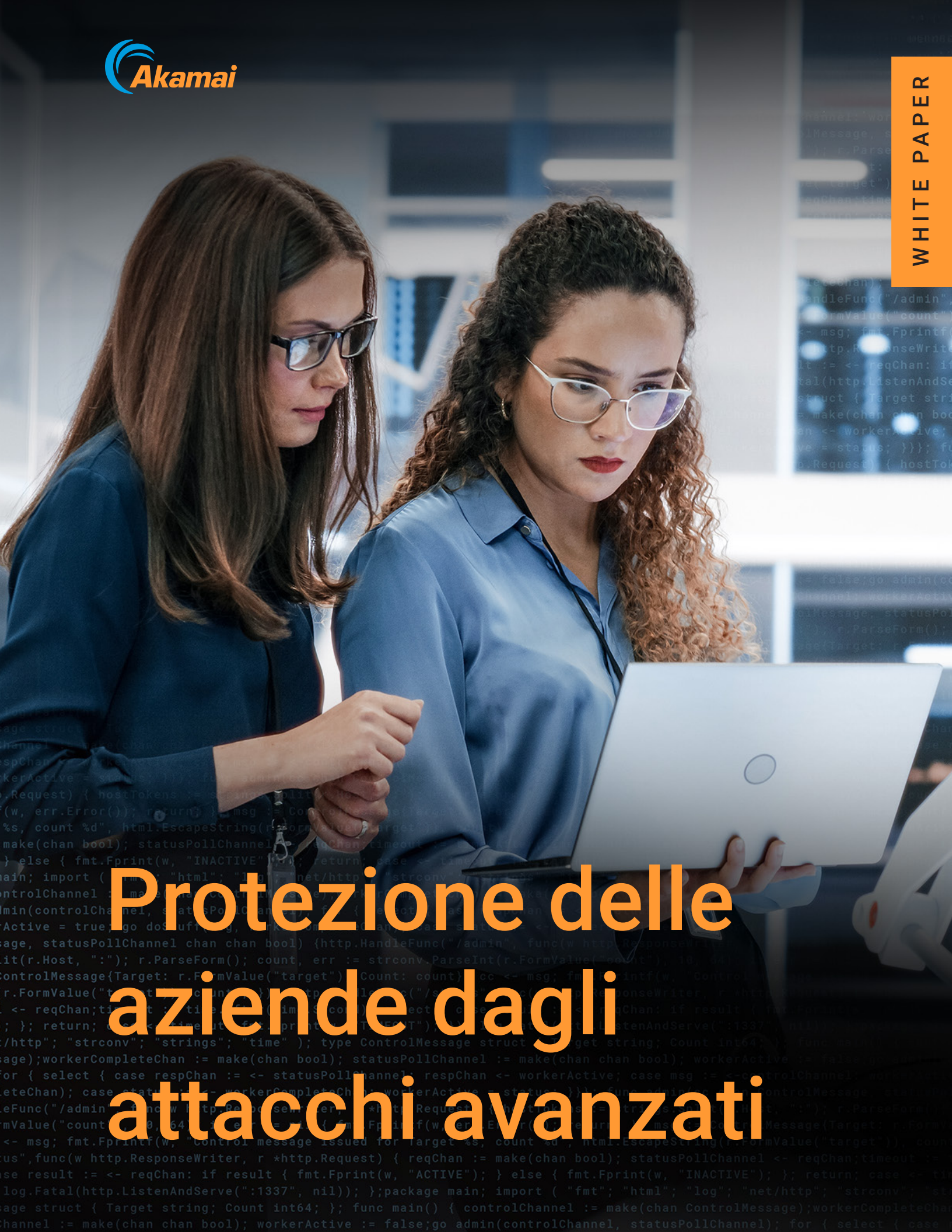
Akamai

WHITE PAPER



Protezione delle aziende dagli attacchi avanzati

Man mano che gli ambienti IT sono diventati più complessi, gli attacchi informatici si sono evoluti per sfruttare nuovi punti deboli. Applicazioni, API, microservizi e componenti sono in continua espansione e cambiano il modo di condurre le attività aziendali online, ma, sfortunatamente, creano anche nuove vulnerabilità e superfici di attacco che i criminali possono sfruttare. Le soluzioni di cybersicurezza devono affrontare sia le minacce esistenti all'interno (protezione dei dati) che all'esterno (blocco di attacchi ransomware, DDoS, esaurimento delle risorse e altri tipi di attacchi).

Lo sappiamo per esperienza diretta, perché i ricercatori di Akamai analizzano, in media, 788 TB di dati al giorno. Con l'ausilio delle conoscenze acquisite, possiamo innovare continuamente i nostri prodotti, proteggendo la vostra azienda e i vostri utenti dai criminali più pericolosi e da avanzate campagne, anche durante l'evoluzione degli attacchi.

Quali sono gli attacchi più pericolosi che la vostra azienda potrebbe affrontare e come potete preparavi per affrontarli?

Il ransomware è in aumento

La perdita di accesso ai vostri dati e a quelli dei vostri clienti è una delle minacce più pericolose per la vostra azienda. Tra il primo trimestre del 2022 e lo stesso periodo del 2023, il numero di attacchi ransomware è aumentato del 143% in tutto il mondo, con i criminali che hanno sfruttato le vulnerabilità zero-day e one-day, secondo il rapporto di Akamai dal titolo Il ransomware in azione. Potete ridurre la probabilità e l'impatto degli attacchi avanzati mediante la segmentazione.

Mentre la segmentazione è un approccio architetturale che divide una rete in segmenti più piccoli per migliorare le performance e la sicurezza, la microsegmentazione è una tecnica di sicurezza che vi consente di dividere in modo logico una rete in segmenti separati fino al livello dei singoli carichi di lavoro. È possibile quindi definire i controlli di sicurezza e la delivery di servizi per ogni singolo segmento.

Akamai Guardicore Segmentation, parte della piattaforma Akamai Guardicore per la sicurezza Zero Trust, agisce per contenere gli attacchi sferrati contro tutti i vostri sistemi critici, impedendo loro di diffondersi tra le vostre risorse (il cosiddetto movimento est-ovest), potenziando quindi la risposta e il ripristino dagli attacchi. Ne risulta una protezione contro i danni alla reputazione, la perdita di dati e le mancate entrate causate da una violazione.

Poiché si tratta di una soluzione senza agente per la microsegmentazione, la piattaforma Akamai Guardicore può essere implementata in modo rapido e semplice, senza dover apportare modifiche fisiche alla rete o preoccuparsi della posizione di server e dispositivi. La piattaforma genera una visualizzazione interattiva di tutte le connessioni presenti nella rete, aiutandovi a superare uno dei principali ostacoli all'implementazione: la mancanza di visibilità. Akamai, inoltre, ha trovato il modo per affrontare attivamente potenziali colli di bottiglia nelle performance e requisiti di conformità, oltre all'applicazione di policy in grado di coprire diversi tipi di infrastrutture, offrendo un'ampia visibilità e un controllo granulare in ogni ambiente, il tutto su un'unica piattaforma.

Akamai offre una visibilità impareggiabile sul traffico online tramite una rete globale ampiamente distribuita. La piattaforma Akamai Guardicore sfrutta queste componenti per fornire una visibilità approfondita sull'ambiente, sulle risorse, sugli accessi e sui flussi di rete della vostra azienda, offrendovi informazioni in tempo reale con cui potrete sapere con certezza che le vostre attività aziendali non subiranno interruzioni.

App e API sotto attacco

Quante applicazioni utilizza la vostra azienda? Quasi certamente più di quante ne siate a conoscenza. Un'azienda media utilizza più di 1.000 app. La forte dipendenza dalle API per quasi tutte le transazioni online e la crescente adozione di architetture basate su microservizi significa anche che le app stanno diventando più complesse. Sfortunatamente, il pressante desiderio di crescita supportato dall'innovazione tecnologica porta spesso le aziende a rilasciare le app prima di averle rigorosamente testate per verificare potenziali problemi di sicurezza, il che introduce maggiori rischi per l'intero ecosistema delle applicazioni.

Il recente rapporto sullo stato di Internet di Akamai ha rilevato che il 29% degli attacchi in tutto il mondo ha preso di mira le API (Application Programming Interface), ossia il componente fondamentale della maggior parte delle trasformazioni digitali. Nell'EMEA (Europa, Medio Oriente e Africa), questa percentuale è risultata poco più del 47%. Le API sono un vettore di attacco comune per i criminali informatici che utilizzano tecniche sia tradizionali che specifiche delle API. Inoltre, è necessario tenere conto anche dei bot, degli attacchi DDoS (Distributed Denial-of-Service) e degli attacchi multivettore.

Proteggere le applicazioni web con Akamai App & API Protector consente di salvaguardare i workflow, gli utenti e la vostra azienda da attività dannose e frodi, fornendo protezioni firewall configurabili in grado di assorbire gli attacchi mirati a livello di applicazioni, compresi quelli sferrati tramite le API. Con una visibilità in tempo reale sul traffico dei bot, potete esaminare i dati analitici alterati, prevenire il sovraccarico dell'origine e personalizzare le autorizzazioni per consentire l'accesso a bot di terze parti e partner senza problemi.

Ma, tornando alla domanda originale, cosa succede se non si conoscono tutte le app e le API di cui si dispone? La visibilità è, ancora una volta, la chiave: Akamai API Security identifica tutte le API, ne valuta i livelli di rischio e risponde agli attacchi, impedendo ai criminali di accedere ai dati, caricare file dannosi sui server o sovraccaricare i server con picchi di traffico.

La difesa dai DDoS e dagli attacchi di esaurimento delle risorse

Gli attacchi DDoS (Distributed Denial-of-Service) sono una delle minacce online più imponenti e comuni. Sono presenti da quando esiste Internet e il loro impatto è cresciuto insieme a tutti gli altri contenuti online. Negli ultimi anni, gli attacchi DDoS sono cresciuti in termini di dimensioni, durata e sofisticatezza con molteplici vettori e destinazioni di attacco. Tra il 2021 e il 2023, il numero di attacchi DDoS altamente volumetrici è raddoppiato, mentre oltre il 60% di tutti gli attacchi DDoS registrati nel 2023 ha avuto un componente DNS.

Anche le aziende più grandi possono essere colpite da queste botnet ostili, interrompendo i servizi per milioni di clienti e bloccando drasticamente le loro attività. I criminali informatici con tante risorse, gli hacker sostenuti dai governi e gli hacktivisti che agiscono con motivazioni geopolitiche sfruttano botnet grandi e distribuite per detronizzare non solo le aziende più grandi, ma anche importanti istituzioni pubbliche, dalle scuole agli ospedali fino agli aeroporti e ai provider di servizi pubblici. I devastanti attacchi DDoS e di esaurimento delle risorse vengono sferrati contro tutti i livelli, le porte, i protocolli e persino il DNS di aziende e istituzioni.

Lo sapevate?

Il numero di attacchi DDoS è raddoppiato tra il 2021 e il 2023

Oltre il 60% di tutti gli attacchi DDoS registrati nel 2023 ha avuto un componente DNS

Per proteggere la vostra infrastruttura dagli attacchi DDoS, è richiesta un'intelligence sulle minacce in tempo reale. I dati da noi raccolti vengono utilizzati per potenziare Prolexic, la nostra soluzione di protezione e mitigazione degli attacchi DDoS. In grado di proteggere l'infrastruttura digitale su cui sono basate le applicazioni e le experience digitali di un'azienda, questa soluzione blocca gli attacchi su tutte le porte e i protocolli (nel cloud, on-premise o in entrambi gli ambienti) prima che influiscano sulle vostre attività.

Negli ultimi anni, si è assistito a una notevole ripresa degli attacchi di esaurimento delle risorse mirati all'infrastruttura DNS di un'azienda. Il DNS è l'elemento fondamentale della presenza online di un'azienda. Se il sistema DNS di un'organizzazione si blocca, la sua presenza online scompare. Akamai Edge DNS e Shield NS53 eliminano il traffico di esaurimento delle risorse DNS sull'edge, consentendo solo alle query DNS legittime di raggiungere l'origine del cliente.

La protezione dagli attacchi DDoS è da tempo un requisito imprescindibile per le aziende online, considerando la dimensione degli attacchi che raddoppia ogni due anni e un concomitante aumento delle complessità. Garantire tutti i potenziali point of failure contro questi attacchi è necessario per evitare la perdita del fatturato e della fiducia dei clienti.

Cosa succede quando si verifica un attacco?

È lecito ritenere che, se un'azienda è presente online, prima o poi verrà presa di mira da un attacco. Uno degli scopi di una strategia di sicurezza è proteggervi prima di un attacco, ossia rendervi meno allettanti per i criminali proteggendo le risorse critiche, fornendo visibilità sulla rete in modo da consentirvi di vedere cosa sta succedendo e rilevando gli attacchi tempestivamente

Ma che succede se si verifica qualcosa come un attacco zero-day? È qui che entra in gioco l'analisi comportamentale, che è fondamentale per soluzioni come Akamai App & API Protector.

Akamai combina soluzioni altamente automatizzate con l'intelligenza artificiale e quella umana di oltre 225 addetti dedicati disponibili nel nostro SOCC (Security Operations Command Center) globale per difendere i dati dei clienti, l'infrastruttura e le experience digitali dei loro utenti finali.

Akamai esamina più di 13 trilioni di query DNS (Domain Name System) al giorno e difende da più di 12 miliardi di attacchi WAF (Web Application Firewall) ogni trimestre. Siamo in grado di vedere la situazione generale che abbiamo sperimentato tramite i nostri clienti, traducendo la nostra analisi degli attacchi in un vantaggio. Akamai utilizza questa intelligence sulle minacce per rendere le nostre soluzioni più reattive ed efficaci.

Anche se non utilizzate ancora le soluzioni per la sicurezza di Akamai, ma state subendo un attacco, potete contattarci tramite la nostra linea diretta per le minacce informatiche. Un esperto di sicurezza vi contatterà per illustrarvi le successive operazioni da eseguire per mitigare gli attacchi attuali.

La sicurezza ovunque c'è una connessione

Inevitabili come la morte e le tasse, gli attacchi informatici sono una delle certezze di questo mondo. Tuttavia, potete proteggere la vostra organizzazione e i vostri clienti con soluzioni per la sicurezza che utilizzano informazioni aggiornate sulle minacce, forniscono un'elevata visibilità sulle vostre app e reti e si evolvono con il panorama delle minacce.

Akamai protegge l'experience dei vostri clienti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. Sfruttando la visibilità sulle minacce della nostra piattaforma globale, la nostra ampia gamma di soluzioni offre un'affidabilità leader del settore per consentirvi di stare al passo con le minacce e di adattarvi rapidamente al mutevole panorama della sicurezza.

Altre risorse

Scoprite i 5 passaggi necessari per distruggere la kill chain del ransomware

Supportate la vostra strategia del cloud ibrido e difendetevi, nel contempo, dagli attacchi DDoS

Difendete gli elementi fondamentali della vostra azienda con una solida sicurezza delle API

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti. La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 06/24.