Il futuro della digitalizzazione

La sfida di Leonardo per la sicurezza dei dati

La crescita delle minacce informatiche rende la cybersecurity strategica L'ad Cingolani: «Per la difesa di un Paese contano più i byte dei proiettili»

LUIGI MERANO

Solo nel 2022 l'incremento medio, rispetto all'anno precedente, è stato del 180%. Si tratta degli attacchi cyber perpetrati tramite le tecniche offensive più diffuse, dai ransomware ai DDoS (distributed denial of service, ossia il tentativo ostile di bloccare il normale traffico di un server), passando per wipers, phishing e campagne di disinformazione. Sono gli analisti di Leonardo ad aver elaborato il dato puntuale, sottolineando nei loro report qualitativi come il conflitto tra Russia e Ucraina abbia inoltre reso l'Europa sempre più oggetto di minacce ibride: combinano molteplici tecniche e attori diversi, con ripercussioni critiche, talvolta anche a livello di sicurezza nazionale. In sintesi, attacchi sempre più numerosi, sofisticati e impattanti. Non a caso, è dal 2012 che la Commissione Europea dedica il mese di ottobre alla promozione dell'importanza della sicurezza informatica per i cittadini e le organizzazioni di tutti gli Stati membri.

Il concetto di guerra ibrida (hybrid warfare) ha assunto, complice lo scoppio del conflitto in Ucraina, una valenza e una importanza strategica di prim'ordine. Nel cyberspazio, che a tutti gli effetti è un dominio militare, essendo decretato tale nel 2016 dalla NATO, l'hybrid warfare supera l'ambiente puramente militare in quanto combina la manipolazione dell'informazione con la guerra informatica. «La difesa sarà sempre più fatta con i bytes, oltre che con i bullets», ha, a più riprese, sottolineato l'Amministratore Delegato e Direttore Generale di Leonardo, Roberto Cingolani, evidenziando che i dati, quindi, oltre e forse più che i proiettili, sono un'arma d'attacco. I dati sono diventati il vero patrimonio da difendere per proteggere una Nazione e per permetterle di prosperare.

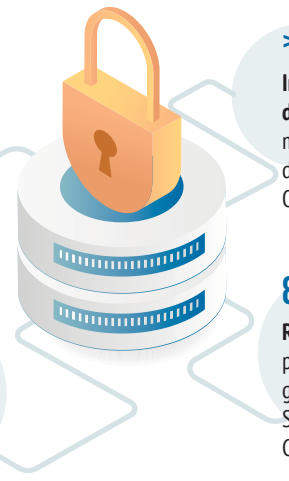
CYBER-SECURE BY-DESIGN

«Il livello di digitalizzazione di un Paese determina il suo posto nel mondo, al pari, o forse più, del PIL», ricorda Cingolani, «e la capacità di calcolo e di storage pro capite è l'indicatore più appropriato per definire il livello di avanzamento di un Paese». Il digitale è sempre più una risorsa strategica, «sia in ambito militare che civile, facciamo sempre più affidamento su tecnologie come il supercalcolo, il cloud e i servizi satellitari, che sono fondamentali per produrre e memorizzare i dati: tutti questi dati e infrastrutture devono essere protetti e tutelati», sintetizza Cingolani.

Se, quindi, il mercato della sicurezza informatica è un mercato in sensibile crescita, è anche vero che questa non può essere considerata come un addendum. Proprio la cyber security, insieme allo spazio, rappresenta uno dei due pilastri del nuovo Piano Industriale di Leonardo che verrà lanciato ad inizio del 2024. «Per noi, la cyber security sarà sempre più una piattaforma tecnologica comune a tutti i prodotti di Leonardo che, dai velivoli agli elicotteri, dai satelliti ai sistemi elettronici, dovranno essere cyber-secure by-design, ossia elaborando gli aspetti di sicurezza informatica sin dalla fase di progettazione e lungo tutto il ciclo di vita», sottolinea Cingolani. «Questo è un vantaggio competitivo che Leonardo deve poter sfruttare: siamo una delle pochissime aziende tecnologiche che possiede il know how per fare tutto, hardware e software», ricorda l'Ad, «e inserendo la cyber security sin dalla progettazione saremo in grado di offrire prodotti più competitivi che ci garantirà, negli anni, un incremento nei ritorni».

Per l'amministratore delegato di Leonardo, Roberto Cingolani, «la capacità di calcolo e di storage pro capite è l'indicatore più appropriato per definire il livello di avanzamento di un Paese»

LA CYBERSECURITY DI LEONARDO



>137.000
Eventi di sicurezza gestiti al secondo dal Global Securit Operation Center (SOC)

>5MLN
Indicatori di compromissione monitorati ogni anno dal Global Security Operation Center (SOC)

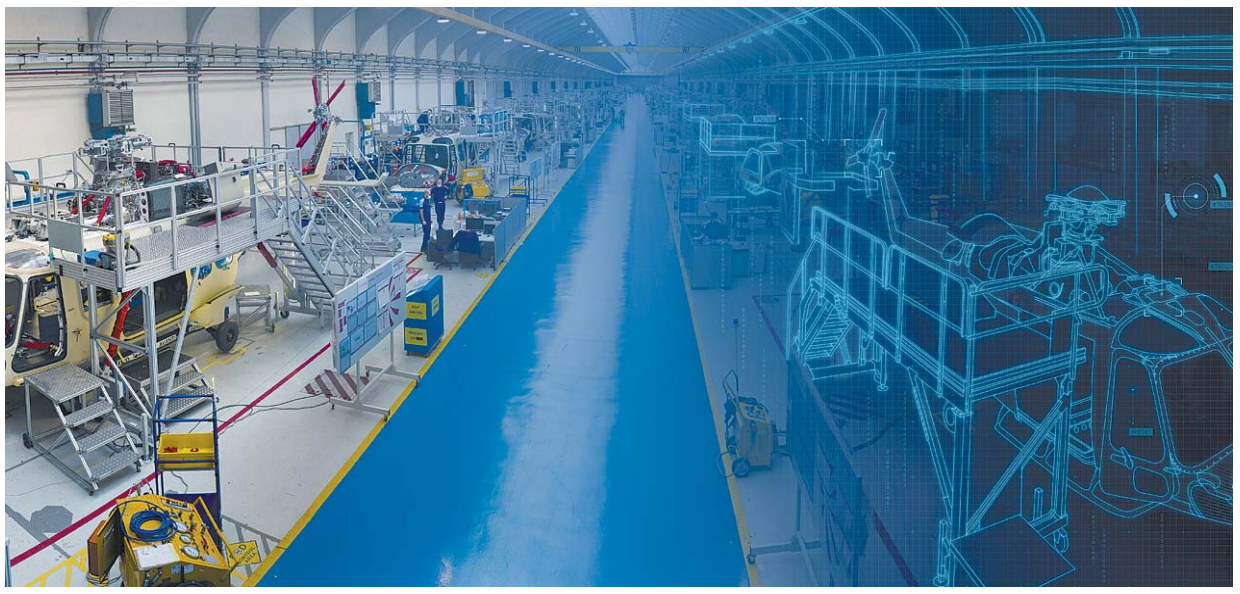
21.600
Incidenti di cyber sicurezza all'anno gestiti dal Global Security Operation Center (SOC)

8.500
Rapporti di intelligence personalizzati generati gni anno dal Global Security Operation Center (SOC)

WITHUB

CYBERSICUREZZA A 360 GRADI

In questa view prospettica, si aggiungono le altre attività che Leonardo sviluppa nel settore: progettazione di infrastrutture di cyber security e di soluzioni per la digitalizzazione, anche basate su cloud e intelligenza artificiale, monitoraggio della cyber security e gestione degli attacchi, piattaforme di threat intelligence (analisi della minaccia) e supporto alle attività investigative, formazione e testing attraverso piattaforme di cyber range. La strategia complessiva di Leonardo nell'ambito della cyber-sicurezza è quindi disegnata con lo scopo di proteggere a 360 gradi il Paese e permettere che i dati, il vero petrolio di oggi, possano essere valorizzati in sicurezza. La cyber security è infatti una conditio sine qua non della digitalizzazione. È necessario sviluppare la sicurezza nel controllo dei dati, così come possedere la capacità di elaborarli in grande quantità: dotarsi di macchine con potenza di calcolo adeguata, come il supercomputer davinci-1 sviluppato dall'azienda e in grado di effettuare 5 milioni di miliardi di operazioni in virgola mobile al secondo, e di capacità di addestrare modelli di intelligenza artificiale.



Il gruppo gestisce il centro europeo di analisi

La prevenzione dei rischi nella Ue

La sicurezza dei dati e delle infrastrutture digitali ha un livello prioritario nelle agende dell'Unione Europea e degli stati membri. Nel quadro del Digital Europe Program per il periodo 2021-2027, l'UE si è impegnata a investire 1,6 miliardi di euro in capacità di cyber-sicurezza a favore di pubbliche amministrazioni, imprese e singoli cittadini.

La sicurezza informatica è tra le priorità nel piano per la ripresa dell'Europa e riveste un ruolo fondamentale anche nello Strategic Compass, piano d'azione per rafforzare la politica di difesa e sicurezza europea di qui al 2030.

Dati, supercalcolo, AI, quindi, sono fondamentali, anche per prevenire e gestire un attacco cibernetico.

È quanto sta facendo Leonardo per DG Connect, la Direzione Generale della Commissione europea per le politiche digitali, per cui sta realizzando il primo centro pan-europeo per la gestione dinamica in real time del rischio cyber. Il centro - quello virtuale è già operativo, mentre si lavora al centro fisico - elabora e analizza terabyte di dati provenienti da fonti quali web, social media, mezzi di informazione, database, deep e dark web. Fa inoltre leva su una knowledge base costituita dagli oltre 5 milioni di Indicatori di Compromissione, tracce digitali di incidenti informatici, gestiti ogni anno da Leonardo anche grazie alle infrastrutture di supercalcolo dell'azienda.

Vengono così messi a disposizione di DG Connect scenari settoriali della minaccia (riferiti ad esempio a finanza, energia, sanità o trasporti), che consentono alla Commissione europea di conoscere in ogni momento il livello di rischio di attacco cyber alle infrastrutture digitali europee, i possibili attori malevoli, prevenire le probabili modalità di attacco, i potenziali obiettivi conoscendone le vulnerabilità.

L'eccellenza del Global Security Operation Center

Il cuore della struttura difensiva

Il centro di eccellenza per la cyber security di Leonardo è rappresentato dal Global Security Operation Center (Global SOC).

Con un'architettura distribuita, basata su una sede principale in Italia a Chieti, e altri centri operativi in Italia, Europa e Medio Oriente, il Global SOC fornisce una copertura di cyber security resiliente, monitorando e gestendo h24 e 365 giorni l'anno le vulnerabilità dei sistemi informatici di organizzazioni e infrastrutture critiche in tutto il mondo.

La sicurezza cyber è garantita in ogni fase: analisi della minaccia, monitoraggio costante dell'infrastruttura da proteggere, rilevazione degli attacchi e risposta, affiancando l'organizzazione sotto offensiva nella gestione della crisi fino alla sua risoluzione.

Le attività si basano sulle competenze degli analisti di Leonardo, esperti in ambito Cyber Security & Intelligence, su strutture di supercalcolo dedicate all'analisi della minaccia (threat intelligence) e su data center che abilitano i servizi di monitoraggio e gestione delle infrastrutture IT e industriali (OT). Le informazioni derivanti dalle attività di threat intelligence sono correlate con i circa 137.000 eventi di sicurezza al secondo provenienti dai sistemi di monitoraggio delle infrastrutture gestite dal Global SOC, per rendere ancora più efficiente il processo di generazione automatica degli allarmi presi in carico dagli analisti di Leonardo. Ogni anno, gli incidenti di cyber sicurezza gestiti dal Global SOC ammontano a circa 21.600.

VkVSlyMjMWU5MmQ3ZDktNjM0NS00YTkwLWFhYTQtNWE0ZDViYmEzMGJlIyMjZmYzYzBiNWMtMWE2Mi00MzdhLThiNjEtMzE0ZTNiOGVlYzI1IyMjMjAyMy0xMC0xOVQwNzo0Mzo0NCMjI1ZFUg==