air2bite | business solutions

NIS2
Cyber Checkup

La sicurezza informatica è una priorità inderogabile per aziende e istituzioni

L'introduzione di una nuova Direttiva NIS emerge come una risposta essenziale alle mutevoli minacce cibernetiche, mirando a colmare le lacune esistenti nella legislazione e a creare un quadro più coeso e robusto per la resilienza digitale europea.

Assessment

La finalità condivisa è quella di individuare una serie di suggerimenti, rimedi, attività, tecnologie e/o servizi aventi il fine di innalzare la protezione dell'azienda rispetto ad eventuali problematiche di sicurezza (accidentali o dolose) che potrebbero compromettere la confidenzialità, integrità o disponibilità dei dati e dei servizi dell'azienda stessa e la non conformità alla Direttiva Nis2.

NIS2
chi deve rispettarla

- Imprese di Medie e Grandi dimensioni a partire da 50 dipendenti e fatturato annuo a partire da 10M
- Le Piccole e Micro Imprese rientrano nella NIS2 solo se hanno un ruolo chiave per la società, l'economia, o settori/servizi specifici.
- La Pubblica Amministrazione è sempre inclusa, a prescindere dalla sua dimensione.
- Supply Chain: Appartenenza alla catena di fornitura dei soggetti essenziali ed importanti

Aree di analisi del cyber-checkup

- Politiche di analisi dei rischi e di sicurezza dei sistemi informatici
- Gestione incidenti
- Continuità operativa
- Sicurezza della supply chain
- Sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete
- Strategie di controllo dell'accesso
- Strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza
- Pratiche di igiene informatica di base e formazione in materia di cybersicurezza
- Politiche e procedure relative all'uso della crittografia e della cifratura
- Sicurezza delle risorse umane
- Uso di soluzioni di autenticazione a più fattori

air2bite | business solutions

Le fasi del Nis2 Cyber-Checkup

Le fasi del Nis2 Cyber-Checkup

Comprensione del contesto aziendale e della Compliance

Viene effettuata un'analisi attraverso interviste ai key users focalizzata su punti essenziali richiesti dalle 5 categorie del Framework NIST.
Il nostro team si dedicherà a comprendere a fondo il contesto operativo, le strutture organizzative, le infrastrutture IT esistenti e i processi di sicurezza informatica attualmente in atto (AS-IS).

Il valore aggiunto del framework NIST è quello di avere una struttura che permette di collegare gli standard ISO 27001, IEC 62443, GDPR, NIS2 e COBIT (serie di best practice per la gestione IT). Di seguito riportiamo nel dettaglio un esempio di «integrazione» tra le aree di analisi NIST.

Le fasi del Nis2 Cyber-Checkup

Analisi e valutazione: Gap Analysis

Questa fase consentirà di identificare con precisione le eventuali lacune e i punti critici che richiedono un intervento per garantire la piena conformità alla Direttiva Nis2.

Metodologia di Analisi

- Mappatura dell'infrastruttura tecnologica in ambito cyberscurity
- Analisi dettagliata dei processi di sicurezza informatica
- Analisi delle attuali pratiche e procedure confrontandole con i requisiti stabiliti dalla normativa NIS2
- Gap Analisys (AS IS vs TO BE)

02

Analisi del rischio

La NIS2 prevede di implementare politiche di analisi del rischio. Al fine di migliorare la valutazione del rischio cyber, sarà previsto l'utilizzo della piattaforma di External Attack Surface Management e Cyber Threat intelligence Cybersonar.

Metodologia di valutazione del rischio

- Analisi fonti OSINT
- Analisi Deep e Dark Web
- Asset Inventory
- Misconfigurazioni
- Analisi delle vulnerabilità
- Ricerca di eventuali indicatori di compromissione, quali credenziali di accesso, documenti esfiltrati, minacce di phishing, etc...

02

Le fasi del Nis2 Cyber-Checkup

Vulnerability Assessment

Valutazione dei singoli elementi dell'infrastruttura oggetto della analisi per identificare le vulnerabilità presenti.

Metodologia di intervento

L'audit sugli elementi del Sistema valuta le migliaia di vulnerabilità conosciute e che vengono aggiornate quotidianamente. È effettuato utilizzando diversi tool al fine di confrontarne i risultati; tali risultati vengono poi epurati degli eventuali falsi positivi dai nostri analisti di sicurezza.

In base alle evidenze emerse, si raccolgono informazioni specifiche sulle vulnerabilità conosciute dei sistemi operativi individuati e sugli applicativi presenti.

02

Elaborazione del report di Gap Analysis

Il risultato dell'analisi sarà sintetizzato in un rapporto dettagliato che include:

Architettura di sicurezza ICT – Gap Analysis

Riporta la valutazione delle criticità che il sistema informativo presenta dal punto di vista della sicurezza ed individua una serie di azioni migliorative, per ogni punto esaminato.

Mappatura delle lacune

Riporta una panoramica chiara delle aree di non conformità alla Direttiva NIS2.

Valutazione della resilienza

Riporta il grado di resilienza dell'azienda, evidenziando le forze e le debolezze della struttura attuale, rispetto ai requisiti della Direttiva NIS2.

Piano di adeguamento e remediation

Sviluppo di un piano completo di adeguamento e di miglioramento: raccoglie le azioni migliorative e gli interventi necessari ad eliminare o mitigare i rischi individuati. Evidenzia ed organizza le aree di intervento in macro-progetti che rappresentino i requisiti richiesti dalla Direttiva NIS2.

Metodologia di intervento

• Raccomandazioni concrete per colmare le lacune identificate, migliorare la sicurezza informatica e allinearsi ai requisiti della Direttiva NIS2

• Definizione di un piano d'azione sequenziale, con priorità assegnate in base all'urgenza e all'impatto delle misure di remediation proposte.

04

Piano di Incident Response

La politica di IR rappresenta uno dei punti chiave della NIS2 e prevede la realizzazione di tutte le procedure da attivare in caso di incidenti informatici. La mancata adozione di politiche e piani di IR prevede pesanti sanzioni.

Metodologia di intervento

• Analisi delle politiche attuali, se esistenti, e redazione/adeguamento delle stesse.

• Le politiche di IR prevedono una analisi dei sistemi, l'identificazione delle figure chiave, l'identificazione dei fornitori chiave e la redazione di tutte le procedure di intervento ed escalation in caso di incidenti informatici incluse tutte le attività di notifica obbligatoria.

04

Elaborazione policy di Backup e resilienza

La NIS2 richiede l'adozione di politiche di backup per garantire la massima protezione e disponibilità dei dati aziendali.

Metodologia di intervento

- Analisi delle politiche attuali, se esistenti, e redazione/adeguamento delle stesse.
- Consultazioni con gli stakeholder chiave.
- Formulazione di nuove linee guida basate su standard normativi di riferimento, che coprono tre aree chiave:
  - **procedure di backup**
  - **politiche di conservazione**
  - **procedure test di ripristino**

04

In conformità con la nuova direttiva NIS2, verranno riviste e integrate le policy di igiene informatica e di sicurezza, mirate a proteggere le risorse digitali aziendali.

Metodologia di intervento

• Analisi delle politiche attuali, se esistenti, e redazione/adeguamento delle stesse.

• Implementazione di protocolli di sicurezza, con policy dettagliate per l'utilizzo sicuro degli strumenti informatici aziendali da parte dei dipendenti, attraverso linee guida e buone pratiche su accesso e uso dei device aziendali.

Politiche di igiene informatica

Awareness dei vertici aziendali

La NIS2 impone ai vertici aziendali il coinvolgimento nella governance della sicurezza informatica aziendale e la partecipazione a formazioni specifiche su tematiche di cybersecurity.

Metodologia di intervento

- Attività di formazione specifica sui temi cyber dedicata ai vertici aziendali e ai membri del Consiglio di Amministrazione.
- Workshop pratici su scenari di minacce reali

air2bite | business solutions

Abacus Company

HEADQUARTERS

Palazzo direzionale Carispaq
Corso Vittorio Emanuele II, 48
67100 L'Aquila (AQ)

sales@air2bite.com

www.air2bite.com