Ricerca su "La Criminalità informatica e i rischi per l'economia e le imprese Italiane ed europee"

L'Istituto Interregionale per la Ricerca sul Crimine e la Giustizia (UNICRI), con il supporto dalla Cassa di Risparmio di Lucca, ha condotto una ricerca su "La Criminalità informatica e i rischi per l'economia e le imprese Italiane ed europee" .

I crimini informatici rappresentano oggi una delle minacce più insidiose. Questo fenomeno che nell'ultimo decennio ha avuto una forte crescita ha un costo per l'economia globale stimato tra i 375 e i 575 miliardi di dollari l'anno[1]. Secondo l'Interpol il costo dei crimini informatici in Europa avrebbe raggiunto i 750 miliardi[2] di euro all'anno.

L'impatto dei crimini informatici sull'economia dei paesi è enorme e non riguarda solo le grandi imprese, ma sempre più anche quelle di piccole e medie dimensioni (PMI). I crimini informatici sono un fenomeno trasversale che colpisce indiscriminatamente tutte le imprese, non solamente quelle del settore informatico o altamente specializzate.

La ricerca ha lo scopo di fornire un quadro sulle conseguenze economiche di questo fenomeno e una valutazione dei rischi e delle vulnerabilità delle piccole e medie imprese. Queste ultime, sono un pilastro della struttura economica e sociale europea e rappresentano il 99,9% delle imprese italiane.

La ricerca ha preso in esame l'impatto dei crimini informatici a livello internazionale, italiano e locale, attraverso un focus specifico sul territorio, interviste mirate e analisi di casi studio. Essa presenta altresì una panoramica degli strumenti attualmente più utilizzati dai criminali, le loro principali motivazioni e i maggiori rischi e vulnerabilità per le imprese. Le interviste con attori istituzionali ed imprese hanno consentito di gettare luce su aspetti chiave e di mettere a fuoco una strategia per una corretta definizione di programmi di prevenzione e contrasto alla criminalità informatica specificatamente indicati per le PMI.

La ricerca evidenzia:

- L'esigenza di investire in formazione è l'aspetto primario emerso in tutte le interviste così come la necessità di far fronte alle barriere culturali che riducono la consapevolezza dei rischi. La vulnerabilità creata dal fattore umano infatti viene considerata più pericolosa degli aspetti tecnici.
- I crimini informatici in sensibile aumento negli ultimi anni risultano essere quelli di tipo mirato, come lo *spear phishing*.
- È emersa la necessità di promuovere una maggiore conoscenza del fenomeno non solo tra gli informatici. Anche amministratori, titolari delle aziende e consigli di amministrazione dovrebbero essere informati al fine di promuovere contromisure e politiche concertate.

---

1 *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II Center for Strategic and International Studies June 2014*, in <http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf> (ultima consultazione 6-11-2014).

2 *Opening Remarks by INTERPOL PRESIDENT KHOO BOON HUI. At the 41ST EUROPEAN REGIONAL CONFERENCE (ISRAEL, TEL AVIV, 8 MAY 2012),* in <http://www.interpol.int/content/download/14086/99246/version/1/file/41ERC-Khoo-Opening-Speech.pdf> (ultima consultazione 10-11-2014).

- La totale mancanza di condivisione e collaborazione riscontrata tra le aziende evidenzia la necessità di creare network tra aziende dello stesso settore o delle stesse dimensioni, al fine di aumentarne il dialogo e la diffusione di buone prassi.

- Lo scenario investigativo e giudiziario delineato dalle interviste evidenzia che questo tipo di crimine è molto difficile da perseguire a causa del suo forte carattere transnazionale.

- La lotta ai crimini informatici necessita, oltre che di azioni legislative forti, di azioni da parte delle forze dell'ordine, di strumenti adeguati e cooperazione, ma soprattutto di una maggiore consapevolezza e conoscenza. Il fattore umano infatti è un elemento assolutamente determinate in questo tipo di criminalità, che spesso sfrutta tale vulnerabilità.

L'affidabilità in termini di sicurezza informatica delle PMI, soprattutto di quelle che operano nei distretti industriali rappresenta un significativo valore aggiunto per gli investitori e i clienti.

La vera frontiera da abbattere è quella culturale, infatti molte azioni difensive possono essere messe in atto anche a costi limitati. Oltre alle politiche di sicurezza interna è necessario incentivare la condivisione delle informazioni a più livelli. A livello preventivo, prima che si verifichi un attacco, la condivisione di buone prassi e informazioni sulle minacce con aziende della filiera, associazioni di categoria e forze dell'ordine può consentire di mettere in atto delle prime contromisure. A livello operativo, durante o dopo un attacco, la condivisione con attori preferenziali, quali forze dell'ordine e istituzioni finanziarie, può aumentare la resilienza del sistema e le capacità di mitigare i danni subiti.

Il carattere transnazionale dei crimini informatici richiede azioni a livello internazionale e nazionale. Nel 2013 l'Unione Europea ha adottato una strategia cibernetica, invitando gli Stati Membri a fare altrettanto. Nel 2014 anche l'Italia si è dotata di un Quadro strategico nazionale per la sicurezza dello spazio cibernetico.

Le azioni da mettere in campo per contrastare questo fenomeno devono essere volte a formare il più possibile l'utente e a favorire la condivisione delle informazioni. Le informazioni raccolte in questa ricerca hanno permesso di ideare e costruire un percorso basato sullo sviluppo di due progetti complementari.

Il primo progetto ha lo scopo di aumentare la conoscenza e la condivisione di informazioni su due diversi livelli aziendali e riguarda l'organizzazione di seminari, workshop e corsi di formazione differenziati, rivolti – da una parte - a decisori non tecnici, quali membri del consiglio di amministrazione e titolari delle imprese e al contempo agli informatici dell'azienda. La proposta mira a favorire la formazione di network per lo scambio di informazioni.

Il secondo progetto prevede la realizzazione di tavole rotonde tra attori specifici, come rappresentanti delle PMI nel settore merceologico, le forze dell'ordine, le associazioni di categoria, le università ed esperti legali. Lo scopo di questo progetto è non solo quello di condividere le informazioni sui rischi emergenti in ambito informatico ma anche quello di favorire l'individuazione di referenti per il settore merceologico delle piccole e medie imprese al fine di creare una rete che alimenti la conoscenza in questo settore e che possa diventare un esempio virtuoso per la prevenzione.

Attraverso la realizzazione di questi due progetti si promuove la creazione di network che possano promuovere una vera cultura della sicurezza, e al contempo offrire una garanzia di costante aggiornamento sulle buone prassi e di adattarsi a qualsiasi tipo di evoluzione del fenomeno registrandone i cambiamenti ed adeguandosi ad essi.