Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

29.11.2023

Rapport explicatif relatif à la révision de novembre 2023 de l'ordonnance sur la sécurité des installations de transport par conduites

Table des matières

1. Contexte

Les technologies de l'information et de la communication (TIC) soutiennent le développement d'un approvisionnement en énergie flexible et efficace. Elles sont ainsi de plus en plus utilisées pour la surveillance et le pilotage des réseaux d'approvisionnement en énergie. Bien qu'elles contribuent à nombre d'optimisations, elles augmentent également l'exposition aux cyberattaques et constituent par conséquent de nouvelles sources de risque.

La sécurité de l'approvisionnement en énergie revêt une importance stratégique certaine. Une exploitation sûre garantit la protection de biens juridiques importants. La dépendance de notre système socio-économique aux sources d'énergie est telle qu'une défaillance grave aurait des conséquences désastreuses. La menace d'une cyberattaque contre les réseaux d'énergie est aujourd'hui particulièrement tangible.

La Stratégie nationale de protection des infrastructures critiques 2018–2022[1] et la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018 à 2022[2] définissent des mesures adéquates destinées à améliorer la résistance générale des infrastructures critiques. La SNPC[3] prévoit à cet effet l'élaboration et l'introduction de normes minimales en matière de sécurité des TIC, lesquelles ont été mises en œuvre par le biais des « normes minimales pour les TIC» [4]. Ces normes définissent un éventail de mesures et constitue par conséquent un instrument important pour assurer la protection contre les cyberattaques. Sur cette base, la branche a élaboré des recommandations[5] qui ont pour la première fois posé les fondements nécessaires à la cybersécurité dans le système d'approvisionnement en gaz. Toutefois, ces normes minimales du secteur sont en principe facultatives et ne sont dès lors pas encore appliquées systématiquement. En raison de l'intensification des menaces[6], il est donc impératif de déclarer ces recommandations contraignantes à moyen terme pour les entreprises dont la défaillance provoquerait des conséquences désastreuses. Pour ce faire, ces recommandations doivent être formulées de manière suffisamment claire et précise. Les bases légales existantes doivent dès lors être révisées rapidement et de façon ciblée, et les responsabilités doivent être clairement définies.

2. Présentation du projet

L'art. 39, al. 3, de l'ordonnance du 4 juin 2021 sur la sécurité des installations de transport par conduites (OSITC; RS 746.12) prévoit déjà que les exploitants sont tenus de protéger leurs équipements des influences perturbatrices extérieures, et par conséquent des cybermenaces. L'introduction du nouvel art. 39*a* vient réglementer spécifiquement l'obligation de protection contre les cybermenaces et définir la procédure visant à élaborer les mesures nécessaires à cet effet. En raison de l'interconnexion des systèmes TIC sur le plan technique et des risques qui y sont liés, cette disposition s'adresse à tous les exploitants, y compris ceux d'infrastructures dont la pression ne dépasse pas 5 bars (art. 1, al. 2).

Le Conseil fédéral précise ainsi la responsabilité quant à la protection contre les cybermenaces. Dans la perspective d'un renvoi direct et contraignant aux normes minimales du secteur concerné, il est nécessaire que celles-ci soient révisées de manière ciblée et avec le concours de l'Office fédéral de l'énergie (OFEN). La présente réglementation confie cette tâche aux exploitants. Les directives à élaborer

[1] FF 2018 491
[2] https://www.ncsc.admin.ch/dam/ncsc/fr/dokumente/strategie/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf.download.pdf/Nationale_Strategie_Schutz_Schweiz_vor_Cyber-Risiken_NCS_2018-22_FR.pdf
[3] Mesure 8, Normalisation et réglementation, SNPC 2018-2022, p.11
[4] Office fédéral pour l'approvisionnement économique du pays OFAE; «Norme minimale pour améliorer la résilience informatique», Berne, 2018 (en cours de révision)
[5] G1008 f Recommandation; Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en gaz, édition de décembre 2020
[6] SNPC 2018-2022, p. 2

devraient s'appuyer sur la norme minimale pour les TIC de l'Office fédéral pour l'approvisionnement économique du pays (OFAE) ainsi que sur les directives existantes de la branche. Elles devraient préciser les exigences opérationnelles et techniques et, sur la base des connaissances actuelles, tenir compte des conditions-cadres suivantes:

1. Définition des différents profils de protection. Chaque profil de protection englobe des mesures techniques et organisationnelles à un niveau de protection différent (p. ex. profil de protection A pour les exigences élevées, profil de protection B pour les exigences moyennes et profil de protection C pour les exigences faibles).
2. Établissement de critères permettant d'attribuer à l'exploitant le profil de protection approprié. Ces critères, qui permettent de catégoriser les exploitants en fonction de leur niveau de risque, sont souvent appelés «profils d'entreprise».
3. Précision de certaines exigences issues des normes actuelles. Une analyse menée avec la branche a montré que certaines exigences figurant dans la norme minimale pour les TIC et dans la directive de la branche doivent être précisées.

Lors de l'élaboration des points susmentionnés, la branche est tenue d'impliquer étroitement l'OFEN en sa qualité d'autorité de surveillance ou de haute surveillance des installations de transport par conduites. L'OFEN assure la coordination avec les services pertinents de l'administration fédérale centrale (l'OFAE, l'Office fédéral de la protection de la population, le Centre national pour la cybersécurité [NCSC]) et l'Inspection Fédérale des Pipelines (IFP).

3. Conséquences financières, conséquences sur l'état du personnel et autres conséquences pour la Confédération, les cantons et les communes

La mise en œuvre des modifications visées n'entraîne pas de coûts notables au niveau du personnel et des finances pour la Confédération, les cantons et les communes. En outre, la présente adaptation ne conduit qu'à un élargissement modéré du cahier des charges de l'OFEN, qui peut être couvert par les ressources en personnel et financières existantes.

Le projet de révision vise à augmenter le niveau de cybersécurité des installations de transport par conduites. Cela permet d'offrir une meilleure protection à moyen et long termes contre les cybermenaces, protection dont bénéficient en fin de compte la Confédération, les cantons et les communes. Les défaillances dues à des cyberattaques entraîneraient des conséquences financières considérables.

4. Conséquences économiques, environnementales ou sociales

Une cyberattaque peut avoir de lourdes conséquences économiques, environnementales et sociales pour le pays et la société, comme l'a montré l'incident survenu sur la Colonial Pipeline[7] aux États-Unis. Les coûts engendrés par un rançongiciel (rançon, fuite de données, temps nécessaire à la remise en exploitation, etc.) peuvent ainsi dépasser les coûts de sécurisation de l'infrastructure d'une entreprise. Les économies réalisées grâce à un niveau de cybersécurité suffisant et, partant, les avantages de la révision, sont donc d'autant plus élevés.

La mise en œuvre de mesures de cybersécurité entraîne des coûts en personnel et financiers pour les entreprises. Comme des mesures appropriées devaient déjà être prises conformément à la réglementation en vigueur, les coûts supplémentaires ne devraient pas être excessifs. Dès lors, seules les entreprises qui sont restées inactives en la matière doivent s'attendre à des conséquences importantes. En

[7] https://www.energy.gov/ceser/colonial-pipeline-cyber-incident (en anglais uniquement)

effet, les entreprises conscientes des risques et qui ont, au vu des menaces actuelles, déjà mis en œuvre des mesures de sécurité conformément à la directive de la branche, ne devront pas supporter de coûts supplémentaires, ou seulement dans une moindre mesure.

5. Comparaison avec le droit européen

L'Union européenne (UE) s'efforce d'améliorer la cybersécurité sur l'ensemble de son territoire et d'accroître la résilience de ses infrastructures critiques. Dans ce contexte, il convient de tenir compte de la directive SRI[8] et de celle qui lui a succédé, la directive SRI 2[9]. L'UE y prévoit notamment que les États membres doivent prendre des mesures afin de protéger les entreprises énergétiques majeures[10]. La directive NIS 2 a renforcé les exigences générales en matière de sécurité.

La présente réglementation améliore la cybersécurité dans le secteur des énergies liées aux installations de transport par conduites et prévoit à cet effet l'élaboration de mesures de protection *ad hoc*. Elle concorde ainsi avec les efforts déployés par l'UE pour améliorer la cybersécurité dans ce domaine. Les travaux menés à ce jour à propos des normes minimales du secteur s'alignent sur les normes internationales.

6. Commentaire des dispositions

Art. 39a Protection contre les cybermenaces

Al. 1: les mesures à prendre par les exploitants doivent prévenir tout dysfonctionnement des installations concernées ou, le cas échéant, y remédier le plus rapidement possible. Les mesures sont aussi bien de nature organisationnelle (p. ex. processus d'inventorisation, réglementation des compétences, sensibilisation) que technique (p. ex. sauvegardes ou recours à des technologies de protection).

Al. 2: cet alinéa charge les exploitants d'élaborer des directives contenant des mesures de protection contre les cybermenaces. Les exploitants peuvent s'organiser en conséquence dans le cadre des structures associatives existantes (Société suisse de l'industrie du gaz et des eaux, Association suisse de l'industrie gazière). Les travaux réalisés jusqu'à présent sur la base de la norme minimale pour les TIC de l'OFAE doivent être poursuivis et précisés dans ce cadre. La consultation prévue à cet alinéa permet de garantir l'implication de tous les acteurs intéressés. Outre les organes explicitement mentionnés à cet alinéa, on peut penser au NCSC, à l'OFAE et aux consommateurs. La conduite de la consultation incombe aux exploitants.

Al. 3: l'exigence selon laquelle les directives doivent être publiées sur un site Internet librement accessible vise à garantir un accès facilité à ces documents sans identifiant ou autre. Une fois les directives finalisées et publiées par les exploitants, le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) examinera si ces dernières se prêtent à un renvoi direct dans l'ordonnance (cf. art. 3, al. 2 et 3, OSITC). Les exploitants sont ainsi incités à élaborer une solution la plus judicieuse possible (il s'agit, autrement dit, d'autorégulation pilotée).

[8] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JO L 194 du 19.7.2016, p. 1
[9] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), JO L 333 du 27.12.2022, p. 80
[10] Voir notamment art. 21, al. 1, et annexe I de la directive SRI 2