Servizi di Pre-screening NIS2

Cyber Risk Management

Telsy

A TIM ENTERPRISE BRAND

Obiettivo dei servizi

L'obiettivo dell'attività di Pre-screening NIS2 è fornire una panoramica generale dell'Organizzazione sul rispetto degli adempimenti e delle misure di sicurezza previste dalla Direttiva NIS2.

Identificando le principali aree che richiedono miglioramenti o azioni correttive, si ottenerà una prima valutazione "pre-screening" rispetto a quanto sarà recepito dalla normativa nazionale il prossimo ottobre 2024.

Benefici per il cliente

01 Aumento del livello di postura di cyber resilienza dell'azienda con il rafforzamento delle misure di sicurezza della NIS2

02 Individuazione delle misure organizzative adeguate per monitorare e rispondere efficacemente agli incidenti

03 Individuazione delle misure tecniche adeguate per la sicurezza dei sistemi e delle reti dell'azienda

04 Responsabilizzazione del management sulla gestione della sicurezza relativa alla supply chain

Quick Assessment NIS2

Aumentare il livello della postura di cyber resilienza dell'Organizzazione rafforzandole misure di sicurezza previste dalla NIS2

Individuare misure organizzative adeguate per monitorare e rispondere efficace mente agli incidenti

Individuare misure tecniche adottate perla sicurezza dei sistemi e delle reti dell'Organizzazione

Maggiore attenzione sulla gestione del rischio legato alla supply chain e responsabilizzazione del management

benefici

Verifica dell'inclusione dell'Organizzazione nel perimetro NIS2 e determinazione dell'Entities come Soggetto Essenziale o Importante operante nei Settori Critici

Valutazione preliminare delle politiche e procedure di sicurezza adottate dall'Organizzazione nelle Aree e negli Ambiti operativi NIS2 (cfr. slide 3).

Identificazione preliminare delle contro misure tecnologiche per mitigazione dei rischi in riferimento alle. Aree e negli Ambiti operativi NIS2 (cfr. slide 3)

Identificazione aree di miglioramento e analisi delle relative criticità, fornendo eventuali «raccomandazioni» per migliorare il livello di compliance NIS2

attività

Risultati / Deliverable

Report finale con i risultati delle analisi di pre-screening

Target clientela

Aziende <250 dipendenti e fatturato medio annuo <50M€ (o bilancio globale annuo <43M€)

Security Posture NIS2

Il servizio si propone, a valle del recepimento della Direttiva a livello nazionale, di identificare, valutare e trattare il rischio cyber, in piena coerenza con l'approccio risk-based adottato dalla Direttiva NIS 2. Il profilo di Servizio di NIS 2 Cyber Risk Assessment & Treatment è erogato in riferimento allo standard ISO 27001 (Information technology – Security techniques – Information security management systems - Requirements), all'ISO 27005 "Information Security Risk Management" e al NIST Cyber Security Framework, e in conformità alla Direttiva UE 2022/2555, c.d. NIS 2 attraverso apposita checklist.

Info Gathering

Identifi azione processi/applicazioni chiave e raccolta informazioni di contesto

Business Impart Analysis

Interviste, Controlli di sicurezza, Analisi dei rischi

Remediation

Individuazione dei principali gap e defin zione di una roadmap degli interventi suggeriti

Risultati / Deliverable

Report finale con i risultati delle analisi di pre-screening che include:

1. **Mappa del rischio su tutta l'organizzazione e relativo livello di maturità rispetto al framework NIS2**
2. **Mappa dei principali fattori di rischio**
3. **Piano delle iniziative di sicurezza e definizione delle priorità per la mitigazione del rischio**

Target clientela

Aziende >250 dipendenti e fatturato medio annuo >50M€ (o bilancio globale annuo >43M€)

Qual è la differenza con il servizio Quick Assessment NIS2?

Questo servizio è pensato per procedere con una valutazione a maggiore dettaglio e profondità, associata ad una valutazione del rischio cyber complessiva per l'azienda.

Attraverso strumenti operativi che combinano un approccio top -down ad uno bottom-up per una valutazione semi-quantitativa dei rischi cyber sull'intera organizzazione, si analizza il livello di esposizione al rischio sui vari livelli aziendali calcolandone la postura di rischio.

Identificando così le aree di rischio e i processi critici del Cliente, si fornisce altresì un efficiente piano strategico di investimenti in cybersecurity, basato sul reale livello di esposizione al rischio cyber e sul rapporto costi/ benefici delle misure da adottare.

Differenze

	Quick Assessment NIS2	Security Posture NIS2
target	**Medie aziende*** per lo più non incluse già nella NIS1 e/o che non erano individuate tra i soggetti importanti/ essenziali o fornitori	**Grandi aziende**** per lo più non incluse già nella NIS1 e/o che non erano individuate tra i soggetti importanti/essenziali o fornitori
strumenti	**Analisi human-driven** non è previsto l'uso di piattaforme oltre agli strumenti Offi	**Semi-automated** attraverso l'utilizzo della piattaforma Cyber Risk DIVE che consente l'analisi scalabile per layer e l'elaborazione di risultati oggettivi
profondità	**Alto livello** valutazione generale del livello delle misure relative alle aree di intervento defin te dalla NIS2 non di dettaglio sui singoli processi e tecnologie "critiche"	**In-Depth Analysis** valutazione approfondita per layer del modello di governance di sicurezza adottato rispetto alle aree di intervento defin te dalla NIS2
durata	**Veloce** 10gg lavorativi più il tempo di elaborazione e condivisione del report final	**Su misura** un'attività disegnata sul cliente con una durata non inferiore alle 8 settimane

* Aziende <250 dipendenti e fatturato medio annuo <50M€ (o bilancio globale annuo <43M€)
** Aziende >250 dipendenti e fatturato medio annuo >50M€ (o bilancio globale annuo >43M€

Telsy

A TIM ENTERPRISE BRAND

telsy.com
contact@telsy.it