Cisco: non farti cogliere impreparato e metti al sicuro le tue vacanze

Milano, 24 luglio 2019 - Come dimostrano i recenti studi, il periodo delle vacanze sono terreno fertile per i criminali informatici. In questo periodo solitamente si registra un aumento delle minacce informatiche. Nei periodi di vacanza, le aziende e i team di sicurezza si preparano a ridurre al minimo le attività, ciò significa che ci sono meno persone che controllano la rete e gli endpoint e si sa, con una minore attenzione alla sicurezza è più facile per i criminali passare inosservati. Non solo aziende e team di sicurezza sono a rischio nel periodo di chiusura estiva, ma anche i dipendenti contribuiscono all'aumento delle attività dannose poiché spesso utilizzano i dispositivi aziendali per collegarsi. Reti non sicure significano un accesso più facile e diretto all'endpoint da parte degli aggressori.

Cosa fare dunque? Ecco alcuni semplici ma importanti suggerimenti da tenere presenti per evitare di cadere nella rete di criminali informatici:

1) **Non lavorare mai da un dispositivo pubblico:** non usare dispositivi che non siano quelli aziendali. Non mandare messaggi e documenti di lavoro da computer presenti in luoghi pubblici come ad esempio negli Internet Café, la maggior parte di essi non è protetta in modo adeguato.

2) **Attenzione alle reti Wi-Fi pubbliche:** fate attenzione quando vi collegate a una rete Wi-Fi pubblica non protetta, il pericolo è dietro l'angolo! Quella stessa rete potrebbe collegarsi a sua volta a un dispositivo infetto e diffondere il virus anche al tuo dispositivo, e di conseguenza alla rete aziendale. Se hai necessità di inviare email di lavoro urgenti o di dover lavorare durante l'estate, chiedi al responsabile IT in azienda di installare una VPN tuo computer.

3) **Fate attenzione alle comunicazioni urgenti:** È possibile che siate contatti tramite email da criminali informatici che si fingono altre persone (ad esempio il consulente di un'azienda conosciuta). Il loro scopo è quello di indurvi a condividere dati sensibili come quelli aziendali, personali, bancari o relativi alla carta di credito, così come le password. Le informazioni vengono quindi utilizzate per accedere agli account, causando furti d'identità e perdite economiche.

4) **Controllate sempre attentamente l'indirizzo del mittente delle mail che ricevete**. C'è forse un piccolo errore ortografico? Verificate immediatamente – controllate sempre con una telefonata la richiesta di bonifici (non limitatevi a rispondere via email perché anche il truffatore può farlo! Dovrete filtrare qualsiasi messaggio che abbia un mittente (Mail-From) e un'intestazione "amichevole" (From) che contenga uno dei vostri domini nell'indirizzo e-mail di ricezione.

5) **Prima di partire, fai il backup dei dati:** ragione in più se sai che dovrai lavorare durante la tua vacanza. Archivia tutti i dati che ti serviranno per lavorare sulla rete aziendale e se sei un libero professionista fai un backup dei dati su un hard disk esterno.

6) **Infine, tenete sotto controllo il vostro dispositivo:** non importa quanto bene conosciate il luogo dove siete, non lasciatelo mai incustodito e non restate loggati ai siti se non li state utilizzando. Allo stesso modo, ricordatevi di disconnettervi se utilizzate un computer in un luogo pubblico, come in un business center o in un hotel.

2 suggerimenti per le aziende

- Se non volete avere brutte sorprese dai vostri dipendenti, assicuratevi che i vostri **sistemi di posta elettronica** siano adeguatamente protetti e aggiornati. In questo modo eviterete la compromissione delle email, bloccando spam, tentativi di phishing o attacchi ransomware.
- Proteggi gli endpoint dei tuoi dipendenti con **strumenti di gestione delle identità** **e** **di protezione avanzata degli endpoint.** Potrai così sempre sapere chi, quando, dove, da quali dispositivi e da dove i dipendenti accedono, bloccando automaticamente il software infetto e dando agli amministratori visibilità di ciò che sta accadendo nella rete aziendale.

E se sei una piccola media azienda, affidati a Cisco per una sicurezza "Senza pensieri"
Sempre più spesso le piccole e medie imprese si devono difendere da attacchi informatici sempre più sofisticati e dannosi, come ad esempio il recente VPN Filter. Per questo Cisco ha creato un pacchetto che include le migliori soluzioni tecnologiche per la sicurezza informatica chiamato "Sicurezza Senza Pensieri": un'installazione semplice, pochi interventi manuali e una fortissima automazione.

Segui Cisco Italia su:
Facebook page: http://www.facebook.com/CiscoItalia
Twitter: http://www.twitter.com/CiscoItalia
Youtube: http://www.youtube.com/CiscoItalia
LinkedIn: https://www.linkedin.com/company/cisco

Cisco
Cisco (NASDAQ: CSCO) è il leader tecnologico mondiale che dal 1984 è il motore di Internet. Con le nostre persone, i nostri prodotti e i nostri partner consentiamo alla società di connettersi in modo sicuro e cogliere già oggi le opportunità digitali del domani. Scopri di più su emear.thecisconetwork.com *e seguici su Twitter @CiscoItalia.*
Digitaliani: *l'impegno Cisco per la Digitalizzazione del Paese*

###

Ufficio Stampa

Cisco
Marianna Ferrigno

Tel: 800 787 854

email: pressit@external.cisco.com

Prima Pagina Comunicazione
Marzia Acerbi, Francesco Petruzzi

Tel: 02/91339811

email: ciscocorporate@primapagina.it