In aumento i cyber attacchi russi contro l’Italia: come difendersi

martedì 28 giugno 2022

Finalità dei cyber attacchi, che siano essi gestiti da singoli o da organizzazioni, è il danneggiamento della riservatezza e dell’integrità dei dati memorizzati nei sistemi informatici

Ogni settimana gli attacchi informatici da parte degli hacker russi aumentano. L’Italia si mantiene ancora “sotto assedio”, e a partire dallo scorso febbraio – mese in cui la Russia ha invaso l’Ucraina – i sabotaggi informatici sono esponenzialmente incrementati. Si alzano le difese, ma è comunque necessaria un’attenta prevenzione da parte degli utenti.

L’Italia nel mirino dei cyber attacchi russi

Finalità dei cyber attacchi, che siano essi gestiti da singoli o da organizzazioni, è il danneggiamento della riservatezza e dell’integrità dei dati memorizzati nei sistemi informatici. Compito dell’ACN, l’Agenzia per la cybersicurezza nazionale, è monitorare e sorvegliare gli incidenti nazionali, contenendo i danni e ripristinando la normale operatività.

A subire recenti attacchi hacker sono stati i siti web del Ministero degli Esteri, dell’Istruzione, dei Beni Culturali, del Csm, dell’Agenzia delle Dogane. Lo scorso 11 maggio anche la finale dell’Eurovision aveva attirato l’attenzione degli hacker.

Gli attacchi sono stati diversi, e se per quello subìto dall’Italia in occasione dell’evento musicale non si sono verificati danni, grazie al pronto intervento della polizia postale, per le altre azioni sono ancora in corso valutazioni da parte delle autorità, per capire se ci sono stati danneggiamenti.

Come proteggersi contro i cyber attacchi?

La sicurezza online è ormai un’emergenza, a causa dell’aumento degli attacchi informatici, i cui principali obiettivi sono estorcere denaro alle vittime. Ma ci sono alcuni accorgimenti che aiutano nel concreto a proteggersi da questi rischi.

L’utilizzo di una vpn, per esempio, consente sicurezza online, protezione della propria privacy, della propria posizione e dei dati di navigazione.

Le virtual private network garantiscono sicurezza anche nell’utilizzo di wi-fi pubbliche, così che l’uso di internet preservi la privacy e le informazioni personali. Ne esistono diverse, ma non tutte sono affidabili e sicure – alcune possono rallentare la velocità di connessione, per esempio – per cui conviene scegliere solo tra le migliori vpn, di cui è possibile leggere delle recensioni

dettagliate online. L’identità dell’utente viene così mascherata, impedendo ai siti web di accedere ai dati privati e agli hacker di rubare informazioni. L’utilizzo di social media e chat, inoltre, viene protetto, garantendo un utilizzo della rete sicuro e affidabile.

Massima attenzione va prestata a mail e messaggi privati: si consiglia di non cliccare e visualizzare link o allegati che possano apparire sospetti e di controllare l’affidabilità del mittente.

Verificare sempre richieste di amicizie, follow e contatti online ricordando di non accettare inviti da persone che non si conoscono realmente. Una navigazione sicura consente di allontanare il rischio di condivisione involontaria e inconsapevole dei propri dati.

Un altro pericolo dal quale tenersi lontano, forse meno noto del più comune “phishing”, è infine il “doxxing”, ovvero la diffusione da parte di hacker di informazioni private quali nome e cognome, indirizzo, numero di telefono, riguardanti una persona. Da questo punto di vista è importante prestare attenzione alle impostazioni sulla privacy settate sui diversi profili social, soprattutto per i minori, per esempio disattivando la funzione che permette di accettare tag di altri a proprie foto che vengono pubblicate online. Seguendo questi semplici navigare sul web sarà molto meno rischioso.

Fonte HelpConsumatori