PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5362 di Venerdì 31 marzo 2023

Le quattro principali tipologie di attacchi a dispositivi mobili

Sempre più spesso i dispositivi informatici mobili vengono attaccati con varie tecniche, di cui non sempre gli utenti di questi dispositivi sono al corrente. Ecco un breve riepilogo.

Quasi ogni giorno abbiamo notizia di attacchi, indirizzati dai criminali informatici a dispositivi mobili. La conoscenza delle principali tecniche di attacco, opportunamente diffusa a tutti soggetti coinvolti, può rappresentare un prezioso strumento di prevenzione e messa sotto controllo di questo crimine informatico.

Phishing

È uno dei modi più semplici per portare un attacco. Il malvivente informatico si spaccia per un amico, conoscente o persona rispettabile, e manda un messaggio per posta elettronica o con chiamata telefonica. Gli hackers utilizzano anche tecniche di ingegneria sociale per individuare i soggetti, che più facilmente potrebbero essere vittima di questo tipo di attacco, cercando di venire a conoscenza dell'azienda in cui operano, la posizione aziendale informazioni, che possono essere usate per rendere più credibile la minaccia.

Come prevenire questo attacco.

La prevenzione più efficiente ed efficace è certamente quella di addestrare gli utenti ad individuare tempestivamente possibili situazioni di rischio. Ove si individui una situazione di rischio, la stessa deve essere immediatamente segnalata e responsabili della sicurezza informatica aziendale. Oggi sono disponibili anche degli applicativi, chiamati mobile threats defenses - MTD, che offrono un elevato livello di sicurezza contro questa tipologia di attacco. Questi strumenti funzionano effettuando uno scan dei collegamenti ed utilizzando algoritmi avanzati per bloccare, in tempo reale, eventuali attacchi.

Le app fraudolente

Queste app sono state progettate per raccogliere dati personali, ed anche aziendali, per un futuro utilizzo fraudolento da parte di soggetti terzi. Anche se i principali siti di app, messi a disposizione di acque, come ad esempio AppleApp Store o Google Play hanno introdotto delle specifiche garanzie, i criminali più di una volta sono riusciti a violarle. Vi è inoltre un rischio legato al fatto che sistemi mobili, come Android, permettono di installare applicazioni provenienti da fonti non certificate.

Come prevenire questo attacco

I responsabili della sicurezza informatica possono bloccare numerose applicazioni sospette, ma solo se l'apparato mobile del soggetto da proteggere è stato inserito in un appropriato database. Questi applicativi di protezione vengono contrassegnati dalla definizione mobile device management- MDM, e possono essere abbinati all'applicativo MTD, precedentemente illustrato. È inoltre importantissimo che i responsabili della sicurezza informatica sensibilizzino gli utenti sul modo corretto di utilizzare degli apparati, che possono essere usati per lo sviluppo di attività connesse all'azienda di appartenenza.

Le reti Wi-Fi non sufficientemente protette

Molte aziende mettono in guardia i propri dipendenti circa il fatto di utilizzare reti Wi-Fi, di cui non è conosciuto il livello di sicurezza. Una delle reti che recentemente ha ricevuto maggiori critiche è quella che si può trovare in una catena di negozi, che vendono vari tipi di caffè. La situazione è aggravata dal fatto che molti smartphone cercano di collegarsi automaticamente ad una rete conosciuta, quando l'apparato si trova nell'ambito operativo della rete. Un hacker può impersonare (spoofing) un servizio Wi-Fi, che viene erroneamente ritenuto accettabile dall'apparato mobile dell'utente.

Come prevenire questo attacco

Se la sicurezza informatica usa già applicativi MDM per stabilire regole rigide nell'utilizzo del collegamento con reti Wi-Fi, il livello di rischio diminuisce in maniera drammatica. Inoltre, applicativi MDM possono prevenire la perdita di dati e introdurre politiche di protezione criptografica di dati aziendali, presenti sull'apparato mobile. Ancora una volta, l'abbinamento di applicativi MDM ed applicativi MTD può consentire di raggiungere un più che soddisfacente livello di protezione

Comportamenti trascurati nell'aggiornamento delle app presenti sul dispositivo mobile

Il costante aggiornamento delle app, presenti sui dispositivi mobili, rappresenta un prezioso strumento di salvaguardia da possibili attacchi. Un'appropriata sensibilizzazione su questo tema permette di migliorare in modo significativo la sicurezza delle applicazioni presenti sul dispositivo mobile, a costi praticamente nulli.

Come prevenire questo attacco

Sia Apple, sia Google pubblicano regolarmente degli aggiornamenti, che permettono di mettere sotto controllo possibili debolezze degli applicativi. Ad esempio, per i sistemi Android, Google ha cominciato a pubblicare quasi ogni mese degli aggiornamenti di sicurezza, che gli sviluppatori di altre app possono inserire nelle proprie applicazioni. Anche Apple pubblica regolarmente degli aggiornamenti, che garantiscono un'elevata sicurezza del sistema. I responsabili della sicurezza informatica devono sensibilizzare, e direi perfino obbligare, i dipendenti su effettuare periodici aggiornamenti delle applicazioni presenti sul dispositivo mobile.

Ringrazio i colleghi di Computer Weekly per queste preziose informazioni.

Adalberto Biasiotti

www.puntosicuro.it