ICT Security – Dicembre 2002
Autore: Daniela Rocca

PENETRATION TESTING E RESPONSABILITA'

SOMMARIO

Il penetration testing professionale

L'utilizzo da parte delle aziende del *penetration testing* "professionale" è cresciuto notevolmente negli ultimi anni.

Ciò nasce dalla consapevolezza che testare dall'esterno la vulnerabilità dei propri sistemi è una delle migliori condotte da tenere per identificare a che tipo di attacchi si è esposti e permette di attrezzarsi per far sì che le vulnerabilità della propria rete non siano sfruttate da una parte ostile. L'identificazione del rischio è prodromica alla soluzione da attuare.

L'obiettivo di chi effettua un *penetration testing* è quindi quello di testare un sistema dalla prospettiva di un hacker, *come se* fosse un hacker.

Ma se un hacker conosce o dovrebbe conoscere le conseguenze della propria attività illecita (ricordandoci che *ignorantia legis non excusat*) e se ne assume l'onere, ci domandiamo a che tipo di responsabilità civili e penali potrebbe andare incontro una società o un individuo che per contratto svolga questo tipo di attività.

Penetration testing e responsabilità

Partiamo quindi dal presupposto che esista un contratto che lega la società A alla società B, nel quale A incarica B di effettuare un *penetration testing*, determinandone modalità di esecuzione e riferimenti temporali.

Si è in presenza di una *obbligazione* derivante da *contratto* (art. 1173 Cod. Civ.), definito dalla nostra normativa come *un accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale* (art. 1321 Cod. Civ.).

Come da prassi, la società B, per tutelarsi da eventuali azioni future di A nei suoi confronti, ha voluto inserire nel contratto una clausola di esonero da ogni responsabilità derivante:

Caso 1

- dal mero accesso al sistema informatico di A;

Caso 2

- da eventuali danni derivanti dalla sua attività di intrusione nel sistema informatico di A.

Da un punto di vista civilistico, le *clausole di esonero da responsabilità* rientrano nell'autonomia contrattuale delle parti (art. 1322 Cod. Civ.), ma sono nulle se limitano o

escludono *preventivamente la responsabilità del debitore per dolo o colpa grave* o se costituiscono una violazione di obblighi di ordine pubblico (art. 1229 Cod. Civ.).

Caso 1

Non è possibile configurare una eventuale responsabilità penale di B dovuta alla mera attività di *penetration testing*, perché *non è punibile chi lede o pone in pericolo un diritto, col consenso di chi può liberamente disporne* (art. 50 Cod. Pen.).

La società A può liberamente disporre della propria rete aziendale? Non trattandosi di un atto di disposizione del proprio corpo, vietato dall'art. 5 del Codice Civile quando cagioni una diminuzione permanente dell'integrità fisica o sia altrimenti vietata dalla legge, dall'ordine pubblico o dal buon costume, la risposta sembra essere positiva.

Né naturalmente si configura una responsabilità a carattere civilistico, visto che l'attività di *penetration testing* corrisponde all'oggetto del contratto.

Si potrebbe quindi prescindere da una clausola nel contratto che espressamente esoneri dalle responsabilità o dalla sottoscrizione di una lettera di esonero, come spesso accade nella prassi.

Naturalmente se si travalicassero i limiti posti dal contratto e, ad esempio, ci si mantenesse nel sistema contro la volontà espressa o tacita di colui che ha il diritto di escluderci, si configurerebbe il reato previsto dall'art. 615-ter di accesso abusivo ad un sistema informatico; tutte le fattispecie introdotte dalla L. 547/1993 sarebbero ipotizzabili e, con tutta probabilità, aggravate dall'abuso della qualità di operatore del sistema.

Caso 2

Nell'adempiere all'obbligazione, B deve usare la diligenza *del buon padre di famiglia*, che deve valutarsi con riguardo all'attività esercitata visto che si è in presenza di una attività professionale (art. 1176 Cod. Civ.).

Le situazioni che si possono verificare quando si è stati autorizzati ad accedere ad un sistema per un *penetration test* sono fondamentalmente di tre tipi:

a) Che si agisca con dolo o colpa grave, ossia consapevolmente senza il rispetto delle normali regole di diligenza. In questo caso la responsabilità civile sarà piena e non sarà possibile escluderla mediante clausole contrattuali.

b) che nell'effettuare il *penetration test* non si rispettino gli obblighi e le procedure alle quali ci si è contrattualmente vincolati. In tal caso, evidentemente, si verifica una fattispecie di inadempimento di un contratto di servizi e pertanto si applicano le norme di cui agli artt. 1175, 1176, 1375 e si è tenuti al risarcimento del danno (art. 1218 Cod. Civ.), che comprende sia la perdita subita da A che il mancato guadagno se conseguenza immediata e diretta dell'inadempimento (art. 1223 Cod. Civ.). In tale ambito, una clausola di esonero dalle responsabilità è lecita.

c) che, pur rispettando gli obblighi espressamente previsti dal contratto, si provochi un danno economico o operativo al proprio cliente. Si sarà responsabili se, pur rispettando la lettera del contratto, si è venuti meno a quegli obblighi di protezione

che secondo la dottrina e la giurisprudenza, fanno parte dei doveri contrattuali anche se non espressamente previsti. Per chiarire il concetto, prendiamo ad esempio una persona che è tenuta a consegnare una statua del peso di tre tonnellate che, nel momento in cui deposita l'oggetto presso il luogo in cui è tenuto a fare la consegna, l'appoggia per terra senza le dovute cautele, con la conseguenza che il pavimento viene sfondato. E' ovvio che, in questo caso, colui che ha effettuato la consegna è tenuto al risarcimento dei danni.

I danni possono essere di natura contrattuale o extracontrattuale, a seconda di come si verificano i fatti. Con riferimento ai sistemi informatici, la casistica è estremamente varia e complessa: in generale il giudice deciderà che cosa si è verificato sulla base di una perizia tecnica che gli renderà comprensibile se e in quale modo siano stati violati questi doveri di protezione, che anche se non espressamente previsti dal contratto sono tipici nell'ambito di un rapporto obbligatorio.

Non essendo tali obblighi di protezione previsti contrattualmente, non ci si può esonerare dalle responsabilità che ne derivano.

Civilmente responsabile del danno eventualmente arrecato è la società legata dal contratto, non il dipendente/collaboratore della società che provoca materialmente il danno.

La responsabilità penale è invece personale e, come nel caso 1, sarebbe punibile penalmente chi effettua il test travalicando i confini contrattuali con una condotta configurante uno o più dei c.d. reati informatici introdotti dalla L. 547/1993.

Penetration testing e normativa sulla privacy

Il D.P.R. 318/1999 sulle misure di sicurezza minime per il trattamento dei dati personali ha in qualche modo legittimato il *penetration testing* quando afferma che *gli elaboratori devono essere protetti contro il rischio di intrusione…mediante idonei programmi la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale* (art. 4 comma 1 lett. c). L'art. 6 prevede inoltre che l'efficacia delle misure di sicurezza deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Il *penetration testing* può a tutti gli effetti essere considerato un metodo di controllo.

Ci si domanda però come il *penetration testing* stesso si concilia con la protezione dei dati personali che dovrebbe aiutare a tutelare.

E' evidente che colui che effettua il test potrebbe venire a conoscenza di dati personali e/o sensibili di clienti/dipendenti/fornitori della società che ha commissionato il test: è necessario il consenso degli interessati al trattamento dei dati? In base all'art. 19 della L. 675/1996, *non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni di trattamento dal titolare o dal responsabile, e che operano sotto la loro diretta responsabilità.*

Sembra quindi potersi escludere la necessità del consenso degli interessati, visto lo stretto legame tra l'attività di *penetration testing* e l'individuazione delle misure minime di sicurezza ex D.P.R. 318/1999.

Daniela Rocca