CONTRATTO

TRA

HT Srl

E

TNT GLOBAL EXPRESS S.p.a.

Il presente Contratto è stipulato da e tra:

- HT Srl, con sede legale in Milano, Via della Moscova n. 13, C. F. 03924730967, P.IVA 03924730967 in persona del legale rappresentante pro-tempore (di seguito "Fornitore"),

E

- TNT GLOBAL EXPRESS S.p.a., con sede legale in San Mauro Torinese (To), Corso Lombardia 63, Codice Fiscale 01273040129, Partita IVA 09399880153, nella persona dell' Amministratore Delegato Ulf Ekstedt e del Consigliere Delegato Joost Bous; (di seguito "TNT")

entrambi di seguito anche indicati come "Parte" o congiuntamente come "Parti".

Premesso che:

A. TNT svolge attività di autotrasporto merci per conto terzi sul territorio nazionale ed internazionale;
B. Il Fornitore è una società operante nel settore della IT Security, specializzata in attività di Penetration Testing e Ethical Hacking;
C. Per l'espletamento delle proprie attività TNT intende avvalersi dei servizi offerti dal Fornitore;
D. il Fornitore è disposto a fornire tali servizi;
E. il presente Contratto è valido per TNT e per tutte le Società da essa controllate e controllanti;
F. le Parti intendono con il presente Contratto disciplinare termini e modalità alla base dei loro rapporti.

Tutto quanto sopra premesso, le Parti convengono e stipulano quanto segue,

PREMESSE E DEFINIZIONI

ARTICOLO 1 PREMESSE ED ALLEGATI

Le Premesse e gli allegati formano parte integrante e sostanziale del presente Contratto.

ARTICOLO 2 OGGETTO

2.1 Oggetto del presente contratto è un intervento cd di Ethical Hacking atto a testare e verificare il livello di sicurezza della infrastruttura rete dati di TNT (d'ora innanzi i Servizi);

2..2 Oggetto del Contratto sono altresì tutte le prestazioni accessorie, preparatorie, necessarie o soltanto utili all'espletamento dei Servizi, quali a titolo esemplificativo e non esaustivo, incontri per riunioni, trasferte, etc, i cui costi si intendono inclusi nel corrispettivo indicato al successivo art.8.Tali prestazioni dovranno essere intraprese di concerto fra le Parti.

2.3 I Servizi e le modallità di esecuzione dei medesimi sono dettagliati nell'Offerta del Fornitore allegata al presente contratto sub lettera A).

ARTICOLO 3 CONTENUTO DELLE PRESTAZIONI DEL FORNITORE

3.1 Il Fornitore per tutta la durata del presente Contratto, si obbliga nei confronti di TNT, ad erogare i Servizi ed a raggiungere gli standard ed i livelli di servizio stabiliti nell'offerta allegata;

3.2 Per erogare tutti i Servizi del presente Contratto il Fornitore si impegna a:

- Porre in essere le attività necessarie;
- Fornire le risorse in termini di materiali;
- Compiere le attività come descritte nell'offerta allegata

3.3 La gestione dell'attività del Fornitore si intende svolta a suo esclusivo rischio e responsabilità e non implica responsabilità di TNT né riconoscimento di applicabilità delle norme di cui al D.Lgs 276/03 o analoga.

ARTICOLO 4 LIVELLI DI SERVIZIO

Il Fornitore si impegna a rispettare le tempistiche concordate.

ARTICOLO 5 RESPONSABILITA' DEL FORNITORE – GARANZIE

5.1 Il Fornitore è responsabile per le difformità ed i vizi della sua prestazione. Sono esclusi i casi di errori od omissioni determinati da TNT, anche nel trasferimento dei dati al Fornitore imputabili esclusivamente a TNT o qualora i programmi informativi non siamo utilizzati da TNT conformemente alle istruzioni ricevute dal Fornitore o qualora TNT abbia modificato il suo ambiente informativo, reti, server e workstation incluse, ad insaputa del Fornitore o abbia comunque dato indicazioni errate o incomplete.

5.2 Il Fornitore si impegna a rispettare le norme comportamentali e di sicurezza vigenti comunicate da TNT;

5.3 Il Fornitore garantisce altresì di avere la piena disponibilità giuridica del software utilizzato per l'erogazione dei Servizi.Tutti i dati, i programmi, i supporti di memorizzazione e gli altri materiali forniti da TNT al Fornitore, in funzione dell'erogazione dei Servizi, saranno eliminati su richiesta di TNT e dietro pagamento al Fornitore delle spese sostenute a fronte di tale eliminazione, alla data di estinzione del presente Contratto.

5.4 Il Fornitore sarà responsabile per ogni danno diretto causato a TNT nell'esecuzione dei Servizi, quali, a titolo meramente indicativo, perdita di dati, generazione di errori, etc.

ARTICOLO 6.ASSICURAZIONI

6.1 Il Fornitore dichiara di aver stipulato con Primaria Compagnia Assicurativa idonea polizza assicurativa, con massimale non inferiore ad Euro 2.500.000,00 (duemilionicinquecentomila/00) contro i danni derivanti dall'esecuzione della propria attività (RC Professionale/ RCT con copertura danni professionali);

6.2 Il Fornitore si impegna a consegnare su richiesta di TNT copia della predetta polizza entro e non oltre 15 giorni dalla richiesta.

ARTICOLO 7 RESPONSABILITA' ED OBBLIGHI DI TNT

TNT si impegna a mettere a disposizione del Fornitore il personale necessario all'analisi dell'ambiente in cui dovranno essere prestati i Servizi. Metterà inoltre a disposizione il personale necessario ad interfacciare quello del Fornitore per il compimento di tutte le operazioni sia nelle sue sedi, sia presso il Fornitore, così come richiesto dallo studio, dalla definizione e dalla prestazione dei Servizi;

ARTICOLO 8 COMPENSO

8.1. Il compenso previsto per i Servizi resi dal Fornitore viene stabilito in complessivi Euro 14.000,00 (quattordicimila/00) oltre IVA, da corrispondersi in una unica soluzione a presentazione di regolare fattura

8.2 I pagamenti saranno effettuati da TNT a mezzo bonifico bancario ed a 60 (sessanta) gg d.f.; la fatturazione è prevista alla sottoscrizione dell'ordine.

9. DURATA DEL CONTRATTO

9.1. Il presente Contratto entrerà in vigore a partire dal 1 Gennaio ed avrà durata sino al 31 Dicembre 2012. E' esclusa ogni facoltà di tacito rinnovo

10. RISOLUZIONE DEL CONTRATTO E RECESSO DELLE PARTI

10.1 Di fronte all'inadempimento di una Parte alle obbligazioni previste dal presente Contratto l'altro contraente potrà intimare per iscritto, mediante una comunicazione specifica e circostanziata, all'inadempiente di porvi rimedio entro il termine perentorio ritenuto congruo. Qualora la Parte intimata, entro tale termine perentorio, non abbia provveduto a porre rimedio all'inadempimento contestatogli, la Parte intimante potrà comunicare per iscritto la sua volontà di ritenere risolto il Contratto o una parte autonoma di esso (con riferimento agli obblighi disciplinati nelle sezioni più avanti descritte) a norma dell'art. 1456 c.c.; e ciò a condizione che la violazione riguardi gli obblighi contrattuali inerenti la qualità e la quantità dei servizi da erogare, il pagamento dei corrispettivi, il segreto aziendale e la riservatezza dei dati, la tutela della proprietà intellettuale, le garanzie prestate da Fornitore;

10.2 A partire dalla comunicazione di risoluzione o di recesso di TNT, ovvero dalla data di scadenza del Contratto, il Fornitore continuerà ad eseguire, dopo il ricevimento della comunicazione riguardante la risoluzione, quei Servizi in corso di esecuzione e dei quali TNT in buona fede possa ragionevolmente chiedere la continuazione, verso la corresponsione dei compensi dovuti per i servizi che saranno resi a seguito di tale richiesta;

10.3 Ognuna delle Parti ha facoltà di recedere in qualsiasi momento, senza onere alcuno, dal presente Contratto, se l'altra Parte è sottoposta a procedura concorsuale, risulta manifestatamente insolvente o è messa in liquidazione anche volontaria.

ARTICOLO 11. DIVIETO DI CESSIONE DEL CREDITO – DIVIETO DI CESSIONE DEL ACCORDO – SUBAPPALTO

11.1 Ai sensi e per gli effetti dell'art. 1260 c.c. per nessuna ragione una Parte può cedere a terzi i crediti derivanti dal presente Accordo, né può porre in essere operazioni comunque volte alla medesima finalità senza una formale autorizzazione scritta dell'altra parte.

11.2 Il presente Accordo ed i singoli ordini non sono cedibili in tutto od in parte senza preventiva autorizzazione scritta di TNT. Tuttavia, TNT avrà il diritto di cedere a qualunque titolo, gratuito o oneroso il presente Accordo e/o i singoli ordini alle società appartenenti al Gruppo TNT NV (inclusi i casi di fusione, di incorporazione, di cessione di ramo di azienda od ogni altra forma di riorganizzazione sociale), senza necessità di autorizzazione alcuna da parte di controparte, intendendosi la stessa concessa in questa sede in via definitiva ed irrevocabile.

11.3 Qualora, previa autorizzazione scritta di TNT, il fornitore dovesse affidare a terzi l'esecuzione del servizio o di una parte di esso, lo stesso dovrà garantire per il terzo prestatore, dovendosi ritenere responsabile per quest'ultimo ed in generale della corretta riuscita dell'opera. Si intende comunque fatto salvo il diritto al risarcimento di eventuali danni patiti da TNT.

ARTICOLO 12 DIRITTI DI PROPRIETÀ INDUSTRIALE ED INTELLETTUALE.

12.1 Fatta eccezione per ragioni di referenziabilità, in nessun momento dovrà essere utilizzato il nome, il marchio o la denominazione sociale di TNT o di società collegate o controllate ed altresì a non fare

riferimento in nessun momento a rapporti intercorrenti con TNT o con società collegate o controllate (prima, dopo, o durante l'esecuzione dell' Accordo), senza la previa autorizzazione scritta di TNT.

12.2 E' fatto altresì divieto di utilizzare in qualsiasi forma il marchio di TNT, o qualsiasi altro segno distintivo della stessa che appaia idoneo, in modo diretto o indiretto, a generare confusione, contraffazione, volgarizzazione o danneggiamento del suddetto marchio, salvi i casi in cui è espressa autorizzazione da parte di TNT all'utilizzo per le finalità e secondo le modalità da convenire fra le parti.

12.3 Eventuali disegni, capitolati, norme e tabelle ed altra documentazione tecnica, nonché i modelli, i campioni e le attrezzature specifiche, il know-how che TNT potrà mettere a disposizione, restano di proprietà di TNT e potranno venire usati soltanto per l'esecuzione dell'Accordo. I medesimi, salvo che per l'esecuzione dei servizi non potranno essere copiati o riprodotti né utilizzati in alcun modo e/o trasmessi utilizzati da terzi, senza l'autorizzazione scritta di TNT.

ARTICOLO 13 RISERVATEZZA – TRATTAMENTO DEI DATI

13.1 L'esecuzione degli obblighi derivanti dal presente Accordo può comportare l'accesso ad informazioni riservate dell'altra Parte (di seguito "Informazioni Riservate"). Le Informazioni Riservate includeranno qualsiasi informazione che sia stata espressamente identificata per iscritto come riservata al momento della rivelazione, qualsiasi informazione che, considerate le circostanze in cui essa viene rivelata, dovrebbe essere identificata come riservata da una persona di media diligenza e, in genere, tutte le informazioni attinenti all'attività svolta, all'organizzazione interna, nonché ai clienti delle Parti, al know-how utilizzato nonché alle attività e ai servizi oggetto di privativa.

13.2 Le Parti si obbligano, salvo che sia richiesto dalla legge, a non rendere disponibili le rispettive Informazioni Riservate a terzi in alcuna forma ed a non usare le Informazioni Riservate dell'altra Parte per alcuna finalità diversa dall'esecuzione delle obbligazioni del presente Accordo.

13.3 Il fornitore si impegna a custodire con la massima attenzione e riservatezza la documentazione che TNT dovesse mettere a sua disposizione. In particolare, il fornitore si impegna a conservare la documentazione ricevuta da TNT come depositaria con obbligo di custodia sino al momento della restituzione della stessa, che dovrà avvenire entro i trenta giorni successivi alla cessazione o risoluzione del presente Accordo, nonché entro dieci giorni dalla richiesta scritta di TNT.

13.4 La violazione dell'obbligo di riservatezza di cui al presente articolo comporterà il diritto di richiedere alla parte inadempiente il risarcimento del maggior danno eventualmente subito.

13.5 Le Parti concordano di mantenere riservate le Informazioni Riservate per tutta la durata del presente Contratto e per i 10 anni successivi. il fornitore si impegna altresì, a non comunicare le Informazioni Riservate ad altri, se non richiesto dalla legge o per fini strettamente legati all'esecuzione del Contratto ed a mettere in atto tutte le ragionevoli precauzioni affinché anche i propri dipendenti, collaboratori, consulenti e/o ausiliari si adeguino alle disposizioni del presente articolo.

13.6 Con la sottoscrizione del presente contratto, le Parti, relativamente al trattamento, alla comunicazione ed alla diffusione dei dati personali reciprocamente forniti, come previsto dal D.Lgs. 30 giugno 2003 n. 196, e riguardanti le due società, danno atto di essere state adeguatamente informate circa le finalità del succitato trattamento, nonché dei diritti sanciti dall'art. 7 della suddetta normativa. Danno altresì atto che, ai sensi dell'art. 24 del suddetto decreto, non è più necessario il reciproco consenso al trattamento stesso.

13.7 Per la TNT titolare del trattamento è la TNT GLOBAL EXPRESS S.p.A. nella persona del Legale Rappresentante. Per la HT Srl. il titolare del trattamento è il Legale Rappresentante

ARTICOLO 14 LEGGE APPLICABILE - FORO COMPETENTE

Ogni questione relativa all'interpretazione, esecuzione ed estinzione dei servizi oggetto del presente documento, che non possa essere risolta in via bonaria, è devoluta alla competenza esclusiva del Tribunale di Torino.

ARTICOLO 15 D.LGS 231/01 E CODICE ETICO

15.1 Ai sensi del D.Lgs. 8 giugno n.231, TNT Global Express Spa ha adottato un Modello di organizzazione, Gestione e Controllo nonché di un Codice Etico (di seguito cumulativamente indicati come "Modello"), entrambi consultabili sul sito Internet aziendale all'indirizzo www.tnt.it. Tale Modello esprime gli impegni e le responsabilità etiche di TNT Global Express Spa nei confronti dei propri stakeholders nella conduzione dei propri affari e risponde all'esigenza di assicurare condizioni di correttezza e trasparenza nello svolgimento delle attività aziendali.

15.2 Con la sottoscrizione del contratto, la controparte dichiara di conoscere il Modello di TNT e che le informazioni fornite a TNT Global Express Spa nel corso delle trattative, sono complete, esatte e veritiere.

15.3 La Parte Contraente si impegna, nell'esecuzione del contratto, a tenere un comportamento conforme al Modello di TNT e comunque tale da non integrare alcuno dei reati di cui al D.Lgs. 231/2001.

ARTICOLO 16 DISPOSIZIONI DIVERSE

16.1 Ognuna delle parti dovrà comunicare immediatamente all'altra per iscritto tutte le variazioni di indirizzo, ragione o denominazione sociale. Al momento le parti dichiarano il proprio domicilio come specificato in epigrafe.

16.2 Ai sensi e per gli effetti degli artt. 1341 e 1342 c.c., le Parti si danno atto e riconoscono che il presente accordo quadro è il risultato di trattative intercorse tra le stesse in piena reciproca libertà e con libera determinazione di ciascuna, dichiarano altresì che il presente accordo quadro è stato oggetto di specifica trattativa e contrattazione in ogni sua clausola, e che pertanto le suddette norme non possono trovare applicazione nel caso di specie.

ALLEGATI:

1 - Offerta HT del 2 Dicembre 2011;

2 - Codice Etico TNT;

3 – TNT Business Principles;

3 – Politica di Responsabilità sociale;

5 – Autocertificazione mancanza conflitti di interesse;

6 – Visura camerale HT con dicitura antimafia;

7 – Casellario giudiziale e carichi pendenti e/o Autocertificazione componenti il Consiglio di Amministrazione di HT.

Letto, confermato e sottoscritto.

S. Mauro T.se, 6 Marzo 2012

TNT Global Express S.p.a.

(Ulf Ekstedt – Amministratore Delegato)

(Joost Bous – Consigliere Delegato)

HT Srl

HT Srl
Via Moscova, 13 - 20121 Milano

]HackingTeam[

Spett.le
TNT Global Express s.p.a.
Corso Lombordia, 63
10099 San Mauro Torinese (TO)

Milano, 2 Dicembre 2011

Offerta n. 20110926.173-3.AL

Alla cortese attenzione: Sig. Angelo Lupatin

Oggetto: Offerta per attività di Ethical Hacking

A seguito dei colloqui intercorsi vi sottoponiamo la nostra proposta per il servizio in oggetto.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

HT Srl

Alessandro Lomonaco

1

Offerta per attività di Ethical Hacking

Sommario

1. RICHIESTA DEL CLIENTE

Il Cliente richiede di formulare una proposta relativa ad intervento di Ethical Hacking sulla propria infrastruttura.

In altre parole, si richiede una consulenza di Security Assessment che verifichi il livello di sicurezza secondo una logica indipendente e supra-partes.

2. SOLUZIONE PROPOSTA

L'intervento proposto comprende un attività di Ethical Hacking relativo a:

2.1. Vulnerability Assessment network interno

Oggetto: da 10 a 250 server.

Approccio: l'attività si svolgerà in modalità black box (senza credenziali).

Documentazione: si prevedono 2 alternative: report dello strumento con riassunto delle principali vulnerabilità; report in inglese e verifica manuale di tutte le vulnerabilità.

Vincoli: non deve essere effettuata alcuna attività di verifica DoS, né di verifica buffer overflow, per i servizi in produzione.

Effettuazione test: presso la sede di San Mauro Torinese, in giorni feriali, durante gli orari lavorativi.

2.2. Simulazione utenti

Oggetto: verifica di 2 profili utente:

- Dipendente con PC aziendale standard
- Consulente con PC proprio

Vincoli: non deve essere effettuata alcuna attività di verifica DoS, né di verifica buffer overflow, per i servizi in produzione.

Effettuazione test: presso le sedi di San Mauro Torinese, in giorni feriali, durante gli orari lavorativi.

2.3. Test WIFI

Oggetto: verifica infrastruttura WIFI (no rogue access point discovery).

Vincoli: non deve essere effettuata alcuna attività di verifica DoS, né di verifica buffer overflow, per i servizi in produzione.

Effettuazione test: presso le sedi di San Mauro Torinese, in giorni feriali, durante gli orari lavorativi.

2.4. Test BES

Oggetto: 1 server BES e 2 PDL Black Berry.

Approccio: l'attività si svolgerà in modalità white box (con credenziali)

Vincoli: non deve essere effettuata alcuna attività di verifica DoS, né di verifica buffer overflow, per i servizi in produzione.

Effettuazione test: presso la sede di San Mauro Torinese, in giorni feriali, durante gli orari lavorativi.

3. METODOLOGIA DELLA SOLUZIONE PROPOSTA

3.1. Security Probe

Un attacco compiuto da hacker reali segue di norma la traccia che segue. Le attività di Ethical Hacking da noi eseguite tentano di emulare al 100% il comportamento di un vero hacker. Di seguito sono riportate le metodologie rispettivamente per la verifica network dall'esterno, per la verifica applicativa. Esse contemplano un livello di approfondimento notevole.

3.1.1. Analisi non invasiva

3.1.1.1. Footprinting

Questa fase ha lo scopo di raccogliere il maggior numero di informazioni sull'obiettivo che si intende attaccare senza "toccare" l'obiettivo stesso, ovvero effettuando una cosiddetta "analisi non invasiva". In particolare in questa fase si cerca di determinare: *domini, blocchi di rete e indirizzi IP dei sistemi direttamente collegati a Internet.* Gli strumenti utilizzati sono: Search Engine, Whois server, Arin database, interrogazione DNS, ecc.

3.1.1.2. Scanning

L'obiettivo dello scanning è ottenere una mappa più dettagliata possibile del sistema da attaccare. Ciò significa acquisire informazioni su quali indirizzi IP dei blocchi di rete trovati nella fase precedente siano effettivamente "contattabili" dall'esterno (IP discovery), quali servizi siano "attivi" (TCP/UDP port scan) e, infine, quali sistemi operativi "posseggano". Gli strumenti utilizzati sono: interrogazioni ICMP (gping, fping, ecc.), scansione delle porte TCP e UDP (strobe, netcat, nmap, ecc.), fingerprint dello stack (nmap, ethercap).

3.1.2. Analisi invasiva

3.1.2.1. Enumeration

Con questa fase si inizia l'"analisi invasiva". Si effettuano, infatti, connessioni dirette ai server e "interrogazioni" esplicite. Tali attività potrebbero, a seconda della configurazione presente sui sistemi target, originare dei logs sui sistemi (tipicamente su sistemi di controllo). Attraverso l'enumerazione si vuole giungere a identificare, sulle macchine riscontrate come raggiungibili, account validi (list user accounts), risorse condivise (list file shares) e applicazioni attive sulle porte in ascolto (identify application). Le tecniche utilizzate variano a seconda dei sistemi operativi delle macchine che vogliamo analizzare.

3.1.3. Attacco

3.1.3.1. Gaining access

Una volta ottenute le informazioni del punto precedente, inizia il vero e proprio attacco che ha come obiettivo riuscire a "entrare" nel sistema remoto. I metodi utilizzati anche in questo caso dipendono dal sistema operativo della macchina target, ma si basano sostanzialmente sulla ricerca di password corrispondenti agli utenti trovati (password guessing), sullo sfruttamento di errori progettuali delle applicazioni e servizi attivi sul server (buffer overflows, attacchi data driven, ecc.) o del sistema operativo stesso.

3.1.3.2. Escalating privileges 1

L'obiettivo di questa fase è sfruttare i risultati ottenuti nella fase precedente per ottenere il pieno controllo del sistema remoto attaccato. Ciò si ottiene, per esempio, reperendo i files presenti sul sistema che contengono le password (/etc/passwd, SAM, ecc.) e tentando di decifrare le password in essi contenute (password cracking), oppure utilizzando appositi exploits.

3.1.4. Consolidamento

3.1.4.1. Pilfering

Se si giunge a questa fase significa che si è ottenuto il pieno controllo del sistema target. Quindi è bene valutare la configurazione del sistema stesso al fine di capire se, dove e cosa il sistema registra (logs). A questo punto la macchina in oggetto può diventare una "testa di ponte" per attaccare altre macchine. In tal caso saranno reperite informazioni riguardanti altri sistemi.

3.2. Assessment Applicativo

Questa analisi è costituita da una serie di tentativi d'attacco che coinvolgono solo i protocolli di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni.
Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server.
Esistono diverse categorie di attacchi verso applicazioni web, che possono portare alla compromissione di uno o più layer dell'intera infrastruttura applicativa: web server, application server, data tier.
Caratteristica comune a tutti gli attacchi applicativi è la completa trasparenza ad ogni sistema di difesa perimetrale (firewall, ids, ecc.): manipolazioni dei protocolli di layer 7 (applicativi) non possono essere rilevate da dispostivi che analizzano il traffico a layer 3 (network).
Il test sarà condotto in modalità anonima ed in "user-mode".

[1] Vogliamo specificare che, considerata la natura della presente offerta, le nostre attivita' *non si spingeranno in nessun caso oltre questo punto (ESCALATING PRIVILEGES) a meno di una specifica autorizzazione in tal senso da parte del cliente.* In altre parole, si cerchera' di **dimostrare l'effettiva possibilità di assumere il controllo dei sistemi senza apportare alcuna modifica agli stessi.**

Ciò significa che, preventivamente, dovra' essere creato un account tramite le usuali procedure di attivazione al fine di permettere a Hacking Team di accedere come utente autorizzato. Non saranno accettati account di altro tipo (di test interno, amministrativi, etc.) poiché non fornirebbero la corretta valutazione circa il rischio che un utente registrato possa cercare di accedere in modo fraudolento ad informazioni per cui non è autorizzato.

L'attività comprende l'analisi dell'applicazione in termini architetturali, verranno analizzate le configurazioni delle macchine interessate, sia a livello di sistema operativo che applicativo.

In generale, le vulnerabilità di livello applicativo sono spesso legate ad errori contenuti nel codice delle applicazioni.

Esistono due classi di errori, che richiedono differenti strategie per essere identificati e rimossi: errori logico-architetturali ed errori di implementazione.

Errori logico-architetturali

Gli errori logico-architetturali consistono nel mancato utilizzo di meccanismi di sicurezza, oppure nell'utilizzo di meccanismi non adeguati a raggiungere lo scopo desiderato. Tali errori sono imputabili ad una non corretta definizione dei requisiti di sicurezza e/o ad una inadeguata progettazione dell'architettura.

Gli errori logico-architetturali più comuni sono i seguenti:

- gestione non corretta delle sessioni;
- uso di meccanismi di autenticazione deboli, che
  - permettono agli utenti di utilizzare password guessable;
  - rilasciano informazioni che permettono di restringere lo spazio di ricerca per attacchi di tipo brute force;
- trasmissione di informazioni sensibili su canali non cifrati;
- assunzioni errate in merito all'attendibilità e veridicità di input ricevuti dall'utente;
- assunzioni errate in merito alla funzionalità di sistemi e/o applicazioni client-side (ad esempio, browser web) che si trovano sotto il controllo dell'utente (o dell'attaccante!).

Errori implementativi

Questi errori si originano in fase di sviluppo, quando specifiche di alto livello, corrette dal punto di vista logico, vengono tradotte in codice che non gestisce correttamente tutti i casi i possibili; i malfunzionamenti che si verificano in casi particolari possono essere sfruttati per indurre nelle applicazioni comportamenti non previsti e/o non desiderati.

La grande maggioranza degli errori implementativi è dovuta ad una non corretta validazione dei parametri in ingresso, oppure alla gestione non corretta di alcuni input particolari, non previsti dal programmatore. La loro natura rende estremamente difficile prevederne l'impatto: in alcuni casi, questi errori possono avere conseguenze gravi sulla sicurezza di una applicazione, anche se gli elementi di codice interessati non sono direttamente legati a funzionalità critiche.

Gli attacchi di livello applicativo sfruttano vulnerabilità (sia di natura logico-architetturale, sia di natura implementativa) per indurre nelle applicazioni comportamenti anomali, le cui conseguenze possono essere le più disparate: crash dell'applicazione, furto di dati, accesso ai sistemi su cui le applicazioni sono eseguite, ecc.
Allo scopo di inquadrare il tema della sicurezza del livello applicativo, sia in termini di "opportunità" offerte all'intrusore, sia di minacce per le potenziali vittime di intrusioni, si dà una sintetica descrizione delle principali tecniche di attacco utilizzate nell'ambito delle applicazioni web.
I concetti e la terminologia introdotti saranno utilizzati nel presente documento per descrivere i risultati dell'assessment svolto.

3.2.1. Authentication brute-forcing

- Obiettivo: accesso aree riservate ad utenti in possesso di opportune credenziali.
- Attaccanti: chiunque non sia in possesso di credenziali valide ed abbia interesse ad accedere alle informazioni contenute nelle aree riservate, oppure chi, pur possedendo credenziali valide, intende accedere all'area riservata con l'identità di un altro utente.
- Descrizione: consiste nella sottomissione, spesso con l'ausilio di tool automatici, di un grande numero di credenziali (ad esempio coppie username,password), fino ad ottenere una risposta di autenticazione riuscita dal sistema. La generazione delle credenziali può prevedere l'uso di regole (ad esempio, generazione di tutte la password di sei caratteri costituite da soli caratteri alfanumerici) oppure di dizionari preesistenti.
- Condizioni necessarie per l'attacco: ogni sistema che dispone di un sistema di autenticazione è esposto a questo attacco.
- Probabilità di successo: dipende dalla dimensione dello spazio delle credenziali.
- Aspetti facilitanti: l'effort necessario per un attacco può essere sensibilmente ridotto da uno o più dei seguenti fattori:
  - password guessable: l'uso da parte degli utenti di password guessable aumenta la probabilità di successo degli attacchi basati su dizionario;

- struttura delle credenziali: l'imposizione di una struttura semplice alle credenziali (ad esempio, password costituite da soli numeri o sole lettere, lunghezza non superiore a sei caratteri, ecc.) può diminuire sensibilmente la dimensione dello spazio di ricerca;
- l'uso di messaggi di errore troppo informativi in caso di autenticazione fallita (ad esempio indicazioni che permettono di distinguere fra username errato e password errata) possono ridurre lo spazio di ricerca.

- Contromisure 2: gli attacchi di tipo brute force non possono essere prevenuti, ma esistono tecniche efficaci per ridurne drasticamente la probabilità di successo:
  - limitazione del numero massimo di tentativi di autenticazione falliti per ogni connessione;
  - adozione di controlli che vietano l'uso di password guessable o troppo semplici;
  - eliminazione dei messaggi di errori informativi.

3.2.2. Cross site scripting (XSS)

- Obiettivo: furto d'identità ai danni di utenti di applicazioni web che fanno uso di cookie per la gestione delle sessioni.
- Attaccanti: chiunque sia interessato al furto dell'identità di un utente autorizzato (che abbia stabilito una sessione con l'applicazione web).
- Descrizione: si tratta di una tecnica che, mediante l'inserimento di elementi di scripting nei parametri inviati all'applicazione, provoca l'esecuzione degli stessi da parte del browser della vittima. In alcuni casi particolari le stesse tecniche e le stesse vulnerabilità applicative possono essere sfruttate per provocare l'esecuzione di codice sul server (esempio: Server Side Include, ecc.). Gli elementi di scripting causano l'invio dei cookie settati dall'applicazione target sul browser della vittima verso server un HTTP sotto il controllo dell'attaccante. Solitamente l'obiettivo dell'attacco è il cookie di sessione della vittima. La conoscenza di questo cookie permette infatti di sottoporre richieste all'applicazione utilizzando l'identità della vittima. Gli attacchi di cross site scripting sono possibili quando l'applicazione web restituisce al browser (per normale logica di funzionamento o a causa di una condizione di errore) parametri sottoposti dall'utente in una precedente richiesta.
- Condizioni necessarie per l'attacco: assenza di controlli sull'input ricevuto ed errori relativi all'escaping di metacaratteri nell'HTML ritornato al browser.
- Probabilità di successo: questo attacco richiede l'uso di tecniche di social engineering per indurre la vittima a stabilire una sessione con l'applicazione target e sottoporre ad essa una

[2] Le contromisure indicate in questo come in tutti gli altri casi sono da intendersi ovviamente come generiche. Caso per caso potranno essere o smentite, o confermate oppure rese più precise e puntuali.

richiesta contenente il codice malizioso. Frequentemente questo viene fatto per mezzo di email che invitano a seguire un link verso l'applicazione target. La probabilità di successo di tali attacchi è solitamente bassa.

- Aspetti facilitanti: in alcuni casi è possibile inserire elementi di scripting in parametri che vengono salvati su database e restituiti all'utente ad ogni successiva richiesta (database XSS). Questo determina l'invio di cookie verso il server HTTP sotto il controllo dell'attaccante ogni volta che la vittima accede all'applicazione ed aumenta in modo considerevole la probabilità che l'attaccante riesca ad utilizzarlo con successo.
- Contromisure: gli attacchi di tipo XSS possono essere neutralizzati mediante le seguenti tecniche:
  - filtraggio dei parametri in input, mediante filtri che eliminano dall'input i metacaratteri utilizzati in HTML e linguaggi di scripting client-side (<, >, apici, ecc.);
  - escaping dei metacaratteri contenuti nei parametri in input che devono essere inseriti in pagine HTML restituite al browser degli utenti.

3.2.3. SQL Injection

- Obiettivo: gli attacchi basati su SQL injection possono avere diversi obiettivi:
- accesso ad informazioni riservate memorizzate sui database server che costituiscono il data layer dell'architettura applicativa attaccata;
- accesso non autorizzato all'applicazione, aggirando il meccanismo di autenticazione;
- esecuzione di comandi sui server del data layer.
- Attaccanti: utenti autorizzati che mirano ad accedere ad informazioni per le quali non possiedono diritti di accesso; utenti non autorizzati.
- Descrizione: si tratta di tecniche di manipolazione dei parametri in input utilizzati dall'applicazione per eseguire query SQL sul database. Lo scopo è sovvertire la logica della query in modo da ottenere:
  - messaggi di errore contenenti informazioni sulla struttura del database utilizzato;
  - informazioni differenti da quelle che la query dovrebbe estrarre;
  - recordset vuoti o tali da produrre un malfunzionamento dei meccanismi di autenticazione, allo scopo di accedere all'applicazione senza essere in possesso di credenziali valide;
  - esecuzione di comandi di sistema tramite stored procedure.
- Condizioni necessarie per l'attacco: mancanza di filtri di validazione dell'input, che eliminano dai parametri inviati dall'utente token pericolosi, come parole chiave riservate del linguaggio SQL (ad esempio, SELECT, OR, ecc.).

- Probabilità di successo: fortemente dipendenti dalla logica applicativa.
- Aspetti facilitanti: la visualizzazione, sul lato client, dei messaggi di errore relativi all'accesso al database permette all'attaccante di raccogliere informazioni sulla sua struttura, aumentando significativamente le probabilità di successo.
- Contromisure: gli attacchi di tipo SQL injection possono essere neutralizzati mediante le seguenti tecniche:
  - filtraggio dei parametri in input, mediante filtri che eliminano dall'input token riservati e metacaratteri del linguaggio SQL;
  - gestione degli errori di accesso al layer di accesso ai dati, allo scopo di intercettare e bloccare la visualizzazione lato client dei messaggi di errore.

3.2.4. Path traversal

- Obiettivo: browsing di directory presenti sul web server ma non appartenenti alle applicazioni web pubblicate su di esso, per le quali non è previsto l'accesso da parte degli utenti.
- Attaccanti: questo tipo di attacco può essere portato da chiunque possa stabilire una connessione HTTP verso i server su cui è pubblicata l'applicazione.
- Descrizione: un attacco di path traversal consiste nella sottomissione di richieste verso il web server per risorse il cui URL contiene path non appartenenti alle applicazioni web pubblicate su di esso. Poiché in generale tali path non sono noti all'attaccante, essi vengono specificati in forma relativa, partendo dalla posizione di risorse note ed utilizzando sintassi del tipo "../../" per navigare a ritroso il file system. Si noti che questo attacco non è in alcun modo correlato alla logica applicativa, ma sfrutta eventuali vulnerabilità del server HTTP.
- Condizioni necessarie: queste tecniche possono essere utilizzate in presenza di web server sui quali non sono installate le security patch opportune; in ogni caso, la loro applicabilità non dipende dalla particolare applicazione pubblicata sul web server.
- Probabilità di successo: dipende dall'accuratezza della manutenzione del web server.
- Aspetti facilitanti: nessuno
- Contromisure: aggiornamento dei web server mediante applicazione delle opportune patches.

3.2.5. OS command injection

- Obiettivo: esecuzione di comandi di sistema sulle macchine su cui insiste l'applicazione.
- Attaccanti: questo tipo di attacco può essere portato da chiunque possa stabilire una connessione HTTP verso i server su cui è pubblicata l'applicazione.

- Descrizione: questo attacco può essere effettuato quando la logica applicativa utilizza dati forniti in input dall'utente come parametri per l'esecuzione di comandi di sistema. Se la logica applicativa non esegue correttamente il parsing di tali dati, è possibile provocare l'esecuzione di comandi aggiuntivi e/o differenti da quelli previsti dagli sviluppatori.
- Condizioni necessarie: queste tecniche possono essere utilizzate in presenza di componenti dinamici che richiamano comandi di sistema senza effettuare un corretto parsing dei parametri di input.
- Probabilità di successo: dipendenti dall'accuratezza della logica di validazione dei parametri in input.
- Aspetti facilitanti: mancanza di funzionalità di filtraggio dell'output ritornato dopo l'esecuzione del comando di sistema.
- Contromisure: gli attacchi di questo tipo possono essere neutralizzati eliminando dai parametri in input token riservati e metacaratteri potenzialmente pericolosi che potrebbero generare ambiguità per l'interprete dei comandi.

3.2.6. Cookie poisoning

- Obiettivo: gli obiettivi possono essere molteplici; essi dipendono dalla logica dell'applicazione attaccata. In generale, le tecniche di cookie poisoning mirano a provocare comportamenti non previsti nell'applicazione attaccata in modo da poter interagire con essa in modi non previsti dal programmatore.
- Attaccanti: gli attacchi di cookie poisoning possono provenire da qualsiasi utente sul cui browser l'applicazione setta cookie.
- Descrizione: le tecniche di cookie poisoning consistono nella modifica dei dati contenuti nei cookie inviati dall'applicazione all'utente, allo scopo di produrre errori e/o portare l'applicazione in stati non correttamente gestiti quando i cookie sono restituiti al server. Per essere in grado di apportare le modifiche opportune, l'attaccante deve conoscere la logica con cui i dati contenuti nei cookie sono processati dall'applicazione.
- Probabilità di successo: dipendenti dal livello di conoscenza da parte dell'attaccante della logica di elaborazione dei dati contenuti nei cookie.
- Aspetti facilitanti: la memorizzazione nei cookie di parametri critici dal punto di vista della sicurezza è un errore comune, che rende pericolosi gli attacchi di cookie poisoning.
- Contromisure: limitare l'uso dei cookie alla memorizzazione di informazioni non critiche; nel caso questo non sia possibile, devono essere utilizzate tecniche (ad esempio crittografia) per impedire la modifica dei cookie.

3.2.7. Forceful browsing

- Obiettivo: accesso non autorizzato a pagine e/o funzionalità dell'applicazione.
- Attaccanti: chiunque non sia in possesso di credenziali per accedere a tali pagine/funzionalità.
- Descrizione: gli attacchi di forceful browsing consistono semplicemente nella sottomissione di richieste HTTP per URL corrispondenti a pagine protette, senza seguire il percorso di navigazione previsto dal programmatore e, in particolare, aggirando le pagine di autenticazione.
- Probabilità di successo: dipendenti dal livello di conoscenza da parte dell'attaccante della struttura dell'applicativo. Tale livello può essere molto elevato per ex utenti che sono stati disabilitati.
- Aspetti facilitanti: messaggi di errore non propriamente gestiti dall'applicazione possono contenere informazioni sulla struttura delle directory dell'applicazione sul web server e semplificare la costruzione degli URL da utilizzare per compiere l'attacco.
- Contromisure: implementare una logica di controllo dello stato della sessione che impedisca l'accesso ad ogni parte dell'applicazione ad utenti non associati a sessioni autenticate.

3.2.8. Information leaking

- Obiettivo: ottenere informazioni sul sistema da attaccare.
- Attaccanti: chiunque possa navigare il sito.
- Descrizione: vengono esaminati i sorgenti HTML delle pagine web ritornate dall'applicazione, allo scopo di individuare informazioni sensibili, come
  - password cablate nel codice;
  - commenti erroneamente lasciati dagli sviluppatori;
  - informazioni su versioni del software utilizzato e configurazione.
- Probabilità di successo: dipendenti dal livello di security-awareness degli sviluppatori.
- Aspetti facilitanti: nessuno.
- Contromisure: eliminare dati sensibili dal codice HTML delle pagine web ritornate dall'applicazione.

3.2.9. Precisazioni

Nel caso in cui il test avvenga su ambienti in produzione occorre utilizzare, ove possibile, un account di test creato appositamente per la scansione.

- Per tale account devono valere le seguenti condizioni:

- Accesso esclusivamente riservato a record di test nei database di back-end.
- Ordini di acquisto o altre tipologie di transazioni dovrebbero essere ignorati.
- Eventuali nuovi record creati da tale account devono essere successivamente cancellati.
- Qualora le transazioni abbiano un qualche tipo di impatto (per esempio in caso di acquisto/vendita di azioni), il loro effetto dovrebbe riguardare esclusivamente dei record di test.

- Qualora l'applicazione preveda diversi livelli di privilegio, è consigliabile effettuare un'analisi con un numero di credenziali di test pari al numero dei profili esistenti e previsti.
- E' consigliabile preventivare e tenere in considerazione il tempo necessario allo sviluppo di script/procedure di clean-up per ripulire tutti i dati creati/modificati dall'utente di test.
- E' utile identificare e comunicare eventuali script o parametri che invalidino le sessioni al fine di evitare che durante le scansioni tali script o parametri vengano eseguiti dai tool di test automatizzati.
- Unitamente alla documentazione dell'analisi verrà rilasciato l'elenco delle URL sottoposte a scansione.

3.3. Criticità di un assessment

3.3.1. Denial of service

Il processo di eliminazione dei falsi positivi, dovuti ai *check* euristici effettuati dai sistemi di *vulnerability assessment* automatico, può richiedere il tentativo diretto di *exploiting* di un servizio, al fine di verificare l'effettiva presenza di una vulnerabilità, la possibilità di sfruttarla per prendere il controllo di un servizio, il suo impatto sulla sicurezza dei sistemi e dei dati in essi contenuti. Tuttavia, non tutte le classi di vulnerabilità richiedono l'utilizzo di *exploit* che possono compromettere la stabilità di un servizio o dell'intero sistema. Tipicamente, le vulnerabilità il cui tentativo di utilizzo può risultare in un D.o.S. sono quelle legate a problemi di *boundary check* e *integer overflow* (*stack/heap overflow*), *memory allocation*, *format string bug*, etc., il cui sfruttamento richiede la sovrascrittura di zone di memoria del processo contenenti strutture dati, indirizzi di ritorno, etc.

3.3.2. Perdita o inconsistenza di dati

Alcune classi di attacco applicativo (es: *SQL Injection*, *Cross Site Scripting*, etc.) prevedono l'accesso non convenzionale o la manipolazione di dati persistenti, tipicamente immagazzinati in un database relazionale. In alcuni casi, l'eliminazione dei falsi positivi (vedi punto precedente), o addirittura la semplice rilevazione della vulnerabilità, richiede la modifica permanente dei dati persistenti. Ad

esempio, per verificare la possibilità di cancellare una tabella da un database SQL, sfruttando dei permessi d'accesso poco restrittivi o una mancata validazione degli input, è richiesta l'effettiva cancellazione della tabella stessa. In altri casi, come ad esempio nelle vulnerabilità di tipo *Database Cross Site Scripting*, è richiesto l'inserimento di particolari *entries* malformate all'interno dei database utilizzati da un applicazione web-based. Questo potrebbe portare ad inconsistenze nel caso tali dati venissero utilizzati da un sistema di reportistica o *data-mining*.

3.3.3. File e processi zombie

Durante una simulazione d'attacco completa, alcuni tipi di approccio richiedono l'upload sulla macchina target di particolari tools (*netcat, pwdump,* etc.) o l'esecuzione di particolari processi, per permettere all'attaccante "simulato" di ottenere un pieno accesso alla macchina, per effettuare la cattura di dati sensibili o eliminare i log in maniera automatizzata, per elevare i propri privilegi, etc. In casi molto particolari non è possibile eliminare i file creati sulla macchina o i processi lanciati, senza un intervento diretto sul sistema da parte di un operatore.

3.4. Metodologia in caso di vincoli o divieti

Qualora i rischi connessi a particolari fasi dell'*assessment*[3] (eliminazione falsi positivi, simulazione d'attacco, etc.) non siano accettabili per il Cliente, è possibile ottenere i medesimi risultati utilizzando i seguenti tipi di approccio, unicamente a prezzo di una maggiore richiesta in termini di tempo:

- **Utilizzo sistemi di test:** E' possibile eliminare il rischio di potenziali disservizi causati dalle fasi di analisi più invasive (ad esempio i *Denial of Service* dovuti a tentativi di *exploiting* falliti), effettuando tali fasi sui sistemi di test. Questo tipo di attività deve essere preceduta da una verifica accurata dell'allineamento fra gli ambienti di test e di produzione. Nel caso non sia presente un ambiente di test, è possibile applicare delle procedure per ottenere una replica esatta dell'ambiente di produzione senza comprometterne l'operatività.
- **Verifica manuale:** Nell'eliminazione dei falsi positivi, in alternativa al tentativo diretto di *exploiting*, è possibile utilizzare un approccio di verifica manuale delle singole vulnerabilità rilevate dai prodotti di *assessment* automatico. Tale tipo di approccio prevede la verifica di presenza, e l'eventuale applicazione, di tutte gli aggiornamenti, *patch*, *best practice*, che possano eliminare o mitigare il problema riscontrato. Questa procedura, che deve essere comunque seguita per tutte

[3] Le fasi più rischiose ed invasive di un assessment sono svolte unicamente qualora il Cliente richieda una particolare accuratezza nei risultati e nella valutazione degli scenari d'attacco e degli impatti. I rischi connessi ad *vulnerability assessment* "generico" sono in genere talmente bassi da essere accettabili per qualsiasi sistema che non sia considerato particolarmente critico.

le vulnerabilità che risultano effettivamente utilizzabili a scopi maliziosi, in questo caso deve essere applicata a tutte le criticità rilevate dai software di *scanning*.

- **Attacco manuale:** Negli attacchi di tipo applicativo è possibile eliminare o minimizzare il rischio connesso alla manipolazione dei dati persistenti non utilizzando software di analisi automatica. Le parti dell'applicazione che accedono a dati critici possono essere verificate manualmente eliminando il rischio di perdite accidentali, e permettendo l'immediato ripristino dei dati per cui è richiesta una manipolazione.

3.5. Tools utilizzati

Si elencano di seguito i tools che potrebbero essere utilizzati durante le attività. Si fa presente che il ruolo fondamentale in un'attività di assessment di qualsiasi tipo è dato dall'esperienza e dalla conoscenza di chi lo porta a termine; non è lo strumento che si utilizza che fa la differenza. Tant'è vero che abitualmente i tools automatici ricoprono solo una piccola parte (discovery e scanning) che è minimale rispetto al totale delle attività da intraprendere in un assessment professionale e di qualità.

3.6. Tools per l'assessment applicativo

I principali tools in questo ambito sono gli scanner applicativi: si tratta di tools che eseguono in modo automatico la navigazione (crawling) delle pagine web dell'applicazione target, riducendo significativamente il tempo necessario a ricostruirne la struttura completa. Tali scanner eseguono inoltre una serie di test finalizzati ad evidenziare l'eventuale vulnerabilità dell'applicazione ad una serie di attacchi comuni.

In alternativa esistono anche

- Web proxy: sono tool di intercettazione del traffico fra browser e server applicativo, che permettono di analizzare e modificare header e body di ogni singola richiesta/risposta HTTP.
- Decompilatori ed analizzatori di codice: per un'analisi approfondita dei binari che compongono la parte client-side dell'applicazione, vengono utilizzati dei software in grado di risalire a porzioni del codice sorgente originale, ed altri strumenti in grado di rilevare tracce di programmazione insicura.

Alcuni tra i tools utilizzati solitamente in questo ambito sono i seguenti:

- Domino Scan II - software vulnerability assessment per Lotus Domino
- NgsSquirrel - software vulnerability assessment per database (Oracle, DB2, SQL Server)
- WebInspect - WEB application assessment tool
- AppScan - WEB application assessment tool
- Paros - WEB Proxy
- Nikto - WEB Server assessment tool
- OraScan - Oracle WEB Application auditing

4. DOCUMENTAZIONE UTENTE

Oltre a quanto specificatamente richiesto nel capitolo 1 (RICHIESTA DEL CLIENTE), al termine dell'attività sarà fornito un report che conterrà:

a. **Topologia rilevata**
b. **Dettagliata descrizione del metodo e degli strumenti**
c. **L'elenco dei sistemi/apparati acceduti in modo non autorizzato**
d. **Descrizione della catena di eventi che hanno portato all'accesso della rete/sistema/applicazione**
e. **Log degli eventi**
f. **Eventuali esempi delle informazioni ottenute**

Sarà inoltre allegata una descrizione dei possibili miglioramenti che potrebbero essere applicati alla rete, ai sistemi o ai servizi, unita all'elenco, supra-vendor, delle soluzioni tecnologiche e/o dei prodotti da adottare per incrementare il livello di security del sistema informativo.

5. DOCUMENTI NECESSARI

Per dare inizio alle attività sarà necessaria la sottoscrizione dei due allegati:

- Allegato A: Accordo Legale (Liberatoria)
- Allegato B: Accordo di Non Divulgazione

6. RESPONSABILITÀ

Sarà responsabilità di HT completare il presente progetto secondo quanto specificato nella definizione delle funzionalità iniziali, fornendo al Cliente la documentazione citata.

Sarà responsabilità del Cliente garantire l'accesso ai locali preposti, nonché la disponibilità di una persona durante le attività previste dal presente progetto.

La presenza di tale persona permetterà a HT di spiegare nel modo più rapido ed efficace le attività svolte, sia in termini di tecniche che di strumenti.

7. OFFERTA ECONOMICA

Le quotazioni di seguito riportate sono a corpo. Nella colonna di destra vengono riportate delle stime di durata in gg.

Servizi	Descrizione	Costo €	gg
Ethical Hacking	**Simulazione utente standard**	**2.000,00**	**4**
Ethical Hacking	**Simulazione consulente**	**2.000,00**	**4**
Ethical Hacking	**VA interno 250 server, inglese manuale**	**7.000,00**	**20**
Ethical Hacking	**Verifica WIFI**	**1.000,00**	**2**
Ethical Hacking	**Verifica BlackBerry**	**2.000,00**	**4**
Totale		**14.000,00**	

N.B:

Il supporto richiesto da parte del cliente si limita al fornire la postazione di lavoro (PC e Black Berry), ad assegnare la collocazione negli uffici per l'esecuzione delle attività, al comunicare gli indirizzi IP da testare.

8. CONDIZIONI GENERALI DI OFFERTA

Modalità di pagamento e condizioni generali di fornitura

Validità offerta	30 gg
Fatturazione servizi	100% all'ordine.
Liquidazione fatture	60 gg D.F.
Trasporti/Trasferta	Ns.carico
Garanzia	A norma di legge

Tutti i prezzi esposti nella presente offerta sono da intendersi IVA esclusa.

Allegato 2
CODICE ETICO
Modello di organizzazione e gestione ex decreto legislativo 8 giugno 2001 n. 231

INDICE

1. PREMESSA

Il presente Codice Etico esprime l'insieme degli impegni di TNT Global Express SpA nei confronti dei suoi Stakeholder; esso contiene norme di comportamento mediante le quali si dà attuazione ai principi che arricchiscono i processi decisionali aziendali e ne orientano i comportamenti.
Esso costituisce parte integrante del Modello di Organizzazione e Gestione disciplinato dal D. Lgs. 231/01 (di seguito Decreto) e viene adottato mediante delibera del Consiglio di Amministrazione.
Il Codice Etico costituisce elemento di riferimento per i Destinatari, come successivamente individuati e abbraccia in modo ampio il ruolo ed i rapporti di TNT Global Express SpA con i propri Stakeholders (ovvero quei soggetti, intesi nel senso di individui, gruppi, organizzazioni, che hanno con l'azienda relazioni significative dalle quali derivano specifici o generici interessi legittimi).

2. MISSION

TNT Global Express SpA esprime la propria Mission secondo quanto definito dalla propria Capogruppo come segue:

- andare oltre le aspettative dei Clienti nel trasporto delle loro merci e nella consegna dei loro documenti in tutto il mondo;
- creare valore per i Clienti offrendo loro le più affidabili ed efficienti soluzioni per la distribuzione e per la gestione dei network;
- cercare di primeggiare nel settore infondendo orgoglio nei propri dipendenti e collaboratori, creando valore per i nostri partner commerciali e operativi e impegnandoci in maniera responsabile per un mondo migliore.

La seguente formulazione, definita a livello internazionale, ma fatta propria esplicitamente da TNT Global Express SpA in Italia mediante il richiamo nel presente Codice Etico, delinea le regole fondamentali attraverso le quali la Società persegue la propria Mission:

- Essere onesti, sempre;
- Mirare sempre alla soddisfazione dei clienti;
- Accettare le sfide e migliorare continuamente in tutto ciò che facciamo;
- Mostrare passione nei confronti dei nostri collaboratori;
- Agire come una squadra;
- Misurare il successo attraverso profitti sostenibili;
- Lavorare per il pianeta.

Attraverso la "Mission", TNT Global Express SpA esplicita lo scopo, il fine comune perseguito dagli individui e dai soggetti che in essa operano e con essa collaborano intrattenendo relazioni esterne.
Nel perseguimento della propria Mission TNT Global Express SpA considera le aspettative legittime dei propri stakeholder che sono individuati nelle seguenti categorie:

- Il Socio;
- le Risorse Umane (dipendenti e collaboratori);
- i Clienti;
- i Fornitori e Partner commerciali;
- la Pubblica Amministrazione (enti pubblici, autorità di vigilanza, ecc);
- la Collettività.

TNT Global Express SpA aspira a mantenere e sviluppare il rapporto di fiducia con i propri stakeholder e persegue la propria Mission ricercando il contemperamento degli interessi legittimi coinvolti.

3. AMBITO DI APPLICAZIONE DEL CODICE ETICO E SANZIONI

Il presente Codice Etico si applica a TNT Global Express SpA e destinatari del Codice Etico sono pertanto il Socio, gli Amministratori, i Dipendenti e i Collaboratori della Società, nonché tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, instaurano e intrattengono rapporti o relazioni con essa (di seguito anche i "Destinatari").
Il Codice Etico costituisce parte integrante del Modello organizzativo di TNT Global Express SpA ai sensi del Decreto e, pertanto TNT Global Express SpA s'impegna alla sua diffusione presso tutti i soggetti interessati, alla corretta interpretazione dei suoi contenuti ed alla messa a disposizione di strumenti che ne favoriscano l'applicazione e l'attuazione, prendendo altresì le necessarie misure al fine di svolgere attività di verifica e monitoraggio dell'applicazione del Codice Etico stesso, prevedendo sanzioni in caso di sua violazione.
I Destinatari hanno pertanto l'obbligo di conoscerne le norme, di astenersi da comportamenti ad esse contrari, di rivolgersi ad un superiore o all'Organismo di Vigilanza per chiarimenti segnalando eventuali violazioni da parte del Socio, Dipendenti, Collaboratori o Terzi, di collaborare con le strutture deputate a verificare le violazioni ed informare le controparti dell'esistenza del presente Codice Etico.

L'osservanza delle disposizioni del Codice Etico è parte essenziale delle obbligazioni contrattuali di tutti i dipendenti ai sensi dell'art. 2104 del Codice Civile. In particolare, al fine di garantire il rispetto delle norme e dei principi espressi, nonché di verificare il funzionamento e l'efficacia del Modello ex D. Lgs. 231/01 adottato da TNT Global Express SpA per la prevenzione dei reati prevista da tali norme, è istituito un Organismo di Vigilanza per svolgere un'efficace attività di verifica e monitoraggio dell'applicazione del Modello stesso nonché un sistema sanzionatorio (delineato in apposito documento) che prevede e disciplina le ipotesi di commissione di illeciti e prevede l'irrogazione di idonee sanzioni su proposta del ricordato Organismo di Vigilanza.
Ogni dipendente che violi il Codice Etico, nel rispetto delle normative vigenti, sarà sottoposto a sanzione disciplinare, alla revoca di poteri e funzioni, al deferimento alle autorità amministrative o giudiziarie ordinarie.
In ogni rapporto d'affari, tutte le controparti devono essere informate dell'esistenza di principi etici contenuti nel Codice e devono rispettarli, pena le conseguenze stabilite dal contratto.

4. PRINCIPI GUIDA

I principi guida di TNT Global Express SpA sono:

1. Rispettiamo tutte le politiche previste per legge e di natura aziendale.
2. Forniamo una visione completa, equa, accurata e puntuale nel nostro reporting.
3. Privilegiamo una comunicazione aperta e trasparente sulle nostre attività sempre nel rispetto della riservatezza.
4. Non siamo coinvolti in alcuna questione legata ai partiti politici.
5. Garantiamo condizioni di lavoro tali da tutelare la sicurezza e la salute dei nostri dipendenti.
6. Creiamo pari opportunità per tutti i dipendenti.
7. Non è consentita alcuna discriminazione per motivi di età, invalidità, etnia, sesso, stato civile, razza, religione o orientamento sessuale.
8. Tutte le persone devono essere trattate in modo imparziale, con considerazione e rispetto.
9. Evitiamo i conflitti d'interesse.
10. Non facciamo uso dei beni aziendali per trarne un vantaggio personale non autorizzato.
11. Non cerchiamo, forniamo o accettiamo vantaggi personali impropri.
12. Non cerchiamo, versiamo o accettiamo tangenti.
13. Ci impegniamo a fornire le soluzioni più affidabili ed efficienti per i nostri Clienti.
14. Tuteliamo i beni e le informazioni affidateci.
15. Le pratiche dubbie sul piano etico non rientrano tra le strategie adottate per accrescere il nostro vantaggio.
16. Le decisioni su eventuali operazioni economiche o collaborazioni sono adottate basandoci sui nostri principi aziendali.

17. Tra gli oggetti della nostra attività figura l'appoggio e l'impegno volti a implementare ogni progresso a vantaggio della sostenibilità ambientale e sociale.

E' peraltro indispensabile che tali principi non rimangano meri enunciati ma vengano tradotti in condotte e comportamenti immanenti alla Società. Come organizzazione e come individui, tutti i Dipendenti e i Collaboratori sono tenuti a vivere, nell'ambiente di lavoro, secondo questi principi e ad applicarli in modo corretto, eticamente ed onorevolmente.

5. I PRINCIPI GUIDA IN DETTAGLIO

Quanto sinteticamente esposto nel paragrafo precedente, viene così delineato:

5.1 Principi etici aziendali TNT

Siamo impegnati a promuovere una condotta aziendale impeccabile: la gestione delle nostre attività si basa pertanto sui nostri standard e sui Principi etici aziendali TNT.

Aderiamo inoltre ai principi del programma Global Compact delle Nazioni Unite su diritti umani, standard occupazionali, ambiente e sistemi anticorruzione.

5.2 Normative di legge e internazionali

Operiamo nel rispetto di leggi, norme e regolamenti vigenti nei Paesi in cui siamo dislocati.

5.3 Rendicontazione pubblica e comunicazione

In conformità alle leggi in materia e ai principi e agli standard contabili generalmente accettati, i nostri bilanci, i documenti di public reporting e qualsiasi altra comunicazione pubblica costituiscono una presentazione completa, equa, accurata, puntuale e chiara della posizione di TNT.
Ci atteniamo alle leggi e alle regole di contabilità in vigore, ai disposti normativi in materia di reportistica finanziaria e marcati dei titoli in cui TNT è quotata.
Le nostre comunicazioni ai clienti, ai dipendenti, agli azionisti e alla collettività sono improntati all'apertura e alla trasparenza, senza però trascurare gli obblighi di riservatezza.

5.4 Attività pubbliche

Non interveniamo in questioni legate ai partiti politici né destiniamo agli stessi contributi di varia natura.
Come società, relativamente al business condotto, esprimiamo la propria opinione su questioni sociali, ambientali, normative o di altro genere che possono avere un impatto per TNT a livello di azionisti, clienti e dipendenti nonché per la collettività.

5.5 Sicurezza

Garantiamo condizioni di lavoro tali da tutelare la sicurezza e la salute di tutti i nostri dipendenti.
A tal fine ci atteniamo alle leggi e alle normative sulla sicurezza e attuiamo politiche atte a prevenire, individuare e eliminare i rischi per tutta la nostra società e le attività condotte. In ciascuna delle sedi in cui operiamo sono presenti rappresentanti per la sicurezza e gruppi di controllo.
Ci sforziamo di adottare procedure ottimali e di superare i requisiti imposti dalla legislazione relativa alla sicurezza, e monitoriamo costantemente le nostre performance in questo contesto.

5.6 Dipendenti

È nel nostro interesse cercare di attrarre, far crescere, premiare e continuare a collaborare con individui con ottime capacità che riconoscono il valore del lavoro di squadra.
Ci preoccupiamo di creare pari opportunità per tutti i nostri dipendenti senza discriminazioni per motivi di età, invalidità, etnia, sesso, stato civile, razza, religione o orientamento sessuale.
Non giustifichiamo alcun tipo di trattamento non equo, perché riteniamo che tutte le persone meritano considerazione e rispetto.
Abbiamo adottato lo standard Investors in People.

5.7 Condotta individuale

Conflitti di interesse
L'onestà rappresenta il principio fondamentale per tutte le attività di TNT, le sue iniziative,
le sue relazioni e le sue comunicazioni e costituisce elemento essenziale della gestione aziendale.

TNT, in coerenza con i valori di onestà e trasparenza, si impegna a mettere in atto tutte le misure necessarie a prevenire ed evitare fenomeni di conflitto di interessi.
Questo vale sia nel caso in cui un Destinatario persegua un interesse diverso dalla Mission della Società o si avvantaggi personalmente di opportunità d'affari della Società, sia nel caso in cui i rappresentanti dei Clienti o dei Fornitori, o delle Istituzioni Pubbliche, agiscano in contrasto con i doveri fiduciari legati alla loro posizione.

Beni aziendali
Non è ammesso alcun uso improprio da parte dei dipendenti dei beni aziendali per conseguire vantaggi non autorizzati. TNT non tollera frodi, furti, perdite per negligenza o sprechi a scapito di tali beni.

Omaggi e intrattenimenti
I Dipendenti non possono trarre vantaggi personali impropri per loro stessi e le rispettive famiglie derivanti dal loro rapporto con TNT. Non è consentito, inoltre, accettare omaggi o intrattenimenti che potrebbero dare vita a un qualsiasi obbligo.

Tangenti
Ai dipendenti e agli agenti è proibito pagare o accettare tangenti per ottenere o ricambiare ordini, servizi o benefici, anche di tipo finanziario. Dipendenti e agenti sono anche tenuti a respingere e segnalare immediatamente qualsiasi occasione di richiesta o offerta di tangenti.

Pagamenti facilitati
In determinate circostanze, piccole somme in contanti o omaggi di scarso valore risultano indicati qualora sia consuetudine o necessario per accelerare o garantire l'esecuzione di ordinarie procedure statali e qualora sia consentito nella giurisdizione dei Paesi di attività. In tutti gli altri casi, è preferibile evitare qualsiasi forma di cosiddetto pagamento facilitato. Prima di ricorrere a tali pagamenti, occorre consultare il Comitato etico (OdV)che agisce per conto del Consiglio di Amministrazione di TNT. È previsto che si registrino e si documentino in maniera corretta e accurata tutti i pagamenti di questo genere.

5.8 Clienti
TNT si impegna a offrire ai Clienti le soluzioni più affidabili e efficienti nel trasporto di prodotti e documenti, tutelando i beni e le informazioni affidate da tutti gli utenti.

5.9 Concorrenza
TNT è sostenitrice di un modello di concorrenza aperta e leale.
Le pratiche dubbie sul piano etico non rientrano tra le strategie adottate per accrescere il proprio vantaggio.
TNT non utilizza informazioni acquisite da attività illegali a scapito dei competitori o di altri attori sul mercato.

5.10 Consociate e agenti commerciali
Le decisioni su eventuali operazioni economiche o collaborazioni sono adottate basandoci sui Principi etici aziendali. Dalle nostre consociate esigiamo che aderiscano quanto più possibile ai Principi TNT, mentre dagli agenti - che si tratti di persone fisiche o giuridiche - ci aspettiamo la completa conformità.

5.11 Responsabilità sociale
Nello svolgimento della propria attività TNT ricorre a risorse che hanno un impatto sulla società e sull'ambiente. Gli sforzi sono volti a sostenere e implementare ogni progresso a vantaggio della sostenibilità ambientale e sociale.
TNT sostiene un uso attento delle risorse limitate. La gestione del rischio ambientale rientra nella formazione delle decisioni. Vengono stilate ed esaminate delle relazioni sull'andamento della responsabilità sociale.
TNT investe nella collettività in qualsiasi parte del mondo intervenendo con le proprie risorse nelle aree collegate alle nostre attività. Con l'investimento sociale messo così in atto si mira a promuovere il risultato migliore per i propri partner commerciali e operativi, gli stakeholder e le proprie operazioni.

5.12 Rapporto con i media
Coerentemente con i principi di trasparenza e completezza dell'informazione, la comunicazione di TNT verso l'esterno è improntata al rispetto del diritto all'informazione. In nessun caso gli Amministratori, il Socio, i

Dipendenti e i Collaboratori si prestano a divulgare notizie o commenti falsi o tendenziosi, sia riguardanti le attività aziendali che le risultanze delle attività professionali o le relazioni con gli stakeholder in generale.
Nella convinzione che l'attività e i risultati d'impresa debbano essere strettamente legati ad una condotta di business responsabile, la comunicazione esterna, inclusa quella finalizzata alla diffusione del marchio e dell'immagine della Firm, rispetta i limiti di legge previsti per il settore ed i principi etici del contesto professionale di riferimento.

5.13 Trasparenza e completezza dell'informazione

TNT assicura una corretta informazione ai propri Soci e agli organi di controllo interni ed esterni in ordine ai fatti significativi concernenti la propria gestione societaria.
Le evidenze finanziarie, contabili e gestionali ed ogni altra comunicazione che la Società rilascia a terzi rispondono ai requisiti di veridicità, completezza ed accuratezza.
Nello svolgimento della professione, in particolare con riferimento ai rapporti con i clienti, i loro organi di controllo e con quanti, legittimamente, sono destinatari delle relazioni ("report") emesse a fronte di incarichi professionali, TNT assicura, oltre la stretta osservanza di norme, leggi, e regolamenti applicabili, il rigore richiesto dalla professione stessa e il rispetto dei principi deontologici di riferimento.

5.14 Riservatezza delle informazioni

TNT assicura la riservatezza delle informazioni in proprio possesso, eccezion fatta per le comunicazioni richieste per legge, l'osservanza della normativa in materia dei dati personali e si astiene dal ricercare dati riservati attraverso mezzi illegali.
I Destinatari del Codice Etico sono tenuti a non utilizzare informazioni riservate per scopi non connessi con l'esercizio della propria attività professionale, a non utilizzare né diffondere informazioni privilegiate, a non manipolarle né diffonderne di false.

5.15 Trattamento delle informazioni

Tutte le informazioni a disposizione di TNT vengono trattate nel rispetto della riservatezza e della privacy dei soggetti interessati.
A questo proposito, sono definite e mantenute in continuo aggiornamento specifiche procedure per la protezione delle informazioni.
Esiste un'organizzazione interna responsabile del trattamento delle informazioni, che si occupa di gestire ruoli e responsabilità al riguardo e di classificare le informazioni per livelli di criticità.
Inoltre, TNT vieta ai soggetti apicali, al personale dipendente, ai consulenti della Società ed ai terzi che operano in nome e per conto della Società di:

- esporre fatti materiali non rispondenti al vero;
- omettere informazioni la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale o finanziaria della Società;
- occultare dati o notizie in modo idoneo a indurre in errore i destinatari degli stessi;
- impedire o comunque ostacolare lo svolgimento delle attività di controllo legalmente attribuite ai Soci agli altri organi sociali o alle autorità di vigilanza competenti.

Per quanto attiene all'utilizzo e tutela delle informazioni dei propri clienti, la deontologia professionale obbliga i Soci, dipendenti e collaboratori della Società a tutelare la riservatezza di tali informazioni sia durante gli incarichi sia successivamente alla loro conclusione eccezion fatta per le comunicazioni richieste per legge.

5.16 Prevenzione del Rischio Terrorismo

TNT rifiuta ogni forma di illegalità con particolare riferimento allo svolgimento delle attività connesse al finanziamento del terrorismo, come previsto dal D. Lgs. 109/2007.
Quanto sopra specificato viene attuato prestando particolare attenzione alla gestione dei flussi finanziari, garantendo la trasparenza degli stessi all'interno della Società. Viene altresì concretizzato tramite l'assunzione di personale interno, qualificato e non qualificato, il cui status escluda ogni tipo di coinvolgimento in fatti di finanziamento del terrorismo. Viene infine realizzato tramite la selezione di fornitori e clienti la cui condotta sia idonea a eliminare ogni sospetto di legami con organizzazioni terroristiche nazionali e internazionali.
Qualora l'OdV riscontri violazione dei principi sopra elencati provvederà a segnalarle con tempestività alla Direzione Risorse Umane, affinchè possa essere attivato il relativo procedimento disciplinare.

5.17 Rapporti con le Autorità Giudiziarie

I rapporti che TNT, in persona dei suoi legali rappresentanti i cui poteri sono conferiti mediante delega del Consiglio di Amministrazione o procura speciale ad hoc, intrattiene con le Autorità Giudiziarie, nonché le deposizioni degli stakeholder afferenti a questioni riguardanti la Società, sono improntati al rispetto della veridicità delle informazioni rese nelle testimonianze.

5.18 Applicazione dei principi

I Principi guida aziendali di TNT sono validi per le società e le joint venture controllate da TNT e per i dipendenti di TNT. TNT si aspetta dai propri agenti il rispetto di tali Principi.
Il Consiglio di Amministrazione di TNT è incaricato di adottare, comunicare e attuare i Principi etici aziendali, nonché di monitorarne il rispetto, affiancato in questo compito dalle funzioni dell'internal audit, dell'integrità aziendale, della gestione del rischio e della sicurezza.
Le eventuali modifiche apportate ai principi o una rinuncia alle disposizioni sono di competenza esclusiva del Consiglio di Amministrazione di TNT previa approvazione del Collegio sindacale. Le modifiche saranno pubblicate tempestivamente sul sito http://group.tnt.com.
Qualsiasi perdita di attività risultante dall'adesione a tali principi non sarà criticata, né alcun dipendente subirà conseguenze negative per aver fatto presente o per avere intrapreso una qualsiasi azione legale rispetto a una violazione, anche solo sospetta.

6 SOCI

Uno degli obiettivi della Società è la valorizzazione dell'investimento dei propri azionisti, mediante il perseguimento di una politica di sviluppo e gestione dei rischi in grado di garantire nel tempo soddisfacenti risultati economici.
TNT si impegna a creare le condizioni affinché la partecipazione del Socio alle decisioni di
loro competenza sia diffusa e consapevole, promuove la parità e la completezza di informazione e tutela il loro interesse.

7. RISORSE UMANE

TNT riconosce la centralità dello stakeholder Risorse Umane (intendendosi per tali sia i
soci che i dipendenti, sia i collaboratori che prestano la loro opera a favore della Società in forme contrattuali diverse da quella del lavoro subordinato) e l'importanza di stabilire e mantenere con questo relazioni basate sulla lealtà e sulla fiducia reciproca

7.1 Selezione del personale e costituzione del rapporto di lavoro

La valutazione del personale da assumere è effettuata in base alla corrispondenza dei profili dei candidati rispetto a quelli attesi ed alle esigenze specifiche della Società, nel rispetto dei principi dell'imparzialità e delle pari opportunità per tutti i soggetti interessati.
Nel momento in cui inizia la collaborazione, il dipendente/collaboratore deve ricevere esaurienti informazioni riguardo alle caratteristiche delle mansioni e della funzione, agli elementi normativi e retributivi ed alle normative e comportamenti per la gestione dei rischi connessi alla salute personale. Tutto il personale deve essere assunto con regolare contratto di lavoro secondo quanto previsto dagli obblighi di legge.

7.2 Tutela della privacy

La privacy dei dipendenti, dei collaboratori è tutelata nel rispetto della normativa di riferimento, anche attraverso standard operativi che specificano le informazioni ricevute e le relative modalità di trattamento e di conservazione. E' esclusa ogni indagine sulle idee, le preferenze, i gusti personali e la vita privata delle persone.

8. CLIENTI

I Clienti costituiscono un asset fondamentale per TNT, che persegue la propria mission
attraverso l'offerta di servizi professionali di alta qualità.
Lo stile di comportamento nei confronti dei clienti è improntato all'integrità, oggettività,
competenza e al rispetto, nell'ottica di un rapporto di elevata professionalità.
I Clienti sono informati dell'esistenza del Codice Etico e dei relativi impegni e, a tale fine, nei singoli contratti sono previste apposite clausole.

9. FORNITORI E COLLABORATORI ESTERNI

Le relazioni con i fornitori e i partner commerciali sono improntate alla ricerca di un giusto vantaggio competitivo, alla concessione delle pari opportunità per i soggetti coinvolti, alla lealtà, all'imparzialità e al riconoscimento della professionalità e competenza dell'interlocutore.
TNT si impegna a richiedere ai propri fornitori e ai propri collaboratori esterni il rispetto di principi comportamentali corrispondenti ai propri, ritenendo questo aspetto di fondamentale importanza per la nascita o la continuazione di un rapporto d'affari. I fornitori e collaboratori esterni sono informati dell'esistenza del Codice Etico e dei relativi impegni e, a tale fine, nei singoli contratti sono previste apposite clausole.

10. PUBBLICA AMMINISTRAZIONE (ENTI PUBBLICI, AUTORITA' DI VIGILANZA, ALTRI ORGANISMI DI CONTROLLO)

I rapporti tra la Società e le Istituzioni Pubbliche sono improntate ai principi di correttezza, trasparenza e collaborazione. Viene rifiutata qualsiasi tipologia di comportamento che possa ricondursi a una natura collusiva o idonea a pregiudicare i principi espressi nel presente Codice.

10.1 Principi di comportamento nei rapporti con la Pubblica Amministrazione

L'assunzione di impegni con le Pubbliche Amministrazioni e le Istituzioni Pubbliche è riservata a personale specifico, secondo le procure conferite, salvo procure speciali eventualmente conferite ad altre risorse interne.
TNT Global Express SpA ricusa ogni comportamento che possa essere interpretato come promessa o offerta di pagamenti, beni o altra utilità di vario genere al fine di promuovere e favorire i propri interessi e trarne vantaggio. E' impegno di TNT Global Express SpA evitare qualsiasi forma di regalo a funzionari pubblici o incaricati di pubblico servizio, di ogni tipo, italiani od esteri, o a loro familiari, anche attraverso interposta persona, tali da potere influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio a se stessa. Omaggi o regalie sono consentiti solo se di valore modesto e, comunque, se non possano essere in alcun modo interpretati come strumento per ricevere favori illegittimi, e sempre nel rispetto delle procedure interne a ciò preordinate.
Qualsiasi dipendente che riceva direttamente o indirettamente proposte di benefici da pubblici funzionari, incaricati di pubblico servizio o dipendenti in genere della Pubblica Amministrazione o di altre Pubbliche Istituzioni che configurino simile fattispecie, deve immediatamente riferire all'organismo interno preposto alla vigilanza sull'applicazione del Codice Etico.

10.2 Comunicazione con Istituzioni Pubbliche

Ogni rapporto con le istituzioni dello Stato o internazionali è riconducibile esclusivamente a forme di comunicazione volte a esplicitare l'attività di TNT Global Express SpA, a rispondere a richieste o ad atti di sindacato ispettivo (interrogazioni, interpellanze, richieste di informazioni collegate ad incarichi professionali in corso o conclusi, ecc), o comunque a rendere nota la posizione di TNT Global Express SpA su temi rilevanti.
A tal fine la Società è impegnata a;

- operare, senza alcun tipo di discriminazione, attraverso i canali di comunicazione a ciò preposti con gli interlocutori Istituzionali a livello nazionale e internazionale, comunitario e territoriale;
- rappresentare i propri interessi e posizioni in maniera trasparente, rigorosa e coerente, evitando atteggiamenti di natura collusiva;
- evitare falsificazioni e/o alterazioni di dati, rendiconti, relazioni al fine di ottenere un indebito vantaggio o qualsiasi altro beneficio per la Società.

10.3 Rapporti con organizzazioni e partiti politici

E' impegno della Società non erogare contributi, diretti o indiretti e sotto qualsiasi forma, a partiti, movimenti, comitati e organizzazioni politiche e sindacali, a loro rappresentanti e candidati, tranne quelli dovuti in base a normative specifiche, salvo che tali finanziamenti, non vietati dalla legge e dallo Statuto, siano stati deliberati dall'organo sociale competente e regolarmente iscritti in bilancio.

10.4 Rapporti con le realtà no-profit e iniziative sociali

TNT Global Express SpA si impegna in iniziative finalizzate al sociale coerenti con la propria attività e, di conseguenza, sostenibili nel tempo.

10.5 Rapporti con le Authority

TNT Global Express SpA dà piena e scrupolosa osservanza alle regole emesse dalle Authority regolatrici del mercato e non nega, nasconde o ritarda alcuna informazione richiesta da tali autorità e dagli altri organi di regolazione nelle loro funzioni ispettive.
Per garantire la massima trasparenza, TNT Global Express SpA ed i propri dipendenti si impegnano a non trovarsi in situazioni di conflitto di interessi con dipendenti di qualsiasi Authority e loro familiari.

11. MODALITA' DI ATTUAZIONE DEL CODICE ETICO

Il Socio, gli Amministratori, i Dipendenti o i collaboratori nonché gli Enti che a qualunque titolo svolgono la propria attività a favore di TNT Global Express SpA sono tenuti a conoscere le norme contenute nel Codice Etico e le norme di riferimento che regolano l'attività svolta nell'ambito della sua funzione, derivanti dalla legge o da policy e procedure interne.
Il Socio, gli Amministratori, i Dipendente o i Collaboratori devono altresì accettare in forma esplicita i propri impegni derivanti dal presente Codice Etico, nel momento di costituzione del rapporto di lavoro, di prima diffusione del Codice Etico o di sue eventuali modifiche o integrazioni rilevanti.

In particolare, i dipendenti/collaboratori hanno l'obbligo di:

- astenersi da comportamenti contrari alle norme contenute nel Codice Etico;
- rivolgersi ai propri superiori, referenti aziendali e all'OdV, in caso di richiesta di chiarimenti sulle modalità di applicazione delle stesse;
- riferire tempestivamente all'OdV, qualsiasi notizia, di diretta rilevazione o riportata da altri, in merito a possibili violazioni e qualsiasi richiesta di violarle gli sia stata rivolta; l'OdV dovrà assicurare l'assoluta riservatezza del mittente la comunicazione;
- collaborare con le strutture deputate a verificare le possibili violazioni;
- informare adeguatamente ogni terza parte con la quale vengano in contatto nell'ambito dell'attività lavorativa circa l'esistenza del Codice Etico e gli impegni ed obblighi imposti dallo stesso ai soggetti esterni;
- esigere il rispetto degli obblighi che riguardano direttamente la loro attività;
- adottare le opportune iniziative interne e, se di propria competenza, esterne in caso di mancato adempimento da parte di terzi dell'obbligo di conformarsi alle norme del Codice Etico.

12. ORGANISMO DI VIGILANZA

Viene appositamente costituito presso TNT Global Express SpA un Organismo di Vigilanza la cui composizione, poteri, compiti e responsabilità sono disciplinati nella parte Speciale B del Modello – Organismo di Vigilanza.
In breve, e per quanto di interesse, l'OdV dovrà:

- monitorare l'applicazione del Codice Etico da parte dei soggetti interessati, attraverso l'applicazione di specifici compliance program, e accogliendo eventuali segnalazioni fornite dagli stakeholder interni ed esterni;
- relazionare periodicamente al Consiglio di Amministrazione sui risultati dell'attività svolta, segnalando eventuali violazioni del Codice Etico;
- esprimere pareri in merito alla revisione delle politiche e procedure, allo scopo di garantirne la coerenza con il Codice Etico;
- provvedere, ove necessario, alla proposta di revisione periodica del Codice Etico.

13. COMUNICAZIONE E FORMAZIONE

Il Codice è portato a conoscenza di tutti i soggetti interessati interni ed esterni mediante apposite attività di comunicazione.
Il Codice è pubblicato sul sito www.tnt.it unitamente ad un estratto del Modello di Organizzazione e Gestione. Una copia del Codice Etico, su supporto cartaceo o informatico è distribuita ai Soci, agli Amministratori, ai dipendenti, ed a tutte le terze parti che entrino in rapporti contrattuali con TNT Global Express SpA.
Allo scopo di assicurare la corretta comprensione del Codice Etico, le funzioni Human Resources e Comunicazione & CSR predispongono e realizzano, anche in base alle eventuali indicazioni dell'organismo preposto alla vigilanza per l'applicazione del Codice Etico, un piano periodico di comunicazione/formazione

volto a favorire la conoscenza dei principi e delle norme etiche contenute nel Codice Etico. Le iniziative di formazione devono essere differenziate secondo il ruolo e la responsabilità dei destinatari.

14. VIOLAZIONI DEL CODICE ETICO.

In caso di accertata violazione del Codice Etico – la cui osservanza costituisce parte essenziale delle obbligazioni contrattuali assunte dai dipendenti e/o collaboratori e/o dai soggetti che a qualunque titolo prestano la propria attività a favore della Società - sono adottati, per la tutela degli interessi aziendali e compatibilmente con la normativa applicabile, provvedimenti sanzionatori, che potranno anche determinare la risoluzione del rapporto e il risarcimento dei danni subiti, secondo quanto disposto nella Procedura aziendale inerente le modalità di richiesta e irrogazione delle sanzioni disciplinari.

I soggetti interessati possono segnalare per iscritto, in forma non anonima, ogni violazione o sospetto di violazione del Codice Etico all'OdV, che provvede ad un'analisi della segnalazione, ascoltando eventualmente l'autore e il responsabile della presunta violazione.

L'OdV agisce in modo da garantire i segnalanti contro qualsiasi tipo di ritorsione, intesa come atto che possa dar adito anche al solo sospetto di essere una forma di discriminazione o penalizzazione. È inoltre assicurata la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge.

L'attività dell'OdV a seguito delle segnalazioni ricevute e delle informazioni raccolte è disciplinata nella parte generale del modello organizzativo sub paragrafo – Organismo di Vigilanza.

HT Srl
Via Moscova, 13 - 20121 Milano

Allegato 3
TNT BUSINESS PRINCIPLES

Noi della TNT riteniamo di avere delle responsabilità nei confronti della comunità che serviamo, verso le persone che lavorano per noi ed i mercati sui quali operiamo. Ci assumiamo la responsabilità di svolgere la nostra attività in modo onesto e trasparente, nel rispetto di regole altamente etiche.

I Principi dell'Attività di TNT sottolineano i nostri standard etici e forniscono le linee guida per poter compiere delle scelte responsabili, scelte che eventualmente possono avere un risvolto nei confronti del nostro marchio e della nostra reputazione. I nostri Principi affermano alcune regolamentazioni comportamentali applicabili a TNT e pertanto anche ai propri collaboratori e rappresentanti, per esempio in relazione alla lotta contro la corruzione, la Riunione per la lotta alla corruzione OECD dei Pubblici Ufficiali Stranieri delle Transazioni d'Affari Internazionali, che possono essere applicabili a voi come a TNT.

Per raggiungere il nostro scopo di svolgere l'attività in modo trasparente ed etico, é importante che lo stesso tipo di impegno ispiri e guidi le persone che noi consideriamo i nostri collaboratori.

Conseguentemente, alleghiamo alla presente una copia dei Principi dell'Attività di TNT e ci aspettiamo che vengano seguiti ed applicati nei rapporti ed attività con TNT, e più genericamente nel modo in cui portiamo avanti il business.
E' possibile visionare il documento anche sul nostro sito:
htpp://group.tnt.com/aboutus/ourbusiness/businessprinciples/index.aspx

Nel caso abbiate delle domande, sentitevi pure liberi di contattarci in assenza di risposte da parte della Vostra società, presupponendo che siete d'accordo con la presente lettera ed il contenuto dei suoi allegati.

Con i migliori saluti.

HT Srl
Via Moscova, 13 - 20121 Milano

POLITICA DI RESPONSABILITA' SOCIALE

LA NOSTRA CULTURA

TNT Express Italy S.p.A. fa parte di TNT N.V., azienda globale che interagisce con le comunità di tutto il mondo. Come azienda che persegue un comportamento ambientale e socialmente responsabile, cerchiamo di aiutare le persone a raggiungere il più alto tenore di vita senza impoverire il mondo che trasmetteremo ai nostri figli.
Sappiamo che la qualità del nostro operato a livello locale e nazionale sarà un fattore determinante nel permetterci di operare nel lungo termine.
Siamo perciò impegnati a sviluppare e mantenere politiche e pratiche lavorative che forniscano un contributo ambientale e sociale positivo e sostenibile alle comunità in cui operiamo.

I NOSTRI PRINCIPI

La strategia adottata per raggiungere il miglioramento continuo nell'ambito della responsabilità sociale, si basa sui nostri Principi Aziendali.

REGOLE DI CONDOTTA

Lavoriamo con onestà, integrità e rispetto nell'interesse di quanti sono coinvolti nelle nostre attività (azionisti, dipendenti, fornitori e più in generale la società).

RESPONSABILITA' SOCIALE

Chiediamo ad ogni nostro dipendente di essere un buon cittadino. Di rispettare le leggi e i regolamenti della società in cui lavoriamo.

CONFLITTO DI INTERESSE

Dalle nostre persone ci aspettiamo che evitino interessi personali, familiari e finanziari o interessi di altra natura che possano essere in conflitto con il loro lavoro. Quando richiesto ci impegniamo a supportarli per il rispetto di questo principio.

LE NOSTRE PERSONE

La nostra missione è essere riconosciuti nel mondo come leader nella qualità del servizio al Cliente. Abbiamo persone competenti, capaci ed entusiaste alle quali garantiamo le risorse necessarie affinché riconoscano e realizzino il loro potenziale e diano il loro contributo individuale al nostro business.
Rispettiamo le leggi nazionali vigenti e le disposizioni dell'industria riguardo l'orario lavorativo.
Per rafforzare e sviluppare la nostra squadra siamo impegnati nel programma Investors In People: quale sistema di gestione che riconosce il ruolo delle persone e garantisce miglioramenti nel business.
Il nostro scopo è creare pari opportunità per tutti i nostri dipendenti sia dal punto di vista economico che professionale, senza discriminazioni di razza, ceto, origine, religione, invalidità, sesso, orientamento sessuale, appartenenza sindacale o affiliazione politica, stato civile.
Per garantire il rispetto di tutte le libertà dell'individuo, ci impegniamo ad impedire qualsiasi forma di comportamento lesivo della dignità personale.

SICUREZZA

Siamo impegnati nel rispetto di tutte le normative e i regolamenti nazionali ed internazionali in materia di sicurezza. In tutte le nostre sedi esistono rappresentanti della sicurezza e gruppi di miglioramento, che hanno il compito di sviluppare politiche della sicurezza per identificare ed eliminare i rischi. Crediamo fortemente nell'adozione delle Best Practices che permettono di superare le richieste imposte dalla legislazione corrente e misuriamo e verifichiamo costantemente i risultati raggiunti in questo settore, così importante per il nostro business.

PROTEZIONE AMBIENTALE

Siamo impegnati a ridurre qualsiasi impatto negativo che la nostra attività può causare all'ambiente. Investiamo in programmi che hanno come obiettivo il raggiungimento dei più alti standard di protezione ambientale e andando oltre alle richieste della regolamentazione locale e nazionale, cerchiamo di minimizzare i potenziali impatti ecologici causati dalla nostra attività.

I NOSTRI FORNITORI

Chiediamo ai nostri fornitori di riconoscersi nei principi etici espressi nella presente politica e ci aspettiamo che sviluppino ed implementino programmi ambientali e sociali che dimostrino il loro impegno sociale.
Ci impegniamo a fornire tutto il supporto consulenziale al fine di trasferire le nostre conoscenze in materia di responsabilità d'impresa verso la Società.

LA NOSTRA SOCIETA' E LA COMUNITA'

Siamo impegnati nell'assumere un ruolo pro-attivo e di guida per lo sviluppo e la promozione di azioni nell'ambito della sostenibilità sociale. Cerchiamo di essere presenti tra le forze governative o di consultazione per assicurare il nostro coinvolgimento nei dibattiti che possono guidarci verso il miglioramento del business.
Siamo attenti a tutte le innovazioni tecnologiche che consentono di migliorare l'impatto del nostro business sulla comunità e sull'ambiente e ci impegniamo ad introdurle non appena si verifichino le condizioni commerciali ed operative.
Supportiamo importanti ricerche ed idee per sfruttare le opportunità più innovative.
Mettiamo a disposizione la nostra esperienza nello sviluppo sostenibile per il beneficio dell'industria e della comunità promovendo il dialogo con tutte le parti interessate.

Uffe Ekstedt
Amministratore Delegato
TNT Express Italy S.p.A.
Luglio 2011

HT Srl
Via Moscova, 13 - 20121 Milano

TNT GLOBAL EXPRESS S.p.A.

Sistema Integrato Qualità, Ambiente ed Etica

AUTOCERTIFICAZIONE PER CONFLITTI DI INTERESSE

Il/la sottoscritto/a BEDESCHI (cognome) VALERIANO (nome)

nato a MILANO (luogo) provincia di MI (prov.) il 20-03-72

in qualità di AMMINISTRATORE DELEGATO

(titolare, legale rappresentante, amministratore, etc.)

della società

H/T S.R.L.

con sede in MILANO Partita I.V.A. 03924730967

Consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 D.P.R. n° 445 del 28/12/2000

DICHIARA

1) di avere ☐ **di NON avere** ☒ (barrare la voce che interessa)

rapporti di parentela di primo o secondo grado con personale dipendente della TNT, delle Società controllate da TNT e Joint Ventures.
In caso positivo specificare Nome, Cognome e grado di parentela:

_____ _____

_____ _____

2) che tra gli addetti della società _____ che rappresenta

sono presenti ☐ **NON sono presenti** ☒ (barrare la voce che interessa)

persone che hanno rapporti di parentela di primo o secondo grado con dipendenti della TNT o con dipendenti delle Società controllate da TNT o Joint Ventures.
In caso positivo specificare Nome, Cognome degli addetti interessati, Nome e Cognome dei dipendenti TNT e grado di parentela:

_____ _____

_____ _____

3) che tra la società _____ che rappresenta e TNT, incluse le Società controllate e Joint Ventures

sussistono ☐ **NON sussistono** ☒ (barrare la voce che interessa)

condizioni tali per cui esistono conflitti d'interesse, non solo relativamente a parenti di primo e secondo grado, ma anche in relazione a conoscenti o amici personali.
In caso positivo specificare Nome, Cognome dei dipendenti TNT interessati

_____ _____

_____ _____

4) ☒ Mi impegno a comunicare tempestivamente a TNT (Servizio Subcontractor Management) e senza alcun ritardo, ogni caso di conflitto d'interesse intervenuto in data successiva alla data del presente documento, come a titolo di mero esempio, il legame di parentela di primo o di secondo grado di un nuovo addetto, con un dipendente TNT, inclusi i dipendenti delle Società controllate da TNT e Joint Ventures.

Data 29-3-2012 Firma _____

H/T S.r.l.
Via Mosqova, 13 - 20121 Milano

MOD. AUT. CI Titolare – ed. 15/01/2008

5