Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

21 septembre 2023

Rapport explicatif concernant l'avant-projet relatif à la révision de mai 2024 de l'ordonnance sur l'approvisionnement en électricité (protection contre les cybermenaces)

1. Contexte

Les technologies de l'information et de la communication (TIC) participent au développement d'un approvisionnement en énergie flexible et efficace. Par conséquent, elles sont de plus en plus utilisées pour surveiller et piloter les réseaux d'approvisionnement en énergie ainsi que la production d'énergie. Bien qu'elles permettent des améliorations, elles augmentent également l'exposition aux cyberattaques et représentent ainsi de nouveaux risques.

La sécurité de l'approvisionnement énergétique a une importance stratégique. Une exploitation sûre permet d'assurer la protection d'importants biens juridiques. Notre système socioéconomique dépend de l'énergie à tel point qu'une défaillance majeure touchant sa production ou sa distribution aurait de lourdes conséquences. La menace d'une cyberattaque visant les réseaux énergétiques s'est fortement accrue; elle est aujourd'hui plus réelle que jamais.

La stratégie nationale pour la protection des infrastructures critiques 2018-2022 (PIC)[1] et la nouvelle cyberstratégie nationale (CSN)[2] prévoient des mesures visant à renforcer la résilience générale des infrastructures critiques. À cette fin, la CSN soutient la mise en œuvre de la norme minimale élaborée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) pour améliorer la résilience informatique (norme minimale TIC)[3] et examine les cas où des mesures contraignantes seraient nécessaires[4]. Ce document est appliqué sur une base volontaire. À l'heure actuelle, les mesures qu'il contient ne sont pas systématiquement mises en œuvre en Suisse dans le secteur de l'énergie.

En raison de la hausse des menaces et de leur caractère critique, il est crucial de pouvoir garantir un haut niveau de cybersécurité. Bien que les efforts entrepris jusqu'ici par les acteurs de la branche doivent être salués, ils restent insuffisants et trop rares au regard de la professionnalisation et de l'organisation des groupes criminels. Le rapport sur la cybersécurité[5] publié par l'Office fédéral de l'énergie (OFEN) en 2021 montre que la protection de l'approvisionnement en électricité est actuellement insuffisante et que l'État se doit par conséquent d'intervenir au niveau normatif. Les dernières évolutions dans le domaine de l'intelligence artificielle (p. ex. ChatGPT) vont encore faciliter la tâche des cybercriminels. Il importe d'améliorer la cyber-résilience des entreprises dans le domaine électrique, afin de pouvoir faire face aux défis à la fois actuels et futurs.

2. Présentation du projet

La révision de l'ordonnance du 14 mars 2008 sur l'approvisionnement en électricité (OApEl; RS 734.71) vise à rendre la norme minimale TIC obligatoire pour les principaux fournisseurs d'électricité. Elle contraint les acteurs tenus d'appliquer cette norme à atteindre un niveau de protection donné pour la mise en œuvre des mesures prévues. Afin de respecter le principe de proportionnalité, plusieurs niveaux (ou profils) de protection permettent d'échelonner les exigences.

2.1 Norme minimale TIC

La norme minimale TIC, qui fixe une série de mesures, est un instrument de protection majeur contre les cyberattaques. Elle se fonde sur le cadre de sécurité publié aux États-Unis par le *National Institute of Standards and Technology* (*NIST Cybersecurity Framework*[6]). Elle comporte 108 mesures réparties

[1] FF 2018 503
[2] www.ncsc.admin.ch > Stratégie CSN > Cyberstratégie nationale CSN
[3] Office fédéral pour l'approvisionnement économique du pays OFAE, «Norme minimale pour améliorer la résilience informatique», Berne, 2023
[4] Mesure 6, *Résilience, normalisation et régulation*, CSN, p. 20-22
[5] Office fédéral de l'énergie OFEN, «Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung» (en allemand avec résumé en français), Berne, juin 2021
[6] www.nist.gov/cyberframework

en 23 catégories. Sa structure permet d'évaluer et d'améliorer l'organisation de la cybersécurité dans les entreprises.

Les mesures ressortant de la norme forment un cadre fixe dans une large mesure, mais restent assez flexibles pour être adaptées aux risques spécifiques aux entreprises ainsi qu'aux nouvelles menaces, aux nouveaux outils technologiques et à l'évolution des connaissances techniques[7]. Elles ne prescrivent pas de solutions techniques: il appartient aux entreprises de les élaborer elles-mêmes. Pour ce faire, celles-ci peuvent aussi se regrouper dans le cadre des structures associatives existantes afin de créer une norme spécifique à leur secteur.

2.2 Niveau (ou profil) de protection

Le niveau de protection fixe les exigences quant au degré de mise en œuvre des mesures prévues dans la norme minimale TIC (valeurs / niveau Tier selon le chap. 3 de la norme minimale TIC). Le niveau de protection A comporte les exigences les plus strictes, les niveaux B et C des exigences moins élevées. Pour les plus petits acteurs du marché, les dispositions du niveau de protection C fixent des exigences régissant un nombre de mesures limité. Les mesures qui ne s'accompagnent pas de valeurs correspondantes ne doivent pas obligatoirement être mises en œuvre et gardent donc valeur de simples recommandations. Les différents niveaux de protection sont définis à la nouvelle annexe 1*a*. Les valeurs qui y figurent ont été fixées pour chaque niveau de protection en tenant compte de la criticité des entreprises et des moyens requis pour la mise en œuvre des mesures. Elles ont été déterminées par un groupe de travail de l'Association des entreprises électriques suisses (AES) auquel ont participé des spécialistes de l'Office fédéral de l'énergie (OFEN).

Des critères sont définis pour les entreprises afin de leur attribuer un niveau de protection (A,B ou C). Si une entreprise remplit les critères d'un niveau de protection donné, c'est ce niveau qui est déterminant pour elle. Par exemple, les gestionnaires de réseau dont le volume d'électricité transportée atteint au moins 450 GWh/an (ch. 1.1, annexe 1*a*) sont tenus d'appliquer le niveau de protection A. Les analyses et les pratiques émanant d'autres services spécialisés ont été prises en compte pour établir les critères. Ainsi, le critère de 450 GWh/an prévu pour les gestionnaires de réseau au niveau de protection A correspond à une valeur fixée par l'Office fédéral de la protection de la population (OFPP) pour les infrastructures critiques d'importance nationale. Quant au critère de 112 GWh/an fixé pour les gestionnaires de réseau et les prestataires au niveau de protection B, il correspond essentiellement à la valeur annualisée caractéristique d'une crise selon l'AES[8].

En ce qui concerne les producteurs et les exploitants de stockage, une puissance de 800 MW a été choisie pour le niveau de protection A et une puissance de 100 MW pour le niveau B. Cette dernière correspond à la valeur définie dans l'ordonnance sur l'énergie[9] pour les centrales de pompage-turbinage revêtant un intérêt national.

Si la puissance est inférieure à 100 MW, les producteurs, les exploitants de stockage et les prestataires de ces deux acteurs ne sont pas concernés par l'obligation de respecter la norme minimale TIC. Aucun profil de protection C n'est prévu pour eux. Dans la mesure où la valeur seuil de 100 MW n'est pas atteinte, la norme reste pour eux une simple recommandation. Ceci car, d'une part, leur influence sur la sécurité d'approvisionnement est plus faible que celle des gestionnaires de réseau qui accèdent directement au réseau via des technologies de pilotage, et car, d'autre part, contrairement aux gestionnaires de réseau, ils ne peuvent intégrer à leurs tarifs les coûts liés à la cybersécurité.

---

7 Chaque entreprise peut constater elle-même, à l'aide d'une analyse de risque, si les mesures minimales qu'elle est tenue de prendre sont suffisantes ou si des mesures supplémentaires sont requises. Pour assurer cette tâche, les entreprises peuvent s'aider du guide pour la protection des infrastructures critiques (PIC), publié par l'Office fédéral de la protection de la population (OFPP) et disponible sous www.infraprotection.ch > Protection des infrastructures critiques > Guide PIC

8 Association des entreprises électriques suisses (AES), «ICT Continuity», 2011

9 Art. 8, al. 4, de l'ordonnance du 1er novembre 2017 sur l'énergie (OEne; RS 730.01)

Si les prestataires externes qui gèrent les systèmes TIC sur mandat d'une entreprise ont un accès durable aux systèmes de pilotage (systèmes de gestion opérationnelle) de la mandante, ils sont soumis aux mêmes prescriptions qu'elle.

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 prévues n'a pas de conséquence notable sur les finances ou l'état du personnel pour la Confédération, les cantons ou les communes. Le projet de révision vise à rehausser le niveau de cybersécurité du secteur de l'électricité. Il a pour but d'offrir une meilleure protection contre les cybermenaces à moyen et à long terme, ce qui profite en dernier lieu à la Confédération, aux cantons et aux communes, étant donné que des perturbations dues à des cyberattaques entraîneraient de lourdes conséquences financières.

4. Conséquences économiques, environnementales ou sociales

Une cyberattaque peut avoir de graves conséquences économiques, écologiques ou sociales. Ainsi, les frais qu'entraîne l'attaque d'un rançongiciel pour une entreprise (rançon, perte de données, délai de restauration du service, etc.) peuvent dépasser les coûts requis pour assurer la sécurité de son infrastructure. Un niveau de cyberprotection adéquat permet d'éviter ces coûts élevés, c'est pourquoi la révision prévue revêt un intérêt majeur.

Étant donné que la réglementation en vigueur prescrit déjà des mesures préventives visant à garantir la sécurité de l'exploitation du réseau (art. 8 de la loi du 23 mars 2007 sur l'énergie [LApEl; RS 734.7] et art. 5 OApEl), aucune charge supplémentaire notable ne devrait être générée. Les entreprises conscientes des risques qui ont d'ores et déjà instauré des mesures de sécurité n'auront pas à prendre en charge des coûts supplémentaires, ou seuls des coûts mineurs. Seules les entreprises qui, malgré les prescriptions existantes, n'ont rien entrepris en matière de cybersécurité doivent s'attendre à des conséquences majeures.

En général, on estime que les coûts liés à la cybersécurité d'une entreprise représentent environ 6 à 14% des dépenses allouées à l'informatique ou environ 0,3 à 0,5% de son chiffre d'affaires annuel. Il faut toutefois mettre ces coûts en perspective en les comparant à ceux causés par un cyberincident, tel que le chantage d'un pirate informatique après une attaque au rançongiciel, qui sont estimés en moyenne à 1,4 millions de francs[10] pour une PME et dépassent largement cette somme pour les grandes entreprises.

[10] Sophos, «The State of Ransomware 2021», disponible (en anglais) à l'adresse suivante: news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/

5. Comparaison avec le droit européen

L'Union européenne (UE) s'emploie à renforcer la cybersécurité sur tout son territoire et à rehausser la résilience de ses infrastructures critiques. Sur cette question, on peut prendre en compte notamment la directive de l'UE dite SRI[11] et la directive SRI 2[12] lui ayant succédé. L'UE y prévoit notamment que ses États membres doivent définir des mesures de protection pour les entreprises énergétiques majeures[13]. L'UE a rehaussé ses exigences générales en matière de sécurité et s'attache à les renforcer plus encore. En outre, elle élabore actuellement des codes de réseau sur la cybersécurité (*network codes on cybersecurity*), qui comporteront des prescriptions sur divers aspects de cette thématique dans le domaine de l'électricité.

La présente réglementation améliore la cybersécurité dans le secteur de l'électricité et prévoit l'élaboration de mesures de protection à cette fin. Elle s'inscrit dans le droit fil des efforts de l'UE pour améliorer plus encore la cybersécurité dans le secteur de l'électricité.

6. Commentaire des dispositions

Art. 1, al. 2

L'art. 1, al. 2, OApEl dispose que le réseau de transport d'électricité des chemins de fer suisses (réseau de courant de traction) exploité à la fréquence de 16,7 Hz et à la tension de 132 kV est soumis à la LApEl dans la mesure où celle-ci vise à créer les conditions d'un approvisionnement sûr en électricité. La réglementation de l'art. 8*a* LApEl[14] sert à assurer la sécurité de l'approvisionnement en électricité, c'est pourquoi elle pourrait également s'appliquer au domaine du réseau de courant de traction. Les applications télématiques du réseau de courant de traction font quant à elles déjà l'objet de dispositions de droit spécial sur la cybersécurité, supervisées par l'Office fédéral des transports (OFT)[15]. Pour éviter une double attribution des compétences entre l'OFT et la Commission fédérale de l'électricité (ElCom), les prescriptions de l'art. 8*a* LApEl et les dispositions d'exécution de l'art. 5*a* OApEl correspondantes ne s'appliquent donc pas au secteur du réseau de courant de traction.

Art. 5a

Al. 1: la disposition comporte un renvoi statique direct à la norme minimale TIC. Elle établit que la version 2023 de cette norme devient contraignante et que les recommandations qu'elle contient doivent être mises en œuvre par les acteurs visés en tenant compte des niveaux de protection définis à l'annexe 1*a* (voir ci-dessous). Sont soumis à cette obligation uniquement les producteurs et les exploitants de stockage (let. b), ainsi que leurs prestataires (let. c, ch. 2), dont l'accès à la puissance définie peut se faire via un seul système. L'influence qu'exerce l'acteur sur le système de pilotage (système de contrôle industriel / système de gestion opérationnelle) est déterminante pour calculer la somme de la puissance dans le contexte d'une cyberattaque. Si plusieurs systèmes de pilotage sont reliés de telle manière que si l'un d'entre eux était compromis, les autres le seraient également, alors ils sont considérés comme un seul et même système dans le cadre de cette disposition. L'obligation ne s'applique pas, par exemple, au producteur qui exploiterait plusieurs installations ayant chacune une puissance inférieure à 100 MW via plusieurs systèmes de pilotage, c'est-à-dire des systèmes non reliés

[11] 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

[12] 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) nº 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

[13] Cf. notamment art. 21, al. 1, et annexe I directive SRI 2

[14] Pas encore en vigueur; cf. message du 2 décembre 2022 relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), 22.073, FF 2023 84

[15] DE-OCF relative à l'art. 42, DE 42.2; dispositions d'exécution de l'ordonnance sur les chemins de fer (DE-OCF; RS 742.141.11); en cours de révision

entre eux. Sur la base de l'art. 8*a*, al. 2, LApEl, les exploitants de centrales nucléaires (titulaires de l'autorisation d'exploiter une centrale nucléaire) sont exclus du champ d'application de la nouvelle disposition car ils sont déjà soumis à des prescriptions en la matière supervisées par l'Inspection fédérale de la sécurité nucléaire (IFSN)[16]. L'accès à distance d'un prestataire (let. c) est considéré comme durable s'il lui a été accordé dans le cadre d'un contrat sans que l'entreprise mandante ne doive lui accorder chacun des droits d'accès *ad hoc* correspondants.

Al. 2: la disposition clarifie le fait que les règles (références) citées dans la norme minimale TIC ne sont pas contraignantes.

Al. 3: en raison de sa compétence générale subsidiaire (art. 22, al. 1, LApEl), l'ElCom veille au respect des art. 8*a* LApEl et 5*a* OApEl.

Annexe 1a: les niveaux (ou profils) de protection définissent les exigences concernant le degré de mise en œuvre des mesures définies dans la norme minimale TIC. Les exigences du niveau de protection A sont les plus strictes et s'adressent aux entreprises pour l'approvisionnement en électricité les plus importantes. Les niveaux B et C comportent des exigences moindres, respectivement pour les acteurs de taille moyenne ou de petite taille. Conformément à la procédure de vérification énoncée au chap. 3 de la norme minimale TIC, les exigences sont définies à l'aide de «valeurs» (niveau Tier). Ces valeurs sont réparties entre «partiellement mis en œuvre» (valeur 1) et «mis en œuvre dynamiquement» (valeur 4). La totalité de l'électricité transportée via le réseau d'un gestionnaire de réseau (distribution aux consommateurs finaux ou transfert à d'autres réseaux) est considérée comme son volume d'électricité transportée (ch. 1.1 et 1.2). En ce qui concerne les prestataires, la somme de l'électricité transportée (gestionnaires de réseau) ou de la puissance installée (producteurs et exploitants de stockage) de tous leurs mandants est prise en compte pour déterminer le niveau de protection déterminant. Si, par exemple, un prestataire a accès via un seul système (cf. explications ci-dessus concernant l'art. 5*a*, al. 1) aux systèmes de pilotage de dix gestionnaires de réseau pour un volume d'électricité transportée de 13 GWh/an pour chacun d'eux, la somme de l'électricité transportée est égale à 130 GWh/an. Le prestataire doit donc respecter les valeurs du niveau de protection B, tandis que pour chacun des gestionnaires de réseau concerné, c'est le niveau de protection C qui s'appliquerait. Pour les petits acteurs du marché, le niveau de protection C ne fixe des prescriptions contraignantes que pour environ 40 des 108 mesures que comporte la norme minimale TIC au total. En raison du principe de proportionnalité, seules les mesures prioritaires dans la hiérarchie doivent être mises en œuvre. Si un acteur remplit les critères pour plusieurs niveaux de protection, c'est le niveau le plus élevé qui s'applique. L'OFAE propose sur sa page Web un formulaire dédié à la vérification des valeurs fixées dans l'annexe 1*a*[17].

[16] Art. 5 et 6 de l'ordonnance du DETEC sur les hypothèses de risque et sur les mesures de sûreté pour les installations et les matières nucléaires (RS 732.112.1)

[17] IKT-Minimalstandard Assessment Tool, disponible sous www.bwl.admin.ch > Thèmes > TIC > Norme minimale pour les TIC