Acronis

WHITE PAPER

# La minaccia crescente del ransomware è un'opportunità di business per gli MSP

Dai impulso al tuo business con i servizi di Cyber Protection

Il crimine informatico è un'attività in piena espansione e continua a infliggere danni ad aziende e organizzazioni di ogni tipo. Nel 2021, il costo medio di una violazione dei dati è aumentato da 3,86 a 4,24 milioni di dollari, il valore più alto degli ultimi 17 anni.[1] Per le aziende, gli attacchi informatici sono un problema costoso, con conseguenze quali interruzioni operative che riducono i profitti, mancati utili, danni alla reputazione del marchio, perdita di valore azionario e sanzioni amministrative.

Per il recente Report Acronis sulla preparazione digitale abbiamo intervistato 3.600 utenti in 18 paesi diversi, tra responsabili IT e lavoratori remoti, al fine valutarne la preparazione digitale durante il secondo anno della pandemia. Dai risultati è emerso che il 30% delle aziende subisce almeno un attacco informatico al giorno, e che l'81% di tutti gli intervistati riferisce di aver subito un attacco almeno una volta a settimana durante l'anno precedente[2]. Al contempo, numerose ricerche indicano che le interruzioni operative hanno costi che variano dai 10.000[3] ai 260.000 dollari l'ora[4].

Dei numerosi tipi di malware in circolazione, il ransomware rappresenta al momento la minaccia digitale più agguerrita. L'Internet Crime Complaint Center dell'FBI ha ricevuto 2.084 segnalazioni di ransomware da gennaio al 31 luglio 2021, che rappresentano un aumento del 62% anno su anno[5]. Nel periodo di riferimento, il ransomware ha colpito indistintamente tutti i settori. Ad esempio, sulla base dei dati sottratti con il ransomware e pubblicati negli appositi siti di divulgazione, il settore dei servizi professionali e legali è stato quello più colpito dalle violazioni nel 2021, seguito da quello edilizio[6].

**Non sorprende che i leader aziendali e dei reparti IT temano un attacco ransomware che può mettere a repentaglio la propria azienda e la propria carriera.**

Il ransomware danneggia seriamente le sue vittime – spesso è sufficiente ingannare un dipendente inconsapevole che apre un'email di phishing, causando interruzioni brusche dei sistemi che si diffondono in breve tempo in modo dirompente. I pagamenti in criptovalute ostacolano inoltre l'intervento delle forze dell'ordine. È una tipologia di crimine più semplice e redditizia rispetto alle violazioni delle difese di un'azienda che puntano a sottrarre e rivendere dati sensibili.

## Ransomware: una minaccia e un'opportunità

Come Managed Service Provider (MSP), dovrebbe esserti chiaro che questo particolare crimine informatico rappresenta tanto una minaccia quanto un'opportunità.

Parte della minaccia deriva dal fatto che vendor tecnologici e Service Provider vengono sfruttati per colpire clienti aziendali e istituzioni governative, con complessi attacchi alle supply chain: il più noto è la violazione di SolarWinds, scoperta nel dicembre 2020[7]. Irrompendo nelle aziende software e infiltrando il malware nelle applicazioni più diffuse, i criminali informatici compromettono i sistemi dei Service Provider che utilizzano quegli strumenti, e da lì arrivano ai clienti di cui gestiscono le infrastrutture IT.

Diventare il bersaglio di un attacco ransomware è tuttavia solo una parte della minaccia: altrettanto grave è l'incapacità di arrestare gli attacchi ransomware destinati ai propri clienti, che risulta deleteria sia per la competitività dell'MSP che per le sue potenzialità di crescita. La sfida che gli MSP devono affrontare è complessa e in evoluzione.

**I dati statistici parlano chiaro:**

**30%**

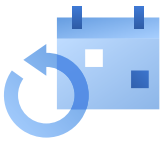
Piccole imprese degli Stati Uniti con punti deboli che possono essere sfruttati dagli hacker[8]

**44%**

Attacchi ransomware che hanno colpito aziende con meno di 1.000 dipendenti nel 3° trimestre 2021[9]

**22 giorni**

Interruzione media dell'attività aziendale per un'impresa a seguito di un attacco ransomware nel 3° trimestre 2021[10]



**350%**

Attacchi di social engineering in più che un dipendente di una piccola azienda (<100 dipendenti) subirà rispetto a un dipendente di un'azienda più grande[11]

**97%**

MSP che temono di subire una violazione della sicurezza con conseguente compromissione anche dei sistemi IT dei clienti nei prossimi 12 mesi[12]

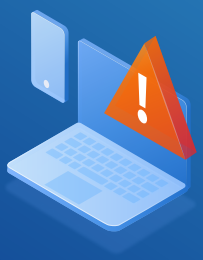
**49%**

MSP che ammettono che i propri clienti non si fidano completamente della sicurezza dei servizi forniti dalla propria azienda[13]

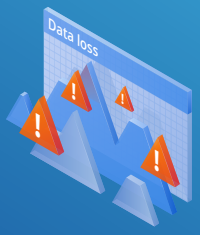
Tuttavia, ogni sfida aziendale porta con sé anche delle opportunità. Devi proteggerti dagli attacchi ransomware e impedirne la diffusione, ma hai anche la possibilità di proporre nuove offerte differenziate e altamente redditizie, con un portafoglio di servizi di Cyber Protection in grado di difendere dal ransomware e da altri pericoli di perdita di dati. Di seguito alcuni aspetti di cui tener conto:

## PRIORITÀ PER L'INCREMENTO DEL BUDGET IT PER IL 2022[14]

**1.** Necessità di aggiornare un'infrastruttura IT obsoleta



**2.** Priorità più alta ai progetti IT




**3.** Timori sulla sicurezza in aumento

**92%**

È la percentuale di PMI che **valuta il passaggio a un nuovo MSP** se questo offre la giusta soluzione per la Cyber Security[15]

**34%**

È il maggiore costo che una piccola-media impresa **sarebbe disposta a sostenere** per ottenere la giusta soluzione di Cyber Security[16]

**61%**

Incremento del numero di responsabili decisionali secondo i quali la propria azienda **non dispone delle competenze interne** per affrontare adeguatamente le problematiche legate alla sicurezza[17]

Alla luce di questi dati, la proposta di valore che puoi presentare ai tuoi clienti PMI è semplice e convincente: "Possiamo eliminare ogni vostra preoccupazione in merito agli attacchi ransomware e malware, e proteggervi anche da diverse altre minacce che possono causarvi perdite di dati."

Quella di Acronis è un'offerta semplice, gestibile, con margini elevati e compatibile con l'infrastruttura esistente, che ti consente di incrementare il fatturato e ridurre il tasso di abbandono dei clienti.

## Tre modi frequenti con cui gli MSP contrastano il ransomware e le insidie ad essi associate

Le soluzioni a disposizione degli MSP per cogliere questa nuova opportunità commerciale si possono suddividere in tre categorie: backup, backup con difese limitate contro il ransomware e backup combinato con software anti-malware di terze parti installato sugli endpoint. Ogni categoria presenta dei limiti:

**1. Backup**: consiste nel riportare i sistemi compromessi a un momento precedente all'attacco. Da solo, l'approccio presenta numerosi punti deboli: il ripristino di decine o centinaia di sistemi dal backup, soprattutto se si usano dispositivi lenti come i nastri o il cloud, richiede molto tempo, causa interruzioni dell'attività, è soggetto a errori ed è molto costoso. Inoltre, se il punto di ripristino (il giorno e l'ora del backup più recente) è troppo lontano nel tempo, molti dati importanti creati tra il backup e l'attacco andranno persi.

**2. Backup con difese limitate contro il ransomware**: soluzioni di questo tipo possono contrastare alcuni attacchi, riducendo la necessità di affidarsi al solo backup per eseguire il ripristino. In genere, tuttavia, il rilevamento degli attacchi si basa su calcoli statistici grossolani che confrontano la percentuale di modifiche apportate ai file con una soglia di base. Un aumento repentino delle modifiche apportate può indicare un possibile attacco, ma si tratta di un approccio reattivo e soggetto a errori di identificazione e a falsi positivi, entrambi aspetti potenzialmente costosi.

Come nel caso delle soluzioni basate solo sul backup, neanche questa è d'aiuto quando l'attacco riesce a individuare e a danneggiare i file di backup impedendone il ripristino. Molte varianti del ransomware possono farlo.

**3. Backup combinato con software antimalware di terzi**: per contrastare il ransomware, questo approccio adotta una protezione più raffinata, ubicata sull'endpoint. La mancata integrazione tra i due componenti e i rispettivi agenti può tuttavia provocare rallentamenti nelle prestazioni dei sistemi, conflitti tra processi con interruzione dei backup, difficoltà di deployment e gestione per gli MSP.

## Un'alternativa più avanzata ed efficiente studiata per gli MSP

Esiste infine una quarta opzione destinata agli MSP, semplice ma di grande efficienza ed efficacia: Acronis Cyber Protect Cloud con tecnologia Acronis Active Protection. Questa soluzione, già adottata da oltre 10.000 MSP, consente di fornire servizi di Cyber Protection che combinano Backup-as-a-Service e funzionalità integrate di Cyber Security basate su intelligenza artificiale (per la difesa da virus, malware e cryptojacking) e funzioni di riparazione automatica dei danni:

- Grazie alle tecnologie di intelligenza artificiale (IA) e di machine learning (ML), Acronis Active Protection rileva e arresta gli attacchi ransomware. L'apprendimento continuo del motore di rilevamento comportamentale avanzato all'interno dell'infrastruttura Acronis Cloud AI garantisce la più bassa percentuale di falsi positivi del settore per quel che riguarda il rilevamento del malware, inclusi gli attacchi di tipo zero-day, ovvero quelli ancora ignoti.
- I meccanismi di autodifesa integrati impediscono al ransomware di danneggiare i processi, gli agenti e gli archivi di backup Acronis.
- La funzionalità di riparazione dei danni automatica utilizza una cache locale per ripristinare all'istante qualsiasi file danneggiato prima del rilevamento dell'attacco, garantendo l'immediata ripresa delle attività aziendali senza dover procedere a un ripristino completo dal backup.
- Vulnerability assessment e patch management automatizzati chiudono ogni varco nella sicurezza che potrebbe consentire l'accesso del ransomware ai sistemi, mentre il filtraggio degli URL blocca i siti web che diffondono malware.
- Il motore di rilevamento comportamentale avanzato è in grado di individuare e bloccare anche gli attacchi di cryptojacking, un tipo di malware che, all'insaputa dell'azienda, consuma le risorse di sistema e l'energia destinata all'alimentazione e al raffreddamento, utilizzandole per il mining di criptovalute. Finora, nel corso del 2022, sono stati registrati 15,02 milioni di eventi di cryptojacking al mese, un aumento dell'86% rispetto al 2020.[18]

In breve, l'integrazione esclusiva di backup, Cyber Security e gestione degli endpoint di Acronis Cyber Protect Cloud ti consente di ridurre all'istante l'esposizione dei tuoi clienti al ransomware. È sufficiente installare un agente per fornire la Cyber Protection completa, evitando conflitti tra processi e problemi prestazionali.

**"La soluzione di Acronis offre prestazioni eccellenti, è di facile impiego e ricca di funzionalità. In più, è l'unica tra quelle testate che integra una protezione dedicata contro gli attacchi ransomware. Per questo motivo si è guadagnata il primo certificato di approvazione per il backup e la sicurezza dei dati mai assegnato da AV-TEST."**

**David Walkiewicz**
Direttore ricerche per i test,
av-test.org

## Collaborare con Acronis per offrire servizi di Cyber Protection completi

Acronis non offre ai Service Provider solo funzionalità avanzate di protezione dal ransomware. Acronis Cyber Backup Cloud è parte integrante di Acronis Cyber Cloud, una piattaforma di Cyber Protection multiservizi concepita specificamente per i Service Provider, una sorta di **coltellino svizzero multiuso per l'erogazione di servizi di Cyber Protection, che offre:**

1. Un set integrato di soluzioni che include **il miglior backup del mercato, disaster recovery, Cyber Security (con protezione da virus, malware, ransomware e cryptojacking), file sync and share, autenticazione dei file, software-defined storage e gestione degli endpoint.**
2. Una **piattaforma** per il provisioning unificato dei servizi, gestione degli account, monitoraggio, integrazione, personalizzazione del marchio e altro ancora.

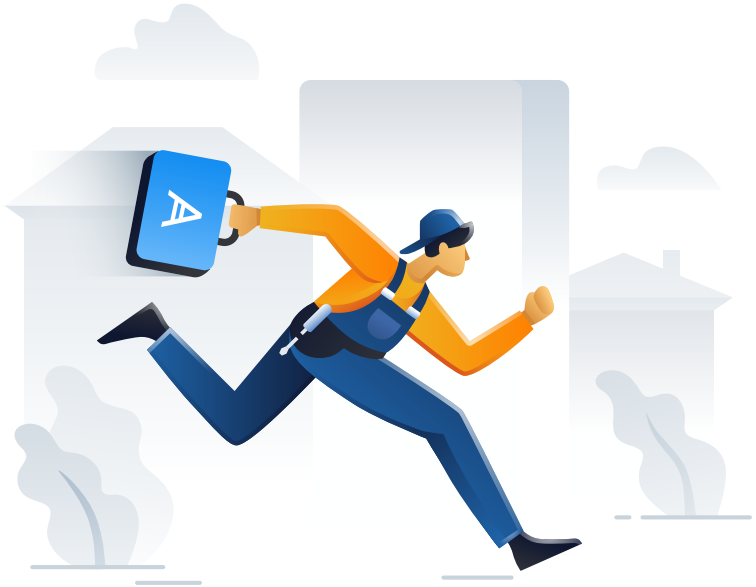
Acronis Cyber Protect Cloud consente ai Service Provider di erogare redditizi servizi di Cyber Protection a ridotto tasso di abbandono, grazie ai quali i vostri clienti potranno dedicarsi alle proprie attività senza preoccupazioni, anche in un panorama sempre più minacciato dai crimini digitali. La suite offre ai Service Provider un'efficienza straordinaria a 360°, dal deployment iniziale dei sistemi al provisioning dei servizi unificato, fino alla gestione dei clienti. La piattaforma Acronis Cyber Cloud include:

- Supporto multi-tenant per un numero illimitato di clienti
- Un portale di gestione multiservizi
- Funzionalità di personalizzazione del marchio
- Quote di utilizzo del servizio e funzionalità di creazione di report
- Integrazione con i più diffusi sistemi RMM e PSA
- Integrazione personalizzata di servizi aggiuntivi grazie all'API open source

**Scopri come offrire ai tuoi clienti la Cyber Protection in modo semplice, efficiente e sicuro con Acronis:**

Contatta il reparto commerciale Acronis per una dimostrazione del prodotto più adatto ai tuoi scenari d'uso. CONTATTA L'UFFICIO VENDITE

Inizia a utilizzare la tua versione di prova gratuita valida 30 giorni. PROVA LA SOLUZIONE



**Fonti**


[1] https://www.ibm.com/security/data-breach

[2] https://www.acronis.com/en-us/blog/posts/acronis-cyber-readiness-report-2021-reveals-critical-security-gaps/

[3] https://www.cloudradar.io/cost-of-downtime

[4] https://www.stratus.com/assets/aberdeen-maintaining-virtual-systems-uptime.pdf

[5] https://www.cisa.gov/uscert/ncas/alerts/aa21-243a

[6] https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html?utm_source=google-rapp-amer-rapp&utm_medium=paid-search&utm_campaign=Unit_42-Americas-EN-Search-Lead_Gen-US/CA_Q4&utm_content=gs-{16992445439}-{135418592603}-{593884840443}&utm_term=ransomware&sfdcid=7014u000001hKM8AAM&_bt=593884840443&_bm=p&_bn=g&gclid=Cj0KCQjwz96WBhC8ARIsAATR252kVW2uoMmVZ0db3W8lONQy7qL2NJyO2wW6_f5By5aEtVAIMMpXO44aAhFaEALw_wcB

[7] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[8] https://www.inc.com/melissa-angell/small-business-cyber-threats-data-protection.html

[9] https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts#companies

[10] Ibid.

[11] https://www.barracuda.com/spearphishing-vol7

[12] https://www.acronis.com/en-us/resource-center/resource/648/

[13] Ibid.

[14] https://swzd.com/resources/state-of-it/#chapter-2

[15] https://www.globenewswire.com/news-release/2021/06/22/2251268/27043/en/SMBs-would-pay-on-average-34-more-for-an-IT-service-provider-who-could-provide-the-right-solution-a-rise-from-25-in-2019.html

[16] Ibid.

[17] Ibid.

[18] https://www.top10vpn.com/research/cybercrime-statistics/