Seminario 4

Aerospace cybersecurity

Le attività spaziali rivestono un ruolo fondamentale nella società moderna, influenzando settori critici come l'economia, le comunicazioni e la sicurezza nazionale. La crescente dipendenza da infrastrutture satellitari le rende, tuttavia, un bersaglio sempre più appetibile per attacchi informatici, con potenziali conseguenze devastanti.

Il **segmento spaziale** si compone di due elementi fondamentali:

- **Stazioni terrestri**: inviano e ricevono segnali dai satelliti;
- **Satelliti in orbita**: amplificano e ritrasmettono i segnali sulla Terra.

Vulnerabilità intrinseche del segmento spaziale

La proliferazione di piccoli satelliti a basso costo, basati su hardware e software commerciali (COTS), ha amplificato le vulnerabilità del segmento spaziale. Questi sistemi, spesso progettati con standard di sicurezza inadeguati, presentano numerosi punti deboli.

> **Info**
>
> L'espressione *"componente COTS"* o **componente OTS**, si riferisce a componenti hardware e software disponibili sul mercato per l'acquisto da parte di aziende di sviluppo interessate a utilizzarli nei loro progetti.

Tra i fattori che contribuiscono alla vulnerabilità del segmento spaziale, possiamo individuare:

- **Complessità della crittografia:** L'implementazione di robusti meccanismi crittografici sui satelliti è ostacolata dalle limitate risorse computazionali e dalla necessità di garantire la longevità delle chiavi crittografiche.
- **Vulnerabilità software:** La lunga durata di vita dei satelliti e la difficoltà di effettuare aggiornamenti remoti comportano la presenza di software obsoleto e vulnerabilità note non *patchate*. L'utilizzo di componenti COTS aggrava ulteriormente il problema, introducendo potenziali *backdoor* e falle di sicurezza.

- **Dipendenza da infrastrutture Cloud:** La crescente dipendenza dai servizi cloud per la gestione dei dati e il controllo dei satelliti introduce un ulteriore vettore di attacco. Un malfunzionamento o un attacco a queste infrastrutture potrebbe avere conseguenze catastrofiche sull'operatività dei sistemi spaziali.
- **Catena di approvvigionamento e terze parti:** La complessa catena di approvvigionamento del settore aerospaziale, con il suo intreccio di software, hardware e servizi forniti da terze parti, introduce numerosi potenziali punti di vulnerabilità. Attacchi mirati alla *supply chain* o a entità terze potrebbero compromettere l'integrità e la sicurezza dei sistemi spaziali.
- **Controllo fisico del satellite:** Tramite accessi al sistema di propulsione non autorizzati è possibile prendere il controllo del satellite e potenzialmente causarne lo schianto con un altro.

Le grandi organizzazioni come la NASA sono frequentemente bersaglio di **Advanced Persistent Threats (APTs)**, attacchi sofisticati e persistenti condotti da attori statali e non, con l'obiettivo di esfiltrare informazioni sensibili o sabotare le operazioni.

Tipologie di attacco e potenziali conseguenze

Le conseguenze di un attacco informatico al segmento spaziale possono essere estremamente gravi. Un attacco riuscito a una stazione terrestre potrebbe compromettere il controllo di uno o più satelliti, interrompere le comunicazioni o causare danni permanenti ai sistemi di bordo.

Gli attaccanti potrebbero **manipolare** le trasmissioni satellitari, **accedere** a informazioni riservate, **alterare** dati critici o addirittura **eliminare** le chiavi di crittografia, rendendo i satelliti inutilizzabili. Un'altra minaccia concreta è rappresentata dalla possibilità di causare collisioni tra satelliti o di deorbitare un satellite, facendolo rientrare nell'atmosfera terrestre con potenziali rischi per la popolazione e le infrastrutture.

L'isolamento fisico dei satelliti e la loro dipendenza dalle comunicazioni wireless li rendono vulnerabili a tecniche di attacco come il **jamming** (disturbo intenzionale del segnale), lo **spoofing** (falsificazione del segnale) e l'**intercettazione** delle comunicazioni. Inoltre, le limitazioni in termini di potenza di elaborazione e larghezza di banda disponibile rendono estremamente complessa l'implementazione di aggiornamenti software regolari, aggravando le vulnerabilità esistenti.

Gli attacchi informatici al segmento spaziale possono essere classificati in tre categorie principali:

- **Interferenza informatica spaziale:** Volta a causare interruzioni temporanee nella disponibilità o nella trasmissione dei dati, senza danni permanenti.

- **Attacchi informatici spaziali:** Mirati a produrre danni permanenti, come la distruzione del satellite o di componenti critici per il suo funzionamento.
- **Spionaggio informatico spaziale:** Finalizzato all'esfiltrazione di informazioni riservate senza causare danni evidenti. Lo spionaggio può essere propedeutico a successivi attacchi più mirati.

Sfide e prospettive future per la cybersecurity aerospaziale

L'attuale livello di sicurezza informatica delle infrastrutture satellitari esistenti è spesso **insufficiente**, e le politiche internazionali non sono ancora allineate alle sfide emergenti in questo ambito. La crescente dipendenza dai servizi satellitari rende la sicurezza informatica del segmento spaziale una priorità non più procrastinabile.

Molti dei satelliti attualmente in orbita sono basati su software obsoleto e vulnerabile, e la loro sostituzione o aggiornamento è un processo complesso e costoso. È quindi necessario un cambio di paradigma, che estenda le *best practice* di cybersecurity al settore spaziale commerciale, tenendo conto delle sue specificità.

La collaborazione tra agenzie spaziali, industria, comunità scientifica e organizzazioni internazionali è cruciale per migliorare la resilienza del segmento spaziale agli attacchi informatici. L'adozione di tecnologie innovative e l'implementazione di processi di "**security-by-design**", che integrino la sicurezza fin dalle prime fasi di progettazione dei sistemi spaziali, sono elementi chiave per proteggere le comunicazioni satellitari e garantire la continuità dei servizi offerti.