La CyberSecurity nel mondo arabo

del Col. Michele Lippiello e del Ten. Gabriele Donadei dell'Arma dei Carabinieri

CYBERSECURITY: UNO SGUARDO D'INSIEME NELLA REGIONE ARABA

Gli esperti in materia di *cybersecurity* sono i responsabili della protezione della *confidentiality*, *integrity* e *availability*, meglio conosciuta con il termine *CIA Triad*, delle informazioni e dei relativi sistemi informatici delle organizzazioni. L'assicurazione di questi obiettivi richiede l'applicazione del concetto di *defense-in-depth*, che prevede l'uso di differenti e sovrapposti livelli di controlli di sicurezza. Inoltre, è richiesta agli analisti una profonda conoscenza delle possibili minacce che la propria organizzazione deve fronteggiare affinché vengano sviluppati strumenti di sicurezza appropriati.

Attualmente gli obiettivi chiave della *cybersecurity* sono tre e vengono così definiti:

- *Confidentiality*, assicura che individui privi delle necessarie autorizzazioni non abbiano accesso ad informazioni sensibili, attraverso lo sviluppo e l'implementazione, tra gli altri, di *firewall*, *access control lists*, tecniche di criptaggio;
- *Integrity*, assicura che non vi siano modifiche non autorizzate alle informazioni o ai sistemi, sia intenzionali che accidentali, mediante l'uso di tecniche di *hashing* o di monitoraggio;
- *Availability*, assicura che le informazioni e i sistemi siano pronti e disponibili al legittimo uso degli utenti ogni volta che questi ne facciano richiesta, attraverso l'uso di *backups* o *redundancy systems*.

In una regione dove le tensioni politiche e sociali sono ricorrenti, la sicurezza - fisica e digitale - rappresenta un obiettivo e una necessità sempre più consistente. L'*Internet Penetration Rate*[1] sottolinea come la percentuale della popolazione araba che ha accesso ad Internet è superiore del 90% rispetto alla media mondiale, evidenziando che gli Emirati Arabi Uniti e l'Arabia Saudita raggiungono quasi il 100% di diffusione tecnologica tra i cittadini.

La maggior parte dei Paesi arabi hanno riconosciuto, negli ultimi anni, la sicurezza del *cyberspace* come parte integrante del sistema economico e della sicurezza nazionale. Questo livello di consapevolezza è accompagnato dalla pubblicazione di *policies* e normative nazionali che hanno innalzato il livello del perimetro di sicurezza cibernetica, portando il Qatar, l'Oman, l'Arabia Saudita e l'Egitto tra i venti Paesi, a livello globale, con i maggiori standard di consapevolezza ed impegno nel campo della cibersicurezza, secondo il *Global Cybersecurity Index*[2],con molti Paesi della regione in una posizione nel ranking superiore rispetto ad altre nazioni europee.

L'impegno dei Paesi arabi è stato rimarcato dall'organizzazione dell'*Arab Security Conference-Hybrid Edition* (المؤتمر العربي لأمن المعلومات), che si è tenuta il 18 ed il 19 settembre 2022 a Il Cairo, in Egitto. La conferenza, che ha visto intervenire i maggiori esperti dei governi e delle aziende arabe, si è posta l'obiettivo di supportare i *business leaders* per assicurare l'effettività della sicurezza delle informazioni per la crescita economica nell'era della digitalizzazione. Durante l'incontro, sono stati trattati i temi più vari, dai *cybercrimes* all'economia digitale, per passare attraverso la sicurezza *cloud* e i *BigData*.
I problemi etici posti dall'uso delle tecnologie, quali la *privacy*, l'onestà, la sicurezza e l'integrità delle

1 International Telecommunication Union (ITU) World Telecommunication/ICT Indicators Database

2 International Telecommunication Union (ITU) Global Cybersecurity Index, misura l'impegno dei singoli Stati nel tema della *cybersecurity*

informazioni, possono essere spiegati, inoltre, attraverso una prospettiva religiosa. L'Islam dà grande rilevanza ai problemi etici in tutti gli aspetti della vita umana e la violazione dei sistemi di sicurezza informatica, sotto questa ottica, può essere considerato "حارم", proibito.

Il concetto di informazione è considerato dall'Islam come un valore significativo per ottenere conoscenza e raggiungere il successo della società islamica, accelerato ulteriormente dall'uso delle *Information Technologies*. L'Islam ha posto particolare attenzione alla sicurezza e all'accuratezza del processo di distribuzione dell'informazione, con l'intento di raggiungere pienamente l'obiettivo posto dalla religione islamica. Inoltre, l'effettività della comunicazione risulta essere centrale anche nelle scritture coraniche. Nella storia del profeta Mosè e del Faraone, Mosè chiede a Dio di essere libero da ogni impedimento di parola affinché possa trasmettere efficacemente il messaggio al Faraone e al suo popolo. Ciò rivela che, solo quando una comunicazione è libera da ogni ostacolo, l'informazione può essere trasmessa e diretta verso la verità.

" اديدَس اَلْوَق اوُلوُقَو َهللا اوُقَّتا اوُنَمآ َنيِذَّلا اَهُيَأ اَي "[3]

Il sistema giuridico islamico rappresenta il problema della sicurezza delle informazioni sotto differenti profili:

- Onestà della fonte;
- Verifica e autenticazione delle informazioni, attraverso un processo che filtri, confermi e ne assicuri la veridicità;
- Prove documentali delle informazioni, ponendo sotto un controllo giuridico il tema del "*no repudiation*", dove la notizia è privata del suo valore;
- Distribuzione delle informazioni, richiamando il tema della *confidentiality*.

Risultano, perciò, facilmente riconducibile questi principi ai pilastri evidenziati dalla *CIA Triad*.

APPROCCI NAZIONALI ALLA TEMATICA DELLA SICUREZZA INFORMATICA

Il governo del Regno del Bahrain considera la *cybersecurity* come un pilastro per lo sviluppo economico del Paese, dipendente dalla sicurezza delle infrastrutture ICT. Negli ultimi anni, il Bahrain ha compiuto grandi sforzi per la protezione delle strutture private e pubbliche online, attraverso il *General Directorate of Anti-Corruption and Economic & Electronic Security* ed il *National Cyber Security Centre*. Il primo, istituito nel 2004, considera il tema della sicurezza informatica in diversi settori, dall'energetico alla finanza, dal sistema bancario a quello sanitario; il secondo, invece, fondato nel 2017, provvede a stabilire le strategie di contrasto ai crimini informatici, fornendo consulenza ed assistenza tecnica a tutti gli enti nazionali. Il *National Cyber Security Centre*, nell'elaborazione della strategia nazionale di cibersicurezza, ha individuato cinque pilastri per supportare le richieste ed i requisiti della sicurezza informatica: protezione tecnologica forte e flessibile, *governance* e *standard* efficaci, costruzione di una società consapevole, potenziamento della sicurezza attraverso partenariati e collaborazioni, sviluppo di un quadro nazionale. Inoltre, ha provveduto all'organizzazione dell'*Arab International Cybersecurity Summit* (*AICS*), il più grande *summit* della regione, in cui hanno preso parte governi, industrie ed esperti del settore, per discutere le strategie di sicurezza *cyber* e delle infrastrutture IT. Particolare attenzione è stata posta al tema dell'intelligenza artificiale (*AI*), tecnologia altamente richiesta negli ultimi anni, che rappresenta un ulteriore rischio sfruttabile dai cyber criminali.

L'Arabia Saudita è emersa recentemente tra i Paesi in prima linea nello sviluppo tecnologico. Come

3 "O credenti, temete Allah e parlate onestamente", Corano 33:70

risultato dell'impegno sul tema della sicurezza informatica, il *Global Cybersecurity Index* ha posizionato il Paese, nel 2020, al secondo posto nel ranking mondiale, dietro solo agli Stati Uniti d'America. È necessario evidenziare che nel 2017 e nel 2018 l'Arabia Saudita si posizionava, rispettivamente, al 46° e al 13° posto nel ranking, dimostrando, negli ultimi anni, un elevato impegno nel settore, attraverso regolamentazioni e programmi. Per far fronte alle sfide dell'era digitale, il governo saudita ha elaborato il *Vision 2030*, un *framework* strategico per lo sviluppo economico dei settori pubblici, privati e no-profit, ed il *National Transformation Program 2020*, per l'identificazione delle potenziali sfide e per stabilire i relativi piani e procedure. Per dare piena attuazione agli standard di crescita tecnologica, nel 2017 è stato istituito il *National Digital Transformation Unit* (*NDU*), al fianco del *National Digital Transformation Committee*, con l'obiettivo di fornire supporto tecnico al governo ed alle organizzazioni private per la realizzazione di un ambiente digitale attraverso l'innovazione. Con Decreto Reale 57231 del 10 novembre 1439[4], inoltre, l'Arabia Saudita ha provveduto all'accentramento delle politiche di *cybersecurity risk management* con la costituzione del *National Cybersecurity Authority* (*NCA*) per "proteggere gli interessi vitali del Regno, la sua sicurezza nazionale, le sue infrastrutture critiche, i settori prioritari, i servizi e le attività governative"[5]. L'*NCA* sviluppa regolamentazioni ed attività operative, fornendo supporto per la protezione di *hardware*, *software* e sistemi IT. In linea con il *Vision 2030*, la *National Cybersecurity Authority*, inoltre, ha sviluppato la guida "*Essential Cybersecurity Controls*" (*ECC*), individuando 114 tipologie di controlli, suddivisi in cinque macro-aree (*governance*, *defence*, *resilience*, *third-party and cloud computing*, *industrial control systems*), per indirizzare le industrie del Paese nelle attività di mitigazione dei rischi cibernetici. Nel corso di quest'anno, infine, il governo saudita, attraverso l'*NCA*, ha dato il via al progetto "*CyberIC*" per sostenere le oltre 40 *startups* del settore e sviluppare le abilità e le conoscenze di oltre 10000 giovani sauditi.

Le industrie qatariote sono state, nell'ultimo decennio, le protagoniste di una massiva crescita digitale, rafforzata anche dalle necessità sorte per l'organizzazione della Coppa del Mondo FIFA 2022. Per far fronte alla portata dell'evento calcistico, il Paese ha notevolmente ampliato i suoi sforzi, non solo per assicurare ai tifosi un evento che difficilmente verrà dimenticato, ma anche per garantire la sicurezza delle *Internet of Things* (*IoT*) e dei sistemi di controllo industriali, l'implementazione delle capacità nazionali di *cybersecurity* e di gestione del rischio; il lancio di *TASMU*, un programma per *smart city* avanzate, permetterà la trasformazione dei settori industriali nonché l'adozione della struttura *cloud* più grande del Medio Oriente. Nel 2014 il governo del Qatar ha redatto e pubblicato la Strategia Nazionale di Cybersecurity, per fronteggiare i rischi collegati ai sistemi informatici ed istituire enti e strutture idonee per contrastare le minacce cibernetiche; le esigenze di organizzazione della Coppa del Mondo FIFA 2022 hanno richiesto l'elaborazione del *Cybersecurity Framework 2022* per istituzioni, infrastrutture critiche ed aziende privati, affiancato dal *National Cyber Security Agency* (*NCSA*). L'Agenzia, sin dalla sua fondazione, ha organizzato corsi di apprendimento sui rischi informatici per gli impiegati governativi e ha collaborato con le industrie ICT per rafforzare il livello di resilienza. È fondamentale rimarcare, infine, che il Paese ha ospitato numerosi incontri del *Cyber Security Expert Group* organizzati nell'ambito del progetto *Stadia*[6] dell'Interpol, nonché promosso attività di collaborazione con Paesi terzi, tra i quali gli Stati Uniti d'America; nel giugno del 2022, il *U.S. Department of Homeland Security* (*DHS*) e la *NCSA* hanno siglato un *Joint Statement of Intent on Cybersecurity Cooperation* (*JSOI*), per rafforzare le attività di cooperazione tra i due enti per la realizzazione di *policy*, strategie e attività di *info-sharing*.

4 2017 nel calendario gregoriano

5 https://nca.gov.sa/en

6 Progetto ideato nel 2012 dal Qatar per implementare la condivisione delle informazioni e la collaborazione tra gli Stati nell'organizzazione di eventi sportivi

CONCLUSIONI

Le continue sfide dell'avanzamento tecnologico stanno rendendo sempre più sofisticati strumenti e tecniche informatiche. Il futuro del mondo cibernetico è rappresentato, ad oggi, dal *machine learning* e dall'intelligenza artificiale (*AI*), ideate con lo scopo di estrarre ed elaborare automaticamente enormi quantità di informazioni. Tecniche di *machine learning* sono attualmente utilizzate da molte organizzazioni private e pubbliche, fornendo attività di analisi automatica di dati, riducendo l'intervento umano, che si concentrerà maggiormente sull'analisi degli *output*, incrementando notevolmente la produttività aziendale.

Le sfide nel settore della *cybersecurity* risultano essere, oggi, prioritarie per i governi nazionali nonché per ogni organizzazione che opera nel settore privato. I Paesi della regione araba stanno affrontando con grande serietà ed intensità i problemi nati all'interno del *cyberspace*, con ingenti quantità di denaro investito per la transazione digitale. Risulta, però, fondamentale incentivare attività di cooperazione e collaborazione non solo tra gli Stati della regione, ma fornire altresì supporto tecnico e finanziario alle realtà dei Paesi in via di sviluppo, per garantire un perimetro di sicurezza informatica globale che sia in grado di contrastare le minacce della criminalità informatica.