*La collaborazione tra imprese per la sicurezza informatica**

di **GIAN DOMENICO MOSCO**

SOMMARIO: **1.** LE DOMANDE. – **2.** I FATTORI RILEVANTI PER LA *CYBER SECURITY* DELLE IMPRESE: L'OPPORTUNITÀ DI UNA RISPOSTA IN *POOL*. – **3.** GLI STRUMENTI PER LA COLLABORAZIONE TRA IMPRESE: CONSORZI E CONTRATTO DI RETE. – **4.** IL CONSORZIO COME ALTERNATIVA ALL' *OUTSOURCING*. **5.** – *INFORMATION SHARING* E RAPPORTO TRA PUBBLICO E PRIVATO. – **6.** L'INFLUENZA DELL'INTELLIGENZA ARTIFICIALE SULLA *CYBER SECURITY*.

Abstract

The complexity and costs linked with *Cyber Security* represent real obstacles for businesses, especially the smaller ones. One way to overcome them is to cooperate in order to create information technology security systems. In Italy two different tools may be used for this goal: the *contratto di rete* (network contract) and, to a greater degree, consortiums.
Information sharing however requires a public intervention. A step in this direction has been undertaken by the EU, with the NIS directive 1148/2016 which paves the road for cooperation between public institutions and the private sector, mainly companies.
Artificial intelligence will interfere more and more with cyber security, generating risks and opportunities, which can already be foreseen.

1. Le domande. In questo breve intervento vorrei pormi tre domande e cercare di dar loro una prima risposta.

La prima e principale domanda è la seguente: le imprese per elevare i livelli di sicurezza informatica devono muoversi necessariamente da sole o vi sono ragioni – e si dispone di strumenti – per incrementare la *Cyber Security* attraverso forme di collaborazione e condivisione tra loro?

La seconda domanda riguarda più specificamene l'*Information Sharing* e il rapporto tra privato e pubblico alla luce, soprattutto, della direttiva 2016/1148 UE del luglio dell'anno scorso.

La terza e ultima domanda è: quale influenza avrà sulla *Cyber Security* il diffondersi dell'intelligenza artificiale e, se la avrà, sarà positiva o negativa?

2. I fattori rilevanti per la *Cyber Security* delle imprese: l'opportunità di una risposta in *pool*. Per cercare di rispondere alla prima domanda vorrei ricordare anzi tutto alcuni fattori di carattere sia generale, sia specifico che assumono rilievo ai fini della sicurezza informatica delle nostre imprese.

Il primo è che il nostro sistema imprenditoriale è notoriamente costituito soprattutto da PMI.

Per l'ISTAT le imprese fino a 10 dipendenti (le c.d. micro imprese) sono il 95% del totale (dati 2015). Per Confindustria e CERVED (rapporto PMI 2016) tra le sole società di capitali ed escludendo sia le grandi, sia le micro imprese si contano circa 112 mila piccole imprese (<50 addetti e fino a 10 milioni di euro di fatturato o attivo) e quasi 24 mila medie imprese (23.736) (< 250 addetti e fino a 150 milioni di euro di fatturato o 43 milioni di attivo).

La grandissima parte delle micro e delle piccole imprese ha difficoltà nel disporre di risorse economiche e organizzative sufficienti per consolidarsi, innovare, crescere.

Sotto il profilo della sicurezza informatica, le imprese minori sono un bersaglio privilegiato degli attacchi informatici, sia *random*, sia mirati, e per loro le conseguenze negative sono in proporzione ancora maggiori che per le grandi poiché il dato dimensionale accentua l'asimmetria informativa della vittima rispetto all'attaccante, in quanto per queste imprese è più difficile dotarsi di un sistema di protezione e così reagire ai danni, economici e reputazionali, causati da una violazione informatica.

Una ragione, forse la più importante, di questo stato di cose è rappresentata dai costi della sicurezza informatica, il secondo fattore da ricordare.

Il *Cybersecurity Report 2016* realizzato dal CIS-Sapienza e dal Laboratorio Nazionale di *Cybersecurity*, che rappresenta una tappa fondamentale del percorso evolutivo di sicurezza informatica per le nostre p.m.i., ha operato una difficile semplificazione del sistema dei controlli (il *Framework Nazionale di Cybersecurity* delineato dal *Cybersecurity Report*

2015), riuscendo a selezionare 15 misure protettive che possono definirsi «essenziali» per resistere, quanto meno, agli attacchi più comuni. Si tratta, in sostanza, di un sistema difensivo minimale ma imprescindibile.

Anche puntando a realizzare solo questo sistema difensivo di base i costi sono significativi, secondo il Rapporto stimabili in circa 41.000 euro in 5 anni per una micro impresa, in poco più di 100.000 euro nello stesso periodo per una media impresa, ricompresi in questa forbice (41-100) per una piccola impresa.

Il terzo fattore è la consapevolezza, messa in luce dal *Framerwork* Nazionale per la *Cybersecurity* 2016 che, anche per le imprese maggiori, una risposta di sicurezza informatica è bene che non sia in *outsourcing*, ma affrontata all'interno dell'impresa come espressione di una propria cultura di gestione del rischio *cyber*, la sola che può assicurare risultati ottimali.

Infine, va ricordato che sempre il Rapporto 2016 del CIS Sapienza sottolinea che molti attacchi informatici a grandi impese passano attraverso le PMI della loro filiera produttiva, fornitrici di beni e servizi.

In conclusione, ci sono diverse ragioni – dimensioni delle impese, costi della sicurezza, inconvenienti della esternalizzazione, trasmissibilità lungo la filiera degli attacchi – che spingono nella direzione di una risposta in *pool* ai problemi di sicurezza informatica delle imprese, certamente di quelle più piccole ma anche, con loro, di quelle grandi o medie al vertice di una filiera.

3. Gli strumenti per la collaborazione tra imprese: consorzi e contratto di rete. Per agevolare il diffondersi della sicurezza informatica tra le imprese va dunque incentivata la collaborazione tra imprese.

Non mancano nel nostro ordinamento gli strumenti, contrattuali e organizzativi, utilizzabili dalle imprese per collaborare e affrontare senza ulteriori rinvii la questione della sicurezza informatica con costi accettabili, realizzando un sistema di controlli *cyber* che risponda almeno al modello "essenziale" delineato dal *Cybersecurity Report 2016*.

Due sono gli strumenti d'elezione per la collaborazione tra imprese che già hanno un'ampia diffusione, specie tra le piccole e medie imprese.

Anzi tutto, il consorzio tra imprenditori. Si tratta di uno strumento che prevede l'istituzione di un'organizzazione comune e che lascia ampio spazio all'autonomia contrattuale nel configurare la *governance* secondo le concrete esigenze delle imprese. Il codice civile prevede infatti un ordinamento interno corporativo, con un organo di tipo assembleare e uno di gestione, ma fortemente semplificato rispetto a quello di una società di capitali o cooperativa.

Allo stesso tempo il consorzio con attività esterna beneficia della limitazione della responsabilità patrimoniale (art. 2615, comma 1, c.c.), senza particolari vincoli quanto a fondo comune (che non deve avere un ammontare minimo) e controlli interni ed esterni. Insomma, uno strumento agile, sufficientemente sicuro e ben collaudato (MOSCO, 2017).

Il secondo strumento, più recente, è il contratto di rete, una figura contrattuale introdotta dall'art. 3, comma 4-*ter*, della legge 9 aprile 2009, n. 33, di conversione del d.l. 10 febbraio 2009, n. 5, poi ripetutamente modificato dal legislatore.

Il ricorso al contratto di rete è consigliabile soprattutto se non si vuole dar vita a un nuovo soggetto di diritto (anche se possono essere costituite reti entificate), ma limitare la collaborazione sul versante C*yber Security* alla messa in comune di informazioni o alla predisposizione di strumenti di difesa regolati solo sul piano contrattuale istituendo, se occorre, un fondo e un rappresentante comune (IAMICELI, CAFAGGI, MOSCO, 2013)

In definitiva, uno strumento adatto, anche per via di una disciplina normativa non del tutto convincente, per una prima collaborazione, non troppo intensa e impegnativa.

4. Il conosorzio come alternativa all'*outsourcing*. Vorrei chiarire a questo punto perché ho incluso il superamento dell'*outsourcing* tra le ragioni che spingono verso network imprenditoriali nel campo della *Cybersecurity*.

Credo che ci sia una terza via tra una gestione interna del rischio informatico e una sua esternalizzazione: per l'appunto, il ricorso a un consorzio (o a una rete) che possano offrire un approccio culturale alla Cybersecurity e valutazioni e presidi di sicurezza analoghi alla prima, ma con risparmi anche superiori alla seconda.

Del resto, agire in *pool* può consentire di andare oltre alle «misure essenziali di sicurezza» per muovere con decisione lungo il «percorso virtuoso» ipotizzato dal Rapporto 2016 del CIS, mettendo in atto «norme di sicurezza via via più complesse e articolate». E questo non solo affidandosi ancora al consorzio o alla rete, ma anche affiancando al sistema di controllo «essenziale», condiviso con le altre imprese, misure difensive realizzate dalla singola impresa, più evolute e calibrate sul proprio profilo di rischio.

Se per le imprese più grandi il tema della *Cybersecurity* è ormai uno dei più importanti e ricorrenti tra quelli oggetto d'esame da parte dei consigli di amministrazione, è auspicabile che ogni imprenditore, ogni organo amministrativo avverta come ricompreso tra i propri doveri quello di predisporre un assetto organizzativo adeguato anche con riguardo alla sicurezza informatica.

5. *Information Sharing* e rapporto tra pubblico e privato. Vorrei ora provare a rispondere alla seconda domanda.

È evidente, anzitutto, che la condivisione delle informazioni in relazione ad attacchi e minacce informatiche è, forse, la prima tappa di un *network* di imprese, consentendo di avere più informazioni a minor costo, interne ed esterne alla rete, di realizzare archivi comuni, ovviamente con caratteri di neutralità concorrenziale e garanzia di riservatezza, di mettere in campo a costi condivisi analisti capaci di prevenire, sulla base delle esperienze del passato, gli attacchi del futuro (CONSORZIO CINI, 2015).

La C*yber Security* richiede però un campo d'azione dei «difensori» molto ampio e ben coordinato con un *Information Sharing* non lasciato solo a iniziative volontarie e circoscritte.

In questo senso mi pare vada, a livello europeo, la recente direttiva europea c.d. NIS – la 2016/1148 del 6 luglio 2016 – che chiede a ciascun stato membro di dotarsi di una strategia nazionale di C*ybersecurity* che definisca obiettivi strategici, politiche adeguate e misure di regolamentazione nonché uno o più *team* (c.d. CSIRT) responsabili del monitoraggio degli incidenti nazionali e che forniscano allarmi tempestivi e diffondano informazioni su rischi e incidenti.

Mi limito a ricordare che il funzionamento del sistema si basa proprio su un meccanismo di *Information Sharing* basato su un *obbligo* di notifica degli incidenti significativi a carico degli operatori di servizi essenziali (le imprese pubbliche o private che gestiscono le c.d. «infrastrutture critiche») e dei fornitori di servizi digitali (mercati on-line, servizi di cloud e motori di ricerca).

Vi è però anche la *facoltà* di notifica da parte delle altre imprese e degli utenti informatici, dunque su base volontaria, «degli incidenti aventi un impatto rilevante sulla continuità dei servizi da loro prestati», posto che la loro conoscenza può essere di pubblico interesse e che il loro trattamento non rappresenta necessariamente un onere sproporzionato o eccessivo.

La direttiva 2016/1148 valuta infatti le informazioni sugli incidenti «sempre più preziose per il pubblico in generale e per le imprese, in particolare le piccole e medie imprese» e incoraggia il segretariato della rete di CSIRT a gestire un sito o una pagina web per mettere a disposizione del pubblico le informazioni sui principali incidenti che si verificano nell'Unione, «con particolare attenzione agli interessi e alle esigenze delle imprese» (considerando 40).

6. L'influenza dell'intelligenza artificiale sulla *Cyber Security*. L'ultima questione sulla quale, come ho anticipato, vorrei interrogarmi, limitandomi a qualche considerazione assai semplice, è il ruolo dell'Intelligenza Artificiale con riguardo alla C*yber Security*.

Ormai è sicuro che sempre più attività saranno affidate alla I.A. e alla robotica. Già oggi, per fare solo qualche esempio, è noto che si usano algoritmi per lanciare notizie (così fanno, per esempio, Agenzie quali Reuters o

Associated Press), per valutare il merito creditizio o i candidati a un posto di lavoro, per costruire modelli predittivi di atti terroristici o identificare sui *social media* i profili dei possibili terroristi, per definire strategie di investimenti e, sempre più spesso, per effettuarli. Sperimentazioni e prime applicazioni, anche con robots e alcune già consolidate, si registrano nei campi della medicina e delle professioni, in alcuni paesi della stessa giustizia.

Sempre maggiore, allora, sarà il rischio di subire attacchi a sistemi che agiscono, nonostante il riferimento all'intelligenza, sia pure artificiale, su base automatica e non «intelligente», utilizzando degli algoritmi che possono essere falsati o mandati in tilt.

Ne deriva la necessità di aumentare i livelli di protezione dalle minacce informatiche lasciando un ruolo fondamentale alla I.U., agli uomini, perché, come da più parti si sottolinea, le decisioni fondamentali e il controllo dei sistemi digitali hanno bisogno dell'intelligenza umana, di una *vera* intelligenza.

Allo stesso tempo, è evidente che i sistemi di I.A. possono dare una grossa mano nella lotta ai pirati informatici attraverso lo sviluppo di algoritmi capaci di adattare il sistema alle dinamiche dell'ambiente nel quale operano e di tener conto dell'esperienza maturata, il c.d. *deep learning* (pure a sua volta, evidentemente, fonte di pericoli). Il che può consentire non solo di analizzare velocemente quantità enormi di dati, ma di anticipare gli attacchi informatici o almeno di rispondervi velocemente.

*Intervento al Convegno "*Cybersecurity: una sfida per trasformare un rischio in opportunità per le PMI*", organizzato a Roma il 25 maggio 2017 da UNINDUSTRIA.

Riferimenti bibliografici

F. CAFAGGI, P. IAMICELI E G.D. MOSCO [2012], *Gli ultimi interventi legislativi sulle reti*, in *Il contratto di rete per la crescita delle imprese*, a cura di F. Cafaggi, P. Iamiceli, G.D. Mosco, Milano, p. 489 ss.

CIS SAPIENZA E CONSORZIO CINI [2016], *2015 Italian Cyber Security Report. Un Framework Nazionale per la Cyber Security*, 4 febbraio 2016, disponibile all'indirizzo *www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf*

CIS SAPIENZA E CONSORZIO CINI [2017], *2016 Italian Cyber Security Report. I controlli essenziali di sicurezza in un ecosistema cyber nazionale*, 2 marzo 2017, disponibile all'indirizzo *www.cybersecurityframework.it/sites/default/files/csr2016web.pdf*

CONFINDUSTRIA E CERVED [2016], *Rapporto PMI 2016,* disponibile all'indirizzo *https://know.cerved.com/it/studi-e-analisi/rapporto-cerved-pmi-2016*
CONSORZIO CINI [2015], *Il futuro della Cyber Security in Italia. Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni*, aa cura di R. Baldoni e R. de Nicola, disponibile all'indirizzo *https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco*
ISTAT [2015], *Struttura e competitività del sistema delle imprese industriali e dei servizi – Report anno 2013*, 9 dicembre 2015, disponibile sul sito www.istat.it
G.D. MOSCO [2017], *Consorzi per il coordinamento della produzione e degli scambi*, in *Commentario del codice civile Scialoja-Branca-Galgano,* Bologna, 2017