Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Elektrizitätskommission ElCom
Segreteria tecnica

Comunicazione

Computabilità dei costi della cibersicurezza

Berna, 28.09.2022

Indice

Indice delle figure

1 Introduzione

Con l'avanzare della digitalizzazione, le reti elettriche sono sempre più controllate e monitorate da tecnologie dell'informazione e della comunicazione intelligenti. In questo contesto aumenta il rischio che la disponibilità, l'integrità o la riservatezza dei dati siano compromesse. In casi estremi, un incidente informatico può portare a un blackout elettrico su larga scala, con gravi conseguenze. La cibersicurezza sta quindi diventando un elemento centrale per la garanzia di un approvvigionamento elettrico sicuro.

I gestori di rete hanno la responsabilità di garantire una rete sicura, performante ed efficiente (art. 8 cpv. 1 lett. a LAEl). Secondo la ElCom, ciò include anche la protezione dai ciber-rischi. Anche in caso di incidente informatico, i gestori di rete devono essere in grado di garantire la fornitura di energia elettrica ai gestori a valle e ai consumatori finali e la stabilità del sistema svizzero non deve essere compromessa.

In qualità di regolatore, la ElCom si aspetta pertanto che i gestori di rete implementino i documenti di settore «ICT Continuity», «Handbuch Grundschutz für Operational Technology in der Stromversorgung» (standard minimo per garantire la sicurezza delle TIC nell'approvvigionamento elettrico) e le «Richtlinien für die Datensicherheit von intelligenten Messsystemen» (direttive per la sicurezza dei dati dei sistemi di misurazione intelligenti) dell'Associazione delle aziende elettriche svizzere. L'attuazione di queste misure deve essere efficiente e basata sul rischio. I relativi costi sono computabili ai sensi dell'articolo 15 LAEl.

Scopo della presente comunicazione è chiarire eventuali dubbi circa la loro computabilità e contribuire così alla rapida attuazione di misure di cibersicurezza.

2 Computabilità dei costi

Come già menzionato, i costi sono computabili solo se le misure di cibersicurezza sono attuate in modo efficiente e in base ai rischi. La Guida alla protezione delle infrastrutture critiche PIC dell'Ufficio federale della protezione civile (UFPP) costituisce una buona base di partenza. Conformemente agli articoli 11 LAEl e 7 OAEl, i gestori di rete presentano ogni anno un calcolo dei costi alla ElCom. I costi computabili vengono attribuiti in base alla Guida alla contabilità analitica della ElCom nonché, sussidiariamente, al « Kostenrechnungsschema für Verteilnetzbetreiber der Schweiz (KRSV)» (schema del calcolo dei costi per i gestori della rete di distribuzione svizzera) dell'Associazione delle aziende elettriche svizzere (AES). La seguente ripartizione serve da ausilio per l'esatta indicazione di questi costi. In generale, i costi per la protezione delle OT[1] devono essere riportati nelle posizioni 200 e 500 e i costi per la protezione delle IT[2] nella posizione 600 della contabilità analitica. La tabella 1 dello schema si applica al periodo di ammortamento di hardware e software. Nell'ambito della sua attività di vigilanza, la ElCom si riserva il diritto di verificare l'efficacia dell'attuazione delle misure di protezione e dei costi. La contabilità finanziaria dovrebbe quindi essere concepita in modo da facilitare il più possibile l'indicazione dei costi delle misure di protezione contro gli incidenti informatici. Va tenuto presente che sono computabili solo i costi del settore rete (art. 15 in combinato disposto con l'art. 10 LAEl). I costi per la protezione dei sistemi TIC di altri settori (ad es. energia, telecomunicazioni, gas, ecc.) devono essere separati direttamente o in base a una chiave di ripartizione appropriata (art. 7 cpv. 5 OAEl) e addebitati ai settori corrispondenti (cfr. anche capitolo 2 dello schema summenzionato). La seguente figura 1 illustra come vengono attribuiti i costi. Il principio viene illustrato nei seguenti capitoli sulla base di esempi.

[1] Il concetto di «operational technology» (OT) comprende le tecnologie necessarie per la messa a disposizione o la fornitura dirette di energia elettrica (p. es. SCADA, PIA, accesso remoto a impianti situati in sottostazioni, sistemi di telecomando centralizzati, gestione dei dati energetici MDE, smart meter).

[2] Il concetto di «information technology» (IT) comprende tutte le tecnologie per l'elaborazione dei dati che non hanno a che fare direttamente con la messa a disposizione di energia elettrica (p. es. gestione dei dati dei clienti, gestione dei dati del personale, applicazioni per ufficio).

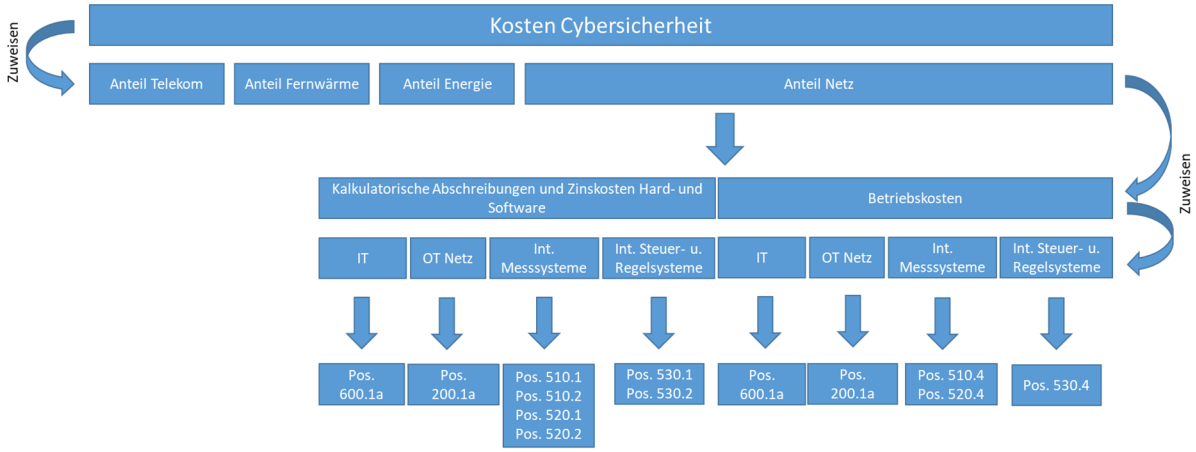

Figura 1 Panoramica dell'attribuzione dei costi della cibersicurezza nella contabilità analitica della ElCom

In caso di incertezze sull'attuazione in base ai rischi delle misure di cibersicurezza o sulla computabilità, la Segreteria tecnica è a disposizione per chiarimenti (Philippe Mahler, philippe.mahler@elcom.admin.ch).

2.1 Costi del capitale calcolatori e costi per l'esercizio delle reti (OT) (contabilità analitica 200.1a)

Gli ammortamenti e gli interessi calcolatori dei sistemi di sicurezza (hardware e software) per i sistemi di controllo e regolazione nonché i costi di esercizio per le misure di sicurezza della rete (OT) sono indicati nella posizione 200.1a della contabilità analitica. Esempio:

- hardware e software per DMZ per centro di controllo della rete (SCADA)
- quota hardware e software OT per la protezione delle interfacce tra le zone
- manutenzione dei sistemi di sicurezza nel centro di controllo della rete o nelle sottostazioni
- costi per la protezione della gestione dei dati energetici (MDE)
- consulenti / mandati esterni
- costi dei pen test
- patch / aggiornamenti
- audit
- quota costi Security Operation Center (SOC)
- formazione dei collaboratori OT
- quota costi Intrusion Detection System (IDS) OT
- quota costi Security Information and Event Management (SIEM) OT
- quota costi Information Security Management System (ISMS) OT
- Security as a Service (SECaaS) OT
- partecipazione al programma BugBounty OT

2.2 Costi del capitale calcolatori dei sistemi di misurazione intelligenti (contabilità analitica 510.1, 510.2, 520.1, 520.2)

I costi per gli ammortamenti e gli interessi calcolatori relativi alla sicurezza dei sistemi di misurazione intelligenti, compresi i sistemi di cui agli articoli 17a LAEl nonché 8a e 8b OAEl (510.1, 510.2) e altri sistemi di misurazione (520.1, 520.2) sono indicati nelle posizioni 510.1, 510.2, 520.1 e 520.2 della contabilità analitica. Essi comprendono anche i costi per la protezione dei sistemi secondo la figura 5 delle direttive per la sicurezza dei dati dei sistemi di misurazione intelligenti dell'Associazione delle aziende elettriche svizzere per i sistemi di misurazione intelligenti secondo l'articolo 8b OAEl, come ad esempio le misure di protezione per:

- sistemi di misurazione intelligenti
- concentratore di dati / gateway
- sistema Head End (HES), compresa la gestione delle chiavi
- Meter Data Management (MDM)
- protezione accesso remoto fornitori di servizi esterni

2.3 Costi di esercizio dei sistemi di misurazione intelligenti (contabilità analitica 510.4, 520.4)

I costi per le misure di sicurezza dei sistemi di misurazione intelligenti, compresi i sistemi secondo gli articoli 17a LAEl nonché 8a e 8b OAEl (510.4) e altri sistemi di misurazione (520.4) sono indicati come altri costi. Essi includono anche l'attuazione delle direttive per la sicurezza dei dati dei sistemi di misurazione intelligenti dell'Associazione delle aziende elettriche svizzere. Sono comprese anche le misure di sicurezza ad esempio per:

- sistemi di misurazione intelligenti
- concentratore di dati / gateway
- sistema Head End (HES), compresa la gestione delle chiavi
- Meter Data Management (MDM)
- protezione accesso remoto fornitori di servizi esterni
- costi dei pen test
- patch / aggiornamenti
- backup

2.4 Costi del capitale calcolatori dei sistemi di controllo e regolazione intelligenti (contabilità analitica 530.1, 530.2)

In queste posizioni sono indicati gli ammortamenti (530.1) e gli interessi (530.2) calcolatori dei sistemi di protezione contro incidenti informatici riguardanti i sistemi di controllo e regolazione intelligenti secondo l'articolo 8c OAEl, nonché i classici sistemi di telecomando centralizzati. Le misure comprendono ad esempio:

- misure di protezione per l'accesso remoto ai sistemi di controllo e regolazione intelligenti
- firewall

2.5 Costi di esercizio di sistemi di controllo e regolazione intelligenti (contabilità analitica 530.4)

Si tratta di sistemi di controllo e regolazione intelligenti secondo l'articolo 8c OAEl e dei classici sistemi di telecomando centralizzati. Sono compresi anche i sistemi di protezione contro gli incidenti informatici. Gli ammortamenti e gli interessi calcolatori per tali sistemi di sicurezza sono indicati nelle posizioni 530.1 e 530.2. Nella posizione 530.4 sono indicati tutti i costi delle misure di sicurezza, come ad esempio:

- costi dei pen test
- patch / aggiornamenti
- backup

2.6 Costi del capitale calcolatori e costi per l'esercizio delle reti (IT) (contabilità analitica 600.1a)

I costi del capitale (ammortamenti e interessi) e i costi di esercizio per i sistemi e le misure di sicurezza delle IT sono indicati come costi amministrativi nella posizione 600.1a. Essi comprendono ad esempio:

- quota di costi SOC
- (quota) costi locali (ad es. per il SOC)
- costi per le campagne di sensibilizzazione
- formazione dei collaboratori IT
- quota costi Intrusion Detection System (IDS)
- quota costi Security Information and Event Management (SIEM)
- quota costi Information Security Management System (ISMS)
- Security as a Service (SECaaS)
- costi segmentazione della rete
- quota costi per la protezione delle interfacce tra le zone IT - OT
- audit
- certificazione
- creazione inventario IT
- analisi log IT

3 Allegato

3.1 Glossario

Abbreviazione	Significato
MDE	Gestione dei dati energetici
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 Operation Center
LAEl	Legge sull'approvvigionamento elettrico, RS 734.7
OAEl	Ordinanza sull'approvvigionamento elettrico, RS 734.71