eBook

10 modi per difendersi dai ransomware con lo zero trust

- **Il 50% dei ransomware sfrutta la doppia estorsione**
  Ogni attacco ransomware può comportare una potenziale violazione dei dati
- **Ogni 14 secondi, nel mondo, un attacco va a segno**
  Ogni organizzazione è a rischio, e gli attacchi crescono di volume e portata
- **Aumento di oltre il 500% dei ransomware criptati dall'inizio del 2020**
  Gli aggressori nascondono gli attacchi per aggirare i controlli di sicurezza tradizionali

I ransomware rappresentano la più grande minaccia per le aziende digitali

Sebbene i ransomware siano in circolazione da decenni, la loro diffusione è esplosa negli ultimi due anni. Questi attacchi in passato venivano perpetrati da singoli individui, mentre ora vengono scagliati da gruppi di affiliati che acquistano e vendono i propri toolkit e le proprie competenze specializzate. Un tempo, gli attacchi non avevano obiettivi precisi ed erano unidimensionali, mentre oggi impiegano tattiche mirate e multilivello che sono molto più difficili da contrastare, e i riscatti richiesti sono più elevati. **Secondo le stime, entro la fine del 2024, i ransomware causeranno danni per un ammontare pari a 42 miliardi di dollari.**[1]

Probabilmente, la tendenza più impattante nel mondo dei ransomware moderni consiste nell'avvento degli attacchi a doppia estorsione, in cui gli aggressori rubano dati e minacciano di pubblicarli oltre che criptarli. Attualmente, circa il 50% degli attacchi ransomware include dei tentativi di esfiltrazione dei dati.

Per mitigare il più possibile i danni derivanti da attacchi ransomware andati a buon fine, le organizzazioni possono adottare un approccio zero trust.

Lo zero trust è un approccio alla sicurezza che si basa sul concetto che una violazione sia già avvenuta. Vengono configurate architetture, policy di controllo degli accessi e tattiche di monitoraggio e autenticazione, volte a mitigare la quantità e la gravità dei danni che un aggressore è in grado di infliggere.

Ecco dieci modi attraverso cui lo zero trust può aiutare le organizzazioni a difendersi dai ransomware.

[1] *Secondo Cybersecurity Ventures, si stima che i costi dei danni globali provocati dai ransomware supereranno i 265 miliardi di dollari entro il 2031.*

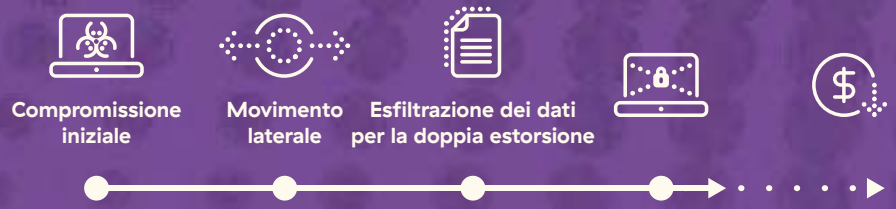
La sequenza di attacco dei ransomware

In un attacco ransomware, gli aggressori devono portare a termine una serie di azioni per riuscire ad avere successo. Innanzitutto, devono penetrare nell'ambiente e riuscire a infettare un sistema attraverso il payload dannoso di un ransomware. **Il primo passo per fermare un attacco consiste quindi nel mettere in atto controlli preventivi che riducano al minimo la superficie di attacco e le vulnerabilità e che consentano di bloccare, controllare e ispezionare il traffico.**

In secondo luogo, gli aggressori effettuano una ricognizione e individuano le risorse ad alto valore da rubare e criptare. A tal fine, devono essere in grado di muoversi lateralmente in tutta la rete. **Il secondo passo per bloccare un attacco e ridurre al minimo i danni che un aggressore è in grado di infliggere consiste nel limitare la sua capacità di muoversi lateralmente.**

In un attacco a doppia estorsione, gli aggressori rubano i dati e li trattengono in ostaggio per aumentare le loro possibilità di successo e l'ammontare in dollari delle richieste di riscatto. **Il terzo passo per difendersi da un attacco ransomware consiste nella prevenzione sulla perdita dei dati.**

Vediamo in che modo lo zero trust consente di estendere la difesa abbracciando tutta la catena di attacco.



N°1

Rendendo le applicazioni invisibili agli aggressori, un'architettura zero trust riduce al minimo la superficie di attacco.

Lasciare che applicazioni, utenti e identità dei dispositivi siano apertamente individuabili su Internet equivale a esporre al pubblico le informazioni più preziose. Se queste risorse sono visibili, gli aggressori sono in grado di individuare e sfruttare rapidamente le vulnerabilità, come il software di un server web senza patch o una password debole che può essere violata in un attacco di forza bruta. In questi modi possono ottenere un punto di accesso immediato e diretto all'ambiente.

L'utilizzo di una soluzione come Zscaler Private Access™ consente alle applicazioni di connettersi agli utenti, anziché far sì che questi ultimi si connettano alle applicazioni. Con questa connettività dall'interno verso l'esterno, tutte le applicazioni rimangono private e di conseguenza invisibili agli aggressori. Estendendo questo approccio a tutti i dispositivi e alle applicazioni dell'ambiente, si rende praticamente impossibile la ricognizione da parte degli aggressori.

N°2

In un'architettura zero trust, tutto il traffico, incluso il traffico criptato, è soggetto a un'ispezione approfondita e accurata.

La maggior parte del traffico Internet utilizza la crittografia, e il traffico dannoso non fa eccezione. Oltre il 90% del traffico Internet oggi è criptato, e la crittografia dei ransomware è aumentata di oltre il 500% dall'inizio del 2020. I team addetti alla sicurezza non possono più permettersi di considerare sicuro tutto il traffico SSL.

L'ispezione di tutto il traffico ora è essenziale in una solida strategia difensiva, e le architetture che fanno affidamento su firewall di nuova generazione e altre difese basate sul perimetro non sono più in grado di garantire la sicurezza. È del tutto impossibile, persino per gli strumenti di sicurezza on-premise più avanzati, ispezionare tutto il traffico criptato con SSL senza introdurre colli di bottiglia a livello prestazionale che ostacolano la produttività. Un'architettura con base proxy sul cloud, creata appositamente per rilevare malware criptati con SSL su larga scala, potrà proteggere tutto il traffico ed eliminare i punti ciechi.

N°3

Le strategie zero trust includono controlli per rilevare le minacce ransomware sconosciute, prima che siano in grado di causare danni.

Sempre più attacchi ransomware utilizzano malware creati su misura. Per difendersi da questo tipo di insidie, è necessario essere in grado di rilevare e bloccare le nuove minacce. Sfruttando sandbox native del cloud e il rilevamento basato sull'intelligenza artificiale, è possibile utilizzare l'analisi comportamentale per individuare varianti di ransomware precedentemente sconosciute, mettere in quarantena i file e analizzarli approfonditamente prima che vengano consegnati agli utenti o che ne venga autorizzata l'esecuzione.

Con una soluzione come Zscaler Cloud Sandbox, puoi definire le policy in base agli utenti, ai gruppi e ai tipi di contenuti, e avrai un controllo granulare delle azioni sui file in quarantena. Poiché questa soluzione fa parte di Zero Trust Exchange™ di Zscaler, puoi ricevere valutazioni sui file praticamente in tempo reale, grazie alle informazioni provenienti dalla community globale, e ridurre al minimo l'impatto sull'utente, massimizzando al contempo l'accuratezza del rilevamento dei malware.

N°4

Lo zero trust semplifica le policy per il controllo degli accessi, nonché migliora la visibilità e l'efficacia.

La microsegmentazione è un aspetto fondamentale dello zero trust, e implica la limitazione dell'accesso alle applicazioni e alle risorse, in modo che gli aggressori che riescono a perpetrare una violazione non possano causare danni alle altre entità. Nell'approccio legacy alla microsegmentazione basato sulla rete, i firewall applicavano le regole esaminando gli indirizzi di rete. Questo approccio richiedeva la ridefinizione e l'aggiornamento delle policy con lo spostamento e l'evoluzione delle reti. Si trattava di un'operazione già abbastanza complessa per un data center on-premise, che con il cloud si è fatta ancora più complicata, fino a diventare impossibile da gestire.

Le architetture proxy riducono significativamente la complessità dell'implementazione della microsegmentazione, e forniscono al contempo una protezione più solida per i workload. Dato che le policy e le autorizzazioni sono gestite in base alle identità delle risorse, esse sono indipendenti dall'infrastruttura di rete sottostante e sono in grado di adattarsi automaticamente alla dinamicità dell'architettura di rete o alla rapidità con cui cambiano i requisiti aziendali. In questo modo la gestione si fa anche più semplice, perché è possibile proteggere un segmento con poche policy basate sull'identità anziché centinaia di regole basate sull'indirizzo.

N.5

Un'architettura zero trust protegge utenti e dispositivi ovunque si trovino.

Quando la pandemia di COVID–19 ha reso la possibilità di lavorare da remoto determinante per le aziende di tutti i settori, in molte hanno fatto ricorso alle reti private virtuali (VPN) o al protocollo RDP per consentire ai dipendenti di connettersi alle reti e alle risorse aziendali a distanza. Purtroppo, gli utenti malevoli si sono adattati al cambiamento di queste organizzazioni, e hanno lanciato una nuova ondata di attacchi basati su RDP e VPN. Il famigerato attacco a Colonial Pipeline, che ha bloccato totalmente il trasporto di quasi la metà della fornitura di carburante degli Stati Uniti orientali, è stato scagliato proprio sfruttando una VPN.

In un approccio basato sullo zero trust, per proteggere gli utenti in remoto, ogni connessione ottiene la stessa protezione, indipendentemente dalla posizione degli utenti. L'aggiunta di un agente endpoint leggero, Zscaler Client Connector, sul dispositivo di ogni utente in remoto, offre l'accesso a tutta la sicurezza, all'applicazione delle policy e ai controlli dell'accesso disponibili con Zero Trust Exchange di Zscaler. Inoltre, poiché Zscaler è una soluzione distribuita su 150 data center in tutto il mondo, gli utenti godono sempre di una connessione veloce attraverso un data center nelle vicinanze, evitando così la latenza della VPN.

N.6

Una vera architettura zero trust rende impossibile agli aggressori spostarsi lateralmente sulla rete.

Troppi team di sicurezza continuano a fare affidamento sulla segmentazione della rete basata su firewall legacy per mantenere il traffico dannoso fuori dalle reti aziendali. Queste strategie non solo sono complesse da distribuire e da gestire, ma lasciano comunque esposte le risorse interne. Se gli aggressori riescono a violare un'applicazione o un firewall, hanno comunque la possibilità di spostarsi lateralmente all'interno dell'ambiente e di criptare e rubare molti più dati.

Un vero approccio zero trust collega gli utenti direttamente alle applicazioni di cui hanno bisogno mediante un segmento 1:1, senza mai esporre la rete. I team addetti alla sicurezza possono utilizzare un'architettura proxy per autenticare continuamente gli utenti e collegarli direttamente alle applicazioni anziché fidarsi del traffico proveniente da una rete interna o da una sottorete, eliminando così il rischio digitale più grande che le aziende odierne si trovano a dover affrontare. Inoltre, un proxy funziona indipendentemente dalla posizione di utenti, dispositivi o applicazioni, e questo offre una connettività sicura, sia on-premise che da remoto.

N.7

Un'architettura zero trust impedisce agli aggressori di sfruttare i workload.

In un'architettura zero trust, le policy di sicurezza vengono applicate in base all'identità dei workload che tentano di comunicare tra loro. Tali identità vengono controllate costantemente, e i workload non verificati non possono comunicare con gli altri. Questo significa che non possono interagire con i server di comando e controllo remoti dannosi o con host, utenti, applicazioni e dati interni.

Una piattaforma come Zero Trust Exchange di Zscaler assicura automaticamente che, quando viene effettuato l'accesso alle risorse, tutto il traffico, indipendentemente dalla sua origine, aderisca a tutte le policy aziendali. Inoltre, applica le policy in modo completamente uniforme, siano le risorse in questione interne, esterne o SaaS terzi. Si tratta di un approccio alla microsegmentazione della rete molto più semplice ed efficace rispetto all'applicazione di policy multilivello.

N.8

Lo zero trust include strategie proattive per sconfiggere gli avversari sfruttando il loro stesso gioco.

I ransomware di oggi sono gestiti da avversari sofisticati, in grado di aggirare le misure di prevenzione iniziali. Un aspetto importante dello zero trust è quindi quello di utilizzare strategie per individuare e isolare gli attacchi prima che possano causare dei danni. L'unica piattaforma zero trust al mondo che integra funzionalità di deception, Zscaler Deception™ utilizza tattiche di inganno avanzate per attirare, rilevare e intercettare gli aggressori, indipendentemente da quanto siano avanzate o mirate le loro strategie.

Questo approccio proattivo alla difesa comporta la distribuzione di esce nell'ambiente IT, quali endpoint, directory, database, file e percorsi utente fittizi. Tali esce imitano le risorse di produzione ad alto valore, ma rimangono nascoste agli utenti reali. Il loro unico scopo è quello di avvisare il team di sicurezza della presenza di un aggressore, quando vengono toccate. Dato che il traffico legittimo non può mai raggiungere le esche, gli avvisi sono pertanto ad alta attendibilità, il che offre prove concrete di una minaccia o di una violazione che hanno un'affidabilità di gran lunga superiore rispetto a quella degli avvisi ottenuti attraverso altri sistemi di rilevamento. Questo costituisce un vantaggio per il team di sicurezza, consentendogli di interrompere i tentativi di attacco degli aggressori e mitigare i danni.

N.9

Le architetture zero trust offrono una protezione completa contro la perdita dei dati.

La crescente prevalenza delle strategie di attacco ransomware a doppia estorsione ha reso necessario considerare ogni attacco ransomware come una violazione dei dati. Le misure che impediscono l'esfiltrazione e la pubblicazione dei dati sensibili sono estremamente importanti, quando si tratta di mitigare le conseguenze più devastanti di un attacco ransomware.

L'utilizzo di una soluzione CASB (Cloud Access Security Broker) ti consente di applicare controlli granulari sulle applicazioni cloud, proteggendo i dati inattivi all'interno delle piattaforme SaaS e prevenendo la condivisione eccessiva accidentale e le attività dannose. Potrai anche godere di una maggiore visibilità sulle applicazioni cloud, e sarà più semplice identificare le vulnerabilità, gli errori di configurazione e lo shadow IT, ovvero l'uso di app cloud non autorizzate. Grazie alle funzionalità di prevenzione della perdita di dati (DLP, Data Loss Prevention), è possibile bloccare automaticamente l'esfiltrazione dei dati, riducendo quindi le minacce associate alle tecniche di doppia estorsione.

N.10

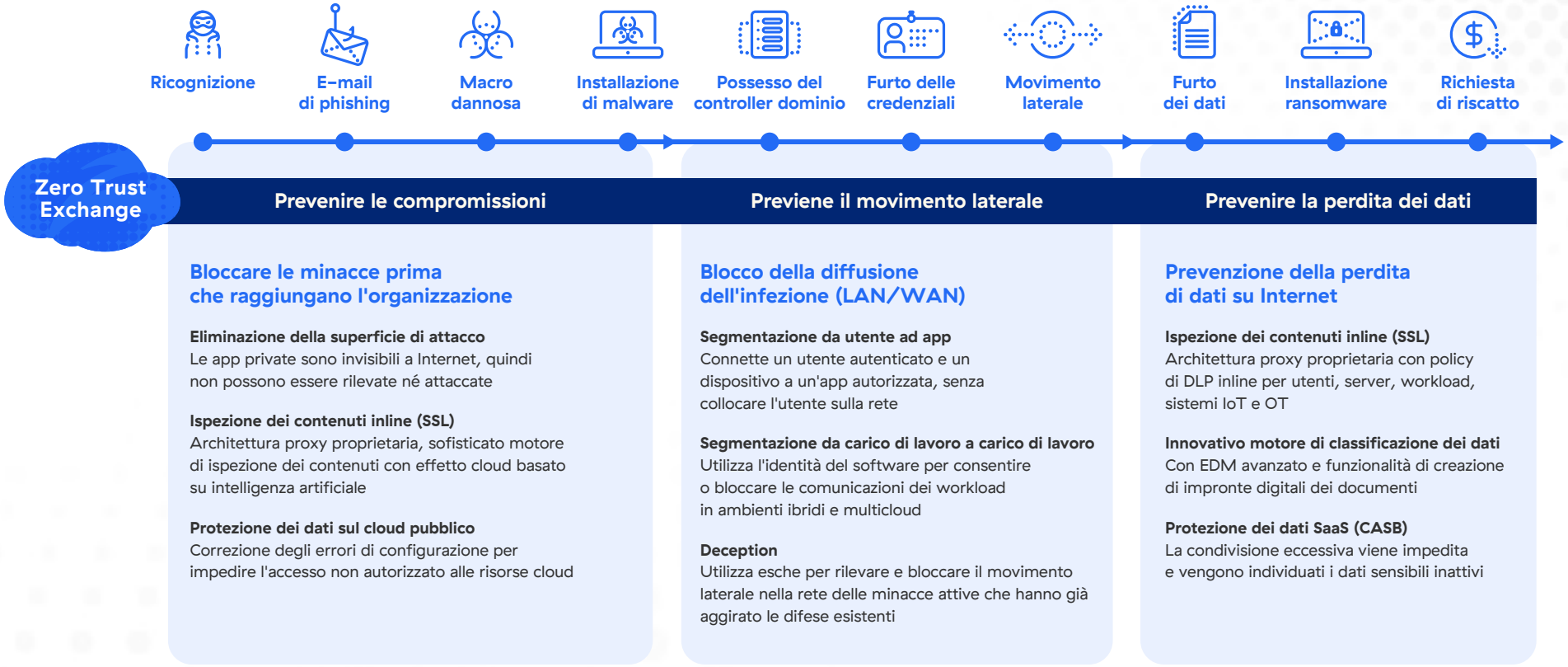
Con l'ispezione completa inline di tutto il traffico in uscita, un'architettura zero trust ti permette di bloccare completamente il furto dei dati.

Se gli attori malevoli nascondono malware nel traffico criptato con SSL in entrata, possono utilizzare la medesima strategia, ossia sfruttare la crittografia per nascondere l'esfiltrazione dei dati aziendali sensibili e di valore. Essere in grado di ispezionare il traffico criptato con SSL è fondamentale per prevenire la perdita dei dati e identificare le vulnerabilità O-day correlate all'esfiltrazione dei dati.

Una soluzione con un'architettura basata sullo zero trust, come Zscaler Zero Trust Exchange, assicura che ogni connessione nel proprio ambiente venga verificata e sia protetta individualmente, indipendentemente dal fatto che sia in entrata o in uscita. Con un'architettura proxy nata sul cloud, è possibile eseguire l'ispezioni SSL su larga scala, senza influire sulle prestazioni o incorrere a costi eccessivi. Ciò consente di eliminare le lacune della sicurezza che gli operatori di ransomware hanno finora sfruttato per lanciare devastanti attacchi a doppia estorsione.

Implementare lo zero trust per proteggersi dai ransomware

Zero Trust Exchange di Zscaler offre la difesa più completa contro l'intera sequenza di azioni che gli aggressori devono intraprendere per avere successo.
Scopri in che modo Zscaler impiega lo zero trust per offrire alle aziende una protezione senza precedenti.



Per fermare gli attacchi moderni è necessaria una sicurezza moderna.

Proteggi la tua azienda con la difesa contro i ransomware più completa del settore.

Per saperne di più

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata sull'SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it