Memoria - A C. 3161, di conversione del decreto-legge 14 giugno 2021 n. 82 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"

1° luglio 2021

Negli ultimi mesi abbiamo osservato alcuni tra i più estesi e preoccupanti attacchi cyber della storia diretti ad infrastrutture digitali strategiche, quali organizzazioni governative, aziende ed utilities, ma anche ai cittadini dei Paesi democratici. Queste minacce sono più che mai efficaci ed in grado di penetrare anche in prodotti e servizi ampiamente diffusi ed utilizzati sia nel pubblico quanto nel privato.

In questo contesto, valutiamo positivamente le iniziative messe in campo dal Governo e dal Parlamento in materia di cybersecurity e supportiamo il processo di razionalizzazione degli strumenti normativi e degli attori istituzionali impegnati in questo settore. In particolare, concordiamo con l'approccio di istituire processi che garantiscano un efficace dialogo tra i soggetti istituzionali ed il settore privato.

La cybersecurity è per Google cardine e fondamento della sua strategia di prodotto. Negli ultimi dieci anni abbiamo lavorato alla progettazione di un'infrastruttura e di prodotti in grado di garantire la sicurezza su larga scala: ogni giorno Gmail blocca oltre 100 milioni di tentativi di phishing prima che raggiungano i nostri utenti nel mondo e Google Play Protect passa in scansione 100 miliardi di app alla ricerca di malware e altre insidie. Il nostro obiettivo è offrire il **cloud più affidabile** nel mercato e a questo scopo abbiamo dedicato un team come Project Zero che è specializzato nella ricerca e correzione di vulnerabilità nel Web per rendere internet più sicuro per tutti noi.

Il nostro approccio è basato sulla consapevolezza di un ambiente caratterizzato da minacce cibernetiche in evoluzione, la condivisione di informazioni con l'intera industria e la leadership della comunità internazionale dedicata alla sicurezza. Accogliamo con favore il crescente impegno da parte dei governi di tutto il mondo, Italia in primis, ad affrontare le più recenti sfide di cybersecurity. I recenti attacchi hanno reso necessaria una maggiore collaborazione internazionale nelle aree più critiche.

Modernizzazione e innovazione nell'ambito della cybersecurity

Google supporta con convinzione le iniziative di modernizzazione dei sistemi ICT e di rafforzamento della resilienza delle catene digitali del valore previste dal PNRR. A tal proposito, supporta l'adozione di best practices globali come il ***framework zero trust.*** Come la comunità internazionale ha potuto osservare nell'ambito degli attacchi a SolarWinds e a Microsoft Exchange, i sistemi proprietari e limiti all'interoperabilità e alla portabilità dei dati amplificano le

vulnerabilità di rete, rendendo gli attacchi più distruttivi. Restare legati ad un unico sistema di legacy, inoltre, impedisce alle organizzazioni pubbliche e private di beneficiare delle più recenti soluzioni di cybersecurity basate sul Cloud. Queste consentono di aggiornare e modificare le proprie impostazioni di sicurezza rapidamente e frequentemente - un elemento fondamentale di ogni strategia di cyber-defense.

In aggiunta alla modernizzazione dei sistemi ICT, e su modello di quanto recentemente proposto dal Governo americano, Google sostiene da sempre l'importanza di mettere in sicurezza la supply chain del software, realizzando tecnologie e lavorando per la diffusione di standard che migliorano l'integrità e la sicurezza del software.

Partnership pubblico-private

Come recentemente sottolineato dal Sottosegretario alla Presidenza del Consiglio Franco Gabrielli, l'infrastruttura cibernetica italiana del settore pubblico presenta numerose criticità e richiede tempestive azioni di modernizzazione.

Pertanto, giudichiamo positivamente che tra i compiti dell'Agenzia vi sia quello di perseguire obiettivi di eccellenza per realizzare innovazione attraverso partnership con il sistema delle università e della ricerca e il settore privato. Miglioramenti significativi nella cybersecurity richiedono infatti che il settore pubblico ed il privato lavorino insieme in aree strategiche come la condivisione di informazioni sulle minacce cibernetiche, lo sviluppo di una strategia difensiva completa contro i ransomware e il coordinamento su come identificare ed investire negli strumenti di sicurezza di nuova generazione.

Google si impegna per il progresso della sicurezza informatica collettiva. Negli ultimi anni, abbiamo bloccato numerosi attacchi, inclusi quelli provenienti da entità governative. Questo ci ha consentito di sviluppare una grande esperienza pratica sulle soluzioni più efficaci per proteggere i nostri clienti e per consentire a governi ed aziende di non dipendere da quelle stesse tecnologie che hanno provocato incidenti ed attacchi.

I Governi possono trarre numerosi vantaggi dalla collaborazione con l'industria e Google è orgogliosa di fare la sua parte. Il nostro auspicio è che pertanto il dibattito italiano ed europeo sulle regole di un digitale "sovrano ed europeo" si collochi in una cornice di collaborazione con gli Stati Uniti, alleato strategico dell'Europa, che con l'Europa condivide mentalità e valori fondamentali, come quelli della democrazia, dei diritti umani, della privacy e della protezione in sicurezza dei dati di cittadini e aziende, anche in linea con la recente creazione del TTC - Trade and Technology Council.