Sicherheitsanweisung

SA Film- und Fotoaufnahmen

Swisscom AG

Group Security
Postfach
3050 Bern

Version	Datum	Person	Vorgenommene Anpassungen/Bemerkungen
0.5	20.08.2022	André Papageorgiu	Entwurf
0.6	25.08.2022	Claudio Passafaro	Finalisierung für Vernehmlassung
0.7	19.10.2022	Daniel Zysset	Formatierung und Struktur
0.8	10.11.2022	Claudio Passafaro	Letzte Rückmeldungen eingepflegt
0.9	09.12.2022	Daniel Zysset	Übersetzt und finalisiert
1.0	09.12.2022	Thomas Dummermuth	Prüfung/Freigabe
1.0	01.05.2023	Daniel Zysset	Kleine formelle Anpassungen vorgenommen

Verantwortlich: SiBe Brand-Objektschutz
Herausgeber: SiBe Brand-Objektschutz
Erstellung: 20.08.2022
Ersteller: Passafaro Claudio
Geht an: gemäss 1.1 Geltungsbereich

Inhalt

1 Einleitung

[1] Swisscom ist ein bekanntes Telekommunikationsunternehmen. Sicherheit hat für Swisscom einen zentralen Stellenwert und damit sind auch Vertrauenswürdigkeit und Zuverlässigkeit zentrale Qualitätsattribute. Als grösstes Telekommunikationsunternehmen der Schweiz sind wir nicht nur als primäres Angriffsziel attraktiv, unsere Infrastruktur ist für Kriminelle oder Nachrichtendienste auch als Sprungbrett interessant, um an Daten von Dritten beziehungsweise unserer Kunden zu gelangen. Hackerangriffe erfolgen nicht mehr ausschliesslich online, zunehmend wird für erfolgreiches Hacking vorgängig sogenanntes Social Engineering betrieben.

[2] Social Engineering ist ein Verfahren, um mittels Ausnutzens menschlichen Verhaltens an Informationen zu gelangen, die letztlich für verschiedenste Betrugsmaschen verwendet werden. Dabei werden menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft, Angst oder Respekt vor Autorität ausgenutzt, um an vertrauliche Informationen zu gelangen, unbewusst Schadsoftware einzuschleusen oder Sicherheitsfunktionen ausser Kraft zu setzen.

[3] Zentrales Merkmal bei Angriffen mithilfe Social Engineering ist die Täuschung über die Identität und die Absicht der Täterschaft. Dabei verwendet die Täterschaft betriebsinterne Informationen zu Personen, Funktionen, Standorte, Prozesse, Firmenslang usw.

[4] Als primäre Informationsquelle nutzt die Täterschaft gezielt öffentlich zugängliche Quellen wie Fotos und Filme, die in sozialen Netzwerken oder im Internet publiziert wurden.

1.1 Geltungsbereich

[5] Dieses Dokument gilt für die gesamte Swisscom (Schweiz) AG, mit allen Geschäfts[1]- und Konzernbereichen[2] mit Sitz im In- und Ausland folgend Swisscom genannt.

[6] Die Konzerngesellschaften bauen ein eigenes Security Management auf oder schliessen sich dem Security Management der Swisscom an. Die Verantwortung für die Security liegt weiterhin bei der Konzerngesellschaft. Der Entscheid liegt in der Verantwortung der Konzerngesellschaft und wird von Group Security unterstützt

[7] Die vorliegende Sicherheitsanweisung regelt dem Umgang mit Film- und Fotoaufnahmen durch Swisscom-Mitarbeitende und auf sämtlichen von Swisscom genutzten Flächen.

[8] Sie gilt zudem für Tochtergesellschaften mit deren Mitarbeitenden sowie für Auftragnehmer, die von Swisscom genutzte Flächen betreten. Sie gilt hingegen nicht für deren Flächen und Gebäude.

[9] Sie gilt ergänzend zu gesetzlichen Bestimmungen wie beispielsweise für den Daten- und Persönlichkeitsschutz.

1.2 Referenzierte Dokumente

[1] Zu den Geschäftsbereichen zählen Retail Customers („B2C“), Business Customers („B2B“) sowie IT, Network & Infrastructure („INI“)

[2] Zu den Konzernbereichen zählen Group Business Steering („GBS“), Group Human Resources („GHR“), Group Communications & Responsibility („GCR“) und Group Security & Corporate Affairs („GSA“)

[1] Direktive-Sicherheit

[2] Security-Policy

[3] Schweizerisches Bundesgesetz über den Datenschutz (DSG) 235.1

1.3 Schutzziel

[10] Bei Film- und Fotoaufnahmen ist sichergestellt, dass:

- der Schutz vertraulicher und geheimer Informationen gewährleistet ist,
- die unkontrollierte Verbreitung vertraulicher und geheimer Informationen verhindert wird und
- der öffentliche Einblick in unternehmensinterne Abläufe, Rollen und Informationen begrenzt wird.

2 Bestimmungen

2.1 Allgemeine Bestimmungen

[11] Jeder Betreiber von Flächen kann aufgrund des lokalen Schutzbedarfs generelle Film- und Fotoverbote und Ausnahmebewilligungsprozesse erlassen.

[12] Es sind keine persönlichen, vertraulichen oder geheimen Informationen preiszugeben, die Swisscom, Mitarbeitenden, Kunden oder Partnern gehören.

[13] Nur als öffentlich klassifizierte Informationen (C1) dürfen veröffentlicht werden.

[14] Zitate, auch sinngemässe, sind nur nur mit Einverständnis der Originalquelle zu machen. Die Rechte an geistigem Eigentum sind zu wahren.

[15] Offizielle Mitteilungen und Stellungnahmen von Swisscom sind dem Mediendienst zu überlassen. Falls sich Journalisten wegen eines Eintrags bei dir melden, verweise sie an den Mediendienst.

2.2 Foto- und Filmaufnahmen zur innerbetrieblichen Verwendung

[16] Aufnahmen, denen ein innerbetrieblicher Verwendungszweck zugrunde liegt, sind zulässig. Beispielsweise für Schulungszwecke oder Mängelerfassung (nicht abschliessende Aufzählung).

[17] Aufnahmen, welche nicht für die Veröffentlichung vorgesehen sind, sind mindestens mit C2 zu klassifizieren und zu behandeln.

[18] Aufnahmen dürfen nur die für den konkreten Verwendungszweck relevante Informationen enthalten.

[19] Entfällt der Verwendungszweck, so sind die Aufnahmen zu löschen bzw. entsprechend ihrer Klassifizierung abzulegen.

[20] Der Zugriff auf die Aufnahmen ist auf das Minimum zu beschränken.

2.3 Foto- und Filmaufnahmen zur ausserbetrieblichen Verwendung

[21] Swisscom ist seit 2009 auf diversen Social-Media-Plattformen aktiv. Wenn Foto- oder Filmaufnahmen von Swisscomliegenschaften, -anlagen, -shops sowie dort befindlicher Personen auf öffentlichen oder privaten Kanälen publiziert werden sollen, sind folgende Sicherheitsregeln zu beachten:

[22] Vor der Publikation ist vom Nutzer bzw. Betreiber der Fläche, der Anlage oder des Gebäudes eine Einwilligung einzuholen. Die Ansprechperson für die Flächen und Anlagen ist der Value Stream Manager vom Value Stream Basic Infrastruktur und von den Gebäuden der Security Agent von Corporate Real Estate Management.

[23] Need to know-Prinzip: Es sind nur so viele Informationen preiszugeben wie unbedingt notwendig.

[24] Adressen und Aufnahmen im Freien, die eine örtlich exakte Zuordnung erlauben, sind bei Infrastrukturbauten zu vermeiden – ausser es handelt sich um öffentlich bekannte Standorte.

[25] Sicherheitseinrichtungen sind nicht zu zeigen oder – wenn nötig – ohne konkreten Bezug zu einem Standort und ohne konkreten Einsatzbereich bei Swisscom.

[26] Erkennbare Personen dürfen nicht ohne deren Einverständnis aufgenommen und gezeigt werden.

[27] So wenig Mitarbeitende mit Namen und Funktion vorstellen wie möglich.

[28] Vermeiden, Marken- und Produktenamen von Infrastruktur sowie IP- und andere technische Zuordnungsnummern zu zeigen (Netzwerkinformationen, Router- oder Switchnamen).

[29] Es dürfen keine Kundennamen (Firmenlogos, Namen, Adressen etc.) genannt oder gezeigt werden.

[30] Prüfe die Aufnahme sorgfältig, bevor du sie veröffentlichst. Du bist dafür verantwortlich. Beachte, dass einmal im Internet publizierte Inhalte grundsätzlich permanent öffentlich zugänglich bleiben.

3 Vollzug

[31] Die Betreiber von Gebäuden und Flächen wenden diese Sicherheitsanweisung an. Namentlich beurteilen sie Gesuche für Film- und Fotoaufnahmen und erteilen entsprechende Einwilligungen und Auflagen.

[32] Group Security - Physical Security überwacht die Umsetzung dieser Sicherheitsanweisung und unterstützt die Betreiber in der Auslegung.

4 Dokument Information

Dieses Dokument regelt den Umgang mit Film- und Fotoaufnahmen durch Swisscom-Mitarbeitende auf sämtlichen von Swisscom genutzten Flächen

4.1 «Version 1.0»

Doc ID	SECDOC-111
Titel	SA Film- und Fotoaufnahmen
Classification	C1 Public
Scope of application	Swisscom AG
Issue date	20.08.2022
Status	realeased
Document subject	Sicherheitsanweisung
Related LLV	LLV-DAT-001, LLV-DAT-003, LLV-DAT-004, LLV-DAT-005,