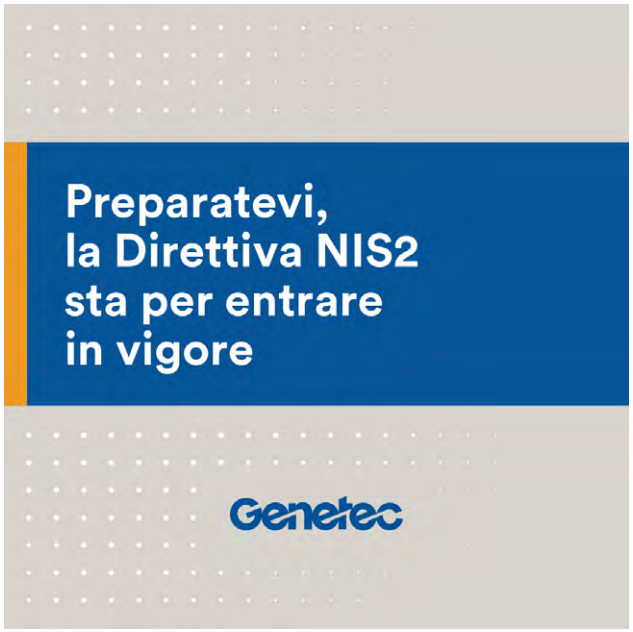
Countdown NIS2, ottobre 2024: con Genetec verso la compliance cybersecurity

comunicato aziendale



La seconda Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS2) diventa legge in tutta l'Unione Europea a ottobre di quest'anno; dunque, organizzazioni e imprese non possono farsi trovare impreparate. Riportiamo di seguito una sintesi del ***White Paper di Genetec*** *disponibile a questo* ***LINK****, per un approfondimento sul tema.*

Nel percorso verso la compliance alle norme sulla sicurezza, **Genetec** mette a disposizione una guida pratica per identificare soluzioni tempestive, ottimizzare tempistiche e investimenti a beneficio di direttori IT, responsabili operativi, responsabili della sicurezza fisica e tutti i professionisti che si occupano di gestione strutture e sicurezza. Un processo che può rappresentare una sfida enorme, ma prendere le decisioni più opportune può offrire un vantaggio, soprattutto nelle aree in cui la cybersecurity è correlata alla sicurezza fisica. NIS2, rispetto alla normativa precedente, ha allargato il campo di applicazione e ora migliaia di aziende ed enti pubblici dovranno adottare livelli più elevati di cybersecurity e processi di notifica degli incidenti, coinvolgendo, in questo iter, anche i fornitori e i partner di outsourcing. Eventuali violazioni della sicurezza saranno ora punite con sanzioni molto più severe.

Genetec ha riassunto in cinque passi il percorso verso la compliance.

1. CONTROLLO ACCESSI

Il primo passo è la valutazione dei metodi adottati per proteggere i beni, le persone e l'organizzazione dalle minacce sia fisiche e sia cybersecurity, tramite misure tecniche, come il controllo accessi e la crittografia, per proteggere i sistemi informativi.

La **gestione degli accessi fisici** può rivelarsi complessa. I team devono provvedere al provisioning delle credenziali dei dipendenti e quindi alla gestione dei diritti di accesso. Ciò può richiedere molto tempo, indurre errori ed eventuali lacune possono implicare rischi significativi per la sicurezza. In questo ambito, le soluzioni Genetec, in linea con la Direttiva NIS2 sulle misure tecniche, sono in grado di garantire che solo le persone autorizzate possano accedere in modo sicuro alle aree e alle risorse critiche consentono, per esempio, di mantenere in sicurezza le persone e le risorse lungo le aree perimetrali e negli armadietti tecnici grazie a un sistema di controllo accessi robusto, basato sui ruoli utente e sulle credenziali.

2. INCIDENTI

In base alla NIS2, i soggetti interessati da episodi di cybersecurity, con un impatto significativo sulla fornitura dei servizi, devono notificare l'incidente alle autorità competenti

con tempistiche ben precise. La normativa richiede ora **massima trasparenza su ciò che è accaduto.**
Genetec consente la gestione delle chiamate di emergenza e il coordinamento delle parti in causa, l'acquisizione dei dati critici sugli incidenti per un impact assessment accurato, mentre il supporto tecnico di Genetec può fornire competenze e risorse per qualsiasi incidente. In linea con i requisiti di segnalazione previsti dalla Direttiva NIS2, la soluzione si integra perfettamente con i sistemi di gestione degli incidenti, e automatizza l'invio delle notifiche alle autorità competenti a fronte di incidenti significativi di cybersecurity.

3. SUPPLY CHAIN FORNITORI

È importante valutare attentamente la scelta dei vendor perché il **61% delle violazioni proviene da attacchi indiretti** alle organizzazioni attraverso la loro supply chain. Un passo fondamentale è individuare fornitori in grado di rafforzare la privacy delle informazioni e la cybersecurity, ad esempio, è possibile scoprire se aderiscono a standard di sicurezza delle informazioni come l'ISO 27001.

4. OUTSOURCING

La Direttiva NIS2 obbliga le organizzazioni a mettere in atto misure per rendere sicuri i rapporti in outsourcing. Si prevede che il mercato europeo dell'outsourcing dei processi aziendali (Business Process Outsorcing-BPO) crescerà con un tasso di crescita composto (CAGR) del 7,8% dal 2023 al 2030.
Ma i vantaggi derivanti dall'outsourcing - come agilità, estensione della portata geografica e migliore scalabilità - possono passare in secondo piano se un partner espone l'impresa al rischio di una violazione della sicurezza. In questo contesto, i fornitori di servizi devono aderire a protocolli di sicurezza molto rigorosi che possono essere contenuti nella due diligence e negli accordi contrattuali.

5. ASSESSMENT

La NIS2 richiede di definire piani di risposta agli incidenti e piani di continuità operativa aziendale, inoltre, è inoltre necessario condurre valutazioni periodiche e gestire i rischi identificati. Adottare un approccio unificato alla sicurezza rappresenta sicuramente un vantaggio per affrontare le crescenti minacce.
In questo senso, la piattaforma Genetec di sicurezza integrata offre il controllo accessi, la gestione video e altre funzioni di sicurezza avanzate per proteggere i sistemi informatici. Consente di raggruppare i dati, gestire criteri di sicurezza, monitorare gli eventi e svolgere indagini, vigilando su eventuali incidenti.

Il mese di ottobre 2024 si avvicina: è fondamentale comprendere l'evoluzione del panorama delle minacce e adottare adeguate soluzioni in conformità con le nuove normative di sicurezza. Un modello di sicurezza software multilivello può aiutare a ridurre i rischi e a rispettare le norme implementando le migliori pratiche di cybersecurity per rafforzare l'infrastruttura di sicurezza fisica a tutti i livelli.
A questo ***LINK*** è disponibile il White Paper di Genetec per un approfondimento.

Genetec™

Contatto:
Genetec
www.genetec.com/it