Cove
Data Protection

Gli errori da non commettere in caso di ransomware

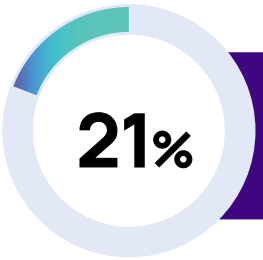
White paper

N-ABLE™

Gli errori da non commettere in caso di ransomware

I disastri assumono diverse forme, ma gli attacchi informatici come i ransomware continuano a far parlare di sé sui giornali, dimostrando che rappresentano la tipologia di disastro più preoccupante. I professionisti IT e i fornitori di servizi gestiti devono prepararsi a rispondere in modo tempestivo e appropriato iniziando a informarsi sui problemi principali e sui potenziali errori che fanno la differenza.

I ricercatori nell'ambito della sicurezza informatica hanno registrato l'aumento del 21% degli attacchi ransomware tra il primo e il secondo trimestre del 2022, a causa del significativo aumento dell'attività di tre delle principali aree produttive.[1] Gli Stati Uniti sono l'area più interessata e hanno registrato quasi il 40% di tutti gli incidenti. Germania e Regno Unito seguono, rispettivamente al secondo e al terzo posto.[1]



21% di aumento degli attacchi ransomware tra il T1 e il T2 del 2022

Aree geografiche maggiormente interessate

Stati Uniti | **Germania** | **Regno Unito**

Di che tipologia di disastro si tratta?

I tradizionali disastri come incendi, inondazioni o guasti hardware danno la priorità al ripristino istantaneo per ridurre al minimo i tempi di inattività. In queste situazioni è un buon approccio, ma il ripristino istantaneo nell'ambiente di produzione non rappresenta la soluzione ideale in caso, invece, di attacchi informatici. In questa circostanza, la rete somigli a una vera e propria scena del crimine che richiede requisiti differenti da quelli di un tradizionale disaster recovery.

Considerazioni	Disastro tradizionale	Attacco informatico
Volume dei dati	Completo, tutti i dati	Selettivo (include i servizi di base)
Ripristino	Disaster recovery standard/ failback	Iterativo (ripristino selettivo come parte della risposta agli incidenti)
Tempistiche di ripristino	Quasi istantaneo	Affidabili e veloci
Punto di ripristino	Virtualmente continuo	Un giorno, in media
Natura del disastro	Inondazione, interruzione di corrente, meteo avverso	Attacco informatico mirato
Impatto del disastro	Locale, di solito contenuto	Globale, con diffusione rapida
Topologia	Connessa, bersagli multipli	Isolata (in aggiunta al disaster recovery)

Gli esperti di rischi e conformità di Arcas Risk Management suggeriscono diverse best practice fondamentali per la sicurezza informatica: nell'era post-COVID che ha visto la diffusione del lavoro da remoto, un'adeguata soluzione per il backup e la protezione dei dati è stata aggiunta all'elenco dei requisiti critici, insieme a strumenti quali **antivirus o rilevamento e risposta per gli endpoint, firewall, monitoraggio della sicurezza 24 ore al giorno, tutti i giorni e l'impiego dell'autenticazione a più fattori.**

Queste precauzioni sono particolarmente importanti se consideriamo il grado di commercializzazione dei ransomware, aumentando a dismisura il numero dei criminali in grado di implementarli, che vanno ad aggiungersi agli esperti o ai vari stati. È sempre più chiaro che questo tipo di crimini finanzia chi li commette e pagare il riscatto non sempre garantisce il ripristino sicuro dei dati. Di fatto, dimostrare la volontà di pagare il riscatto potrebbe favorire altri attacchi; secondo una ricerca, infatti, l'80% delle aziende che ha pagato il riscatto ha subito un altro attacco, spesso per mano degli stessi criminali.[2] Un altro aspetto da considerare è che il ransomware si è evoluto e si rivolge sempre di più alle infrastrutture di backup nel tentativo di evitare che le aziende recuperino i dati con la speranza che paghino il riscatto.

Ripristino selettivo come parte della risposta agli incidenti

A differenza dei tradizionali disastri naturali o fisici, il piano di ripristino per un attacco informatico dovrebbe far parte di una più ampia strategia di risposta agli incidenti che non si limiti a recuperare i dati da un backup recente funzionante. Arcas consiglia una strategia composta da quattro livelli.

Visibilità: se non vedi eventuali problemi, non puoi risolverli in modo efficace. Con gli strumenti giusti puoi vedere dove si nasconde il software dannoso nel tuo ambiente, quando vi è penetrato e stabilire cosa fare. Un modo per fare tutto questo è scegliere N-able EDR.

Protezione: anche prima di un attacco è buona norma rivedere la separazione della rete, i sistemi resilienti e la strategia di sicurezza su più livelli complessiva. In questo modo potrai proteggerti dagli attacchi futuri.

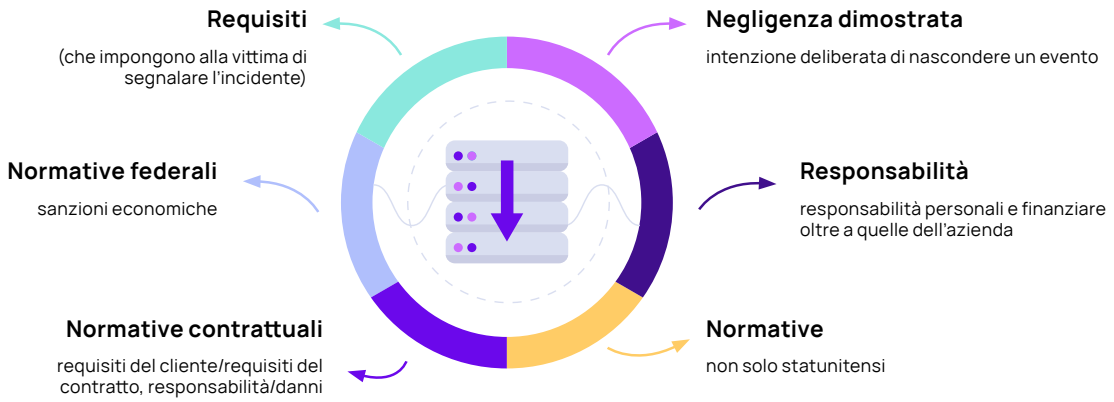
Controllo: metti in sicurezza il tuo ambiente utilizzando strumenti come l'autenticazione a due fattori e assicurati di gestire deprovisioning dei dipendenti, timeout dell'accesso e altre misure simili per ridurre al minimo eventuali falle che i criminali potrebbero sfruttare a loro vantaggio. Prendi anche in considerazione l'idea di applicare il principio dei privilegi minimi limitando il numero di super user, degli addetti alla sicurezza o degli amministratori con accesso API.

Applicazione di rimedi: una volta gestita e neutralizzata la minaccia immediata, è importante assegnare e chiarire le opportune responsabilità circa l'applicazione di rimedi.

Troppo spesso, i professionisti IT che implementano il tradizionale disaster recovery si lasciano sfuggire i più ampi requisiti di risposta agli incidenti e non si coordinano con i colleghi degli altri team. Le discussioni informali aiutano a pianificare i diversi aspetti e a preparare l'azienda agli attacchi praticamente inevitabili.

Come già detto in precedenza, un ripristino istantaneo troppo frettoloso in ambiente di produzione potrebbe potenzialmente reintrodurre il malware nell'ambiente. Meglio sarebbe eseguire il ripristino in una sede secondaria separata, così che l'attività possa riprendere senza influire sulle indagini forensi contaminando la "scena del crimine".

Il ripristino istantaneo può essere costoso
(e costare milioni a un'azienda)



Considerazioni assicurative

Un altro modo di considerare il ransomware è ricordarsi che alla base vi è un reale problema legato alla gestione dei rischi e non solo una complessità tecnica. Questo deve portare ad aumentare l'adozione dell'assicurazione informatica, ma l'idoneità a tale tipo di copertura comporta domande e requisiti aggiuntivi, oltre che indubbi vantaggi.

L'assicuratore informatico probabilmente necessiterà di informazioni circa l'igiene informatica complessiva implementata in azienda, ad esempio i criteri di sicurezza adottati, registri di backup, del controllo degli accessi e il registro eventi. Potrebbe inoltre suggerire di investire in strumenti di gestione importanti oltre che di nominare un team addetto alla risposta agli incidenti, se non è già presente. Potrebbe inoltre fornire le risorse utili per formare i dipendenti su phishing e altre minacce.

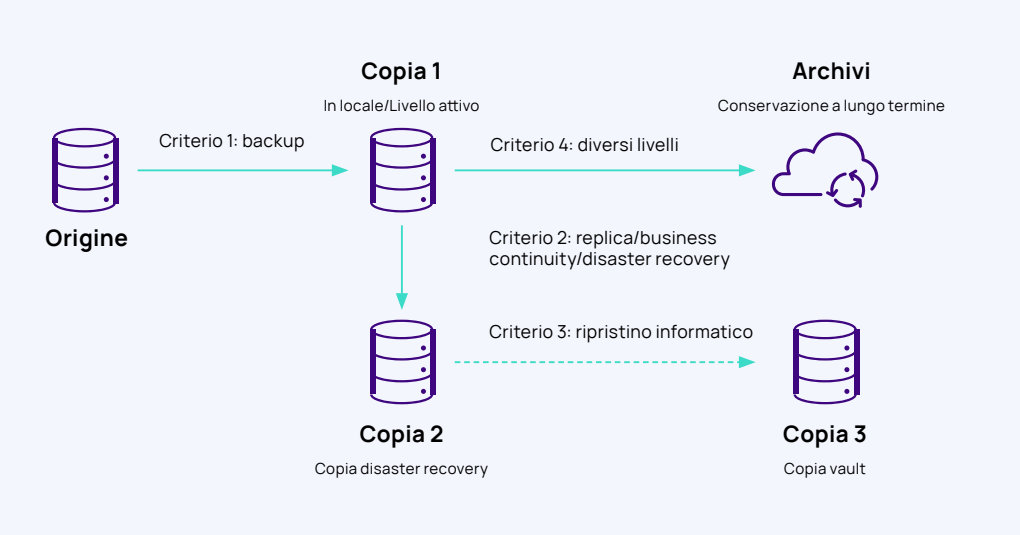
Anche solo prepararsi a ottenere tutti i requisiti necessari per sottoscrivere una polizza assicurativa informatica potrebbe migliorare l'approccio alla sicurezza presente in azienda.

La resilienza informatica non richiede complessità

La maggior parte dei tradizionali prodotti per il backup è stata concepita per disastri naturali e fisici e i tentativi per adattarli ai moderni ripristini informatici comporterebbero ulteriori complessità e altre copie di dati di backup, archiviate in altri luoghi. In realtà, non sono necessarie altre copie e ulteriori complessità per prepararsi al ripristino da ransomware. Di fatto, un'architettura di protezione dei dati basata su cloud riduce le vulnerabilità rimpicciolendo la superficie di attacco e semplificando al contempo la procedura di ripristino.

I prodotti per il backup tradizionali sono stati progettati per il backup in locale e memorizzano le copie di backup sulla rete locale. La popolare strategia di protezione dei dati "3-2-1" comportava la replica o la presenza di una seconda sede di archiviazione. Quindi, le copie di standby venivano aggiunte a un vault in attesa del ripristino. Successivamente, quando sono stati compresi i vantaggi dello storage cloud, molti fornitori di soluzioni di backup hanno implementato la possibilità di aggiungere un'altra copia ancora archiviandola su cloud. Questa catena di eventi ha comportato una serie complessa di criteri che richiedono una opportuna gestione e tempo extra del personale per gestire tutte le fasi della procedura.

Approccio tradizionale e impatto sul disaster recovery



Flusso di protezione:

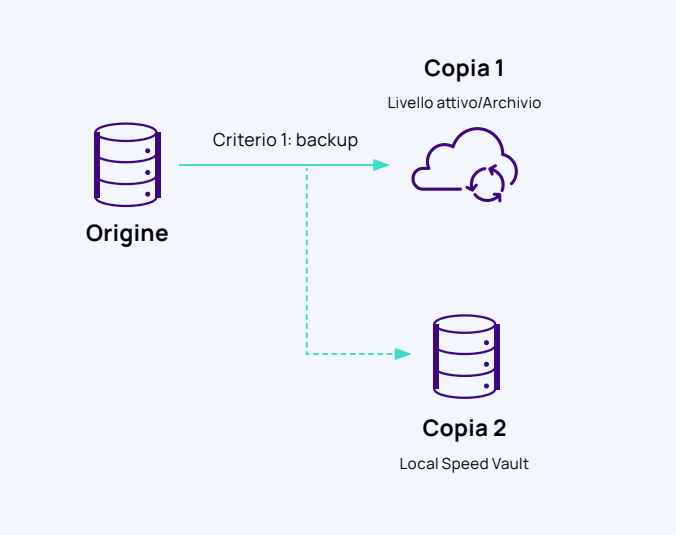
- Come faccio a coordinare i quattro criteri?
- Chi gestisce la procedura e di quante persone ho bisogno?
- Necessito di fino a quattro destinazioni?
- Gestione delle patch?
- Quali copie devono essere non modificabili?
- Come proteggo l'infrastruttura di backup della rete principale?

Flusso di ripristino:

- Come faccio a creare un runbook di disaster recovery/ripristino istantaneo per questo?
- Prendi in considerazione una discussione informale per questo aspetto.
- Ripristino del catalogo di backup se compromesso in produzione?

Per contro, un'architettura moderna e basata su cloud invia ogni backup direttamente al cloud per impostazione predefinita, memorizzando le copie principali di backup all'esterno della rete locale, al riparo da ransomware. Puoi scegliere di tenere una seconda copia in locale per il ripristino rapido, ma anche con questa aggiunta, l'approccio semplifica significativamente i criteri e riduce i costi operativi.

Approccio alternativo e impatto sul disaster recovery



Flusso di protezione:

- Criteri semplificati
- Complessità e carico di gestione ridotti
- Importanza della preparazione a disaster recovery/ripristino istantaneo
- Riduzione del numero di copie ››› Riduzione dei costi
- Vantaggi della gestione delle patch come servizio
- Copie off-site per impostazione predefinita

Flusso di ripristino:

- Topologia e procedure di disaster recovery semplificate ››› Runbook di disaster recovery/ripristino istantaneo semplificato
- Opzioni flessibili di ripristino per una serie di disastri
- Riduzione della superficie di attacco per ridurre le probabilità di dover ricreare il catalogo di backup

Riduzione delle dimensioni della superficie di attacco

I criminali informatici tenteranno di avere accesso alla tua rete in una serie di modalità. Sono diversi i vettori di attacco comunemente utilizzati rispetto ai quali le applicazioni di backup on premise tradizionali restano vulnerabili. Alcuni gruppi e tecniche cercano specificamente nella rete locale i file di backup di fornitori noti e li eliminano o li sottopongono a crittografia, sbarrando di fatto una strada per il ripristino[3]. Potrebbero anche eliminare o disabilitare il server applicazioni di backup.

Optando per la protezione dei dati basata su cloud come servizio, puoi ridurre la vulnerabilità agli attacchi ransomware in tre modi:

- Memorizzando le copie di backup principali nel nostro cloud privato, esternamente alla rete locale e al riparo da ransomware.
- Le applicazioni SaaS, infatti, non dispongono di alcun server di backup locale interno alla rete.
- L'autenticazione a due fattori obbligatoria limita gli accessi non autorizzati ai backup.

>>> **Per saperne di più sui suggerimenti di Arcas Risk Management** per prepararsi a un attacco ransomware, guarda questo webinar on-demand: https://youtu.be/ON28_27swlo.

>>> **Per scoprire come la protezione dei dati basata su cloud come servizio di Cove Data Protection** riduce la superficie di attacco, dai uno sguardo a questo breve video: https://youtu.be/c-rHzx-qqTM.

Informazioni su N-able

N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e a espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore. n-able.com/it

[1]https://www.digitalshadows.com/blog-and-research/ransomware-in-q2-2022-ransomware-is-back-in-business

[2]https://www.infosecurity-magazine.com/news/most-ransomware-victims-hit-again/

[3]https://threatpost.com/conti-ransomware-backups/175114/