WHITE PAPER

5 MODI PER GESTIRE I RISCHI LEGATI A MOBILITÀ E IOT

Ridurre i rischi del network applicando le policy di sicurezza

aruba
a Hewlett Packard Enterprise company

TechTarget | Custom Media

INTRODUZIONE

I lavoratori di oggi sono più mobili che mai e non si intravede la fine della crescita della connettività dentro e fuori l'ufficio. Secondo Gartner, nel 2020 il mondo sarà saturo di dispositivi connessi, che supereranno i 21 miliardi.[1] Altri esperti sostengono che nello stesso anno ci saranno più persone dotate di dispositivo mobile rispetto a quelle che dispongono di acqua corrente e di un'automobile, mentre il traffico Internet sfonderà la barriera dello zettabyte.[2]

Il dibattito sulla sicurezza BYOD è chiaramente superato, dato che le organizzazioni si sono rese conto da tempo che, per restare competitive, hanno bisogno di avere una flessibilità tale da concedere agli utenti la libertà di connettere molteplici dispositivi, sia che essi appartengano o meno all'IT. La maggior parte delle organizzazioni è riuscita a raggiungere questo tipo di flessibilità con un approccio misurato, secondo cui occorre soddisfare determinate condizioni prima che il dispositivo di un utente possa avere accesso a dati sensibili. Tra queste vi sono condizioni relative allo stato del dispositivo, alle procedure di autenticazione utilizzate, la criticità dei dati a cui si accede e così via. Le organizzazioni di grande esperienza elaborano questi requisiti sulla base di solide valutazioni dei rischi e li codificano attraverso policy ufficiali. Queste policy sono volte a proteggere il network e i dati, sia in transito che inattivi, sui dispositivi mobili e Internet of Things (IoT, Internet delle cose).

Ma si tratta solo del primo passo verso la vera e propria gestione del rischio, in questa nuova era di connettività mobile always-on e iniziative IoT. Le policy sono valide in proporzione ai propri meccanismi di applicazione. Inoltre, molte organizzazioni non dispongono purtroppo della tecnologia e dei processi per trasformare realmente le policy di sicurezza in un'azione coerente, ossia tramite workflow di applicazione efficaci e automatizzati. Per attenuare realmente i rischi di violazione dei dati mobili e IoT, le organizzazioni devono prendere in considerazione i seguenti cinque passaggi.

CONTA ESCLUSIVAMENTE SAPERE CHI E COSA SI STA TENTANDO DI CONNETTERE

La maggior parte delle organizzazioni non è in grado di quantificare i rischi in un dato momento perché mancano la visibilità e i controlli relativi alle connessioni al network. Senza questa capacità fondamentale, le organizzazioni fanno fatica ad applicare le policy all'interno del network, individuare le spie di un'eventuale compromissione e comprendere il proprio grado di vulnerabilità rispetto alle nuove minacce derivanti da utenti e app mobili o IoT.

Le organizzazioni necessitano di una sistema automatizzato per inventariare tutto ciò che si connette al network e che tenta di connettersi.

Questa capacità dovrebbe includere il modo di sapere:

- Chi si connette
- Come e con quale dispositivo un utente sta tentando di connettersi
- Quali risorse saranno accessibili per il dispositivo dell'utente
- Quali rischi comporta quel particolare dispositivo o il permesso di accesso ai dati

LA VISIBILITÀ DEL DISPOSITIVO DEVE ESSERE ABBINATA ALL'APPLICAZIONE DI REGOLE NELLA NETWORK

Anche se il mercato offre diversi strumenti di gestione dei dispositivi che permettono alle imprese di avere uno sguardo panoramico dello stato della sicurezza dei dispositivi, tali strumenti hanno dei limiti. L'utilizzo di strumenti per la gestione di dispositivi mobili o endpoint è solo uno dei componenti di una solida strategia di sicurezza mobile, in quanto ad essi mancano i mezzi per realizzare l'applicazione di regole nel network.

Le organizzazioni devono essere in grado non solo di inventariare i dispositivi che si connettono al network, ma anche di limitare l'accesso in base allo stato di quei dispositivi. Le organizzazioni necessitano di un modo per visualizzare in maniera contestuale informazioni sul dispositivo come lo stato delle impostazioni sui permessi al suo interno, se sul dispositivo sia stato o meno eseguito il rooting, se esso disponga o meno di software completamente aggiornato e se mostri o meno sintomi di potenziale compromissione.

La possibilità di visualizzare questi elementi contestuali è un primo passaggio cruciale. Il passaggio successivo consiste nell'abbinare questo aspetto con un efficace mezzo di applicazione di regole nella network in base al grado di rispondenza delle condizioni del dispositivo alle attuali policy di sicurezza. Per proteggere meglio le risorse di rete e prevenire attacchi dai dispositivi a rischio, le organizzazioni necessitano di un controllo degli accessi automatizzato per garantire che

1 "Gartner: 21 Billion IoT Devices to Invade by 2020," InformationWeek, nov. 10, 2015
2 "Phones Will Drive Internet Traffic Past the Zettabyte Mark This Year," Recode, feb. 3, 2016

i dispositivi che non rispondono ai requisiti della policy non possano connettersi finché non vengono rimessi a norma.

IL CONTESTO CHE DEFINISCE UTENTE E AMBIENTE È UN FATTORE CRUCIALE

Quanti più dati sul contesto fluiscono nei controlli degli accessi, tanto più rifinite saranno le policy per determinare gli accessi stessi. Lo stato del dispositivo è importante, ma egualmente importanti sono le informazioni su chi sta mettendo le mani sui touchscreen in questione, da dove e addirittura per quanto tempo al giorno si stanno connettendo gli utenti.

Mentre le organizzazioni applicano le policy, è necessario che il controllo degli accessi sia abbastanza granulare da filtrare le risorse di rete in base ai privilegi degli utenti, alla località, all'orario del giorno e altro ancora. Inoltre, le aziende hanno bisogno di un modo per collegare più dispositivi ad un singolo utente e creare processi di applicazione di regole trasparenti che mantengano l'attenzione incentrata sul contesto dell'utente. Questo stesso contesto può essere utilizzato per monitorare il comportamento sia degli utenti che delle entità all'interno del network.

Infine, il controllo degli accessi dovrebbe avere l'automazione sintonizzata sul compito da svolgere, utilizzando il relativo contesto per ridurre al minimo i rischi associati alla mobilità.

NON IGNORARE LE CONNESSIONI VIA CAVO

Oggi la sicurezza mobile dipende in gran parte dalla qualità con cui le organizzazioni mettono in sicurezza le connessioni wireless. Le organizzazioni non dovrebbero tuttavia dimenticare l'importanza delle connessioni via cavo.

Le porte via cavo non protette in luoghi pubblici sono molto spesso il tallone d'Achille di una strategia di protezione del network che altrimenti sarebbe solida. I problemi si verificano quando un visitatore si muove in uno spazio pubblico, scollega una stampante o un telefono IP in un'aula conferenze, collega un laptop per un istante ed effettua un accesso.

TENERE SEMPRE PRONTA UNA STRATEGIA DI REMEDIATION CHE FUNZIONI IN TUTTI GLI SCENARI

Effettuare un ottimo controllo degli accessi è sicuramente un aspetto importante, ma un'organizzazione deve disporre di un piano o di un workflow per la risoluzione dei problemi in caso si presentino. Uno dei più gravi errori che le organizzazioni commettono consiste nell'introdurre tecnologia per il controllo delle connessioni al network dei dispositivi omettendo di configurare un messaggio automatico per gli utenti che spiega il perché è stata limitata la connessione per i loro dispositivi. Una svista di questo tipo sommerge i collaboratori dell'help desk di ticket relativi a problemi, fa perdere tempo agli utenti e irrita i direttori.

Mentre si muniscono di sistemi di controllo degli accessi, le organizzazioni necessitano di un programma e di una procedura per ottimizzare il workflow dopo che un dispositivo è stato bloccato. Ciò si traduce, se è possibile, in un sistema automatico di attivazione della remediation. Significa informare gli utenti del problema che ha causato la restrizione. Significa impegnare l'help desk e il supporto IT. Significa inoltre fornire la documentazione o le altre risorse necessarie per guidare gli utenti attraverso la procedura di remediation nel modo più fluido possibile.

CHE TIPO DI AIUTO OFFRE ARUBA CLEARPASS?

ClearPass offre la visibilità, il controllo della policy, l'automazione del workflow e l'integrazione con altri prodotti di sicurezza necessari per mettere in atto questi cinque passaggi. Sono incluse le seguenti caratteristiche:

- Profiling integrato che raccoglie dati in tempo reale come le categorie di dispositivo, i vendor e le versioni del sistema operativo.
- Processi di autenticazione che permettano l'uso da parte degli utenti e contesto del dispositivo per l'applicazione di regole.
- Condivisione del contesto che funziona con sistemi di terze parti. Sistemi di questo tipo includono firewall, gestione endpoint, analisi del comportamento degli utenti e delle entità, gestione dei dispositivi e dei servizi IT che offrono dati accurati sugli utenti e i dispositivi per migliorare i workflow di remediation.

Queste potenzialità offrono alle organizzazioni il potere di imporre a utenti e dispositivi le modalità d'uso delle risorse interne, a prescindere dal ruolo dell'utente, dal tipo di dispositivo o dalla località dalla quale viene stabilita la connessione.

CONCLUSIONE: METTERE TUTTO ASSIEME

Anche se le organizzazioni si sforzano di compiere tutti questi passi verso la riduzione dei rischi legati alla mobilità, non esiste una singola «bacchetta magica» tecnologica. Le organizzazioni necessitano di un ecosistema di controlli ben bilanciato che affronti tutte le dimensioni del rischio. Devono considerare il fatto che avranno bisogno di abbinare controlli degli accessi granulari al network e visibilità delle connessioni con piattaforme di orchestrazione IT per la remediation.

Per fare ciò, le organizzazioni devono dispiegare soluzioni tenendo presente innanzitutto l'integrazione, garantendo che i vendor che selezionano funzionino bene assieme per un sostegno alla sicurezza senza soluzioni di continuità.