NUOVE STRATEGIE PER LA CYBERSICUREZZA

di BENIAMINO MUSTO

LA GUERRA PARALLELA CHE SI COMBATTE TRA L'OCCIDENTE E LA RUSSIA, QUELLA INFORMATICA, APRE MOLTI SCENARI CHE PUBBLICA AMMINISTRAZIONE E AZIENDE PRIVATE DEVONO VALUTARE PER PROTEGGERE LE LORO ATTIVITÀ E I DATI CONNESSI: L'AVVOCATO VALENTINA FREDIANI DI COLIN & PARTNERS INVITA A FARE ATTENZIONE ALLE NUOVE IMPLICAZIONI IN OTTICA DI ACCOUNTABILITY

In tema di cyber sicurezza esistono diversi aspetti normativi e di compliance sui quali, alla luce del conflitto tra Russia e Ucraina, occorre tenere alta l'attenzione. A partire dalle sanzioni: con il regolamento europeo 328/2022, una versione aggiornata di quello già emanato nel 2014 in seguito all'annessione della Crimea da parte di Mosca, l'Ue ha imposto lo stop all'export in Russia di tutta una serie di forniture di prodotti informatici.

Ma, soprattutto, lo scorso marzo è arrivata la raccomandazione dell'*Agenzia nazionale sulla cyber sicurezza*. Non si tratta di una blacklist specifica che banna irrevocabilmente gli strumenti russi, ma è un invito urgente a rivalutare i rischi di accordi pregressi attraverso una "analisi del rischio derivante dalle soluzioni di sicurezza informatica utilizzate e di considerare l'attuazione di opportune strategie di diversificazione".

UNA RACCOMANDAZIONE DA TRATTARE COME UN OBBLIGO

In altre parole, spiega **Valentina Frediani**, founder e ceo di **Colin & Partners**, "l'Agenzia ha chiesto alle aziende e alla pubblica amministrazione di fare un controllo sui rischi riguardanti tutto ciò che si ha di collegato in rete e che sia legato alla Federazione Russa". Sui media generalisti si è parlato quasi solo degli antivirus **Kaspersky**, ma esistono moltissimi altri prodotti che provengono dalla Russia e che hanno un'ampia diffusione in Europa.

Sebbene l'Autorità non imponga una sostituzione ma solo una valutazione, la raccomandazione ha un'ampia portata sotto il profilo normativo, osserva Frediani, "basti pensare al Gdpr, al decreto legislativo 231/2001, alla Nis (la direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Ue, ndr) sulla base dei quali la valutazione dei rischi e il suo aggiornamento è un adempimento obbligatorio. Non ottemperando a tale raccomandazione, nel momento in cui si dovessero subire degli attacchi e dovessero emergere mancanze rispetto alle prescrizioni o a soggetti terzi o rispetto all'erogazione dei servizi, ci sarebbe dunque una responsabilità omissiva da parte dell'azienda o dell'ente".

LA GOLDEN POWER DEL GOVERNO

Insomma, il messaggio è abbastanza chiaro: molto probabilmente assisteremo a un intensificarsi degli attacchi cyber, e dobbiamo farci trovare pronti. A que-

sto proposito lo scorso 21 marzo è stato emanato il decreto legge n. 21/2022 in tema di "Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina". Il provvedimento ha introdotto novità nel campo della cybersecurity con l'obiettivo di consolidare la sovranità tecnologica e digitale nazionale, ridefinendo i poteri speciali in materia di difesa e sicurezza nazionale (cioè la *golden power*) attorno a sistemi sensibili come le architetture cloud o le reti 5G. Il dl prevede la tempestiva diversificazione dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, con particolare riferimento a strumenti per la protezione di endpoint e a firewall. Oltre ad eventuali attacchi, un altro rischio concreto riguarda anche la possibilità che le aziende produttrici di prodotti e servizi tecnologici di sicurezza informatica legate alla Russia non siano in grado di fornire servizi e aggiornamenti ai propri prodotti. "Il Governo – spiega Frediani – vuole che vengano fatte delle diversificazioni nella pubblica amministrazione, andando a capire quanto sono presenti elementi di influenza russa sugli end point, e quali soluzioni sostitutive adottare per procedere a un distacco da essi, in modo da prevenire indebiti attacchi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle PA".

L'UCRAINA CHIAMA ALLE ARMI GLI HACKER DI TUTTO IL MONDO

L'avvocato Frediani invita a fare attenzione ai pericoli di un'escalation della cyber war, di cui si sta parlando poco. "Nelle prime settimane dell'invasione russa, **Mykhailo Fedorov**, giovane ministro dell'Innovazione tecnologica e transizione digitale dell'Ucraina, ha costituito un esercito informatico, con una vera e propria chiamata alle armi rivolta agli hacker di tutto il mondo. La strategia portata avanti da Fedorov prevede attacchi organizzati e coordinati, esattamente come quelli di un esercito, dove ognuno ha un ruolo programmato". Gli obiettivi li ha rivelati lo stesso ministro in una recente intervista all'AdnKronos: le risorse web di **Gazprom**, **Lukoil**, le banche **Sberbank**, **Vtb**, **Gasprombank**, e i portali web statali del Cremlino e del parlamento russo. Il ministro ha detto di avere arruolato 300mila specialisti cyber.

***Valentina Frediani**, founder e ceo di Colin & Partners*

"La costituzione di un vero e proprio esercito per condurre cyber attacchi – commenta Frediani – è un fatto rilevante perché una chiamata alle armi vera e propria fino a oggi non era mai stata palesata. Questo ci dà la misura anche delle possibili contromosse russe, perché mentre il ministro ucraino dichiara queste cose pubblicamente, la Russia non resta certo con le mani in mano: può organizzarsi e far partire attacchi mirati, anche nei nostri confronti, condotti in modo coordinato e programmato, e con una possibile escalation".
È chiaro che in un simile contesto trovare un'efficace modalità di gestione dei rischi diventa sempre più complicato. Quale contributo può arrivare dal sistema assicurativo? "Come Colin & Partners – risponde Frediani – stiamo raccomandando fortemente a tutti i nostri clienti di chiedere ai propri fornitori ICT l'inserimento nei contratti di una clausola per l'adozione di una polizza per il risarcimento per gestione del cyber risk e di aumentare gli audit (già obbligatori in conformità al Gdpr) in modo da capire realisticamente quali possono essere le fragilità. Dall'altra parte però, ciò che osserviamo è che i fornitori non stanno facendo audit interni, se ne stanno preoccupando molto poco. Da un punto di vista assicurativo andrebbe aumentata molto di più la sensibilizzazione su questo tema, visto lo scarso risultato che noi vediamo dal punto di vista pratico quando richiediamo questo requisito".