Rapporto

numero	data	competenza
7707 R	14 giugno 2022	DIPARTIMENTO DELLE FINANZE E DELL'ECONOMIA

della Commissione economia e lavoro sulla mozione 5 novembre 2018 presentata da Marco Passalia per il Gruppo PPD+GG "Posti di lavoro nuovi e innovativi portando in Ticino il centro di competenza federale di sicurezza cibernetica"

(vedi messaggio 4 settembre 2019 n. 7707)

1. INTRODUZIONE

Negli ultimi due anni gli attacchi hacker sul nostro territorio sono aumentati drasticamente e molte imprese, complice anche il telelavoro, si sono scoperte indifese e vulnerabili. In questo contesto la protezione dei dati diventa quindi cruciale, non solo per le grandi aziende, che possono permettersi i costi di un piano di risposta in caso di attacco, ma anche per le piccole aziende. Semplicemente rispondere agli attacchi non è più sostenibile, perché nessuno è al sicuro. La Confederazione ha colto il problema è sta prestando molta attenzione alla questione della sicurezza informatica, avendo anche varato una nuova legge sulla protezione dei dati. Questo nuovo quadro giuridico cambierà le regole del gioco in futuro e le aziende dovranno prestare sempre più attenzione verso il settore della sicurezza informatica, perché per la prima volta entra in gioco il concetto di responsabilità. In caso di attacco informatico le imprese saranno direttamente responsabili dell'inaccessibilità dei dati ai propri clienti e dovranno risponderne legalmente.

Tuttavia, per far fronte al problema della sicurezza informatica gli strumenti giuridici non sono sufficienti e serviranno anche risorse umane qualificate, al momento insufficienti. Per queste ragioni sarebbe quindi opportuno creare un Centro di competenza federale (o antenna in coordinazione con il futuro Ufficio federale) anche in Ticino, in modo da integrare con la Rete nazionale svizzera di sicurezza (RSS; vedi: www.rss.admin.ch) che si occupa non solo di cybersicurezza, formando esperti capaci di lavorare in un settore in rapidissima evoluzione. Per quanto riguarda l'amministrazione cantonale sono già integrati sia nella RSS che in contatto permanente con il Centro Nazionale per la Cybersicurezza (vedi: www.ncsc.admin.ch).
L'opportunità più grande per il Ticino sarebbe dunque quella di essere inserito in un discorso e in una strategia nazionale di cyberanalisi e cybersicurezza dal quale sarebbe altrimenti solo interessato di rimando, visto che i centri principali per questo tipo di problematiche sono, ovviamente, i due Politecnici federali insieme all'Università di Zurigo e di Losanna

2. SICUREZZA INFORMATICA

Le tecnologie dell'informazione e della comunicazione sono ormai parte integrante della nostra vita quotidiana essendo costantemente in contatto con dispositivi interconnessi e interattivi. Lo abbiamo potuto vedere negli ultimi due anni di pandemia, in cui l'utilizzo di

reti e dispositivi è aumentato in modo sproporzionato per far fronte al distanziamento sociale.

Questo sistema di reti e dispositivi interconnessi fra loro viene definito come "Cyber Spazio" ed è proprio in questo contesto che bisogna intervenire per minimizzare le minacce ai sistemi informatici. La struttura aperta del sistema Internet è vulnerabile ad attacchi che possono avere origine: criminale (cyber crime), terroristica (*cyber terrorism*), attività di spionaggio (*cyber espionage*) o, addirittura, dar vita ad una *cyber war*, cioè un vero e proprio conflitto tra nazioni combattuto attraverso la paralisi di tutti i sistemi vitali per le attività sociali dei reciproci contendenti. Questa situazione la stiamo osservando con la guerra tra Russia e Ucraina che ha aumentato considerevolmente gli attacchi cyber.

Questo ampliamento del mondo virtuale ha reso vulnerabili le persone fisiche, le aziende e le istituzioni pubbliche. Nessuno è ormai al sicuro dalle minacce cibernetiche e la privacy delle cittadine e dei cittadini è messa in continuo pericolo da potenziali hacker che si intrufolano all'interno di database di banche, aziende pubbliche e sistemi sanitari.

Pensiamo sempre che questi eventi accadano a qualcun altro, ma cosa succede quando siamo noi ad essere i protagonisti dell'attacco?

Se l'attacco alla persona potrebbe essere considerato un affare personale legato all'individuo, non si può dire altrettanto degli attacchi ad aziende private, para-statali e enti pubblici che sempre di più sono oggetto di attacchi, non più "dimostrativi", ma di azioni reali con rischi rilevanti: intrusioni nella rete WiFi pubblica (comunale o cantonale) con accesso a dati sensibili, vittime di spionaggio industriale con conseguenze finanziarie gravi, manipolazione di informazioni confidenziali del contribuente in ambito fiscale, modifica del sito web dell'ente attaccato con danni concreti nei confronti degli utenti, ecc. Nel momento in cui più enti privati e pubblici di un certo rilievo sono sotto attacco e sotto l'attenzione di entità esterne il problema non coinvolge più solo la singola azienda, ma dovrebbe essere considerato un problema generale di sicurezza cantonale e nazionale.

Infatti, se fino a poco tempo fa si reputava che un attacco informatico potesse arrecare solo danni informatici, l'attualità ci conferma che un attacco cyber può avere conseguenze cinetiche, ovvero danni materiali a persone e cose. Proviamo ad esempio ad immaginare i danni causati dalla eventuale manomissione del sistema di controllo dell'altezza dell'acqua in una diga, o se tutti i semafori e gli scambi di un importante nodo ferroviario venissero hackerati o ancora, se il sistema di dosaggio del disinfettante di un acquedotto venisse compromesso.

La minaccia cyber evolve con la stessa rapidità con cui evolvono le tecnologie. È evidente a tutti che le regole di difesa tradizionali, ovvero contrastare un attacco, non sono più praticabili con efficacia nel contesto attuale.

In questo contesto, rispondere a degli attacchi già avvenuti è insostenibile e molto costoso dal punto di vista finanziario, soprattutto per le piccole e medie imprese. Bisognerebbe, infatti puntare molto di più sulla prevenzione e la formazione, perché riparare i danni di un cyberattacco costa due volte e mezzo in più rispetto alla prevenzione. Prevenire gli attacchi e proteggersi è però possibile, puntando maggiormente sulla formazione dei dipendenti per esempio, soprattutto coloro che si collegano su reti esterne all'azienda per lavorare in smartworking.

3. CONTESTO NAZIONALE

Il 18 aprile 2018 il Consiglio federale ha licenziato la nuova Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) per gli anni 2018–2022.

La strategia si basa sui lavori svolti nel quadro della prima SNPC (2012–2017), li estende laddove necessario e li completa con nuove misure, affinché possa rispondere alla situazione di minaccia attuale. Messa a punto negli ultimi mesi in collaborazione con il mondo economico, i Cantoni e le scuole universitarie, questa seconda SNPC funge da base per la necessaria concentrazione di sforzi comuni volti a ridurre i cyber-rischi.

La strategia stabilisce sette obiettivi ripartiti su dieci campi d'azione molto diversificati, che vanno dall'acquisizione di competenze e conoscenze alla promozione della cooperazione internazionale passando per il rafforzamento della gestione degli incidenti e delle crisi, la collaborazione nel perseguimento penale dei reati informatici e le misure di ciberdifesa dell'esercito e del Servizio delle attività informative della Confederazione (SIC). Nella nuova SNPC è stato introdotto un campo d'azione concernente la standardizzazione e la regolamentazione mediante il quale si incarica la Confederazione di collaborare con il mondo economico per sviluppare standard minimi in materia di cibersicurezza e di esaminare l'introduzione di obblighi di notifica per gli incidenti informatici.

La Svizzera ha un grande potenziale per incentivare e attrarre organizzazioni e società nell'ambito informatico e cybersicurezza. A titolo informativo per esempio: la Svizzera ospita numerose organizzazioni, come Internet Society, Internet Governance Forum (IGF), DiploFoundation, International Telecommu-nication Union (ITU), ICT4Peace, Centro di Ginevra per la politica di sicurezza (GCSP) e WEF Cyber Security Center.

Nel 2020 i cantoni di Vaud e Ginevra hanno collaborato alla creazione della «Trust Valley», un centro di eccellenza nel campo del digital trust e della cybersicurezza volto a produrre un ecosistema unico e a incoraggiare lo sviluppo di progetti innovativi.

Nella seduta del 18 maggio 2022, il Consiglio federale ha deciso di trasformare il Centro Nazionale per la Cibersicurezza (NCSC) in un Ufficio federale, incaricando il Dipartimento federale delle finanze (DFF) di elaborare entro la fine del 2022 delle proposte per l'organizzazione della struttura del nuovo ufficio e il dipartimento a cui sarà aggregato (https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa/comunicati-stampa-consiglio-federale.msg-id-88878.html.

Nella stessa seduta il Consiglio federale ha preso conoscenza del rapporto sulla verifica dell'efficacia della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) dal 2018 al 2022. L'attuazione della SNPC in vigore si concluderà a fine 2022, nel frattempo il Consiglio Federale ha deciso di potenziare le risorse creando altri 25 posti di lavoro in questo ambito (https://www.efd.admin.ch/efd/it/home/il-dff/nsb-news_list.msg-id-88880.html).

Dal rapporto presentato emerge che la strategia è concentrata eccessivamente sulle infrastrutture critiche, sulle grandi imprese e sulle autorità nazionali e cantonali, mentre per le PMI, i Comuni e la popolazione gli effetti diretti sono ancora troppo limitati.

È importante menzionare anche il **Centro svizzero di calcolo scientifico**, un'unità autonoma dell'Istituto Federale Svizzero di Tecnologia di Zurigo (ETH Zurigo) che

collabora strettamente con l'Università della Svizzera italiana (USI). Il CSCS già oggi fornisce risorse di calcolo dedicate a specifici progetti di ricerca e mandati nazionali, come nel caso delle previsioni del tempo (esempio che si potrebbe utilizzare anche in Ticino promuovendo le collaborazioni nel campo della cybersicurezza).

4. CONTESTO REGIONALE

In Ticino se ci sono competenze di cybersicurezza sono più nel settore privato. Alcune società già offrono servizi di protezione per ditte e Comuni tramite un SOC (Security Operation Center), ma queste prestazioni possono essere ottenute tranquillamente da fornitori presenti in altri Cantoni che sono più avanti nelle competenze di cybersicurezza.

Comunque, il Ticino nonostante sembri lontano da queste logiche, può vantare numerose competenze specifiche che permetterebbero al nostro Cantone di ritagliarsi uno spazio importante nella **protezione cibernetica della Svizzera**.

Il 21 febbraio 2020 è stato anche istituito un gruppo di lavoro a livello cantonale: Cybersicuro. Questo gruppo di lavoro si identifica come il punto di riferimento a livello cantonale - ufficiale e autorevole - per tutte le questioni legate al tema della sicurezza informatica. In compenso il gruppo di lavoro Cybersicuro ha messo in rete diversi attori e ha fatto una buona ed efficace attività di sensibilizzazione.

Presenti anche sul territorio ticinese il **Laboratorio di informatica forense del Dipartimento tecnologie innovative della SUPSI**, condotto dal Dr. Alessandro Trivilini. Il Dr. Trivilini funge anche da rappresentante della Svizzera in seno al comitato di gestione dell'azione COST *"Multi-modal imaging of forensic science evidence - tools for forensic science*", del programma intergovernativo di cooperazione europea nella ricerca scientifica e tecnologica.

Si pensi anche all'**Istituto Dalle Molle di studi sull'intelligenza artificiale**, precedentemente diretto da Luca Gambardella (attualmente docente USI) e Jürgen Schmidhuber. Si tratta di un istituto di ricerca non profit, affiliato sia con l'Università della Svizzera italiana di Lugano che con la Scuola universitaria professionale della Svizzera italiana. Le attività di ricerca dell'Istituto Dalle Molle si concentrano su apprendimento automatico, intelligenza artificiale universale ottimale, agenti razionali ottimali, ricerca operativa, teoria della complessità, informatica ambientale e supporto alle decisioni, sistemi bio-ispirati e sistemi di robotica.

5. PROPOSTA

Nonostante in Ticino non ci siano delle entità o istituzioni del calibro dei Politecnici federali, Google o IBM, il potenziale non manca. Infatti, negli ultimi anni non solo si è sviluppata la facoltà di scienze informatiche (USI) che nell'ambito della sicurezza cibernetica beneficerebbe anche delle competenze legate alla facoltà di comunicazione e di economia, ma ha trovato spazio anche la SUPSI con il Laboratorio di informatica forense, l'istituto Dalle Molle di studi sull'intelligenza artificiale e il gruppo di lavoro Cybersicuro, senza dimenticare vari enti parastatali e aziende private che potrebbero certamente contribuire alla creazione di un centro di competenze di interesse nazionale e internazionale.

In questo ambito è anche fondamentale creare delle reti di collaborazione sia nazionali che internazionali, perché anche gli esperti in questo campo ammettono che è necessario "fare squadra". Infatti, nessuno può dirsi al sicuro da questo tipo di eventi, eppure se tutti adotterebbero delle contromisure preventive a possibili attacchi, i cibercriminali incontrerebbero sicuramente maggiori ostacoli. Le aziende devono essere consapevoli dei rischi, ma è altrettanto importante rendersi conto che il comportamento individuale può influenzare la sicurezza di tutti gli altri.

In questo senso è importante investire nella formazione e nella sensibilizzazione della popolazione sui temi inerenti la sicurezza informatica. Le cittadine e i cittadini dovrebbero disporre di nozioni basiche di sicurezza informatica, soprattutto in un contesto in continua evoluzione e sempre più digitalizzato.

Nel prossimo futuro il Ticino ha anche in cantiere il Parco dell'innovazione che sorgerà a Bellinzona, il quale sarà un crocevia importante per il nostro Cantone. Questo parco si situerà in mezzo ai due grandi poli di Zurigo e di Milano e sarà quindi una grande opportunità per attrarre talenti anche nell'ambito dell'informatica e della cybersicurezza. Inoltre, la prossimità geografica con questi due poli non deve per forza essere un fattore determinante, in quanto la natura stessa delle sue attività è "in rete" e distribuita, oltre che fatta di molteplici collaborazioni, non esclusivamente in loco.

6. CONCLUSIONE

Il Ticino, grazie alla formazione del gruppo Cybersicuro, ha fatto notevoli progressi e oggi è anche un riferimento ma il cyber crime è un grande rischio all'economia ed è considerato una delle minacce più serie a livello mondiale. Ogni aspetto della vita quotidiana privata e lavorativa è altamente informatizzato e come sottolineato in uno studio del WEF, se le imprese e i governi non svilupperanno politiche di difesa adeguate e veloci, le perdite economiche causate dai cyber attacchi saranno notevoli.

La Confederazione ha istituito il centro di Cyber nazionale e con le recenti decisioni il Consiglio federale ha deciso di investire ulteriori risorse nel settore e rendere la rete nazionale proattiva. Punti di forza della Svizzera come neutralità, certezza del diritto e stabilità politica, protezione della privacy, una rete di energia elettrica affidabile e conveniente, contribuiscono a rendere il nostro territorio attrattivo per l'insediamento di aziende internazionali come sede per i loro centri di calcolo regionali. Anche il Ticino può offrire un'opportunità di nuovi insediamenti e generare nuovi posti di lavoro molto attrattivi.

Concretamente, facendo uso delle facoltà previste dall'art. 101 LGC, chiede con il presente rapporto, alla luce delle indicazioni e considerazioni espresse in precedenza, così come segnalato nella mozione 1329:

1. che venga preso contatto con l'autorità federale per dare la disponibilità ad accogliere in Ticino un centro (o ufficio) di competenze federale nell'ambito della sicurezza cibernetica collegato alla facoltà di scienze informatiche e di comunicazione;
2. che la nuova struttura si occupi di incrementare sinergie strategiche locali in forma public-private-partnership, con lo scopo di contenere i costi generati dalla lotta al crimine informatico, in forma interdisciplinare, con il supporto di ricercatori scientifici di

SUPSI e USI, e di rafforzare l'impatto e la condivisione di buone pratiche per meglio mettere in sicurezza i dati e le infrastrutture critiche;

3. di incrementare e coordinare con l'autorità/ufficio federale e con il gruppo di lavoro Cybersicuro gli interventi di difesa nonché di aumentare azioni periodiche di esercitazione contro attacchi cyber;
4. di promuovere gli interventi di sensibilizzazione a partire dalle famiglie e dalle scuole, per passare dai contesti lavorativi pubblici e privati fino ai massimi livelli aziendali ed istituzionali;
5. di incrementare le collaborazioni sia nazionali che internazionali nell'ambito delle best practices in materia di cybersicurezza;
6. recuperare lo svantaggio che abbiamo rispetto ad altri Cantoni/Regioni in questo ambito dando un incoraggiamento/incentivo ad una maggiore collaborazione fra pubblico e privato.

Per la Commissione economia e lavoro:

Roberta Passardi, relatrice
Ay (con riserva) - Balli - Bignasca - Censi - Dadò -
Forini - Isabella - Maderni - Minotti - Noi - Ortelli P. -
Passalia - Sirica - Speziali - Tenconi