UIL CREDITO ESATTORIE
E ASSICURAZIONI

VIA LOMBARDIA 30 - 00187 ROMA - TEL. 06.4203591 - FAX 06.484704

Centro Studi Orietta Guerra
Aderente a UNI Global Union

NEL CYBERSPAZIO FINANZIARIO TRA

CYBERSECURITY E OCCUPAZIONE

a cura di Massimo Bramante

Novembre 2017

CYBERSECURITY E CRIMINALITA' INFORMATICA NEL MONDO DELLA FINANZA

La gestione della *Cybersecurity* delle infrastrutture critiche d'impresa è stata al centro dell'ultimo G7 Industria/ICT di Torino, dove si è convenuto che imprese industriali, commerciali e finanziarie italiane sono ancora molto indietro nel campo del contrasto attivo al *cyber crime* e più in generale, ai crescenti attacchi che si avvalgono delle non irrilevanti falle nei sistemi informatici d'impresa. E' necessario pertanto – a detta degli esperti – "*una strategia di difesa appropriata che deve formare alla cybersecurity industriale sia professionisti informatici sia gli impiegati comuni, per ridurre il gap di conoscenze del personale e mitigare il rischio di errori umani*"[1].E' un compito assai gravoso ma oggi indispensabile se si vuole procedere sulla via della difesa e della crescita della c.d. "*Data-Economy",* come banche ed assicurazioni proclamano ad ogni piè sospinto di voler fare. Come si è osservato in quella sede di discussione – è questo il momento di "*strutturare organizzazione e processi per supportare una rapida comprensione degli attacchi , creando un frame work onnicomprensivo per la gestione dei rischi operativi".*

Dovremo fare presto dunque, riconvertire risorse umane già presenti nei settori creditizio/assicurativo/esattoriale, trovarne delle nuove formatesi in Università o Istituti di ricerca italiana, anche attraverso forme di partnership pubblica/privato. Lo afferma, un attento studioso di tali problematiche, Luca de Biase, rilevando che *"robotica, intelligenza artificiale, big data, cloud computing, internet delle cose, sensoristica, cyber security hanno avuto un'accelerazione straordinaria a causa della scalabilità dei processi e dei servizi avviati nello straordinario ecosistema internettiano, fisso e mobile, rivolti agli utilizzatori"*[2]. Lo affermano gli esperti e lo confermano i numeri.

Recentemente i pirati informatici sono penetrati negli archivi di Equifax, importante società americana di valutazione dei crediti, ed hanno sottratto dati sensibili di 143 milioni di clienti, hanno avuto facile accesso ai numeri delle carte di credito di 209 mila consumatori ed ai profili riservati di altre 182 mila persone. Un danno enorme per la società privata, per chi vi lavora, per i clienti. Il titolo Equifax, il giorno dopo l'attacco, è crollato del 14 %[3]. L'attacco hacker ha dunque preso con una fava "avvelenata" due piccioni.

Gli istituti di credito e le compagnie assicurative sono oggi uno dei bersagli preferiti dagli hacker, lo sottolinea il Rapporto *Banking & Financial Services Cyber-security: US market 2015-2020, che* rileva come negli Stati Uniti la sicurezza dei servizi finanziari ha un costo di circa 9,5 miliardi di dollari e lo riconfermano le parole del technical consultant di Venustech, Long Junao, che evidenzia come una banca americana è stata oggetto di 30 mila attacchi in una sola settimana, uno quindi ogni 34 secondi!

E' pertanto assodato che "*gli attacchi contro le aziende di credito sono quelli che potenzialmente possono causare i maggiori danni, portando a risultati a volte davvero catastrofici…"*[4]. Parlano i numeri, più che le parole: "*Il costo medio di un attacco informatico continua a salire* – ha osservato Alessandro Livrea, esperto nella protezione informatica in campo assicurativo – *oggi è salito a 11 milioni di dollari, crescendo di oltre il 22 % rispetto ad un anno fa. In Italia il danno medio è di circa 6 milioni di euro* "[5]. Il sistema finanziario italiano è nell'occhio del ciclone, con un numero stimato di circa 35 mila computer aziendali infettati e ciò può seriamente compromettere la nostra competitività a livello internazionale[6].

E' urgente, per banche ed assicurazioni, dedicare alla *cyber security* non solo maggiori risorse economiche, come in parte stanno facendo, ma soprattutto risorse umane, rafforzando l'apparato interno di *intelligence* per individuare in modo tempestivo le nuove minacce, investendo in ricerca e formazione del personale. È cruciale comprendere che il riconoscimento dei nuovi attacchi e la conseguente difesa dagli stessi dipendono non solo dal *software* a disposizione ma anche dalla *expertise* interna, dalla qualità e, non da ultimo, dalla quantità dei dipendenti che operano in questo delicato settore, che richiede, pertanto, - come documenta l'*Osservatorio Information Security & Privacy* della School of Management del Politecnico di Milano – nuovi modelli organizzativi[7].

Sappiamo che Phishing, ransomware, intercettazione delle comunicazioni, furto d'identità, *fake news,* utilizzo indebito dei dati relativi a persone decedute, blocco delle aree di rete, accesso criptato e conseguente richiesta di riscatto attraverso bitcoin sono le "infezioni" che contaminano da tempo il *cyberspazio finanziario* ed è quindi necessario – per la UILCA – qualificare ed assumere personale per contrastarne la perniciosa diffusione.

Nei più accreditati studi sul fenomeno del *Cybercrime* (eNet Losses: *Estimating the Global Cost of CyberCrime*, 2014, come pure *The Economy Impact of CyberCrime and CyberEspionage,* 2013) emerge con forza che le organizzazioni internazionali specialistiche in crimini informatici non si limitano al solo trasferimento diretto di denaro dal conto di prelievo a quello di utilizzo, ma operano spesso con metodologie più raffinate che prevedono l'impiego di prestanome (*money-mules)* o d'intermediari (*financial manager*) che accolgono versamenti su conti correnti appositamente creati e che, in un secondo tempo, attraverso servizi di *money-transfer,* girano le somme carpite ad altri soggetti, trattenendo per sé una commissione[8]. E' stato il caso di due banche mediorientali che hanno subito un furto di 45 milioni di dollari a ragione dell'opera criminale di 500 *money-mules,* tra loro collegati, che hanno utilizzato carte di credito clonate ed hanno trasferito il denaro sul conto indicato dagli hacker, trattenendo una commissione di servizio, che hanno pagato banche, clienti e dipendenti bancari. Una banca che vede decrescere i profitti tenderà inevitabilmente a ridurre nel breve periodo il proprio personale,

più che assumere nuove risorse umane specializzate per fronteggiare eventuali nuovi attacchi.

IL RUOLO ATTIVO DEL SINDACATO PER RAFFORZARE LA CYBERSECURITY NEL CYBERSPAZIO

Il volume prima citato "*La sicurezza nella cyber dimension*", dedica il capitolo quarto all'illustrazione della *cyberstrategy* europea ed USA per fare fronte al fenomeno del *cyber crime*.

La strategia tedesca di difesa, ad esempio, elaborata già nel 2011, prevede un Consiglio di sicurezza del Governo federale (*Cyber-Sicherheitsrat*) per il controllo della criminalità informatica ed in tale contesto si fa esplicito riferimento alla necessità di un piano di formazione del personale che coinvolga istituzioni e singole aziende.

In Italia sono stati redatti un *Quadro Strategico Nazionale* ed un *Piano Nazionale per la protezione cibernetica e la sicurezza informatica* (in G.U. 19 febbraio 2014, n.41) in cui si evidenzia la necessità di azioni congiunte settore pubblico/privato finalizzate ad adottare una idonea capacità di prevenzione e contrasto del *cyber crime.* Ciò che a noi come UILCA qui interessa evidenziare è che tali documenti ufficiali enfatizzano la necessità di "*un'adeguata formazione, sensibilizzazione e responsabilizzazione del personale, mediante l'adozione di misure di sicurezza fisiche, logiche e procedurali".*

Piani organici di formazione del personale, nuove assunzioni di giovani professionalizzati, partnership pubblica/privato sono le tre gambe su cui può e deve reggersi un organico programma di *cyber security* per banche e assicurazioni. Un programma che, a sua volta, deve poggiare su un'organica intesa che veda la partecipazione attiva e consapevole delle OO.SS. (ad esempio, in sede di rinnovo del C.C.N.L.).

La *cyber security* è un investimento, non solo un costo.

Purtroppo l'Italia è in questo campo ancora molto indietro, sia per numero di addetti sia per i livelli retributivi degli stessi, con rischio incombente di "fuga di cervelli". Uno specialista di sicurezza informatica, in Italia, può guadagnare anche il 50 % in meno di un collega che sceglie il mercato estero. Sul mercato del lavoro internazionale – osserva Andrea Zapparoli Manzoni di Kmpg – "*non si prende meno di 80/100 mila euro l'anno, anche per chi ha meno di 27 anni. Qui in Italia si va di rado sopra i 40 mila euro e viene considerata una cifra eccezionale…Così rischiamo di perdere know-how prezioso e la nostra stessa sicurezza"*[9].

E' necessario innescare un "circolo virtuoso della sicurezza informatica finanziaria", dove più sicurezza significa più qualità nell'offerta dei servizi,

maggior fiducia della clientela nei confronti di banche/assicurazioni, più occupazione qualificata ed adeguatamente remunerata.

---

[1] Cfr. "*Non solo tecnologia per la cybe security",* Il Sole 24 Ore, 10 ottobre 2017.
[2] Cfr. "*Nuova era tecnologica, nuova era per il lavoro",* Il Sole 24 Ore, 10 ottobre 2017.
[3] RICCARDO BARLAAM, "*Gli haker rubano i dati di 143 milioni di americani",* Il Sole 24 Ore, 9 settembre 2017.
[4] ALBERTO MAZZA, "*2017, attacco alle banche",* BancaFinanza, maggio 2017, pp. 60-62.
5 ANDREA BOERIS, "Cresce il bisogno di cyber security", Milano Finanza, 7 ottobre 2017.
[6] GUARNIERO MESSERSI, *"Rischio competitività senza web security",* BancaFinanza, marzo 2017, pp. 62-65.
[7] "*Cresce la consapevolezza sulla sicurezza informatica, ma le minacce su Cloud, Big Data, Internet of Things, Mobile e Social richiedono nuovi modelli organizzativi: solo il 39 % delle grandi imprese ha un piano di intervento generale, solo il 46 % ha in organico un Chief Information Security Officer. Quasi tutte le grandi imprese hanno azioni di sensibilizzazione sul comportamento dei dipendenti. Ma appena il 15 % ha attivato assicurazioni sul rischio cyber".* Si veda la nota "*CyberCrime: la minaccia invisibile che cambia il mondo",* reperibile su web.
[8] Il tema è ampiamente trattato in MASSIMO FARINA e PIETRO LUCANIA, *"La sicurezza nella cyber dimension",* Key edizioni, 2016.
[9] ALBERTO MAGNANI, " *Cyber security: come si formano (e quanto guadagnano) i guardiani del web",* reperibile su web.