Allerta Cyber: La Minaccia Hacker alle Infrastrutture Critiche e l'Incidente ai Radar di Linate

Pubblicato il 30/06/2025

Il governo del Regno Unito, insieme ai suoi alleati internazionali, ha esposto **una campagna di cyberattacchi russi mirata a organizzazioni logistiche e tecnologiche occidentali**, tra cui quelle impegnate nell'assistenza all'Ucraina. In questo contesto, l'Italia deve affrontare la crescente minaccia informatica globale, che richiede un urgente potenziamento delle proprie capacità satellitari per rafforzare la resilienza nelle comunicazioni.

La campagna di cyberattacchi russi

Il governo britannico e i suoi alleati hanno recentemente svelato una serie di attacchi informatici condotti dal servizio di intelligence militare russo. **L'Unità 26165, nota anche come APT 28, ha preso di mira aziende logistiche e tecniche occidentali,** con un focus particolare su quelle coinvolte nell'assistenza all'Ucraina. Questi attacchi hanno sfruttato tecniche comuni

come il ***credential guessing*****, il *spear-phishing*** e l’esploitazione di vulnerabilità nei sistemi Microsoft Exchange. Inoltre, è stato rilevato un tentativo da parte dei cyber-attaccanti di monitorare i trasporti di aiuti umanitari destinati all’Ucraina, utilizzando sistemi di telecamere connesse a Internet localizzate ai valichi di confine.

Minacce alle organizzazioni logistiche

Secondo il National Cyber Security Centre (NCSC) del Regno Unito, gli attacchi informatici mirano non solo ai sistemi informatici ma anche alle infrastrutture critiche, tra cui i settori della difesa, dei servizi IT e della gestione del traffico aereo. La NATO, di cui l'Italia fa parte, è particolarmente vulnerabile a queste minacce, che potrebbero compromettere la sicurezza delle operazioni vitali per il supporto internazionale. Le aziende logistiche e i gestori di infrastrutture critiche devono essere consapevoli della vulnerabilità crescente di questi settori.

Nigel Smart, Direttore IT e Sviluppo di Logistics UK, ha sottolineato l'importanza di rafforzare la resilienza informatica delle catene di approvvigionamento. **Le organizzazioni devono adottare misure di sicurezza immediate per affrontare le minacce informatiche**. Le raccomandazioni del NCSC includono il monitoraggio continuo delle reti aziendali per rilevare attività sospette, l’adozione dell’autenticazione multi-fattore con metodi di sicurezza robusti, e l’applicazione tempestiva degli aggiornamenti di sicurezza. Le organizzazioni coinvolte nell'assistenza all’Ucraina sono particolarmente esposte a questi rischi e devono intervenire senza indugi.

Allerta Cyber: La Minaccia Hacker alle Infrastrutture Critiche e l'Incidente ai Radar di Linate - brigatafolgore.net

L'incidente ai radar di Linate e la necessità di protezione satellitare

Un recente guasto ai radar dell’aeroporto di Milano Linate ha sollevato preoccupazioni sulla vulnerabilità delle infrastrutture italiane. Sebbene l’Enav abbia inizialmente attribuito il problema a un malfunzionamento tecnico, non si può escludere la minaccia Cyber. Questo evento ha messo in evidenza l**a necessità di una protezione robusta delle infrastrutture di comunicazione, come i sistemi radar e le reti di navigazione aerea.** La protezione delle infrastrutture critiche italiane, in particolare quelle legate alla sicurezza nazionale e internazionale, richiede un potenziamento delle capacità satellitari.

Satelliti per IRIDE - brigatafolgore.net

Espansione delle capacità satellitari per l'Italia

In un contesto geopolitico e tecnologico in rapido cambiamento, l**’Italia deve potenziare le proprie capacità satellitari per rafforzare la resilienza nelle comunicazioni e proteggere le infrastrutture critiche. Le reti satellitari possono garantire la continuità delle operazioni in caso di attacchi alle reti terrestri.** La crescente diffusione di costellazioni satellitari come Starlink ed Eutelsat Oneweb dimostra come il settore privato stia investendo per garantire connessioni sicure, anche in contesti remoti. L’Italia deve accelerare l’espansione di queste capacità per rafforzare la propria sicurezza e quella delle operazioni logistiche vitali.

Conclusioni

La protezione delle infrastrutture critiche italiane passa attraverso il rafforzamento della resilienza informatica e l'espansione delle capacità satellitari. Gli attacchi informatici, in particolare quelli provenienti dalla Russia, rappresentano una minaccia crescente per la sicurezza globale. L’Italia deve affrontare queste sfide con soluzioni tecnologiche avanzate, tra cui l'integrazione delle comunicazioni satellitari, per proteggere le proprie infrastrutture e garantire la sicurezza delle operazioni internazionali. La capacità di monitorare e coordinare operazioni in tempo reale è essenziale per difendere il Paese da future minacce.

Link notizia: https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF