**ATTI PARLAMENTARI**

**XVI LEGISLATURA**

# CAMERA DEI DEPUTATI

Doc. **XVII**
n. **26**

## DOCUMENTO APPROVATO DALLA IX COMMISSIONE PERMANENTE (TRASPORTI, POSTE E TELECOMUNICAZIONI)

*nella seduta del 22 gennaio 2013*

**A CONCLUSIONE DELL'INDAGINE CONOSCITIVA**

*deliberata nella seduta del 1º febbraio 2012*

## SULLA SICUREZZA INFORMATICA DELLE RETI

*(Articolo 144, comma 3, del Regolamento della Camera dei deputati)*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

# INDAGINE CONOSCITIVA SULLA SICUREZZA INFORMATICA DELLE RETI

## DOCUMENTO CONCLUSIVO APPROVATO

SOMMARIO

PAGINA BIANCA

## PREMESSA

Negli ultimi anni, i servizi forniti dai cosiddetti *service provider*, appartenenti tanto ad amministrazioni pubbliche, quanto e soprattutto ad imprese private *(Utilities*, banche, assicurazioni, eccetera), sono cresciuti in maniera esponenziale, sia su reti *wired*, ossia basate su connessioni cablate, sia su reti *wireless*, cioè senza fili.

La diffusione di transazioni espletate interamente « a distanza », infatti, ha prodotto un notevole aumento dell'efficienza a livello sistemico, misurabile in termini di abbattimento dei costi, di accorciamento della filiera di servizio, di tempestività nella raccolta e trattamento delle informazioni, che ha incentivato, sia nel settore pubblico che in quello privato, la diffusione di sistemi di pagamento in rete, anche per transazioni finanziarie e di *e-commerce* di importo contenuto.

Tutto ciò ha però comportato l'emergere di notevoli problemi di sicurezza e di affidabilità delle transazioni in moneta elettronica, tanto che la barriera più rilevante alla crescita di tali transazioni è rappresentata proprio dalla scarsa dimestichezza e dalla diffidenza degli utenti/clienti nell'uso degli strumenti elettronici, spesso dovute ad una non adeguata informazione sui rischi reali che i predetti strumenti comportano e sulle corrette contromisure che possono essere adottate.

Cresce quindi l'esigenza di una diffusione e di una standardizzazione dei sistemi di protezione dei flussi di comunicazione, unitamente ad un'attività su vasta scala di acculturamento dell'utenza, per rendere quest'ultima edotta riguardo alle informazioni frammentarie, errate e talvolta ingannevoli che corrono sulla rete nonché in merito alle tecniche semplici ed efficaci di protezione che possono essere conseguentemente adottate.

I sistemi attualmente disponibili per la protezione dei dati che viaggiano sulle reti telematiche, infatti, presentano numerosi aspetti di debolezza, sia dal punto di vista della *security* sia sotto il profilo della *privacy*, che rendono relativamente facile, anche per soggetti non particolarmente esperti di *Information Technology*, mettere in chiaro comunicazioni riservate ed utilizzarle a fini dolosi e comunque illegali.

Altro tema rilevante è quello della conservazione sicura dei dati. Le politiche di *backup*, ossia volte alla conservazione di dati al fine di prevenirne la perdita totale, e di *Disaster Recovery*, cioè finalizzate al recupero delle funzionalità e dei dati dopo un evento grave, ove non risultino affidabili, possono condurre a conseguenze potenzialmente disastrose sulla recuperabilità dei dati, sia a livello locale sia a livello di sistema.

In questo quadro, il 1º febbraio 2012, la Commissione ha deliberato lo svolgimento di un'indagine conoscitiva sulla sicurezza informatica delle reti che si è focalizzata su tre argomenti principali:

l'identità digitale, il « *Cloud computing* » e le reti di telecomunicazione *wired* e *wireless*. In relazione a ciascuno di tali argomenti sono state acquisite dalla Commissione specifiche informazioni.

Nel corso dell'indagine sono stati auditi: il dottor Mario Magini, esperto di sicurezza informatica; l'amministratore delegato di Poste italiane Spa, ingegner Massimo Sarmi; rappresentanti di Confindustria; il direttore del Servizio di polizia postale e delle comunicazioni, dottor Antonio Apruzzese; rappresentanti di UIRNet Spa; rappresentanti di Cisco Systems Italy srl; rappresentanti dell'European Electronic Crime Task Force; rappresentanti della Conferenza delle regioni e delle province autonome; rappresentanti di ABI-Lab. Il ciclo di audizioni si è quindi concluso il 18 dicembre 2012 con l'intervento del sottosegretario di Stato per lo sviluppo economico, professor Massimo Vari.

I risultati dell'indagine sono esposti nel presente documento, che, prendendo le mosse da una ricostruzione delle principali tipologie di minacce alla sicurezza delle reti, esamina i fondamentali elementi di criticità delle reti con specifico riferimento ai tre argomenti sopra richiamati, anche alla luce del quadro normativo di riferimento, europeo e nazionale, evidenziando i possibili rimedi. Nelle conclusioni del documento, infine, vengono riepilogate le soluzioni proposte ai fini del potenziamento della sicurezza informatica delle reti.

## 1. Le tipologie di minacce alla sicurezza delle reti

L'importanza di Internet, ai fini dello sviluppo economico e sociale di un Paese, è un dato di comune esperienza. Basti pensare che il numero degli utenti della rete è enormemente aumentato negli ultimi anni, anche grazie alla telefonia mobile che ha reso più agevole la connessione a Internet. In Italia, ad esempio, risultano attivate più connessioni telefoniche di quanti siano gli abitanti, il che significa che ogni abitante risulta titolare, mediamente, di più schede telefoniche. Dal 2000 ad oggi, quindi, il numero degli utenti della rete è passato da 360 milioni a 2 miliardi e 200 mila. A tutto ciò ha fatto però riscontro l'emergere di notevoli problemi di sicurezza e di affidabilità della rete soprattutto per quanto concerne le transazioni in moneta elettronica.

Risulta quindi sempre più determinante costruire un ambiente digitale sicuro che offra a tutti i cittadini nuove possibilità e prospettive di sviluppo. Si tratta di un obiettivo da realizzare con assoluta priorità, giacché il numero delle minacce e delle violazioni della sicurezza ha già provocato notevoli danni economici, riducendo la fiducia degli utenti nell'utilizzo delle nuove tecnologie e ostacolando lo sviluppo del commercio elettronico.

In questo quadro, appare essenziale definire preliminarmente quali siano le possibili minacce alla sicurezza della rete. In particolare, la Comunicazione COM(2011)163 definitivo della Commissione europea, suddivide le minacce, a seconda della loro finalità, in tre grandi categorie:

– finalità di sfruttamento, che riguarda le minacce persistenti a fini di spionaggio economico e politico e furti di identità digitale;

– finalità di perturbazione, che si riferisce agli attacchi volti all'interruzione di un servizio, con origine da più fonti, come lo *spamming* realizzato mediante *botnet* o gli attacchi DDoS (*Distributed Denial of Service)*, di cui si dirà tra breve;

– finalità di distruzione, che riguarda le minacce volte alla distruzione delle infrastrutture critiche – reti elettriche e sistemi idrici intelligenti – che concretamente non sono mai state attuate, ma che non si può escludere che lo possano essere in futuro.

Venendo ai temi che più da vicino interessano la presente indagine, è opportuno passare in rapida rassegna, tra le minacce dianzi menzionate, quelle consistenti nel furto di identità digitale e quelle rivolte al *Cloud computing* e alle reti *wired*, ossia basate su connessioni cablate, e alle reti *wireless*, cioè senza fili, facenti capo a organizzazioni pubbliche o private.

### *1.1 Il furto di identità digitale*

Prima di affrontare il tema del furto dell'identità digitale è opportuno definire innanzitutto che cosa si intenda con l'espressione « identità digitale », giacché essa segna in un certo senso il superamento della nozione classica di identità fondata sulla presenza fisica di una persona. In particolare, l'identità digitale è la rappresentazione di un soggetto esistente nel mondo reale, sia esso persona fisica o ente, all'interno di un sistema informatico. L'identità digitale può essere declinata in diversi contesti. Vi sono contesti più consolidati, come il mondo delle transazioni finanziarie e della posta elettronica, delle *utility* e delle carte di pagamento, ma emergono anche nuovi contesti come quelli legati ai *social network* e alla partecipazione a *community on line*.

Il ciclo di utilizzo delle identità digitali si sviluppa essenzialmente in tre fasi:

– il *provisioning*, vale a dire la creazione, da parte di un *identity provider*, dell'identità digitale per definire un'attribuzione univoca all'utente finale;

– l'autenticazione ossia l'utilizzo operativo delle credenziali per l'accesso al servizio da parte dell'utente;

– la fruizione del servizio.

Il fenomeno del furto d'identità digitale ha trovato espressione principalmente sotto due forme di diffusione: il *phishing* e il *crimeware*. Il primo consiste nella creazione e nell'uso di messaggi e-mail o SMS che invitano a consultare siti *web* realizzati dai frodatori per apparire come se fossero siti autentici, come ad esempio quello di una banca, con l'obiettivo di carpire informazioni personali e riservate. Il secondo si riferisce invece a una specifica classe di codici malevoli, che si diffondono attraverso Internet, in grado di installarsi direttamente sul PC dell'utente e rendere disponibili informazioni personali e codici di accesso a un potenziale truffatore. Tali codici

malevoli possono consentire a chi li ha trasmessi di « governare da lontano », come se fossero propri, le migliaia o i milioni di computer colpiti, realizzando il cosiddetto *botnet* (*robot network)*.

Secondo i dati forniti dalla polizia postale, in Italia si è registrato un aumento dei casi di furto di identità digitale denunciati dai circa 5 mila registrati nel 2009 ai 45 mila e 807 del 2011. I clienti bancari vittime di tali attacchi sono passati dallo 0,06 per cento del 2010 allo 0,16 per cento del 2011. Nel 96 per cento dei casi, inoltre, si è fatto ricorso a *botnet*, tanto che nel 2011 l'Italia è risultata seconda solo all'India per la localizzazione di *botnet*. Inoltre, in base ai dati forniti da Poste italiane, in Italia vengono rilevate in media 240 mila infezioni giornaliere originate da sette *botnet* principali. Rispetto a questo quadro allarmante è stata posta in essere una significativa attività di contrasto da parte delle istituzioni: in base ai dati forniti dalla polizia postale, nel 2011 sono stati effettuati 95 arresti, mentre nei soli primi sette mesi del 2012 sono stati effettuati ben 109 arresti.

Tutti i soggetti coinvolti nel processo di utilizzo delle identità digitali, si trovano a dover gestire, per la parte di rispettiva competenza, alcune informazioni che possono essere oggetto di attacchi informatici volti ad intercettare, modificare o rendere non disponibili le informazioni in transito. Le criticità che possono manifestarsi vanno pertanto considerate sull'intero processo di gestione, nel loro insieme, al fine di mitigare il rischio complessivo di tutti gli attori coinvolti, dall'*identity provider* all'erogatore del servizio, fino ad arrivare all'utente finale.

Il ruolo dell'*identity provider*, tanto nella fase di *provisioning* quanto in quella di autenticazione e verifica delle credenziali di accesso – ai fini del controllo del corretto accoppiamento tra credenziali e utente reale – appare comunque particolarmente importante, in quanto volto a garantire l'affidabilità dell'intero sistema di gestione sicura delle identità digitali. La gestione dell'identità digitale da parte di *service provider* pubblici e privati può rappresentare un fattore di freno per la diffusione dei servizi e di difficoltà e complicazione per gli utenti.

È necessario affrontare questo tema in modo generale e sistemico, valutando con estrema attenzione l'opportunità di individuare un *identity provider* nazionale ovvero di promuovere la realizzazione di una federazione degli i*dentity provider* per garantire la circolarità dell'identificazione, a prescindere dallo strumento operativo utilizzato, su tutto il territorio nazionale, consentendo al cittadino di operare con un'unica identità digitale. Per realizzare servizi integrati non è sufficiente, infatti, asserire l'identità nel momento in cui l'utente accede, ma le asserzioni d'identità devono essere trasferite anche tra *service provider* in base a relazioni fiduciarie attualmente non regolamentate, anche se alcuni aspetti tecnici sono stati sviluppati nel modello di Gestione Federata dell'Identità Digitale GFID di DigitPA.

Il tema dell'identità digitale è in discussione anche presso le istituzioni dell'Unione europea con una proposta di regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (COM(2012)238), che è volta a fissare le condizioni a cui gli Stati membri riconoscono e accettano reciprocamente i mezzi di identificazione elettronica delle persone

fisiche e giuridiche, fermo restando che, come rilevato dalla Commissione europea, l'emissione di mezzi di identificazione rimane una prerogativa nazionale.

Per quanto riguarda le fasi di autenticazione, va tenuto presente che gli strumenti di autenticazione ai servizi digitali costituiscono spesso un elemento di forte discrezionalità, nonché una leva e un vantaggio competitivo per chi eroga il servizio, in quanto in questa fase bisogna trovare un compromesso tra la facilità di accedere al servizio e il livello di protezione che deve essere assicurato, in quanto più si alza il livello di protezione minore è la facilità di accesso al servizio. Il Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ad esempio, identifica tre livelli di sicurezza. Il primo che prevede il solo inserimento di *username* e *password*, è il più basso e garantisce pochissima sicurezza di accesso. Il secondo che invece prevede, oltre che l'inserimento di *username* e *password*, anche l'utilizzo di un codice generato da appositi dispositivi, come ad esempio le chiavette, che può essere usato una sola volta (*one-time password)*. Infine, il terzo livello, per identificare in maniera forte l'utente, prevede l'impiego di *smart card* utilizzabili a contatto con un lettore, oppure anche senza contatto (cosiddette *contactless)*, ovvero prevede l'utilizzo di sistemi biometrici, che introducono un elemento di autenticazione legato a caratteristiche fisiche del soggetto, come, ad esempio, impronte digitali, iride, e simili.

Per quanto attiene alla fruizione del servizio, si rileva come spesso gli utenti *online* non abbiano l'attenzione che dovrebbero avere ai temi della sicurezza e della protezione dell'identità digitale. Come risulta, infatti, da una recente indagine condotta dalla Commissione europea nei 27 Paesi dell'Unione, i cui esiti sono riportati nel *Cyber Security Report* 2012, il 40 per cento degli italiani intervistati, in ciò secondi soltanto ai portoghesi, dichiara di non avere alcuna conoscenza del *cybercrime*. Il tema della consapevolezza dei rischi da parte dell'utente finale dovrebbe assumere, pertanto, un'importanza sostanziale al duplice fine di proteggere l'utente stesso, da sempre considerato l'anello debole nella catena di sicurezza dell'erogazione dei servizi *online*, e di incrementare e facilitare l'utilizzo di strumenti innovativi con una piena consapevolezza delle loro caratteristiche e, quindi, anche dei loro rischi. In questa prospettiva, si dovrebbe, quindi, intervenire con azioni di sensibilizzazione molto forti, con particolare riguardo ai minori. Infatti, sulla base di quanto già realizzato in altri Paesi membri dell'Unione europea e sulla scia dell'obiettivo indicato tra le priorità dell'Agenda digitale europea, i tempi potrebbero essere maturi per effettuare anche in Italia una campagna di comunicazione allargata, continuativa, intersettoriale e coordinata centralmente da un organo governativo. In particolare, per quanto riguarda i minori, si dovrebbe promuovere la loro formazione attraverso percorsi educativi in grado di fornire, fin dai primi livelli scolastici, le competenze necessarie.

Infine, per combattere efficacemente il furto di identità digitale, oltre alle misure di carattere preventivo a cui dianzi si è fatto cenno, appare necessario dotare le istituzioni di adeguati strumenti normativi, introducendo nell'ordinamento il reato di furto di identità digitale, prevedendo adeguate sanzioni penali.

### *1.2 Le minacce al* Cloud computing

Gli attacchi informatici possono essere finalizzati, come accennato in precedenza, anche a carpire informazioni diverse dall'identità digitale o a pregiudicare il funzionamento stesso della rete, ostacolando l'erogazione dei servizi.

In questo quadro, particolare attenzione va posta al *Cloud computing* che è rappresentato dall'insieme di tecnologie che permettono, tipicamente come forma di servizio offerto al cliente da un *provider*, di memorizzare, archiviare ed elaborare dati grazie all'utilizzo di risorse *hardware* o *software* distribuite in rete. Il paradigma alla base della logica del *Cloud computing* è quello di offrire su richiesta l'accesso a risorse informatiche geograficamente distribuite, rendendole disponibili sotto forma di servizi al consumo, secondo il modello tipico del *pay-per-use*.

A seconda del tipo di servizio che viene erogato si possono distinguere tre differenti tipologie di *Cloud computing*, con tre livelli crescenti di complessità.

Il primo è quello del *software service*, in cui le applicazioni vengono erogate come servizio in *cloud* (*Software as a Service)*. In tale situazione, nel *cloud* l'utente è soltanto un consumatore: non gestisce nulla direttamente, né le applicazioni, né i dati. Ha soltanto a disposizione alcune funzionalità e ha la possibilità di raggiungere su richiesta servizi applicativi.

Il secondo è quello delle piattaforme, per cui il *cloud* eroga la piattaforma tecnologica su cui il cliente sviluppa, testa ed esegue eventualmente le proprie applicazioni (*Platform as a Service)*. In tal caso gli aspetti di attenzione concernono principalmente le modalità di trattamento dei dati: il *provider* espone e manutiene una piattaforma che viene messa a disposizione dell'utente; a gestire i dati e le applicazioni su tale piattaforma è tuttavia l'utente stesso.

Il terzo è quello delle infrastrutture, che consiste nel mettere a disposizione dei clienti infrastrutture configurabili, come per esempio macchine e reti virtuali o *storage,* ossia dispositivi *hardware* o supporti per la memorizzazione *(Infrastructure as a Service)*. In tale situazione particolare attenzione dovrebbe essere dedicata alle modalità di memorizzazione, archiviazione e conservazione dei dati: il *provider* mette a disposizione nel *cloud* un'infrastruttura nella quale gli utilizzatori possono memorizzare i loro dati o applicazioni. In tal caso il fornitore dei servizi detiene la responsabilità del funzionamento della rete, del suo accesso, dell'*hardware* eccetera.

Anche se non vi sono particolari criticità di natura tecnica, a oggi in Italia la diffusione del *Cloud computing* è ancora molto parziale e il *trend* di crescita appare inferiore rispetto a quello di altri Paesi. Le maggiori criticità che si registrano in questo settore riguardano innanzitutto il quadro normativo piuttosto incerto, con riferimento anche alla difficoltosa valutazione di possibili ricadute per quanto riguarda la normativa europea in materia di *privacy* e la non piena disponibilità di connessioni a banda larga in tutto il Paese, a causa del cosiddetto *digital divide*.

Inoltre, il *cloud* può rappresentare anche un fattore di rischio importante ai fini della sicurezza della rete, in quanto, ove venisse trasformato in una base d'attacco informatico, potrebbe portare a danni molto diffusi e amplificati. L'utilizzo di infrastrutture *cloud* per compiere attacchi DDoS (*Distributed Denial of Service)*, ossia volti ad impedire il corretto funzionamento di un sistema, occupando tutte le sue risorse – ad esempio attraverso l'invio massivo di *spam* – avrebbe un impatto amplificato proprio dall'infrastruttura stessa.

Il *cloud* è quindi una forma di esternalizzazione *dell'Information Technology* che può portare a conseguire economie di scala nell'erogazione dei servizi, ma può anche trasferire alcune categorie di rischio dal cliente al fornitore. La mitigazione di tali rischi può avvenire su due fronti, dal lato del fornitore che eroga il servizio e dal lato del fruitore.

Dal primo punto di vista la protezione dei sistemi deve avvenire con riferimento all'intensificazione dell'attività di monitoraggio e di aggiornamento dei processi di *incident response*, nonché di integrazione e di monitoraggio dei servizi erogati attraverso il *cloud* con processi di sicurezza, impiego di politiche, procedure e strumenti di sviluppo sicuro in accordo a *best practice* internazionali. Inoltre appare necessario l'aggiornamento tempestivo dei sistemi e delle applicazioni servite dal *cloud* rispetto a potenziali vulnerabilità individuate sulle infrastrutture del supporto. Si può intervenire anche sulle certificazioni previste, nonché sul miglioramento dell'interfaccia verso il cliente fruitore, con riferimento, per esempio, all'utilizzo di protocolli sicuri per l'integrazione.

Per quanto riguarda la mitigazione dei rischi dal lato del cliente fruitore, gli interventi possibili possono riguardare lo studio di fattibilità preliminare per individuare applicazioni, sistemi e dati adatti alla migrazione sul *cloud*. Ad esempio, potrebbero essere esternalizzate in un'ottica *cloud* le applicazioni e/o piattaforme che si riferiscono ad *asset* non strategici e a informazioni aziendali non particolarmente sensibili o confidenziali, o comunque a informazioni per le quali non è necessario mantenere una *governance* stretta.

A livello generale, non si evidenziano particolari criticità di una gestione in *cloud* attraverso un s*ervice provider*, pur essendo fondamentale definire a livello contrattuale alcuni aspetti, quali ad esempio: i livelli di servizio offerti e garantiti; la disponibilità, riservatezza e integrità dei dati, la trasparenza nel trattamento dei dati da parte del s*ervice provider*; la conoscenza della localizzazione dei *data center*; la condivisione di procedure in termini di sicurezza degli accessi, eccetera.

Con riferimento al tema del *Cloud computing* sono stati prodotti, nel corso del 2011, due significativi documenti da parte di amministrazioni pubbliche: il quaderno Consip « *Cloud Security*: una sfida per il futuro », concepito come strumento di approfondimento e di orientamento, e la scheda di documentazione del Garante per la protezione dei dati personali « *Cloud computing*: indicazioni per l'utilizzo consapevole dei servizi », che mira a contribuire all'aumento della conoscenza dei temi rilevanti per la sicurezza nell'utilizzo dei servizi *cloud*. A questi due documenti si sono poi aggiunte le raccomandazioni e le proposte sull'utilizzo del *Cloud computing* nella

pubblica amministrazione elaborate da DigitPA. In tutti questi casi si insiste sulla necessità di un'attenta regolamentazione dei servizi *cloud* nel contesto governativo, tale da fornire suggerimenti e indicazioni a tutti gli altri comparti nazionali.

### *1.3 Le minacce alle reti* wired *e* wireless

Le reti di telecomunicazioni realizzate da organismi pubblici o privati hanno assunto nel corso del tempo un'importanza crescente.

Nell'ambito delle pubbliche amministrazioni lo sviluppo delle reti informatiche risale all'inizio degli anni Novanta con l'istituzione della Rete Unitaria della Pubblica Amministrazione (RUPAR), che ha condotto, nel corso degli anni, alla realizzazione del più avanzato Sistema Pubblico di Connettività. Il Codice dell'amministrazione digitale definisce il Sistema Pubblico di Connettività come « l'insieme di infrastrutture tecnologiche e di regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione ». Il coordinamento del sistema, svolto fino al 2012 da DigitPA, è stato ora ereditato dall'Agenzia per l'Italia digitale istituita dal decreto-legge n. 83 del 2012.

Nel settore privato, invece, va ricordata, innanzitutto, la rete a banda larga realizzata da Poste italiane, che si affianca alla sua tradizionale infrastruttura fisica, collegando 11 mila uffici postali. Inoltre nel campo della logistica merita particolare attenzione la rete in corso di realizzazione da parte di UIRnet, società partecipata da soggetti pubblici come le autorità portuali e le società che gestiscono interporti, che si configura come una infrastruttura di comunicazione digitale per lo scambio di informazioni destinata agli operatori della logistica, ai fini dell'efficientamento del trasporto e della distribuzione delle merci. Infine, all'interno del settore bancario si evidenzia, a livello di sistema, una dotazione diffusa di un'infrastruttura di rete in grado di supportare adeguatamente l'operatività bancaria, sia nei rapporti con la clientela sia nei rapporti interbancari.

L'efficienza e la sicurezza della rete hanno un impatto considerevole sulla qualità dei servizi. Nel corso del tempo, quindi, gli operatori coinvolti hanno sviluppato misure di protezione della rete sempre più forti, che richiedono significativi investimenti. In questo quadro, va segnalato, in primo luogo, il sistema di allarme realizzato dal Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) che fa capo alla polizia postale. Il sistema coinvolge, attraverso una rete di collegamento, numerosi enti pubblici e privati, tra cui Poste italiane e molte banche, consentendo di allertare immediatamente tutti gli enti interessati in caso di attacco informatico sferrato ad uno di essi, al fine di consentire loro di adottare tempestivamente le necessarie contromisure.

La rete realizzata da Poste italiane, inoltre, è dotata di 5 *data center*, che garantiscono anche il *Disaster Recovery*, vale a dire l'insieme di misure tecnologiche e organizzative/logistiche atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi, a fronte di gravi emergenze che ne intacchino la regolare attività, anche al fine assicurare la continuità operativa dell'azienda *(Business Continuity)*.

Per quanto riguarda il settore bancario, infine, in tema di continuità operativa di reti e infrastrutture critiche, dalle rilevazioni svolte nel 2009 dall'Osservatorio *Business Continuity* di ABI-Lab, emerge come la totalità delle banche intervistate si sia dotata di un piano di continuità operativa al proprio interno, mentre il 95 per cento delle stesse abbia previsto un piano di *Disaster Recovery* e il 90 per cento abbia individuato un responsabile interno dello stesso piano, evidenziando un elevato livello di efficienza in relazione ai processi critici interni alle diverse strutture bancarie. Tuttavia, ulteriori analisi effettuate negli anni passati nello stesso settore bancario hanno rivelato come, con riferimento al rapporto con alcuni fornitori qualificati, in particolare, con gli operatori di telecomunicazioni, la condivisione delle informazioni sui piani di continuità operativa e di *Disaster Recovery* avvenga con criticità, evidenziando come sia opportuno normare più nel dettaglio il rapporto con i predetti fornitori. In particolare, l'esperienza passata ha evidenziato come, nel verificarsi di eventi catastrofici che hanno compromesso la normale operatività della banca, si siano riscontrate difficoltà di gestione della crisi, riconducibili in linea di massima a una non corretta condivisione dei rispettivi piani di continuità operativa tra i diversi attori coinvolti. Da ciò nasce l'esigenza di disciplinare, sotto il profilo normativo, adeguate strategie e politiche di continuità operativa e *Disaster Recovery* anche nei riguardi degli operatori di telecomunicazioni, nonché di regolamentare le procedure e le azioni di blocco che possono essere effettuate da *provider* di servizi Internet e operatori di telecomunicazioni in caso di accessi a siti sospetti, transazioni e comunicazioni anomale.

Sotto il profilo operativo, va segnalato come l'Italia abbia partecipato alle principali esercitazioni sulla sicurezza cibernetica fin qui svolte a livello internazionale, al fine di aumentare il grado di cooperazione tra i partecipanti nella gestione di una crisi cibernetica. Si pensi, ad esempio, alla prima esercitazione paneuropea *CyberEurope* 2010, all'esercitazione UE-USA *Cyber Atlantic 2011* nonché l'esercitazione *CyberEurope* 2012 che, rispetto alla prima edizione, si è caratterizzata per la partecipazione anche di soggetti privati, come Telecom Italia, oltre che di pubbliche amministrazioni.

## 2. Il quadro normativo europeo

Negli ultimi anni l'Unione europea ha manifestato una crescente attenzione al tema della sicurezza informatica delle reti.

Dal 2004, infatti, l'Unione si è dotata di un'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), a cui è affidato il

compito di analizzare i rischi attuali ed emergenti al fine di contribuire ad assicurare un elevato livello di sicurezza delle reti e dell'informazione nell'Unione e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione a vantaggio dei cittadini, dei consumatori, delle imprese e delle pubbliche amministrazioni. Due ulteriori importanti iniziative sono state poi assunte dall'Unione nel 2009.

Si è trattato, in primo luogo, della Comunicazione della Commissione europea COM(2009)149 definitivo sulla protezione delle infrastrutture critiche informatizzate, che ha prospettato la necessità dell'adozione di un piano di azione CIIP (*Critical Information Infrastructure Protection)*. In questo quadro le infrastrutture critiche informatizzate sono state definite come quelle infrastrutture concernenti le tecnologie dell'informazione e della comunicazione la cui perturbazione o distruzione appare suscettibile di determinare gravi ripercussioni su funzioni vitali della società. Tra le iniziative del piano di azione CIIP rientra la costituzione del Forum europeo degli Stati membri, istituito nello stesso 2009 e sostenuto dall'ENISA, quale sede di confronto e discussione nell'ambito degli Stati membri, con l'obiettivo di promuovere i contatti e la cooperazione tra attori pubblici e privati.

In secondo luogo, è stata adottata la direttiva 2009/140/CE in base alla quale gli Stati membri sono chiamati ad assicurare che le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico adottino adeguate misure di natura tecnica e organizzativa per gestire i rischi per la sicurezza delle reti e dei servizi e garantire l'integrità delle loro reti e la continuità della fornitura dei servizi su tali reti. Inoltre, gli Stati membri assicurano che le imprese che forniscono reti pubbliche di comunicazioni o servizi di comunicazione elettronica accessibili al pubblico comunichino all'autorità nazionale di regolamentazione competente ogni violazione della sicurezza o perdita dell'integrità che abbia avuto conseguenze significative sul funzionamento delle reti o dei servizi. Viene inoltre previsto che, se del caso, l'autorità nazionale interessata informi le autorità nazionali degli altri Stati membri e l'ENISA.

Successivamente, nell'ambito della Comunicazione COM(2010)245 definitivo/2 sull'Agenda digitale europea, la Commissione ha prospettato l'esigenza della costituzione di *Computer Emergency Response Team (CERT)*, ossia squadre per la risposta ad emergenze informatiche, di livello nazionale; la cooperazione tra i vari CERT nazionali degli Stati membri dell'Unione; l'istituzione di un CERT europeo. A tale proposito l'ENISA ha stabilito una *roadmap* in vista dell'integrazione dei sistemi nazionali di condivisione delle informazioni e di allarme.

Anche la già citata Comunicazione COM(2011)163 definitivo della Commissione europea, concernente il piano d'azione CIIP 2011, si sofferma sull'importanza di un rafforzamento della cooperazione tra gli Stati membri e il settore privato a livello nazionale, europeo e internazionale. La comunicazione è stata oggetto di dibattito nell'ambito della Conferenza ministeriale sulla protezione delle infrastrutture critiche di Balatonfüred del 14-15 aprile 2011, le cui indicazioni sono state recepite nelle Conclusioni del Consiglio telecomunicazioni del-

l'Unione del 27 maggio 2011. In tale documento il Consiglio ha invitato gli Stati ad intraprendere una serie di azioni tra le quali rientra, oltre alla costituzione di CERT nazionali, l'adozione di una strategia di sicurezza informatica nazionale, l'elaborazione di piani di emergenza nazionali, l'organizzazione di esercitazioni nazionali e la partecipazione ad esercitazioni europee. Con riferimento a tale ultimo aspetto nel periodo 2010-2011 si sono svolte le tre esercitazioni a cui si è fatto cenno in precedenza.

Da ultimo, per quanto concerne il tema specifico dell'identità digitale, è in discussione presso le istituzioni dell'Unione europea, la proposta di regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (COM(2012)238) di cui si è detto in precedenza.

## 3. Il quadro normativo nazionale

Nell'esaminare il quadro normativo nazionale è opportuno innanzitutto menzionare quali sono i principali soggetti istituzionali che, ai sensi della disciplina vigente, si occupano della sicurezza informatica delle reti. Si tratta, in particolare, dei seguenti soggetti:

– la Presidenza del Consiglio dei ministri, tramite il Dipartimento informazioni per la sicurezza, ai fini della valutazione della minaccia e l'Ufficio del Consigliere militare del Presidente del Consiglio dei ministri;

– il Ministero dell'interno, per la tutela dell'ordine e della sicurezza pubblica e il contrasto al crimine informatico e per la difesa civile. Presso il Dipartimento di pubblica sicurezza, in particolare, opera la polizia postale, con compiti di contrasto al crimine informatico e alla pedopornografia *on line*, nonché di tutela del diritto di autore sul *web*. La polizia postale opera attraverso due centri nazionali: il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC) e il Centro nazionale per il contrasto alla pedopornografia sulla rete Internet (CNCPO);

– il Ministero della difesa, per la difesa dello Stato e la sicurezza delle reti e dei sistemi facenti capo al settore della Difesa;

– il Ministero dello sviluppo economico, per la sicurezza delle reti e la tutela delle comunicazioni elettroniche;

– il Ministero degli affari esteri, per le attività internazionali.

Inoltre, tra il 2011 e il febbraio 2012, ha operato presso la Presidenza del Consiglio dei ministri un gruppo di studio per la sicurezza dell'utilizzo dello spazio cibernetico con l'obiettivo di: effettuare la ricognizione delle strutture esistenti presso le varie amministrazioni in relazione alle rispettive competenze, valutando l'adeguatezza delle stesse rispetto alle potenzialità delle minacce; individuare gli assetti organizzativi realizzati in altri Paesi, con particolare riguardo a quelli facenti parte dell'Unione europea, della

NATO e del G8; formulare una proposta organizzativa per mettere a sistema le strutture nazionali esistenti.

Infine, sempre in ambito nazionale operano due CERT istituzionali: il CERT-SPC (Sistema Pubblico di Connettività), istituito presso DigitPA (ora Agenzia per l'Italia digitale), rivolto agli utenti delle pubbliche amministrazioni e il CERT-DIFESA istituito presso lo Stato maggiore della difesa, con il compito di servire gli utenti della Difesa.

Dal punto di vista normativo, il quadro di riferimento, oltre al Codice dell'amministrazione digitale a cui si è fatto cenno in precedenza, è rappresentato dal Codice delle comunicazioni elettroniche di cui al decreto legislativo 1° agosto 2003, n. 259, come da ultimo modificato dal decreto legislativo n. 70 del 2012, con il quale è stata recepita la già citata direttiva 2009/140/CE. Con tale ultimo intervento normativo, è stata affidata al Ministero dello sviluppo economico, l'individuazione di misure minime di sicurezza di natura tecnica ed organizzativa che gli operatori di rete ed i fornitori di servizi di comunicazione elettronica sono tenuti ad adottare per gestire adeguatamente i rischi. La verifica del rispetto delle misure compete al medesimo Ministero, o ad un organismo indipendente da esso incaricato, che può applicare sanzioni in caso di violazioni o di inadempimenti alle norme. Al fine di tale verifica, le imprese sono tenute a fornire al Ministero le informazioni necessarie. Le segnalazioni degli incidenti di sicurezza sono indirizzate dagli operatori al Ministero che provvede a comunicarle, su base annuale o quando lo richieda, alla Commissione europea ed all'ENISA.

Il medesimo decreto legislativo n. 70 del 2012 ha previsto poi l'istituzione di un CERT nazionale presso il Ministero dello sviluppo economico, con il compito di svolgere un ruolo di coordinamento degli altri CERT istituzionali e privati verso il CERT europeo. Infatti, i due CERT esistenti in Italia e sopra richiamati, quello del sistema pubblico di connettività e quello Difesa, non rispondono ai requisiti previsti dall'Unione europea in quanto sono rivolti a specifiche utenze – le pubbliche amministrazioni, nel primo caso, il settore della difesa, nel secondo – e non alla generalità dei cittadini e delle imprese.

In particolare, il CERT nazionale è chiamato a: effettuare il monitoraggio delle vulnerabilità e l'osservazione dei comportamenti ostili registrati in rete; predisporre un sistema articolato di comunicazione mediante avvisi e segnalazioni delle emergenze; predisporre e impiegare procedure di coordinamento, in occasione del verificarsi di incidenti informatici; interagire con una pluralità di interlocutori omologhi per funzioni, al fine di verificare i dati ottenuti; migliorare i meccanismi e le misure di protezione sulla base degli incidenti avvenuti.

Infine, con riferimento all'identità digitale merita ricordare il recente decreto legislativo 28 maggio 2012, n. 69, di recepimento della direttiva 2009/136/CE, che ha modificato il codice in materia di protezione dei dati personali. In particolare, è stato introdotto nel codice l'obbligo per le imprese fornitrici di servizi di comunicazione elettronica accessibili al pubblico di notificare sollecitamente al Garante per la protezione dei dati personali ogni avvenuta violazione

di dati personali. Tale comunicazione si deve rivolgere anche al contraente del servizio o altra persona qualora la violazione dei dati personali rischi di arrecare pregiudizio ai loro dati personali e alla riservatezza.

**Conclusioni**

Negli ultimi anni l'emergere di notevoli problemi di sicurezza e di affidabilità della rete soprattutto per quanto concerne le transazioni in moneta elettronica ha reso sempre più pressante l'esigenza di costruire un ambiente digitale sicuro che offra a tutti i cittadini nuove possibilità e prospettive di sviluppo. Si tratta di un obiettivo da realizzare con assoluta priorità, giacché il numero delle minacce e delle violazioni della sicurezza ha già provocato notevoli danni economici, riducendo la fiducia degli utenti nell'utilizzo delle nuove tecnologie e ostacolando lo sviluppo del commercio elettronico.

Ai fini della presente indagine conoscitiva, tra le minacce che appaiono più significative per la sicurezza della rete figurano quelle consistenti nel furto dell'identità digitale e quelle rivolte ai *Cloud computing* e alle reti *wired* e *wireless* facenti capo a organizzazioni pubbliche o private.

Per quanto riguarda il furto dell'identità digitale, tutti i soggetti coinvolti nel processo di utilizzo delle identità digitali, si trovano a dover gestire, per la parte di rispettiva competenza, alcune informazioni che possono essere oggetto di attacchi informatici volti ad intercettare, modificare o rendere non disponibili le informazioni in transito. Le criticità che possono manifestarsi vanno pertanto considerate sull'intero processo di gestione, nel loro insieme, al fine di mitigare il rischio complessivo di tutti gli attori coinvolti dall'*identity provider*, all'erogatore del servizio fino ad arrivare all'utente finale.

In questo quadro, dovrebbe essere valutata l'opportunità di individuare un *identity provider* nazionale ovvero di promuovere la realizzazione di una federazione degli *identity provider* per garantire la circolarità dell'identificazione, a prescindere dallo strumento operativo utilizzato, su tutto il territorio nazionale, consentendo al cittadino di operare con un'unica identità digitale.

Inoltre, gli strumenti di autenticazione dovrebbero essere concepiti in modo da trovare un giusto compromesso tra la facilità di accesso e il livello di protezione, fermo restando che la protezione più affidabile è quella che prevede non solo l'inserimento di *username* e *password*, ma anche l'autenticazione dell'utente attraverso l'impiego di sistemi *one-time-password*, *smart card* o addirittura di sistemi biometrici.

Risulta altresì necessario incrementare e facilitare l'utilizzo di strumenti innovativi da parte degli utenti finali con una piena consapevolezza delle caratteristiche di tali strumenti e, quindi, anche dei loro rischi. In questa prospettiva, si dovrebbe, quindi, intervenire, sulla scia dell'obiettivo indicato tra le priorità dell'Agenda digitale europea, con azioni di sensibilizzazione molto forti, con particolare riguardo ai minori, attraverso una campagna di comunicazione allargata, continuativa, intersettoriale e coordinata centralmente da un

organo governativo. In particolare, per quanto riguarda i minori, si dovrebbe promuovere la loro formazione attraverso percorsi educativi in grado di fornire, fin dai primi livelli scolastici, le competenze necessarie.

Infine, per combattere efficacemente il furto di identità digitale, oltre alle misure di carattere preventivo a cui dianzi si è fatto cenno, appare necessario dotare le istituzioni di adeguati strumenti normativi, introducendo nell'ordinamento il reato di furto di identità digitale, prevedendo adeguate sanzioni penali.

Per quanto attiene al *Cloud computing*, in Italia la sua diffusione è ancora molto parziale e il *trend* di crescita appare inferiore rispetto a quello di altri Paesi. Il *Cloud* può rappresentare un fattore di rischio importante ai fini della sicurezza della rete, in quanto, ove venisse trasformato in una base d'attacco informatico, potrebbe portare a danni molto diffusi e amplificati.

La mitigazione di tale rischio può avvenire su due fronti, dal lato del fornitore, attraverso l'intensificazione dell'attività di monitoraggio e di aggiornamento dei processi di *incident response* nonché mediante l'integrazione dei servizi erogati attraverso il *cloud* con processi di sicurezza, e dal lato del fruitore, individuando applicazioni, sistemi e dati adatti alla migrazione sul *cloud*, come per esempio quelli che attengono ad informazioni per le quali non è necessario mantenere una *governance* stretta.

Nel caso di gestione in *cloud* attraverso un *service provider*, appare necessario definire a livello contrattuale alcuni aspetti, quali ad esempio: i livelli di servizio offerti e garantiti; la disponibilità, riservatezza e integrità dei dati; la trasparenza nel trattamento dei dati da parte del *service provider*; la conoscenza della localizzazione dei *data center*; la condivisione di procedure in termini di sicurezza degli accessi, eccetera.

Infine, per quanto concerne l'utilizzo del *Cloud computing* nella pubblica amministrazione appare necessaria un'attenta regolamentazione dei servizi *cloud* nel contesto governativo, tale da fornire suggerimenti e indicazioni a tutti gli altri comparti nazionali.

Per quanto riguarda le reti *wired* e *wireless*, si evidenzia come le reti di telecomunicazioni realizzate da organismi pubblici o privati, abbiano assunto nel corso del tempo un'importanza crescente. Si pensi, ad esempio, nel settore pubblico al Sistema Pubblico di Connettività e nel settore privato alla rete a banda larga realizzata da Poste italiane – che si affianca alla sua tradizionale infrastruttura fisica, collegando 11 mila uffici postali – alla rete in corso di realizzazione da parte di UIRnet, destinata agli operatori della logistica, e alla rete diffusa nel settore bancario in grado di supportare adeguatamente l'operatività bancaria, sia nei rapporti con la clientela sia nei rapporti interbancari.

In proposito, appare necessario disciplinare, sotto il profilo normativo, adeguate strategie e politiche di continuità operativa e *Disaster Recovery*, anche nei riguardi degli operatori di telecomunicazioni, nonché regolamentare le procedure e le azioni di blocco che possono essere effettuate da *provider* di servizi Internet e operatori di telecomunicazioni in caso di accessi a siti sospetti, transazioni e comunicazioni anomale.

Più in generale, ai fini della sicurezza della rete, ferma restando l'esigenza di proseguire lungo la strada della cooperazione tra Stati e tra operatori pubblici e privati, come emerso nelle Conclusioni del Consiglio telecomunicazioni dell'Unione del 27 maggio 2011, appare necessario intraprendere una serie di azioni tra le quali merita segnalare, oltre alla costituzione di squadre di livello nazionale per la risposta ad emergenze informatiche (CERT nazionali), l'adozione di una strategia di sicurezza informatica nazionale, l'elaborazione di piani di emergenza nazionali, l'organizzazione di esercitazioni nazionali e la partecipazione, come già avvenuto nel recente passato, ad esercitazioni europee.

DOC16-17-26
€ 2,00