VIACIALDINI

Sicurezza cibernetica proteggere le reti

Sicurezza cibernetica. Nuovo assetto cyber nazionale, perché proteggere le reti è vitale per l'economia. Vitalità dei nuovi studi sulla crittografia, sulla scia di quello che tanti paesi stanno realizzando.

di Marco Santarelli

Sicurezza cibernetica. Proteggere il perimetro cibernetico vuol dire proteggere le reti in generale e anche, di riflesso, l'economia: ecco perché il nuovo disegno di legge sul perimetro di sicurezza nazionale cibernetica rappresenta una polarizzazione su tutto l'asse delle infrastrutture critiche. Vediamone l'impatto.

La direzione presa col disegno di legge sul nuovo Perimetro di Sicurezza Nazionale Cibernetica rappresenta da una parte una rivendicazione di maggiore autonomia dell'Italia nei confronti di altri paesi, uno strumento per assumere un ruolo centrale nella gestione delle problematiche web e soprattutto sociali.

Dall'altra fa percepire la vitalità dei nuovi studi sulla crittografia, sulla scia di quello che tanti paesi stanno realizzando per una propria crittografia o una propria rete non attaccabile dall'esterno, vedi Russia, Cina, Iran, Venezuela, in parte Israele e Cile.

Facciamo quindi qualche riflessione sul disegno di legge, partendo innanzitutto dal presupposto che non dobbiamo fare l'errore di quanti stanno continuando ad abbinare questo disegno con il solo mondo del web. La cibernetica non è infatti una singola scienza che gestisce le sole connessioni eteree: essa è un controllo o studio dei sistemi integrati, naturali ed artificiali, vivi o non-vivi, fondata nel 1948 dal matematico americano Norbert Wiener.

Un disegno di legge non solo per il web

Il nostro mondo è ormai integralmente costituito di sistemi intrecciati tra loro e che interagiscono. Il disegno di legge si rivolge, quindi, a questi sistemi che sono gli oggetti che ci circondano, le interazioni sociali, le economie di più paesi, la rete fisica di una strada ma anche una rete di computer, una cellula, un organismo vivente che produce ecosistema e tutti i macchinari intelligenti che interagiscono tra loro e con i vari device.

Lo strumento normativo sta cercando di dare più sicurezza alle infrastrutture esistenti che colloquiando ad una velocità altissima possono essere vulnerabili. Quindi proteggere il perimetro cibernetico vuol dire proteggere le reti in generale e anche, di riflesso, l'economia. La possibilità che ogni connessione ad alta velocità (anche e non solo 5G) sia attuabile è chiaramente alta, ma non può essere realtà se non ha il supporto delle reti e, appunto, delle infrastrutture che sono alla base della struttura di ogni connessione.

Da questo lato non dimentichiamo le parole di qualche giorno fa del presidente del Copasir, Lorenzo Guerini, che ha affermato che un provvedimento del genere (in quel

caso riferendosi al Golden Power) può essere uno "snodo fondamentale nel contesto del sistema di sicurezza cibernetica nazionale". Qui non è in ballo la mera velocità di un collegamento o la sua ipotetica applicazione secondo solo delle norme, bensì l'incertezza del nostro Paese che ha di fronte dei pericoli seri che vanno dagli hacker ai blackout.

Dopo la direttiva NIS e il nuovo comma 3-bis inserito nell'art. 1-bis del DL 21/2012, questo disegno di legge fa il paio e completa l'indagine di qualche tempo fa sui big data di Agcom, Antitrust e Garante Privacy. Con tale disegno, non si assiste, quindi, solo ad una politica di attenzione maggiore sulla Cyber Security, ma una polarizzazione su tutto l'asse delle infrastrutture critiche. Si rendono consapevoli i tanti che ancora oggi approcciano il sistema cibernetico a piccoli mattoni, senza capirne l'interezza e la loro dipendenza.

I tre compiti principali e i relativi impatti

In tal senso nel suo interno ci sono tre principali compiti con relativi impatti. Vediamo quali.

Il primo è l'acquisizione da parte dello Stato di veri poteri speciali (citati ed ereditati anche dal già Golden Power).

Il secondo è generare, in una sorta di reticolarità di informazioni, la tutela della difesa e della sicurezza nazionale e

il terzo va a definire in maniera finalmente seria una disciplina come quella dell'omogenizzazione degli interventi (in termini di contratti) su reti fisiche e reti "eteree" date dai cloud o server dislocati.

Cosa accade fattivamente all'interno di questi tre compiti? Il primo, quello dei poteri, nasce in maniera diretta nel controllo e nella valutazione di un'eventuale gestione errata delle reti nelle loro interazioni. Ovvero si monitorano i fattori di vulnerabilità dei dati, di una cosiddetta tecnologia emergente, ma anche di come tali tecnologie impattano nella nostra realtà quotidiana. In pratica nel momento in cui si vanno ad aggiornare le reti in base al nuovo flusso dei dati si tende a controllare l'integrità e la caducità degli stessi che circolano ad una velocità mai conosciuta prima.

Questo aspetto è fondamentale nella cosiddetta "catena di valore" dei prodotti in circolazione e dei contratti in essere. Da qui si dovrebbe obbligatoriamente capire il flusso della realizzazione di una rete. Cioè dal contenuto del dato, ai suoi tempi e relative modalità di sviluppo informativo. Questo aspetto è proprio fondamentale per la riduzione delle asimmetrie tra utenti e operatori digitali.

Viene monitorato il processo dalla prima fase della raccolta dati e viene studiato nella sua trasformazione a informazione nelle piattaforme digitali degli operatori. Quindi come i dati transitano nei cavi sotto forma di flusso e come vengono utilizzati dalle società di rilievo e come tali dati si intersecano con gli oggetti. In questo scenario sarà importante tenere conto della provenienza delle sorgenti dei dati e come queste ultime generano quelle che possiamo chiamare "entità destinanti". Se questi dati hanno una sorgente definita, la vera sfida sta nella possibilità di comprensione del come vengono interpretati e di quale ruolo avranno. Il primo compito apre la strada al secondo: ciò che questo perimetro può dare nella tutela della difesa e della sicurezza nazionale. Qui riusciamo a tracciare il percorso dei dati in una rete definita, per capirne i collegamenti, i canali di interconnessione tra nodi e i nodi di commutazione chiamati switching nodes.

Questi ultimi sono da controllare bene perché se non si controlla questo percorso (il vero perimetro che di per sé è illimitato) si tende a non individuare l'informazione finale. Se non c'è controllo dell'interconnessione, provenienza e sviluppo dei dati sulla rete, si potrebbero perdere i nodi terminali e le informazioni in cui un sistema si pone come tale. Tale interconnessione è proprio della rete sociale ma anche degli attacchi Cyber. Questo

atteggiamento mette in “contatto” i dispositivi con i loro stessi collegamenti.

Qui un altro punto importante del disegno di legge e della sua necessaria ricezione. I device oggi sono interconnessi con le cose (anche se in una percentuale bassa rispetto a ciò che dicono) e queste ultime hanno lo scopo di tramutare e consentire il messaggio iniziale in un’altra realtà fisica, che chiamiamo comunemente Internet del Tutto (che sta sostituendo Internet delle cose) o segnali di commutazione.

Se ad esempio aumenta la velocità del trasferimento dei dati, deve altresì aumentare la possibilità di capire come quel trasferimento sta avvenendo e come farlo “dialogare” con le altre cose. Qui con l’istituzione del perimetro il controllo dovrà essere l’oggetto di quel trasferimento. Se aumentiamo questo controllo dobbiamo essere consapevoli che le reti, passando dalla banda larga, diventano dei core networks, cioè degli smistatori integrati in cui in mezzo dovrà passare il controllo delle reti pubbliche, private, integrate, radio, wireless e tanto altro. Questo secondo compito mira a individuare possibili fattori di vulnerabilità e apre le porte alla verticalizzazione e alla consapevolezza di delineare, nel suo terzo compito, una disciplina e “l’omogenizzazione” di talune regole.

Qui iniziamo a parlare seriamente di applicare il perimetro cibernetico. Si delimita e si sensibilizza, da parte dello Stato, tanto l’impresa privata che le PA, per riportarle ad un senso di responsabilità transnazionale in cui i timori della piramide della vulnerabilità, posti dalla velocità dei dati stessi, sia non un quadro normativo da incorniciare, ma un possibile riferimento dei pericoli della rete stessa. Quest’ultimo compito mira a rendere consapevoli gli addetti ai lavori, del fatto che portare la sicurezza nella propria infrastruttura attraverso un percorso articolato composto da link propedeutici può causare solo problemi e danni di tipo trasversale ed è esattamente obsoleto.

L’approccio Directory Trasversal

Il disegno di legge andrebbe a contrastare questo composito approccio chiamato anche Directory Traversal. Da una pagina di informazioni di una singola impresa o PA qualsiasi hacker può risalire ad ogni singola informazione di quel file. Una sorta di informazione su come quel sistema colloquia nel suo interno. Dai sistemi di movimentazioni delle merci, alle abitudini degli impiegati al sistema sociale in genere fino a poter entrare nella rete aziendale per poi linkare file depositati sui server e attaccare il sistema stesso.

Studiato il sistema e represse tutte le informazioni (anche quelle operative e di controllo) basta lanciare una query SQL dentro l’azienda studiata e distruggere i sistemi. Si agisce sugli script che alterano la stabilità del sistema. In tal caso, oltre che ai dettagli tecnici come l’introduzione delle Intrusion Detection System (IDS) e Web Application Firewall (WAF) serve la presenza forte e dettagliata dello Stato. Il perimetro cibernetico può fare questo: si potrebbe iniziare a sentire forte anche la possibilità delle imprese di investire nelle risorse interne e in consulenti seriamente competenti. (https://www.agendadigitale.eu)

di Marco Santarelli
(30/07/2019)