MARZO 2022

Luiss Business School

Il Sole 24 ORE Radiocor

DigitEconomy.24 – CONFLITTO UCRAINO E RISCHI DI CYBER WAR

PARLA IL PRESIDENTE DEL COMITATO PARLAMENTARE ADOLFO URSO

Copasir: «L'attacco cibernetico su vasta scala va considerato atto terroristico»

Nuove proposte in arrivo da parte del Copasir, il Comitato parlamentare per la sicurezza della Repubblica, per migliorare l'asseto normativo e fronteggiare i rischi cyber che emergono dal conflitto tra Russia e Ucraina. Lo annuncia a DigitEconomy.24 (report del Sole 24 Ore Radiocor e della Luiss Business School) il presidente Adolfo Urso. «In passato - spiega - abbiamo anche sottolineato come la Russia sia il Paese più attrezzato al mondo per la guerra cibernetica

↑ **Adolfo Urso**, presidente del Copasir

e come sia necessario anche predisporre una difesa pro-attiva». Il Comitato ha di recente audito il direttore dell'Agenzia per la cybersicurezza nazionale e ritiene che l'attacco cibernetico non vada perseguito come truffa ma come atto terroristico. Quanto alla sicurezza di un asset strategico come la rete di tlc, Urso rimarca che la soluzione migliore sarebbe «una rete unica a controllo pubblico».

In occasione del conflitto russo-ucraino e dell'ipotesi di uno scenario di guerra cibernetica che cosa si

>> continua a pag. 2

L'INTERVISTA A EUGENIO SANTAGATA, CEO DI TELSY (TIM)

«In Ucraina non è ancora cyber war ma occorre prepararsi»

Nel caso del conflitto russo-ucraino, al momento, non è corretto parlare di cyber war e, secondo Eugenio Santagata, ceo di Telsy, società della cybersecurity del gruppo Tim, è improbabile che ci sia un'escalation. Ma in questi casi è bene prepararsi e, indipendentemente da quello che si registra, aggiunge il manager nell'intervista a DigitEconomy.24 (report del Sole 24 Ore Radiocor e della Luiss Business School), «stiamo cercando di trovare le vulnerabilità delle nostre infrastrutture e simulare attacchi cyber su larga scala». Occorre, inoltre, innalzare gli investimenti per i progetti di cybersecurity: i 650 milioni previsti dal Pnrr sono «un buon inizio», ma «la necessità di investimenti è molto più alta». Santagata, già ceo di Cy4Gate e vicedirettore generale di Elettronica, ha trascorso 15 anni in vari ruoli operativi come ufficiale di comando in operazioni militari.

Quali sono i settori più a rischio in caso di attacchi cyber?

I settori che presentano un maggior livello di esposizione al rischio riguardano sicuramente le infrastrutture su cui si basano i servizi di pubblica utilità e dove operano sia le grandi aziende sia le Pmi. Le prime, grazie a una sensibilizzazione continua, hanno già sviluppato sistemi di difesa avanzati. Nel vasto mondo delle Pmi, invece, per fattori culturali o di budget, c'è ancora una scarsa percezione dell'utilità degli investimenti nella difesa da attacchi cyber. Per queste ragioni stiamo ponendo particolare attenzione a questo comparto, con una rinnovata strategia di offerta. In generale Telsy, grazie alle

↑ **Eugenio Santagata**, ceo di Telsy (Tim)

proprie competenze e in piena sinergia con la forza vendite di Tim, offre le più avanzate tecnologie e servizi di sicurezza per le diverse tipologie di clienti, pubblici e privati. Per la loro strategicità vanno considerati con attenzione anche il mondo della sanità e quello della pubblica amministrazione, settori nei quali è necessario innalzare il livello di sicurezza informatica. Anche perché

>> continua a pag. 4

CLUSIT

«Infrastrutture critiche ben difese da cyber attacchi, anello debole sanità»

↑ **Gabriele Faggioli**, presidente di Clusit

Per il momento la percentuale di attacchi cyber attribuibili alla cosiddetta 'guerra cibernetica' è bassa, intorno al 2 per cento. Ma Clusit, l'associazione italiana per la sicurezza informatica, si aspetta che questa quota aumenti. Tra i possibili target degli attacchi ci sono le infrastrutture critiche, come le reti di tlc, che però, spiega il presidente Gabriele Faggioli a DigitEconomy .24 (report del Sole 24 Ore Radiocor e della Luiss Business School) sono «ben difese ormai da anni», mentre l'anello debole resta la sanità. In generale, riguardo ai rischi futuri, il nostro Paese «è stato sempre abbastanza marginale nella partecipazione alle azioni sanzionatorie e militari

>> continua a pag. 4

«Preferibile la rete unica a controllo pubblico»

può fare per migliorare la risposta dell'Italia?

Proprio ieri abbiamo audito il direttore della Agenzia per la cybersicurezza nazionale e nei prossimi giorni presenteremo nostre specifiche proposte per migliorare l'assetto normativo anche per fronteggiare nuovi rischi che emergono dal conflitto in Ucraina. Già nella prima relazione in questa legislatura il Copasir, tra i tanti aspetti, aveva sottolineato che mancava allora e manca ancora oggi una fattispecie di reato specifico. L'attacco cibernetico è perseguito come truffa, una fattispecie inadeguata tantopiù nel caso in cui l'autore sia uno Stato o un gruppo terroristico. In passato abbiamo anche sottolineato come la Russia sia il Paese più attrezzato al mondo per la guerra cibernetica e come sia necessario anche predisporre una difesa pro-attiva. Alla stregua di quanto già detto da alcuni colleghi del Copasir, posizione che io condivido, occorre anche configurare l'attacco cibernetico su vasta scala come attacco terroristico. In generale, la guerra russo-ucraina, nel cuore della nostra Europa, ci rende consapevoli di quanto importante sia la sicurezza nazionale. Credo che sia un punto di svolta il dibattito che si terrà martedì prossimo in Senato sulla nostra relazione al Parlamento: non era mai accaduto dal 2007 ad oggi, cioè dalla istituzione del Copasir.

Gli asset strategici come la rete di tlc sono adeguatamente tutelati?

Come Copasir abbiamo individuato alcuni aspetti per rafforzare la sicurezza cibernetica del Paese: l'implementazione dell'Agenzia per la cybersicurezza nazionale, l'accelerazione del cloud nazionale della Pa, la realizzazione della rete unica a controllo pubblico, l'importanza dell'industria strategica dei cavi marittimi e la interconnessione globale, l'implementazione del perimetro nazionale sulla sicurezza cybernetica. Sono aspetti per migliorare non solo la sicurezza, ma anche la difesa del Paese e la sua competitività.

Sulla rete fissa di tlc, per la quale si parla di integrazione tra l'infrastruttura di Tim e quella di Open Fiber, qual è la soluzione migliore, anche in chiave sicurezza?

Noi diamo indicazioni sulla strada da seguire per garantire la sicurezza nazionale, quindi la parola passa al Parlamento, per quanto riguarda l'aspetto legislativo, e soprattutto al governo che può agire relativamente a eventuali attori pubblici in campo e soprattutto c'è il mercato con le sue regole e con i suoi attori, da valorizzare. Ci tengo a sottolineare che non interferiamo sul mercato, ma diamo un quadro di insieme su quanto secondo noi, in materia di politica strategica della rete, sia più utile per garantire la sicurezza nazionale.

Tornando al conflitto russo-ucraino, che ha fatto alzare l'allerta sugli asset strategici, era prevedibile ed evitabile?

Nella relazione al Parlamento al 9 febbraio, prima dell'inizio del conflitto, abbiamo già evidenziato la situazione critica nelle relazioni tra Russia e Ucraina e delineato una accresciuta postura aggressiva di Mosca non solo in Europa Orientale ma anche nei Balcani, nel Mediterraneo e nel Sahel. Attualmente c'è un confronto su scala globale, che speriamo non si trasformi mai in conflitto, tra sistemi autoritari e democrazie occidentali, confronto che trova un esempio drammatico nella invasione Russia in Ucraina. Il confronto si estrinseca già in forme di competizione, la prima delle quali riguarda la supremazia tecnologica e il controllo delle materie prime. Altrimenti non si spiegherebbe perché la Russia è così interessata alla Libia e alla regione del Sahel, dove guarda caso si trova anche la Cina che, a sua volta, utilizza altri mezzi, ovvero la sottomissione del debito, in Africa come nella realizzazione della via della Seta. L' obiettivo dei due Paesi è lo stesso: il controllo delle materie prime, dei minerali preziosi e delle terre rare, ma anche delle risorse energetiche e alimentari, sicuramente di tutto ciò che serve alla transizione digitale ed ecologica.

Alla luce delle emergenze epocali come la pandemia e l'attuale conflitto, quale è la migliore strada da seguire in tema di politica industriale?

L'Italia deve essere protagonista dell'autonomia strategica europea e occidentale. Per alcuni settori ci vuole tempo, ma è importante che ci sia la consapevolezza in Italia ed Europa della strategia da seguire per garantire la sicurezza del Continente che passa anche da una politica industriale che metta in salvaguardia gli asset strategici italiani ed europei e l'investimento sulle nuove frontiere della tecnologia. L'autonomia strategica che viene giustamente declamata per la difesa europea, infatti, vale anche per la sicurezza europea e ancor più per i nostri asset strategici, per l'economia digitale e per la transizione ecologica, senza le quali è impossibile realizzare e garantire una piena indipendenza.

Il Copasir ha da tempo messo in guardia dall'utilizzo di tecnologia cinese per asset strategici, non c'è lo stesso pericolo di ingerenze con le big tech americane?

Siamo consapevoli, e lo sono anche negli Usa, dello strapotere delle big tech. Un ambito per cui vale quello che sostengono autorevoli pensatori liberali sui problemi che sorgono quando una azienda ha dimensioni superiori allo Stato in cui opera. In più, in questo caso, vi sono problemi connessi non solo alla privacy, che noi giustamente tuteliamo, ma anche alla sfera più intima delle nostre libertà. Oggi con il riconoscimento facciale è possibile individuare persino quali siano le opinioni politiche di un individuo. E questo richiama quel che prima affermavo sul confronto in corso tra democrazie occidentali e sistemi autoritari che hanno altre scale di priorità, per esempio il controllo sociale e di ogni forma di dissenso. Per semplificare, quale dovrebbe essere il nostro approccio sugli asset strategici? Siamo italiani, di conseguenza fondatori dell'Europa e parte essenziale dell'Occidente. Quindi, quando cerchiamo una soluzione, in prima istanza proviamo a trovarla in sede nazionale, se ciò non fosse possibile per motivi di dimensione finanziaria, tecnologica o produttiva, è bene che sia europea, se per motivi di economia di scala o altre ragioni non può essere solo europea, è bene che sia occidentale. Un principio che si applica, per esempio, anche per il progetto di cloud nazionale o nell'ambito della produzione di microchip, materia prima che scarseggia per varie ragioni geopolitiche. La logica, in quest'ultimo caso, dovrebbe privilegiare una soluzione europea, in partnership con le aziende americane o taiwanesi o coreane. Credo che la guerra nella nostra Europa, con gli orfanotrofi e gli ospedali pediatrici bombardati, abbia cambiato ogni paradigma. Chi poteva immaginare che la Polonia aprisse per prima le frontiere? L'Europa oggi è rinata proprio con la resistenza ucraina che scuote le nostre coscienze e che ci fa capire il valore delle libertà su cui si fonda la nostra civiltà. L'Europa rinasce a Kiev. Sono convinto che tornerà ad affermare sua volontà più forte che mai, sta rinascendo un sentimento europeo. ■

«Indispensabile aumentare le sinergie europee di fronte a emergenza cyber»

Per contrastare gli attacchi cibernetici la parola d'ordine è «cooperazione» ed è «indispensabile aumentare le sinergie europee di fronte all'emergenza cyber». Lo afferma Emanuele Galtieri, ceo di Cy4Gate, società di cybersecurity, in un'intervista a DigitEconomy.24 (report del Sole 24 Ore Radiocor e della Luiss Business School), alla luce dei rischi legati al conflitto russo-ucraino. Rischi che, spiega il manager, erano prevedibili visto che «l'attuale condizione di conflittualità nel dominio cyber si protrae sin dal 2014, anno in cui la Russia occupò la Crimea».

Cy4Gate è una società quotata in Borsa e controllata al 54% dal gruppo Elettronica, che opera principalmente con governo, forze armate, forze di polizia e agenzie di intelligence. Nelle attuali

> *La guerra cibernetica è da anni parte integrante delle modalità di condurre un conflitto*

circostanze è pronta ad aiutare le istituzioni «con servizi a valore aggiunto quali le attività di penetration testing e vulnerability assessment, finalizzate a valutare il livello di resilienza del 'perimetro cibernetico' sotto esame». D'altronde, in generale, il numero di attacchi registra, spiega il ceo, «un trend crescente nell'ultimo biennio che, in circostanze di conflitto quali quello attuale, tende ad acuire un fenomeno di cui spesso si rimane vittime inermi di un nemico invisibile per mancanza di consapevolezza, formazione e competenze».

L'emergenza Ucraina sul fronte degli attacchi cyber era prevedibile?

Il Centro degli studi Strategici e Internazionali di Washington fa risalire i primi attacchi cyber con finalità di cyber war addirittura al 2003. E sin da allora ogni conflitto regionale o di più ampia portata è stato sempre preceduto e affiancato ad attacchi cibernetici. L'e-

↑ **Emanuele Galtieri**, ceo di Cy4gate

mergenza ucraina non sfugge a queste stesse strategie e tattiche che oggi si combinano in contesti di guerra cosiddetta "ibrida", pienamente prevedibile in questo frangente non solo perché la guerra cibernetica è da anni parte integrante delle modalità di condurre un conflitto ma anche perché l'attuale condizione di conflittualità nel dominio cyber si protrae sin dal 2014, anno in cui la Russia occupò la Crimea e i separatisti russofoni del Donbass, sostenuti da Mosca, hanno ingaggiato l'Ucraina in un conflitto i cui effetti sono ancor oggi pienamente percepibili. Si fa risalire al 2016 il primo importante attacco all'Ucraina con il ramsoware "Petya", che mandò nel panico un gran numero di aziende e istituzioni pubbliche, mietendo vittime illustri come, ad esempio, il colosso francese della grande distribuzione Auchan, sebbene il bersaglio principale fosse proprio l'Ucraina, destinataria di circa l'80% degli attacchi del nuovo e micidiale virus.

Come potete supportare le istituzioni italiane?

Le profonde skill tecniche delle nostre persone ci permettono di supportare le istituzioni ove siamo richiesti con servizi a valore aggiunto quali le attività di penetration testing e vulnerability assessment, finalizzate a valutare il livello di resilienza del "perimetro cibernetico" sotto esame, nell'ottica di fornire gli strumenti necessari a irrobustirne le difese, elevandone il livello di protezione. Le iniziative sin qui descritte resterebbero ancora poco efficaci se non corroborate da una fase di training per generare awareness sul tema della cybersecurity e abilitare gli operatori del settore nell'identificare e respingere un attacco. È in quest'ottica che si innesta la Cy4Gate Academy, una palestra cyber, costituita da un mix di attività teoriche abbinate da periodi di esperimento pratico presso i nostri laboratori cibernetici, ove è possibile toccare con mano l'intensità di una cyber war, sebbene simulata. Contiamo di poter, a breve, ulteriormente rafforzare il nostro apporto alle istituzioni e alle aziende nazionali grazie all'acquisizione del 100% di Aurora, società collocata al vertice di un gruppo leader nell'ambito della cyber intelligence e data analysis.

Avete approntato strumenti nuovi qualora l'emergenza per l'Ucraina dovesse crescere?

Bisogna entrare nell'ottica che, nella cyber, ciò che fino a qualche anno fa poteva essere definito un'emergenza è oggi da considerarsi la "nuova normalità". In questo contesto di conflitto permanente sul campo di battaglia digitale, per un'azienda che fa della cybersecurity il proprio core business, i piani di gestione delle emergenze rappresentano il pane quotidiano. Abbiamo costituito un "Incident response team" capace di identificare e contrastare gli attacchi cibernetici tanto a tutela della nostra realtà aziendale quanto a supporto di enti e istituzioni che richiedano il nostro coinvolgimento. Dobbiamo, purtroppo, segnalare come il numero di attacchi registri un trend crescente nell'ultimo biennio che, in circostanze di conflitto quali quello attuale, tende ad acuire un fenomeno di cui spesso si rimane vittime inermi di un nemico invisibile per mancanza di consapevolezza, formazione e competenze. Inoltre l'innovazione, nel dominio della cybersecurity è indispensabile per la realizzazione di prodotti in grado di contrastare una minaccia in perenne evoluzione. Cy4Gate ha creato una rete di collaborazioni tra la propria ingegneria e le principali università e centri di ricerca nazionali su temi di frontiera in questo settore. Abbiamo creato da gennaio il "Center of competence for artificial intelligence", reparto di risorse dedite esclusivamente alla creazione di efficaci algoritmi di intelligence artificiale applicati trasversalmente ai nostri prodotti. L'azienda aderisce, inoltre, ai principali tavoli europei di ricerca e innovazione.

E' auspicabile un maggior coordinamento in chiave europea?

Nel dominio cibernetico la parola d'ordine è "cooperazione". Serve collaborare tra pubblico e privato poiché la maggior parte delle infrastrutture, specialmente quelle definite "critiche", opera in un ambiente digitale, è posseduta e gestita da privati ma viene regolamentata dal settore pubblico; ma è, altresì, indispensabile generare sinergie a livello europeo. Su questo versante se ne parla, tra alterne fortune, già dal 2000 ma con successi al-

> *La parola d'ordine è 'cooperazione', pubblico e privato devono collaborare*

terni. Da allora il quadro normativo europeo in materia si è molto evoluto e a ciò ha contribuito l'istituzione del 2004 dell'Enisa (European union agency for cybersecurity) che, tra i suoi obiettivi, ha quello di stimolare un'ampia cooperazione tra gli attori del settore pubblico e privato sia a livello di singoli Stati sia comunitario e il ruolo è stato ulteriormente rafforzato nel 2019 quando, con il "Cyber Security Act", gli è stato attribuito anche il mandato di operare come centro di informazioni e conoscenze, promuovendo lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato. La recente istituzione in Italia dell'Agenzia per la cybersicurezza nazionale, quale punto unico di contatto per la cooperazione tra omologhi enti degli Stati Membri, completa un quadro in materia che lascia decisamente ben sperare sull'efficacia del coordinamento cyber in chiave europea. ■

«Servono più investimenti in cybersecurity»

dal 6 marzo, nell'ambito del conflitto russo-ucraino, c'è stata la segnalazione, da parte del Csirt di un potenziale incremento di attività cyber rivolto agli obiettivi italiani. È stato importante sensibilizzare una platea più ampia possibile di attori in concomitanza con la recrudescenza di azioni offensive. Peraltro, stiamo vivendo in un periodo in cui tutti i giorni si registrano azioni con motivazioni varie, un fenomeno che in realtà perdura da tutto l'anno h24. La presa d'atto del pericolo è di per sé una buona notizia, spinge a porre in essere come sistema Paese delle contromisure.

Bastano i 650 milioni stanziati dal Pnrr per la cybersecurity?

Sicuramente costituiscono un buon inizio, ma la necessità di investimenti per progetti di cybersecurity è molto più alta. Il tema è comprendere il valore intrinseco della sicurezza cibernetica in ogni settore. Se pensiamo, ad esempio, ad investimenti di intelligenza artificiale per le smart city oppure alla sensoristica occorre chiedersi: qual è la quota destinata alla cybersecurity? E così via. Un altro aspetto rilevante per poter pensare a una strategia difensiva solida è quello di avere tecnologie di proprietà: l'80% delle tecnologie è di provenienza estera, il rischio è dunque quello di finanziare, anche con il Pnrr, soprattutto le aziende straniere. Sono temi sui quali stiamo lavorando direttamente. Il terzo tema è quello dei talenti. In questo periodo di incremento della campagna offensiva, si fa sempre più fatica, per varie ragioni, a reperire le competenze necessarie.

In caso di escalation campagna offensiva, si può parlare di rischio di cyber war per il conflitto russo-ucraino?

Su questo c'è molta disinformazione, proviamo a fare chiarezza. È vero che si è registrato un aumento significativo di operazioni finalizzate a creare disservizio; al tempo stesso, non credo si possa parlare di cyber war nel caso dell'Ucraina. Quello a cui abbiamo assistito sono principalmente attacchi dimostrativi, volti a fare rumore. Niente di paragonabile a quanto accaduto in Ucraina nel 2014 e nel 2016-2017, quando la Russia dimostrò di poter colpire la rete elettrica nazionale. Non è detto che non avvenga in seguito, ma a mio avviso è improbabile sulla base di diverse considerazioni. Se da un lato la forza difensiva ucraina è più solida rispetto al 2016-2017, d'altro canto quando si passa a operazioni militari di tipo convenzionale, l'attacco cyber, se c'è, diventa secondario. Negli ultimi 20 anni le operazioni di attacco cyber in grande scala sono state poche, considerando anche quelle rivolte contro l'Ucraina nel 2014 e nel 2017. Quando avviene l'attacco cyber in larga scala in genere tacciono le armi. Al momento l'arma cyber è stata usata più per creare fake news o fare propaganda.

Nel caso, che lei ritiene improbabile, di escalation dei cyber attacchi, l'Italia è pronta?

In questo campo vale il detto "se vuoi la pace devi preparare la guerra", indipendente da quello che registriamo anche a fronte di un fenomeno cyber poco rilevante. Vale da stimolo per aumentare la nostra capacità di resilienza. Stiamo cercando di trovare le vulnerabilità delle nostre infrastrutture, simulare attacchi cyber su larga scala, ci concentriamo talvolta sui servizi più esposti di un'azienda, come il sito web o la posta.

Avete studiato prodotti per l'emergenza, state portando avanti iniziative ad hoc?

Tra le soluzioni sul mercato ne abbiamo una di education sotto forma di tutorial rivolta al mondo delle Pmi, ma anche alle grandi aziende che vogliano dotare tutti i dipendenti di conoscenze, coinvolgendo pure coloro che non lavorano nel settore della sicurezza. Occorre ricordare che nella maggior parte dei casi l'anello debole è proprio l'uomo. In ottica nazionale, noi stiamo interagendo continuamente con gli stakeholder, con l'Agenzia per la cybersicurezza, i nostri partner storici come la Difesa o le forze armate. ■

e, quindi, potrebbe essere meno un target di attacco, d'altro canto l'Italia ha fatto investimenti in sicurezza inferiori rispetto agli altri e, in quanto più debole, potrebbe essere preferita per realizzare attacchi perlomeno dimostrativi».

Avete calcolato l'impatto della crisi russo-ucraina sugli attacchi informatici?

La stima dell'impatto della crisi russo-ucraina è molto difficile in questo momento. Guardando ai numeri che abbiamo già pubblicato, e che si riferiscono a dicembre, la percentuale di attacchi classificabili come guerra cibernetica è intorno al 2% mentre il numero largamente preponderante è quello relativo al cyber crime volto a guadagnare soldi. Negli ultimi due-tre anni, rispetto alla minaccia dell'Isis, la fettina riconducibile alla guerra cibernetica si è più che dimezzata ed è scesa dal 4-5% all'attuale 2% circa. Ci aspettiamo ora che questa percentuale aumenti. Di quanto? Dipenderà da quanti attacchi gravi, contro chi, e con quale virulenza.

Le nostre infrastrutture critiche sono ben tutelate? Ci sono anelli deboli?

Esistono normative che definiscono le infrastrutture critiche, che tra le altre sono quelle riguardanti l'energia, i trasporti, le banche sistemiche, gli ospedali, le Pa e quindi le società su cui si incentra la vita civile del Paese. Se qualcuno vorrà provare a porre in essere attacchi rilevanti, è probabile che proveranno contro queste tipologie di strutture. Ovviamente, ammesso che accada, dovremo vedere se si tratterà di attacchi volti solo a realizzare pesanti disservizi oppure se l'obiettivo sarà quello di arrecare danno diretto alle persone o addirittura vittime. Faccio un esempio: un conto è bloccare una rete di telecomunicazioni per qualche ora, un altro è attaccare il sistema del traffico aereo cercando di impedire la funzionalità dei sistemi che controlla la sicurezza dei voli. È pur vero, tuttavia, che le infrastrutture critiche sono quelle meglio difese in quanto, anche per la leva normativa, sono stati fatti ingenti investimenti in sicurezza ormai da anni. Penso faccia un po' eccezione il sistema sanitario nel quale, perlomeno sulla base dei dati che posso analizzare, penso non siano stati fatti abbastanza investimenti nel passato con la conseguenza che oggi si tratta di un settore strutturalmente più debole rispetto per esempio al comparto tlc o alle banche.

Le infrastrutture di tlc sono in sicurezza?

Di sicuro le tlc rappresentano un ambito critico e se ne sta parlando moltissimo, anche in merito alla possibile disconnessione della Russia da Internet, ma le aziende del settore sono attente, hanno fatto importanti investimenti e utilizzano tecnologie molto avanzate. Non vuol dire che siano impermeabili agli attacchi, ma la possibilità di anticiparli e di mitigarne gli effetti è più alta che in tanti altri settori.

L'Italia è pronta in caso di escalation degli attacchi?

Esiste l'Agenzia per la cybersicurezza nazionale guidata da Roberto Baldoni che assieme ad altre autorità coinvolte sta facendo un grande lavoro a tutela della nostra nazione. Inoltre, a livello normativo, l'Italia ha seguito il percorso indicato dalla Ue, varando in maniera molto efficace il perimetro nazionale di cybersecurity. Infine, il Governo italiano e le istituzioni preposte stanno applicando correttamente la politica di difesa. Per fare un esempio il 6 marzo scorso il Csirt (Computer security incident response team) e l'Agenzia nazionale hanno inviato una comunicazione per innalzare l'allerta in vista di possibili attacchi cibernetici anche verso obiettivi italiani. L'allerta sarà alta in tutti questi giorni del conflitto. Sono scese in campo forze che si fronteggiano, come Anonymous e Conti. La possibilità che si realizzino degli attacchi è quindi molto alta. Se da un lato il nostro Paese è stato sempre abbastanza marginale nella partecipazione alle azioni sanzionatorie e militari e, quindi, potrebbe essere meno un target di attacco, d'altro canto l'Italia ha fatto investimenti in sicurezza inferiori rispetto agli altri Paesi e, in quanto più debole, potrebbe essere preferita per realizzare attacchi perlomeno dimostrativi. ■