Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Département fédéral des finances
Centre national pour la cybersécurité (CNCS)
3003 Berne

Par voie électronique à: ncsc@gs-efd.admin.ch

28 mars 2022

Markus Riner, ligne directe +41 62 825 25 27, markus.riner@strom.ch

Prise de position concernant l'obligation pour les exploitants d'infrastructures critiques de signaler les cyberattaques

Mesdames, Messieurs,

L'Association des entreprises électriques suisses (AES) vous remercie de lui donner la possibilité de prendre position sur l'introduction d'une obligation pour les exploitants d'infrastructures critiques de signaler les cyberattaques.

En tant qu'association faîtière, l'AES représente les intérêts du secteur suisse de l'électricité tout au long de la chaîne de création de valeur: production, négoce, transport et distribution finale de l'électricité. Un approvisionnement sûr en électricité est vital pour le bon fonctionnement de la société et de l'économie. Les infrastructures de la branche de l'électricité font donc indéniablement partie des infrastructures d'approvisionnement critiques les plus importantes. Afin de protéger ces dernières le plus efficacement possible contre les cybermenaces croissantes, l'AES s'engage fortement à travers la rédaction de documents de la branche, et soutient les entreprises de la branche en matière de cybersécurité. L'AES s'est également investie activement et de façon constructive dans les travaux de fond qui ont précédé la présente révision de la Loi sur la sécurité de l'information (LSI).

Concernant les modifications de la LSI, l'AES soutient le renforcement proposé du positionnement du CNCS, lequel serait le point de contact centralisé de la Confédération pour l'économie, y compris pour le secteur énergétique, concernant les questions liées au cyberespace, de même que le service d'aide pour maîtriser les cyberattaques. Cela correspond aux attentes de la branche, en particulier en vue d'une amélioration conjointe de la cybersécurité dans le cadre de l'obligation de signaler les cyberattaques.

De manière générale, l'AES attend du CNCS, en cas de cyberattaque, qu'il propose des prestations CERT rapidement disponibles afin d'apporter un soutien dans l'analyse et la compréhension précise de la situation, ainsi que dans l'initiation des étapes nécessaires pour se défendre rapidement et pour maîtriser l'incident.

L'AES salue la volonté de ne pas faire entrer les prestations du CNCS en concurrence avec les offres de l'économie privée. Les prestations de soutien du CNCS auxquelles on peut s'attendre selon les art. 73a et 74, al. 3 LSI, ainsi que l'interaction entre le CNCS en tant que CERT pour les infrastructures critiques et les fournisseurs privés de prestations CERT doivent toutefois être définies plus précisément dans le cadre de

l'ordonnance et adaptées aux exigences liées à la protection des infrastructures critiques. L'AES demande que le CNCS, en tant que «GovCERT», joue le rôle de coordinateur des CERT de l'économie privée et qu'il soutienne ceux-ci pour maîtriser les crises, en fonction de la situation et des besoins.

Concernant l'accès à des prestations de soutien fournies par le CNCS, l'art. 74, al. 3 LSI fait la distinction entre les exploitants privés et non privés. Le rapport explicatif n'apporte néanmoins pas suffisamment de clarté quant aux motifs et aux conséquences concrètes de cette distinction. Certains exploitants d'infrastructures critiques dans la branche de l'électricité font partie de l'administration publique, d'autres font partie du secteur privé; ils présentent cependant une même exposition au risque. L'organe responsable ou les rapports de propriété ne sont donc pas des critères de distinction pertinents et vont à l'encontre du principe selon lequel le CNCS soutient tous les exploitants d'infrastructures critiques, conformément à l'art. 73a, let. f LSI.

Proposition:

Art. 74 Soutien aux exploitants d'infrastructures critiques

3 Il les conseille et les aide dans la gestion des cyberincidents et la correction des vulnérabilités lorsqu'il existe un risque imminent de conséquences graves pour l'infrastructure critique ~~et que, pour autant qu'il s'agisse d'exploitants privés, il n'est pas possible d'obtenir un soutien équivalent sur le marché en temps utile~~.

Dans son Rapport explicatif, le Conseil fédéral souligne qu'il faut préciser dans l'ordonnance les critères sur la base desquels les cyberattaques selon art. 74d LSI doivent être signalées. L'AES considère elle aussi qu'une telle précision est nécessaire. En particulier, savoir si, selon let. b, une cyberattaque a été exécutée par un État étranger ou à l'instigation de cet État, pourrait s'avérer difficile, voire impossible à déterminer pour les personnes concernées. La let. d, elle, ne clarifie pas si la survenance de composantes d'attaque antérieures, éventuellement stoppées ou qui n'ont pas abouti est déjà soumise à l'obligation de signalement, ou si ce n'est le cas que pour celles qui ont été introduites avec l'objectif direct et immédiat de perpétrer la cyberattaque.

Selon l'art. 73b, al. 2 LSI, des informations sur les cyberincidents peuvent être publiées ou communiquées aux autorités et aux organisations intéressées si cela permet de prévenir ou de combattre les cyberattaques. L'AES reconnaît que de telles informations peuvent être utiles, mais souligne que les données personnelles et les données de personnes morales ne doivent être publiées qu'avec le consentement explicite et préalable des personnes concernées. De plus, l'ordonnance devrait définir plus précisément à quel moment des informations sont publiées, et ce dans le but d'exclure que des personnes concernées qui sont vulnérables soient exposées, suite à des déductions, à d'autres attaques ou actes délictueux.

Enfin, l'AES fait remarquer que l'art. 24 de la LPD révisée prévoit une obligation d'annoncer au PFPDT les attaques impliquant des données personnelles (avec un risque élevé). De ce fait, un même incident pourrait faire l'objet d'annonces à au moins deux autorités différentes. Les entreprises concernées devraient cependant pouvoir annoncer un incident au PFPDT via le même canal, coordonné par le CNCS, si cela s'avérait nécessaire en fonction du type d'attaque. Une double annonce entraînerait au contraire une charge de travail supplémentaire et des questions de délimitation compliquées.

Concernant les modifications de la LApEl, l'AES salue que, d'après le rapport explicatif, le Conseil fédéral souhaite baser d'éventuelles prescriptions pour les infrastructures critiques de la branche de l'électricité au niveau de l'ordonnance sur les réglementations subsidiaires de la branche. L'AES considère comme pertinent que le Conseil fédéral déclare applicables les normes de la branche dans ce domaine, car cela permet une adaptation rapide à l'évolution dynamique des situations et des scénarios de menace possibles. Si des dispositions d'ordonnance sont édictées, le risque potentiel relatif à la sécurité d'approvisionnement doit être pris en compte dans la définition des prescriptions à respecter et dans la désignation des acteurs engagés. Il s'agit de s'assurer que les dispositions de l'ordonnance prévoient une application pragmatique de l'obligation de signaler, afin que les petites et moyennes entreprises puissent elles aussi gérer plus aisément ces situations.

Nous vous remercions de tenir compte de nos requêtes et nous apporterons volontiers notre soutien au CNCS afin de poursuivre la mise en place d'une interaction efficace entre les acteurs au cas réel d'une cyberattaque.

Nous nous tenons à disposition pour toute question ou discussion.

Meilleures salutations,

Michael Frank
Directeur

Michael Paulus
Responsable Réseaux et Formation professionnelle