Directive 1/2024

Surveillance de la cybersécurité assurée par l'ElCom

8 février 2024

1 Contexte

En vertu du nouvel article 8*a* de la loi fédérale du 23 mars 2007 sur l'approvisionnement en électricité (LApEl ; RS 734.7) et de l'article 5*a* du projet de révision de l'ordonnance du 14 mars 2008 sur l'approvisionnement en électricité (OApEl ; RS 734.71), qui entreront en vigueur en juillet 2024, les gestionnaires de réseau, les producteurs, les agents de stockage et les prestataires (ci-après : « entreprises ») prennent des mesures pour protéger adéquatement leurs installations contre les cybermenaces. Pour assurer une exploitation sûre et stable du réseau électrique suisse, les technologies de l'information[1] (IT), et plus particulièrement les technologies opérationnelles[2] (OT), doivent être protégées contre les cybermenaces.

En vertu de l'article 22, alinéa 1 LApEl, l'ElCom surveille le respect des dispositions de la LApEl, et donc également l'état de mise en œuvre des mesures de protection contre les cybermenaces. L'ElCom se concentre en premier lieu sur l'exploitation sûre et stable du réseau électrique suisse. Les bases de la surveillance exercée par l'ElCom sont définies par le cadre de cybersécurité NIST (*Cybersecurity Framework NIST*). Celui-ci est aussi employé dans la norme minimale pour les TIC de l'Office fédéral pour l'approvisionnement économique du pays (OFAE), dans les documents de la branche de l'Association des entreprises électriques suisses (AES), ainsi que dans les futures dispositions légales.

Pour permettre à l'ElCom d'exercer son activité de surveillance, les entreprises sont tenues, en vertu de l'article 25, alinéa 1 LApEl, de lui donner les informations nécessaires à l'exécution de la LApEl et de lui mettre à disposition les documents requis.

---

1 Par technologies de l'information, on entend les technologies de traitement des données qui ne sont pas directement liées à la fourniture d'électricité (p. ex. gestion des données clients, gestion des données du personnel, applications bureautiques).

2 Par technologies opérationnelles, on entend les technologies directement nécessaires à la mise à disposition ou à la fourniture d'électricité (p. ex. SCADA, PIA, accès à distance aux installations dans les sous-stations, télécommande centralisée, gestion des données énergétiques (EDM), compteurs intelligents, systèmes de commande et de réglage intelligents).

Commission fédérale de l'électricité ElCom
Christoffelgasse 5, 3003 Berne
Tél. +41 58 462 58 33, Fax +41 58 462 02 22
info@elcom.admin.ch
www.elcom.admin.ch

En prévision de l'entrée en vigueur, en juillet 2024, de la LApEl et de l'OApEl révisées, comprenant de nouvelles dispositions concernant la protection contre les cybermenaces, l'ElCom a révisé son concept de surveillance. La présente directive précise les éléments clés de la mise en œuvre de cette surveillance sur le plan régulatoire. L'ElCom se réserve le droit d'adapter la présente directive si les bases valables au moment de son élaboration devaient changer de manière significative.

Avec l'entrée en vigueur de l'OApEl révisée prévue pour juillet 2024, les gestionnaires de réseau, les producteurs, les agents de stockage et les prestataires seront soumis à des exigences minimales en matière de cybersécurité. Dans l'OApEl révisée, les exigences minimales sont définies selon les cinq fonctions NIST « *Identify*, *Protect*, *Detect*, *Respond* et *Recover* ». Elles sont considérées comme un moyen de renforcer la résilience de l'approvisionnement en électricité de la Suisse face aux cybermenaces.

Les exigences minimales varient en fonction de la taille et du type d'entreprise mais, selon l'exposition aux risques d'une entreprise, elles ne suffisent toutefois pas à garantir une exploitation à la fois sûre et stable. Dans tous les cas, les entreprises restent toujours responsables de la protection adéquate de leurs installations et de leurs systèmes contre les cybermenaces. Les exigences minimales de l'OApEl révisée sont contraignantes dès leur entrée en vigueur, sans délai transitoire. En vertu de sa compétence en matière de surveillance, il incombe à l'ElCom de définir le délai et le processus de contrôle de la réalisation des exigences minimales.

Pour les gestionnaires de réseau, les coûts de la mise en œuvre des mesures de cybersécurité sont des coûts de réseau imputables, pour autant qu'ils remplissent les exigences en matière d'imputation des coûts au sens de l'article 15, alinéa 1 LApEl. Dans sa communication du 28 septembre 2022, l'ElCom a précisé le principe d'imputation des mesures de cybersécurité.

2 Surveillance

En matière de surveillance, l'ElCom adopte une approche basée sur les risques en ce qui concerne l'exploitation sûre du réseau électrique suisse. La surveillance a pour but de renforcer la résilience face aux cybermenaces. Ainsi, les entreprises sont surveillées à différents niveaux, en fonction de leur pertinence et de leur situation de risque pour l'exploitation sûre et stable du réseau électrique suisse. Les instruments de surveillance doivent permettre à l'ElCom d'évaluer si les mesures prises correspondent aux considérations de l'entreprise en matière de risques et si les prescriptions légales sont respectées. Cela signifie également que l'ElCom peut, sur la base de son activité de régulation, émettre des recommandations et / ou ordonner des mesures. Pour faire appliquer les mesures, l'ElCom dispose des moyens de droit habituels. Actuellement, l'ElCom prévoit d'utiliser et de combiner trois instruments de surveillance de manière complémentaire.

2.1 Enquêtes

Après l'entrée en vigueur de l'OApEl révisée, les entreprises seront tenues de remplir certaines exigences minimales. Dans un premier temps, l'ElCom recensera celles-ci par le biais d'une auto-évaluation dans le cadre d'une enquête basée sur l'outil d'évaluation de l'OFAE. Les auto-évaluations remises doivent être confirmées par une lettre de la direction concernée. Cette enquête sera menée chaque année auprès de toutes les entreprises concernées selon l'OApEl révisée. Elle permet à l'ElCom d'établir une vue d'ensemble de la réalisation des exigences légales, d'une part, et de recueillir et d'évaluer des informations sur l'état des mesures de cybersécurité, d'autre part.

2.2 Entretiens de sensibilisation

Les entretiens de sensibilisation sont menés en premier lieu avec des entreprises déterminantes pour l'exploitation sûre et stable du réseau électrique suisse. En complément, des entretiens de sensibilisation sont également possibles sur la base de certaines réponses obtenues dans le cadre de l'enquête ou d'un échantillon aléatoire. L'objectif de ces entretiens est de recueillir des informations concrètes sur la mise en œuvre des mesures de cybersécurité et de compléter ainsi qualitativement les résultats de l'enquête. Les entretiens de sensibilisation ont lieu régulièrement dans les entreprises concernées.

Les conclusions tirées des entretiens constituent une base pour évaluer la cybersécurité au sein de l'entreprise ainsi que pour décider d'éventuelles recommandations de mesures, dont la mise en œuvre peut être examinée lors d'entretiens de sensibilisation ultérieurs.

2.3 Audits

Comme troisième instrument de surveillance, l'ElCom peut procéder à des audits individuels, qui doivent permettre d'approfondir certains aspects techniques en fonction des anomalies relevées lors de l'enquête ou des entretiens de sensibilisation. De même, des audits peuvent être réalisés sur la base d'indications externes ou d'un échantillon aléatoire. Selon l'objectif et le but, ces audits peuvent être réalisés par l'ElCom ou par un organisme d'audit externe.

3 Passage aux exigences minimales de l'OApEl

L'OApEl révisée ne prévoit pas de délai transitoire pour atteindre les valeurs cibles minimales requises. Afin que les auto-évaluations issues de l'enquête menée auprès des entreprises reflètent le mieux possible la situation actuelle, l'ElCom autorise un délai transitoire pour prouver que les valeurs cibles exigées ont été atteintes au plus tard 24 mois après l'entrée en vigueur de l'OApEl révisée.

En ce qui concerne les catégories pour lesquelles les valeurs cibles n'ont pas été atteintes, un plan de mesures et de mise en œuvre validé par la direction doit être soumis avec des objectifs de mise en œuvre concrets et contraignants. Si l'ElCom estime que les mesures qui y sont proposées ne sont pas mises en œuvre dans les meilleurs délais, elle cherche le dialogue avec les entreprises concernées. Si, pour des raisons justifiées, les valeurs cibles n'ont pas pu être atteintes durant ce délai transitoire, l'ElCom peut exceptionnellement accorder un délai supplémentaire.

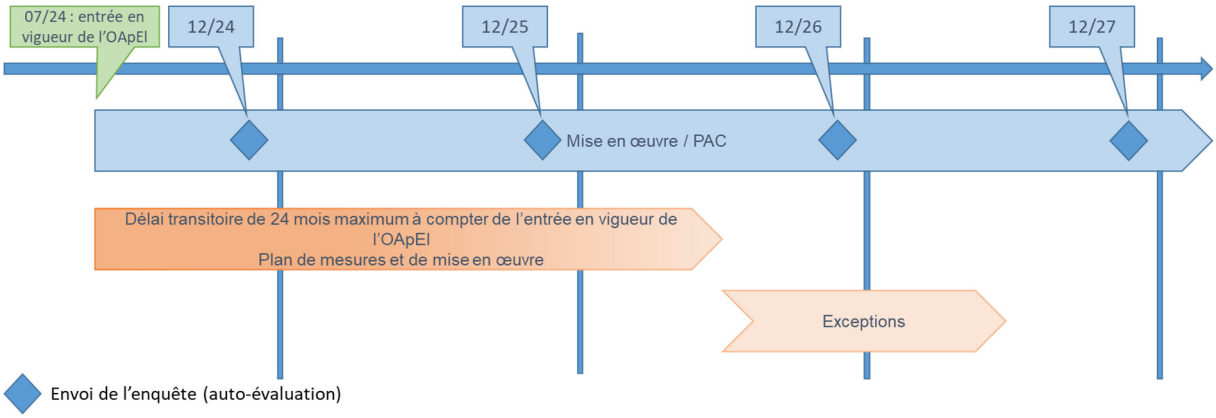

Figure : Schéma présentant les étapes de la mise en œuvre des exigences minimales de cybersécurité