INFINIDAT

CRESCIUTI DEL 65% GLI ATTACCHI INFORMATICI IN ITALIA: PER LE AZIENDE DIVENTA INDISPENSABILE L'ATTUAZIONE DI UNA STRATEGIA DI SICUREZZA COMPLETA ED EFFICACE

Dopo il regolamento DORA e la direttiva NIS2, il NIST ha rilasciato la versione 2.0 del proprio Cybersecurity Framework (CSF).

Milano, 12 giugno 2024 – Gli attacchi informatici stanno aumentando in tutto il mondo e l'Italia non fa eccezione. Secondo il Rapporto Clusit 2024, presentato il marzo scorso, gli attacchi cyber nel nostro Paese nel 2023 sono aumentati del 65% rispetto all'anno precedente. Sanità, Finanza e Manifatturiero risultano i settori più colpiti. In questo scenario, il semplice backup non è più sufficiente a proteggere i propri dati, perché i cyber-criminali sono in grado di attaccare anche il backup e l'infrastruttura di storage che ospita queste soluzioni. Per questo motivo, poter contare su una strategia completa di Cyber storage resilience e ripristino dei dati è essenziale per un efficiente piano di sicurezza informatica.

Per far fronte a questa situazione, negli ultimi anni, l'UE è scesa in campo su più fronti per promuovere la cyber resilienza, combattere la criminalità e rafforzare la protezione dei sistemi informatici. Ne sono un chiaro esempio il Digital Operational Resilience Act (DORA), sviluppato per consolidare e armonizzare a livello europeo i principali requisiti di cybersecurity con focus sul settore finanziario, e la direttiva NIS2, che ha introdotto misure specifiche e più stringenti in termini di cyber risk management, di segnalazione e condivisione delle informazioni relative agli incidenti di sicurezza.

A fianco di questi due utilissimi strumenti, il 26 febbraio 2024, è stata pubblicata oltreoceano la versione 2.0 del Cybersecurity Framework (CSF) dal National Institute of Standards and Technology (NIST). La nuova versione di uno dei framework di sicurezza maggiormente adottati a livello mondiale, mantiene lo stesso approccio pragmatico della precedente, introducendo però alcuni aggiornamenti chiave.

La modifica principale consiste nell'ambito di applicazione. Quest'ultimo è stato, infatti, aggiornato per abbracciare un più ampio numero di settori, a differenza della versione originale sviluppata specificatamente per le infrastrutture critiche. Questo nuovo approccio, più inclusivo, permette al Framework di essere utilizzato da organizzazioni di tutte le dimensioni e settori, tra cui industria, governo, università e organizzazioni non profit, indipendentemente dal livello di maturità dei loro programmi di cybersecurity. Un cambiamento che si sposa perfettamente con le evoluzioni normative del settore, che impongono un'attenzione sempre crescente sull'adozione di strumenti tecnici idonei alla tutela di tutti i sistemi informatici.

INFINIDAT

Un'altra novità fondamentale è l'introduzione di una funzione di governance per la gestione del rischio. Se svolta correttamente ed efficacemente, un'azione di governance, secondo il NIST, "stabilisce, comunica e monitora la strategia, le aspettative e le politiche di gestione del rischio di cybersecurity". Questo sesto pilastro va ad aggiungersi ai cinque già presenti nella precedente versione (identificare, proteggere, rilevare, rispondere e recuperare), per fornire delle indicazioni mirate su come le aziende possano prendere e attuare decisioni interne volte a sostenere la propria strategia cyber.

"*I dati relativi all'Italia e riportati dal nuovo rapporto Clusit sono allarmanti. Il numero degli attacchi informatici non accenna a diminuire e per le organizzazioni la gestione dei rischi legati alla cybersecurity è diventata una questione di massima priorità, sia che si tratti di aziende, pubblica amministrazione o università. Per prepararsi ad affrontare le minacce di attacchi sempre più sofisticati, è fondamentale sviluppare una strategia mirata, che garantisca il giusto livello di resilienza informatica. È indubbio, infatti, che le infrastrutture IT stiano diventando sempre più complesse, con un conseguente aumento delle probabilità di errori o guasti e un ampliamento della superficie di attacco, terreno fertile per tutti i cyber criminali. A tal fine, strumenti come il Regolamento DORA, la Direttiva NIS2 e la recente versione aggiornata del Cybersecurity Framework del NIST forniscono utilissime linee guida da seguire. Ma prima di tutto le aziende dovrebbero esser in grado di cambiare il proprio approccio organizzativo, che da reattivo deve diventare proattivo. Per questo motivo molti clienti sono alla ricerca di soluzioni che possano aiutarli a effettuare questo cambiamento e a raggiungere la corretta resilienza IT. Da tempo Infinidat fornisce soluzioni di storage enterprise che garantiscono sia resilienza informatica sia cyber detection e soddisfano i requisiti richiesti dal NIST. Con la tecnologia InfiniSafe® supportiamo le aziende nell'abilitazione di una solida cyber resilience, garantendo un ripristino dei dati quasi istantaneo. Le funzionalità di cyber recovery fanno parte della lunga serie di caratteristiche di resilienza informatica offerte da Infinidat, che includono snapshot immutabili, air-gapping logico, ambiente forense isolato/separato e cyber detection. Inoltre, grazie alla nuova funzionalità di* ***Automated Cyber Protection (ACP) di InfiniSafe®*** *siamo oggi l'unico fornitore di storage a offrire una soluzione di protezione informatica automatizzata per lo storage enterprise e in grado di integrarsi perfettamente con i software delle applicazioni di cybersecurity (SIEM e SOAR). Un incidente o un evento legato alla sicurezza attiva immediatamente snapshot automatici e immutabili dei dati, aiutando così le aziende a resistere e a reagire rapidamente agli attacchi informatici e a identificare potenziali attacchi latenti. InfiniSafe Automated Cyber Protection è la funzionalità di sicurezza proattiva di cui le aziende hanno bisogno per includere lo storage enterprise in una strategia completa volta a contrastare le minacce informatiche. Automated Cyber Protection, infatti, migliora la resilienza informatica complessiva, riducendo la finestra di minaccia e minimizzando l'impatto dei cyberattacchi per gli ambienti di storage enterprise",* ha commentato **Donato Ceccomancini, Country Manager di Infinidat Italia.**

INFINIDAT

Informazioni su Infinidat

Infinidat offre alle aziende e ai service provider un'architettura di storage primario e secondario che rende disponibile in maniera nativa tutte le funzionalità e i servizi dati tramite InfiniVerse. Questa piattaforma unica garantisce straordinari vantaggi operativi per l'IT e supporta i moderni carichi di lavoro in ambienti on-premise e ibridi multi-cloud. L'infrastruttura cyber resiliente di Infinidat, i modelli di utilizzo a consumo con prestazioni garantite, la disponibilità al 100% e gli SLA garantiti per la cybersecurity sono in linea con le priorità IT e di business delle aziende. I pluripremiati servizi dati della piattaforma e l'acclamato servizio con i "guanti bianchi" di Infinidat sono costantemente raccomandati dai clienti, come riconosciuto anche nelle recensioni raccolte dal Gartner® Peer Insights. Ulteriori informazioni su Infinidat sono disponibili su www.infinidat.com/it

Ufficio Stampa
Meridian Communications Srl
Via Cuneo, 3 – 20149 Milano Tel. +39 02 48519553

Silvia Ceriotti	335 7799816	silvia.ceriotti@meridiancommunications.it
Viviana Bandieramonte	329 4776937	viviana.bandieramonte@meridiancommunications.it
Ilaria Malgrati	339 2143042	ilaria.malgrati@meridiancommunications.it