Rödl & Partner

PRESENTI NEL MONDO

"Energy , Cybercrime e Cybersecurity: la gestione dei rischi ed il modello organizzativo integrato"

Avv. Giuliana Viviano, LL.M.

Introduzione: Cybercrimes nel mondo energy

CYBERCRIMES – GLI ATTACCHI INFORMATICI

Gli attacchi informatici che suscitano allarme e causano danni ingenti alle imprese ed all'economia sono quelli che colpiscono le reti di distribuzione di servizi essenziali, tra i quali l'energia, ovvero le c.d. infrastrutture critiche.

L'utilizzo di nuove tecnologie e di reti elettriche intelligenti offre nuovi punti di accesso per gli attacchi *hacker* alla *cyber* sicurezza dell'utilizzatore, dell'impresa e potenzialmente di tutti i fruitori della rete.

E' una minaccia concreta!

- Furto o uso illecito dei dati personali acquisiti;
- *Hackeraggio* delle reti e dei contatori *smart* con pericolo di alterazione dei dati;
- *Hackeraggio* delle reti e dei contatori *smart* con blocco della *business continuity* e danni alle stesse

Da ricordare…. l'attacco hacker condotto dal malware **"Black-Energy"**, che ha spento tre centrali ucraine nel dicembre del 2015

I principi generali di Cybersecurity

Con il termine Cybersecurity si intende un insieme di comportamenti, mezzi e tecnologie, tesi alla protezione di asset informatici in termini di disponibilità, confidenzialità e integrità.

La sicurezza informatica deve preoccuparsi di impedire l'accesso sia agli utenti non autorizzati, che ai soggetti con privilegi limitati, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati, cancellati o “esfiltrati”.

Se la sicurezza di dati e informazioni viene meno, a risentirne non è solo la privacy, ma anche la tutela del patrimonio aziendale per le Società.

Si sottolinea **l’IMPORTANZA DELLA PREVENZIONE**, delle STRATEGIE di DIFESA e di RIPRISTINO **IN CASO DI ATTACCO**.

Cybersecurity: la normativa in materia in sintesi

Sono numerosi i provvedimenti in tema di Cybersecurity negli ultimi tempi:

- Il **Decreto Legge n.105/2019** – convertito con la recentissima legge del 18 novembre 2019, n. 133 - ha ufficialmente istituito il c.d. «***perimetro di sicurezza nazionale cibernetica***».
- Il **D. Lgs n. 65/2018** di recepimento della **Direttiva NIS n. 2016/1148** sulla sicurezza delle reti.
- **Il Regolamento (UE), n. 943 del 5 giugno 2019** sul mercato interno dell'energia elettrica, facente parte del c.d. "***Clean Energy Package***".

- Il **Regolamento (UE), n. 881 del 17 aprile 2019** relativo all'ENISA, ed alla certificazione della cyber-sicurezza nell'ambito delle nuove tecnologie («***Cybersecurity Act»).***
- **Raccomandazione n. 553 del 3 aprile 2019 della Commissione Europea**, che ha indicato misure consigliate agli Stati Membri al fine di conseguire un livello di cybersecurity elevato nel settore dell'energia.

SANZIONI E RESPONSABILITA’

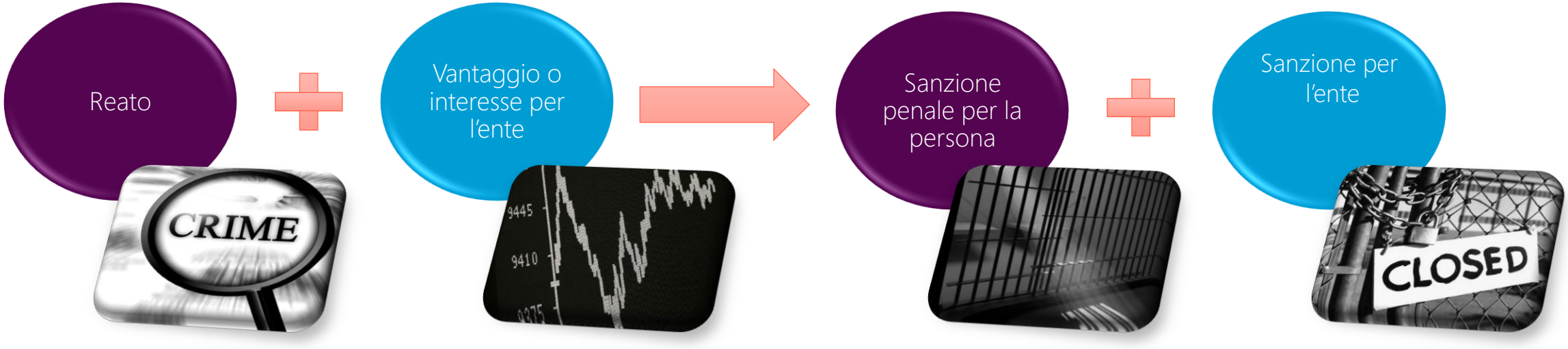
- Regime sanzionatorio severissimo a carico dei soggetti appartenenti al perimetro di sicurezza e che risulteranno inadempienti rispetto alle condizioni imposte dal Centro di valutazione e certificazione nazionale (CVCN) → **Sanzione pecuniaria massima pari sino a 1.800.000 euro**

- Nuove fattispecie di reato presupposto, in materia di responsabilità amministrativa degli enti ex D. lgs 231/2001, qualora siano ostacolati gli adempimenti e le attività ispettive e di vigilanza, necessari per la formazione e il mantenimento del perimetro di sicurezza → **Sanzione pecuniaria per l’Ente ai sensi del Decreto.**

Il Decreto 231 in sintesi

Il D.Lgs. 231/2001 introduce in Italia la responsabilità amministrativa degli enti (sia italiani che esteri operanti in Italia) per alcuni reati c.d. presupposto, commessi, nel loro interesse o a loro vantaggio, da amministratori e dipendenti dell'ente, nonché da terzi sottoposti alla direzione e vigilanza di questi.

Tra i reati presupposto ci sono anche **i c.d. Reati IT.**



EFFICACIA ESIMENTE DEL MODELLO ORGANIZZATIVO

NECESSARIO IL RISK ASSESSMENT E LA MAPPATURA DEI RISCHI

CYBERCRIME E CYBERSECURITY:MAPPATURA INTEGRATA DEI RISCHI

La Normativa in tema di Cybersecurity, il D. Lgs. 231/01 in tema di Responsabilità Amministrativa degli Enti e Cybercrimes, nonche' il c.d. GDPR (REG. UE 679/2016) – **Rischi sanzione**

Rischi di danno ai propri dati ed al proprio patrimonio aziendale, perdita di **Business Continuity** – **Rischi patrimoniali**

Rischio di **Danni reputazionali**

Quale *Compliance* per le Imprese del Settore Energy?

L'elaborazione normativa non è giunta ancora a enucleare al massimo livello di dettaglio le misure di *cyber security*, stante il complesso processo di implementazione della normativa di attuazione

...le imprese possono quindi attendere l'esatta definizione delle misure da adottare, giusto?

Per le imprese, risulta prioritario prevenire e gestire sin da subito tutti i rischi *cyber* in modo integrato, al fine di MITIGARE non solo LE **SANZIONI**, ma anche IL RISCHIO DI **INCIDENTI**

I Modelli Organizzativi Integrati

Le imprese operanti nel settore energy devono quindi procedere al ***Risk Assessment***, così da mappare e circoscrivere **tutti** i rischi in ambito «***cyber***».

L'adozione di ***Policy e procedure organizzative*** **adeguate,** anche nell'ambito di Modelli Organizzativi integrati, risulta indispensabile per prevenire e mitigare i rischi cyber

SONO 4 LE QUALITA' DA GARANTIRE

Disponibilità, Integrità, Confidenzialità e Resilienza

Disponibilità

- Garantire la disponibilità agli utenti legittimi, protezione delle infrastrutture, policy/procedure di business continuity & disaster recovery
- Errori sw/hw, eventi ambientali (terremoti, allagamenti, mancanza energia elettrica), azioni malevole

Integrità

- La capacità di mantenere la veridicità dei dati e delle risorse e garantire che non siano in alcun modo modificate o cancellate
- Controllo degli accessi (Identity/access management)

Confidenzialità

- Accessibilità dei dati solo agli utenti (e ai processi) che ne hanno effettivamente diritto
- Cifratura dei dati («a riposo» e «in transito»), adozione di procedure di autenticazione adeguate, attività di formazione

Resilienza

- capacità di assorbire il disturbo e mantenere funzionanti i propri processi di business, i servizi e i sistemi

CONCLUSIONI

In attesa di maggiore dettagli da parte degli ulteriori provvedimenti attuativi, l'auspicio, in conclusione, è che le impresse che operano nel settore *energy*, ivi comprese le PMI, e che stanno sviluppando nuovi modelli di business nel contesto digitale, siano sempre più consapevoli della pericolosità dei rischi cyber e si convincono quindi dell'ineluttabilità di adottare Modelli Organizzativi Integrati, volti a mitigare tali rischi.

ANCHE IN AMBITO CYBER PREVENIRE E' MEGLIO CHE CURARE!