Alla cortese attenzione del Legale Rappresentante e del Responsabile della Sicurezza delle Informazioni (CISO / IT Security Manager)

Oggetto: Comunicazione di conformità ai sensi del D.Lgs. 138/2024 (Direttiva NIS2)

Gentile Cliente,

in qualità di registrar e fornitore di servizi digitali (inclusi servizi di hosting e posta elettronica erogati anche tramite partner terzi), qualificato come "soggetto importante" ai sensi del Decreto Legislativo 4 settembre 2024, n. 138 (attuativo della Direttiva (UE) 2022/2555 - NIS2), desideriamo fornirvi evidenza della nostra conformità normativa e del sistema di gestione della cybersicurezza implementato.

Il presente documento intende assolvere agli obblighi di trasparenza lungo la supply chain, come richiesto dal decreto e dalle linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN).

Inquadramento normativo

- Qualificazione giuridica: soggetto importante ex art. 6 D.Lgs. 138/2024
- Ambito operativo: registrazione di nomi a dominio, servizi digitali, hosting e posta elettronica, con impatto potenziale su servizi pubblici e privati
- Autorità di vigilanza: ACN – Agenzia per la Cybersicurezza Nazionale
- Canale di notifica incidenti: CSIRT Italia
- Registrazione ufficiale: completata entro i termini previsti dalla normativa vigente tramite piattaforma ACN, con aggiornamenti annuali obbligatori

Misure tecniche e organizzative implementate

- Governance e gestione dei rischi
- Politica aziendale formalizzata per la sicurezza delle informazioni
- Mappatura e classificazione dei servizi digitali e dei relativi asset
- Valutazione e gestione dei rischi informatici legati a domini, account, sistemi di gestione, hosting e infrastrutture cloud (anche se erogati anche tramite partner terzi)

Controlli tecnici e architetturali

- Autenticazione forte e gestione delle credenziali per l'accesso ai pannelli di controllo
- Protezione delle interfacce di amministrazione.
- Sistemi di monitoraggio per il rilevamento di accessi anomali o non autorizzati
- Backup periodici dei dati critici e verifica di integrità
- Coordinamento tecnico con fornitori terzi per garantire l'aderenza agli standard di sicurezza richiesti dalla normativa

Gestione incidenti e business continuity

- Piano di gestione incidenti per i servizi digitali, di hosting e di posta elettronica
- Monitoraggio h24 con alerting automatizzato e procedure di escalation
- Redazione di post-incident report con azioni correttive e preventive

Formazione e sensibilizzazione

- Programma di awareness per il personale con focus su phishing, social engineering e compromissione account
- Il nostro approccio è conforme alle best practice di settore (ENISA, NIST) e alle raccomandazioni ACN

Incident reporting e cooperazione attiva

In conformità con l'art. 23 del decreto, in caso di incidente rilevante:

- Invio notifica preliminare ad ACN/CSIRT entro 24h dall'identificazione
- Aggiornamento tecnico entro 72h
- Report completo entro 30 giorni, con analisi tecnica e misure attuate
- Nel caso di impatti verso i clienti, attiviamo tempestivamente i canali di comunicazione previsti contrattualmente.

Impegni verso clienti e stakeholder

Ci impegniamo a:

- Garantire continuità e integrità dei servizi digitali forniti
- Collaborare in modo trasparente alla gestione del rischio cyber
- Fornire su richiesta evidenze documentali e informazioni tecniche

- Supportare eventuali attività di compliance e audit condivisi

Punto di contatto designato (NIS2 – Art. 11)

Nome: A. LAZZARA
Ruolo: Responsabile Cybersicurezza e Coordinamento NIS2
Email: lazzara@teknadoc.com
Telefono diretto: 0932641949
PEC: teknadoc@gov.ecert.it

Rimaniamo disponibili a condividere ulteriori evidenze tecniche o partecipare ad attività di coordinamento con i vostri team di sicurezza.

Cordiali saluti,

TEKNADOC ITALIA SRL

30 giugno 2025