PROTEZIONE DDoS NETTAMENTE MIGLIORE

Soluzioni nettamente più efficaci e vantaggiose per le piccole e medie imprese

È ORA DI PRENDERE SUL SERIO GLI ATTACCHI INFORMATICI

Anche se sono gli attacchi alle grandi organizzazioni a finire in prima pagina, i governi e le multinazionali non sono le uniche vittime di attacchi di criminalità informatica. Anche le piccole e medie imprese (PMI) possono diventare una preda interessante, e infatti sono sempre più spesso sotto attacco.

I criminali informatici si basano sul fatto che la maggior parte delle aziende di piccole dimensioni non dispongono della stessa protezione IT che contraddistingue invece le organizzazioni più grandi, di solito a causa della mancanza di risorse tecniche, finanziarie e umane. Tuttavia, alcune piccole imprese e start-up sono spesso innovative e altamente specializzate, e quindi la loro proprietà intellettuale e i dati dei loro clienti possono avere un grande valore. Gli hacker possono anche voler colpire la loro supply chain per raggiungere obiettivi più grandi o più preziosi tra i loro clienti e fornitori.

Inoltre, una crescente dipendenza da applicazioni e servizi web-based, come i portali dei clienti o dei partner, sta aumentando il rischio (e il costo potenziale) di attacchi Distributed Denial of Service (DDoS). Tanto più che il costo e la complessità tecnica per dare vita a questa tipologia di attacchi sono ormai molto ridotti, per cui le motivazioni alla base di attacchi DDoS sono più diversificate che mai: un tentativo di estorsione, una protesta contro alcune pratiche aziendali oppure un gesto di vendetta da parte di un cliente insoddisfatto o di un ex-dipendente

Al giorno d'oggi, con conoscenze tecniche di basso livello e pochissimo denaro, chiunque provi una sorta di rancore per un'azienda è in grado di lanciare un attacco, e potenzialmente soffocare la crescita di un'azienda o, nel peggiore dei casi, portarla alla chiusura.

La questione della sicurezza informatica per le piccole imprese è resa ancora più incombente dalle nuove normative europee volte a proteggere i dati dei clienti. Il nuovo Regolamento Generale sulla Protezione dei Dati (GDPR) dell'UE entrerà in vigore nel 2018 e potrebbe portare a sanzioni ai danni delle aziende fino a 20 milioni di euro o pari al 4% del loro fatturato annuo, la cifra maggiore tra le due, per impedire che eventuali violazioni della sicurezza possano compromettere i dati dei loro clienti.

Le PMI hanno bisogno di una protezione DDoS nettamente migliore, perché per proteggere l'utente non si può sempre contare sul proprio Internet Service Provider (ISP).

"Due terzi delle piccole imprese hanno subito attacchi di criminalità informatica nel corso degli ultimi due anni."
Federation of Small Businesses[1]

[1] "Resilienza informatica: come proteggere le piccole imprese nell'economia digitale", Federation of Small Businesses, Giugno 2016

UN MODO ECONOMICO PER PROTEGGERE IL TUO BUSINESS

L'Availability Protection System (APS) di Arbor Networks® è una soluzione di sicurezza on-premise basata sulla difesa del perimetro di rete per proteggere la continuità e la disponibilità dei sistemi e dei servizi aziendali dalla crescente costellazione di attacchi DDoS e di altre minacce avanzate

Sviluppato inizialmente per soddisfare i sempre più stringenti requisiti di sicurezza delle grandi aziende, Arbor ha introdotto una nuova opzione di licenza 100M per la sua applicazione APS 2600. Questo consente alle piccole e medie imprese di beneficiare di una protezione on-premise di livello premium, ma ad un prezzo accessibile e basata su una piattaforma facile da implementare.

Questo sistema integra tecnologie sofisticate per il rilevamento degli attacchi e la mitigazione dei rischi, che forniscono una visione completa delle attività di rete e consentono di reagire immediatamente con sistemi avanzati di blocco, in modo da neutralizzare automaticamente gli attacchi prima che possano colpire le applicazioni e i servizi critici.

Inoltre, ha anche la capacità di estendere ulteriormente la vostra protezione, utilizzando il Cloud Signaling per connettere servizi DDoS basati sul cloud. È quindi possibile allertare automaticamente i service provider a monte, come ad esempio l'ISP o Arbor Cloud, quando eventuali attacchi su ampia scala minacciano la disponibilità, e garantire che questi rischi siano mitigati molto più rapidamente.

CINQUE MOTIVI PER SCEGLIERE APS 2600

1) Conveniente
La maggior parte dei prodotti per la protezione DDoS a disposizione delle PMI sono add-on di altri prodotti oppure non dispongono delle caratteristiche essenziali per essere convenienti.

Con Arbor APS 2600, si può beneficiare di una sicurezza di livello enterprise senza compromessi. La versione 100M è disponibile a partire da 17.995 $, così da poter finalmente implementare la soluzione che hai sempre voluto e che serve al tuo business.

2) Semplice
APS 2600 è l'ideale se disponete di competenze tecniche limitate.
Chiunque può implementarla. Grazie alla sua configurazione "plug & play", può essere installata rapidamente e facilmente utilizzando le impostazioni predefinite.

Questa applicazione consente di proteggere la vostra organizzazione quasi immediatamente, anche durante un attacco. Poi, col passare del tempo, potete anche personalizzarla facilmente, in base alle vostre esigenze aziendali specifiche.

La semplicità della sua struttura e l'interfaccia utente hanno vinto svariati riconoscimenti nel settore, tra cui il Gold Award per il "Best Hardware Security" in occasione degli Info Security Products Guide's Awards 2016.

"Arbor APS rappresenta una soluzione collaudata e fuori dagli schemi per l'identificazione degli attacchi con funzionalità di mitigazione che possono essere implementate con una semplice configurazione, anche durante un attacco."
Info Security Products Guide's Awards 2016

3) Efficace
Nonostante la sua convenienza e fruibilità, APS 2600 offre un ampio ventaglio di strumenti di livello enterprise per attacchi di tipo "TCP State-Exhaustion" e attacchi all'application layer, prima che questi possano ripercuotersi sulla rete e sulla disponibilità del servizio. Questo consente di beneficiare esattamente dello stesso livello di protezione delle più grandi aziende del mondo per le quali questo sistema è stato originariamente sviluppato.

In particolare, riceve ininterrottamente informazioni accurate sulle più recenti minacce dall'ATLAS Intelligence Feed di Arbor. Non appena vengono scoperti maggiori dettagli sui nuovi attacchi, tali informazioni vengono inviate automaticamente a tutti i prodotti Arbor, affinché siano pronti a reagire contro ogni minaccia e bloccare e mitigare i più recenti tipi di attacco o di minaccia avanzata, prima che il vostro business possa esserne compromesso.

Nessun'altra soluzione è in grado di fare altrettanto!

CINQUE MOTIVI PER SCEGLIERE APS 2600

4) Scalabile
La versione di APS 2600 per le PMI è la nostra applicazione più “piccola”, ma può comunque gestire fino a 100 Mbps di throughput ispezionato in loco.

Tuttavia, per un abbonamento mensile a prezzi accessibili, può anche essere abbinata, senza interruzione di continuità, al servizio DDoS di Arbor basato sul cloud. Questo andrà quindi automaticamente e rapidamente ad aumentare le difese contro gli attacchi DDoS volumetrici che sono troppo grandi per essere mitigati on-premise, senza interrompere l’accesso alle vostre applicazioni e servizi.

Questo consente di reagire ad attacchi di qualsiasi dimensione, senza appesantire le difese on-site e senza dover attendere che il vendor dei sistemi di sicurezza debba attivare manualmente un’ulteriore protezione basata sul cloud.

“Una soluzione ibrida è l’unico modo efficace per affrontare attacchi volumetrici e all’application layer.”
Frost & Sullivan[2]

Questo approccio riflette le best practice del settore. Per bloccare i più recenti attacchi DDoS e le minacce avanzate, gli analisti del settore raccomandano un approccio globale multi-livello, che consente di rilevare, prevenire e rispondere agli attacchi in maniera più rapida e intelligente.

5) Completa
È importante capire la distinzione tra le soluzioni di rilevamento DDoS e di protezione DDoS. Alcune tecnologie, in particolare quelle che sono spesso vendute come add-on a un firewall, sono progettate semplicemente per rilevare quando un’organizzazione diventa il bersaglio di un attacco DDoS, ma non offrono funzionalità di protezione o di mitigazione.

Al contrario, Arbor offre una combinazione completamente integrata di prodotti e di servizi di protezione in-cloud e on-premise, costantemente supportati dalla Threat Intelligence globale di Arbor.

Nessun altro provider offre una soluzione di protezione DDoS così completa, e proprio questo è il motivo per cui Arbor è il fornitore numero uno di applicazioni di prevenzione DDoS, nei segmenti enterprise, carrier e mobile [3].

Fornendo una soluzione completa per tutte le vostre esigenze di protezione dei dati, Arbor si assume la piena responsabilità di proteggere il vostro business, in modo da non dover perdere tempo con fornitori diversi e le responsabilità sono molto più chiare, senza alcun rischio di scaricare le responsabilità gli uni sugli altri.

È inoltre possibile accedere ad un livello di competenza tecnica senza paragoni. L’Arbor Security Engineering & Response Team (ASERT) è un gruppo di ingegneri della sicurezza e ricercatori di fama mondiale impegnato a monitorare costantemente le minacce on-line. Grazie all’ASERT, le organizzazioni dispongono della competenza necessaria per rafforzare i propri gruppi incaricati delle risposte di sicurezza, già oberati di lavoro, e ottimizzare la difesa di tutta la loro infrastruttura di rete.

---

[2] “Scoprire il fiorente mercato della mitigazione DDoS”, Frost & Sullivan, agosto 2014
[3] “Applicazione per la prevenzione DDoS”: market tracker biennale”. IHS Infonetics, giugno 2016

IL MOMENTO DI AGIRE È ADESSO

Con l’aumento del volume e della complessità degli attacchi DDoS, è quasi inevitabile che la vostra azienda finirà prima o poi sotto attacco, con conseguenze potenzialmente gravi per la vostra redditività, le relazioni con i clienti, la reputazione e le prospettive di crescita.

APS 2600 fornisce una protezione di livello enterprise, ma a un prezzo adatto alle piccole imprese. E voi pensate davvero di potervi permettere di farne a meno?

ARBOR NETWORKS

Arbor Networks, la divisione sicurezza di NETSCOUT aiuta a proteggere le più grandi reti enterprise e service provider da attacchi DDoS e minacce avanzate. Secondo Infonetics Research, Arbor è il principale fornitore al mondo di protezione DDoS nei segmenti enterprise, carrier e mobile. Le soluzioni alle minacce avanzate di Arbor Networks Spectrum™ offrono una visibilità completa della rete, combinando la cattura dei pacchetti e la tecnologia NetFlow, in modo da consentire la rapida individuazione e la mitigazione di malware e di minacce interne. Arbor vuole essere un “moltiplicatore di forze”, facendo rete e creando squadre di esperti. Il nostro obiettivo è fornire un’immagine più accurata delle reti e del contesto di sicurezza, così che i clienti possano risolvere i problemi più velocemente e ridurre il rischio per il proprio business.

Per maggiori informazioni sui prodotti e i servizi Arbor, contattaci!

Moris Tomasini

moris.tomasini@westcon.com

0396072232

https://it.linkedin.com/company/westcon-security-italy

@Westcon_Italy