Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Commission fédérale de l'électricitéEidgenössische Elektrizitätskommission ElCom
Secrétariat technique

Communication

Imputation des coûts de la cybersécurité

Berne, le 28.09.2022

Table des matières

Liste des figures

1 Introduction

Dans un contexte de numérisation croissante, les réseaux électriques sont de plus en plus pilotés et surveillés par des technologies intelligentes d'information et de communication. Cela augmente le risque de compromettre la disponibilité, l'intégrité ou la confidentialité des données. Dans les cas extrêmes, un cyberincident peut entraîner une panne de courant à grande échelle avec de graves conséquences. La cybersécurité devient donc une question centrale pour garantir la sécurité de l'approvisionnement en électricité.

Les gestionnaires de réseau doivent pourvoir à un réseau sûr, performant et efficace (art. 8, al. 1, let. a, LApEl). Selon l'ElCom, la protection contre les cyberrisques en fait également partie. Même en cas de cyberincident, les gestionnaires de réseau doivent être en mesure de garantir la fourniture en électricité aux clients en aval et aux consommateurs finaux, et la stabilité du système suisse ne doit en aucun cas être menacée par un cyberincident.

En tant que régulateur, l'ElCom attend donc des gestionnaires de réseau qu'ils appliquent les documents de la branche : « ICT Continuity », « Protection de base pour les technologies opérationnelles (OT) dans l'approvisionnement en électricité » et « Directives pour la sécurité des données des systèmes de mesure intelligents » de l'Association des entreprises électriques suisses. Cette mise en œuvre doit être efficace et basée sur les risques. Les coûts sont imputables au sens de l'art. 15 LApEl.

La présente communication vise à clarifier les éventuelles incertitudes concernant l'imputation des coûts et à contribuer ainsi à une mise en œuvre rapide des mesures de cybersécurité.

2 Imputation des coûts

Comme mentionné ci-dessus, seuls les coûts résultant d'une mise en œuvre efficace et basée sur les risques des mesures de cybersécurité peuvent être imputés. Pour ce faire, le guide PIC de l'Office fédéral de la protection de la population (OFPP) constitue une bonne référence. Conformément à l'art. 11 LApEl et à l'art. 7 OApEl, les gestionnaires de réseau présentent chaque année à l'ElCom une comptabilité analytique. Pour l'attribution des coûts imputables, le Guide d'utilisation du fichier de comptabilité analytique élaboré par l'ElCom ainsi que, subsidiairement, le Schéma de calcul des coûts pour les gestionnaires de réseau de distribution CH (SCCD) de l'Association des entreprises électriques suisses s'appliquent. La structure suivante doit aider à saisir ces coûts de manière appropriée. En règle générale, les coûts liés à la protection des technologies opérationnelles (OT)[1] devraient être indiqués sous les positions 200 et 500 et les coûts liés à la protection de l'informatique (IT)[2] sous la position 600 de la comptabilité analytique. En ce qui concerne la durée d'amortissement du matériel et des logiciels, le tableau 1 du SCCD s'applique. L'ElCom se réserve le droit de vérifier, dans le cadre de sa surveillance, la mise en œuvre efficace des mesures de protection et des coûts. La comptabilité financière devrait donc être conçue de manière à ce que les coûts des mesures de protection contre les cyberincidents puissent être présentés le plus facilement possible. Il faut tenir compte du fait que seuls les coûts concernant le réseau peuvent être imputés (art. 15 LApEl en relation avec l'art. 10 LApEl). Les coûts de protection des systèmes TIC d'autres secteurs (p. ex. énergie, télécoms, gaz, ...) doivent être séparés directement ou par une clé de répartition appropriée (art. 7, al. 5, OApEl) et imputés aux secteurs correspondants (cf. également chapitre 2, SCCD). La figure 1 ci-dessous illustre l'idée de la répartition des coûts, mise en évidence à l'aide d'exemples dans les chapitres suivants.

[1] Par technologies opérationnelles (Operational Technology, OT), on entend les technologies qui sont 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).

[2] Par technologies de l'information (IT), 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).

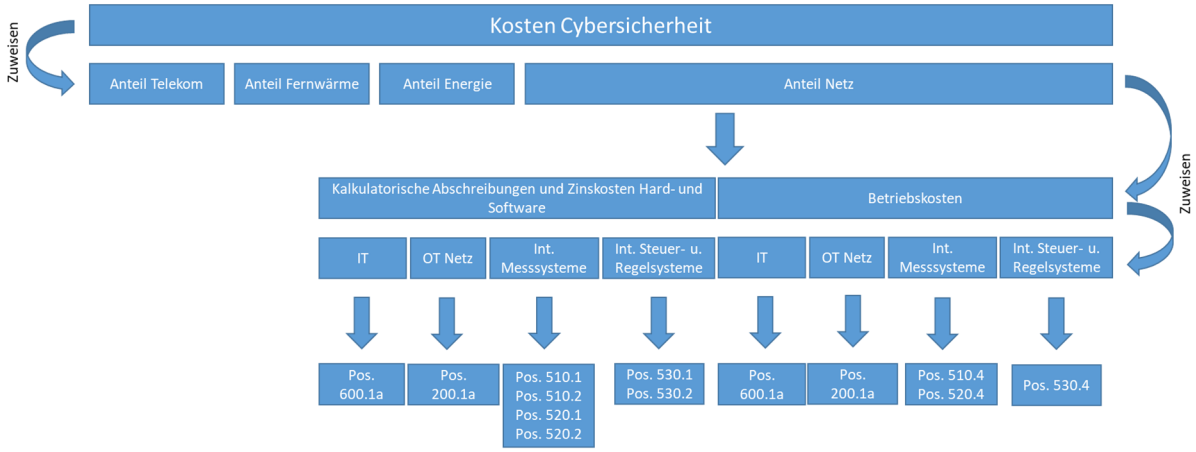

Illustration 1 Aperçu de la répartition des coûts de cybersécurité dans la comptabilité analytique de l'ElCom

En cas d'incertitudes lors de la mise en œuvre des mesures de cybersécurité en fonction des risques ou lors de l'imputation, le secrétariat technique de l'ElCom se fera un plaisir de vous renseigner (Philippe Mahler, philippe.mahler@elcom.admin.ch).

2.1 Coûts de capital calculés et coûts d'exploitation des réseaux (OT) (Compta. anal. 200.1a)

Les amortissements calculés et les intérêts des systèmes de sécurité (matériel et logiciel) pour les systèmes de commande et de régulation ainsi que les coûts d'exploitation pour les mesures de sécurité du réseau (OT) sont comptabilisés sous la position Compt. anal. 200.1a. Par exemple :

- Matériel et logiciel DMZ pour le centre de commande du réseau (SCADA)
- Part du matériel et des logiciels OT pour la protection des zones
- Maintenance des systèmes de sécurité dans le centre de commande du réseau ou les sous-stations
- Coûts en lien avec la protection de la gestion des données énergétiques (EDM)
- Consultants / mandats externes
- Coûts des tests d'intrusion
- Patches / Updates
- Audits
- Coûts proportionnels SOC
- Formation des collaborateurs OT
- Coûts proportionnels Intrusion Detection System (IDS) OT
- Coûts proportionnels Security Information and Event Management (SIEM) OT
- Coûts proportionnels Information Security Management System (ISMS) OT
- Security as a Service (SECaaS) OT
- Participation au programme BugBounty OT

2.2 Coûts de capital calculés des systèmes de mesure intelligents (Compt. anal. 510.1, 510.2, 520.1, 520.2)

Les coûts des amortissements calculés et des intérêts des systèmes de sécurité correspondants pour les systèmes de mesure intelligents, y compris les systèmes selon l'art. 17a LApEl et les art. 8a et 8b OApEl (510.1, 510.2) et les autres systèmes de mesure (520.1, 520.2) sont comptabilisés sous les positions Compt. anal. 510.1, 510.2, 520.1 et 520.2. En font également partie les coûts pour la protection des systèmes selon la figure 5 des « Directives pour la sécurité des données des systèmes de mesure intelligents » de l'Association des entreprises électriques suisses pour les systèmes de mesure intelligents selon l'art. 8b OApEl, comme par exemple des mesures de protection pour :

- Systèmes de mesure intelligents
- Concentrateur de données / Gateway
- Head End System (HES) y compris gestion des clés
- Meter Data Management (MDM)
- Protection Accès à distance des prestataires de services externes

2.3 Coûts d'exploitation des systèmes de mesure intelligents (Compt. anal. 510.4, 520.4)

Les coûts des mesures de sécurité pour les systèmes de mesure intelligents, y compris les systèmes selon l'art. 17a LApEl et les art. 8a et 8b OApEl (510.4) et les autres systèmes de mesure (520.4) sont comptabilisés comme autres coûts. Cela comprend également la mise en œuvre des « Directives pour la sécurité des données des systèmes de mesure intelligents » de l'Association des entreprises électriques suisses. Il s'agit par exemple de mesures de protection pour :

- Systèmes de mesure intelligents
- Concentrateur de données / Gateway
- Head End System (HES) y compris gestion des clés
- Meter Data Management (MDM)
- Protection Accès à distance des prestataires de services externes
- Coûts des tests d'intrusion
- Patches / Updates
- Backups

2.4 Coûts de capital calculés des systèmes de commande et de contrôle intelligents (Compt. anal. 530.1, 530.2)

Sont comptabilisés ici les amortissements calculés (530.1) et les intérêts (530.2) des systèmes de protection contre les cyberincidents des systèmes de commande et de réglage intelligents selon l'art. 8c OApEl ainsi que des installations de télécommande centralisée classiques. En voici quelques exemples :

- Mesures de protection Accès à distance aux systèmes de commande et de contrôle intelligents
- Firewall

2.5 Coûts d'exploitation des systèmes de commande et de régulation intelligents (Compt. anal. 530.4)

Sont abordés ici les systèmes de commande et de régulation intelligents selon l'article 8c OApEl ainsi que les installations de télécommande centralisée classiques. Cela inclut les systèmes de protection contre les cyberincidents. Les positions 530.1 et 530.2 comprennent les amortissements calculés et les intérêts de tels systèmes de sécurité. La position 530.4 comprend tous les coûts des mesures de sécurité. En voici quelques exemples :

- Coûts des tests d'intrusion
- Patches / Updates
- Backups

2.6 Coûts de capital calculés et coûts d'exploitation des réseaux (OT) (Compt. anal. 600.1a)

Les coûts de capital (amortissements et intérêts) et d'exploitation pour les systèmes et mesures de sécurité dans le domaine informatique sont enregistrés sous la position 600.1a en tant que frais administratifs. Il peut s'agir, par exemple, de :

- Coûts proportionnels Security Operation Center (SOC)
- Coûts (proportionnels) des locaux pour, par exemple, SOC
- Coûts des campagnes de sensibilisation
- Formation des collaborateurs IT
- Coûts proportionnels Intrusion Detection System (IDS)
- Coûts proportionnels Security Information and Event Management (SIEM)
- Coûts proportionnels Information Security Management System (ISMS)
- Security as a Service (SECaaS)
- Coûts de la segmentation du réseau
- Coûts proportionnels de protection des passages de zone IT - OT
- Audits
- Certification
- Création d'un inventaire IT
- Analyse des logs IT

3 Annexe

3.1 Glossaire

Abréviation	Signification
EDM	Gestion des données énergétiques (EDM)
HES	Head End System
IDS	Intrusion Detection System
ISMS	Information Security Management System
MDM	Meter Data Management
SCADA	Supervisory Control and Data Acquisition
SECaaS	Security as a Service
SIEM	Security Information and Event Management
SOC	Security Operations Center
LApEl	Loi sur l’approvisionnement en électricité, RS 734.7
OApEl	Ordonnance sur l’approvisionnement en électricité, RS 734.71