LA CYBERSECURITY NELLA FILIERA DEI RIFIUTI: I NUOVI ADEMPIMENTI OBBLIGATORI

LA CONVERGENZA TRA SOSTENIBILITÀ AMBIENTALE E RESILIENZA CIBERNETICA NEL QUADRO DEL D.LGS. 138/2024

Studio Europa S.r.l.
Servizi e Assistenza alle Imprese

DI COSA PARLIAMO?
UN CAMBIO DI PARADIGMA NECESSARIO

Il comparto della gestione, trattamento e smaltimento dei rifiuti è stato ufficialmente classificato come "Settore Critico" (Allegato II) dal Decreto Legislativo 4 settembre 2024, n. 138, l'atto normativo che ha recepito in Italia la Direttiva UE 2022/2555 (NIS2).

La digitalizzazione dei processi industriali, l'adozione dell'IoT nella tracciabilità dei rifiuti e l'integrazione obbligatoria con sistemi statali (come il RENTRI) hanno trasformato i player di questo settore in bersagli sensibili per attacchi cyber.

L'interruzione delle attività di smaltimento o il blocco logistico non costituiscono più solo un danno economico aziendale, ma una minaccia diretta alla salute pubblica e alla sicurezza ambientale della nazione.

Questo documento definisce i criteri di applicabilità, gli adempimenti urgenti, i rischi specifici e la roadmap tecnologico-organizzativa per garantire la conformità delle aziende del comparto alle scadenze previste dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Studio Europa S.r.l.
Servizi e Assistenza alle Imprese

CHI DEVE ADEGUARSI?
I NUOVI CRITERI

Rientrano nel perimetro NIS2 le aziende operanti nella filiera dei rifiuti che superano le soglie di Media Impresa:

- Organizzazioni con almeno 50 dipendenti.
- Fatturato annuo o totale di bilancio superiore a 10 milioni di euro

Praticamente ogni anello della catena: dalla raccolta al trasporto dei rifiuti urbani e industriali, fino agli impianti di termovalorizzazione, compostaggio, trattamento biologico meccanico (TMB) e alla gestione delle discariche o dei rifiuti speciali e pericolosi.

Studio Europa S.r.l.
Servizi e Assistenza alle Imprese

LE VULNERABILITÀ DEL SETTORE: IL PUNTO DI CONTATTO TRA IT E OT

La vera sfida per chi gestisce i rifiuti sta nella convivenza di due mondi informatici molto diversi, che oggi si trovano a dialogare costantemente: il mondo IT (la rete dell'ufficio, le email, i gestionali di fatturazione) e il mondo OT (l'infrastruttura industriale, i bracci meccanici, i sistemi SCADA, i PLC, i sensori delle discariche e i sistemi di pesa).

🌱 Minaccia Principale	⚙️ Meccanismo d'Azione	⚠️ Conseguenze e Impatti Critici
Blocco operativo degli impianti	Un ransomware cripta i sistemi di controllo industriale (es. forni o sistemi di filtraggio).	Spegnimento forzato dei sistemi ed emergenza ecologica nel giro di poche ore.
Manomissione della tracciabilità	Attacco informatico ai portali logistici per alterare i registri di carico/scarico e i codici EER	Copertura di traffici illeciti di rifiuti e gravissime sanzioni penali per l'azienda.
Effetto domino della Supply Chain	I criminali sfruttano le difese informatiche più deboli di un fornitore esterno per penetrare nei sistemi centrali.	Compromissione dell'azienda madre attraverso la rete di subfornitori e trasportatori.

LA LINEA DEL TEMPO:
LE SCADENZE DA RISPETTARE

L'Agenzia per la Cybersicurezza Nazionale (ACN) ha tracciato una roadmap precisa e vincolante:

Mappatura dei Servizi:
Nella prima parte dell'anno le aziende già registrate hanno dovuto caricare sulla piattaforma di ACN l'elenco dettagliato delle proprie attività digitali.

Obbligo di notifica (Già attivo):
In caso di attacco informatico significativo, non si può più aspettare.
C'è l'obbligo stringente di inviare una prima notifica di allerta (early warning) al CSIRT Italia entro 24 ore dall'evento, seguita da un report dettagliato entro le 72 ore.

Traguardo 31 Ottobre:
Entro questo termine, tutte le aziende coinvolte devono aver implementato le misure di sicurezza tecniche e organizzative previste dalla legge.
Oltre questa scadenza, l'ACN darà il via alle attività ispettive sul campo.

Studio Europa S.r.l.
Servizi e Assistenza alle Imprese

COSA FARE IN PRATICA?
I REQUISITI MINIMI

Ogni organizzazione deve muoversi su due fronti:

Presidi di Governance e Organizzazione

- Responsabilità del Management

Gli organi direttivi approvano formalmente le misure di gestione dei rischi cyber e rispondono personalmente in caso di non conformità.

- Formazione Obbligatoria: Introduzione di programmi periodici di cybersecurity awareness per tutto il personale, con focus specifico sui rischi legati all'utilizzo dei sistemi industriali nei siti di stoccaggio.

Presidi Tecnici

- Business Continuity: Scrivere e testare piani di emergenza per capire come continuare a raccogliere e trattare i rifiuti anche se i server aziendali dovessero essere completamente spenti.

- Segmentazione della rete: Separare nettamente la rete degli uffici da quella dell'impianto industriale. Se un virus infetta il computer della contabilità, non deve assolutamente poter raggiungere i PLC che controllano i macchinari.

- Autenticazione forte (MFA): Introdurre l'autenticazione a due fattori per qualsiasi tipo di accesso, specialmente per i tecnici esterni che si collegano da remoto per fare manutenzione.

COSA SI RISCHIA?
IL SISTEMA SANZIONATORIO

Il D.Lgs. 138/2024 prevede sanzioni calibrate per i "Soggetti Importanti" che non si adeguano o non segnalano gli incidenti:

- **Sanzioni pecuniarie**: Multe che possono arrivare fino a 7 milioni di euro o al 1,4% del fatturato globale annuo dell'azienda (scegliendo l'importo più alto).

- **Sanzioni operative**: Nei casi più gravi o in caso di recidiva, l'autorità può sospendere temporaneamente le autorizzazioni ambientali o le certificazioni necessarie per operare sul mercato.

Studio Europa S.r.l.
Servizi e Assistenza alle Imprese

LA ROADMAP PER PARTIRE OGGI

Adeguarsi alla NIS2 è un percorso a tappe.
Per non farsi trovare impreparati, i primi tre passi da compiere immediatamente sono:

- Effettuare un Cyber Assessment completo che metta in luce le vulnerabilità reali dei sistemi d'impianto (OT) e degli uffici (IT).
- Rivedere i contratti con i fornitori, inserendo clausole minime di sicurezza informatica per proteggere la catena di approvvigionamento.
- Definire una procedura interna di Incident Response per essere pronti a segnalare un attacco entro le 24 ore previste dalla legge.