cpl.thalesgroup.com/it

THALES
Building a future we can all trust

Soluzioni di Thales per prevenire attacchi ransomware

Adeguamento delle soluzioni Thales al Cybersecurity Framework e alle linee guida sulla prevenzione degli attacchi ransomware di NIST

Gli attacchi ransomware sono un problema da anni, ma recentemente sono diventati molto più dannosi: i criminali prendono di mira qualunque tipo di sistema, dalle infrastrutture critiche agli ospedali e ai commercianti, chiedendo riscatti da decine di milioni di dollari. Oggi, mentre i leader globali discutono di questi attacchi in vertici di alto profilo, le agenzie governative stanno assumendo un ruolo attivo nell'educazione e nella fornitura di risorse ad aziende e organizzazioni per aiutarle a proteggersi dagli attacchi.

Linee guida NIST per la prevenzione degli attacchi ransomware

Il NCCoE (National Cybersecurity Center of Excellence), sotto l'egida del NIST (National Institute of Standards and Technology) statunitense, ha rilasciato una guida su come identificare e proteggere le risorse contro gli attacchi ransomware. La SP (Special Publication) sulla sicurezza informatica 1800-25 definisce le misure per una strategia globale di protezione delle risorse. Mostra anche che non esiste un metodo infallibile per affrontare la minaccia rappresentata dagli attacchi ransomware.

Soluzioni di Thales per la prevenzione degli attacchi ransomware

Le soluzioni di Thales per la protezione dei dati e la gestione degli accessi forniscono alcune delle componenti più essenziali del Cybersecurity Framework proposto dal NIST per proteggere le organizzazioni dagli attacchi ransomware. Il portfolio leader di settore di Thales offre alle organizzazioni la possibilità di:

- Scoprire i dati sensibili e classificarli in base al rischio
- Implementare un controllo solido delle identità e della gestione degli accessi
- Proteggere e controllare i dati sensibili a riposo e in transito attraverso la crittografia e la tokenizzazione
- Monitorare la sicurezza dei dati per un risanamento intelligente

Di seguito riportiamo uno schema di come le nostre soluzioni si adeguano al Cybersecurity Framework e alle linee guida di NIST sugli attacchi ransomware:

Adeguamento delle soluzioni Thales al Cybersecurity Framework e alle linee guida sugli attacchi ransomware di NIST

Categoria	Requisito	Soluzioni di Thales
IDENTIFICAZIONE **Valutazione dei rischi (ID.RA)**	ID.RA-1: documentazione e identificazione delle vulnerabilità delle risorse.	**CipherTrust Data Discovery and Classification** rileva i dati sensibili regolati, strutturati e non, che si trovano nel cloud, in big data e data store tradizionali. Un pannello unico di controllo fornisce informazioni sui dati sensibili e sulle relative vulnerabilità, consentendo decisioni migliori per colmare le lacune nella sicurezza, privilegiare azioni di risanamento e garantire la trasformazione del cloud e la condivisione dei dati di terze parti.
PROTEZIONE **Controllo degli accessi (PR.AC)**	PR.AC-1: le identità e le credenziali sono emesse, gestite, verificate, revocate e sottoposte ad audit per dispositivi, utenti e processi autorizzati. PR.AC-3: gestione degli accessi da remoto. PR.AC-4: vengono gestiti i permessi e le autorizzazioni di accesso, incorporando i principi del privilegio minimo e della separazione delle responsabilità.	**SafeNet Trusted Access fornisce una gestione centralizzata degli accessi** che permette alle aziende di attuare criteri di autenticazione coerenti in tutte le piattaforme, automatizzando e semplificando la distribuzione e la gestione di un patrimonio distribuito di token e proteggendo allo stesso tempo un ampio spettro di risorse on-premises, basate sul cloud o virtualizzate. **SafeNet Trusted Access offre inoltre un'autenticazione multi-fattore commerciale in pronta consegna** con la gamma più ampia di metodi di autenticazione e fattori di forma. Ciò permette ai clienti di affrontare svariati casi d'uso, livelli di assicurazione e vettori di minacce grazie a criteri unificati e gestiti in maniera centralizzata direttamente da un back-end di autenticazione distribuito on-premises o nel cloud. **CipherTrust Transparent Encryption offre controlli granulari degli accessi** ai dati business-critical per definire chi ha accesso a file o cartelle specifiche protette e le operazioni che possono eseguire. • Impedisci agli utenti amministrativi di sfruttare i loro privilegi per accedere in lettura a file o database sensibili. • Implementa rigide politiche di controllo degli accessi agli archivi di backup e crittografa i backup per impedire l'esfiltrazione dei dati. • Implementa una separazione dei compiti in modo tale da permettere agli utenti del database di ottenere accesso a lettura / scrittura lasciando al software di backup l'accesso esclusivamente di lettura a quello stesso database.

Categoria	Requisito	Soluzioni di Thales
PROTEZIONE **Protezione dei dati (PR.DS)**	PR.DS-1: Protezione dei dati a riposo.	**La CipherTrust Data Security Platform** unifica data discovery, classificazione e protezione dei dati, nonché controlli granulari degli accessi senza precedenti con una gestione delle chiavi centralizzata, il tutto da un'unica piattaforma. Ne risulta una riduzione delle risorse dedicate alle operazioni di sicurezza dei dati, ai controlli onnipresenti di conformità, ma anche un rischio minore per tutta l'organizzazione. • **CipherTrust Transparent Encryption** fornisce una crittografia dei dati a riposo, controlli degli accessi degli utenti privilegiati e registrazioni dettagliate degli accessi ai dati senza modifiche alle applicazioni esistenti. Permette alle organizzazioni informatiche di implementare criteri per impedire a processi canaglia e utenti non autorizzati di crittografare i tuoi dati più sensibili e impedire altresì l'esposizione di dati sensibili in caso di esfiltrazione, proteggendo quindi le organizzazioni dagli attacchi ransomware. Gli agenti proteggono dati in file, volumi e database su sistemi operativi Windows, AIX e Linux in server fisici e virtuali in ambienti cloud e big data. • **CipherTrust Application Data Protection** fornisce funzioni crittografiche come servizi di gestione delle chiavi, firma e crittografia attraverso API, in modo che gli sviluppatori possano facilmente proteggere i dati presso il server dell'applicazione o il nodo big data. • **CipherTrust Tokenization** offre soluzioni con e senza vault e può aiutare a ridurre i costi e le complessità associati alla conformità con gli obblighi di legge che impongono di proteggere dati come PCI-DSS. • **Le soluzioni CipherTrust Database Protection** integrano la crittografia dei dati per i campi sensibili nei database con una gestione sicura e centralizzata delle chiavi e senza la necessità di modificare le applicazioni del database. Le soluzioni CipherTrust Database Protection supportano database Oracle, Microsoft SQL Server, IBM DB2 e Teradata. • **CipherTrust Manager è il principale punto di gestione per la piattaforma**. Permette alle organizzazioni di gestire in maniera centralizzata le chiavi di crittografia, fornire un controllo granulare degli accessi e configurare i criteri di sicurezza. Gestisce infatti le attività legate al ciclo di vita delle chiavi come la generazione, la rotazione, l'eliminazione, l'importazione e l'esportazione, fornisce alle chiavi e ai criteri un controllo degli accessi basato sui ruoli, supporta audit e report validi e offre REST API facili da utilizzare per gli sviluppatori. È disponibile in fattori di forma virtuali e fisici conformi allo standard FIPS 140-2 livello 3. Gli **HSM (Hardware Security Module) Luna** generano, proteggono e gestiscono chiavi crittografiche utilizzate per proteggere dati sensibili e applicazioni critiche. Gli HSM Luna offrono il maggior numero di certificazioni del settore, tra cui Common Criteria, FIPS 140-2 livello 3, ITI e altri. Affidati completamente alla tua infrastruttura, sostenuta da una base crittografica certificata di HSM riconosciuti a livello internazionale. Gli HSM Luna di Thales stabiliscono una root of trust per tecnologie esistenti ed emergenti tra cui la PKI (Public Key Infrastructure) e garantiscono l'archiviazione sicura di chiavi utilizzate nella firma del codice per mantenerne l'integrità. Thales offre anche una soluzione di firma del codice personalizzata basata su HSM Luna, container e API REST, disponibile on-premises, come servizio HSM cloud e in ambienti ibridi. **La protezione dati on-demand (DPoD)** è una piattaforma basata sul cloud che fornisce un'ampia gamma di servizi HSM cloud e di gestione delle chiavi grazie a un semplice marketplace online.

Categoria	Requisito	Soluzioni di Thales
PROTEZIONE **Data Security (PR.DS)**	PR.DS-2: Protezione dei dati in transito.	Gli **HSE (High Speed Encryptor) di Thales** offrono la soluzione ideale comprovata e certificata per la protezione dei dati in movimento, inclusi i flussi video e vocali a tempo limitato, per aziende e organizzazioni governative: • Le soluzioni di crittografia di rete CN sono appliance hardware di rete che forniscono una crittografia indipendente dai livelli di rete (livelli 2, 3 e 4) per i dati in transito. Queste soluzioni hardware di crittografia sono certificate per FIPS 140-2 livello 3, Common Criteria, NATO e sono elencate nell'elenco DoDIN APL della difesa statunitense. • Le soluzioni CN sono appliance temprate virtuali che forniscono una crittografia solida dei dati in movimento in vettori ad alta velocità WAN e SD-WAN, utilizzando NFV (Network Function Virtualization).
RISPOSTA (RS) **Mitigazione (RS-MI)**	RS.MI-3: Le vulnerabilità recentemente individuate sono attenuate o documentate come rischi accettati.	**CipherTrust Intelligent Remediation** integra data discovery dei dati sensibili basata sul rischio con una crittografia trasparente basata sui criteri per attenuare automaticamente il rischio di esposizione ai dati. Aiuta le organizzazioni a visualizzare i rischi aziendali e automatizzare le azioni di bonifica per impedire attacchi ransomware. **SafeNet Trusted Access** permette alle organizzazioni di rispondere e mitigare il rischio di attacchi ransomware fornendo un audit trail immediato e aggiornato di tutti gli eventi di accesso a ogni sistema. Ampi report automatizzati documentano tutti gli aspetti dell'applicazione e dell'autenticazione degli accessi. Inoltre, il servizio trasmette automaticamente i log a sistemi SIEM esterni.

Una serie completa di soluzioni per soddisfare il Cybersecurity Framework di NIST

Anche se le soluzioni di Thales forniscono alcune delle funzionalità più essenziali nel Cybersecurity Framework di NIST, nessun'azienda singola è in grado di fornire una serie di soluzioni veramente complete per soddisfare ogni requisito. È per questo che Thales vanta oltre 400 partner tecnologici leader di settore per offrire ai clienti una serie completa di soluzioni e integrazioni per soddisfare il Cybersecurity Framework di NIST. Contattaci per saperne di più su come possiamo aiutarti a impedire non solo gli attacchi ransomware, ma anche malware dannosi, minacce dall'interno e altre minacce persistenti avanzate.

Informazioni su Thales

Thales, leader di mercato nella protezione dei dati, gode della fiducia di governi e aziende fra le più riconosciute a livello globale che si affidano a noi per proteggere i loro dati più sensibili. Le persone a cui ti affidi per tutelare la tua privacy si affidano a loro volta a Thales per proteggere i propri dati. Le organizzazioni si ritrovano ad affrontare sempre più spesso momenti decisivi in materia di sicurezza dei dati. Qualunque sia l'obiettivo del momento, dal creare una strategia di crittografia al passare al cloud o garantire il rispetto degli obblighi di compliance, puoi contare su Thales per proteggere la tua trasformazione digitale.

> https://protect-eu.mimecast.com/s/PiuLCj2z6cvB5EKTYPE8D?domain=cpl.thalesgroup.com <

Contattaci – per tutti i recapiti e per conoscere l'ubicazione dei nostri uffici, visita https://protect-eu.mimecast.com/s/RZTMClOBECWnG0TDd0SJ?domain=cpl.thalesgroup.com