arcserve®

Non ridurti a una statistica:

Stai un passo avanti ai criminali informatici implementando una strategia olistica di protezione dal ransomware

Negli attuali ambienti aziendali, sempre operativi e ossessionati dai dati, le minacce informatiche sono la priorità principale per i team di sicurezza IT.

Il ransomware, in particolare, sta causando all'IT parecchie notti insonni: la frequenza degli attacchi è in aumento e le più recenti sollecitazioni e tattiche diventano sempre più mirate, distruttive e difficili da rilevare rapidamente.

Ad esempio, dal 2019 sono stati almeno 440 gli attacchi ransomware mirati contro i settori delle infrastrutture critiche, tra cui sanità, servizi finanziari, governo e istruzione. E, nel 2020, COVID-19 ha dato il via a un proliferare di frodi di phishing e attacchi ransomware a tema pandemico che hanno approfittato di dipendenti distratti, alla ricerca di risposte e rassicurazioni in un periodo molto incerto.

Il ransomware continua a evolversi, con nuove tattiche e tecnologie che emergono regolarmente, come:

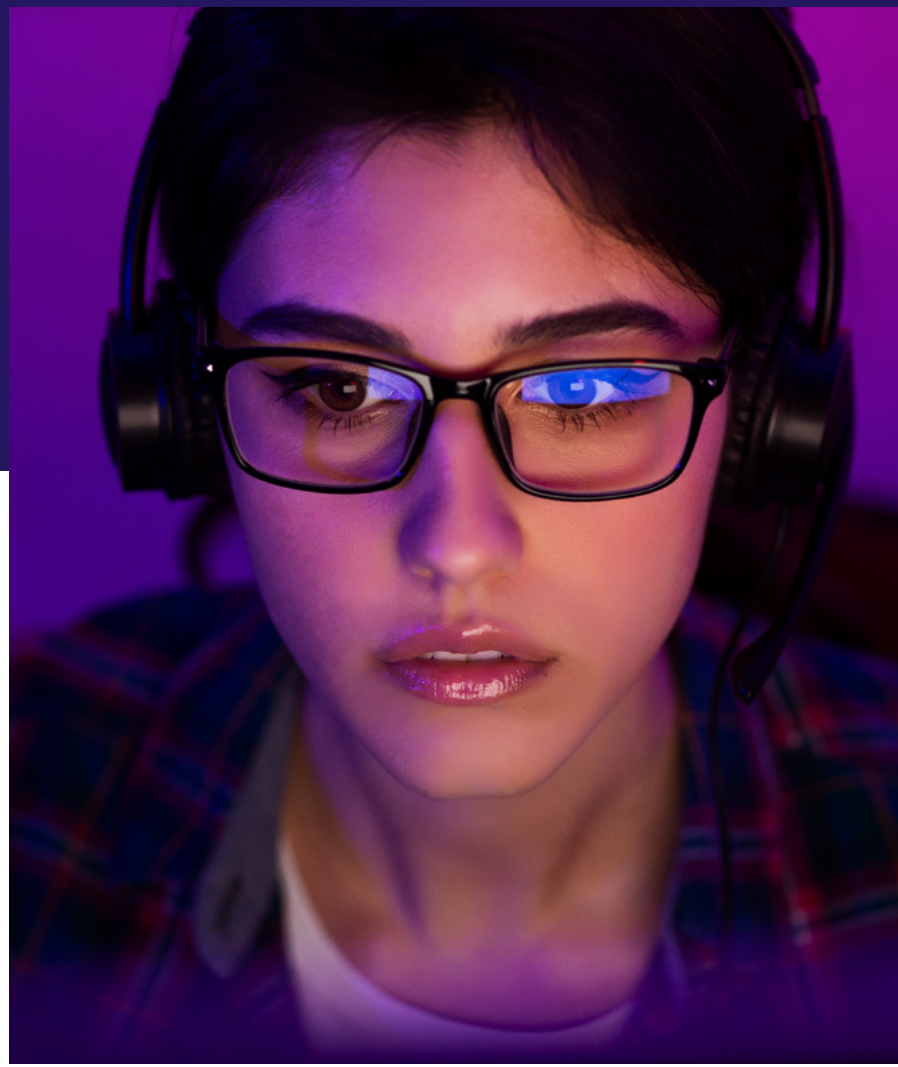
Doppia estorsione
Gli operatori ransomware non solo criptano i dati, ma li pubblicano anche su internet.

Crittografia ritardata
Il ransomware rimane inattivo per un periodo di tempo prima di crittografare i dati, in attesa dei backup.

Targeting del backup
Alcuni ceppi di ransomware cercano i file di backup e li criptano, rendendo il disaster recovery un incubo.

In che modo gli attuali ambienti IT favoriscono il ransomware

La natura e la progettazione dei moderni ambienti IT hanno creato un ecosistema con molte parti in movimento e sistemi diversi.



Questo tipo di struttura amplia invariabilmente la superficie di attacco di un'organizzazione, rendendo più difficile la difesa dal ransomware. Alcune delle vulnerabilità maggiormente sfruttate derivano da poche fonti comuni.

Livelli elevati di complessità

Le attuali infrastrutture IT sono notoriamente complesse. Molte organizzazioni faticano a supportare e proteggere una vasta gamma di piattaforme e applicazioni. I team IT spesso si trovano a destreggiarsi in una varietà di elementi dell'infrastruttura, tra cui:

- Infrastrutture in locale e su cloud pubblici/privati/ibridi
- Computer e dispositivi mobili
- Soluzioni come SaaS (Software as a Service), PaaS (Platform as a Service) e IaaS (Infrastructure as a Service)
- E molto altro ancora

Rischi legati a fornitori terzi

Nella ricerca di una terza parte con cui collaborare, è essenziale accertarsi che la sicurezza informatica venga presa sul serio. Tutti i punti di accesso, le reti e i database condivisi diventano punti deboli per gli operatori ransomware, pertanto la due diligence e una valutazione della sicurezza di terze parti sono fondamentali.

Team distribuiti

COVID-19 ha reso quasi tutti i team distribuiti, ma con poco tempo per prepararsi alla transizione, le organizzazioni si sono dovute accontentare di mettere insieme un'infrastruttura di supporto e sicurezza "abbastanza buona". In molti casi non è stata nemmeno "abbastanza buona", rendendo i lavoratori remoti obiettivi perfetti per i malintenzionati.

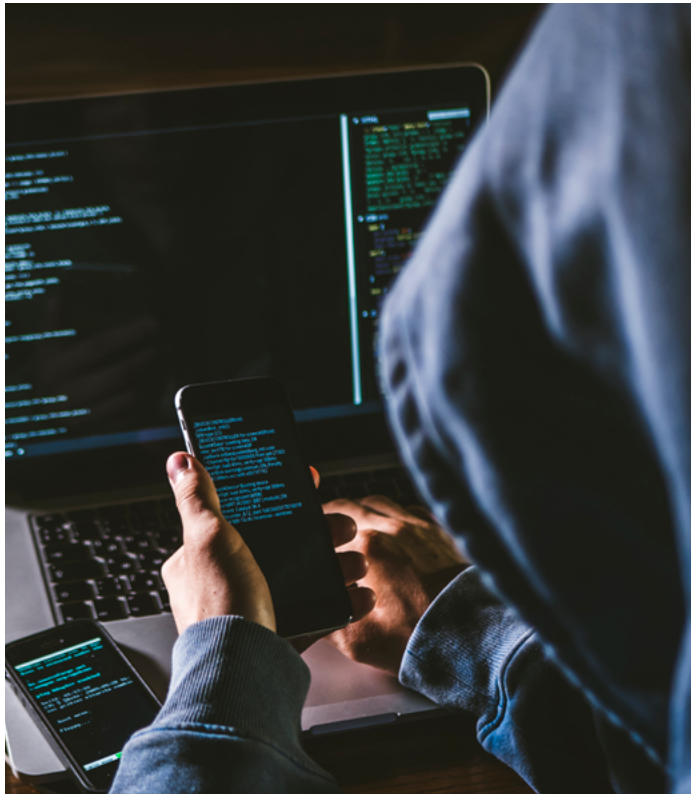
Patch e aggiornamenti mancanti

Le patch e gli aggiornamenti di sicurezza sono lunghi e noiosi. Sono anche due dei modi migliori per prevenire il ransomware. Gli studi dimostrano che una violazione della sicurezza su tre avrebbe potuto essere evitata se le patch fossero state aggiornate. La realtà è che viene rilasciato un flusso infinito di patch e molti team IT sono troppo sottodimensionati per stare al passo.

Sistemi legacy

I sistemi e i software legacy costituiscono un chiaro invito agli operatori ransomware. I sistemi più vecchi non si integrano bene con le nuove soluzioni di sicurezza informatica e, di conseguenza, non sono adeguatamente protetti.

COVID-19 ha reso quasi tutti i team distribuiti, ma con poco tempo per prepararsi alla transizione, le organizzazioni si sono dovute accontentare di mettere insieme un'infrastruttura di supporto e sicurezza "abbastanza buona".



Costi diretti e indiretti del ransomware

L'impatto di un attacco ransomware riuscito varia notevolmente da un'organizzazione all'altra, a seconda del settore, del livello di rischio e della gravità dell'attacco. Tuttavia, tutte le imprese devono ricordare una verità universale: Il danno da ransomware va ben oltre l'attacco iniziale.

Gli impatti più evidenti e immediati del ransomware sono numerosi, tra cui:

- tempi di inattività e perdita di produttività a causa della crittografia dei dati
- perdita di ricavi a causa dell'inevitabile downtime
- possibilità di perdita di dati se i backup sono incompleti o non protetti
- costi diretti per gli sforzi di pulizia e i pagamenti di riscatto, se si sceglie di seguire questa strada (cosa che non consigliamo)

Tuttavia, ci sono diverse conseguenze meno tangibili, ma altrettanto dannose e a lungo termine di cui essere consapevoli. Ad esempio, è difficile quantificare i danni arrecati alla reputazione dell'azienda. Le violazioni della sicurezza influiscono sulla fiducia dei clienti e degli stakeholder, pertanto si potrebbe notare un calo dei nuovi clienti, il passaggio improvviso dei clienti attuali a un nuovo fornitore di soluzioni o la perdita del vantaggio competitivo sul mercato.

A seconda del settore e della gravità della violazione, l'organizzazione potrebbe anche trovarsi a gestire mancanze di conformità e conseguenze normative o a essere invischiata in procedure di contenzioso e restituzione che comportano multe e sanzioni significative.

Le violazioni della sicurezza influiscono sulla fiducia dei clienti e degli stakeholder, pertanto si potrebbe notare un calo dei nuovi clienti, il passaggio improvviso dei clienti attuali a un nuovo fornitore di soluzioni o la perdita del vantaggio competitivo sul mercato.

Approccio olistico alla protezione ransomware

Di fronte a nuovi tipi di minacce ransomware, molte organizzazioni trovano che le vecchie strategie di sicurezza e difesa non siano più sufficienti. Per combattere il ransomware, invece, i team di sicurezza IT stanno scegliendo soluzioni olistiche e proattive .

Adottare un approccio olistico alla protezione ransomware è come mettere un campo di forza intorno all'organizzazione. Questo tipo di soluzione incorpora una strategia di sicurezza completa che blocca l'accesso e riduce al minimo i danni all'infrastruttura IT, adottando misure sia offensive che difensive.

La protezione completa contro il ransomware comporta una combinazione dei seguenti elementi:

- **strumenti e tecnologie per la sicurezza informatica**
- **funzionalità di ripristino orchestrate**
- **piani realistici per la gestione di persone, policy e processi**

Strumenti e tecnologie per la sicurezza informatica

La protezione dell'infrastruttura multigenerazionale e dei dati business-critical è un obiettivo primario per i team di sicurezza IT. Come parte di una strategia olistica di protezione ransomware, la sicurezza informatica comprende tutto, dalla protezione degli endpoint e dei firewall, alla gestione delle identità e degli accessi e alla prevenzione della perdita di dati.

Per affrontare le attuali sfide del ransomware, una soluzione affidabile per la sicurezza informatica deve disporre di tecnologie di rilevamento e prevenzione, tra cui:

- rilevamento di malware basato su firma e senza firma
- una rete neurale di apprendimento profondo
- tecnologia anti-exploit, come Sophos Intercept X Advanced

Funzionalità di ripristino orchestrate

In un mondo ideale, il 100% del ransomware si potrebbe prevenire il 100% delle volte. Nella realtà, a un certo punto un'organizzazione ha buone probabilità di essere colpita. Il ripristino rapido dopo una crisi dipende dal livello di preparazione e dalle capacità di orchestrazione, che dovrebbero essere affrontate all'interno della strategia di protezione olistica.

Le organizzazioni altamente resilienti dispongono di un piano di disaster recovery (DR) testato e pronto per essere eseguito molto prima del necessario. Uno dei componenti principali di un solido piano di DR è un backup sicuro, completo e aggiornato, ma questo da solo non è sufficiente.

Il piano di ripristino deve assolutamente includere il backup su cloud, ma è anche necessario includere la protezione contro nuovi ceppi ransomware che cercano proprio i file di backup. La tradizionale strategia di backup 3-2-1 non è più valida. Per garantire funzionalità di ripristino complete, è ora necessario includere backup con air-gap, in modo da pianificare una strategia 3-2-1-1.

Poiché un numero sempre maggiore di organizzazioni supporta i lavoratori remoti utilizzando soluzioni basate su cloud come Microsoft Office 365, è fondamentale disporre di un piano per proteggere le applicazioni SaaS dalla perdita di dati. Molte soluzioni SaaS utilizzano un modello di responsabilità condivisa, il che significa che se non si esegue il backup dei dati, si potrebbero avere guai.

Azioni per persone, politiche e processi

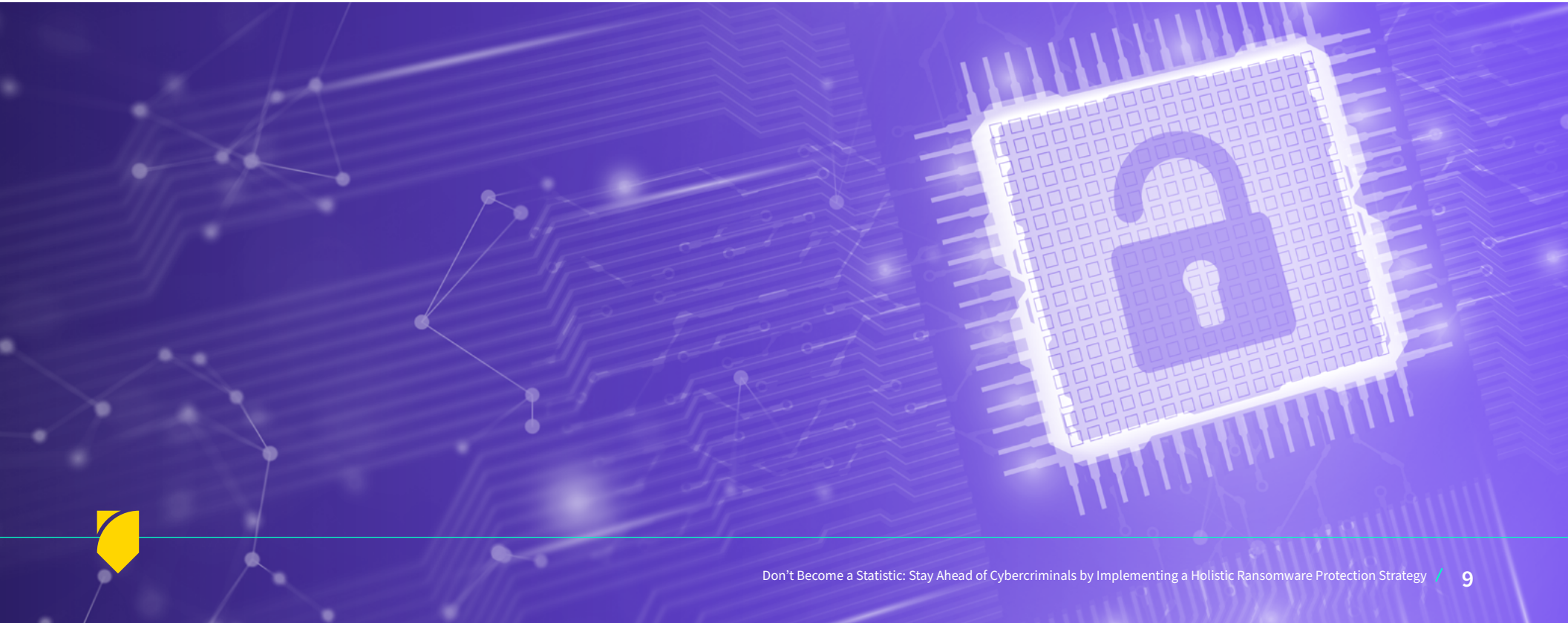
Gli esseri umani sono generalmente l'anello debole della catena di protezione dal ransomware. E se fosse possibile rendere tutti i dipendenti un'estensione dell'IT, in modo che diventino la prima linea di difesa dell'organizzazione?

La formazione è il primo passo per ridurre l'errore umano. Alcune delle aree principali su cui concentrarsi sono:

- esercitazioni sul disaster recovery dei datis
- formazione sulla sicurezza informatica, in modo che i dipendenti sappiano a cosa devono prestare attenzione
- formazione sulla consapevolezza della sicurezza, che insegna cosa fare (o non fare) per prevenire violazioni e infezioni da malware

Altri modi per ridurre al minimo la possibilità di errore umano nelle minacce ransomware consistono nell'implementazione di policy di accesso sicuro, come l'autenticazione a più fattori e la due diligence, con controlli in background dei dipendenti, valutazione dei rischi di terze parti e la buona, vecchia sicurezza fisica.

Gli esseri umani sono generalmente l'anello debole della catena di protezione dal ransomware.



Un futuro senza ransomware con il partner giusto

Dopo aver elaborato una strategia olistica di protezione dal ransomware, è importante collaborare all'implementazione con un fornitore di soluzioni con esperienza specifica nel settore.

Anche considerata l'esperienza, si deve trovare qualcuno che condivida i valori dell'azienda e ne comprenda l'attività.

Quando si trova un partner con cui parlare la stessa lingua e condividere gli stessi obiettivi, è molto più facile lavorare in team per il successo aziendale. Il fornitore di soluzioni giusto è fondamentale per l'implementazione una strategia olistica di protezione ransomware, perché aiuta a individuare i componenti chiave di un solido piano di sicurezza dei sistemi e dei dati.

Quando si trova un partner con cui parlare la stessa lingua e condividere gli stessi obiettivi, è molto più facile lavorare in team per il successo aziendale.

Integrazione e sicurezza

L'integrazione di sicurezza informatica e protezione dei dati è l'unico modo per proteggersi veramente dal ransomware. Se la strategia di protezione ransomware include le forze combinate di soluzioni come Sophos Intercept X, Nutanix HCI and Arcserve Unified Data Protection è possibile:

- ridurre la complessità dell'infrastruttura
- migliorare gli SLA (Service Level Agreement)
- integrare perfettamente la protezione dei dati e dell'infrastruttura, che siano carichi di lavoro in locale, cloud, HCI (Hyperconverged Infrastructure) e basati su SaaS

Backup e ripristino

Non si esagera mai enfatizzando l'importanza di un backup sicuro, testato e aggiornato per il ripristino dopo un attacco ransomware o altre interruzioni non pianificate. Il partner giusto può aiutare l'organizzazione a trovare le soluzioni di backup e ripristino più adatte alle attuali esigenze aziendali di storage e protezione dei dati e ad adattarle alle esigenze di scalabilità necessarie per garantire una strategia di sicurezza a prova di futuro,

Protezione dei dati basata su abbonamento

Il partner giusto è quello che sa mantenere il fine e gli obiettivi dell'azienda al centro di ogni transazione. Ciò è particolarmente vero quando si tratta di preventivare una soluzione di protezione ransomware.

Quando si collabora con un fornitore di soluzioni che offre licenze universali, si può essere sicuri che tutti i dati sono protetti e si sa esattamente per che cosa si sta pagando. Non ci sono costi nascosti e si paga solo per ciò di cui si ha bisogno, in modo da essere liberi di scalare verso l'alto o il basso, secondo necessità.

Difendere, evolvere e adattarsi

Il ransomware e altre minacce informatiche sono destinati a restare, quindi la nostra unica possibilità è quella di imparare a difendere sistemi, applicazioni e dati.

Le minacce sono sempre in evoluzione e in costante adattamento, il che significa che dobbiamo saper evolvere e adattare anche le nostre strategie di sicurezza.

La sicurezza completa dei dati inizia con un approccio gestito per proteggere le infrastrutture IT e i dati di backup dagli attacchi informatici, ma non finisce qui.

Il percorso verso un futuro privo di ransomware deve includere la tecnologia di sicurezza informatica, il backup e il ripristino orchestrati, e politiche, processi e formazione completi, per gestire il lato umano della prevenzione ransomware. I team di sicurezza IT devono affrontare in modo proattivo e continuo le minacce ransomware con una strategia di protezione olistica in grado di evolversi insieme al panorama delle minacce.

Il percorso verso un futuro privo di ransomware deve includere la tecnologia di sicurezza informatica, il backup e il ripristino orchestrati, e politiche, processi e formazione completi, per gestire il lato umano della prevenzione ransomware.

arcserve®

Per scoprire come Arcserve può aiutarti a stare al passo con i criminali informatici, contattaci di seguito.

PER SAPERNE DI PIÙ