STRATEGIE

Cybersecurity, è lo spazio la nuova frontiera: l'Europa schiera 7Shield

Il progetto dà una volata innovativa alla protezione dei segmenti di terra e delle risorse di dati satellitari. Mettendo le infrastrutture critiche al riparo delle cyber-minacce. Dall'IoT al machine learning, ecco le tecnologie avanzate integrate nel framework

12 ore fa

Luigi Romano
Ordinario di Sistemi per l'Elaborazione dell'Informazione, Università degli Studi di Napoli Parthenope

Nell'ambito della strategia della Commissione europea Horizon 2020, il **progetto 7Shield** contribuirà a rafforzare la resilienza e la sicurezza dei segmenti di terra dei sistemi spaziali per contrastare le crescenti minacce di carattere cyber-fisico dirette alle infrastrutture critiche europee. Analizziamo premesse e obiettivi delle nuove misure per la **cybersecurity**.

Indice degli argomenti

Sistemi spaziali, attacchi ai segmenti di terra

All'interno dell'attuale panorama europeo, **i segmenti di terra dei sistemi spaziali sono diventati ormai i principali obiettivi di tentativi di attacco**, soprattutto di carattere **cyber-fisico**. Gli impianti e le reti di comunicazione di tali stazioni sono, infatti, esposti a nuove e sempre più sofisticate minacce che rischiano di provocare gravi conseguenze in termini di sicurezza pubblica.

È noto, infatti, che **attacchi di carattere fisico destinati a segmenti terrestri sono in grado di inficiare la corretta distribuzione dei dati satellitari**.

Attacchi informatici rivolti, invece, alle **attività di archiviazione, accesso e scambio delle informazioni** rischiano di influire non solo sull'**affidabilità dei dati**, ma anche sui relativi standard "FAIR", vale a dire i cd. standard di reperibilità (findability), accessibilità (accessibility), interoperabilità (interoperability) e riutilizzabilità (reusability).

Ne consegue che l'affidabilità e la capacità di resilienza di tali segmenti assumono oggi un ruolo strategicamente rilevante per la **sicurezza complessiva delle infrastrutture critiche europee.**

Il valore della space economy

Questo anche alla luce del fatto che sono sempre maggiori le attività che si avvalgono del funzionamento di tali sistemi: **previsioni meteorologiche, telecomunicazioni, servizi audiovisivi, sistemi di sorveglianza delle catastrofi, operazioni connesse alla navigazione marittima, aerea e terrestre**, così come molteplici altre settori sfruttano, infatti, quotidianamente i servizi offerti da tali sistemi satellitari. Inoltre, **particolarmente elevato e di rilievo risulta il numero dei soggetti coinvolti nella gestione e nel funzionamento di tali sistemi**: si pensi, ad esempio, alle organizzazioni pubbliche nazionali e a quelle europee interessate, nonché ai grandi produttori di satelliti e ai fornitori dei relativi servizi, applicazioni ed attrezzature.

Tuttavia, nonostante l'importanza strategica di tali stazioni all'interno del panorama europeo della sicurezza, gli strumenti attualmente impiegati al fine di minimizzare e fronteggiare tentativi di attacco **non si avvalgono dei più recenti progressi in tale ambito basati sull'utilizzo dell'intelligenza artificiale e di tecnologie robotiche**.

Sicurezza informatica, il nodo responsabilità

Inoltre, nonostante la maggior parte dei segmenti terrestri incorporino già da tempo, sia all'interno dei propri processi orientati alla *product quality assurance*, sia all'interno dei relativi dipartimenti di sicurezza, i concetti di sicurezza informatica e di minaccia fisica, **le relative amministrazioni risultano essere responsabili esclusivamente della definizione e controllo delle attività connesse alla sicurezza dei prodotti e alla convalida delle attrezzature spaziali utilizzate**. Non ricade, invece, nella loro sfera di competenza la **responsabilità relativa all'implementazione dei protocolli di sicurezza**, attività che invece è generalmente **esternalizzata ed affidata a soggetti terzi specializzati.** Questo nonostante le stesse amministrazioni richiedano comunque l'adozione di un moderno sistema di controllo della qualità.

Da ultimo, i meccanismi di sorveglianza utilizzati, come è noto, sono realizzati nel rispetto degli **European Space Standards emanati dall'European Cooperation for Space Standardization (ECSS)**, tenuto conto anche di altri standard consolidati (ad es. ISO) e di ulteriori specifici requisiti di carattere individuale richiesti per gli *asset* spaziali. Tra questi assume particolare rilievo l'**Hazard Analysis standard** con il quale vengono definiti i principi, il processo e i requisiti da implementare nelle **attività di analisi dei rischi connessi ai segmenti di terra dei sistemi spaziali**. Tale standard opera ogni qualvolta emergano nell'ambito dei progetti spaziali pericoli per il personale o per il pubblico in generale, per i sistemi di volo spaziale, per le attrezzature di supporto a terra, per le proprietà pubbliche e private coinvolte, nonché in caso di minaccia per l'ambiente. Tuttavia, sebbene si tratti di uno standard attivo utilizzato dalla maggior parte degli operatori europei, **l'Hazard Analysis standard è stato creato nel 2008 ed è considerato ormai obsoleto.**

Sulla base di quanto evidenziato, è quindi necessario comprendere se gli esistenti livelli di protezione e di resilienza delle stazioni terrestri dell'Unione Europea possano considerarsi effettivamente **adeguati ed in grado di contrastare l'affermarsi crescente di nuove minacce fisiche ed informatiche**. Ed inoltre, se gli attuali **investimenti orientati al potenziamento dell'attuale quadro di sicurezza** e all'attuazione di sistemi di protezione avanzati porterà al desiderato miglioramento della relativa resilienza.

Come si articola il progetto 7SHIELD

Al fine di fornire risposte concrete ed efficienti ai problemi di cybersecurity delle applicazioni spaziali, la Commissione Europea nell'ambito del programma **Horizon 2020** ha finanziato il progetto **7SHIELD** (Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats), con il **Grant Agreement 883284**.

Il coordinamento del Consorzio rappresentato da 22 partner appartenenti a 12 diversi paesi europei e provenienti dal mondo accademico, della ricerca, delle PMI e delle organizzazioni rilevanti per il funzionamento delle stazioni terrestri, è affidato alla società **ENGINEERING Ingegneria Informatica** SPA, leader nel settore IT in Italia e tra i primi 10 gruppi IT in Europa. La società con i suoi quasi 12.000 professionisti operanti nelle 65 sedi dislocate in Europa, nel Nord e Sud America ha il suo core business nella **realizzazione di soluzioni digitali innovative per tutti i principali settori di mercato**.

Oltre a ENGINEERING, la partecipazione italiana è arricchita dalla presenza del **Centro Regionale Information Communication Technology**, organizzazione no-profit che promuove la cooperazione nell'ambito delle ricerca ICT, **RESILTECH s.r.l.**, PMI operante nel campo dei sistemi elettronici e informatici critici per la sicurezza e **SERCO Italia SPA**, azienda leader nell'ambito dell'industria e dei servizi spaziali.

ENGINEERING e i partner coinvolti lavoreranno per 24 mesi al rafforzamento della sicurezza e della resilienza dei segmenti terrestri dei sistemi spaziali europei (cd. *Ground Segments of Space Systems*) nel rispetto dei relativi criteri trasversali e settoriali ai sensi della Direttiva 2008/114/CE[1]. **L'obiettivo perseguito è quello di creare un quadro olistico che consenta di affrontare minacce complesse coprendo tutte le macro-fasi della gestione delle crisi**.

L'attività, infatti, prevede lo sviluppo e l'implementazione di **tecnologie di prevenzione degli attacchi fisici ed informatici** che contribuiranno ad ottimizzare la fase pre-crisi attraverso modelli di previsione analitica delle minacce future. In particolare, il progetto contempla l'impiego della **Cyber Threat Intelligence** (CTI) al fine di anticipare ed identificare minacce nuove ed emergenti, nonché di tipo complesso o ibrido. In tale ottica, **l'early warning mechanism (il meccanismo di allarme rapido) stimerà il livello di rischio prima del verificarsi di un attacco informatico o fisico** e consentirà l'adozione di risposte efficaci ed efficienti nel corso di un evento critico, tenendo conto anche dei vincoli di bilancio.

Obiettivi da raggiungere

Il progetto porterà anche alla realizzazione di un **risk-mitigation plan** aggiornato automaticamente e finalizzato ad offrire attività di ripristino in seguito ad un attacco intenzionale o ad un errore del sistema. Infine, a supporto della sicurezza e della resilienza delle installazioni private di segmenti spaziali terrestri **il progetto realizzerà scenari di continuità operativa, basati su un'innovativa articolazione delle più recenti tecnologie di monitoraggio e di previsione.**

Il risultato atteso è la creazione di un framework integrato, ma flessibile che consentirà l'**implementazione di servizi innovativi per la protezione cyber-fisica dei segmenti di terra**. Tali servizi saranno in grado di migliorare le capacità di protezione dei sistemi terrestri, integrando o **interagendo al contempo con le soluzioni di protezione già esistenti e implementate nelle relative installazioni a livello nazionale e sovranazionale**. Il framework, inoltre, avrà carattere **aperto** e perfezionerà tecnologie avanzate destinate all'integrazione, all'elaborazione e all'analisi dei dati, ai sistemi di machine learning, alla protezione dalle minacce informatiche e al rilevamento di attacchi informatici.

Integrazione di tecnologie di frontiera

La particolarità di **7SHIELD** consiste nel fatto che **il progetto integra al proprio interno una serie di risultati tecnologici all'avanguardia provenienti da settori multidisciplinari che spaziano dall'IOT alla tecnologia dei sensori**, dal ragionamento semantico alle attività di analisi del tipo high-level, dai sistemi di supporto alle decisioni alla gestione delle crisi. Nel quadro delle procedure previste dal progetto i dati ottenuti dalle reti di sensori di **7SHIELD** e quelli provenienti dalle infrastrutture già esistenti dei segmenti di terra saranno elaborati da innovativi **algoritmi di rilevamento delle minacce e da tecniche di fusione multimodale di alto livello.**

Utilizzando strumenti di **analisi visiva su misura**, il risultato sarà poi presentato agli operatori tramite un'interfaccia utenti interattiva. I professionisti del settore della sicurezza, i primi soccorritori e i fornitori di servizi di pubblica utilità saranno così abilitati ad utilizzare il **sistema di allarme rapido e di decisione di 7SHIELD**, disponendo anche di funzionalità per il monitoraggio di situazioni pericolose.

7SHIELD sarà, inoltre, distribuito e testato in diverse località, tra cui Finlandia, Grecia, Spagna, Italia e Belgio e le relative tecnologie saranno sperimentate in cinque casi d'uso pilota, costituiti da diversi scenari che coinvolgeranno episodi di attacco fisico, cibernetico o cibernetico/fisico.

Una così estesa fase di test e di dimostrazioni sarà strumentale al perfezionamento dell'approccio e all'analisi dell'efficacia delle nuove tecnologie, nonché alla solidità della piattaforma 7SHIELD e dei suoi moduli. Inoltre, consentirà di garantire l'interoperabilità di 7SHIELD con tutti i segmenti di terra e favorirà la standardizzazione dei processi.

Coordinamento con l'Agenzia Ue per la difesa

Il progetto 7SHIELD prevede, infine, una importante attività di coordinamento con l'Agenzia europea per la difesa (**EDA**) attraverso la realizzazione di opportune sinergie con i progetti **PYTHIA** (**Predictive methodologY for TecHnology Intelligence Analysis**) e **SOLOMON** (Strategy-Oriented anaLysis Of the Market fOrces in EU defeNce), entrambi coordinati da ENGINEERING Ingegneria Informatica SPA e finanziati nell'ambito della Preparatory Action for Defence Research (PADR).

Come è noto, tramite PYTHIA è stata sviluppata una metodologia innovativa destinata alla realizzazione di **previsioni tecnologiche strategiche nel campo della difesa** al fine di individuare le future sfide che emergeranno nel settore della ricerca nei prossimi 3-5 anni.

SOLOMON, facendo leva su PYTHIA, mira, invece, a **fornire all'Unione europea metodologie e strumenti necessari a garantire che le industrie operanti nel settore della difesa possano fare affidamento su un approvvigionamento affidabile**, superando le problematiche relative alle **dipendenze tecnologiche** della difesa critica. Con riferimento al progetto 7SHIELD, PYTHIA e SOLOMON contribuiranno con approfondimenti e previsioni su tendenze e forniranno scenari futuri per le tecnologie destinate alla difesa e alla sicurezza. A sua volta 7SHIELD trasmetterà a SOLOMON una serie di informazioni critiche relative alle emergenti minacce C/P, nonché soluzioni CIP che potranno anche influenzare il settore della difesa.

Note

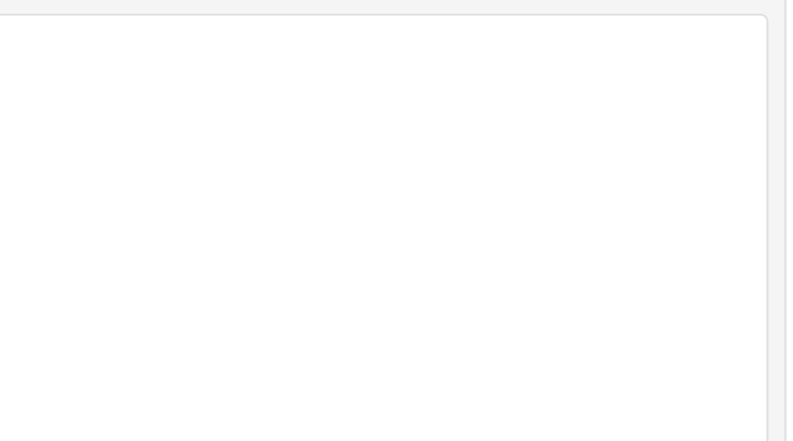
---

1. Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

Argomenti
Machine Learning | Tutto su Cyber Security
Canali
Sicurezza digitale

Articoli correlati

L'ANALISI
Microtargeting per la pubblicità politica: come funziona, per Usa 2020
13 Nov 2019
di Barbara Calderini
Condividi



PRIVACY E SANITÀ
Big data nel settore farmaceutico: gestirli nel rispetto del Gdpr
19 Nov 2019
di Anna Capoluongo
Condividi

INFRASTRUTTURE DIGITALI
Cybersecurity per IoT e 5G, il ruolo strategico degli standard
03 Mar 2020
di Giovanni Gasbarrone
Condividi

TUTTE LE TESTATE

Applicazioni e Tecnologie
AI4BUSINESS
BIGDATA4INNOVATION
BIG DATA & ANALITYCS ZEROUNO
BLOCKCHAIN4INNOVATION
CLOUD COMPUTING ZEROUNO
CYBERSECURITY CORCOM
CYBERSECURITY360
DOCUMENTI AGENDADIGITALE.EU
ECOMMERCE AGENDADIGITALE.EU
FATTURAZIONE AGENDADIGITALE.EU
INDUSTRIA 4.0 CORCOM
INDUSTRY 4.0 AGENDADIGITALE.EU
INFRASTRUTTURE AGENDADIGITALE.EU
INDUSTRY4BUSINESS
INTERNET4THINGS
PAGAMENTIDIGITALI
RISKMANAGEMENT360
SEARCHDATACENTER ZEROUNO
SEARCHSECURITY ZEROUNO
SICUREZZA AGENDADIGITALE.EU
SMART CITY AGENDADIGITALE.EU
SMART MOBILITY ECONOMYUP

PA
CITTADINANZA AGENDADIGITALE.EU
FORUMPA
PA DIGITALE CORCOM
SANITÀ AGENDADIGITALE.EU
SCUOLA AGENDADIGITALE.EU

Digital Transformation
AGENDADIGITALE.EU
CORCOM
DIGITAL4EXECUTIVE
DIGITAL4PMI
TECHCOMPANY360
ZEROUNO

Funzioni di Business
DIGITAL4FINANCE
DIGITAL4HR
DIGITAL4LEGAL
DIGITAL4MARKETING
DIGITAL4PROCUREMENT
DIGITAL4SUPPLYCHAIN
PROCUREMENT AGENDADIGITALE.EU

Startup e Open Innovation
ECONOMYUP
STARTUP AGENDADIGITALE.EU
STARTUPBUSINESS

Industry
AGRIFOOD.TECH
AUTOMOTIVEUP
BANKINGUP
ENERGYUP
INDUSTRY4BUSINESS
INSURANCEUP
MEDIA CORCOM
RETAILUP
SANITÀ AGENDADIGITALE.EU
SCUOLA AGENDADIGITALE.EU
TELCO CORCOM
TURISMO AGENDADIGITALE.EU

Studenti
UNIVERSITY2BUSINESS