ANALISI, SOLUZIONI E TECNOLOGIE PER GARANTIRTI LA COMPLIANCE ALLA NUOVA DIRETTIVA NIS2

COMPLIANCE NIS2

Datasheet

Le aziende del Gruppo MEET IT

Via di Corticella, 89/2
40128 Bologna BO

+39 051 4070383
www.3cime.com | info@3cime.com

Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it

RAGGIUNGI LA CONFORMITÀ ALLA NIS2

Affrontiamo insieme la Direttiva NIS2, in maniera personalizzata, esperta e affidabile.

Il **17 ottobre 2024** entra in vigore la **Direttiva NIS2** con lo scopo di rafforzare il livello di sicurezza in tutti gli Stati membri. Può essere difficile affrontarla da soli o con un insieme eterogeneo di partner e provider.

Insieme a MEET IT, invece, puoi trasformare questa sfida in un'**opportunità per semplificare la gestione della tua sicurezza**, migliorare la tua **postura di security** e incrementare la **competitività** sul mercato.

COS'È NIS2

La **Direttiva europea NIS2** è un upgrade della versione NIS1, molto più ampia e articolata.
Il suo scopo principale, alla luce dei conflitti mondiali in corso e dell'evoluzione delle minacce informatiche, è **proteggere le organizzazioni critiche ed il tessuto sociale ed economico europeo dai rischi informatici**.

Per questo motivo si ampliano i settori coinvolti e crescono anche i controlli e gli obblighi per la conformità. Le principali novità rispetto alle direttive precedenti:

- Gli **Amministratori** delle aziende sono ritenuti direttamente responsabili delle violazioni e sono tenuti ad avere formazione specifica.
- Viene inserita fra gli obblighi la **sicurezza della catena di approvvigionamento**, in questo modo sono coinvolte tutte le realtà che forniscono servizi e prodotti alle organizzazioni critiche. Sono inclusi anche i fornitori extra UE.
- **Obblighi di segnalazione** in caso di attacco.
- Misure **tecniche, operative e organizzative** appropriate per raggiungere un certo livello di sicurezza.
- Le **sanzioni** in caso di mancata conformità sono le seguenti: per gli enti essenziali massimo 10 milioni di euro o almeno il 2% del fatturato annuo mondiale corrente, per le entità importanti almeno 7 milioni di euro o almeno 1,4% del fatturato annuo mondiale totale.

VISITA IL SITO *MEETIT.CLOUD*

Iniziamo dal principio. La tua organizzazione è coinvolta dalla nuova normativa NIS2?
Scopri se appartieni a uno dei **18 settori critici**, di cui **11 essenziali** (in grassetto) e **7 importanti**, individuati dalla NIS2.

Sono coinvolte, infatti, tutte le società che occupano **almeno 50 persone**, hanno un **fatturato annuo oppure un totale di bilancio annuo superiore a 10 milioni di €** e appartengono ad almeno uno dei seguenti settori considerati critici:

SOCIETÀ COINVOLTE DALLA NIS2

In base al livello di criticità si intensificano i requisiti da rispettare, i **controlli delle autorità** e le **sanzioni** in caso di mancata osservanza.

Non solo: anche i **fornitori** di tali categorie sono da considerarsi inclusi.
Una importante novità della NIS2, rispetto alla normativa precedente, è l'introduzione della **sicurezza nella catena di approvvigionamento**. Ed è per questo che, in realtà, al di là delle organizzazioni definite come critiche, tutti siamo coinvolti indirettamente e dobbiamo adeguarci per poter continuare a erogare i nostri servizi/prodotti alle aziende direttamente coinvolte e per mantenerci al sicuro e competitivi.

A differenza degli altri framework di cybersecurity, questo non è facoltativo.

IL NOSTRO APPROCCIO ALLA NIS2

Per adeguare i tuoi sistemi ai requisiti NIS2, adottiamo un **approccio olistico**.

La nostra strategia comprende le **persone**, le **procedure** e le **tecnologie** in un rapporto continuativo e di costante aggiornamento e monitoraggio.

La sicurezza, proprio come le minacce informatiche, è un'**evoluzione continua**, una continua corsa in avanti.
Ecco perché affrontiamo la NIS2 nella tua azienda partendo dall'analisi della situazione di partenza, per accompagnarti fino alla gestione delle tecnologie che apporteremo insieme.

CONSULENZA E RISK ANALYSIS

Analisi tecnica e legale con esperti del settore e della normativa per capire insieme rischi, vulnerabilità e necessità specifiche.

ASSESSMENT

Valutazione del tuo attuale stato di sicurezza e delle migliorie da apportare ai fini della compliance e del miglioramento della tua postura di sicurezza.

SOLUZIONI E SERVIZI PER IL RAGGIUNGIMENTO DEI TARGET

Partiamo dal **design** fino alla **fornitura** di servizi/infrastrutture custom per la tua cybersecurity & business continuity, grazie al nostro laboratorio interno e ad una fitta rete di partner. Definiamo insieme le **procedure**, gli **strumenti** e le **persone** coinvolte.

GESTIONE E MONITORAGGIO

Non ti abbandoniamo a te stesso. Continuiamo a lavorare sulle soluzioni applicate, al fine di garantire massima **efficienza e la continuità aziendale**, in sostituzione o affiancamento dei tuoi team.

VISITA IL SITO ***MEETIT.CLOUD***

Fase di Risk Analysis e consulenza, detta anche di Pre-assessment

Le attività di pre-assessment hanno natura **preliminare/conoscitiva** e sono propedeutiche all'eventuale fase di assessment.

L'analisi è finalizzata a raccogliere, tramite **interviste e documentazioni** richieste al Cliente, una serie di informazioni conoscitive essenziali (anagrafiche, dimensionali, strutturali, organizzative/funzionali, strategiche/governance in ambito IT/cyber, status quo generale delle principali misure di sicurezza adottate e applicate in ambito aziendale, ecc.).

La raccolta di informazioni è finalizzata ad esprimere una **prima indicazione** di massima su come l'azienda si colloca, a livello di adeguatezza, rispetto alle tematiche di cybersecurity e, più nello specifico, rispetto ai requisiti richiesti dalla direttiva NIS2 con una prima evidenziazione generale dei **maggiori elementi critici/non conformi rilevati**.

Fase di Assessment

Questa fase prende l'avvio con lo svolgimento di un **audit** da svolgersi presso la sede del Cliente con la conseguente **raccolta e riesame delle informazioni** documentate in materia di gestione della security aziendale. Ovvero, **verifica specifica delle misure organizzative e tecniche adottate, perimetri, responsabilità, tasso di implementazione, maturità, ecc.**

L'attività è finalizzata a **determinare e dimensionare l'eventuale gap** tra quanto esistente e applicato in azienda rispetto a quanto richiesto dalla NIS2.

Gli scostamenti rilevanti identificati nel corso delle attività di audit vengono trascritti in un **report finale** rilasciato al Cliente che conterrà, per ogni requisito analizzato, una relativa **valutazione di aderenza** o meno e i **consigli sulle azioni correttive**.

Fase di implementazione di soluzioni, servizi e supporto

Una volta raccolti tutti i dati e redatto il report di assessment, siamo pronti per mettere in pratica le **azioni correttive** e adeguare i sistemi con **nuove configurazioni** o **nuove soluzioni tecnologiche e procedurali**.

Per questo motivo, questa fase si articola nelle fasi di **progettazione o riprogettazione**, **configurazione o riconfigurazione**, **redazione di policy e procedure** operative e **fornitura di servizi e infrastrutture** ad-hoc, dimensionate secondo i casi specifici.

Fase di gestione, follow up e monitoraggio

In questa fase affianchiamo i team IT del Cliente per **gestire e monitorare costantemente** le soluzioni e le infrastrutture realizzate ai fini della conformità, della security e business continuity.

Il servizio comprende **patch management**, **aggiornamenti periodici**, **assistenza**, **gestione degli alert** e di eventuali criticità, **monitoraggio proattivo e predittivo** e **ottimizzazione costante** ai fini della business continuity.

Si attuano inoltre **audit periodici** volti a valutare l'efficacia delle misure adottate, determinando il livello di allineamento/compliance alla Direttiva nel tempo, con il variare delle minacce, delle soluzioni disponibili e delle modifiche normative.

Requisiti	Soluzioni
Politiche di analisi dei rischi e di sicurezza dei sistemi informativi	• Risk analysis tecnica e legale • Penetration Test Continuativo • Vulnerability assessment tecnici e legali
Gestione degli incidenti	• SOC - Security Operation Center • SOC su storage
Continuità operativa, come backup e ripristino in caso di disastro	• Business Continuity • Disaster Recovery • Backup immutabile (e Hardened Repository) • Archiviazione dei dati • Infrastrutture iperconvergenti in alta affidabilità
Dimostrabilità della sicurezza della catena di approvvigionamento, includendo le valutazioni del Cybersecurity Act se deciso da Commissione ed ENISA	• Consulenza tecnica e legale dedicata • Garantiamo la compliance dei nostri sistemi • Penetration Test Continuativo
Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informatici e di rete	• DDI Security • Wi-FI Survey & Design • Monitoraggio continuo e proattivo • Firewall e Firewall OT • IP Telephony
Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi cyber	• Analisi tecnica e legale per definire procedure e strategie • Penetration Test Continuativo • DarkWeb Scan • Antispam Elevator
Igiene informatica e formazione in materia cyber	• Ci avvaliamo di consulenza esperta e siamo supportati da società dedicate alla formazione del personale a tutti i livelli
Politiche di crittografia e cifratura	• Crittografia dei dati • WAF as a Service • PAM - Privileged Access Management
Sicurezza delle risorse umane, strategie di controllo di accesso e gestione degli attivi	• Data Security & Governance • PAM - Privileged Access Management • Asset Management & Intelligence • SOC - Security Operation Center • VDI - Virtual Desktop Infrastructure
Strong authentication continua, comunicazioni vocali, video e testuali protette, sistemi di comunicazione di emergenza protetti	• Multifactor Authentication • PAM - Privileged Access Management • SOC - Security Operations Center • Firewall • Smart Working sicuro

Un piccolo approfondimento sulle soluzioni di cui abbiamo accennato nella checklist precedente.

DETTAGLIO SOLUZIONI

Penetration Test Continuativo
Il servizio di ethical hacking che simula gli attacchi cyber per valutare continuamente il livello di sicurezza del perimetro aziendale.

SOC - Security Operation Center
Un team di esperti di security dedicato a te, h24/365 che monitora e risponde in caso di attacco.

Business Continuity
La continuità operativa passa per planning, management, soluzioni, hardware, software e monitoraggio continuo. Ti supportiamo in tutto questo.

Disaster Recovery
Pianifichiamo e progettiamo infrastrutture e sistemi di ripartenza in caso di disastro, in modo che tu possa ripartire il più velocemente possibile in qualunque situazione.

Backup dei dati (immutabile e su hardened repository)
Configuriamo, gestiamo e monitoriamo i backup rendendendoli immutabili e sicuri con le più recenti best practice e repository differenti e ridondati.

Archiviazione dei dati
Identifichiamo e archiviamo data e big data in storage ridondati e resilienti per ottimizzare le prestazioni e le risorse necessarie al business, eseguendo backup periodici ed eventuali restore.

Infrastrutture iperconvergenti in alta affidabilità
Confezioniamo infrastrutture convergenti e iperconvergenti per ottimizzare le risorse e garantire la business continuity del Cliente.

DDI Security
Il servizio razionalizza i livelli di Sicurezza Informatica per semplificare le procedure e proteggere il traffico dati.

Monitoraggio continuo e proattivo
Monitoring IT as a Service volto a prevedere guasti e malfunzionamenti e monitorare e ottimizzare costantemente i propri sistemi, la loro efficienza e sicurezza.

Wi-Fi Survey & Design
Analisi e progettazione di reti WiFi ottimizzate, ultraveloci, sicure ed efficienti.

VISITA IL SITO *MEETIT.CLOUD*

IP Telephony
Il centralino basato su un server di rete, clusterizzato e virtualizzato, che riduce i costi e rende ancora più sicure ed efficienti le comunicazioni.

Antispam Elevator
Protegge gli ambienti di posta elettronica MS 365, combinando AI, integrazione profonda e protezione del marchio.

PAM - Privileged Access Management
Strategie e tecnologie per gestire e proteggere gli accessi privilegiati alla propria rete aziendale.

VDI - Virtual Desktop Infrastructure e Smart Working sicuro
Un'infrastruttura personalizzabile che permette di creare postazioni di lavoro indipendenti dal device fisico, grazie ad un server centralizzato e a cui accedere in sicurezza anche da remoto.

Data Security & Governance
Una piattaforma agentless gestita per identificare, classificare e proteggere i dati critici e i loro repository, applicare policy di accesso e sicurezza.

Firewall, Firewall OT e WAF as a Service
Un filtro composto di hardware e software che protegge la tua navigazione in Internet, i tuoi endpoint, app e dispositivi OT da contenuti malevoli o indesiderati.

DarkWeb Scan
Analizza periodicamente il DarkWeb per sapere se i tuoi dati e le tue credenziali sono finite nel DarkWeb, in modo da correre immediatamente ai ripari.

Crittografia dei dati
Rendiamo illeggibili i tuoi dati a chiunque cerchi di esportarli o accedervi senza la chiave di cifratura.

Asset Vulnerability Intelligence & Management
Un servizio che consente di avere visibilità e inventario di tutte le risorse IT aziendali su un'unica piattaforma, di prioritizzare e automatizzare le attività di gestione e sicurezza.

Multifactor Authentication
Controllo degli accessi ai sistemi aziendali tramite autenticazione multifattoriale. Un login che va oltre user e password, ma utilizza almeno un ulteriore criterio di riconoscimento.

VISITA IL SITO *MEETIT.CLOUD*

Partiamo dal presupposto che tutti i nostri servizi - dalla virtualizzazione ai backup, fino allo sviluppo di Private AI - sono stati pensati nell'ottica di **garantire la sicurezza del dato**. La centralità dei dati e la loro protezione si trovano in ogni soluzione che mettiamo in campo e ci distinguono sul mercato.

Per questo, e grazie anche alla nostra esperienza maturata con gli assessment dedicati alla **conformità al GDPR**, ci proponiamo come **provider unico** per realizzare la tua compliance al NIS2.

SCADENZE CRITICHE

17 luglio 2024 - **Avvio della relazione sulla valutazione di EU-CyCLONe**
Entro questa data e poi ogni 18 mesi, la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) è tenuta a presentare al Parlamento Europeo una relazione sul proprio operato.

17 ottobre 2024 - **Pubblicazione Misure Nazionali**
Entro questa data, gli Stati membri dovranno pubblicare e adottare le misure necessarie per conformarsi alla nuova Direttiva europea.

18 ottobre 2024 - **Applicazione misure nazionali**
Da questo momento in poi verranno applicate le misure pubblicate dagli organi nazionali.

17 gennaio 2025 - **Revisioni tra pari dell'Istituzione**
Prima revisione da parte del gruppo di cooperazione (Commissione, ENISA e CSIRT) per la metodologia e gli aspetti organizzativi.

17 aprile 2025 - **Elenco enti essenziali e importanti coinvolti**
Definizione dell'elenco delle società effettivamente coinvolte dalla NIS2 e revisione biennale.

17 ottobre 2027 - **Avvio revisione NIS2**
Entro questa data e poi ogni 3 anni, la Commissione rivede la Direttiva ed il suo funzionamento, riferendo al Parlamento europeo.

VISITA IL SITO *MEETIT.CLOUD*