AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Ottobre, mese della sicurezza. Il cloud è sicuro? Il punto di vista di Proofpoint

Roma - 11 ott 2018 (Prima Pagina News) **Ottobre è il mese della sicurezza e in questo articolo Proofpoint risponderà alla domanda: il cloud è sicuro? I rischi del cloud computing Il cloud computing ha trasformato il modo in cui le aziende utilizzano, archiviano e condividono i dati, introducendo nuove minacce e sfide.**

Il panorama della cybersicurezza è in continua evoluzione e tenere il passo non è semplice. La protezione ha un impatto diretto sulla reputazione e sui risultati di business di un'azienda, quindi è sempre più importante affrontare gli argomenti e le sfide di sicurezza in modo che tutti possano comprenderli, anche le figure meno tecniche. Ottobre è il mese della sicurezza e in questo articolo Proofpoint risponderà alla domanda: il cloud è sicuro? I rischi del cloud computing Il cloud computing ha trasformato il modo in cui le aziende utilizzano, archiviano e condividono i dati, introducendo nuove minacce e sfide. A causa del volume di dati salvati nel cloud, è diventato naturalmente un obiettivo dei cybercriminali. Ad esempio, strumenti cloud come Office 365 e GSuite sono ottimi a livello di collaborazione ed efficienza, ma se la persona sbagliata dovesse accedervi dall'account di un dipendente, un'azienda sarebbe davvero a rischio. Non solo perché l'aggressore avrebbe accesso ai dati sensibili nel cloud, ma perché potrebbe procedere con il furto dell'identità degli impiegati. Un account cloud compromesso può portare a frodi, violazioni dei dati e molto altro. I più colpiti in azienda Si potrebbe pensare che gli unici bersagli siano dirigenti e manager di alto livello, ma la ricerca di Proofpoint ha rivelato che il 60% circa degli attacchi ha coinvolto collaboratori e middle management. I dipartimenti più colpiti sono operations e produzione, management e R&S/engineering. Tecniche di attacco I cyber criminali utilizzano numerose tecniche per ottenere accesso al cloud. Qui di seguito i tre metodi più comuni: 1. Violazione dei dati È la divulgazione intenzionale (o meno) di dati confidenziali in ambienti pubblici o non sicuri. Questo rischio non è esclusivo del cloud computing, ma è tra le prime preoccupazioni dei clienti di questa tecnologia. Le violazioni possono includere l'esposizione di informazioni e brevetti aziendali, dati personali sanitari, finanziari, proprietà intellettuale. 2. Attacchi phishing per furto delle credenziali L'obiettivo di questi attacchi è il furto di credenziali degli utenti, attraverso l'appropriazione dell'identità di un'azienda di fiducia e la richiesta dei dati di login dell'account cloud su un sito fittizio. Circa una persona su quattro aprirà un'email di phishing e oltre il 10% cliccherà il link pericoloso o aprirà l'allegato "armato" incluso nel messaggio. Ciò significa che a un aggressore è sufficiente inviare dieci email per avere il 90% delle probabilità di colpire un utente. 3. Brute Force Attack Un brute force attack è un metodo utilizzato per individuare una password di accesso inserendo tutte le possibili combinazioni fino a trovare quella giusta. È un procedimento più lungo rispetto al phishing, ma spesso si rivela efficace, in quanto molti utenti utilizzano la stessa password su diversi

account. Quale può essere la miglior difesa? Definire una strategia di sicurezza che abbia come primo obiettivo la protezione delle persone e non delle tecnologie utilizzate. Proofpoint mette a disposizione delle aziende una guida dedicata alla Cybersecurity nell'era moderna.

(Prima Pagina News) Giovedì 11 Ottobre 2018

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it