Istruzioni sulla sicurezza

SA-02159-C1-Piano di protezione degli edifici del Gruppo

Swisscom SA

Group Security
Casella postale
3050 Berna

Versione	Data	Persona	Modifiche apportate/osservazioni
0.1	05.04.2022	Claudio Passafaro	-
0.2	14.10.2022	Claudio Passafaro	Rettifica di lieve entità
0.9	09.12.2022	Daniel Zysset	Tradotto e finalizzato
1.0	09.12.2022	Thomas Dummermuth	Collaudo/rilascio

Responsabile: SiBe Brand-Objektschutz
Edito da: SiBe Brand-Objektschutz

Redazione: 05.04.2022

Creato da: Passafaro Claudio
Destinatari: come da 1.2 Campo di applicazione

Indice

1 Introduzione

1.1 Obiettivo e scopo del documento

[1] La sicurezza è un concetto fondamentale per Swisscom.

[2] Nel presente documento viene descritta l'applicazione della Security Policy emanata dal responsabile Group Security nel campo della protezione degli edifici. A tal fine vengono fissati il livello d'ambizione, gli obiettivi di protezione e i requisiti minimi.

[3] Esso costituisce la base per garantire un livello di sicurezza adeguato nell'intero Gruppo Swisscom nonché per analizzare e applicare misure adeguate.

1.2 Campo di applicazione

[4] Il presente documento è valido per l'intera Swisscom SA, incluse tutte le società del Gruppo, le divisioni operative e del Gruppo aventi sede in Svizzera e all'estero. Con «Swisscom» si intendono le unità seguenti: divisioni operative e del Gruppo Swisscom SA e Swisscom (Svizzera) SA.

[5] I locali esistenti devono essere verificati per accertarne la conformità. Qualora vengano riscontrate carenze, occorre apportare miglioramenti fissando delle priorità in funzione del rischio.

[6] I nuovi piani di protezione per singoli edifici (soluzioni complete) devono essere presentati a Group Security, che li sottopone a una verifica caso per caso.

2 Piano

[7] Poiché ogni edificio presenta le proprie peculiarità, non è stato predisposto un unico piano di protezione per tutti gli edifici. La procedura di massima è la seguente:

- Individuare le minacce e gli edifici degni di protezione
- Individuare i rischi
- Sulla base di queste informazioni, fissare obiettivi di protezione specifici
- Determinare la politica risp. il sistema di sicurezza (strategia di prevenzione/sorveglianza e d'intervento)

[8] Gli obiettivi di questo approccio sono:

- Valutazione dei rischi obiettiva e specifica per l'azienda
- Definizione di misure orientate agli obiettivi di protezione sulla base di criteri misurabili
- Base per misure di sicurezza equilibrate e ottimizzate sotto il profilo economico
- Piano di sicurezza modulare e orientato al gruppo target
- Basi di auditing per il controllo periodico delle misure di sicurezza adottate

2.1 Misure

[9] Tutti gli edifici e/o i locali vanno classificati in base alla protezione richiesta e tutelati per mezzo di un adeguato piano di protezione degli edifici o di adeguate misure di protezione degli edifici.

[10] Un piano di protezione scritto include almeno:

- Valutazione e analisi dei rischi
- Requisiti operativi (tolleranza al rischio e obiettivi di protezione)
- Sistema di sicurezza (misure di sicurezza)

2.2 Obiettivi di protezione

[11] I seguenti obiettivi di sicurezza generali del Security Management hanno un'importanza centrale per Swisscom (sulla base della Swisscom Security Policy):

- Protezione delle persone
- Protezione delle informazioni
- Protezione dei beni materiali
- Protezione della performance aziendale

[12] Per la protezione degli edifici, tali obiettivi di protezione vengono ulteriormente suddivisi e priorizzati nel modo seguente:

- Vita e salute dei collaboratori e delle persone che si trovano nei nostri locali
- Asset dell'azienda
- Know-how dell'azienda
- Processi commerciali, comunicazione, IT e infrastruttura
- Ambiente
- Reputazione
- Sedimi confinanti

2.3 Applicazione degli obiettivi di protezione

[13] Sulla base dei risultati dell'analisi dei rischi, le misure di protezione degli edifici vengono valutate caso per caso. Il loro obiettivo è prevenire gli eventi rilevanti per la sicurezza (atti dolosi, delitti e altre situazioni indesiderate). Inoltre, gli eventi e i danni che ne derivano devono risultarne limitabili e gestibili.

[14] I rischi possono essere prevenuti, ridotti, trasferiti o accettati.

[15] Sulla base di un'analisi dei rischi è possibile individuare e valutare le necessarie misure di prevenzione, sorveglianza e intervento. Vanno adottate misure per ridurre i rischi a un livello accettabile. Le possibilità sono:

[16] Dissuasione – I potenziali infrattori vengono dissuasi dal proseguire la loro azione dalla presenza di inattese misure o reazioni finalizzate alla prevenzione del danno.

[17] Impossibilitazione – La prosecuzione dell'azione dei potenziali infrattori viene resa impossibile per mezzo di elementi ostacolanti.

[18] Dilazione – Il successo dei potenziali infrattori viene ritardato in modo che la reazione finalizzata alla prevenzione del danno possa risultare molto probabilmente efficace.

[19] Prevenzione – Il successo dei potenziali infrattori viene impedito fintanto che una reazione finalizzata alla prevenzione del danno risulta sicuramente efficace.

[20] Detezione – Gli eventi rilevanti per la sicurezza devono essere individuati in tempo utile per disporre reazioni finalizzate alla prevenzione e alla riduzione del danno.

[21] Intervento – Gli eventi rilevanti per la sicurezza richiedono un intervento per la prevenzione o la riduzione del danno.

2.4 Principi guida per la protezione degli edifici

[22] Un'effrazione alla periferia dell'edificio (porte, finestre e involucro) deve essere ostacolata in modo che i tentativi di effrazione possano essere con ogni probabilità rilevati.

[23] Il furto di asset, beni e attrezzature aziendali deve essere ostacolato e, nel caso di informazioni e asset sensibili, non deve passare inosservato.

[24] Deve essere garantita un'immediata evacuazione delle persone dagli edifici con pericoli particolari o un'elevata occupazione nell'arco di 15 minuti qualora si verifichino scenari di potenziale pericolo in caso di permanenza nell'edificio.

[25] Gli atti di sabotaggio non devono avere conseguenze gravi sull'attività operativa che eccedono il valore prestabilito negli obiettivi di protezione generali per l'interruzione dell'attività operativa e i danni materiali.

[26] L'accesso all'edificio al di fuori dell'orario di lavoro deve essere controllato e registrato a tutte le entrate in modo che possa essere impedito un ingresso non autorizzato.

[27] L'accesso all'edificio all'interno dell'orario di lavoro deve essere controllato e registrato a tutte le entrate in modo che possa essere impedito un ingresso non autorizzato.

[28] La presenza di persone non autorizzate nell'edificio deve essere prevenuta.

[29] I danni prevedibili causati dagli elementi naturali (carte dei pericoli) devono essere prevenuti per mezzo di misure di protezione.

[30] Ove possibile, vanno implementate misure preventive contro le aggressioni. Dopo un evento di questo genere va assicurata un'assistenza professionale alle vittime.

[31] Lo spionaggio deve essere prevenuto con misure proporzionate, in particolare nei luoghi particolarmente a rischio.

3 Standard di sicurezza minimo

3.1 Obiettivi legali di protezione

[32] Occorre garantire che vengano rispettati tutti i requisiti di legge locali vigenti (leggi, condizioni di autorizzazione, direttive e standard).

3.2 Edificio

[33] L'edificio deve essere in grado di sopportare le condizioni atmosferiche abituali della località in cui è ubicato. Per quanto possibile, gli accessi non autorizzati devono essere prevenuti.

3.3 Protezione perimetrale

[34] Ai confini degli stabili o al più tardi al passaggio dalle zone pubbliche o miste alle zone interne devono essere posizionati sbarramenti fisici chiaramente riconoscibili.

3.4 Videosorveglianza

[35] Qualora dall'analisi dei rischi risulti la necessità di un sistema di videosorveglianza, le registrazioni devono essere indicizzate in funzione degli eventi.

[36] È richiesto un piano scritto in cui siano indicati i parametri applicati.

[37] Devono essere rispettate le disposizioni di legge vigenti in materia di protezione dei dati, in Svizzera la Legge federale sulla protezione dei dati (RS 235.1).

3.5 Organizzazione

[38] Ove imprese e persone svolgono compiti di sicurezza, le loro mansioni e i loro obblighi devono essere documentati in forma scritta e sottoscritti dal committente responsabile.

3.6 Impianti di segnalazione delle effrazioni

[39] Qualora dall'analisi dei rischi risulti la necessità di un impianto di segnalazione delle effrazioni, occorre garantire che gli allarmi vengano tracciati e documentati.

3.7 Verifica, ispezione e manutenzione

[40] Occorre garantire che tutti i dispositivi, gli impianti e i sistemi di sicurezza vengano periodicamente sottoposti a verifiche, test e manutenzione. Gli impianti disattivati a fini di manutenzione, riparazione o verifica devono essere immediatamente riattivati al termine dell'intervento.

3.8 Documentazione

[41] Il piano di protezione e, ove presenti, le analisi dei rischi devono essere tenuti aggiornati e verificati a intervalli prestabiliti. I piani di protezione (o parti di essi) devono essere resi accessibili e disponibili alle persone coinvolte nella protezione degli edifici.

4 Assistenza

4.1 Controlli

[42] Group Security esegue controlli nelle sedi secondo un approccio basato sul rischio. Qualora si verifichino modifiche rilevanti presso sedi importanti per l'azienda, queste ultime sono tenute a contattare Group Security.

4.2 Consulenza generale sulla protezione degli edifici

[43] Per consulenza e assistenza è possibile contattare Group Security, che funge da centro di competenze. GSE-SEL fornisce assistenza in merito alla metodologia di valutazione dei rischi per stabilire il livello di sicurezza adeguato.

5 Informazioni sul documento

Nel presente documento viene descritta l'applicazione della Security Policy nel campo della protezione degli edifici. A tal fine vengono fissati il livello d'ambizione, gli obiettivi di protezione e i requisiti minimi.

Esso costituisce la base per garantire un livello di sicurezza adeguato nell'intero Gruppo Swisscom nonché per analizzare e applicare misure adeguate.

5.1 «Versione 1»

Doc ID	SA-02159-C1-Piano del gruppo per la protezione degli edifici
Classificazione	C1 Public
Ambito di applicazione	Swisscom SA
Data di emissione	05.04.2022
Stato	released
Oggetto del documento	Direttiva di sicurezza
Correlazioni	LLV-IAM-032/ LLV-SYS-002/ LLV-SYS-003/ LLV-SYS-006/ LLV-IAM-068/ LLV-SYS-024/ LLV-ANA-002/ LLV-ANA-010