LA RUSSIA E LA NUOVA CYBER SECURITY STRATEGY

A cura di Mario Avantini - Roma, 15 febbraio 2015

I Paesi occidentali valutano le cyber-attività della Russia soprattutto come una minaccia, se effettuate a scopo di spionaggio, nell'ambito della criminalità organizzata, oppure se condotte da attivisti a favore o contro la politica estera e nazionale del proprio Paese. Occorre premettere che la Russia, in questo caso, tende a utilizzare l'aggettivo "information security" al posto del suffisso "cyber" o "cyber security".

Per il popolo russo le minacce nel cyberspace sono esattamente le medesime di quelle individuate dall'Occidente, anche se il Governo russo ha presentato una serie di punti di vista radicalmente diversi in merito al "chi" e al "cosa" può effettivamente rappresentare una minaccia, tra cui una prospettiva differente in merito alla libertà individuale, contro gli interessi dello Stato. Di conseguenza, il Governo russo sta adottando nuove misure per il contrasto del cyber-crimine e del furto di identità, al fine di garantire la sicurezza delle informazioni, introducendo una nuova strategia sul cyberspace. Gli obiettivi principali della nuova strategia consistono nella tutela delle risorse russe sul web, nella protezione dell'attività in Internet da attacchi di hacker, dal cyber-terrorismo e cyber-spionaggio proveniente da Paesi stranieri. Tra i principali obiettivi individuati si menziona la protezione delle reti pubbliche e statali. Come parte della nuova strategia, il Governo russo intende prendere in seria considerazione gli attacchi informatici rivolti ai propri siti web e le risorse online, come tentativi di presa di potere. Di conseguenza, tali azioni saranno soggette a una responsabilità penale.

La nuova strategia dovrebbe essere applicata come parte di un decreto promulgato nel 2014, denominato "Principi della Politica di Stato della Federazione Russa nel Campo della Sicurezza Informatica Internazionale fino al 2020", firmata con un certo ritardo dal Presidente russo Vladimir Putin.

Il decreto è stato elaborato congiuntamente dal Consiglio di Sicurezza russo, dal Ministero degli Affari Esteri, dal Ministero della Difesa, dal Ministero delle Comunicazioni e dal Ministero della Giustizia.

Si è rilevato che, come tanti altri Paesi, anche la Russia ha riscontrato difficoltà a contrastare le organizzazioni di cyber crime. Analizzando alcuni rapporti informativi si è constatata, nel migliore dei casi, una certa indifferenza verso la criminalità russa e una maggiore

propensione a perseguire i criminali stranieri, rendendo in tal modo difficile l'applicazione delle regole internazionali contro eventuali soggetti sospettati di provenienza russa. Invece nel peggiore dei casi, è stata evidenziata una probabile collusione diretta tra lo Stato russo e gruppi criminali organizzati, i quali agiscono per conto dello Stato stesso. Tra i gruppi criminali locali accusati di avere instaurato solide relazioni politiche si menziona il Russian Business Network (RBN), descritto da VeriSign come "il più malvagio dei malvagi", il quale offre servizi di web hosting e connessioni internet a favore di tutte le tipologie di attività criminali, ottenendo guadagni nell'ordine di centinaia di milioni di Dollari in un anno. L'RBN non è una società registrata e i domini web di cui si avvale sono costituiti da indirizzi anonimi. I soggetti legati a tale gruppo criminale sono conosciuti unicamente tramite soprannomi. Essi non pubblicizzano i propri servizi e svolgono attività commerciali solo attraverso transazioni elettroniche non rintracciabili.

Un'attività nota attribuita all'RBN è la consegna di exploit informatici attraverso falsi programmi anti-spyware e anti-malware, sia per infettare PC che per attuare furti di identità personale. McAfee Site Advisor ha condotto 279 test di download "cattivi" dal sito www.malwarealarm.com, rilevando che Malware Alarm è un aggiornamento del falso anti-spyware Malware Wiper. Secondo un rapporto Spamhaus, RBN è "tra i peggiori spammer al mondo di malware, phishing e cyber-crimine" nel Web.

L'intenzione di creare una cyber-strategia è stata annunciata da Vladimir Putin già all'inizio del 2000, in seguito a una percezione in rapida crescita della minaccia del crimine informatico e del terrorismo su Internet.

Un rappresentante ufficiale dell'Amministrazione Presidenziale appartenente alla Russia commenta: "La costante e crescente popolarità di social network e micro-blog ha contribuito a una diffusione massiccia dell'ideologia del terrore su Internet. Le moderne tecnologie informatiche hanno fornito l'occasione per i terroristi di reclutare estremisti suicidi. Allo stesso tempo, il numero di cyber-criminali è aumentato, in particolare, coloro i quali trafugano informazioni personali online e colpiscono i sistemi di pagamento elettronico. La nuova strategia dovrebbe aiutarci a innalzare il livello di informazione e di sicurezza IT nel Paese e iniziare più attivamente a combattere i cyber-criminali".

In particolare, la nuova strategia Russa individua quattro principali minacce di sicurezza informatica e dell'informazione.

La prima minaccia: consistente nell'utilizzo di tecnologie dell'informazione e della comunicazione come armi di informazione, per raggiungere obiettivi nazionali, al fine di compiere atti ostili e aggressivi.

La seconda minaccia: prevede l'utilizzo di tecnologie informatiche a fini terroristici.

La terza minaccia: consiste in un numero sempre crescente di cyber-crimini, sufficientemente abili ad accedere illegalmente alle informazioni contenute in computer, oltre che a essere in grado di creare e distribuire programmi maligni.

La quarta minaccia: tipicamente russa, prevede l'utilizzo di tecnologie informatiche per portare a termine un azione criminale negli affari interni dello Stato, disturbando l'ordine pubblico, fomentando l'odio nazionale (quest'ultimo aspetto interpretato come un problema molto rilevante in Russa, per la presenza di numerose associazioni regionali) e lo stato di propaganda sovversiva.

Secondo fonti del governo russo, il motivo principale dell'esistenza delle quattro minacce nel disegno di legge è il risultato dei recenti eventi politici e dei massicci disordini registrati in alcune aree del Medio Oriente, a seguito della "primavera araba", fenomeno questo che ha dimostrato la grande potenzialità insita in Internet (in particolare dei social network), inteso come strumento per organizzare e coordinare azioni anti-governo.

L'attuazione della strategia è destinata ad avere accesso sia in ambito interno che internazionale. In quest'ultimo caso, il Governo russo prevede di attuarla in collaborazione con i propri Alleati, e in particolare con i Paesi membri dell'Organizzazione di Cooperazione di Shangai, dell'Organizzazione del Trattato di Sicurezza Collettiva, oltre che gli Stati BRICS.

La Russia auspica fortemente di vedere molte delle proprie iniziative di sicurezza informatica internazionale come chiave di utilizzo da parte delle Nazioni Unite, per la creazione di una convenzione sulla garanzia di sicurezza delle informazioni internazionali. Ciò condurrebbe allo sviluppo di un codice riconosciuto a livello internazionale di condotta in materia di cyber-spazio, così come a una internazionalizzazione del sistema di gestione Internet, oltre alla creazione di un regime giuridico internazionale di non proliferazione riguardo le armi di informazione.

Fino a oggi la maggior parte dei Paesi occidentali hanno manifestato una certa diffidenza nei confronti di iniziative per la sicurezza informatica provenienti dalla Russia, interpretandole essenzialmente come un tentativo volto al rafforzamento del controllo statale russo su Internet. Tuttavia negli ultimi anni proprio il Governo russo ha compiuto notevoli sforzi per superare quest'interpretazione. Appare quindi evidente come tale questione viene descritta come un accordo "senza precedenti", come il documento (OSCE) firmato lo scorso anno dai Presidenti di Russia e Stati Uniti in occasione di un meeting Irlanda del Nord, con l'obiettivo di prevenire cyber-incidenti ed eventuali escalation di conflitti internazionali. Suddetti accordi sono considerati molto importanti dalla Russia, paragonabili perfino alla famosa

“linea rossa” di telecomunicazioni tra l’URSS e gli Stati Uniti durante la Guerra Fredda e progettati per la prevenzione di un conflitto militare oppure di una guerra nucleare.

Secondo i termini indicati nell’accordo menzionato, saranno utilizzati i Centres/Facillities per i rapporti e le notifiche di attacchi alle infrastrutture critiche informatizzate di entrambi i Paesi. Inoltre, verranno creati due canali comunicativi speciali per lo scambio di informazioni su incidenti informatici e cyber-crimini.

Il primo di questi canali sarà utilizzato per la comunicazione da parte delle Agenzie di Sicurezza Nazionale di entrambi i Paesi, per quanto riguarda la sicurezza delle informazioni, mentre il secondo canale per incidenti informatici di tipo “first response” sarà specializzato nel monitoraggio delle attività dannose su Internet.

Il Governo russo prevede di accelerare i negoziati con altri Paesi NATO nel prossimo futuro, con l’obiettivo di firmare accordi simili.

Inoltre, il Governo russo intende sviluppare e proporre alle Nazioni Unite una convenzione globale in materia di cyber crime, il che rafforzerebbe ulteriormente la cooperazione con gli Stati Uniti in tale ambito. Ciò si riflette nei recenti accordi sulla lotta al cyber crime che garantisce la sicurezza delle informazioni. Tali accordi sono stati raggiunti grazie alla collaborazione di Vladimir Kolokoltsev, Ministro degli Interni della Russia, e Robert Mueller dell’FBI durante un incontro svoltosi a Washington D.C. nel 2014. Secondo Kolokoltsev, tale cooperazione comprenderà l’elaborazione e la realizzazione di operazioni speciali congiunte, così come lo scambio di informazioni, per contribuire a contenere il cyber crime, oltre a identificare un modello operativo comune contro il crimine informatico. Il Governo russo intende progettare anche una struttura di sicurezza efficace contro elevati programmi maligni, simili al famoso e altamente complesso worm “Stuxnet” (in grado di mettere fuori uso le centrifughe per l’arricchimento dell’uranio presso l’impianto di Natanz in Iran nel 2010), oppure il più recente worm denominato “Regin”. Sarebbe stata valutata anche l’eventualità di prendere le distanze dalle precedenti proposte avanzate dal Servizio Federale di Sicurezza della Russia il quale ha posto un veto sull’utilizzo di Skype per la comunicazione online e Gmail come servizio di posta elettronica, in quanto tali servizi non consentono, in un Paese come la Russia, un controllo del traffico dati da parte delle Agenzie di Intelligence, a causa delle modalità di cifratura del traffico dati. In ogni caso è possibile prevede l’imposizione di un divieto di utilizzo per quel che concerne l’algoritmo crittografico RSA nei sistemi di informazione russi.

Un'altra parte della nuova strategia contempla un maggiore impiego di sistemi di sicurezza biometrica a partire dal primo semestre del 2015. Ciò dovrebbe includere l’utilizzo di impronte digitali per i passaporti biometrici per tutti i cittadini russi a

partire dall'età di 12 anni. L'attuazione della strategia sarà effettuata da una Commissione Speciale dello Stato russo, coordinata dal Senatore russo Ruslan Gattarov.

Secondo Gattarov, attualmente solo gli Stati Uniti possiedono una "sovranità digitale" e un buon livello di sicurezza delle informazioni. L'attuazione della nuova strategia è destinata ad aumentare il livello di sicurezza delle informazioni in Russia, sostenuto da un elevato livello di sviluppo interno. Appare evidente che i sistemi informativi hanno un ruolo cruciale e decisivo.

Una linea guida ulteriore è la crescente importanza di una rete Web di matrice russa (RuNet) per l'economia nel proprio complesso, come evidenziato nel rapporto "Il Passaggio a un Internet Russo" di Frost & Sullivan. In tale rapporto è ravvisabile sia la posizione dominate da operatore nazionale sia l'enorme potenziale di crescita, con un numero di utenti Internet russi di base molto elevato. Tuttavia gli esperti spiegano che la piena separazione del segmento russo di internet, conosciuto come RuNet, dalle rete globale sembra sia impossibile sia per ragioni tecniche che politiche. Alexey Salnikov, Vice Direttore dell'Istituto "Information Security" presso l'Università Statale di Mosca, ha scartato questa eventualità. È improbabile che l'ICANN abbia le possibilità tecniche di tagliare fuori completamente uno o più segmenti della rete globale di Internet. La struttura di Internet prevede che se qualsiasi provider spegnesse gli apparati di rete, il traffico passerebbe attraverso un altro provider, in base a quanto dichiarato da Salnikov. In tutti i casi il Consiglio di Sicurezza della Russia, presieduto dal Vladimir Putin, è già all'opera per individuare una modalità con cui la Russia possa effettivamente riuscire a separarsi da Internet in caso di emergenza.