arcserve®

Protect what's priceless.

LA TUA GUIDA PER UN FUTURO SENZA RANSOMWARE

UN APPROCCIO PROATTIVO

PER AFFRONTARE

LA MINACCIA RANSOMWARE

WHITE PAPER

IL RANSOMWARE È DIVENTATO UNO DEI PRINCIPALI FATTORI DI RISCHIO PER LE AZIENDE E COSTITUISCE LA MINACCIA PIÙ PREOCCUPANTE.

Il ransomware è diventato uno dei maggiori rischi aziendali e costituisce la minaccia più seria per le organizzazioni IT. A livello globale ha raggiunto proporzioni epidemiche e si prevede che i costi relativi raggiungeranno i 20 miliardi di dollari entro il 2021.1

Tuttavia, per i professionisti IT e i responsabili aziendali questa non è necessariamente una notizia disastrosa. Anche se i malintenzionati non danno segni di stanchezza, i progressi nelle tecnologie per la lotta alla criminalità informatica e la prevenzione dei disastri, uniti a solide pratiche di gestione IT, aiutano le organizzazioni a reagire.

Questo documento approfondisce l'evoluzione della minaccia ransomware, le tecnologie innovative utilizzate per la difesa e fornisce un approccio lungimirante verso un futuro senza ransomware.

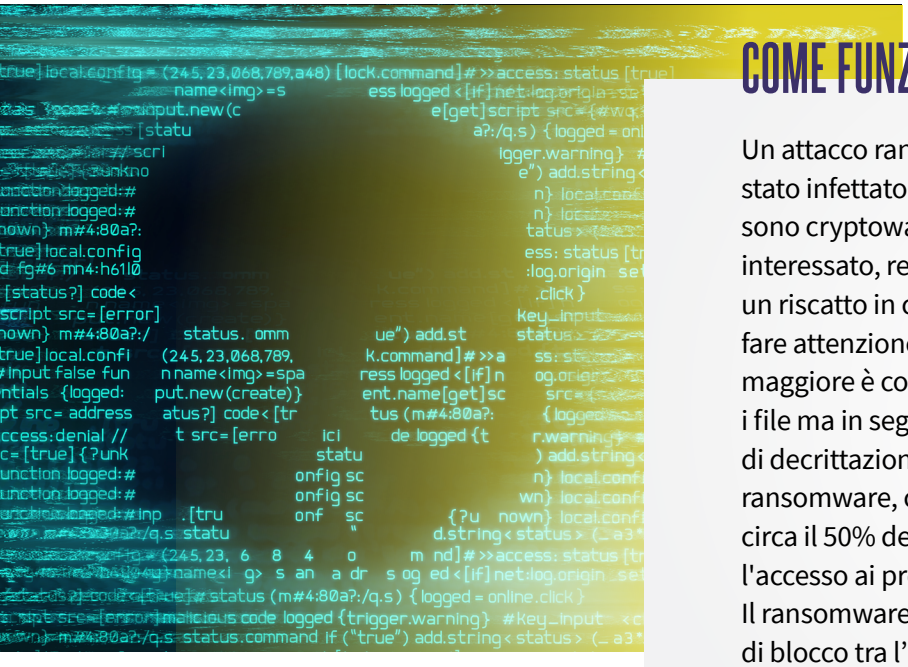
CONOSCI IL NEMICO

Un saggio consiglio dello stratega militare cinese Sun Tzu recita: "Conosci il tuo nemico". Per sviluppare una strategia utile a proteggere i sistemi IT dal ransomware, è necessario conoscerlo. Iniziamo quindi a capire in cosa consiste questo tipo di virus.

I dati sono la linfa vitale di un'azienda. Costituiscono le attività che procedono da una business unit all'altra. Tengono traccia del passato, comunicano lo stato attuale del business e guidano le decisioni. Senza di essi, non è un'esagerazione dire che non ci sono affari. E questa è l'idea su cui il ransomware capitalizza.

Il ransomware è un software dannoso progettato per impedire l'accesso ai sistemi o ai dati del computer fino al pagamento del riscatto. Può bloccare all'improvviso le attività o, se si tratta anche di leakware o extortionware, può fare un passo ulteriore e minacciare di far trapelare ed esporre dati privati.

Ogni organizzazione con dati importanti archiviati su computer o reti è a rischio, e questo oggigiorno riguarda praticamente ogni azienda. I governi statali e locali, le forze dell'ordine, le organizzazioni sanitarie, le banche e le società di carte di credito sono tutti obiettivi importanti e l'industria del furto di identità alimenta il mercato: nel 2018 sono stati segnalati dai consumatori danni per 14,7 miliardi di dollari.2 Obiettivo dei criminali non sono solo le grandi aziende: gli attacchi di ransomware si verificano ai danni di consumatori e imprese, di qualunque dimensione.



COME FUNZIONA IL RANSOMWARE?

Un attacco ransomware si verifica quando un computer è stato infettato da un virus. La maggior parte dei ransomware sono cryptoware e crittografano i file sul computer interessato, rendendoli inaccessibili fino al pagamento di un riscatto in cambio della chiave per decrittarli. Ma si deve fare attenzione a ciò per cui si paga. Un pericolo ancora maggiore è costituito da falsi cryptoware, che crittografano i file ma in seguito al riscatto non forniscono una chiave di decrittazione funzionante. Le vittime di questo tipo di ransomware, che, secondo alcune stime, rappresentano circa il 50% dei casi, potrebbero non riguadagnare l'accesso ai propri file, anche dopo aver pagato il riscatto. Il ransomware non crittografante inserisce una schermata di blocco tra l'utente e i suoi dati, senza crittografarli direttamente.

Il ransomware può attaccare file specifici o l'intero sistema attraverso il Master Boot Record (MBR) di un'unità o l'NTFS di Microsoft, impedendo così l'avvio del sistema operativo. Questo virus spesso non viene rilevato perché utilizza una rete con traffico crittografato HTTPS o Tor. A differenza di altri tipi di malware che possono operare in background, una volta che il ransomware si è infiltrato nello sfortunato host, renderà nota la sua presenza con la richiesta di criptovalute non rintracciabili per il riscatto.

È sufficiente una piccola azione involontaria da parte di un utente innocente, ad esempio un clic su un collegamento dannoso, affinché un computer venga infettato. Il ransomware si diffonde in genere tramite e-mail di phishing, ma i criminali informatici utilizzano numerose tecniche per colpire le proprie vittime. L'infezione si verifica in genere dopo l'apertura di un allegato e-mail o facendo clic su un collegamento ingannevole. I vettori comuni utilizzati per diffondere malware includono:

- **E-mail e messaggi di testo** contenenti collegamenti che scaricheranno malware o un allegato contenente malware
- **Siti web** il cui unico scopo è attirare gli utenti e indurli a fare clic su un link dannoso o su un download
- **Malvertising** o pubblicità dannose che sono essenzialmente trucchi per indurre a fare clic che comportano download non intenzionali
- **Social media** che possono sembrare collegati a fonti attendibili, ma portano rapidamente a un criminale informatico malintenzionato. Le vittime inconsapevoli sono colpite dal virus direttamente all'interno di un'applicazione di social media o possono essere attratte da un link o annuncio dannoso.
- **App mobili che** gli utenti scaricano volontariamente sul proprio dispositivo, senza rendersi conto che in realtà sono false e progettate per trasferire un virus alla successiva connessione del dispositivo mobile a un computer.

Gli hacker stanno diventando più sofisticati e prendono di mira gli utenti inviando allegati infetti tramite un'e-mail che sembra provenire da qualcuno nel loro elenco di contatti. Anche se le politiche di utilizzo e la formazione sono utili per ridurre il comportamento rischioso da parte degli utenti finali, è impossibile eliminare completamente questa vulnerabilità poiché i punti di ingresso potrebbero non essere sempre così ovvi. I contenuti dannosi possono sfruttare le vulnerabilità di browser o plug-in ed eseguire codice nocivo all'insaputa dell'utente. Una volta stabilita su un host, un'infezione può diffondersi facilmente su altri computer sulla stessa rete.

Oltre a indurre gli utenti a scaricare inconsapevolmente ransomware, i criminali informatici ottengono tramite Internet l'accesso ai sistemi incustoditi. I malintenzionati usano sia metodi di forza bruta sia credenziali acquistate sul dark web per ottenere accesso a risorse e dati, sfruttando il Remote Desktop Protocol e le vulnerabilità del software

Un resoconto del 2019 ha rivelato che tra le imprese e le organizzazioni governative, gli obiettivi più comuni per il ransomware sono risorse di alto valore come server, infrastruttura applicativa e strumenti di collaborazione. Le organizzazioni IT possono giustamente dare priorità alle vulnerabilità più comuni e più critiche, ma non si possono permettere di ignorare quelle meno recenti o meno critiche. Nel resoconto, le vulnerabilità più vecchie (di tre anni o più) rappresentavano più di un terzo degli attacchi, più della metà dei quali sfruttava le vulnerabilità meno critiche.[3]

RANSOMWARE ATTACKS ON AVERAGE CAUSE NEARLY 10 DAYS OF DOWNTIME.[4]

Quali sono gli effetti di un'infezione da ransomware?

I notiziari riportano di continuo storie di attacchi ransomware e un esplodere di statistiche inquietanti ha già spinto le aziende a prenderne atto e a cercare soluzioni di sicurezza o protezione dei dati realmente efficaci. L'effetto immediato di un attacco ransomware è una grave interruzione delle attività aziendali, con dispositivi e sistemi che vengono messi offline per la disinfezione, nella speranza che una strategia di backup e disaster recovery ben pianificata renda possibile il ripristino di dati puliti senza perdite. Gli attacchi di ransomware causano in media 10 giorni di inattività.[4]

L'FBI raccomanda di non pagare il riscatto e riferisce che nel 2018 sono stati pagati oltre 2,57 milioni di dollari.[5] In generale, un'azienda può aspettarsi un costo medio di 133.000 dollari per attacco, solo per riguadagnare l'accesso ai propri dati.6 Purtroppo, alcune vittime pagano senza alcuna garanzia che recupereranno le loro informazioni. Gli studi rivelano che gli autori di ransomware guadagnano generalmente più del doppio dello stipendio medio degli sviluppatori che lavorano su progetti legittimi.7 È evidente che il vantaggio per gli aggressori è a danno delle organizzazioni e del personale IT professionale.

2,57$ MILIONI DI RISCATTO PAGATI[5]

133.000$ COSTO MEDIO PER ATTACCO[6]

Le aziende sperano ardentemente che le loro difese anti-ransomware funzionino. Ma anche prevenendo il peggio, pur solo in parte, potrebbero comunque trovarsi di fronte a una perdita di dati conseguente all'aggressione. In media un attacco informatico causa la perdita di circa l'8% dei dati.8 Oltre a tentare di ottenere un riscatto, gli aggressori possono estrarre dati da un computer o un server compromesso, esponendo informazioni sensibili, inclusi nomi utente e password, dati di pagamento e indirizzi e-mail dei contatti. Il ransomware moderno aggredisce i file di backup sulle condivisioni di rete e può persino eliminare le copie shadow sulla workstation per impedirne il ripristino. L'attacco e la conseguente perdita di dati sono un potente colpo e i rischi a lungo termine per la reputazione del marchio possono avere un impatto devastante, che compromette gravemente la credibilità.

> *"I criminali informatici stanno diventando sempre più sofisticati nelle loro tattiche e sembra che nessun settore sia immune dagli attacchi di ransomware. Mirando ai sistemi di backup, gli hacker aumentano le probabilità che le organizzazioni compromesse paghino il riscatto, dato che le gravi conseguenze della perdita di dati e dei tempi di inattività spesso vanno ben oltre le ripercussioni finanziarie. I responsabili di IT e le aziende devono inoltre considerare l'impatto negativo sulla produttività dei dipendenti, sulla fiducia dei clienti, sulla reputazione del marchio e sulla conformità normativa in caso sistemi e dati siano compromessi."*
>
> *- Oussama El-Hilali, Chief Technology Officer di Arcserve*

In che modo i professionisti IT proteggono le loro organizzazioni dal ransomware?

Esistono diversi modi di rilevare ransomware e proteggere sistemi e dati preziosi, tra cui:

- **Software per la protezione dal ransomware** che identifica potenziali attacchi ed è in grado di trovare e prevenire le intrusioni nel momento in cui si verificano.
- **Firewall** per bloccare l'accesso non autorizzato a un computer o una rete.
- **Filtri di file e antispam** che bloccano i siti web sospettati di malware e impediscono agli allegati indesiderati di arrivare alle caselle di posta elettronica dell'utente.
- **Policy di gruppo per il software** per impedire dalle cartelle locali l'esecuzione di file che potrebbero infettare il sistema.
- **Gestione delle informazioni sulla sicurezza e degli eventi** (SIEM) applicativi che forniscono informazioni sul traffico di rete per individuare anomalie che indicano una violazione.
- **Software di backup** per proteggere i dati aziendali effettuando una copia dei dati da server, database, desktop, laptop e altri dispositivi.
- **Monitoraggio dell'integrità dei file** per verificare la coerenza tra file correnti e validati.
- **Software antivirus e antimalware** per prevenire, rilevare e rimuovere malware.
- **Unified Threat Management (UTM)** soluzioni per affrontare varie minacce tramite console che gestisce un unico punto di difesa.

Anche se i metodi per rilevare il ransomware e proteggere sistemi e dati preziosi sono singolarmente importanti e utili, le organizzazioni sono sempre più a rischio. Gli aggressori di oggi diventano sempre più sofisticati e intraprendenti. Le strategie di attacco spesso combinano tecniche diverse nello stesso momento, mirando contemporaneamente a parti differenti della rete IT. Gli attacchi ransomware utilizzano nuove varianti di malware per aggirare i programmi antivirus. Quindi, quali sono le insidie delle tradizionali strategie di protezione dai ransomware?

Molti sistemi sono privi di funzionalità importanti

È stato più facile affrontare il problema del malware quando gli exploit potevano essere associati alla tecnologia antivirus basata sulla firma. Poiché le minacce si evolvono e includono attacchi precisi contro vulnerabilità diffuse, è diventato più difficile identificare i pericoli utilizzando la tecnologia basata sulla firma.

Inoltre, molti vendor di soluzioni per la protezione dati hanno approfittato del ransomware, sottolineando "funzionalità" per la sicurezza informatica che, in realtà, possono rilevare solo anomalie dei dati non necessariamente correlate al ransomware. E questi prodotti, dopo aver rilevato l'anomalia, spesso forniscono solo un avviso, anziché attivarsi per risolvere il problema

La difficoltà di gestione di strumenti separati aumenta la vulnerabilità

Molte aziende utilizzano più strumenti di diversi fornitori per disporre delle funzioni di sicurezza in grado di combattere il ransomware: ad esempio, possono utilizzare un vendor per il firewall, un altro per il filtro DLP o web, uno che fornisce backup e disaster recovery e uno ancora diverso per il backup su cloud, un altro per il data center e uno differente per il backup mobile.

L'uso di appliance separate e di diversi fornitori per le differenti funzioni di sicurezza rende più difficile identificare e prevenire gli attacchi. Strumenti e software richiedono gestione e aggiornamenti e, quando si mettono insieme diverse soluzioni, è ancora più difficile rimanere al passo con le ultime forme di malware. La gestione di più fornitori e soluzioni moltiplica i rischi, le vulnerabilità e gli errori. Ne soffre la produttività e i costi aumentano.

Oggi, si possono sostituire complessi strumenti legacy e soluzioni multi-vendor contro il ransomware con un'unica soluzione di difesa approfondita che garantisce backup e ripristino dei dati completi, rete neurale e protezione endpoint da malware, exploit e ransomware sconosciuti.

I professionisti del settore hanno anche bisogno di pratiche di gestione IT

Per la sicurezza informatica e la protezione dai ransomware sono fondamentali le soluzioni tecnologiche, inclusi firewall, sistemi di rilevamento e prevenzione delle intrusioni e sicurezza della posta elettronica. Le soluzioni avanzate per la sicurezza e la protezione dei dati integrate contribuiscono notevolmente alla protezione dell'organizzazione. Allo stesso tempo, sono fondamentali solide pratiche di gestione IT.

È importante riconoscere che la minaccia principale è rappresentata dal comportamento dell'utente finale. Le aziende devono implementare controlli di gestione IT che rilevano quando i dipendenti eludono una policy o una procedura. Le pratiche di gestione dovrebbero includere il coinvolgimento attivo degli utenti, istruendoli su come regolare i comportamenti per la sicurezza.

I professionisti IT devono anche valutare i rischi considerando il portafoglio IT complessivo. Anche se qualsiasi sistema è vulnerabile agli attacchi, i malintenzionati sono più interessati alle informazioni di valore che non sono adeguatamente protette. Le aziende devono dare la priorità alla protezione delle risorse e implementare una gestione IT proattiva, che include Obiettivi del punto di ripristino (RPO) per valutare in che quantità è accettabile la perdita di dati in caso di guasto e per rafforzare le difese. I responsabili devono conoscere le risorse di cui dispongono e come sono configurate, e devono controllare rigorosamente qualsiasi modifica.

Un framework come ITIL (Information Technology Infrastructure Library) può aiutare le organizzazioni a mettere in atto le migliori pratiche per la gestione IT. ITIL fornisce pratiche per la gestione della configurazione, delle modifiche e delle versioni, che sono i processi chiave che le organizzazioni devono implementare per padroneggiare la sicurezza informatica e la minaccia ransomware.

SENZA RANSOMWARE: UNA PROSPETTIVA REALISTICA?

Respingere un attacco ransomware sfaccettato richiede una difesa coordinata che combina la giusta tecnologia con solide pratiche di gestione IT. L'alternativa ideale è una soluzione di sicurezza e protezione multi-layer end-to-end.
Se un'organizzazione IT fosse in grado di mettere in atto una prima e ultima linea di difesa contro il ransomware, potrebbe praticamente eliminare la minaccia e trasformare il modo in cui protegge e mantiene al sicuro i dati delle organizzazioni da estorsori, hacker e ladri.

Un recente sondaggio globale tra professionisti IT ha rivelato che due intervistati su tre ritengono di vitale importanza trovare soluzioni che uniscano sicurezza e protezione dei dati.9 Gli intervistati ritengono questo aspetto ancora più importante rispetto al trovare soluzioni che sfruttino l'intelligenza artificiale per prevedere i disastri o che automatizzino la conformità.[10]

STRATEGIE DI PROTEZIONE DAL RANSOMWARE

Di seguito elenchiamo cinque strategie di protezione dal ransomware che possono aiutare a portare la propria azienda oltre gli approcci di sicurezza reattivi, integrando anti-ransomware e altre tecnologie di prevenzione delle minacce con funzionalità di disaster recovery e alta disponibilità per neutralizzare gli attacchi informatici.

1 Gestire attivamente l'accesso

Impostare i controlli e le procedure necessari per proteggere applicazioni e sistemi da utenti non autorizzati.

- L'accesso a punti di ingresso comuni per il ransomware, come account di posta elettronica personali e siti web di social network, è limitato e si utilizzano filtri web sul gateway e sull'endpoint per bloccare i tentativi di phishing che potrebbero indurre gli utenti a selezionare un link.
- Vengono utilizzati l'autenticazione a più fattori e standard avanzati per le password, e sono stati definiti requisiti per le password degli utenti che comunicano con siti web non classificati dal proxy o dal firewall.
- Vengono utilizzati server proxy e software di blocco degli annunci, e le autorizzazioni all'installazione ed esecuzione di applicazioni software sono limitate.
- Vengono controllate e monitorate le terze parti che hanno accesso remoto alla rete dell'organizzazione e le connessioni a terze parti, per assicurarsi che stiano applicando le migliori pratiche di sicurezza informatica.
- Viene utilizzato il whitelisting dell'applicazione in modo che sulla rete vengano eseguiti solo programmi approvati

2 Gestire la configurazione dei sistemi per tutti i vettori di attacco

Distribuire sistemi e procedure di gestione centralizzata per contrastare l'intero spettro di minacce ransomware.

- I dati sensibili per l'azienda vengono valutati e classificati ed è stata implementata la separazione fisica e logica di server, reti e archivi di dati.
- Si fa in modo che le soluzioni antivirus e antimalware abbiano la possibilità di aggiornare e scansionare automaticamente le e-mail in entrata e in uscita per rilevare il phishing, prevenire lo spoofing delle e-mail e filtrare i file eseguibili.
- Viene utilizzato un sistema di gestione centralizzata delle patch per correggere tutti gli endpoint non appena vengono rilevate vulnerabilità; sono inclusi dispositivi mobili, sistemi operativi, software e applicazioni, posizioni cloud e IoT.
- Vengono installate tecnologie di deep learning, anti-exploit e anti-ransomware senza firma, in grado di rilevare malware noti e sconosciuti.
- Vengono installate tecnologie integrate di protezione degli endpoint e di business continuity, per accelerare la prevenzione delle minacce e consentire il ripristino immediato dei dati.
- Si proteggono le applicazioni e i server web utilizzando firewall appropriati.
- Dai file di Microsoft Office inviati per email sono disabilitati gli script; si valuta la possibilità di utilizzo del software Office Viewer per aprire i file di Office.

- La rete viene monitorata per verificare i sistemi utilizzando Remote Desktop Protocol, chiudendo le porte inutilizzate e tramite autenticazione a due fattori.
- Vengono rilevati e identificati come dannosi i comportamenti come la crittografia di massa dei file, e quindi vengono bloccati.
- Alle e-mail che arrivano dall'esterno viene aggiunto un banner che ricorda agli utenti i pericoli che derivano dal selezionare link e aprire allegati.
- Si utilizzano le appliance Unified Threat Management (UTM) che combinano firewall, gateway antivirus e funzionalità di di rilevamento e prevenzione intrusioni per bloccare l'accesso a indirizzi IP dannosi noti.

3 Combinare soluzioni di sicurezza e protezione dei dati

Integrare, testare e mantenere la completa sicurezza informatica e protezione dei dati per la protezione end-to-end.

- I repository dei backup sono protetti da malware, ransomware e attacchi zero day.
- Vengono fermate e rimosse dai backup minacce come malware e ransomware.
- I backup dei dati vengono conservati su dispositivi separati e si utilizza storage offline nel caso in cui gli archivi non possano essere raggiunti direttamente da dispositivi infetti.
- Backup di macchine virtuali, cloud storage e sistemi operativi basati su RPO - considerando quale quantità di perdita di dati è accettabile in caso di guasto.
- Viene utilizzato un sistema che consente di salvare più iterazioni di backup, nell'eventualità in cui una copia contenga file crittografati o infetti.
- Le appliance per il disaster recovery e la disponibilità delle applicazioni sono integrate e viene sfruttata l'intelligenza artificiale per la protezione degli endpoint.
- Vengono utilizzate scansione delle vulnerabilità, crittografia SSL ed effettuate altre verifiche tecniche per confermare l'esecuzione dei backup
- Viene utilizzata la regola 3-2-1: creare tre copie dei dati, memorizzarli su due supporti diversi e uno di questi conservarlo fuori sede.
- I backup vengono testati regolarmente per verificare l'integrità dei dati e assicurarsi che siano operativi.
- I dati e i processi di disaster recovery vengono testati per garantire la preparazione.

4 Coinvolgere gli utenti con formazione e comunicazioni

Offrire agli utenti educazione ed esempi pratici necessari per proteggersi dalle minacce ransomware.

- Distribuire formazione e comunicazioni periodiche di sensibilizzazione in modo che in azienda tutti comprendano la minaccia costituita dal ransomware e abbiano familiarità con le tecniche di sicurezza.
- Sono state stabilite policy e procedure di sicurezza e di prevenzione da ransomware per gli utenti finali.
- Gli utenti sono stati istruiti a non aprire e-mail sospette, non fare clic su link né allegati e ad essere cauti prima di visitare siti web sconosciuti, oltre a chiudere il browser quando non viene utilizzato.
- Garantire che i dipendenti sappiano dove e come segnalare attività sospette.

5 Mantenere e testare un piano di business continuity e disaster recovery

Stabilire, testare e mantenere pratiche, procedure e strumenti tecnologici per garantire che applicazioni e dati possano essere completamente recuperati in caso di catastrofe.

- Sono stati impostati piani di emergenza e di riparazione, fondamentali per il ripristino e la continuità aziendale indipendentemente dall'origine dell'interruzione.
- Vengono condotte valutazioni dei rischi per classificare i tipi di catastrofe che possono verificarsi e stabilire le priorità per il recovery e la business continuity.
- Soluzioni di disaster recovery, backup e disponibilità elevata sono distribuite in sede e off site.
- È stato predisposto un piano di reazione agli incidenti che delinea le procedure da seguire in caso di attacco ransomware, inclusa la disconnessione del sistema infetto dalla rete per impedire la propagazione dell'infezione, rilevando la sensibilità dei dati.
- Testare il piano, compresi i sistemi e gli apparecchi tecnologici, per garantire la protezione completa. Vengono segnalate eventuali infezioni alle autorità competenti.

SEI PRONTO AD AFFRONTARE IL RANSOMWARE?

Scarica **Valutazione della competenza sul ransomware** per stimare le tue capacità e costruire il percorso verso un futuro senza ransomware.

LA NUOVA TECNOLOGIA PROMETTE UN FUTURO SENZA RANSOMWARE

Per anni, i professionisti IT sono andati inutilmente alla ricerca di una soluzione di sicurezza / protezione dei dati end-to-end a più livelli per garantire la resilienza IT e la prevenzione del ransomware. La buona notizia è che ora esiste una soluzione che risponde esattamente ai requisiti, in grado di costituire una prima e ultima linea di difesa contro la minaccia ransomware. Questa soluzione combina la serie di appliance Arcserve con Sophos Intercept X Advanced per Server per fornire un approccio a più livelli che offre protezione e sicurezza dei dati complete, il tutto in un'unica piattaforma integrata.

Gli utenti beneficiano delle capacità complete dei sistemi autonomi che, grazie a un'interfaccia centrale per gestire processi, strumenti e infrastrutture di backup, eliminano la necessità di procurarsi componenti separati da combinare tra loro. Le apparecchiature Arcserve offrono caratteristiche uniche di gestione storage deduplicato con accelerazione flash, elaborazione server robusta e rete ad alta velocità con hardware e servizi cloud altamente ridondanti.

In aggiunta, la protezione endpoint di Sophos Intercept X Advanced per Server garantisce una soluzione end-to-end che include rilevamento di malware basato su firma e non basato su firma, rete neurale avanzata di intelligenza artificiale (deep learning), tecnologia anti-exploit e tecnologie anti-ransomware per offrire protezione contro la più ampia gamma di minacce endpoint.

Il risultato: Una combinazione "tutto in uno" senza pari: sicurezza informatica dall'inizio alla fine, backup dei dati, disaster recovery ed elevata disponibilità, il tutto riunito in un'unica soluzione per coprire adeguatamente ogni esigenza infrastrutturale.

RIEPILOGO

Anche se il ransomware ha rappresentato un rischio aziendale significativo e una minaccia severa, il futuro è luminoso. Oggi le aziende possono:

- **Distribuire soluzioni integrate di protezione approfondita** fper backup avanzati, disaster recovery, alta disponibilità e sicurezza informatica;
- **Abilitare pratiche IT** con pratiche efficaci di coinvolgimento degli utenti, gestione dei dati e disaster recovery che realizzano un ritorno sull'investimento (ROI); e
- **Fornire una prima e ultima linea di difesa** che accelera il rilevamento delle minacce e consente il ripristino immediato dei dati di backup.

Quindi, perché lasciare le cose come stanno? Perché sopportare un mondo in cui criminali informatici, hacker e ladri usano il ransomware per ricavare guadagni illeciti a spese di aziende che stanno semplicemente cercando di portare avanti i loro affari? Ribellati. Mantieni i tuoi dati al sicuro. Utilizza la tecnologia di protezione end-to-end e le solide pratiche di gestione IT oggi disponibili, in modo che finalmente tu e la tua azienda possiate godervi un futuro senza ransomware.

ARCSERVE

Arcserve offre soluzioni eccezionali per la sicurezza delle inestimabili risorse digitali delle aziende che necessitano di una protezione completa e approfondita dei dati. Fondata nel 1983, Arcserve è il fornitore più esperto al mondo di soluzioni di business continuity che salvaguardano le infrastrutture IT multigenerazionali con applicazioni e sistemi in qualsiasi luogo, in sede e nel cloud. Organizzazioni in più di 150 paesi in tutto il mondo si affidano alle tecnologie e alle competenze integrate e altamente efficienti di Arcserve per eliminare il rischio di perdita di dati e tempi di inattività prolungati, riducendo al contempo il costo e la complessità del backup e del ripristino dei dati fino al 50%.

SOPHOS

Oltre 100 milioni di utenti in 150 paesi si affidano a Sophos valutandola la migliore protezione contro minacce complesse e perdita di dati. Sophos ha l'obiettivo di fornire soluzioni di sicurezza complete, semplici da implementare, gestire e utilizzare e con il più basso TCO del settore. Sophos offre una tecnologia di crittografia pluripremiata, sicurezza per endpoint, web, e-mail, mobile, server e di rete, con il supporto di SophosLabs, una rete globale di centri di intelligence sulle minacce.

FONTI

1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

2 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt
https://www.aarp.org/money/scams-fraud/info-2019/survey-identity-fraud-decline.html

3 https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomware-attacks/

4 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

5 https://pdf.ic3.gov/2018_IC3Report.pdf

6 https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx

7 https://twitter.com/CarbonBlack_Inc/status/925348051782373382

8 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

9 Arcserve EMEA Survey, July 31, 2019

10 Arcserve EMEA Survey, July 31, 2019

Per maggiori informazioni su Arcserve, **visitate il sito arcserve.com**