FONDAZIONE BRUNO KESSLER
MAGAZINE

La Cyber sicurezza alle Olimpiadi

18 Febbraio 2026

Intervista a Matteo Rizzi che, con il Centro Cybersecurity FBK, sta attenzionando l'area attorno a Milano-Cortina dove crescono gli attacchi di hacker a istituzioni, centri di servizi e piccole imprese.

Sono generalmente cyber-attacchi fatti con l'intenzione di creare scompiglio, rendendo indisponibili siti web istituzionali e del governo (38%), di organizzazioni olimpiche (24%) e infrastrutture critiche (12%). Solo nella settimana di inaugurazione delle Olimpiadi, dal 2 all'8 febbraio, sono stati registrati 8.000 attacchi europei: il 42.9% di questi in Italia.

Non sono azioni fatte per rubare dati, al momento, "*ma non penso si faranno scrupoli, se questi hacker dovessero trovare il modo*", spiega **Matteo Rizzi, Science Ambassador e Security Administrator presso il Centro Cybersecurity FBK.**

Rizzi, perché un grande evento come le Olimpiadi invernali diventa un obiettivo privilegiato per gruppi di hacktivisti? E chi sono questi "hacktivisti".

Sono per la maggior parte hacker russi a rivendicare gli attacchi: gruppi autonomi mossi da motivi geopolitici, in particolare per contestare i finanziamenti all'Ucraina e l'esclusione della Russia dalle Olimpiadi. Il loro obiettivo è avere visibilità e dare allo stesso tempo una prova della loro forza: lo fanno colpendo siti web istituzionali o infrastrutture critiche.

Che tipo di attacchi dobbiamo aspettarci?

Sono azioni volte a creare disordine, inefficienze, a rendere indisponibili alcuni servizi.

Colpiscono ad esempio i sistemi di automazione industriale, quelli che servono per regolare pompe di calore o turbine, mandando in tilt alberghi e strutture di ospitalità come i villaggi olimpici. Spesso questi sistemi non sono aggiornati e basta una configurazione sbagliata per essere esposti al pericolo. Un'altro obiettivo hackerabile sono le telecamere a circuito chiuso, in luoghi pubblici e istituzionali.

In che modo FBK supporta il territorio e le istituzioni in vista di Milano-Cortina 2026?

Alla Fondazione Bruno Kessler abbiamo un **Laboratorio Congiunto tra il Centro Cybersecurity e il Servizio Soluzioni Digitali e Infrastrutture IT** che si occupa di gestire i rischi legati alla cyber security e in particolar modo quelli tecnici con attività di monitoraggio continuo della situazione in tempo reale. Per quanto riguarda il rischio umano, il **Joint Lab** mette in campo azioni di formazione e sensibilizzazione destinate ad aziende e istituzioni del territorio sui possibili attacchi.

Abbiamo visto, infatti, che questi attacchi puntano molto **sull'errore umano**: un'email, un click sul link sbagliato. E' quindi importante far crescere la consapevolezza collettiva, avvisare dei pericoli e sensibilizzare gli utilizzatori.

Quali misure concrete dovrebbe adottare oggi un'azienda per ridurre il rischio?

Italia è composta da piccole medie imprese, che possono facilmente diventare un obiettivo.

I **consigli** che diamo sono su due fronti: quello umano, ovvero essere molto attenti, soprattutto se ci si trova nell'area geografica "Milano-Cortina" e quello tecnico. Se le aziende sentono di non avere strumenti sufficienti per far fronte a questi attacchi ci si può appoggiare a dei provider più grandi (ce ne sono molti, anche gratuiti) che fanno da scudo assorbendo il traffico malevolo, un vero e proprio filtro nel caso di uno spam di richieste.

Come può un'organizzazione prepararsi a un possibile attacco senza creare allarmismo?

Ancora, la consapevolezza è importante. Gli occhi di tutto il mondo sono puntati sull'area delle Olimpiadi e sapere di essere un bersaglio è già buona parte del lavoro: porta già a tenere alta l'attenzione e attuare delle difese.

Seguirai le Olimpiadi? Qualche disciplina in particolare?

Non tantissimo, mi capita di vedere alcuni momenti. Mi piace molto lo sci da discesa, ammiro lo sfoggio di professionalità in uno sport che, personalmente, non so praticare.

LINK

https://magazine.fbk.eu/it/news/la-cyber-sicurezza-alle-olimpiadi/

TAG

- #ambassador
- #cyberattacchi
- #cybersicurezza
- #fbkscienceambassador
- #hacker
- #hacktivisti
- #jointLab
- #malevolo

- #olimpiadi
- #PMI

AUTORI

- Giovanna Rauzi