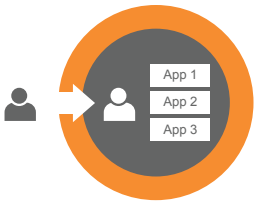
RISTAMPA DAL BLOG

PERCHÉ FOSSATI E CASTELLI APPARTENGONO AL PASSATO

LORENZ JAKOBER

Lorenz Jakober, Director of Product Marketing, Akamai Technologies. Responsabile del Product Marketing per la linea di prodotti Cloud Networking di Akamai, Jakober vanta un'ampia esperienza incentrata sulle architetture di cloud networking, sul design delle applicazioni mobili e web, sull'ottimizzazione delle performance, nonché sull'usabilità e la delivery dei contenuti.

L'impiego di fossati come misura di difesa perimetrale ha avuto inizio nell'Antico Egitto. Al giorno d'oggi conosciamo tutti l'approccio alla sicurezza aziendale che vede l'organizzazione come un castello da difendere attraverso la costruzione di mura sempre più alte e fossati sempre più profondi. Nonostante questo approccio abbia funzionato bene in passato, inizia a mostrare i segni del tempo.



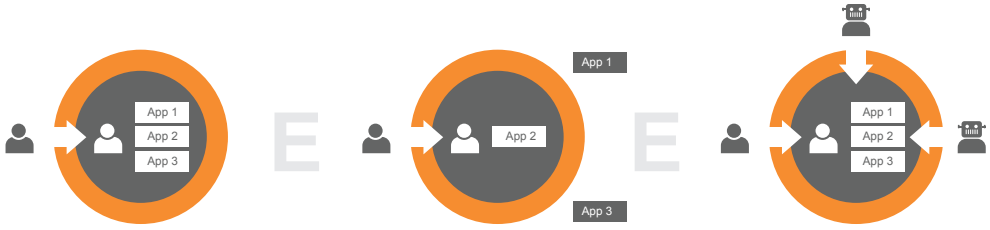
FOSSATI E CASTELLI

L'approccio alla sicurezza aziendale basato sulla costruzione di mura e fossati non è solo antiquato, ma sta anche perdendo efficacia in un mondo come quello odierno sempre più mobile e basato sul cloud. L'evoluzione delle aziende, delle applicazioni e del panorama delle minacce ne è la conferma.

Le aziende si stanno evolvendo e trasformando radicalmente. I dipendenti vogliono poter accedere alle applicazioni aziendali in qualunque istante e da qualsiasi dispositivo. Per di più, l'ecosistema aziendale è diventato un fattore essenziale per il successo di questa trasformazione digitale. Per tutti i componenti dell'ecosistema di partner, collaboratori e fornitori il requisito è analogo a quello dei dipendenti: accesso sicuro alle applicazioni aziendali sempre e da qualsiasi dispositivo. Come sottolinea il Senior Director of Enterprise Security & Infrastructure Engineering di Akamai: "Non c'è più un dentro e un fuori".

Anche le app aziendali si stanno evolvendo. Quando gli utenti finali inviano un rapporto di spesa o un rapporto su un bug si aspettano la stessa experience di quando aggiornano il proprio profilo sui social media o controllano l'estratto conto sul cellulare. Per questa ragione, molti team IT si trovano oggi in affanno. In molti casi, interi segmenti aziendali scelgono di aggirare completamente l'IT optando invece per il cloud e le soluzioni SaaS. Offrire la possibilità di lavorare ovunque, da qualsiasi dispositivo, in modo veloce ed efficiente è chiaramente un vantaggio per la redditività aziendale, e di conseguenza deve diventare una priorità. Questo presuppone spesso una qualche riorganizzazione, che per la maggior parte di noi fa rima con cloud, in particolare con Internet, IaaS o SaaS.

In più, anche il panorama delle minacce è in continua evoluzione. L'approccio alla sicurezza aziendale che mira a costruire mura sempre più alte e fossati sempre più profondi si basa su due semplici presupposti. Primo, mura e fossati funzionano. Secondo, una volta all'interno delle mura del castello un intruso può fare praticamente ciò che vuole. Certo, si possono sempre chiudere a chiave determinate stanze, ma per lo più l'intruso potrà muoversi liberamente, imparare a conoscere la pianta del castello, scoprire dove si trovano le stanze chiuse a chiave e se eventualmente dispongono di una finestra aperta o di una seconda porta, magari meno protetta. Tutto questo vi suona in qualche modo familiare? Senz'altro sarà così, perché si tratta del piano che viene messo in atto nella maggior parte dei moderni attacchi informatici. Riuscire a entrare, fare una ricognizione, identificare i punti deboli, impossessarsi di ciò che si sta cercando e fuggire, il tutto senza che nessuno se ne renda conto fino a quando è ormai troppo tardi.

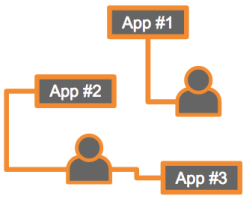


EVOLUZIONE DELL'AZIENDA | EVOLUZIONE DELLE APP AZIENDALI | EVOLUZIONE DEL PANORAMA DELLE MINACCE

Combinate insieme l'evoluzione delle aziende, delle applicazioni e del panorama delle minacce e capirete perché ci stiamo sempre più rendendo conto che castelli e fossati appartengono al passato.

Che si tratti del programma BeyondCorp di Google o del modello Zero Trust di Forrester, lo scopo è lo stesso: trattare tutti gli utenti finali allo stesso modo, che si trovino all'interno o all'esterno delle mura del castello/azienda.

Noi di Akamai abbiamo adottato un approccio nuovo e migliore, il perimetro cloud. Il perimetro cloud si riduce all'utente e all'applicazione a cui tenta di accedere. Gestisce l'autenticazione, l'autorizzazione e la delivery delle applicazioni su diversi dispositivi e posizioni e non rivela dove è ospitata l'applicazione, indirizzando automaticamente l'utente alla posizione giusta, ma solo se dispone dei privilegi appropriati. La potenziale superficie di attacco viene così spostata sulla piattaforma Akamai, che fornisce accesso a specifiche applicazioni solo a utenti finali attendibili e autenticati e ai rispettivi dispositivi. Niente più accesso alla rete. Niente più fossati e castelli. Tutti sono considerati potenzialmente non attendibili, sia dentro che fuori.

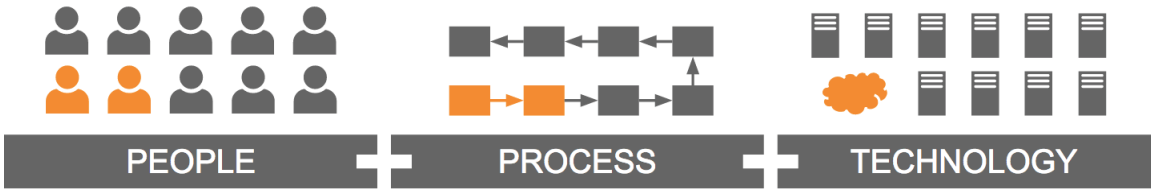


CLOUD PERIMETER

Questo approccio semplifica non poco la vita ai team IT e che si occupano della sicurezza aziendale, i quali continuano a essere responsabili della visibilità, della sicurezza e delle performance anche se dati, app e dipendenti aziendali sono stati spostati al di fuori della zona che tradizionalmente rientrava sotto il controllo dell'azienda. In questo modo i team possono dedicarsi a migliorare l'agilità dell'IT e a semplificare l'infrastruttura. Solo il traffico aziendale non dannoso può attraversare il perimetro cloud in entrata e in uscita, tutto il resto viene bloccato.

Quali sono le implicazioni per chi sceglie di passare a un approccio basato sul perimetro cloud? Tanto per cominciare, non potrà usufruire e beneficiare dei vantaggi dell'evoluzione dell'azienda e delle applicazioni aziendali. Chi non va avanti, va indietro. Un fattore probabilmente ancora più importante è l'inquietudine per i professionisti del settore IT e sicurezza associata al maggior rischio derivante dall'accesso completo a livello di rete fornito senza autenticazione multifattore o integrazione SSO (Single Sign-On). Un altro modo di guardare alle implicazioni per chi sceglie di non adottare un approccio basato sul perimetro cloud è l'osservazione dalla prospettiva delle persone, dei processi e della tecnologia.

In che modo l'adozione di un perimetro cloud influisce su questi ambiti? In termini di persone è una questione di competenze, ore di lavoro e produttività. In termini di processi, è una questione di semplificazione. In termini di tecnologia, è molto semplice.



Anziché dover realizzare una propria infrastruttura integrando tra loro svariate soluzioni di accesso e ottimizzazione, Akamai è in grado di semplificare il tutto fornendo un perimetro cloud sotto forma di servizio. Enterprise Application Access (EAA), la nostra prima soluzione di perimetro cloud, offre un accesso semplice e sicuro alle applicazioni aziendali che si trovano dietro al firewall. Scoprite di più su EAA.

È tempo di lasciare al passato castelli e fossati.

Akamai FASTER FORWARD