La tua guida completa ai ransomware: scopri le best practices e salva la tua azienda

Cubbit Next Generation Cloud Pioneers

La più grave minaccia per la tua azienda

Ad oggi i ransomware rappresentano il problema più comune e insidioso per le aziende. Secondo l'agenzia di cyber sicurezza Purple Sec, questo tipo di attacco informatico è incrementato del 64% nella prima metà del 2021, con un **riscatto medio di $570.000**. Oltre metà delle vittime paga il riscatto, ma solo ¼ riacquisisce i propri dati. Il danno cresce ulteriormente se consideriamo che - riporta Gartner - il server downtime ha un costo medio di $5600 al minuto, pari a oltre $300.000 l'ora. Quella dei ransomware è dunque una seria minaccia, che affligge ogni tipo di impresa. Un'azienda ne cade vittima una volta ogni 14 secondi. Una su cinque è una PMI.

Come correre ai ripari? La NATO, il G7, il governo federale USA e l'esercito degli Stati Uniti hanno recentemente riconosciuto i ransomware come un pericolo non solo per l'economia ma anche per la sicurezza nazionale. Ma se la risposta coordinata delle istituzioni fornisce certo un solido aiuto, essa è insufficiente, ad oggi, a prevenire questo attacco su larga scala. La significativa carenza di personale qualificato unita alla costante crescita del numero di malware fa sì che le imprese, soprattutto quelle più piccole, siano **sole e impreparate di fronte a una tale minaccia.**

È dunque necessario che ogni imprenditore si faccia carico in prima persona di gestire questo problema, istruendosi sugli errori più comuni e le più efficaci strategie di disaster recovery per salvare la propria azienda. Questa guida contiene tutte le informazioni utili a tale scopo.

I 3 errori sui ransomware che (quasi) tutte le aziende commettono

#1 Patch di sicurezza non aggiornate

Una patch è un aggiornamento software volto a migliorare un programma. Nel contesto della cyber sicurezza è di assoluta importanza che le patch siano aggiornate per evitare violazioni di sistema. Qualsiasi sistema informatico, che si tratti di hardware, software o infrastrutture complesse, richiede un'attenzione costante affinché possa dirsi sicuro. Come indicato nel recente report del National Institute of Standards and Technology (NIST), **il numero di vulnerabilità scoperte nel solo 2021 è di 18.378** - equivalente a più di 50 al giorno. I sistemi informatici operano in un ambiente ostile, in cui organizzazioni di hacker "blackhat", ossia malevoli, fanno dei ransomware il loro business. Per questa ragione, aggiornare i propri protocolli di sicurezza regolarmente è la prima linea di difesa.

Anche una singola vulnerabilità non corretta può condurre a perdite catastrofiche. È questo il caso di un'organizzazione - il cui nome, per ragioni di privacy, non è stato reso noto - che nel marzo 2022 è stata vittima di un attacco da parte di BlackCat, uno dei gruppi più attivi al mondo. Causa dell'incidente, citato nel research paper dell'agenzia Forescout, che ha partecipato alle indagini, è stata una singola falla di sicurezza. Grazie a essa gli hacker hanno effettuato una *SQL injection*, impadronendosi di buona parte del network. Una patch per la vulnerabilità in questione esisteva dal 2019; ciononostante, l'azienda non aveva mai provveduto ad applicarla.

#2 Penetration testing inadeguato

Con penetration testing si intende un modello di valutazione di una rete o applicazione che consiste nel testare l'oggetto dell'analisi "sul campo", ossia cercando di violarne la sicurezza tramite un attacco. Il vantaggio di questa metodologia è che obbliga a ragionare come un hacker, svelando vulnerabilità che diversamente non risultano apparenti. Simulando un attacco vero e proprio, è possibile inoltre mettere alla prova i tempi e le capacità di risposta, assicurando la business continuity.

Secondo una ricerca condotta da Informa Tech, il penetration testing è inadeguato anche nelle più grandi aziende. Solo il 38% delle imprese con 3000 dipendenti o più testa più di metà della sua superficie di attacco. È comune, per aziende così grandi, avere oltre 10.000 asset connessi a internet. Ciononostante, **meno del 10% di questi asset sono oggetto di**

penetration testing. In aggiunta, il 45% conduce simili analisi solo una o due volte l'anno, con il risultato che i dati dell'azienda, inclusa la sua proprietà intellettuale, sono esposti al rischio crescente di ransomware potenzialmente distruttivi.

#3 L'assenza di un backup immutabile

L'obiettivo numero uno di qualsiasi criminale informatico che opera nel business dei ransomware è crittografare non solo dati e metadati di uso corrente, ma anche ogni eventuale copia di backup. Se difatti l'hacker riesce in tale impresa, le sue probabilità di estorcere denaro con successo aumentano considerevolmente. Onde evitare che questo accada, sempre più aziende si affidano a una tipologia di backup detta backup immutabile. Il backup immutabile, altresì detto resiliente, non può essere distrutto dall'avversario nemmeno in caso egli abbia acquisito privilegi di root.

Questo è possibile giacché il backup immutabile è fisicamente e digitalmente isolato dagli altri dati — è, in altre parole, offline e custodito in un luogo diverso da quello in cui sono conservate le altre copie. Così facendo, se anche l'hacker riuscisse a violare il sistema informatico non avrebbe comunque accesso al backup immutabile, dal momento che esso non è parte dello stesso network in cui si trovano tutti gli altri dati. Il backup immutabile è pertanto fondamentale in qualsivoglia strategia di prevenzione. In presenza di una copia resiliente di tutto il sistema, l'azienda può effettuare un **ripristino completo in maniera automatica e repentina**, senza che il ransomware costituisca mai un problema.

La mancanza di un backup immutabile può fare la differenza tra il successo e il fallimento. Secondo il recente report di Hosting Tribunal, ogni cinque anni il 20% delle PMI incappa in una perdita di dati. **Nel 60% dei casi, tale perdita porta al fallimento dell'azienda entro sei mesi.**

Le best practices per una disaster recovery garantita

#1 Seguire il principio del privilegio minimo

Il principio del privilegio minimo, o PoLP (dall'inglese, principle of least privilege), è una regola seconda la quale ogni modulo computazionale deve avere privilegi di accesso solo alle risorse necessarie al suo funzionamento. Per estensione, ogni utente deve avere accesso solo a ciò di cui ha assolutamente bisogno per eseguire i propri compiti. Quanto più frequentemente l'accesso non necessario viene fornito, tanto peggiori saranno le conseguenze qualora l'account di uno o più utenti venisse compromesso.

Ogni catena è forte quanto il suo anello più debole. Per analogia, la sicurezza di qualsiasi sistema informatico è direttamente proporzionale alla sicurezza degli amministratori di sistema. **Ecco perché il principio del privilegio minimo è la base per minimizzare l'esposizione al rischio.** Una delle più effettive misure di protezione in questo contesto è l'utilizzo di endpoint e entry point per tutti i dispositivi all'interno dell'azienda. In questo modo è possibile garantire un accesso granulare e selettivo, limitando eventuali danni. Tale pratica è uno strumento cardine nella prevenzione del phishing, ad oggi tra i più comuni metodi di violazione, recentemente tornato in auge secondo la compagnia di cyber sicurezza Proofpoint.

#2 Applicare la 3-2-1 backup rule

La 3-2-1 backup rule è universalmente riconosciuta come il fondamento di una gestione dei dati sicura. **Secondo l'agenzia di intelligence americana CISA, "tutte le aziende dovrebbero utilizzare la 3-2-1 backup rule."**

Promossa da Veeam e da tutti i principali fornitori di servizio, la 3-2-1 backup rule consiglia di:

- Conservare almeno tre copie dei dati importanti.
- Su almeno due differenti tipi di supporto.
- Con almeno una di queste copie custodita off-site.

L'applicazione di questa semplice regola riduce sostanzialmente le probabilità di incorrere in una perdita di dati catastrofica. Ogni copia infatti ha una intrinseca probabilità di rompersi dovuta all'usura, incidenti e problemi non preventivati. Ne consegue che all'aumentare del numero delle copie scende di pari misura la probabilità che tutte le copie vadano distrutte o perdute.

#3 Scegliere un Object Storage S3 con manutenzione completa e continua

Per complementare la propria sicurezza, la migliore strategia è quella di affidarsi a un fornitore di servizi con elevata expertise in materia. Per essere idoneo, il fornitore deve essere in grado di offrire una piattaforma dotata dei seguenti requisiti:

- **Affidabilità**: il fornitore deve essere affidabile. Nella crittografia esiste un detto: "don't roll your own crypto" — ossia, non usare in produzione un protocollo crittografico che non sia stato testato precedentemente. Lo stesso concetto è applicabile anche nella sicurezza in senso lato: mai affidare la sicurezza dei dati e della proprietà intellettuale a un fornitore che non abbia dimostrato la propria credibilità.

- **Sicurezza**: il fornitore deve essere in carico della sicurezza della piattaforma. A tale scopo deve fare penetration testing continuo su tutta la superficie di attacco, verificando costantemente la presenza di eventuali vulnerabilità nonché implementando e, quando risulta necessario, progettando patch ad hoc per proteggere l’azienda.

- **Scalabilità**: che l'azienda utilizzi un'infrastruttura on-premises, cloud, IaaS o SaaS e/o si affidi a container, essa deve essere messa in condizione di focalizzarsi sul proprio business, senza che la gestione dei dati sia d'ostacolo. È fondamentale pertanto che la piattaforma possa scalare in qualsiasi condizione ambientale,

integrando i dati in maniera *seamless*, indipendentemente dalle soluzioni già utilizzate dall'azienda.

L'integrazione è il requisito primario per gestire i propri dati in maniera scalabile e al contempo rispondere ai ransomware in real-time. Ecco perché è essenziale che il servizio offerto si basi su un Object Storage S3 compatibile con l'intero ecosistema AWS Amazon S3, il framework più efficiente, scalabile e sicuro per la gestione dei dati.

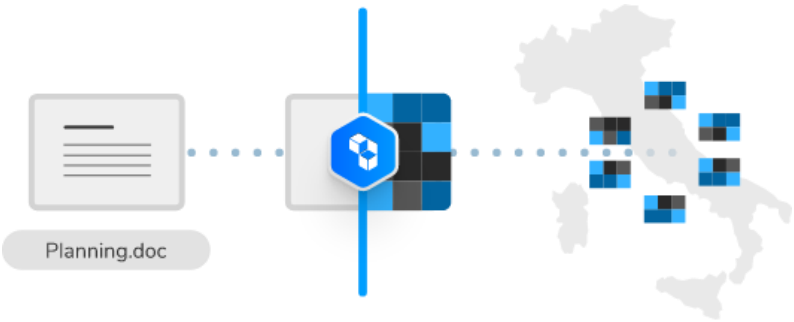
La rete anti-ransomware di Cubbit: il massimo in affidabilità, sicurezza, e scalabilità

Cubbit è il primo cloud distribuito d'Europa. Partner di Gaia-X, Cubbit è supportata da investitori di prim'ordine quali la Commissione Europea, Barclays, Techstars, CERN e Cassa Depositi e Prestiti. Insieme a **50+ aziende leader italiane**, tra le quali sono incluse Amadori, Bonfiglioli, SCM Group e numerose cooperative, Cubbit ha creato la prima e unica rete di cloud distribuito d'Europa, **technology trend del decennio secondo Gartner.** La rete Cubbit si fonda sui valori della collaborazione, sicurezza e sovranità del dato e protegge, ad oggi, decine di milioni di data points.

Diversamente dal cloud tradizionale, Cubbit non si affida a data center proprietari, bensì a una **rete di nodi sotto il controllo dei propri utenti** — una rete distribuita, potenziata dall'Intelligenza Artificiale e protetta da tecnologia zero-knowledge e crittografia di grado militare. Questa innovativa architettura garantisce tre benefici:

- Disaster recovery garantita con backup anti-ransomware distribuito.
- Integrazione seamless tramite Object Storage S3 Compatible.
- Collaborazione sicura e privata grazie al Sync & Share a tecnologia zero-knowledge.

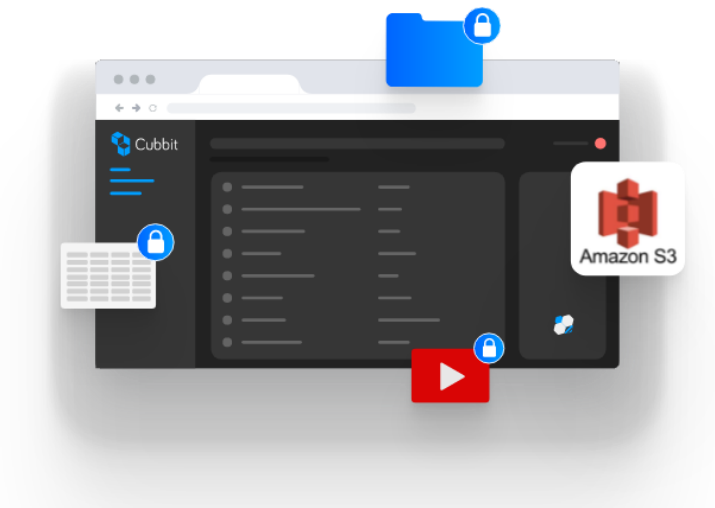
Backup distribuito



Il cloud tradizionale centralizza i tuoi dati, esponendoti al rischio di ransomware, leak e catastrofi naturali. Cubbit invece cifra, frammenta e distribuisce ogni tuo dato su una rete a perimetro italiano, senza single point of failure. Questo ti garantisce disaster recovery e business continuity — sempre, qualsiasi cosa accada.

Ogni copia all'interno della rete Cubbit è una copia off-site su un supporto unico, la qual cosa rende Cubbit un **potenziamento della 3-2-1 backup rule**. In aggiunta, la rete Cubbit è soggetta a **penetration testing** continui e **manutenzione costante** e completa per garantire la piena e totale sicurezza.

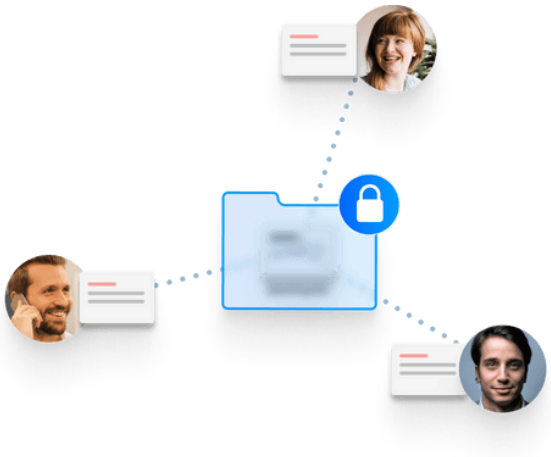
Object Storage S3 Compatible



Sfrutta le nostre API e liberati dal vendor lock-in una volta per tutte. Scalabile, sicuro e compatibile con l'intero ecosistema Amazon S3, il cloud object storage di Cubbit ti offre movimentazioni e accessi illimitati a un prezzo fisso e trasparente.

IoT, multimedia, logging: qualunque sia il tuo use case, il nostro **data lake** ti permette di archiviare e recuperare tutti i dati puntuali di cui necessiti per le tue analisi. Finalmente puoi sfruttare l'Object Storage S3 con una strategia multi cloud e trasferire grandi moli di dato da un cloud all'altro gratuitamente — minimizzando il rischio di downtime.

Collaborazione sicura e privata in Sync & Share



Collabora su file e cartelle in totale sicurezza, anche con chi non ha un account Cubbit. Accedi da ovunque, senza la necessità di una VPN aziendale. Dormi tranquillo sapendo che, grazie alla nostra crittografia zero-knowledge, nessuno può accedere ai tuoi dati senza il tuo consenso, nemmeno noi.

Ogni utente della rete ha un accesso granulare, basata sul principio del privilegio minimo. L'architettura distribuita del network, combinata con la crittografia zero-knowledge di Cubbit, ti garantisce che i dati rimarranno disponibili e immutati. Per violare la tua sicurezza, un hacker dovrebbe violare l'Intelligenza Artificiale Cubbit e **ogni nodo della rete in cui i tuoi dati sono archiviati**. Infine dovrebbe violare AES-256, la qual cosa richiede più tempo dell'età dell'universo.

Vuoi saperne di più su Cubbit?

Contattaci

Il nostro team di esperti sarà felice di rispondere alle tue domande e aiutarti a capire come Cubbit può aiutare la tua azienda.

> *Next Generation Cloud di Cubbit ci è dunque sembrata la piattaforma giusta per dirottare almeno parte delle esigenze di storage in cloud verso una soluzione italiana e intrinsecamente sicura.*

Enrico Andrini - CDO, Bonfiglioli [La storia]

L’azienda

Cubbit, partner di Gaia-X, è un’azienda italiana e la prima scaleup in Europa ad aver lanciato un **cloud distribuito e zero-knowledge** - un nuovo modo di archiviare i dati basato su un modello data center-less.

Gartner identifica il cloud distribuito come uno dei **Top Strategic Technology Trends del prossimo decennio**. Al posto di data center, **Cubbit forma un cloud cooperativo basato sui principi del Web 3**: ogni server, computer, device può essere riciclato e diventare un nodo della rete. Cubbit garantisce **il più alto livello di sicurezza, privacy by-design e sovranità del dato**, mentre riduce l’impatto ambientale fino a 10x ed offre servizi economicamente competitivi.

Nata nel 2016 e cresciuta tra l'Italia e Tel Aviv, ad oggi Cubbit conta **+5,500 clienti b2c e b2b** in 70 paesi del mondo e ha raccolto **€10M+ di investimenti**. Tra i suoi partner e investitori globali ci sono: Barclays, Techstars, Azimut, CDP Venture Capital Sgr, Primo Ventures, Gellify, IAG, CERN, EIT Digital, Gaia-X and the European Commission.

Ad inizio 2022, Cubbit ha lanciato Next Generation Cloud Pioneers: la prima rete B2B di cloud distribuito in Europa — una soluzione tecnologica che garantisce disaster recovery by design. **50+ aziende italiane cooperano con Cubbit** per portare in Europa un nuovo modo di archiviare e condividere i dati.

Cerchiamo Pionieri che vogliano adottare e veder crescere questa nuova tecnologia: **il programma è ideale per CEO, CMO, CIO, CTO e IT Manager** che vogliono **intercettare** il nuovo trend tecnologico del **cloud distribuito**.

Cubbit

Cubbit ha sede a Bologna, con una filiale a Tel Aviv, Israele.

Telefono: +39 347 97 33 457
Email: hello@cubbit.io
Website: https://ngc.cubbit.io/
Ufficio registrato: Via della Zecca 1 - 40121 - Bologna (BO) - Italy
Indirizzo per consegne e meeting: Via Altabella 17 - 40125 - Bologna (BO) - Italy