Attacchi informatici nel contesto Militare: una minaccia crescente alla sicurezza globale

Pubblicato il 10/02/2024

Negli ultimi anni, l'evoluzione tecnologica ha portato a un cambiamento significativo nel modo in cui vengono condotte le guerre e difese le nazioni. Al centro di questa trasformazione c'è l'ascesa degli attacchi informatici nel contesto militare, che sono diventati una delle minacce più significative e insidiose alla sicurezza globale.

Questi attacchi, che spaziano dal furto di informazioni riservate alla destabilizzazione di infrastrutture critiche, offrono agli aggressori un mezzo potente per influenzare le dinamiche geopolitiche senza necessariamente ricorrere alla forza militare convenzionale.

Gli attacchi informatici possono assumere molteplici forme, ognuna con obiettivi e metodi specifici. Ecco una panoramica dei tipi più comuni:

1. **Malware**: Qualsiasi software malevolo progettato per danneggiare o sfruttare qualsiasi programma, rete o sistema. Include virus, worm, trojan, ransomware, spyware e adware.

2. **Phishing**: Tentativi di ingannare le vittime affinché rivelino informazioni personali, come password e dettagli della carta di credito, attraverso email o siti web falsi che sembrano legittimi.
3. **Attacchi Man-in-the-Middle (MitM)**: Gli attaccanti intercettano la comunicazione tra due parti per rubare o manipolare i dati.
4. **Denial-of-Service (DoS) e Distributed Denial of Service (DDoS)**: Questi attacchi mirano a sovraccaricare le risorse di un sistema o di una rete, rendendolo inaccessibile agli utenti legittimi.
5. **SQL Injection**: L'attaccante sfrutta vulnerabilità nel software dell'applicazione per inserire o "iniettare" codice SQL malevolo in un database, consentendo loro di accedere o distruggere dati sensibili.
6. **Cross-Site Scripting (XSS)**: Un attaccante inserisce codice malevolo in pagine web visualizzate da altri utenti per rubare informazioni o per compromettere l'interazione dell'utente con l'applicazione.
7. **Zero-day Exploit**: Attacchi che sfruttano vulnerabilità di sicurezza non ancora note ai creatori del software o al pubblico. Gli attaccanti li usano prima che vengano corretti.
8. **Attacchi alla catena di approvvigionamento**: Mirano a compromettere i fornitori o i partner nella catena di approvvigionamento di un'organizzazione per accedere ai sistemi o alle reti dell'obiettivo principale.
9. **Ransomware**: Un tipo di malware che cripta i file della vittima, rendendoli inaccessibili, e richiede un riscatto per la decrittazione.
10. **Attacchi di Credential Stuffing**: Utilizzano elenchi di nomi utente e password rubati da un sito per tentare l'accesso ad altri siti, sfruttando il riutilizzo delle credenziali da parte degli utenti.
11. **Social Engineering**: Manipolazione psicologica degli utenti per farli compiere azioni o rivelare informazioni confidenziali. Non si basa su vulnerabilità tecniche, ma su quelle umane.
12. **Insider Threats**: Minacce alla sicurezza che provengono da persone all'interno dell'organizzazione, come dipendenti, ex dipendenti, appaltatori o partner commerciali, che hanno accesso interno ai sistemi o ai dati.

Questi attacchi possono avere obiettivi diversi, come furto di dati, interruzione dei servizi, danneggiamento di sistemi o reti, o truffa finanziaria. Le misure di sicurezza efficaci richiedono un approccio multistrato che comprende la protezione fisica, tecnica e amministrativa per mitigare questi rischi.

La nuova frontiera della guerra cibernetica

Gli attacchi informatici nel dominio militare rappresentano una nuova frontiera della guerra cibernetica, consentendo agli Stati e ai gruppi non statali di impegnarsi in azioni ostili con un grado di anonimato e deniabilità. Questi attacchi possono avere obiettivi diversi, tra cui:

- **Spionaggio Cibernetico**: Il furto di dati sensibili e segreti militari attraverso intrusioni informatiche è diventato una pratica comune, offrendo agli aggressori preziose informazioni su piani di difesa, tecnologie avanzate e strategie operative.
- **Sabotaggio**: Gli attacchi informatici possono essere mirati a disabilitare infrastrutture critiche, come reti elettriche, sistemi di comunicazione e controlli di armamenti, causando disordini e compromettendo la capacità di risposta di una nazione.
- **Disinformazione e Operazioni Psicologiche**: L'utilizzo di campagne cibernetiche per diffondere disinformazione e influenzare l'opinione pubblica è un altro strumento potente che può alterare l'equilibrio politico e minare la coesione sociale.

Sfide e risposte

La natura asimmetrica della guerra cibernetica pone sfide uniche per la difesa nazionale. La difficoltà di attribuzione, la velocità degli attacchi e la loro portata globale richiedono risposte innovative e collaborative. Le nazioni stanno investendo significativamente nel rafforzamento delle loro capacità di difesa cibernetica, sviluppando unità militari specializzate nella guerra informatica e cooperando a livello internazionale per contrastare le minacce cibernetiche.

Verso un framework di sicurezza collettiva

La crescente minaccia degli attacchi informatici nel contesto militare sottolinea la necessità di un approccio multilaterale alla sicurezza cibernetica. La creazione di norme internazionali per il comportamento nello spazio cibernetico, insieme allo sviluppo di meccanismi di condivisione delle informazioni e alla cooperazione in materia di difesa cibernetica, sono passi fondamentali

per prevenire l'escalation di conflitti e per garantire la stabilità globale.

Recentemente l'Esercito Italiano ha inoltre intrapreso un'iniziativa per rafforzare la consapevolezza e la preparazione delle sue forze di fronte a tali sfide. Di recente, è stata sviluppata e lanciata l'App Cyber Security Awareness (ne parliamo in questo articolo), una piattaforma progettata per educare e formare il personale militare e civile sulla sicurezza informatica. Con l'introduzione di questa app, l'Esercito Italiano sottolinea il suo impegno nel promuovere una cultura della sicurezza digitale che sia all'altezza delle sfide del XXI secolo.

Conclusione

Gli attacchi informatici nel contesto militare rappresentano una sfida complessa e in continua evoluzione alla sicurezza internazionale. Mentre le nazioni si adattano a questa nuova forma di conflitto, la capacità di prevenire, rilevare e rispondere efficacemente agli attacchi informatici sarà cruciale per mantenere la pace e proteggere le infrastrutture critiche. In questo scenario, la collaborazione internazionale e l'innovazione tecnologica giocano un ruolo chiave nel definire il futuro della sicurezza globale nell'era digitale.