Synology®

Proteggi dai ransomware la tua organizzazione

Secondo le previsioni, gli attacchi ransomware costeranno alle organizzazioni una cifra totale di 8 trilioni di dollari USA nel solo 2023.[1] I piani di protezione dei dati con opzioni di ripristino veloci sono cruciali per mitigare l'impatto dei ransomware e altre tipologie di crimini informatici.

Date 13 ott 2023

Backup: l'ultima risorsa per difendersi in caso di attacco

Quando i dati vengono persi a seguito di una cancellazione o di una modifica dannosa, i backup consentono di ripristinare dati importanti per mission aziendale ed evitare costosi tempi di inattività. Le soluzioni Synology per la protezione dei dati sono ideali per progettare una strategia di backup per l'intera infrastruttura IT.

Protezione completa

Proteggi gli endpoint e i backup primari per creare più reti di sicurezza per i dati.

Recupero veloce

In caso di emergenza, le opzioni di recupero immediato consentono di ridurre al minimo i tempi di inattività.

Archiviazione non modificabile

Previeni le modifiche non autorizzate a dati e snapshot.

Backup senza licenza

Esegui il backup di tutti i dati consentiti dall'archiviazione, senza limitazioni o costi nascosti.

Protezione centralizzata dai ransomware

Consolida i backup da flotte di workstation, server, macchine virtuali e applicazioni cloud. Ottimizza il consumo dello spazio di archiviazione, senza problemi per la larghezza di banda, attraverso la deduplicazione dei dati e le tecnologie di backup incrementali. https://www.synology.com/dsm/solution/infrastructure

Carichi di lavoro fisici

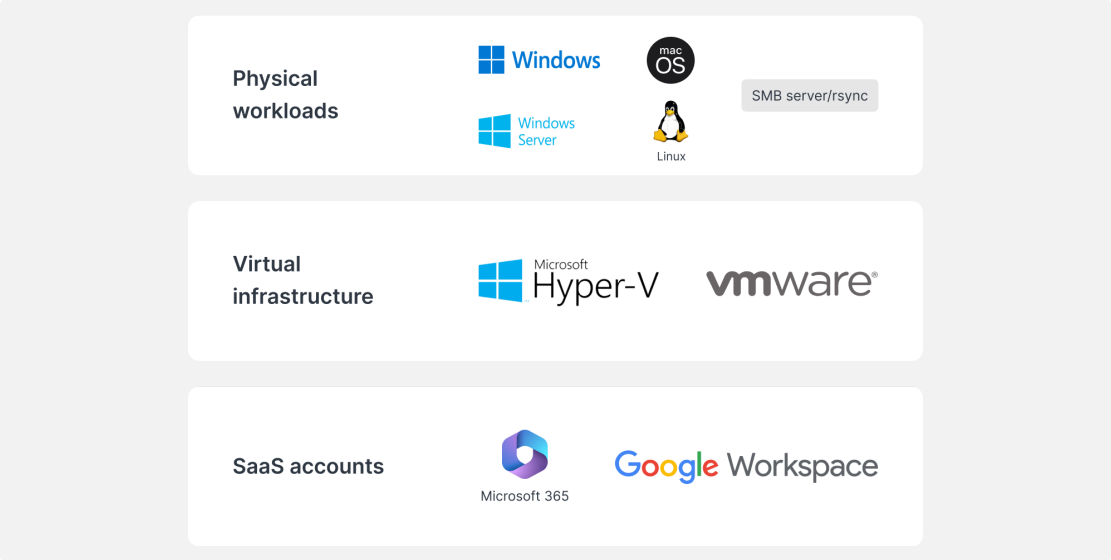
Proteggi gli endpoint in caso di attacchi dannosi mediante backup bare-metal completo e ripristino flessibile a livello di file.

Infrastruttura virtuale

Backup delle VM VMware® vSphere™, Microsoft® Hyper-V® e delle LUN con potenti tecnologie di riduzione dei dati.

Account SaaS

Consenti la protezione continua dei dati archiviati nel cloud con il rilevamento automatico degli account aggiunti di recente.



Recupero efficiente

Riduci al minimo i tempi di inattività per i sistemi di produzione critici attraverso il ripristino veloce dei backup da un sistema Synology locale o esterno.

RTO quasi zero

Esegui il montaggio delle immagini di backup su VMware®, Hyper-V® o Synology Virtual Machine Manager per riprendere il lavoro il più rapidamente possibile. Ripristina le VM su un hypervisor alternativo per evitare interruzioni del servizio.

RPO minimo

Configura la frequenza di backup in base alle esigenze, riducendo al minimo la quantità di dati potenzialmente interessati durante un attacco. Proteggi rapidamente i sistemi grazie alla tecnologia di deduplicazione e backup incrementali.

Funzionamento intuitivo

Consenti ai dipendenti di consultare e visualizzare in anteprima e-mail, contatti e file attraverso un comodo portale, prima di ripristinarli, offrendo un'esperienza più intuitiva e riducendo il carico di lavoro per i team IT.

Aggiungi un livello di protezione extra

La strategia di backup 3-2-1 consente di archiviare un terzo set di dati fuori sede o sul cloud, proteggendo i dati da incendi, disastri naturali o furti.

In server fuori sede

Archivia i backup su un server Synology che si trova in una sede secondaria per difenderti dai disastri materiali e replica le snapshot non modificabili come ulteriore forma di difesa dai ransomware.

Su cloud

Esegui il backup su qualsiasi provider principale di storage cloud, proteggendo i dati da accessi non autorizzati tramite la crittografia AES-256 sul lato client. https://c2.synology.com/storage/nas

Affidabilità in diversi settori

"Synology [...] ci ha permesso di ridurre la spesa per l'hardware dei server [...] rendendo al contempo molto più semplice il backup dell'infrastruttura e delle postazioni di lavoro, la registrazione dei sistemi e la gestione dei file"
https://www.synology.com/company/case_study/Investortools

"Grazie ad Active Backup for Business, oggi tutti i nostri backup sono centralizzati e disponibili h24 e 7 giorni su 7; questo ci aiuta a ridurre al minimo i tempi morti e rispettare i requisiti FERPA."
https://www.synology.com/company/case_study/University_of_Washington

[...] Active Backup for Business possiede velocità di backup stupefacenti ed è imbattibile nell'eliminazione dei dati duplicati: appena 28 TB utilizzati dei 58 TB totali del server [...].
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"Active Backup for Business [...] ci permette di centralizzare e gestire tutte le attività di backup da una singola console. Il recupero veloce e affidabile assicura, inoltre, la continuità operativa."
https://www.synology.com/company/case_study/UNESCO

FAQ

Che cos'è un ransomware?

Ransomware è un tipo di malware che crittografa i file delle vittime. Gli autori degli attacchi chiedono quindi un riscatto per ripristinare l'accesso ai dati, spesso minacciando di distruggere definitivamente i dati se non viene pagato alcun riscatto. Gli attacchi ransomware possono essere altamente dirompenti e causare perdite finanziarie significative per individui e organizzazioni. È importante proteggersi e proteggere i propri dispositivi da ransomware, ad esempio mantenendo il software aggiornato ed eseguendo regolarmente il backup dei file.

Che tipi di ransomware esistono?

Esistono molti tipi diversi di ransomware, e nuovi ceppi sono in costante sviluppo. Alcuni dei tipi più comuni di ransomware includono:

- **Ransomware con crittografia**: il tipo più comune di ransomware crittografa i file della vittima in modo che non possano essere accessibili senza chiave di decrittografia. Gli autori degli attacchi chiedono quindi il pagamento di un riscatto in cambio della chiave
- **Locker ransomware**: un tipo di ransomware impedisce alle vittime di utilizzare il proprio computer modificando le credenziali di accesso o visualizzando un messaggio che impedisce alla vittima di accedere al loro sistema. Gli autori degli attacchi chiedono quindi il pagamento di un riscatto per sbloccare il computer
- **Ransomware-as-a-Service (Raas)**: una sorta di business con cui gli autori degli attacchi offrono ransomware ad altri individui o gruppi che vogliono effettuare attacchi. In questi casi, gli autori degli attacchi forniscono il ransomware e gestiscono i pagamenti, mentre gli altri individui o gruppi ricevono una percentuale dei riscatti pagati
- **Scareware**: ransomware progettato per indurre le vittime a pagare il riscatto. In genere, si tratta della visualizzazione di falsi avvisi di sicurezza o di messaggi che comunicano che il computer della vittima è infettato da un virus. L'autore dell'attacco richiederà quindi il pagamento di un riscatto per rimuovere la presunta infezione

Come si diffonde il ransomware?

In genere, il ransomware si diffonde attraverso e-mail di phishing o sfruttando le vulnerabilità di un sistema informatico. In un attacco di phishing, un utente malintenzionato invierà un messaggio e-mail che sembra provenire da una fonte legittima, ad esempio una banca o un'azienda nota. L'e-mail conterrà spesso un link o un allegato che, se cliccato, installerà il ransomware sul computer della vittima. Lo sfruttamento delle vulnerabilità in un sistema è simile, tranne che l'utente malintenzionato sfrutta un difetto nella protezione del sistema per installare il ransomware senza che la vittima ne sia a conoscenza. In entrambi i casi, dopo essere stato installato, il ransomware può rapidamente diffondersi sugli altri computer della stessa rete.

Qual è il processo tipico di un attacco ransomware?

Il processo di un attacco ransomware in genere segue questi passaggi:

1. L'utente malintenzionato può accedere al computer di una vittima inviando un messaggio di phishing o sfruttando una vulnerabilità del sistema
2. Dopo avere ottenuto accesso al computer della vittima, l'autore dell'attacco installerà il ransomware sul sistema
3. Il ransomware quindi codificherà i file della vittima, rendendoli inaccessibili all'utente
4. L'utente malintenzionato richiederà quindi un riscatto alla vittima, in genere sotto forma di valuta digitale come Bitcoin, in cambio della chiave di decrittografia che sbloccherà i file crittografati
5. Se la vittima paga il riscatto, l'utente malintenzionato fornirà la chiave di decrittografia e la vittima potrà accedere nuovamente ai file. Tuttavia, non vi è alcuna garanzia che l'utente malintenzionato fornisca effettivamente la chiave e, anche in questo caso, i file della vittima potrebbero essere danneggiati o danneggiati a seguito del processo di crittografia

È importante notare che ci sono molte variazioni in questo processo, e non tutti gli attacchi ransomware seguiranno esattamente questi passaggi. Alcuni attacchi potrebbero non comportare la crittografia dei file, ad esempio, mentre altri potrebbero comportare altre forme di estorsione o ricatto.

Come si concretizza un attacco ransomware?

Un attacco ransomware si scatena in vari modi. Uno dei modi più comuni è fare clic su un collegamento o un allegato dannoso in un'e-mail di phishing. Questo tipo di e-mail è progettato per sembrare legittimo, spesso sembra provenire da una società o organizzazione ben nota. Quando si fa clic sul link o sull'allegato, il ransomware viene installato sul computer. Un altro modo con cui si attiva un attacco ransomware è attraverso la visita di siti Web compromessi. Questi siti Web sono stati violati da hacker, che hanno inserito il codice che installerà automaticamente il ransomware nel computer se si visita il sito. È anche possibile subire un attacco ransomware scaricando file infetti da Internet. Ad esempio, se si scarica un file da un sito Web sospetto o se si scarica un file condiviso da un utente sconosciuto. In breve, è importante essere prudenti quando si naviga in Internet ed evitare di fare clic su link o scaricare file provenienti da fonti sconosciute. In questo modo è possibile proteggersi da attacchi ransomware e altri tipi di malware.

Chi sono gli obiettivi del ransomware?

Gli attacchi ransomware possono colpire chiunque utilizzi un computer o un altro dispositivo connesso a Internet. Tuttavia, alcuni gruppi hanno maggiori probabilità di essere presi di mira rispetto ad altri. Ad esempio, gli attacchi ransomware spesso si rivolgono ad aziende in possesso di dati preziosi e più disponibili a pagare un riscatto per recuperarli. Anche ospedali, scuole e altre organizzazioni che forniscono servizi critici sono obiettivi comuni, in quanto un attacco ransomware può interrompere le loro operazioni e mettere a rischio la vita delle persone. Anche gli individui possono essere bersaglio di attacchi ransomware. In questi casi, gli autori degli attacchi possono cercare di estorcere denaro alla vittima minacciando di cancellare i file personali o di pubblicare informazioni sensibili a meno che non venga pagato un riscatto. Gli obiettivi degli attacchi ransomware sono spesso selezionati in base al valore dei loro dati e alla volontà di pagare un riscatto per riottenerli.

Quali sono i rischi di pagare ransomware?

Pagare un riscatto all'autore di un ransomware può sembrare il modo più semplice per recuperare i file, ma potrebbe rivelarsi molto rischioso. I rischi associati al pagamento di un riscatto sono vari, tra cui:

- Non vi è alcuna garanzia che l'autore dell'attacco fornisca effettivamente la chiave di decrittografia. In molti casi, le vittime che pagano il riscatto non ricevono mai la chiave e non possono più accedere ai file
- Il pagamento del riscatto potrebbe incoraggiare gli autori a continuare gli attacchi. Se le vittime si dimostrano disposte a pagare il riscatto, gli autori potrebbero essere indotti a sferrare più attacchi in futuro
- Un riscatto pagato può rendere la vittima bersaglio di attacchi futuri. Se l'autore dell'attacco scopre che la vittima è disposta a pagare, quest'ultima sarà più soggetta a rischi di attacchi futuri
- Il pagamento di un riscatto può essere illegale. In alcuni casi, il pagamento di un riscatto a un'organizzazione criminale può essere considerato una forma di finanziamento del terrorismo o di altre attività illegali

Sebbene pagare il riscatto possa sembrare il modo più semplice per recuperare i file, potrebbe rivelarsi in realtà una decisione molto rischiosa. È importante considerare attentamente i rischi prima di prendere una decisione.

Quali sono i costi del ransomware?

Il costo di un attacco ransomware può variare notevolmente in base a diversi fattori, come il tipo di ransomware utilizzato, il numero di file crittografati e l'efficacia dell'attacco. In alcuni casi, il costo di un attacco ransomware può essere relativamente basso, con gli autori degli attacchi che richiedono poche centinaia di dollari in riscatto. In altri casi, il costo può essere molto più alto, con gli autori degli attacchi che chiedono migliaia di dollari, o più, per ripristinare l'accesso ai file della vittima. Oltre ai costi diretti associati al pagamento di un riscatto, gli attacchi ransomware possono avere anche costi indiretti significativi. Ad esempio, un attacco ransomware può causare tempi di inattività e perdita di produttività, con conseguente perdita di ricavi e reddito. Può anche danneggiare la reputazione dell'azienda e la fiducia dei clienti, con effetti negativi a lungo termine sull'azienda. Questi costi indiretti sono spesso molto più alti del riscatto stesso.

Quali sono i sintomi del ransomware?

Il sintomi di un attacco ransomware possono variare in base al tipo specifico di ransomware utilizzato. In generale, alcuni sintomi comuni includono:

- I file sono crittografati e non è possibile accedervi
- L'utente malintenzionato riceve un messaggio che richiede il pagamento di un riscatto in cambio della chiave di decrittografia
- Sul computer vengono visualizzati programmi o processi non familiari in esecuzione
- Il computer diventa lento o non risponde
- Il computer visualizza messaggi di errore insoliti o finestre a comparsa

Se si sospetta che il computer sia stato infettato da ransomware, è importante agire rapidamente. È necessario scollegare il computer da Internet per evitare che il ransomware si diffonda.

Come prevenire gli attacchi di ransomware?

Per prevenire gli attacchi di ransomware, esistono diverse procedure, ad esempio:

- Utilizzare un software antivirus o di sicurezza affidabile e mantenerlo aggiornato. In questo modo è possibile proteggere il computer da attacchi ransomware e altri tipi di malware
- Prestare attenzione quando si aprono allegati e-mail o collegamenti. Il ransomware è spesso recapitato tramite e-mail di phishing, quindi è importante fare attenzione agli elementi su cui si fa clic
- Mantenere aggiornato il sistema operativo e altri software. Gli aggiornamenti software spesso includono patch di sicurezza che possono aiutare a proteggere il computer da ransomware e altre minacce
- Backup regolare dei file. Questa procedura contribuisce a proteggere i dati in caso di attacco ransomware al computer. È importante adottare una delle strategie di backup consigliate, ad esempio la strategia di backup 3-2-1
- Essere consapevoli dei rischi del ransomware e istruire gli altri utenti dell'organizzazione su queste minacce. Queste azioni contribuiscono a prevenire gli attacchi ransomware e ne semplificano il rilevamento e la risposta se si verificano

Il modo migliore per prevenire gli attacchi ransomware è mantenere il controllo e adottare misure per proteggere il computer e i dati. Queste azioni contribuiscono a ridurre il rischio di un attacco ransomware e ne semplificano il recupero se si verifica un attacco.

Quale protezione da ransomware offre Synology?

Delle misure preventive sono essenziali per proteggerti dal rischio di restare vittima del ransomware. Oltre al software antivirus, è possibile utilizzare una delle soluzioni Synology.

- **Prevenire l'accesso** - La diffusione dei ransomware può essere contenuta impostando le autorizzazioni per file, applicazioni e accessi e configurando le credenziali di accesso sicuro con Secure SignIn e C2 Password.
- **Proteggere i dispositivi** - I sistemi di vecchia generazione sono esposti a un rischio maggiore. È possibile aggiornare insieme tutti i NAS con Synology CMS e proteggere altri dispositivi utilizzando i criteri di gruppo in Synology Directory Server e C2 Identity.
- **Evitare file sospetti** — E-mail di spam e phishing contenenti file sospetti sono metodi comuni per diffondere ransomware. Synology MailPlus offre una solida strategia di prevenzione dello spam e anti-malware.
- **Controllo delle vulnerabilità** Con Synology Security Advisor è possibile eseguire sistematicamente le analisi che permettono di rilevare la presenza di eventuali malware, vulnerabilità di sistema e anomalie nelle operazioni di login. Applica le modifiche consigliate per migliorare la sicurezza del tuo NAS.
  https://www.synology.com/dsm/overview/security

Altri modi per proteggere i tuoi dati

Gestione della flotta

Sfruttando le funzionalità estese sarà possibile gestire centralmente le autorizzazioni di accesso ai dati, lo stato del software, lo stato del sistema e altro ancora.
https://www.synology.com/dsm/overview/administration

Monitoraggio di tutti i NAS

Identificazione di attività di accesso sospette, gestione degli aggiornamenti e monitoraggio dello stato dei dispositivi, indipendentemente dalla posizione dei dispositivi.
https://www.synology.com/dsm/feature/active-insight

Protezione dati

Con la regola di backup 3-2-1 è possibile proteggere i dati da modifiche o eliminazioni accidentali e dannose.
https://www.synology.com/dsm/solution/data_backup

Come iniziare

Contattaci

Per maggiori informazioni, contatta il servizio vendite regionale
https://www.synology.com/form/inquiry/sales

Dove acquistare

Trova il partner Synology più vicino nella tua regione
https://www.synology.com/wheretobuy

Note:

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Proteggi dai ransomware la tua organizzazione

https://www.synology.com/it-it/dsm/solution/ransomware

Sito web di Synology

https://www.synology.com/

Contattaci

https://www.synology.com/company/contact_us