HWG Sababa

NIST CSF 2.0: i nuovi vantaggi per le aziende



Segnando un punto di svolta epocale nell'ambito della sicurezza informatica, il National Institute of Standards and Technology (NIST) ha realizzato il primo grande aggiornamento del suo framework di sicurezza informatica creato nel 2014.

Gli aggiornamenti espandono sia il **raggio di azione** che l'**efficacia** del NIST Cybersecurity Framework (CSF). Pensato inizialmente solo per le infrastrutture critiche, *NIST CSF 2.0* ora potrà supportare direttamente ogni tipo di azienda nelle gestione e nella mitigazione dei rischi di sicurezza informatica. Il nuovo framework offre anche un set di risorse a cui le aziende potranno attingere e che potranno essere combinate per rispondere a eventuali esigenze future.

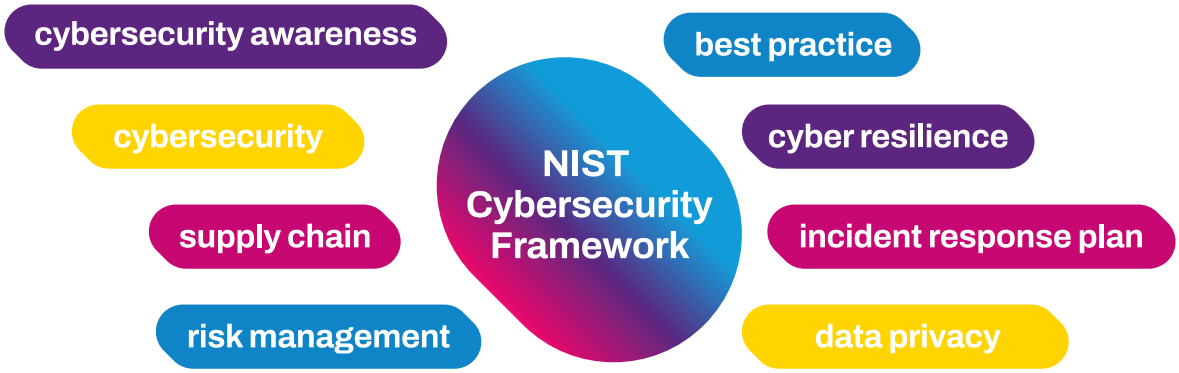
L'aggiornamento è il risultato dei numerosi feedback ricevuti in anni di discussioni e commenti pubblici ed è stato sviluppato per migliorare l'efficacia e l'applicazione del framework CSF. Sono state aggiornate le guide principali ed è stata sviluppata una suite completa di risorse affinché le **aziende di ogni dimensione e settore** abbiano a disposizione i framework necessari per **proteggere i loro asset digitali e raggiungere i loro obiettivi di sicurezza.**

Un raggio d'azione più ampio

La versione 2.0 introduce modifiche significative, al fine di migliorare la sicurezza informatica e i processi di governance aziendali. L'aspetto più importante da evidenziare è che, se il framework originale era composto da cinque funzionalità (**Identificare, Proteggere, Rilevare, Rispondere e Recuperare**), il NIST 2.0 aggiunge una sesta funzionalità: **Governare**. L'obiettivo di questa integrazione risale nel voler offrire una guida, un contesto e altre informazioni necessarie per sviluppare un modello di governance della sicurezza informatica.



Inoltre, amplia il suo raggio d'azione ben oltre i sistemi informatici classici e va a comprendere una più **vasta gamma di tecnologie emergenti**, come i dispositivi IoT, le blockchain, il cloud computing e gli strumenti di IA. Tutto ciò riflette la continua evoluzione dell'adozione della tecnologia a livello aziendale, assicurando che le misure di sicurezza informatica siano complete e conformi nel difendersi dalle minacce emergenti.



L’integrazione della privacy

Un’altra modifica importante è l’integrazione delle considerazioni sulla privacy. Dato che sicurezza informatica e privacy sono interconnesse, il NIST 2.0 mira anche a **proteggere la privacy dei dati** in quanto si tratta di un aspetto cruciale per mantenere la **fiducia del cliente.**

Questo aspetto è inoltre fondamentale anche per motivi di conformità a regolamenti come GDPR, HIPAA e CCPA, per cui le aziende sono obbligate ad adottare misure di tutela della privacy e di sicurezza informatica per **proteggere i dati sensibili**.

Maggiore attenzione alla supply chain



L’aggiornamento NIST 2.0, all’interno delle varie integrazioni, pone maggiore attenzione alla sicurezza delle catene di fornitura. Riconoscendo la natura interconnessa degli ecosistemi aziendali contemporanei, il framework offre una guida su come stabilire solide strutture di governance e **gestire i rischi di sicurezza informatica su tutta la supply chain**.

Incoraggia le aziende a valutare la **cybersecurity posture** dei loro **fornitori e partner**, a eseguire controlli per mitigare i rischi nella catena di fornitura e a stabilire piani di contingenza per ridurre al minimo le conseguenze di eventuali interruzioni della supply chain.

Identificazione e gestione del rischio

Il NIST CSF 2.0 si concentra anche sull’importanza di una **gestione dinamica del rischio**, superando la vecchia concezione di gestione statica, basata sulla conformità. Le aziende vengono incoraggiate a valutare e ad adattare continuamente le proprie strategie di cybersecurity per mitigare le minacce in continua evoluzione e i cambiamenti inevitabili nel contesto aziendale attuale.

Inoltre, poiché il lavoro da remoto e la forza lavoro distribuita rappresentano ormai la normalità, è cresciuta l’adozione di servizi basati sul cloud così come la gestione dell’autenticazione e dell’identità è diventata un anello chiave della catena di sicurezza.

Questo nuovo framework offre una **guida aggiornata per ottenere meccanismi di autenticazione più sicuri**, come l’autenticazione a più fattori (**MFA**) e sottolinea l’importanza di adottare una solida strategia di gestione dell'identità e dell'accesso (**IAM**) per prevenire l’accesso non autorizzato a sistemi e dati.

Un approccio strutturato alla misurazione

Altra novità è un approccio più strutturato per allineare gli sforzi di sicurezza agli obiettivi aziendali, oltre che ai parametri di sicurezza informatica e alle misurazioni. Ciò aiuta le aziende a valutare meglio l'efficacia dei programmi di cybersecurity e a tenere traccia dei propri progressi.

Introducendo indicatori di performance e benchmark ben definiti, le aziende possono individuare le aree su cui è necessario lavorare e assegnare le risorse in modo più appropriato per colmare eventuali gap di sicurezza.

Alimentare la cultura della sicurezza informatica



Considerando che i malintenzionati sfruttano i normali errori umani per raggiungere i propri obiettivi, il nuovo framework sottolinea l'importanza di sensibilizzare i vari reparti all'interno delle aziende in merito alla cybersecurity.

Incoraggia quindi le aziende ad avviare **corsi di formazione** regolari sulla sicurezza informatica e propone programmi di sensibilizzazione per formare **dipendenti e collaboratori** sulle minacce più comuni e sulle **best practices per mitigare i rischi**.

Attraverso un'adeguata formazione, le risorse aziendali apprendono quindi le conoscenze necessarie per individuare le minacce e le relative contromisure, permettendo alle aziende di **rafforzare la propria cybersecurity posture**.

La minaccia arriverà, che siate pronti o meno

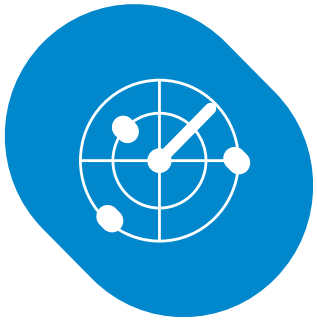
Nonostante gli enormi sforzi profusi nel settore per prevenire gli attacchi informatici, non esistono rischi zero. Si può però lavorare per essere pronti a reagire rapidamente di fronte ad eventuali incidenti di cybersecurity.

NIST 2.0 offre quindi una guida aggiornata in merito ad un **incident response plan**, sottolineando l'importanza di sviluppare solidi processi, condurre regolarmente delle simulazioni di potenziali situazioni d'emergenza per testare le capacità di risposta dell'azienda e avviare collaborazioni con fornitori esterni che vantino una solida esperienza nel campo della cybersecurity.

La ripresa di fronte ad un incident dipende in gran parte dalla preparazione e dalla capacità di reagire rapidamente per **individuare, contenere e mitigare gli incidenti di sicurezza**. Adottando una buona strategia di incident response, le aziende possono ridurre al minimo le conseguenze degli attacchi informatici sia dal punto di vista business che reputazionale.

Affrontare le aree critiche

Esaminando le varie aree critiche, NIST CSF 2.0 permette alle aziende di capire come **rafforzare** efficacemente la propria **cybersecurity posture**.



Le modifiche introdotte con la versione 2.0 mirano quindi a supportare le aziende a migliorare i propri processi di cybersecurity e privacy. Espandendo il raggio d'azione del framework, NIST 2.0 offre così uno schema completo per la **creazione di programmi che rendano il business cyber resilient**.

Nel complesso, NIST 2.0 migliora notevolmente le best practice di sicurezza informatica e le rende applicabili ad una più vasta gamma di settori, dalle piccole aziende alle multinazionali. Offre un framework flessibile e scalabile, pensato per soddisfare le esigenze specifiche di ogni singola azienda.

Contestualmente, attraverso un *portfolio completo*, HWG Sababa può supportare le aziende a mettere in pratica quanto introdotto con la nuova versione NIST 2.0. Accompagnamo il tuo business in un percorso di crescita e consapevolezza, offrendo soluzioni verticali personalizzate per diversi settori: finanziario, sanitario, telco, retail, moda, energia, utility, automotive e infrastrutture critiche.

Grazie un approccio one-stop-shop, riduciamo notevolmente la complessità che i clienti si troverebbero a fronteggiare e garantiamo un'ampia copertura della sicurezza aziendale in ambito IT, OT e IoT.

La nostra suite completa di soluzioni strategiche di sicurezza, servizi gestiti e consulenza rende il tuo business cyber resilient.

HWG Sababa

Follow us on:

www.hwgsababa.com