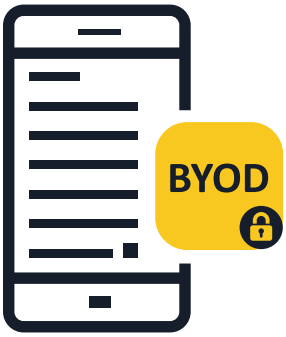
MALWARE MOBILE

SUGGERIMENTI E CONSIGLI PER LE AZIENDE

1 Informate il vostro personale sui rischi esistenti in mobilità

- In caso di lavoro in mobilità, i confini tra uso aziendale e uso personale diventano poco chiari. In caso di attacco inizialmente diretto al dispositivo mobile di un individuo, le conseguenze per un'impresa possono essere catastrofiche. Un dispositivo mobile è un computer e come tale deve essere protetto.



2 Attuate una politica aziendale di tipo "bring your own device" (BYOD)

- I dipendenti che utilizzano i propri dispositivi mobili per accedere ai dati ed ai sistemi aziendali (anche se solo e-mail, calendari o database di contatti) devono attenersi alle politiche aziendali. Selezionate attentamente quali tecnologie devono essere utilizzate per gestire e proteggere i dispositivi mobili ed esortate il vostro personale ad agire con cautela.

3 Cercate di includere politiche di protezione mobile nel vostro piano di sicurezza globale

- Se un dispositivo non è conforme alle politiche di sicurezza aziendale, non dovrebbe essere autorizzato a connettersi alla rete aziendale e ad accedere ai dati aziendali. Tutte le aziende dovrebbero implementare soluzioni di Mobile Device Management (MDM) o Enterprise Mobility Management (EMM).
- A completamento di queste soluzioni, è fondamentale installare una soluzione di Mobile Threat Defence. Ciò consentirà di avere una maggiore visibilità e consapevolezza contestuale delle minacce a livello di app, rete e sistema operativo.

4 Diffidate delle reti Wi-Fi pubbliche per accedere ai dati aziendali

- In generale, le reti Wi-Fi pubbliche non sono sicure. Se un dipendente accede ai dati aziendali utilizzando una connessione Wi-Fi gratuita presso un aeroporto o un locale pubblico, i dati potrebbero essere esposti a utenti malintenzionati. È consigliabile che le aziende sviluppino politiche per un "utilizzo efficace" in questo senso.

5 Tenete sempre aggiornati i sistemi operativi e le app dei dispositivi

- Raccomandate al vostro personale di scaricare gli aggiornamenti software per il sistema operativo dei loro dispositivi mobili non appena viene loro richiesto. Soprattutto per Android, cercate di acquisire informazioni sui gestori di telefonia mobile e i produttori di cellulari per conoscere la loro politica relativa agli aggiornamenti. Installando gli ultimi aggiornamenti, un dispositivo non solo è più sicuro ma ha prestazioni migliori.

6 Installate applicazioni provenienti solo da fonti attendibili

- Le aziende dovrebbero autorizzare esclusivamente l'installazione di app provenienti da fonti ufficiali sui dispositivi mobili che si connettono alla rete aziendale. In alternativa, vi consigliamo di valutare l'introduzione di uno store aziendale di app attraverso il quale gli utenti finali possono accedere, scaricare e installare app approvate dall'azienda. Consultate il vostro fornitore di soluzioni per la sicurezza per avere dei consigli per la configurazione o l'allestimento di uno store interno.

7 Impedite il jailbreak dei dispositivi

- Il jailbreak consiste nella rimozione delle limitazioni di sicurezza imposte dal fornitore del sistema operativo per acquisire l'accesso completo al sistema operativo stesso e alle sue caratteristiche. Effettuando il jailbreak del vostro dispositivo, la sua sicurezza può essere compromessa in modo significativo e aprire falle a livello di sicurezza che potrebbero non risultare subito evidenti. I dispositivi di tipo "root-enabled" non dovrebbero essere autorizzati ad accedere all'ambiente aziendale.

8 Valutate alternative per l'archiviazione cloud

- Gli utenti mobili desiderano spesso accedere a documenti importanti non solo tramite il PC che usano al lavoro ma anche dal loro telefono o tablet privato al di fuori dell'ufficio. Le aziende dovrebbero valutare l'allestimento di una soluzione di archiviazione sicura basata su cloud e l'introduzione di servizi di sincronizzazione di file per soddisfare queste esigenze in modo sicuro.

9 Incoraggiate il vostro personale a installare un'app per la sicurezza mobile

- Tutti i sistemi operativi sono a rischio di infezione. Se possibile, verificate che i vostri dipendenti utilizzino una soluzione per la sicurezza mobile in grado di rilevare e proteggere dal malware, dallo spyware e da applicazioni dannose, oltre ad offrire altre funzionalità a tutela della privacy e antifurto.