

21 avril 2020
16h00 (GMT+2)

Web conférence COVID-19 pour les opérateurs électriques Que faut-il retenir ?

Session 2 - La cybersécurité et la sécurité physique des salariés dans la crise du COVID-19



ENJEUX DE CYBERSÉCURITÉ ET SÉCURITÉ PHYSIQUE

Le contexte de la crise du COVID-19 est propice à la multiplication d'actes de malveillance, qu'il soient cyber ou physiques. La crise favorise l'exposition au risque cyber en créant de nouvelles opportunités pour des acteurs malveillants (manque d'organisation, process de travail à distance moins contrôlés, pratiques non autorisées des employés...). La mise en place d'une réelle gouvernance, en particulier sur le volet sensibilisation, est essentielle pour gérer le risque cyber.

INFORMATIONS CLÉS POUR LE SECTEUR DES OPÉRATEURS ÉLECTRIQUES

Quels impacts de la crise COVID-19 ?

- **Demande** : baisse de la consommation observée dans la plupart des pays, avec des variations selon la typologie de la demande propre à chaque pays (ordre de grandeur moyen 10 - 20%).
- **Augmentation du prix des modules photovoltaïques** prévu en Chine (de 10 à 15% sur la seconde moitié de 2020) : causée par la hausse du prix des matières premières (baisse de la production et difficultés d'approvisionnement). Potentiel impact sur des projets à venir, notamment pour les énergies renouvelables.
- **Difficultés pour mener à bien certaines actions de maintenance** : du fait de l'impossibilité de déplacements international ou transnational (ex : besoin d'experts internationaux ou d'ingénieur certifié par le constructeur), qui doivent ainsi être reportées.
- **Action du secteur public** de plus en plus marquée : soit par une intervention au niveau des sociétés d'électricité soit par des aides auprès des consommateurs.
- **Enjeux de sécurité des sites et des stocks** : vols de composants, câbles, carburants... des types d'actes malveillants qui se produisent souvent en période de crise.
- **Nécessité de mettre à jour temporairement les méthodes de production**, de reporter la production pour les semaines à venir. Ex : EDF (France) qui diminue sa production d'électricité d'origine nucléaire.

Quels risques de cybersécurité et sécurité physique ?

- Les **risques cyber** présentés peuvent s'appliquer à tous les opérateurs, quel que soit leur niveau d'activités. De manière générale, de nombreux opérateurs ne sont **pas suffisamment préparés pour les enjeux cyber** liés au télétravail, en particulier pour leurs fonctions administratives et financières.
- Principaux risques :
 - Dans les centrales, sur des sites isolés, il est important de **sensibiliser les employés** pour éviter l'utilisation d'applications personnelles sur des **ordinateurs connectés à des SCADA**.
 - Vérifier que les **producteurs indépendants** sont à même de sécuriser leur SI et de réagir en cas d'attaque.
 - Importance de la **mise à jour régulière des pare-feux pour les SI (en particulier ceux liés au dispatching)**.
 - Enjeux de **protection des données confidentielles au niveau du siège** pour la réputation de l'entreprise (plans de développement, appels d'offres, données commerciales des contrats).
 - Enjeux de **protection des données personnelles des usagers** contre le risque de fuite.
- Sur les sites de production isolés, les **mesures contre les risques d'hygiène, sécurité et sûreté des personnels peuvent également s'appliquer aux familles** qui vivent à proximité. Les **sous-traitants** doivent également être pris en compte pour l'application de ces mesures, en particulier les fournisseurs individuels ou entrepreneurs (ex : relève).
- Dans le contexte du COVID-19, la **fonction HSE doit répondre à de nouvelles attentes** : capacité de **conseiller et orienter les opérations et la production (organisation des équipes, des rotations, etc.)**.

Date de la prochaine session : Jeudi 23/04 à 16h00 (GMT+2)

Si vous souhaitez échanger sur vos difficultés, vos bonnes pratiques OU si vous avez des questions à aborder pour les prochaines sessions, n'hésitez pas à nous contacter :

fr_conferencecovid19@pwc.com