e sensibilizzarli affinché evitino l’esposizione di documenti riservati. La mobilità informatica e lo scambio di informazioni riservate deve accompagnarsi ad una certa prontezza di riflessi. I manuali di sicurezza aziendale devono riportare con chiarezza tutti i possibili casi a rischio e le reazioni o i rimedi corrispondenti. Per limitare i rischi e rafforzare la protezione delle informazioni riservate.

# LA SICUREZZA INFORMATICA DELLE POSTAZIONI FISSE E MOBILI UN MODELLO CHE FUNZIONA

È ORMAI INDISPENSABILE CONTROLLARE LA FUGA DI INFORMAZIONI E I COSTI GENERATI DALLA PROTEZIONE DEI POSTI DI LAVORO. JEAN-LUC LARGENTON, DIRETTORE DEI PROGETTI STRATEGICI DI ARKOON, DESCRIVE UNA METOLOGIA DI IMPLEMENTAZIONE.

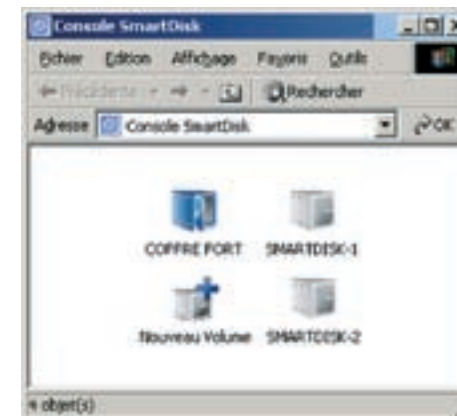
La creazione di un ambiente affidabile e sicuro che includa le postazioni itineranti richiede metodologia e coerenza di comportamento. *“Un approccio strutturale è ovviamente preferibile ad uno sviluppo empirico che non prenda in considerazione le esigenze e l'organizzazione dell'azienda”*, spiega Jean-Luc Largenton. Secondo lui, un approccio corretto per garantire buoni risultati deve passare attraverso

cinque fasi:

- Studio preliminare
- Definizione della politica di sicurezza aziendale
- Stesura del piano di investimenti
- Testi di fattibilità e di accettabilità della soluzione

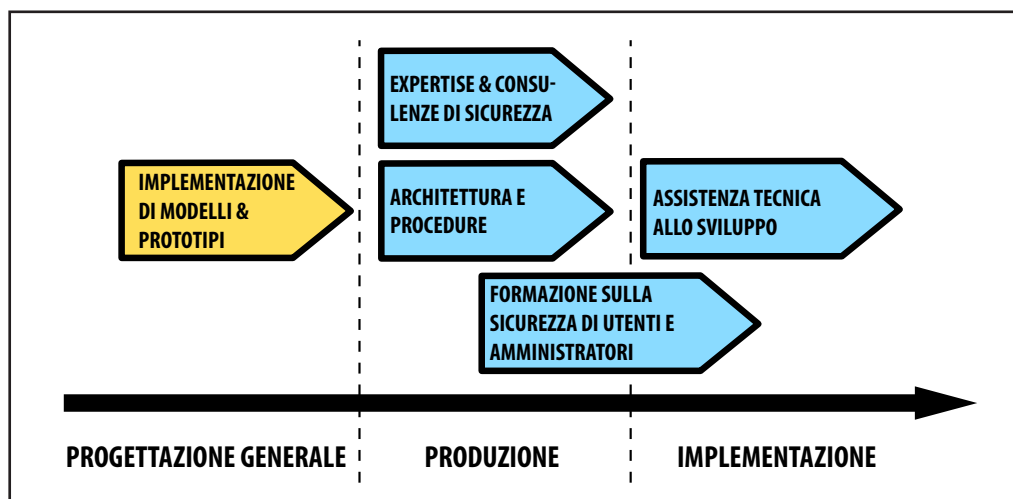
Implementazione, totale o per fasi successive. In questo modo si potrà tenere sotto controllo sia il flusso dei costi di implementazione rispetto

al budget sia l'attuazione delle singole fasi. Al di là di una semplice check-list, occorre varare un processo sistematico di analisi dei risultati e delle singole azioni. *“Ciascuna fase deve essere definita in funzione del contesto tecnico e organizzativo dell'azienda”*, suggerisce Largenton. E precisa che l'amministrazione della sicurezza deve contribuire alla creazione di un ambiente affidabile (PKI, Public Key Infrastructure), al fine di applicare proficuamente la politica di sicurezza. Fra i servizi da supervisionare, la cifratura certificata (EAL4+) e la gestione delle chiavi, essenziali, queste ultime, per la cifratura di files, cartelle e dischi, dei canali di comunicazione fra i PC itineranti e i server aziendali per lo scambio di informazioni riservate e per l'identificazione univoca dell'utente. Gli integratori certificati da Arkoon accompagneranno l'azienda lungo tutto l'iter del suo progetto avvalendosi del supporto degli specialisti di Arkoon. Il primo passo consisterà nella implementazione di un modello operativo e di un suo prototipo. Subito dopo si potrà definire la nuova architettura. Quindi si inizierà la formazione e si proseguirà nel completamento della soluzione prevista.



## ESSENZIALE L'UTENTE

Criteri di praticità e tempi di risposta condizionano l'accettazione da parte dell'utente degli strumenti di sicurezza e di integrità della comunicazione implementati per le apparecchiature itineranti. Sintetizza il direttore dei sistemi informativi di un grande gruppo industriale *“Il top management della nostra azienda è sensibilizzato sui rischi incombenti sulle informazioni aziendali, in modo particolare per quanto riguarda la mobilità. I manager sono coscienti dell'importanza dello scambio di informazioni sul campo e conoscono bene i rischi di fughe per furto o smarrimento di un palmare o di un portatile. L'evoluzione della regolamentazione implica una loro precisa responsabilità e una disciplina comportamentale di utilizzo. La mia difficoltà più grande consiste nel rendere operativa una soluzione di protezione pratica per l'utente e facile da gestire. Entrano in gioco criteri tecnici, ergonomici e tempi di risposta. I prodotti e i servizi di Arkoon mi hanno aiutato a definire una corretta metodologia di implementazione e una gestione efficace della sicurezza. Questo evita di fare passi falsi e garantisce una configurazione ottimale.”*



# GLOSSARIO DELLA SICUREZZA

**Analisi comportamentale:** Nella sicurezza informatica, la dinamica dell'uso della tastiera o quella della stesura della firma o lo studio dell'impronta vocale fanno parte dell'analisi comportamentale.

**AES:** Advanced Encryption Standard. Algoritmo simmetrico di cifratura

**Autenticazione:** Sistema di associazione dei diritti ad una identità (remota) basato su una password talvolta singola, una card con processore, un dispositivo biometrico o un algoritmo temporaneo attuato da entrambe le estremità del collegamento, ad esempio per convalidare la connessione di un utente remoto.

**Autenticazione forte:** Protocollo basato su due elementi di autenticazione per permettere l'accesso al sistema.

**Biometria:** Tecnica di identificazione o di tracciatura dell'utente basata su una o più caratteristiche fisiche (impronte digitali, retina, profilo o contorno del viso).

**Cifratura:** Sistema di mascheratura delle

informazioni. È detta simmetrica quando la stessa chiave è utilizzata per cifrare e decifrare; asimmetrica quando sono necessarie due chiavi: pubblica e privata.

**Certificato digitale:** Blocco di dati che contiene una coppia di chiavi asimmetriche, informazioni sul possessore di tali chiavi e una firma digitale di certificazione dei dati individuali.

**DES:** Metodo di cifratura asimmetrica. Ne esistono anche altri: AES, Triplo DES, o RSA.

**IPSec:** Internet Protocol Security. Protocollo di comunicazione IP di dati protetti, i cui obiettivi sono l'autenticazione, la cifratura e l'integrità degli scambi via Internet.

**LDAP:** Lightweight Directory Access Protocol. Protocollo di servizi di elenchi per la gestione delle identità e dei diritti di accesso alle risorse condivise.

**Firewall:** Appliance hardware o software che filtra il flusso delle informazioni circolanti in rete. Permette l'attuazione di una politica di sicurezza di accesso

ai server e alle risorse di rete, mediante l'applicazione di regole predefinite di filtraggio. Il router/firewall segmenta la rete in più sottoinsiemi e DMZ.

**PKI:** Public Key Infrastructure. Infrastruttura gestionale delle chiavi che include le procedure, il software e l'hardware per creare e gestire i certificati digitali.

**Security BOX®:** Suite di software Arkoon per la protezione delle informazioni riservate memorizzate sui dischi dei PC portatili, chiavette USB e apparecchiature similari: affari in corso, strategie di prodotto, progetti di sviluppo, ecc. Si basa su una serie di strumenti di cifratura molto potenti e su una infrastruttura fidata per garantire all'azienda trasparenza, accessibilità e sicurezza.

**Server di autenticazione:** Server a cui è affidata la verifica dell'identità dell'utente, generalmente con nome e password.

**Firma digitale:** Procedura normalmente basata su certificati X.509 che permette di autenticare l'autore e di garantire l'integrità del documento firmato.

**TLS / SSL:** Transport Layer Security, un tempo Secure Socket Layer. Protocollo client/server per la protezione degli scambi di informazioni su Internet, sviluppato inizialmente da Netscape e, nel 2001, ridefinito dall'IETF. Assicura l'autenticazione del server, o quella del client, la riservatezza degli scambi (sessione cifrata) e l'integrità delle informazioni scambiate.

**UTM:** Unified Threat Management. Nuova tipologia di appliance "all-in-one". Evoluzione del firewall, appliance di sicurezza multifunzionale che integra antivirus, antispam, vigilanza sulle intrusioni e filtraggio.

**VPN:** Virtual Private Network. Rete privata virtuale, estensione della LAN aziendale per garantire l'applicazione di norme di sicurezza su un collegamento Internet, tramite i protocolli IPSec o SSL.

**X.509:** Standard che definisce la struttura dei certificati e l'iter verso l'autorità di certificazione (Certification Authority).

## PER SAPERNE DI PIÙ

Le commissioni nazionali per la tutela della privacy e delle libertà informatiche dei vari paesi raccomandano alle imprese di provvedere i PC portatili di strumenti di sicurezza validi, al fine di minimizzare i rischi susseguenti a furto o smarrimento di dati personali e riservati. Arkoon è l'alternativa europea in grado di garantire l'autenticazione forte, la riservatezza e l'integrità degli scambi e delle informazioni condivise, mediante la gestione centralizzata di una politica di sicurezza personalizzata a misura delle esigenze aziendali.

CORPORATE HEADQUARTERS

1, PLACE VERRAZZANO

CS 30603

69258 LYON CEDEX 09

FRANCE

TEL : +33 (0)4 72 53 01 01

[www.arkoon.com](http://www.arkoon.com) / [info@arkoon.net](mailto:info@arkoon.net)

**ARKOON**  
NETWORK SECURITY

