Cybersecurity Awareness per le terze parti

Cybersecurity Awareness for third parties

Italgas

Cybersecurity Awareness per le terze parti

Cybersecurity Awareness for third parties

Italgas

Cybersecurity Awareness per le terze parti

Il Gruppo Italgas, principale Società che distribuisce gas in Italia, è costantemente coinvolta in attività di miglioramento della propria rete infrastrutturale, con lo scopo di sfruttare al massimo le opportunità derivanti dal progresso tecnologico e di garantire un servizio/prodotto sempre più attento ai bisogni del mercato. In tale contesto il Gruppo si avvale sempre di più di sistemi tecnologici interconnessi e di terze parti specializzate che forniscono supporto per l'implementazione e la manutenzione degli stessi.

Al tempo stesso, però, il Gruppo Italgas è consapevole dell'importanza che assume la gestione dei rischi e delle minacce di natura Cyber che sottende il processo di innovazione tecnologica. Per tale motivo il Gruppo promuove attività di sensibilizzazione della propria popolazione aziendale e dei propri partner, al fine di garantire la protezione del patrimonio informativo e mitigare i rischi Cyber. Nello specifico le terze parti coinvolte nei processi del Gruppo Italgas, svolgono un ruolo

Cybersecurity Awareness for third parties

Italgas Group is the main Italian Gas retailer company and it is constantly involved in upgrading activities to improve its network infrastructures. The Company aims, from the one hand, to take full advantage of the opportunities arising from technological progress, and on the other, to offer a service/product that always takes care of market needs. Within this context, Italgas Group takes benefit from high technological and interconnected systems and from specialized third parties able to provide support for its implementation and maintenance.

However, the Italgas Group is aware of the fact that managing cyber threats and risks is a crucial activity in the technological innovation process. At this regard, Italgas Group is engaged in fostering awareness campaigns to its corporate population and to its partners in order to increase the protection of its asset and to mitigate any cyber risk. In particular, third parties involved in Italgas' processes have a crucial and active role within the process of managing cyber risks. Therefore, the

attivo ed importante nella gestione dei rischi Cyber, pertanto il riconoscimento della loro attenzione su tali tematiche è di fondamentale importanza.

Le attività di trattamento delegate a terzi, outsourcers o fornitori, costituiscono spesso rilevanti fattori di rischio per la sicurezza delle informazioni che potrebbero avere un impatto, a titolo esemplificativo e non esaustivo su:

- Fiducia dei clienti nel brand aziendale;
- Perdita di denaro e di valore (ad esempio legata al ripristino dell'infrastruttura di rete);
- Efficacia ed efficienza dell'operatività;
- Erogazione del servizio;
- Riservatezza dei dati;
- Conformità normativa;
- Furto di proprietà intellettuali.

Per tali motivi, l'applicazione degli opportuni processi di Cybersecurity da parte delle terze parti coinvolte si rende necessaria per proteggere il patrimonio informativo del Gruppo

acknowledgement of their commitment on the cyber issue is a key point.

Processing activities outsourced to third parties, outsourcers or suppliers, represents a risk for information security. Cyber-attacks to corporate data could have a negative impact on some elements, such as, by way of example:

- Customer trust in corporate brand;
- Loss of money and value (for example related to network infrastructure recovery);
- Effectiveness and efficiency of operation;
- Provision of the service;
- Confidentiality of data;
- Regulatory compliance;
- Theft of intellectual property.

As a consequence, it is necessary that those third parties involved should adopt some cyber security measures and processes in order to protect from cyber threat firstly Italgas' information asset, but also the third party itself.

Italgas, nonché della terza parte coinvolta, da minacce Cyber. I principi essenziali che concorrono alla definizione di un livello adeguato di sicurezza sono:

- *Conformità alle best practices*: adottare e implementare le best practices in materia di Cybersecurity al fine di assicurare un elevato livello di sicurezza delle reti e dei sistemi informativi utilizzati per erogare i servizi.
- *Controlli di sicurezza*: concordare e garantire l'adozione di controlli di sicurezza che possano prevenire l'insorgenza della minaccia Cyber. I fornitori sono pertanto chiamati a prevenire il verificarsi di scenari di attacco in modo da proteggere sia i propri asset aziendali sia quelli del Gruppo Italgas. L'adozione dei controlli di sicurezza crea pertanto un beneficio comune a tutela del vantaggio competitivo.
- *Ridurre la superficie di attacco*: provvedere proattivamente ad identificare e mitigare i rischi di sicurezza esistenti portandoli ad un livello ritenuto accettabile. La terza parte non dovrà soltanto implementare le misure tecniche ed organizzative a protezione del patrimonio informativo, bensì dovrà inoltre assicurare la consapevolezza dei propri

Core principles of an adequate level of security are:

- *Best practice compliance*: adopt and implement cybersecurity best practice with the aim to ensure a high level of security of those infrastructures and data systems involved in the service supply;
- *Security check*: arrange and ensure the adoption of security checks to prevent the occurrence of attack scenarios in a way to protect both its own and Italgas' asset. The adoption of security controls generates a common benefit to keep competitive edge safe;
- *Reduce attack perimeter*: proactively identify and mitigate security risks addressing them to an acceptable level. Third parties should firstly, implement technical and organizational measures to protect data asset, then, they should guarantee the awareness of their employees concerning misconduct, such as password sharing, and finally they should increase malicious attacks identification activities (ex. social engineering);

dipendenti relativamente a comportamenti scorretti quali, a titolo esemplificativo e non esaustivo, la condivisione di credenziali, e dovrà migliorare le attività di identificazione di eventuali attacchi malevoli (es. attività di social engineering).

- *Set minimo di privilegi*: garantire l'adozione di minimi privilegi necessari per l'adempimento delle attività strettamente necessarie; assegnare i privilegi secondo un approccio tailor-made contribuisce nell'effettivo controllo delle attività consentite ai diversi ruoli aziendali a supporto del Gruppo Italgas e riduce notevolmente la superficie di attacco.
- *Separation of Duties*: garantire la separazione dei compiti per limitare comportamenti fraudolenti. L'applicazione di tali regole favorisce oltre allo sviluppo e il monitoraggio del sistema di controllo interno anche l'individuazione dei processi di business più critici.
- *Gestione sicura degli errori*: gestione proattiva e sicura degli errori generati da un sistema.
- *Risolvere adeguatamente le problematiche di sicurezza*: in presenza di vulnerabilità di sicurezza per un sistema, prima di procedere alla mitigazione della vulnerabilità stessa, occorre verificare che il sistema in questione non

- *Minimum set of privileges*: ensure the adoption of minimum privileges used to fulfill only those activities strictly necessary; assign privileges following a tailor-made approach contributes to the effective control over the activities managed by corporate roles supporting Italgas Group and it also reduces significantly the perimeter of attack;
- *Separation of duties*: ensure the separation of duties in order to limit fraudulent behaviors. Following this rule is useful not only to the development and monitoring of internal control system, but also to the identification of the most critical business processes.
- *Secure management of errors*: proactive and secure management of errors generated by a system;
- *Solve security issues*: in case of security vulnerability for a system, even before mitigating the vulnerability itself, it shall be verified that the system involved does not share the same architecture with other systems. If it does so, it is necessary to identify a solution which may not impact negatively on other systems and that minimizes the risks arose from the identified vulnerability.
- *Secure managing of third parties*: guarantee a secure

condivida la medesima architettura con altri sistemi. In tal caso, è necessario identificare una soluzione che non impatti negativamente anche gli altri sistemi e che minimizzi il rischio derivante dalla vulnerabilità identificata.

- *Gestione sicura delle terze parti*: garantire una gestione sicura di eventuali terze-parti/sub-fornitori che rientrano della Cyber Supply Chain. Tale elemento assume un ruolo ancor più fondamentale in tutte quelle casistiche in cui è previsto il coinvolgimento di ulteriori terze parti. Il monitoraggio e la garanzia dell'implementazione delle opportune misure di sicurezza da parte di quest'ultime non garantisce soltanto la protezione del patrimonio aziendale, bensì favorisce il consolidamento della reputazione del rapporto tra il Gruppo Italgas e la controparte primaria.

Conseguentemente, la definizione e l'applicazione di presidi tecnici ed organizzativi di sicurezza è di fondamentale importanza per la protezione del patrimonio informativo del Gruppo Italgas da attacchi Cyber. Le terze parti coinvolte dal Gruppo dovrebbero quindi assicurare, a titolo esemplificativo e non esaustivo:

management of third parties/ sub-suppliers which are involved within the Cyber Supply Chain; This element is even more relevant when it comes to the engagement of additional third parties. Monitoring activities and the guarantee of third parties' implementation of security requirements permit to protect Italgas' corporate asset as well as to strengthen the reputational relationship between Italgas Group and its primary counterpart.

Consequently, in order to protect Italgas' data asset from cyber-attacks, the definition and the application of technical and organizational security measures result a key point. Third parties involved by Italgas Group should, then, ensure some measures, such as:

- Definition of a documental framework which includes policies and procedures useful to manage cybersecurity and data protection activities;
- Definition of roles and responsibilities to manage efficiently and effectively cybersecurity and data protection processes;
- Definition and implementation of technical measures to ensure network monitoring to prevent cybersecurity events;
- Implementation of technical measures to protect networks,

- Definizione di un framework documentale che preveda policy e procedure per la gestione delle attività di Cybersecurity e Data Protection;
- Definizione di Ruoli e Responsabilità per la gestione efficace ed efficiente dei processi di Cybersecurity e Data Protection;
- Definizione ed implementazione di misure tecniche per assicurare il monitoraggio delle reti per prevenire eventi di Cybersecurity;
- Implementazione di misure tecniche per la protezione delle reti, dei sistemi e degli applicativi dell'organizzazione (es. Firewall, software antimalware, meccanismi di cifratura dei dati, utilizzo di protocolli di sicurezza per la protezione delle comunicazioni, adozione di tecniche di cancellazione sicura, ecc.);
- Definizione di misure tecniche ed organizzative per la protezione fisica dei locali nei quali sono presenti sistemi critici;
- Definizione e implementazione di misure organizzative e tecniche per garantire la continuità operativa dei processi critici a fronte di eventi anomali. A titolo esemplificativo, definizione di policy e procedure in ambito continuità

systems and company applications (ex. Firewall, software anti malware, data encryption, use of security protocols to protect communications, adoption of secure erase techniques etc.)
- Definition of technical and organizational measures for physical protection of premises where critical systems are present;
- Definition of technical and organization measures to guarantee business continuity of critical processes facing unexpected events. For example, definition of policies and procedures in the field of business continuity, implementation of backup systems and redundancy and deployment of high reliability;
- Definition of security requirements in contracts with suppliers and third parties active in the Cyber Supply Chain, also through the adoption of specific business continuity agreements and Service Level Agreement which ensure an acceptable level of service;
- Regularly evaluation of suppliers and third parties through audit, checks or other methods of evaluation to verify the compliance with contractual obligations;

operativa, implementazione di sistemi di backup e ridondanza e l'implementazione di sistemi in alta affidabilità;
- Definizione dei requisiti di sicurezza nei contratti con i fornitori e i partner terzi che rientrano nella Cyber Supply Chain, anche attraverso l'adozione di accordi di continuità operativa specifici e Service Level Agreement che garantiscano un livello di servizio accettabile;
- Valutazione regolare di fornitori e partner terzi attraverso audit, verifiche, o altre forme di valutazione per confermare il rispetto degli obblighi contrattuali;
- Definizione di programmi di Training and Awareness in ambito Cybersecurity per la popolazione aziendale al fine di sensibilizzare l'organizzazione relativamente alle tematiche di Cybersecurity, minacce esistenti e relativi impatti per l'organizzazione.

- Definition of Cybersecurity Training and Awareness programs for the corporate population with the aim to raise the awareness of the organization concerning cyber issues, existing threats and negative impacts on business.

Sede Legale Italgas S.p.A.
Via Carlo Bo, 11
20143 - Milano

Sede Sociale in Milano
Codice Fiscale/P.I. 09540420966
R.E.A. Milano n. 2097057

Società aderente
al "Gruppo IVA Italgas"
P.I. 10538260968

www.italgas.it


Italgas