Tutto ciò che avreste sempre voluto sapere sulla sicurezza sull'edge, ma non avete mai osato chiedere.

Introduzione

Che vi occupiate di siti web per interazioni pubbliche, utenti o risorse aziendali, per quanto riguarda la protezione digitale non potrete sfuggire a queste tendenze, che caratterizzeranno lo stato della sicurezza nel 2019:

Gli attacchi stanno crescendo, evolvendosi e diventando sempre più sofisticati; inoltre, assistiamo al proliferare di vari tipi di attacchi.

Le aziende dipendono da impeccabili experience digitali: ciò vale per le imprese che desiderano comunicare, collaborare e produrre ai massimi livelli, ma anche per prodotti aziendali chiave, come fluide transazioni online, sia di tipo commerciale che finanziario, delivery di contenuti video OTT, portali per l'assistenza sanitaria online e dispositivi connessi negli impianti di produzione.

Una volta, esisteva il concetto di un perimetro di sicurezza immutabile. Si poteva erigere un muro intorno e proteggere tutto ciò che si trovava all'interno del data center. Niente entrava e niente usciva. Il problema ora è: il perimetro, nel senso tradizionale del termine, si sta dissolvendo. E come possiamo proteggere i "gioielli della corona" se il castello non ha mura?

La risposta è: con l'edge.

Quando implementate un sistema di sicurezza dell'edge, da un lato proteggete le vostre mutevoli risorse agendo più in prossimità dell'attacco stesso e, dall'altro, avvicinate le experience digitali agli utenti. In sostanza, state implementando un'unica protezione, un'estensione della vostra infrastruttura, che risiede tra voi (i vostri utenti e le vostre experience digitali) e la sempre mutevole natura dell'odierno ambiente digitale.

Cosa intendiamo dire con il termine "edge".

Bob Gill di Gartner scrive che l'*edge* è semplicemente come "la posizione fisica in cui cose e persone si collegano con il mondo digitale connesso in rete."*

In un certo senso, è una questione di topologia fisica. In un momento in cui gli utenti si aspettano impeccabili experience digitali on demand, l'edge a cui vengono indirizzate le interazioni, più vicino alla fonte dei dati generati, non solo fornisce migliori experience, ma rappresenta anche la migliore posizione per costruire sistemi di protezione tra la vostra azienda e i vostri utenti e consumatori di experience digitali ampiamente distribuiti.

Lo spostamento di interesse verso l'edge è stato favorito da diversi fattori:

- **Crescente intolleranza dei consumatori nei confronti della latenza.**
- **Crescente consumo di contenuti multimediali ad utilizzo intensivo di larghezza di banda.**
- **Enorme quantità di contenuti trasmessi e utilizzati.**
- **Aver compreso che i data center non sono l'ideale per la delivery o la protezione del tipo di contenuti coinvolgenti che tutti noi ci aspettiamo dalle nostre experience digitali.**

Benché alcuni data center siano diventati più grandi e centralizzati che mai prima d'ora, guardando al futuro, si prevede che la topologia si sposterà verso data center più piccoli e distribuiti sull'edge. Molti analisti ritengono che, spostandosi verso l'edge, le aziende potranno creare mercati totalmente nuovi sulla base dei vantaggi da esso offerti.

Si tratta di un'opportunità per i team addetti ai servizi di informazione e della sicurezza di utilizzare una piattaforma di protezione semplice e agile per passare da un mero centro di costo a un partner strategico in grado di promuovere le attività aziendali e favorire i ricavi.

* Gartner, Come l'Edge Computing ridefinisce l'infrastruttura, Thomas Bittman, Bob Gill et al., 23 agosto 2018.

Cosa intendiamo dire con l'espressione "sicurezza dell'edge".

Con i processi che si verificano sempre più vicino al punto in cui vengono generati i dati, l'architettura dell'edge può fornire un miglior livello di experience, efficienza e sicurezza, consentendo, in definitiva, alle aziende di risparmiare denaro e concentrare le risorse su ulteriori opportunità di guadagno.

Insieme ai vantaggi apportati dall'edge, giunge anche l'opportunità di guardare alla sicurezza in modo totalmente nuovo. Il perimetro della rete, nel senso tradizionale del termine, si sta dissolvendo, pertanto è necessario adattare le modalità di approccio necessarie per proteggerlo.

Ecco che qui entra in gioco la sicurezza dell'edge.

La sicurezza dell'edge rappresenta un approccio alla protezione dalle minacce che attentano alle attività aziendali vostre e dei vostri clienti (tutti i vostri utenti) mediante l'implementazione di misure di difesa più vicine al punto di attacco e il più lontane possibile dalle vostre risorse (personale, applicazioni o infrastrutture). La sicurezza offerta dall'edge è dinamica e adattiva poiché vi consente di circondare e proteggere i vostri utenti o consumatori ovunque si trovino, nel nucleo, nel cloud o sull'edge e in tutte le posizioni intermedie.

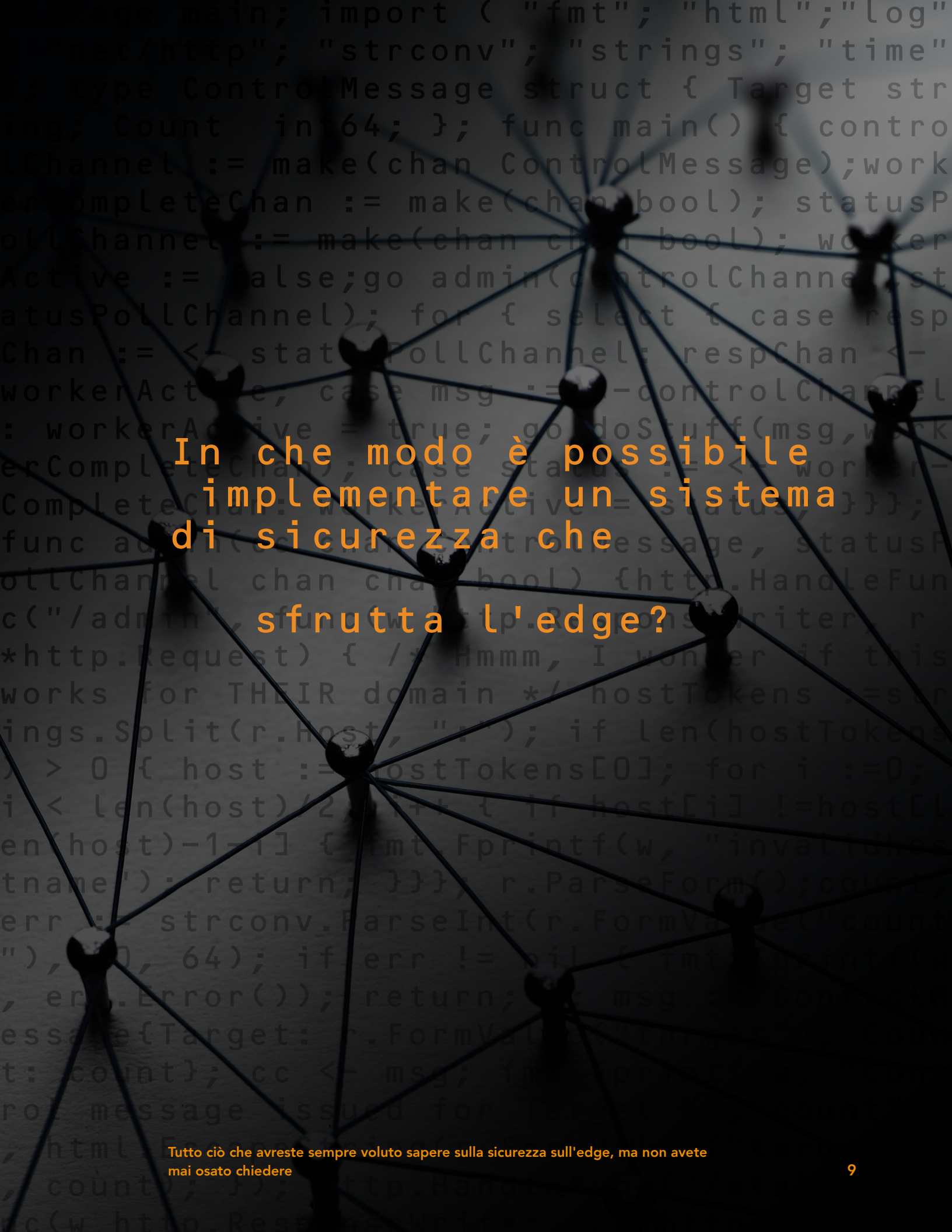

Ciò che ora state
proteggendo
è diverso da
ciò che eravate soliti
proteggere un tempo.

Sia che dobbiate adattarvi alla natura mutevole del perimetro o impegnarvi al fine di proteggere le mutevoli applicazioni per interazioni pubbliche, è chiaro che ciò che ora state proteggendo è sostanzialmente cambiato e continuerà a farlo. La superficie soggetta agli attacchi non è più la stessa. Ad esempio:

- **Le applicazioni si stanno costantemente aggiornando** con nuove versioni, nuove funzionalità e nuovi microservizi.
- **Le applicazioni si stanno continuamente spostando** dalle sedi fisiche al cloud e viceversa.
- **I siti web si stanno trasformando,** passando da infrastrutture di tipo tradizionale a sistemi di back-end basati sulle API e orientati ai dispositivi mobili.
- **I data center si stanno sempre più espandendo o consolidando.**
- **Le infrastrutture sono regolarmente interessate da operazioni di aggiunta o rimozione.**
- **I dipendenti sono sempre più in movimento.** Il modello di orario 9 - 17 è sempre più raro, così come il luogo di lavoro inteso come una sede fisica e centralizzata.

In un ambiente di questo tipo, dovete proteggere una combinazione di applicazioni: in sede, nel cloud o in più cloud. Nello stesso tempo, i team all'interno della vostra organizzazione sono costituiti da diversi gruppi di persone con varie priorità che prendono decisioni indipendenti tra loro, tutte probabilmente inerenti alla strategia aziendale; tuttavia, la natura imprevedibile del processo presenta sfide di ingenti proporzioni.

La risposta risiede in una procedura di sicurezza indipendente dal cloud, in grado di rispondere alle esigenze aziendali quando si cambia direzione o si utilizzano più soluzioni cloud contemporaneamente. La vostra soluzione risiede nell'edge.



In che modo è possibile implementare un sistema di sicurezza che sfrutta l'edge?

La vostra missione consiste nel proteggere le applicazioni ovunque si trovino. L'implementazione di un'unica soluzione per la sicurezza a livello di edge riduce al minimo il tempo e le risorse impiegate nella formazione su tale soluzione. Inoltre, con un'unica soluzione (una singola protezione), potete proteggere le applicazioni ovunque su una qualsiasi piattaforma.

L'esatta combinazione di soluzioni per la sicurezza appropriate per ciascuna organizzazione può variare, ma le seguenti misure sono componenti di fondamentale importanza nell'ambito di un'efficace strategia per la sicurezza dell'edge:

Protezione contro gli attacchi DDoS

Non è insolito per le organizzazioni subire centinaia, se non migliaia, di attacchi DDoS ogni mese. Tuttavia, risulta fondamentale mantenere le applicazioni e i servizi IT disponibili anche durante il più vasto di questi attacchi.

Web Application Firewall

I siti e le applicazioni web stanno aumentando il loro livello di complessità e di rischio, con nuove vulnerabilità che vengono rilevate ogni giorno. Un firewall di livello superiore è in grado di offrire il giusto livello di protezione e performance.

Gestione dei bot

I bot possono rappresentare il 30 - 70% del traffico del sito web di un'organizzazione, influenzandolo con un impatto che varia da performance scadenti alla perdita di clienti fino alle frodi. Per le organizzazioni è d'obbligo implementare una strategia dei bot efficace e adattiva per tenere sotto controllo gli scraper e per mitigare gli attacchi di credential stuffing.

Accesso sicuro alle applicazioni aziendali

I modelli aziendali sono cambiati: gli ecosistemi digitali delle aziende, le applicazioni cloud e gli utenti distribuiti implicano un notevole livello di flessibilità da parte dell'IT, mentre i vostri utenti richiedono un tipo di accesso sicuro, ma agevole. La gestione dell'accesso remoto deve risultare estremamente semplice e sicura per l'IT, garantire una protezione intrinsecamente migliore e offrire un'eccellente user experience.

DNS

Proteggete il vostro servizio DNS autoritativo e restate connessi con i vostri utenti e dipendenti. Progettata per garantire performance e disponibilità, la nostra soluzione mantiene un'experience DNS rapida e disponibile anche durante i più vasti attacchi DDoS, proteggendo anche da tentativi di contraffazione e manipolazione del DNS.

Prevenzione dei malware

Per assicurarvi che i vostri utenti e i loro dispositivi siano connessi in modo sicuro a Internet ovunque e in qualsiasi momento, dovete identificare e bloccare in modo proattivo minacce mirate come malware, ransomware, phishing, esfiltrazione dei dati DNS e attacchi zero-day.

Mantenere la fiducia con la sicurezza dell'edge.

Tutto ciò che avreste sempre voluto sapere sulla sicurezza sull'edge, ma non avete mai osato chiedere

I consumatori di experience digitali si aspettano che i propri dati e le proprie transazioni siano al sicuro e che la loro privacy venga rispettata. Le aziende, dal canto loro, devono proteggere la propria forza lavoro dai tentativi di attacco. Proteggere le vostre risorse e i vostri dipendenti da attacchi provenienti dall'esterno (e dall'interno) è un nodo fondamentale per promuovere la fiducia come valore del brand.

E la fiducia non va sottovalutata: in base ad una ricerca condotta da Frost & Sullivan, l'86% dei clienti intervistati ha affermato di preferire la sicurezza alla convenienza, dichiarandosi propensi a spendere di più se si fidano maggiormente di un'azienda. In realtà, come segnala Forrester, anche un mero sentore di sospetto riguardo pratiche di utilizzo dei dati da parte di un'azienda può ridurre i ricavi fino al 25%.

Il panorama della sicurezza si sta modificando. Oggi, gli addetti alla sicurezza si trovano ad affrontare autori di attacchi persistenti, bot sofisticati e avanzati software C&C (Command and Control), insieme ad un perimetro aziendale sempre più difficile da circoscrivere. Per mantenere la fiducia degli utenti, le organizzazioni necessitano di un sistema di sicurezza dell'edge in grado di circondare e proteggere l'intera architettura (cloud, siti, contenuti, app e utenti).

Conclusione

Le leggi della fisica (la velocità della luce, la gravità dei dati e le limitazioni della larghezza di banda) richiedono un cambiamento nel concetto di sicurezza. La richiesta di interazioni più immediate tra cose, persone e le relative experience digitali ci sta indirizzando tutti verso l'edge, il che è un bene. Tutto ciò sta già espandendo le opportunità commerciali e sta cambiando fondamentalmente il nostro modo di vivere, interagire, effettuare acquisti e lavorare.

Tuttavia, parallelamente a questa evoluzione, le superfici soggette agli attacchi continueranno a cambiare diventando altamente distribuite. Gli attacchi continueranno a crescere mirando ad obiettivi sempre più precisi. La fiducia basata su un solo punto della rete non sarà più rilevante. Queste tendenze e i sistemi sempre più complessi inerenti alle attività digitali, in definitiva, non faranno che aumentare i rischi, ma forniranno anche ai team addetti alla sicurezza una notevole opportunità: quella di diventare partner aziendali aumentando il valore per la propria organizzazione.

Tutto ciò si può ottenere adottando una strategia di sicurezza dell'edge adattiva, approfondita e concepita per contrastare l'espansione della superficie soggetta agli attacchi e per semplificare i controlli di sicurezza. Una strategia in grado di avvicinare gli utenti alle experience digitali e sventare gli attacchi da esse generati. Una strategia in grado di generare fiducia e porre la tranquillità e il controllo nelle vostre mani.

Grazie alla propria piattaforma di cloud delivery più estesa e affidabile al mondo, Akamai supporta i clienti nell'offerta di experience digitali migliori e più sicure da qualsiasi dispositivo, luogo e momento. La piattaforma ampiamente distribuita di Akamai garantisce protezione dalle minacce informatiche e performance di altissimo livello. Il portfolio Akamai di soluzioni per le web e mobile performance, la sicurezza sul cloud, l'accesso remoto alle applicazioni aziendali e la delivery di contenuti video è affiancato da un servizio clienti affidabile e da un monitoraggio 24x7. Per scoprire perché i principali istituti finanziari, i maggiori operatori e-commerce, provider del settore Media & Entertainment ed enti governativi si affidano ad Akamai, visitate il sito https://www.akamai.com/it/it/ o https://blogs.akamai.com/it/ e seguite @Akamailtalia su Twitter. Data di pubblicazione: 05/19.