Avviso di attacco DoS

Potrebbe aver ricevuto una lettera e/o un'e-mail da Sunrise nella quale le ha segnalato di aver ricevuto una notifica relativa a un traffico malevolo proveniente da un dispositivo che utilizza il suo collegamento domestico a banda larga. Se ha ricevuto tale comunicazione, non ha motivo di preoccuparsi. I suggerimenti presenti in questa pagina dovrebbero aiutarla a risolvere la questione.

Perché mi avete scritto?

Crediamo che un dispositivo nella sua rete domestica abbia partecipato a un attacco Denial of Service: un sistema di computer invia una grande quantità di traffico a un altro sistema di computer o rete con l'obiettivo di interromperne il collegamento a Internet.

Prendiamo molto sul serio questi attacchi, pertanto se pensiamo che un nostro cliente abbia un problema di sicurezza sulla sua rete, gli inviamo un avviso con consigli su come procedere.

Cosa è successo?

Abbiamo ottenuto una notifica relativa a traffico dannoso proveniente da un dispositivo nella sua rete domestica. Ci rendiamo conto che una sua diretta responsabilità sia inverosimile, tuttavia questo tipo di abuso viola la nostra politica di utilizzo accettabile. Se l'abuso dovesse proseguire nel tempo, potrebbe rendersi necessario sospendere o disdire il suo servizio a banda larga.

Ecco perché è importante che segua i consigli di questo articolo.

Nota: lo scopo di questo articolo è fornirle alcuni suggerimenti. Sunrise non è responsabile di eventuali inconvenienti occorsi durante la risoluzione del problema e non è in grado di fornire supporto tecnico per tali questioni.

Come si può risolvere il problema?

Se possiede conoscenze informatiche di base e nozioni sui dispositivi connessi, vi sono alcuni passaggi da eseguire per proteggere la sua casella di posta elettronica e la sua rete domestica.

Segua questi passaggi in sequenza:

1. **Verifichi le impostazioni del firewall**
    a. Acceda alla pagina di configurazione del suo router
    b. Acceda con il suo nome utente e password. Di default vengono visualizzati sul router stesso
    c. Selezioni l'opzione Port Forwarding
    d. Rimuova ogni regola relativa alle porte per cui, a meno che non sussista un'esigenza specifica, non vi è necessità che restino aperte. Se non sta utilizzando alcun server, probabilmente non avrà bisogno di lasciare aperte le porte.
2. **Si assicuri che tutti i dispositivi nella sua rete siano protetti da un firewall.**
    a. È importante verificare che tutti i dispositivi siano coperti dalla protezione di un firewall.
3. **Software antivirus**
    a. Consigliamo di eseguire scansioni antivirus su tutti i suoi dispositivi per rilevare e rimuovere eventuali infezioni.
4. **Aggiornamento del software**
    a. Tenga aggiornato il suo sistema operativo e il software delle applicazioni e installi le patch del software affinché i malintenzionati non possano approfittare di problemi o vulnerabilità note. Molti sistemi operativi offrono aggiornamenti automatici. Attivi questa opzione, se disponibile.

Questioni relative a Internet

Sunrise è co-fondatrice e membro di iBarry.ch, un'organizzazione senza scopo di lucro che collabora con esperti di sicurezza online per fornirle tutte le informazioni necessarie volte a proteggere lei e i suoi bambini online.

Ulteriori informazioni su iBarry sono disponibili su https://www.ibarry.ch/it/