Il cyberspazio tra attacchi violenti e pace sperata: come domare il “Pegaso”? Parla Francesca Bosco, del CyberPeace Institute

Le attività criminali informatiche sono in aumento. Tra queste, nuovi capitoli si aggiungono alla nota vicenda Pegasus, malware che ha colpito vari professionisti e personalità di tutto il mondo. Agli inizi di questo mese, infatti, Apple ha dovuto rilasciare aggiornamenti software di emergenza per una vulnerabilità nei suoi prodotti, dopo che i ricercatori del Citizen Lab hanno scoperto una falla che permette allo spyware di infettare iPhone, iPad, Apple Watch o computer Mac di chiunque senza nemmeno un “clic”. Ma lo spazio cyber è un luogo oscuro pieno di pericoli? “Internet e le nuove tecnologie devono essere dei facilitatori per garantire una vita migliore. Per questo è importante parlare di un cyberspazio in cui i comportamenti responsabili regnano sovrani. Responsabilità degli utenti, ma anche e soprattutto responsabilità chiare per chi commette illeciti attraverso queste tecnologie”. Così Francesca Bosco, Chief of Staff, Head of Foresight presso il CyberPeace Institute.

Infografica – La biografia dell'intervistata Francesca Bosco

– Partiamo da Pegasus: cos'è e come ha potuto colpire giornalisti, difensori dei diritti umani, politici, uomini d'affari e persino Capi di Stato?

"Cercando di spiegarlo in maniera semplice, Pegasus è un c.d. spyware, ovvero una tipologia di software usato per finalità di spionaggio che viene installato nell'apparecchio interessato (solitamente telefoni cellulari), e senza che la vittima ne sia al corrente o abbia dato il proprio consenso, monitora tutte le attività e relative informazioni del telefono in questione: ad esempio identifica l'ora e il luogo degli spostamenti e apre messaggi, telecamere e microfono del device colpito. Non stiamo parlando soltanto di attacchi con scopi d'intelligence, legati magari alla lotta al terrorismo, ma di vere e proprie azioni criminali. Pegasus è riuscito a colpire giornalisti, difensori dei diritti umani, politici, uomini d'affari e persino Capi di Stato in quanto può essere installato da remoto, senza alcuna azione da parte della vittima. Per dare un'idea della gravità della situazione: più di 1,65 miliardi di prodotti Apple in uso in tutto il mondo sono stati vulnerabili allo spyware Pegasus da marzo 2021".

– Sempre in tema Pegasus, viste le violazioni delle libertà, cosa possono fare gli Stati per tutelare i propri cittadini da attacchi come questi?

“Leggi e regole più severe. Gli Stati dovrebbero mettere in atto una regolamentazione più dura, che preveda l’esportazione di sistemi avanzati solo in territori in cui vi sia una sorta di “compliance” in tema di diritti umani: il mercato della sorveglianza non sempre è regolato da strumenti normativi in grado di contrastare le violazioni ai diritti fondamentali, tra i quali quello di stampa, (mettendo in pericolo la vita dei giornalisti, basti pensare a cosa successo a Khashoggi) e di opinione (colpendo oppositori politici e leaders stranieri). In caso di preoccupazione, la licenza di esportazione non dovrebbe essere concessa. Dall’altro lato, anche le importazioni dovrebbero essere controllate al fine di evitare possibili abusi. Devono essere posti in atto dei sistemi di responsabilità, ed è estremamente necessario che qualsiasi tipo di scelta venga basata su quella che viene definita “human rights-based approach”, che cerca anche di rafforzare le capacità dei vari stakeholders (solitamente i Governi) nel rispettare, proteggere e garantire i diritti”.

– Pubblico e privato possono collaborare e far fronte a minacce come Pegasus?

“C’è una riflessione da fare dal punto di vista pratico. Le tecnologie di spyware e sorveglianza operano su infrastrutture come il cloud e fornitori di servizi di comunicazione che sono nelle mani di compagnie private e del settore industriale privato. Bisogna incoraggiare tale settore affinché preveda, nei termini di servizio, la negazione nell’utilizzo di queste tecnologie in caso di violazioni di diritti umani. Ma esiste poi anche una cooperazione con lo Stato, e le politiche fanno parte di questo approccio che vede il settore pubblico e quello privato collaborare su diversi aspetti, quale quello di una corretta informazione. Quello che facciamo da tempo al CyberPeace Institute è un lavoro che include aziende e associazioni della società civile nazionali e internazionali (come Amnesty International) per sostenere e tutelare le vittime di abusi. Bisogna concentrare gli sforzi sui diritti delle persone, valutando l’impatto dei cyberattacchi da una prospettiva umana, sostenendo dunque l’human centric approach nelle analisi, poiché questo è essenziale per il processo di risarcimento, riparazione e giustizia per le vittime. Con questo obiettivo stiamo facendo un lavoro di supporto di analisi forense dei possibili devices infettati, potenziali vittime sul caso specifico dello spyware Pegasus, più assistenza alle persone colpite e analisi di mercato per legislazione in materia. Ci sono molte società sensibili all’argomento per avere un mercato più rispettoso dei diritti umani, ma l’approccio coordinato è mancato. Cooperare per amplificare il lavoro pubblico – privato in un dialogo continuo: al CyberPeace Institute lavoriamo in questo senso”.

– In campo UE, a giugno di quest’anno si è parlato della Joint Cyber Unit (JCU). Collaborazioni europee di questo tipo possono essere la risposta per una maggior difesa da attacchi in stile Pegasus oppure è necessario raggiungere una cooperazione globale, con attori quali USA, Russia e Cina?

“È importantissimo collaborare a livello internazionale proprio per assicurare il rispetto dei diritti, abbiamo bisogno di sforzi maggiori che permettano controlli più efficaci. C’è un’altra considerazione da fare: in ambito internazionale esistono strumenti o processi di difesa (come i Principi guida delle Nazioni Unite su imprese e diritti umani, le Linee guida dell’OCSE sulla due diligence, processi come il GGE delle Nazioni Unite e l’OEWG delle Nazioni Unite), ma a causa dell’ambito sovranazionale non sono vincolanti. La natura volontaria di queste norme, combinata con la mancanza di trasparenza dei modelli operativi delle tecnologie di sorveglianza, rende quasi impossibile qualsiasi meccanismo di supervisione. La regolamentazione governativa dello spyware dovrebbe seguire il processo di regolamentazione delle armi convenzionali.

A livello europeo (UE) un buon punto di partenza è il regolamento sull’esportazione di capacità informatiche offensive e il regime dell’Unione di controllo delle esportazioni, dell’intermediazione, dell’assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso (rifusione) (Reg UE 821/2021), entrato in vigore il 9 settembre 2021. Si potrebbe dire un buon punto di partenza, ma diversi attori della società civile hanno evidenziato lacune: un esempio recente è rappresentato dalla richiesta di realizzare (implementare) in maniera più robusta ed efficace il regime dell’Unione di controllo delle esportazioni avanzato da Access Now, Amnesty International, Committee to Protect Journalists, Human Rights Watch, e Reporters Without Borders (RSF). In un loro recente intervento, hanno sottolineato come

vi siano casi di uso scorretto delle tecnologie di sorveglianza anche all'interno dell'Unione Europea (esempio dell'Ungheria) e di quanto sia estremamente necessario portarli alla luce, condannarli, e istituire dei meccanismi di controllo che assicurino il rispetto dei diritti umani in qualsiasi momento. Gli attori della società civile hanno un ruolo fino ad adesso relegato alla denuncia, ma dovrebbero essere coinvolti direttamente nella creazione di questi regolamenti e nel processo di evoluzione normativa.".

– L'ambito cyber sta assumendo, nell'immaginario collettivo, l'immagine di un campo di battaglia infinito e pieno di spiacevoli sorprese. In tutto questo, lei come immagina la pace nel cyberspazio?

"La pace nel cyberspazio si potrebbe descrivere come un contesto in cui le nuove tecnologie vengono usate nel – e per il – rispetto dei diritti umani e nel rispetto della sicurezza, dignità, e giustizia per gli individui. Pace non è tale solo perché contraria al conflitto, e pace cyber dev'essere lo status di partenza al quale aspirare, come sottolineiamo all'Istituto. Le nuove tecnologie devono facilitare e proteggere i servizi essenziali della vita umana, proteggere le infrastrutture critiche e garantire il rispetto dei diritti fondamentali, come i diritti civili e politici, e la protezione da pregiudizi e disuguaglianze. Pegasus è stato ed è particolarmente rilevante perché va ad intaccare sicurezza, dignità e uguaglianza e rappresenta un effetto domino: colpire una persona per colpire la collettività. Bisogna avere un "human centric approach" che sia "evidence lead", non possiamo permetterci di avere difficoltà nell'individuare i responsabili di azioni criminali cyber. È un processo che afferisce spesso a considerazioni di geopolitica, determinati attacchi sono contrari a norme nazionali e internazionali e capire di chi sia la responsabilità della violazione è fondamentale. Per la cyberpeace bisogna dare risposte certe agli abusi che vengono perpetrati attraverso questi strumenti".

Francesca Bosco, Chief of Staff-Head of Foresight-CyberPeace Institute

Francesca Bosco ha una formazione in Diritto Internazionale e Diritti Umani e più di 10 anni di esperienza di lavoro in organizzazioni internazionali (Nazioni Unite e World Economic Forum) in materia di ricerca, capacity building e assistenza tecnica nel campo della giustizia internazionale, del crimine e della sicurezza. Ha sviluppato le sue competenze in materia di criminalità informatica, sicurezza informatica e uso improprio della tecnologia, concentrandosi recentemente sulle opportunità, i rischi e le minacce create dalle nuove tecnologie. All'Istituto, è a capo dello sviluppo strategico e dirige la ricerca e le iniziative sulle disruptive technologies e su come aumentare la resilienza attraverso capacity building.

Read More