



FooIDNS Business

Privacy Overview Whitepaper

Indice

Il problema del controllo della risorsa aziendale Internet	3
Normativa di riferimento	3
Perché monitorare la rete?	4
Le problematiche del proxying	5
Le problematiche dell'url filtering	6
I problemi di Aggregazione	7
La soluzione di FoolDNS	7
FoolDNS ed altri DNS Server	9
Un servizio completo	10
Chi siamo?	11
Service Overview	11
I Servizi	11

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

Il problema del controllo della risorsa aziendale Internet

Normativa di riferimento

Il problema del controllo della navigazione Internet effettuata da parte degli utenti aziendali è una questione aperta, sentita e di non facile risoluzione, tanto da meritarsi menzione, per lo meno in Italia, sia nella normativa concernente il controllo dei lavoratori sia in quella relativamente più recente facente capo alla tutela della Privacy.

I controlli aziendali vanno sicuramente preventivati, utilizzati in modo minimale, concordati con i sindacati e preventivamente autorizzati e sottoscritti dal dipendente, in una trafila burocratica che solamente le aziende più grandi e più sensibili alle problematiche legali – nonché fornite di corposo staff interno legale – sono in grado di affrontare con competenza e ottenendo risultati.

Nella moderna gestione dei sistemi informativi, quindi, il maggior problema dell'abuso del mezzo Internet è caratterizzato dall'impossibilità pratica di controllo del lavoratore o anche solamente del controllo puntuale della risorsa aziendale Internet senza sconfinare nella violazione della normativa facente capo a Privacy o Controllo del Lavoratore.

In questo ambito in particolare la tutela della privacy ha avuto negli anni una evoluzione tale da fornire plurimi distinti punti di interesse per quanto riguarda la concretizzazione delle informazioni e delle definizioni di "controllo": infatti le "Linee Guida per l'utilizzo di Posta Elettronica ed Internet" emanate dal Garante nella Gazzetta Ufficiale n. 58 del 10 marzo 2007 riportano le seguenti affermazioni:

a)(...) il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (...) Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (art. 4, primo comma, l. n. 300/1970), tra cui sono certamente

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

comprese strumentazioni hardware e software mirate al **controllo dell'utente di un sistema di comunicazione elettronica**.

Il trattamento dei dati che ne consegue è **illecito, a prescindere dall'illiceità dell'installazione stessa**. Ciò, anche quando i singoli lavoratori ne siano **consapevoli**.

In particolare non può ritenersi consentito il trattamento effettuato mediante (...) controllo a distanza (...) della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

Appare quantomeno evidente come le indicazioni del Garante forniscano senza ombra di dubbio una interpretazione onnicomprensiva della tematica, arrivando a proclamare che il "trattamento (...) della riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore" è da considerarsi "illecito, a prescindere dall'illiceità dell'installazione stessa".

Il Garante stesso si accorge, probabilmente, delle altissime barriere che questa interpretazione porta con sé, arrivando a concedere nelle linee guida difese "preventive" a quei datori di lavoro che intendano munirsi di sistemi di contrasto all'utilizzo illecito della risorsa Internet. Sempre dallo stesso documento, infatti:

b) Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, (...) l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. (...)

In altre parole la normativa, ostacolando da ogni punto di vista la possibilità di controllo dell'effettiva navigazione, fornisce la possibilità di blocco a priori come palliativo alla impossibilità di trattamento, pensando così di mitigare il problema dell'abuso del mezzo Internet.

Perché monitorare la rete?

L'errore di fondo compiuto dal Garante e dalla normativa di riferimento è, però, considerare l'analisi e la redazione di statistiche dell'utilizzo del mezzo Internet come intrinsecamente legate al controllo del navigatore: se è pur vero che spesso tali statistiche siano utilizzate principalmente in occasione di abusi della disponibilità del mezzo Internet a fini di svago personale, è anche vero che sempre

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

più spesso in un sistema web complesso come quello moderno ci si trova nella necessità di dover sottoporre a controllo una risorsa di comunicazione (Internet) fondamentale non soltanto per la “navigazione” propriamente detta ma anche e soprattutto per il funzionamento della intera infrastruttura di rete.

Episodi recentissimi, come ad esempio il virus Conficker¹, hanno ampiamente dimostrato come sia necessario controllare l'utilizzo della rete per prevenire infezioni o ancora meglio per constatare una avvenuta infezione e porre adeguati ripari alla sua proliferazione.

Non solamente: sempre più spesso accade infatti di trovare traccia nel controllo e monitoring dell'utilizzo di rete di applicativi installati e non autorizzati, di congegni hardware e software presenti ma proibiti e di tutta un'altra serie sterminata di dati importantissimi per l'analisi e la risoluzione di problematiche legate alla rete locale e non che senza continuo e costante controllo rischiano di trasformare la “rete Internet” in una terra di nessuno digitale dedita al solo controllo perimetrico.

L'orientamento del Garante sulla impossibilità di controllo puntuale e la necessità di controllo preventivo equivalgono a voler affermare la necessità per la sicurezza di una nazione di erigere altissimi muri separatori dal resto del mondo e l'impossibilità di controllo interno dell'ordine pubblico: molto spesso, invece, le minacce arrivano e si proliferano all'interno dell'azienda stessa.

Le problematiche del proxying

La soluzione normalmente consigliata ed adottata dalla maggior parte delle realtà della PMI italiana e non solo si basano sempre e comunque sulla necessità di installazione all'interno del perimetro aziendale di un sistema centralizzato di Proxy² attraverso cui tutta la navigazione passa e viene tracciata. I dati contenuti nel Proxy aziendale vengono poi consultati per la redazione di statistiche sull'utilizzo della rete stessa.

Questa tipologia di approccio, sebbene perfetta per il contrasto di taluni comportamenti, rischia per altri di trascinare l'azienda che implementa soluzioni di questo tipo nell'illiceità dell'installazione stessa.

Se è pur vero, infatti, che un sistema di Proxy adempie egregiamente al compito di de-responsabilizzazione dei vertici aziendali dall'abuso del mezzo Internet (ricordando che il legale Rappresentante di una Azienda è responsabile in solido

¹ <http://en.wikipedia.org/wiki/Conficker>

² http://en.wikipedia.org/wiki/Proxy_server

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

della navigazione compiuta da quella stessa azienda) fornendo validissimi strumenti per dimostrare alle autorità di Polizia Giudiziaria in caso di perpetrazione di illecito o reato chi sia effettivamente stato a compiere determinati reati all'interno dell'azienda, è pur vero che l'utilizzo di questi dati al fine di controllo dell'utilizzo del mezzo Internet presenta notevoli problematiche.

E' infatti, ricordiamo, direttamente il garante a sostenere che "il trattamento dei dati" di navigazione "è illecito, a prescindere dall'illiceità dell'installazione stessa, cioè, anche quando i singoli lavoratori ne siano consapevoli", stabilendo quindi precise limitazioni alla memorizzazione ed all'utilizzo di questi dati in possesso dal Proxy per un utilizzo differente da quello di discolpa da accuse da parte della Polizia Giudiziaria.

E non basta neppure la sempre utilizzata "scusante" della semplice memorizzazione e non utilizzo, che sempre più spesso si vede utilizzare da parte di chi si tenta di difendere da accuse di utilizzo illecito dei dati: è infatti dal 2003 che si conosce la definizione di trattamento che nella sua formulazione completa³ recita il Decreto Legislativo 30 giugno 2003, n. 196, conosciuto anche come "Codice in materia di protezione dei dati personali" pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003, che nell'Art.4 cita:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

La mera "registrazione" e/o "conservazione" rappresenta quindi, sottolineiamo ancora una volta, un trattamento e, come tale, va incontro alle problematiche relative.

Le problematiche dell'url filtering

Se complesse e multiformi sono le problematiche relative alla memorizzazione dei dati di Proxy, ancora più critiche sono le quelle relative agli apparati dedicati ad

³ <http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm>

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

implementare il filtro sia in ordine a nome di dominio che eventualmente ad indirizzo internet: tali dati, infatti, possono con estrema probabilità contenere indicazioni precise di preferenze sessuali o ideologie.

Se, infatti, la sola detenzione della navigazione del singolo utente solleva grandissime difficoltà per la gestione, che dire della memorizzazione sistematica dei tentativi di accesso ad un sito bloccato che, per sua propria natura, coinvolge quasi sicuramente tipologie di contenutistica sensibili?

L'unica soluzione, in questo contesto, è il blocco di qualunque log da parte della appliance dedicata al filtraggio ma, ovviamente, questo comporta l'impossibilità pratica della tutela del mezzo internet nella sua interezza.

I problemi di Aggregazione

La normativa di riferimento prevede sicuramente differenti tipologie di risoluzione delle problematiche relative alla gestione dei log: la principale soluzione proposta è quella della aggregazione dei dati.

Ma come intraprendere percorsi di aggregazione dei dati che sia a norma di legge? Non è possibile, infatti, mantenere agevolmente una aggregazione che non riporti in qualche altro punto aziendale il dato non aggregato. Inoltre se è pur vero che sono previsti meccanismi di segregazione dei dati, è anche vero che le realtà in cui sia fisicamente possibile isolare le funzioni di utilizzo ed implementazione dei sistemi di aggregazione e responsabili del dato disaggregato siano tra di loro non comunicanti o, nella maggior parte dei dati, coincidenti.

Ancora una volta, quindi, ci troviamo di fronte ad un binomio: o memorizzare il dato per esigenze di difesa in occasioni di richieste dell'Autorità Competente, ma senza possibilità di utilizzo per il controllo del media Internet, oppure filtraggio dei contenuti senza mantenere alcun tipo di log, anche in questo caso senza la possibilità di inferire dati sull'utilizzo di connessione all'interno della rete aziendale.

La soluzione di FooldNS

FooldNS rappresenta, in questo scenario, la terza via: demandare ad un servizio esterno la gestione del logging e della reportistica. Una terza parte che non solo implementa nel concreto l'isolamento proposto dalla normativa, ma che altresì gestisce per la stessa conformazione della rete il dato in modo aggregato ed anonimo, ma puntuale nella rilevazione delle infrazioni alla policy aziendale.

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

FoolDNS, infatti, è erogato come servizio di SaaS (Software As A Service), che significa semplicemente l'utilizzo di un servizio esterno. Le interrogazioni ai database di FoolDNS avvengono direttamente dalla rete interna del cliente sottoposta a NAT⁴. In termini semplicistici tutte le richieste della società arrivano ai server di FoolDNS come una sola "persona" navigante che a tutti gli effetti non concede in nessun modo di inferire e capire quale sia il client all'interno della rete ad aver sottoposto l'interrogazione.

Mediante questo meccanismo è estremamente semplice, anche in virtù dei molteplici tipi di reportistica messi a disposizione da FoolDNS, individuare le infrazioni alla Policy Aziendale e prendere adeguati provvedimenti sia cautelativi (blocco dei domini che appaiono in statistica) sia repressivi (audit interno per la rilevazione del responsabile) senza in alcun modo contravvenire alle disposizioni di legge.

Sempre nel succitato "Linee guida per l'utilizzo di Posta Elettronica ed Internet", infatti, si cita come trattamento a norma:

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, (...) l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. (...)

In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali: (...)

trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di log riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori);

FoolDNS implementa nativamente queste raccomandazioni essendo stato concepito dall'origine, creato e commercializzato direttamente con l'intento di effettuare un "trattamento di dati in forma anonima" ed è espressamente programmato per implementare un meccanismo "tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni". I dati di FoolDNS sono disponibili

⁴ http://en.wikipedia.org/wiki/Network_address_translation

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

giornalmente, settimanalmente e mensilmente alle singole aziende che possono in questo modo nel pieno rispetto della normativa vigente monitorare con efficacia la propria connessione Internet.

Utilizzando il servizio le aziende riescono, senza preoccuparsi in alcun modo di violare la normativa vigente, ad avere un quadro di utilizzo puntuale e preciso della risorsa Internet, consentendo un controllo capillare sui siti da bloccare o concedere senza utilizzare liste onnicomprensive e di vago sapore censorio. Non ha infatti senso, da un punto di vista implementativo, bloccare milioni di siti internet che vedranno un utilizzo sporadico di qualche host per anno: molto meglio andare a controllare i 300 siti più visitati e capillarmente eliminare quelli che presentano incompatibilità con le policy aziendali.

FoolDNS ed altri DNS Server

Benché FoolDNS sia l'unica soluzione commerciale venduta con questa tipologia di servizio e con la vastità di funzionalità che abbiamo elencato, esistono nel panorama dei servizi Web internazionali differenti realtà che offrono servizi di DNS libero, taluni dei quali anche in modalità freeware o gratuita.

La qualità di questi servizi è sicuramente da valutarsi come eccellente per qualunque utilizzo domestico mentre l'utilizzo in ambito aziendale necessita sicuramente di una approfondita analisi preventiva.

In primo luogo è da considerarsi come i dati di navigazione rappresentino a tutti gli effetti dati personali della "persona giuridica" della società ed, oltretutto, eventualmente di soggetti fisici all'interno della stessa. Per questa tipologia di dati esistono obblighi specifici che FoolDNS, mediante la propria Privacy Policy⁵, tutela direttamente secondo la normativa italiana.

In aggiunta a questo bisogna ricordare che talune tipologie di trattamenti necessitano obbligatoriamente segnalazione al Garante in caso di esportazioni oltre al territorio nazionale e/o Europeo e come moltissimi di questi servizi siano ospitati ben al di fuori dei confini territoriali italiani e/o europei.

Infine è importantissimo segnalare come i dati affidati a questi soggetti terzi ben raramente non vengano ceduti a terzi per esigenze di marketing o profilazione: in questo caso come motiveremmo al CDA o a eventuale ispezione del Garante presso le nostre strutture la rivendita dei nostri dati di navigazione a terzi?

⁵ <http://www.fooldns.com/privacy.html>

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

Nell'appoggiarsi a strutture esterne è sempre necessario controllare che, come FooldNS, esse assicurino la non rivendita dei dati personali e la conservazione degli stessi a norma di legge, entro i confini ove richiesto della nazione di appartenenza.

Un servizio completo

Oltre ai servizi di monitoring della connessione a norma di legge ed alla creazione di reportistica dettagliata su eventuali utilizzi illeciti del mezzo Internet, FooldNS offre una vasta gamma di servizi che vanno dalla creazione e/o abilitazione di blocchi a livello di liste sino alla prevenzione della visualizzazione di pagine di phishing e di pedo-pornografia, passando per la gestione del blocco dei contenuti afferenti a malware e dalla gestione dei contenuti violenti.

Mediante l'installazione di FooldNS è semplice per un'azienda tutelarsi e tutelare il proprio asset internet in una visione sinergica della Rete Internet volta all'utilizzo consapevole e non indiscriminato.

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

Chi siamo?

Service Overview

La navigazione Internet è divenuta un patrimonio fondamentale per il business di centinaia di differenti categorie societarie: mediante Internet è possibile comunicare, informarsi, aggiornarsi e aggiornare.

Sfortunatamente come ogni media di successo anche Internet è stato, nel tempo, utilizzato sempre più pesantemente per veicolare contenuti pubblicitari.

Per meglio strutturare, poi, l'offerta pubblicitaria, la navigazione è stata sempre più sottoposta a tracciamenti e profilazione, sino a fare divenire l'intero mondo del Web, a detta di alcuni, "un concentrato di contenuti a supporto della pubblicità". La pubblicità ed il tracciamento rappresentano oltre il 25% dell'intero volume di traffico che una azienda genera dal suo interno, senza contare l'enorme potenziale di distrazione che questa genera.

In aggiunta a queste problematiche il Web diviene sempre più spesso un veicolo importante per la diffusione di malware, che sfruttandone le doti intrinseche di disponibilità e velocità di trasmissione, ha eletto questo nuovo media a vettore privilegiato per il contagio.

Sempre più spesso l'utilizzo inconsapevole di un utente rischia di creare pesanti danni all'intera infrastruttura.

Infine è necessario sottolineare come un utilizzo non mirato e finalizzato del mezzo Internet possa provocare nella PMI italiana notevoli cali di produttività e fughe di informazioni, con il proliferarsi di siti di intrattenimento non consoni all'ambiente lavorativo o network sociali che richiedono immense quantità di tempo sottratte alla vita lavorativa.

A tutti questi problemi FoolDNS cerca di dare una soluzione concreta, economica ed efficace.

I Servizi

L'offerta del servizio di FoolDns contempla quattro aree di utilizzo: la creazione e l'enforcing delle policy di navigazione, il monitoraggio e reporting dell'utilizzo web, la gestione della profilazione e dell'advertising, la mitigazione dei rischi di contagio malware,.

La visione sinergica di queste singole feature rendono FoolDns un sistema completo per la economicizzazione e sistematizzazione dei servizi Web offerti all'interno dell'azienda, in un approccio pragmatico e di semplice attuazione e deployment.

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL

La gamma di servizi forniti da FoolDns Business, mediante un'unica interfaccia di amministrazione ed un unico sistema di Reporting, erogati in modalità di SaaS (Software As A Service) non prevedono per l'Azienda nessun costo di Hardware, nessuna manutenzione interna della infrastruttura, nessuna installazione sui computer client, nessuna regola da implementare nei sistemi informativi interni e nessun applicativo da testare ed installare. FoolDns è attivo con una semplice configurazione di rete su qualunque sistema operativo, su qualunque browser o dispositivo ed in qualunque software di navigazione, anche personalizzato o installato in modo fraudolento sui computer aziendali.

Reference: DOC-2009-FOOLDNS-PRIVACY	Last revision: 09/07/2009
Version: DRAFT	Status: CONFIDENTIAL



The Fool s.r.l.
C.so di Porta Ticinese, 87
20123 Milano (MI)

P.I./C.F. 06367570964

T. +39.02.00618826
F. +39.02.89455679
M. info@thefool.it