STORIE DI CLIENTI AKAMAI

Tunghai University

Akamai Secure Internet Access Enterprise migliora la sicurezza di Tunghai University e riduce i tempi di gestione degli incidenti

Akamai aiuta un'università a liberare le risorse del team addetto alla sicurezza e a ridurre le notifiche di sicurezza esterne

Le organizzazioni moderne devono affrontare minacce informatiche complesse, dovute ai metodi sempre più sofisticati messi in campo dagli autori degli attacchi per superare le difese di sicurezza. Com'è possibile bilanciare la necessità di proteggersi in modo proattivo da tali attacchi con il bisogno di flessibilità e libertà di una grande popolazione universitaria internazionale?

Questa è la sfida che il team del centro di elaborazione di Tunghai University ha dovuto affrontare. L'università ha adottato con entusiasmo l'apprendimento digitale e ha costruito uno smart campus che offre gratuitamente a studenti e personale l'accesso wireless a Internet ad alta velocità sia nel campus universitario che fuori. All'inizio di ogni anno accademico, gli studenti appena arrivati connettono i propri laptop alla rete dell'università.

Fino a poco tempo fa, poiché la policy IT non imponeva l'installazione di un antivirus sui dispositivi degli studenti, molti dei laptop venivano infettati da malware. I dispositivi compromessi causavano interruzioni delle reti in sede e fuori dall'università, consumavano un'eccessiva larghezza di banda e generavano traffico botnet dannoso. Inoltre, il malware si diffondeva lateralmente nei computer gestiti dall'università, che quindi riceveva dal Taichung Network Regional Center notifiche di attacco e di connessioni anomale.

"Il centro di elaborazione forniva formazione sulla sicurezza delle informazioni e avvertiva gli studenti e il personale di non fare clic su strani link nelle e-mail o sulle pagine web", dice Chien-Hui Ou, direttore delle tecnologie di rete dell'università. "Ma gli autori degli attacchi continuavano a escogitare tattiche sempre più subdole che rendevano molto difficile per gli utenti rendersi conto se i link fossero legittimi, con la conseguenza che spesso cadevano vittime degli attacchi."

Tunghai University
Taichung, Taiwan
eng.thu.edu.tw

Settore
Pubblica amministrazione

Soluzione
Secure Internet Access Enterprise

Risultati principali

- Miglioramento dell'approccio alla sicurezza e riduzione del tempo necessario per la gestione della sicurezza e la risoluzione degli incidenti
- Blocco proattivo del traffico verso i server Command and Control dai dispositivi compromessi e riduzione della diffusione laterale
- Riduzione del volume delle notifiche di sicurezza esterne
- Ottimizzazione del budget per la sicurezza trasferendo gli investimenti da CapEx a OpEx

"I software antivirus e le soluzioni per la sicurezza delle informazioni tradizionali, che si basano sull'analisi e l'identificazione del codice dannoso, non sono abbastanza tempestivi. Se compare sulla scena una nuova variante di malware e i produttori di antivirus non ne hanno ancora analizzato il codice e aggiornato le firme, il malware non viene rilevato", spiega Kuang-Chin Chang del Tunghai University Network Group. "Inoltre, a causa della tendenza a crittografare il traffico web, ora anche gli autori degli attacchi utilizzano questi canali crittografati per lanciare gli attacchi, rendendo sempre più difficile bloccare gli attacchi zero-day."

Akamai blocca efficacemente le connessioni sospette

Rendendosi conto della necessità di migliorare l'approccio alla sicurezza esistente dell'università, il team del centro di elaborazione ha iniziato a prendere in considerazione prodotti che sfruttano il DNS come punto di controllo della sicurezza, ritenendo che questo approccio avrebbe consentito all'università di migliorare la propria sicurezza complessiva senza influire sulla libertà accademica.

Attraverso un processo di valutazione competitivo, l'università ha selezionato Akamai Secure Internet Access Enterprise come soluzione preferita. Secure Internet Access Enterprise è un servizio basato su cloud che protegge in modo proattivo una rete e i suoi utenti analizzando ogni singola richiesta DNS. Ogni query viene messa a confronto con l'intelligence sulle minacce in tempo reale acquisita grazie alla visione impareggiabile di Akamai del traffico Internet per decidere se bloccare o trasmettere i contenuti web richiesti.

"Secure Internet Access Enterprise rileva e blocca le richieste DNS a domini che potrebbero trasmettere contenuti dannosi come ransomware o malware coin-mining oppure impadronirsi delle informazioni degli utenti", dice Chang. "Anche se il computer di uno studente è compromesso dal malware durante l'uso fuori dalla sede universitaria, il malware non sarà in grado di connettersi esternamente al server Command and Control degli autori dell'attacco quando il computer torna sulla rete del campus".

Prima di Secure Internet Access Enterprise, mitigare un incidente di sicurezza delle informazioni era un compito molto difficile. Una volta ricevuta la segnalazione di una connessione anomala, il personale di gestione della rete spesso doveva utilizzare gli indirizzi IP per rintracciare il computer compromesso, trovare le registrazioni delle connessioni nei file di registro per convincere la persona coinvolta che si era verificato un incidente e quindi chiedere a questa persona di collaborare con le procedure di eliminazione del virus.

"Per questo motivo, per risolvere un incidente ci voleva circa una settimana. E questo impegnava una quantità enorme delle nostre risorse di sicurezza", dice Chang. "Dopo aver implementato Secure Internet Access Enterprise, il numero di incidenti di sicurezza segnalati è sceso drasticamente, consentendo alle nostre risorse di dedicarsi ad altri progetti di sicurezza".

Chang aggiunge: "Secure Internet Access Enterprise è particolarmente veloce e facile da implementare e configurare, a differenza delle apparecchiature fisiche tradizionali che richiedono la disconnessione dalla rete prima di poter mettere in funzione un sistema. Con Secure Internet Access Enterprise, è sufficiente indirizzare il traffico DNS direttamente alla piattaforma Akamai e il processo viene completato in pochi minuti".

Il direttore Ou commenta: "Secure Internet Access Enterprise fornisce automaticamente rapporti dettagliati sugli incidenti che consentono al nostro team di sicurezza di capire rapidamente quale malware ha infettato i computer client o quali link web sono stati attivati prima che i computer fossero infettati dal malware coin-mining. I dati si integrano con il nostro SIEM, quindi i rapporti aiutano anche il team a capire le eventuali attività di rete anomale recenti per poter reagire in modo proattivo".

> Dopo aver implementato Secure Internet Access Enterprise, il numero di incidenti di sicurezza segnalati è sceso drasticamente, consentendo alle nostre risorse di dedicarsi ad altri progetti di sicurezza.

Kuang-Chin Chang
Tunghai University Network Group

Significativo risparmio di denaro e personale

Chao-Tung Yang, direttore del centro di elaborazione elettronica di Tunghai University, sottolinea i vantaggi strategici. "La sicurezza delle informazioni è importante oggi e sarà sempre più importante in futuro, con la crescita delle applicazioni digitali. Tunghai ha sempre dato la priorità alla protezione delle applicazioni IT e della sicurezza delle informazioni; inoltre, il rettore dell'università supporta gli investimenti nella sicurezza delle informazioni".

Yang continua: "Se si esamina il quadro complessivo della direzione di crescita dell'IT, è chiaro che i servizi basati su cloud non sono un fenomeno passeggero. I sistemi di difesa precedenti venivano implementati con una combinazione di software e hardware, e la loro manutenzione, l'aggiornamento delle patch e così via richiedevano tempo e manodopera."

I servizi basati su cloud di Akamai cambiano completamente le cose, consentendo una riduzione totale del lavoro di manutenzione. Yang è ottimista sul futuro dei servizi di sicurezza delle informazioni basati su cloud: "Non solo ridurranno la manodopera, ma ridurranno anche la necessità di spazio fisico nei locali per computer e consentiranno di risparmiare sull'aria condizionata e sull'energia elettrica. Una strategia pienamente in linea con gli sforzi del centro di elaborazione di ridurre la quantità di energia utilizzata per i locali delle attrezzature".

"Quanto al costo, l'uso di servizi basati su cloud, a differenza dell'acquisto diretto di apparecchiature fisiche, non richiede un unico investimento finanziario di notevole portata", dice Yang. "Trattandosi di una licenza che viene rinnovata su base annua, Secure Internet Access Enterprise rientra più facilmente nei budget delle università".

"La sicurezza delle informazioni richiede un impegno costante. Con Secure Internet Access Enterprise, tuttavia, la quantità di lavoro per la gestione degli incidenti è notevolmente ridotta, liberando la capacità necessaria per rafforzare le difese contro gli attacchi botnet e per svolgere analisi più complete delle attività", conclude Yang.

> Secure Internet Access Enterprise è particolarmente veloce e facile da implementare e configurare, a differenza delle apparecchiature fisiche tradizionali che richiedono la disconnessione dalla rete prima di poter mettere in funzione un sistema.
>
> **Kuang-Chin Chang**
> Tunghai University Network Group

Tunghai University è stata fondata nel 1955 ed è stata la prima università privata di Taiwan. L'università è il primo e unico istituto di formazione con un programma completo dalla scuola materna alla specializzazione post-laurea. Attualmente, Tunghai comprende nove facoltà: Lettere, Scienze, Ingegneria, Management, Scienze sociali, Agricoltura, Architettura e design creativo, Legge e il College internazionale. Tunghai ha circa 17.000 studenti e quasi 500 docenti: http://eng.thu.edu.tw/.