

POTENZIAMENTO DELLA SICUREZZA DI ACCESSO ALLA RETE CON L'AUTENTICAZIONE MULTIFATTORE



ROBERT BERLIN

Robert Berlin è Sr. Director of Product Marketing presso la Enterprise Access Division di Akamai Technologies, dove si occupa della creazione dei contenuti, dei programmi e delle strategie di marketing. In precedenza è stato a capo della divisione Product and Partner Marketing di Soha Systems (Akamai ha acquisito Soha nell'ottobre 2016). Rinomato esperto nell'ambito della creazione e delle strategie relative ai contenuti, ha diretto le divisioni marketing sia di start-up che di grandi aziende. Fornisce periodicamente anche consulenza a clienti privati in relazione a strategie, contenuti, pubbliche relazioni e servizi di generazione della domanda. Vanta un'esperienza di oltre 25 anni in ambito marketing, product marketing, product management e business development nei settori computing, cloud e networking con aziende quali Cisco, VCE, Fortinet e Onelogin. Ha conseguito un MBA presso la Pepperdine University.

Con una tecnologia in costante sviluppo, sono sempre di più le applicazioni che da utili diventano fondamentali. Meno di dieci anni fa era impensabile ipotizzare "l'esigenza" di portare sempre con sé un dispositivo consumer per accedere a Internet. Oggi è invece una vera e propria necessità. Lo stesso vale per le applicazioni utilizzate negli affari, nelle attività commerciali e amministrative, che devono essere accessibili e a portata di mano 24 ore al giorno, 7 giorni su 7.

Questo livello di disponibilità comporta però inevitabilmente problemi correlati all'accesso sicuro alle applicazioni, che deve avvenire senza compromettere la sicurezza di importanti dati aziendali.

Quali sono i fattori di rischio? Con un numero così elevato di utenti (1) mobile, (2) che utilizzano dispositivi mobili appartenenti o non appartenenti all'IT aziendale e (3) che usano una vasta gamma di applicazioni ospitate in varie posizioni sul cloud o in ufficio, è di fondamentale importanza accertarsi che solamente gli utenti autenticati possano accedere a tali applicazioni. In questo quadro complesso, affidarsi semplicemente a un nome utente e a una password non basta più.

L'autenticazione multifattore, basata su un elemento che l'utente possiede, su un elemento che lo rappresenta e persino su fattori ambientali (ora del giorno, geolocalizzazione e così via), sta rapidamente diventando lo standard necessario a garantire un ulteriore livello di autenticazione e sicurezza. La sfida generale dal punto di vista dell'implementazione IT consiste nel fatto che l'integrazione dell'autenticazione multifattore richiede attività di sviluppo, test e manutenzione costante per:

- Configurazioni aggiuntive (integrazione utente/dispositivo, delivery, formazione)

- Attività di sviluppo e integrazione API per ogni applicazione
- In alcuni casi, supporto per hardware aggiuntivo come i token per l'autenticazione

Questo provoca rallentamenti nella produttività e un aumento dei costi.

L'ottima notizia è che grazie ad Akamai Enterprise Application Access (EAA), l'autenticazione multifattore può essere applicata con un solo clic a utenti, applicazioni e gruppi di applicazioni. Akamai ha semplificato la modalità di attivazione, che non richiede più mesi di sviluppo e test.

L'experience dell'utente finale è ottimale. Se l'autenticazione multifattore è abilitata, quando un utente accede al portale EAA, gli verrà richiesto di inserire il nome utente e la password (primo fattore - l'elemento noto) oltre a un codice di autenticazione generato dal dispositivo per l'autenticazione multifattore, che solitamente è il telefono cellulare (secondo fattore - elemento che l'utente possiede). La combinazione di questi fattori multipli garantisce una maggiore sicurezza di accesso alle applicazioni.

EAA e il set di funzionalità per l'autenticazione multifattore integrato rappresentano la soluzione ideale per le aziende che mirano a superare gli ostacoli posti dall'accesso alle applicazioni dietro il firewall in un'epoca caratterizzata dal cloud e dalla mobilità. E per quanto riguarda l'accesso sicuro alle applicazioni SaaS? Ne parlerò nel prossimo post del blog. Per ulteriori informazioni su EAA e sull'autenticazione multifattore, consultate le nostre [pagine dedicate ai prodotti su www.akamai.com/it/it/](http://www.akamai.com/it/it/).



In qualità di piattaforma di delivery cloud più ampia e attendibile a livello mondiale, Akamai aiuta i propri clienti a fornire le experience digitali migliori e più sicure in qualsiasi dispositivo, luogo e momento. Con oltre 200.000 server distribuiti in 130 paesi, la piattaforma ampiamente distribuita di Akamai non teme confronti in termini di dimensioni, garantendo ai clienti protezione dalle minacce e performance di massimo livello. Il portafoglio Akamai di soluzioni per le web e mobile performance, la sicurezza sul cloud, l'accesso aziendale e la delivery di contenuti video è supportato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7. Per scoprire perché i principali istituti finanziari, leader e-commerce, provider del settore Media & Entertainment ed enti governativi si affidano ad Akamai, visitate il sito <https://www.akamai.com/it/it/> o blogs.akamai.com/it/ e seguite [@Akamaitalia](https://twitter.com/Akamaitalia) su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/it/it/locations. Data di pubblicazione: 05/2017.