Policy Cybersecurity

In un mondo digitale in continua evoluzione e in un quadro internazionale complesso, le minacce informatiche continuano a crescere e la sicurezza informatica svolge un ruolo essenziale nella vita professionale e personale. A tal fine, il Gruppo Eurovo, in linea con le disposizioni previste dalla Direttiva (UE) 2022/2055, nota come NIS2 (*Network and Information System Directive*), intende regolare le modalità in cui i fornitori, in qualità di partner esterni, devono gestire la sicurezza delle informazioni.

Obblighi Generali di Sicurezza Informatica

I fornitori devono implementare adeguate misure di sicurezza per proteggere i sistemi, i dati e le comunicazioni, in conformità con i requisiti di NIS2, che includono, ma non si limitano a:

- **Gestione del rischio**: I fornitori devono attuare politiche di gestione dei rischi che includano l'identificazione, la valutazione e la mitigazione dei rischi relativi alla sicurezza informatica.
- **Cifratura**: Devono essere adottate tecniche di cifratura dei dati sia in transito che a riposo, per proteggere le informazioni sensibili.
- **Accesso e controllo**: I fornitori sono tenuti ad adottare pratiche di gestione degli accessi, inclusi l'autenticazione multifattoriale e la limitazione dei privilegi agli utenti autorizzati.

Gestione degli incidenti di sicurezza

In caso di un incidente di sicurezza informatica (come una violazione dei dati o un attacco informatico), il fornitore è obbligato a:

- **Notifica tempestiva**: Dev'essere fornita una comunicazione tempestiva all'entità committente riguardo a qualsiasi incidente che possa compromettere la sicurezza dei sistemi e delle informazioni.
- **Piano di risposta agli incidenti**: I fornitori devono avere un piano documentato per la gestione e il recupero da incidenti informatici, che comprenda procedure di contenimento, analisi, e recupero.
- **Collaborazione**: I fornitori devono collaborare con le autorità competenti e con l'entità committente per fornire informazioni dettagliate sull'incidente e supportare le attività di mitigazione.

Obblighi di Resilienza e Continuità Operativa

I fornitori devono implementare e mantenere politiche di continuità operativa che includano:

- **Backup e recupero dati**: I fornitori devono effettuare regolari backup dei dati e implementare procedure di recupero in caso di disastro, in linea con i tempi di recupero accettabili concordati.
- **Test di resilienza**: Devono essere effettuati test periodici sui sistemi di backup e sulle procedure di continuità operativa per garantirne l'efficacia.
- **Sistemi ridondanti**: È richiesto che i fornitori adottino soluzioni tecnologiche ridondanti per garantire la disponibilità continua dei servizi critici.

Sicurezza della Supply Chain

I fornitori devono assicurarsi che anche i propri sub-fornitori (inclusi i partner tecnologici e i servizi cloud) rispettino i requisiti di sicurezza definiti dalla NIS2. A tal fine, i fornitori sono tenuti a:

- **Verifiche e audit di sicurezza**: I fornitori devono condurre verifiche e audit regolari sui sub-fornitori per assicurarsi che rispettino i requisiti di sicurezza applicabili.
- **Clausole di sicurezza nei contratti**: Devono essere inclusi obblighi di sicurezza nei contratti con i sub-fornitori, che impongano loro di conformarsi alle disposizioni di NIS2.

Monitoraggio e Audit

I fornitori sono soggetti a un processo di monitoraggio continuo da parte dell'entità committente per garantire che le misure di sicurezza siano effettivamente implementate e mantenute. Il monitoraggio può includere:

- **Audit periodici**: L'entità committente può richiedere audit periodici per verificare la conformità alle normative di sicurezza.
- **Raccolta di informazioni**: I fornitori devono fornire, su richiesta, report di sicurezza, log di sistema e altre informazioni rilevanti per valutare lo stato della sicurezza.

Conformità e Sanzioni

In caso di mancata conformità ai requisiti di sicurezza definiti nel presente regolamento, l'entità committente si riserva il diritto di applicare le seguenti misure:

- **Revisione del contratto**: L'entità committente può avviare una revisione delle condizioni contrattuali e degli obblighi di sicurezza.
- **Interruzione della collaborazione**: In caso di violazione grave, può essere prevista l'interruzione del rapporto di fornitura.
- **Sanzioni legali e risarcimenti**: La mancata protezione delle informazioni e la violazione dei contratti di sicurezza possono comportare sanzioni legali, inclusi danni economici e risarcimenti.

Modifiche al Regolamento

Questo regolamento può essere aggiornato periodicamente per garantire che continui a riflettere le evoluzioni della normativa NIS2 e le migliori pratiche di sicurezza informatica. I fornitori saranno informati tempestivamente di eventuali modifiche e dovranno conformarsi alle nuove disposizioni.