WHITE PAPER

Applicazione di un modello di sicurezza Zero Trust negli odierni ambienti ostili

Akamai

Analisi riassuntiva

Aziende di ogni tipo si interessano sempre di più alla trasformazione digitale. L'obiettivo è migliorare il valore per il cliente, operare con maggiore efficienza e agilità e aumentare l'innovazione. Tuttavia, sin da quando le aziende hanno iniziato a usufruire di nuovi workflow cloud e DevOps per realizzare le proprie aziende digitali, la sicurezza non è riuscita a tenere il passo. Con il continuo proliferare di applicazioni cloud e di una forza lavoro mobile, l'efficacia del perimetro di rete ha subito un calo radicale. Le applicazioni, i dati, gli utenti e i dispositivi si stanno spostando al di fuori della zona di controllo aziendale, provocando, così, un aumento della superficie aziendale soggetta agli attacchi. Se da un lato le infrastrutture diventano più permeabili e consentono nuovi modelli di business, dall'altro i criminali informatici diventano sempre più abili, sofisticati e spinti a cercare modi per eludere le misure di sicurezza. La sicurezza perimetrale tradizionale non è stata mai concepita per arrivare alla realtà odierna.

In che modo le aziende possono difendersi dai sempre più frequenti attacchi informatici e dalle conseguenti violazioni? In questo white paper, viene descritto un paradigma di sicurezza adatto agli odierni ambienti ostili: il modello Zero Trust. Grazie a questo modello, utenti e dispositivi vengono sempre sottoposti a verifiche e l'ambiente viene considerato come ostile. Il modello Zero Trust evidenzia come non debbano esserci distinzioni tra il traffico di rete interno e quello esterno in termini di attendibilità. Con questo modello, tutte le richieste di accesso e tutti i dispositivi vengono sempre verificati con log completi e analisi comportamentali. Inoltre, questo documento spiegherà perché l'IT dovrebbe cercare di adottare i servizi cloud per allontanarsi dalla sicurezza perimetrale.

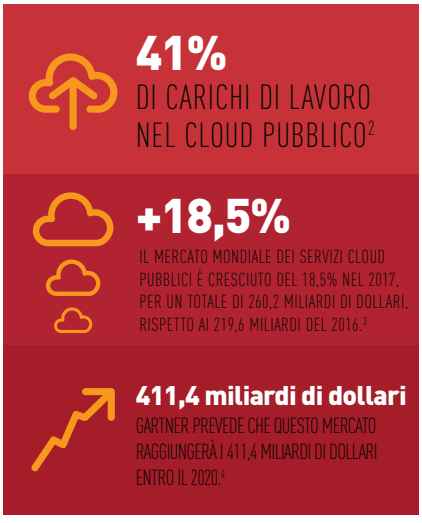
La trasformazione digitale è imprescindibile

Nella gran parte delle aziende, è ormai onnipresente una notevole trasformazione digitale. E questa tendenza diventa sempre più frequente. Dagli studi di IDC, si prevede che gli investimenti nella trasformazione digitale raggiungeranno i 2.200 miliardi di dollari nel 2019, aumentando quasi del 60% rispetto al 2016.[1]

Le aziende si servono di architetture cloud e di rete avanzate, per offrire un nuovo valore per il cliente, aumentando l'efficienza operativa, l'agilità e l'innovazione. La trasformazione digitale è un vantaggio per i clienti, in quanto consente alle aziende di offrire prodotti digitali, servizi migliori, interazioni personalizzate e una customer experience di livello superiore. I dipendenti approfittano delle tecnologie digitali per comunicare e collaborare online con facilità, migliorando la produttività e il morale.

I perimetri affidabili sono scomparsi

Tuttavia, anche se l'utilizzo di servizi digitali comporta molti vantaggi, le aziende stanno notando un aumento della superficie aziendale soggetta agli attacchi, nell'odierno panorama delle minacce sempre più ostile. Di conseguenza, hanno necessità di rielaborare le basi della sicurezza perimetrale e di pensare a come proteggere le proprie applicazioni, i dati e gli utenti di importanza critica.



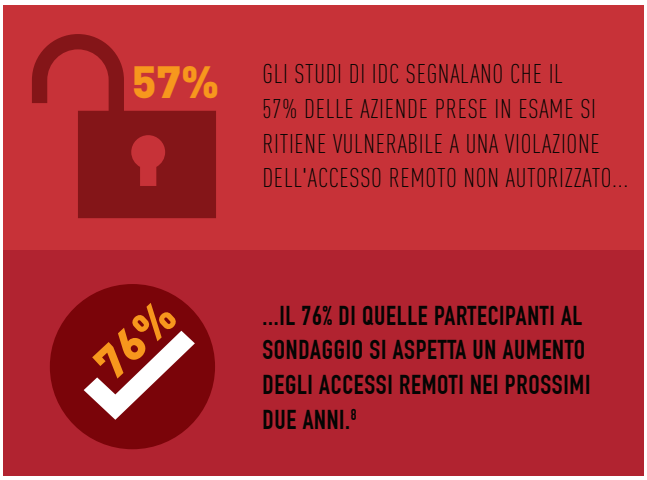
La trasformazione digitale ha un forte impatto sul modo in cui le aziende forniscono le soluzioni IT, nonché sulla loro esposizione alle minacce. Finora, gli utenti interagivano con le applicazioni in modo sicuro tramite reti LAN (Local Area Network) private, WAN (Wide Area Network) o VPN (Virtual Private Network). Le aziende si servivano della sicurezza perimetrale, come i firewall, delle VPN e delle tecnologie NAC (Network Access Control) per mantenere lontani i criminali dalle reti interne. Una volta all'interno della rete, gli utenti venivano considerati intrinsecamente affidabili e potevano spostarsi dove volevano.

Ora che le aziende stanno passando alla trasformazione digitale, sta cambiando tutto. Le applicazioni risiedono sempre di più nel cloud, all'esterno della zona di controllo tradizionale dell'IT. Gli intervistati del sondaggio condotto da RightScale hanno affermato di eseguire il 41% dei carichi di lavoro sul cloud pubblico.[2] Il mercato mondiale dei servizi cloud pubblici è cresciuto del 18,5% nel 2017, per un totale di 260,2 miliardi di dollari, rispetto ai 219,6 miliardi del 2016.[3] Gartner prevede che questo mercato raggiungerà i 411,4 miliardi di dollari entro il 2020.[4]

I dipendenti si connettono dall'ufficio sempre meno spesso. Non è raro che si trovino in viaggio o che lavorino in remoto, sparsi in tutto il mondo, connessi a reti non protette. Il Global Telework Survey di PGI ha evidenziato che il 79% dei knowledge worker del mondo è rappresentato da telelavoratori.[5]

Inoltre, l'idea che un'azienda digitale impieghi soltanto lavoratori a tempo pieno è ormai superata. La produttività della maggior parte delle aziende dipende dai suoi fornitori, dai venditori, dagli appaltatori e dai partner che richiedono l'accesso a specifiche applicazioni interne. Come prevedibile, un qualsiasi accesso da parte di soggetti esterni aumenta il rischio che informazioni aziendali critiche finiscano nelle mani sbagliate. Inoltre, il proliferare di policy BYOD (Bring Your Own Device) implica un minor controllo da parte dell'IT sui dispositivi utilizzati dagli utenti per accedere alle applicazioni e ai dati aziendali.

Al tempo stesso, i criminali informatici continuano a trovare modi per eludere i firewall in modo sempre più semplice. Alcuni entrano con credenziali utente affidabili, altri tramite link o allegati dannosi. Gli studi condotti da Symantec hanno evidenziato che il tasso di malware nelle e-mail è aumentato notevolmente da 1 mail contenente malware ogni 220 e-mail inviate, nel 2015, a 1 mail infetta ogni 131 mail inviate, nel 2016.[6] E, una volta violata la rete, i criminali non vengono identificati per una media globale di 146 giorni.[7] Gli studi di IDC segnalano che il 57% delle aziende prese in esame si ritiene vulnerabile a una violazione con accesso remoto non autorizzato e che il 76% di quelle partecipanti al sondaggio si aspetta un aumento degli accessi remoti nei prossimi due anni.[8] Le perdite conseguenti ad accessi remoti non autorizzati sono ingenti. In media, le aziende prevedono di destinare 6,5 milioni di dollari per questa causa.[9]



La sicurezza perimetrale tradizionale è inadeguata

Con le applicazioni aziendali, i dati, i dispositivi e gli utenti che si spostano al di fuori del perimetro, mentre le minacce informatiche entrano, la sicurezza perimetrale tradizionale non basta più.

Le aziende hanno protetto per tanto tempo le reti aziendali tramite stack perimetrali o DMZ, che includono appliance per il controllo degli accessi (appliance VPN, provider di identità, autenticazione single-sign-on/multifattore, client-server), per la sicurezza (Web Application Firewall, prevenzione della perdita di dati, firewall di nuova generazione, gateway web protetti) e per le performance e la delivery delle applicazioni (bilanciamento e ottimizzazione del carico). Ma queste architetture perimetrali non sono mai state progettate per ottimizzare l'experience degli utenti che accedono alle applicazioni da varie posizioni. Inoltre, non sono state progettate per soluzioni SaaS (Software-as-a-Service) o applicazioni ospitate nel cloud. Per risolvere la questione, i reparti IT spesso devono ripetere questi stack per assicurare ridondanza e disponibilità elevata in tutte le aree e i data center, con costi e complessità crescenti.

Poiché le applicazioni si spostano nel cloud, le aziende non hanno più lo stesso tipo di controllo: la sicurezza di rete tradizionale, basata su pacchetti, porte e protocolli, non funziona quando le aziende non gestiscono l'intero ambiente applicativo e la rete.

Nel prossimo futuro, le aziende continueranno a eseguire sia applicazioni in sede che nel cloud. Avranno necessità di mantenere una combinazione casuale di soluzioni di controllo degli accessi e di sicurezza, che potrebbero non funzionare bene insieme, senza un punto centrale dal quale gestire e controllare queste tecnologie. Sistemi frammentati implicano maggiori rischi e meno visibilità.

Per giunta, la premessa alla base della sicurezza perimetrale (ossia che le mura funzionino) è diventata obsoleta. I criminali spesso riescono ad accedere alle reti aziendali utilizzando nomi utente e password realmente esistenti o installando malware che rilevano le vulnerabilità delle soluzioni di sicurezza esistenti. Un recente rapporto ha rivelato che il 91%

degli attacchi informatici inizia da una tecnica di phishing concepita per sottrarre credenziali utente realmente esistenti.[10] Le soluzioni perimetrali non fanno nulla per salvaguardare i dati e le applicazioni aziendali dagli attacchi originati all'interno del perimetro.

La nuova era del modello Zero Trust

Mentre la tradizionale sicurezza perimetrale arriva a fine corsa, in che modo le organizzazioni possono proteggere le applicazioni, i dati e la forza lavoro dalle minacce di alto profilo che sempre più frequentemente incombono sulla cybersicurezza? La risposta sta nell'implementare un modello di sicurezza Zero Trust, che modifica il concetto di base di "fiducia supportata da continue verifiche" in "verificare sempre, senza fidarsi".

Sostenuto, in origine, da Forrester Research, un modello di sicurezza Zero Trust si basa sull'assunto che non esiste un "dentro" e che tutti gli utenti e tutti i dispositivi sono potenzialmente inaffidabili, senza distinzioni. Questo modello tratta tutte le applicazioni come interfacciate con Internet e considera l'intera rete come compromessa e ostile. I componenti chiave del modello Zero Trust sono:

- Garantire un accesso sicuro a tutte le risorse, a prescindere dalla posizione o dal modello di hosting
- Adottare una strategia basata sul principio del "privilegio minimo" e applicare un rigoroso controllo degli accessi, per limitare i rischi associati ad eccessivi privilegi utente
- Ispezionare e registrare tutto il traffico, al fine di individuare attività sospette e migliorare il rilevamento e la risposta delle misure di sicurezza

Lunga vita al cloud

Man mano che gli utenti, i dispositivi, i dati e le applicazioni continuano a evolversi, le funzionalità adatte ad applicare l'approccio Zero Trust dovrebbero assestarsi nel cloud, e utilizzare Internet come rete principale. Anziché utilizzare i firewall, che bloccano IP e porte, la sicurezza basata sul cloud dovrebbe concentrarsi sul livello applicativo e su protocolli di livello superiore. Utilizzando i controlli di sicurezza basati sul cloud, le aziende possono essere in grado di bloccare i firewall e di nascondere le applicazioni interne da Internet. I servizi di autenticazione e autorizzazione consentono, poi, di controllare gli accessi a ogni tipo di applicazione da dispositivi, gestiti o meno, sia in sede, eseguiti su una piattaforma IaaS (Infrastructure-as-a-Service), come Amazon Web Services, sia di tipo SaaS.

I controlli di sicurezza basati sul cloud devono verificare tutte le richieste DNS in uscita, provenienti dai dispositivi di un'azienda, compresi i portatili e i dispositivi IoT (Internet of Things), per assicurarsi che non si dirigano verso siti dannosi o inaccettabili. La soluzione deve anche monitorare e analizzare il comportamento del traffico, per cercare segnali di attività sospette, come la comunicazione con un server CnC (Command and Control) o l'esfiltrazione dei dati, avvisando immediatamente l'IT in caso di problemi.

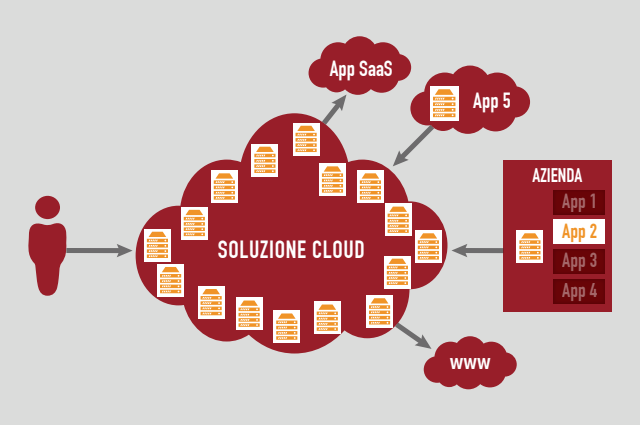
L'implementazione del sistema Zero Trust tramite il cloud risolve la maggior parte delle sfide riscontrate con una sicurezza di rete perimetrale obsoleta. Garantisce che gli utenti autenticati abbiano diritto ad accedere solo alle applicazioni consentite. Impedisce anche agli endpoint infetti di accedere a siti web dannosi o inaccettabili o di connettersi a un'infrastruttura CnC dannosa, che potrebbe prendere il controllo dei computer degli utenti ed esfiltrare i dati. Inoltre, può bloccare i malware e impedire che si spostino lateralmente nella rete.

Attivazione del modello Zero Trust con il cloud

Un servizio cloud aiuta le aziende a ridurre la superficie soggetta agli attacchi, applicando un modello di sicurezza Zero Trust che sfrutta l'agilità, la scalabilità e i vantaggi economici di Internet.

Accesso protetto

Le aziende che intraprendono il processo di trasformazione digitale devono fornire ai dipendenti, ai fornitori, ai consulenti e agli altri partner un accesso rapido, facile e sicuro alle applicazioni dietro il firewall da qualsiasi tipo di dispositivo, in ogni parte del mondo. Le tradizionali tecnologie di accesso, di solito, utilizzano varie appliance hardware e software, per concedere l'accesso alla rete a tutti gli utenti che dispongano delle credenziali appropriate. Tuttavia, gli studi hanno dimostrato che la maggior parte delle violazioni avviene a causa del furto o dell'uso improprio di credenziali utente valide. Un modello di sicurezza Zero Trust si basa sull'assunto che tutti gli utenti sono compromessi e inaffidabili.



L'utilizzo del cloud come estensione della propria infrastruttura consente un accesso Zero Trust, fornendo un accesso solo alle applicazioni necessarie agli utenti, piuttosto che all'intera rete. Questo principio del privilegio minimo si estende a tutti i dispositivi e applicazioni in ogni parte del mondo.

Con la sicurezza basata sul cloud, non è consentito accedere direttamente alle applicazioni, poiché nessuna applicazione è esposta, né in Internet né pubblicamente. Il cloud non risiede soltanto nel percorso di autenticazione e autorizzazione, ma anche direttamente nel percorso dati dell'utente ed è l'unico punto di ingresso che permette agli utenti di accedere alle risorse aziendali critiche. Il servizio cloud offre una connessione TLS sicura, con autenticazione bilaterale dall'interno della rete aziendale o della piattaforma IaaS e distribuisce l'applicazione all'utente. I proxy sicuri applicano rigidi controlli di autenticazione e sicurezza. Queste funzionalità isolano le reti interne e le applicazioni IaaS da Internet e spostano la superficie aziendale soggetta agli attacchi all'edge.

Autenticazione

Per fornire agli utenti accesso sicuro alle applicazioni e ai dati di valore elevato, la sicurezza basata sul cloud dovrebbe integrarsi con i servizi di autenticazione esistenti (ad es., Okta o Microsoft Active Directory) oppure offrire le proprie soluzioni di autenticazione, con funzionalità di sicurezza avanzate, come l'autenticazione a due fattori o multifattore. Poiché viene richiesta l'autenticazione per il dispositivo e l'utente, la sicurezza è ulteriormente migliorata rispetto agli approcci tradizionali, in quanto l'autore di un attacco deve rubare almeno due identità per accedere alle risorse.

Il cloud migliora ulteriormente la sicurezza autenticando gli utenti al di fuori dell'infrastruttura dell'utente, senza richiedere hardware o software aggiuntivi.

Autorizzazione

Servendosi di una strategia di accesso basata sul principio del "privilegio minimo" e applicando un rigoroso controllo degli accessi, le organizzazioni riducono le strade disponibili per cybercriminali e malware per ottenere accessi non autorizzati. Una soluzione cloud può aiutare, fornendo esplicitamente un accesso specifico per le applicazioni, anziché applicare privilegi programmati. Le organizzazioni possono definire le policy di sicurezza per tutti gli utenti, i dispositivi, le applicazioni e i dati.

Sistemi di sicurezza su più livelli

Ma se una rete Zero Trust controlla in modo rigoroso l'accesso a tutte le risorse di rete, anche le applicazioni sono soggette ad attacchi DDoS (Distributed Denial of Service), SQLi (Structured Query Language Injection), attacchi a livello di applicazione e altro. La sicurezza basata sul cloud deve offrire ulteriori livelli di difesa contro questo tipo di attacchi. La protezione DDoS tutela dagli attacchi che inondano le app o i siti con richieste superflue, che tentano di sovraccaricare i sistemi e compromettere l'accesso degli utenti legittimi all'applicazione. La sicurezza a livello delle applicazioni protegge ad esempio da attacchi SQLi, che sono in grado di manipolare, danneggiare o eliminare dati. Queste soluzioni proteggono anche dal frequente utilizzo di attacchi DDoS come tattica diversiva, ossia quando l'attacco DDoS viene sferrato assieme a un attacco a livello dell'applicazione di tipo SQLi o XSS (Cross-Site Scripting).

Ispezione di tutto il traffico basata su proxy

Il controllo degli accessi protegge le applicazioni note, ma molti dipendenti e partner utilizzano applicazioni basate su Internet, come Google o Trello. Queste applicazioni possono risultare un toccasana per la produttività della forza lavoro, ma i siti web possono contenere anche malware dannosi o contenuti inaccettabili, come incitamento all'odio o pornografia. Inoltre, gli attacchi di phishing (che si servono di link a domini dannosi) stanno aumentando e sono fonte di attacchi malware. Mentre molte aziende implementano diversi livelli di protezione, l'esfiltrazione dei dati via DNS resta una grande lacuna nella sicurezza di molte aziende.

Invece di risolvere tutte le richieste DNS ciecamente, le aziende devono servirsi di controlli di sicurezza basati sul cloud, per applicare in modo efficace un'intelligence in tempo reale e fornire una protezione proattiva contro le minacce in continua evoluzione. I servizi di sicurezza basati sul cloud devono poter agire come un server DNS ricorsivo, verificare i nomi di dominio a fronte di un elenco completo e aggiornato di frequente di domini noti come dannosi, applicare la propria intelligence e amministrare i criteri che impediscono alle richieste di raggiungere domini infetti o domini con contenuti inaccettabili. Dal momento che la convalida avviene prima dell'avvenuta connessione IP, le minacce vengono arrestate preventivamente nella kill chain di sicurezza.

Quanto più le aziende si servono di dispositivi IoT, tanto più il sistema Zero Trust diventa sempre più importante. Ad esempio, l'IT potrebbe non sapere che una TV connessa, in una sala conferenze, sta inviando richieste a domini dannosi su Internet: un'azione potenzialmente indicativa di compromissione.

Intelligence sulle minacce in tempo reale

Il concetto del "verificare sempre" implica la necessità di monitorare e ispezionare continuamente il traffico alla ricerca di attività sospette. Il sistema Zero Trust si basa sull'assunto che anche il traffico originato sulla LAN è sospetto e, pertanto, va analizzato e registrato come se provenisse da Internet. L'analisi comportamentale identifica i modelli di traffico sospetti, come quelli che indicano la comunicazione con un server CnC o l'esfiltrazione dei dati.

Conclusione

Con il sistema Zero Trust in un'architettura basata sul cloud, le aziende possono adattare la sicurezza informatica all'odierna realtà dell'IT. Sia che le applicazioni e i dati risiedano nel data center o nel cloud, le aziende sono in grado di arrivare a utenti che potrebbero trovarsi ovunque e utilizzare qualsiasi dispositivo, fornendo loro un accesso sicuro, semplice ed efficiente. Possono impedire agli utenti di accedere ad applicazioni esterne contenenti malware, che potrebbero compromettere la rete o contenere contenuti inaccettabili. E possono monitorare costantemente il traffico, alla ricerca di comportamenti sospetti. Di conseguenza, le aziende possono servirsi a tutto tondo delle tecnologie più recenti per implementare la trasformazione digitale, fiduciose di sapere che i dati e le applicazioni più importanti restano al sicuro.

Fonti

1. https://www.idc.com/getdoc.jsp?containerId=prUS41888916
2. www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey
3. https://www.gartner.com/newsroom/id/3815165
4. https://www.gartner.com/newsroom/id/3815165
5. https://www.ondeck.com/blog/your-complete-guide-to-the-remote-workforce-in-2017
6. https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_
7. https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html
8. https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
9. https://www.computerworld.com/article/3222829/security/state-of-remote-access-security.html
10. https://www.darkreading.com/endpoint/91--of-cyber attacks-start-with-a-phishing-email/d/d-id/1327704?