Swissgrid SA
Bleichemattstrasse 31
Casella postale
5001 Aarau
Svizzera

T +41 58 580 21 11
info@swissgrid.ch
www.swissgrid.ch

Scheda informativa

Cybersecurity per le infrastrutture critiche

Data Giugno 2023

1 Trasformazione digitale e sicurezza informatica: capire i rischi

Il termine «digitalizzazione» si riferisce al processo di utilizzo delle tecnologie digitali per trasformare e automatizzare le operazioni e i processi aziendali. Ciò può includere l'uso di tecnologie come il cloud computing, l'Internet of Things (IoT), l'analisi dei big data e l'apprendimento automatico, tra le altre. Gli obiettivi di questi sforzi di digitalizzazione sono l'ottimizzazione dell'efficienza operativa, il miglioramento dell'accuratezza della pianificazione e il potenziamento dell'affidabilità operativa, della sicurezza e della resilienza.

Di conseguenza, l'infrastruttura delle reti elettriche è sempre più controllata da tecnologie intelligenti delle informazioni e della comunicazione. La disponibilità, l'integrità o la riservatezza dei dati e dei sistemi sono potenziali fattori di rischio: nel peggiore dei casi, le minacce informatiche possono portare a un blackout diffuso, lasciando vaste aree senza elettricità per un periodo di tempo prolungato. Ciò potrebbe causare notevoli interruzioni ai servizi essenziali e alle infrastrutture critiche, nonché alla società e all'economia.

È essenziale che gli operatori delle infrastrutture critiche implementino solide misure di sicurezza informatica per prevenire i cyberattacchi e mitigare l'impatto potenziale di un attacco.

2 Sicurezza informatica: una priorità assoluta

In qualità di gestore di infrastrutture critiche, Swissgrid riconosce l'importanza della sicurezza informatica nell'attuale panorama digitale. Diamo priorità all'implementazione di solide misure di sicurezza per salvaguardare i nostri sistemi e garantire il funzionamento sicuro della rete di trasmissione svizzera.

Il programma di sicurezza informatica di Swissgrid si basa sui seguenti pilastri:

- Valutazione dei rischi: il programma identifica e valuta i rischi di sicurezza informatica per le informazioni e i sistemi dell'organizzazione.
- Governance: il programma definisce ruoli, responsabilità e processi per gestire i rischi di sicurezza informatica e garantire la responsabilità.
- Asset management: il programma identifica e gestisce tutti gli asset, compresi hardware, software e dati, per comprenderne il valore e la criticità per l'organizzazione.
- Controllo degli accessi: il programma limita l'accesso ai dati e ai sistemi sensibili al personale autorizzato e utilizza l'autenticazione a più fattori per proteggere l'accesso.

- Risposta agli incidenti: il programma stabilisce un piano per rispondere agli incidenti di sicurezza informatica e ridurre al minimo il loro impatto sull'organizzazione.

- Formazione sulla security awareness: il programma prevede la formazione continua di tutto il personale sulle best practices legate alla sicurezza informatica e sul loro ruolo nella protezione degli asset dell'organizzazione.

- Monitoraggio continuo: il programma monitora costantemente i sistemi e le reti dell'organizzazione alla ricerca di potenziali minacce per la sicurezza, identificando e riducendo i rischi in modo proattivo.

- Business continuity management (BCM): il programma incorpora pratiche di BCM per garantire la continuità dei processi aziendali critici in caso di incidenti di sicurezza informatica o altre interruzioni.

- Disaster recovery: il programma stabilisce un piano di disaster recovery per ripristinare i sistemi e i dati critici in caso di incidenti di sicurezza informatica o altri eventi che comportino interruzioni.

- Collaborazione esterna: il programma collabora con partner esterni, come aziende del settore, fornitori e autorità, per identificare e mitigare i rischi di sicurezza informatica.

Il panorama delle minacce è in continua evoluzione e gli aggressori informatici sono sempre alla ricerca di nuove vulnerabilità e tecniche per sfruttarle. Pertanto, un programma di sicurezza informatica non può essere implementato una tantum, ma deve essere un processo di miglioramento continuo.

Questo comporta la revisione e la valutazione periodica del programma di sicurezza informatica, l'identificazione dei punti deboli e degli ambiti di miglioramento e l'apporto delle modifiche necessarie per rafforzare il programma. Questo processo dovrebbe essere accompagnato da regolari valutazioni delle minacce e ricerche di vulnerabilità, nonché da una formazione continua per il personale e dalla collaborazione con partner esterni.

Incorporando il miglioramento continuo nel nostro programma di sicurezza informatica, puntiamo ad anticipare le minacce emergenti, adattandoci alle circostanze mutevoli e mantenendo un elevato livello di sicurezza nel tempo.

Il sistema di gestione della sicurezza delle informazioni di Swissgrid è stato certificato secondo la norma ISO/IEC 27001, uno degli standard internazionali di sicurezza delle informazioni più riconosciuti e accettati.

3 Sintesi

La digitalizzazione comporta l'utilizzo di reti, cloud computing e altre piattaforme digitali che possono essere vulnerabili agli attacchi informatici. Le imprese devono implementare solide misure di sicurezza informatica per proteggere i propri sistemi e dati da interruzioni, violazioni, furti e altri tipi di minacce informatiche.

In qualità di gestore di infrastrutture critiche, Swissgrid considera la protezione dalle minacce informatiche una priorità assoluta e si impegna in un processo costante di miglioramento continuo.