Swissgrid AG
Bleichemattstrasse 31
Case postale
5001 Aarau
Suisse

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

Fiche d'information

La cybersécurité pour les infrastructures critiques

Date Juin 2023

1 Transformation numérique et cybersécurité: comprendre les risques

La numérisation désigne le processus d'utilisation des technologies numériques pour transformer et automatiser les opérations et processus opérationnels. Elle peut inclure, entre autres, l'utilisation de technologies telles que l'informatique en nuage, l'internet des objets (IdO), l'analyse du big data et l'apprentissage automatique. Le but de cette numérisation est d'optimiser l'efficacité opérationnelle, d'améliorer la précision dans la planification et de renforcer la fiabilité, la sécurité et la résilience des opérations.

Par conséquent, l'infrastructure des réseaux de distribution est de plus en plus contrôlée par des technologies d'information et de communication intelligentes. La disponibilité, l'intégrité ou la confidentialité des données et des systèmes sont des facteurs de risque potentiels: dans le pire des cas, les cybermenaces peuvent entraîner un effondrement généralisé du réseau, privant d'électricité de vastes zones pendant une période prolongée. Cela pourrait perturber fortement le fonctionnement des services essentiels et des infrastructures critiques, ainsi que la société et l'économie.

Il est essentiel que les exploitants d'infrastructures critiques mettent en œuvre des mesures de cybersécurité solides afin de prévenir les cyberattaques et d'en atténuer les conséquences potentielles.

2 La cybersécurité: une priorité absolue

En tant qu'exploitant d'une infrastructure critique, Swissgrid reconnaît l'importance de la cybersécurité dans le paysage numérique actuel. Nous accordons la priorité à la mise en œuvre de mesures de sécurité robustes afin de protéger nos systèmes et d'assurer une exploitation sûre du réseau de transport suisse.

Le programme de cybersécurité de Swissgrid repose sur les piliers suivants:

- Évaluation des risques: le programme identifie et évalue les risques en matière de cybersécurité pour les informations et les systèmes de l'organisation.
- Gouvernance: le programme définit les rôles, les domaines de responsabilité et les processus permettant de gérer les risques liés à la cybersécurité et de garantir la responsabilisation.
- Asset Management: le programme identifie et gère tous les actifs, y compris le matériel, les logiciels et les données, afin de comprendre leur valeur et leur importance pour l'organisation.

- Contrôle d'accès: le programme limite l'accès aux données et systèmes sensibles au personnel autorisé et utilise l'authentification multifactorielle pour sécuriser l'accès.

- Réponse aux incidents: le programme établit un plan pour répondre aux incidents de cybersécurité et minimiser leur impact sur l'organisation.

- Formation de sensibilisation à la sécurité: le programme offre une formation continue à tous les membres du personnel sur les bonnes pratiques en matière de cybersécurité et sur leurs rôles dans la protection des actifs de l'organisation.

- Surveillance continue: le programme surveille en permanence les systèmes et les réseaux de l'organisation pour détecter les menaces de sécurité potentielles, et il identifie et atténue les risques de manière proactive.

- Business Continuity Management (BCM): le programme intègre des pratiques BCM afin de garantir que les processus opérationnels essentiels puissent se poursuivre en cas d'incident de cybersécurité ou d'autre perturbation.

- Reprise après sinistre: le programme établit un plan de reprise après sinistre pour restaurer les systèmes et données critiques en cas d'incident de cybersécurité ou d'autre perturbation.

- Collaboration externe: le programme collabore avec des partenaires externes, tels que des pairs de l'industrie, des fournisseurs et des agences gouvernementales, afin d'identifier et d'atténuer les risques liés à la cybersécurité.

Le paysage des menaces est en constante évolution et les cyberattaquants sont toujours à la recherche de nouvelles vulnérabilités et de techniques pour les exploiter. Par conséquent, un programme de cybersécurité ne peut pas être mis en œuvre une seule fois; il doit faire l'objet d'une amélioration continue permanente.

L'amélioration continue consiste à examiner et à évaluer régulièrement le programme de cybersécurité, à identifier les failles et les domaines à améliorer, et à procéder aux ajustements nécessaires pour renforcer le programme. Ce processus doit s'appuyer sur des évaluations régulières des menaces et sur des analyses de vulnérabilité, ainsi que sur la formation continue du personnel et sur la collaboration avec des partenaires externes.

En intégrant l'amélioration continue dans notre programme de cybersécurité, nous visons à garder une longueur d'avance sur les menaces émergentes en nous adaptant aux circonstances changeantes et en maintenant un niveau élevé de sécurité au fil du temps.

Le système de gestion de la sécurité de l'information de Swissgrid a été certifié ISO/IEC 27001, l'une des normes internationales les plus largement reconnues et acceptées en matière de sécurité de l'information.

3 Résumé

La numérisation implique l'utilisation de réseaux, de l'informatique en nuage et d'autres plateformes numériques qui peuvent être vulnérables aux cyberattaques. Les organisations doivent mettre en œuvre des mesures de cybersécurité solides pour protéger leurs systèmes et leurs données contre les perturbations, les intrusions, le vol et d'autres types de cybermenaces.

En tant qu’exploitant d’une infrastructure critique, Swissgrid considère la protection contre les cybermenaces comme une priorité absolue et s’engage dans un processus d’amélioration continue.