A tutti i sigg.ri Clienti
Loro sedi

Of counsel
Dott. Sandro Guarnieri

Dott. Marco Guarnieri
Dott. Corrado Baldini
Dott. Paolo Fantuzzi

Dott.ssa Clementina Mercati
Dott.ssa Sara Redeghieri
Dott.ssa Beatrice Cocconcelli
Dott. Daniele Pecora
Dott.ssa Veronica Praudi
Dott.ssa Federica Lusenti
Dott. Andrea Friggeri
Dott.ssa Martina Carobbi
Dott. Matteo Giovannini

Avv. Francesca Palladi

Reggio Emilia, lì 19/11/2024

CIRCOLARE N. 42/2024

Approfondimento

Oggetto: Direttiva NIS 2 e Cybersecurity: adempimenti per le aziende

Il Decreto Legislativo n. 138 del 4 settembre 2024 ha recepito nell'ordinamento italiano la Direttiva UE 2022/2555 (nota come Direttiva NIS 2) con l'obiettivo di implementare il livello di **sicurezza informatica** nei paesi membri dell'Unione Europea.

Cosa si intende per Cybersecurity?

La sicurezza informatica (o **cybersicurezza**) è l'insieme di pratiche, tecnologie e processi volti a proteggere sistemi informatici, reti, dispositivi e dati da attacchi, danni o accessi non autorizzati. Questa disciplina si occupa della protezione delle informazioni digitali e delle infrastrutture tecnologiche contro minacce quali malware, attacchi hacker, ransomware, phishing e altre forme di crimini informatici.
Gli obiettivi principali della cybersicurezza sono:

1. **Riservatezza:** garantire che solo le persone autorizzate possano accedere a determinate informazioni.
2. **Integrità:** assicurare che i dati non vengano alterati in modo non autorizzato o non intenzionale.
3. **Disponibilità:** garantire che i sistemi e le informazioni siano accessibili agli utenti legittimi quando necessario.

Nell'ambito della cybersecurity, si sviluppano anche pratiche di **resilienza**, cioè la capacità di un sistema di prevenire, rilevare e riprendersi dagli attacchi informatici, e di **mitigazione** dei rischi, con l'implementazione di misure preventive per ridurre l'impatto degli attacchi.

Le principali novità introdotte dalla Direttiva NIS 2:

- **Ampliamento dell'ambito di applicazione:** la direttiva estende i requisiti di sicurezza a un numero maggiore di settori e servizi considerati critici per il funzionamento socioeconomico dell'UE. Oltre ai settori già coperti dalla

SGB & Partners
Sede legale
Via Meuccio Ruini, 10
42124 Reggio Emilia
CF e Piva 01180810358

Tel. +39 0522 941069
Fax +39 0522 941885
Mail info@sgbstudio.it
Web www.sgbstudio.it

precedente direttiva NIS, vengono inclusi nuovi ambiti come la gestione dei servizi TIC, le infrastrutture dei mercati finanziari, la ricerca, i servizi postali, la chimica, l'alimentazione, i fornitori digitali, la gestione dei rifiuti e la produzione.

L'elenco completo dei settori ad alta criticità e dei soggetti può essere consultato collegandosi al sito della Gazzetta Ufficiale, www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG, prendendo visione degli allegati al testo del Decreto.

- **Obblighi in materia di gestione dei rischi e di segnalazione degli incidenti:** i soggetti interessati dovranno adottare misure di sicurezza adeguate ai rischi concreti connessi alla propria attività e/o implementare quelle già esistenti, creare un piano per gestire gli incidenti (Data Breach Recovery Plan), monitorare i livelli di sicurezza informatica con un approccio continuo e notificare al CSIRT (www.csirt.gov.it) ogni incidente eventualmente occorso. Queste misure devono essere proporzionate ai rischi specifici, alle dimensioni dell'entità e alla gravità potenziale degli incidenti.
- **Classificazione delle entità:** La direttiva distingue tra "entità essenziali" e "entità importanti", in base alla criticità dei servizi offerti e all'impatto potenziale di eventuali interruzioni. Le entità essenziali sono soggette a requisiti di sicurezza più stringenti rispetto alle entità importanti.
- **Verifiche e ispezioni:** l'Autorità Nazionale competente NIS può sottoporre i soggetti che rientrano nell'ambito di applicazione del D. Lgs. 138/2024 a verifiche, ispezioni, ovvero può avanzare richieste di accessi a dati e documenti.
- **Sanzioni per il mancato rispetto:** La Direttiva NIS 2 prevede sanzioni amministrative pecuniarie per le entità essenziali e importanti che non rispettano gli obblighi in materia di sicurezza informatica. Le sanzioni variano in base alla gravità della violazione e alla tipologia dell'entità coinvolta.

  Per le entità essenziali:

  Sanzioni fino a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se tale importo è superiore.

  Per le entità importanti:

  Sanzioni fino a 7.000.000 di euro o all'1,4% del fatturato mondiale totale annuo dell'esercizio precedente, se tale importo è superiore.

  È importante notare che le pubbliche amministrazioni possono essere soggette a sanzioni pecuniarie da 25.000 a 125.000 euro.

Lo Studio rimane a disposizione per eventuali chiarimenti.

SGB & Partners
Sede legale
Via Meuccio Ruini, 10
42124 Reggio Emilia
CF e Piva 01180810358

Tel. +39 0522 941069
Fax +39 0522 941885
Mail info@sgbstudio.it
Web www.sgbstudio.it

SGB & Partners – Commercialisti