Herstellererklärung Cybersicherheit

NEWLIFT
NEUE ELEKTRONISCHE WEGE

Cybersicherheit Elevision 4.0

Herausgeber: NEW LIFT Neue elektronische Wege Steuerungsbau GmbH

Lochhamer Schlag 8
82166 Gräfelfing

Tel.: +49 (0) 89/89 866 – 0
Fax: +49 (0) 89/89 866 – 300
E-Mail: info@newlift.de
WEB: http://www.newlift.de

Dokument-Version: 1.1

Herstellererklärung Cybersicherheit

NEWLIFT
NEUE ELEKTRONISCHE WEGE

Historie der Dokumentversionen

Dokument Version	Datum	Ersteller	Freigabe	Bemerkungen
1.1	08.03.24	Thomas Früchtl	Ja	Ersterstellung

Freigabe durch:

Name	Datum	Funktion	Abteilung	E-Mail
Peter Zeitler	16.03.24	GF	GL	info@newlift.de

Inhaltsverzeichnis

1 Allgemein 3
2 Verwendete Standards und Normen 3
3 Begriffe und Abkürzungen 3
4 Produkt Anforderungen 4
4.1 Grundsätzliche Anforderungen aus der ISO62443 4
4.2 Security Level 4
5 Elevision 4.0 4
5.1 FR1 Identifikation und Authentifizierungskontrolle 4
5.1.1 Ergebnis 4
5.2 FR2 Nutzungskontrolle 4
5.2.1 Ergebnis 5
5.3 FR3 Systemintegrität 5
5.3.1 Ergebnis 5
5.4 FR4 Datenvertraulichkeit SL-T1 5
5.4.1 Ergebnis 5
5.5 FR5 Eingeschränkter Datenfluss SL-T1 5
5.5.1 Ergebnis 5
5.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1 5
5.6.1 Ergebnis 5
5.7 FR7 Ressourcenverfügbarkeit SL-T2 5
5.7.1 Ergebnis 5

6 Gesamtübersicht 6

1 Allgemein

Nach der TRBS 1115-1 müssen nach Stand der Technik MSR Systeme vor Cyberbedrohungen geschützt sein, so das Gefährdungen von Personen bei überwachungsbedürftigen Anlagen vermieden werden.

Zur Beurteilung der Gefährdungen durch Cyber-Angriffe wird für die NEW LIFT FST Familie die ISO8102-20 als Richtlinie herangezogen. Diese verweist an vielen Stellen auf die IEC62433.

NEW LIFT sieht sich in erster Linie als Komponenten Hersteller und Entwickler
Daher wird die IEC62443 Teil 4 als relevant betrachtet.

2 Verwendete Standards und Normen

TRBS 1115-1
ISO8102-20
IEC62443-4

3 Begriffe und Abkürzungen

E4 Elevision 4.0 Cloud Plattform
EUC Geräte unter Kontrolle (Equipement under Control)
SL-C Security-Level Capability; Security-Level, den ein Gerät oder System erreichen kann, wenn es richtig eingesetzt und konfiguriert ist
SL-A Security-Level Achieved; Der im Gesamtsystem erreichte und messbare Security-Level
SL-T Security-Levlel Target; Dieser zu erzielende Security-Level ist ein Ergebnis der Bedrohungs-/Risikoanalyse (ISO 8102-20)
FR1 bis FR7 Basic Requirement, Grundlegende Anforderung siehe IEC62443-3-3 ab Punkt 5

4 Produkt Anforderungen

4.1 Grundsätzliche Anforderungen aus der ISO62443

Grundvoraussetzung FR
FR1- Identifikation und Authentifizierungskontrolle
FR2- Nutzungskontrolle
FR3- Systemintegrität
FR4- Datenvertraulichkeit
FR5- Eingeschränkter Datenfluss
FR6- Rechtzeitige Reaktion auf Ereignisse
FR7- Ressourcenverfügbarkeit

4.2 Security Level

Level	Beschreibung
0	Keine besondere Anforderung oder Schutz erforderlich.
1	Schutz vor unbeabsichtigtem oder zufälligem Missbrauch.
2	Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
3	Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation
4	Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation

5 Elevision 4.0

5.1 FR1 Identifikation und Authentifizierungskontrolle

Das Elevision 4.0 System verfügt über verschiedene Authentifizierungs und Identifizierungs Verfahren so das unterschiedlicher Security Level erreicht werden können.

5.1.1 Ergebnis

Mit Elevision 4.0 kann durch Aktivierung der 2 Faktor Authentifizieren **mindesten SL-C3** (erreichbarer Security Level) erreicht werden.

5.2 FR2 Nutzungskontrolle

E4 bietet unterschiedliche Nutzerrollen an. Zugriffe und Veränderungen werden im Systemlog mitprotokolliert, sind vom Admin jederzeit einsehbar und können als PDF archiviert werden.

5.2.1 Ergebnis

Das E4 besitzt für den FR2 **mindestens den SL-C3**

5.3 FR3 Systemintegrität

Das E4 wird bei einem Hoster(Serverfarm) der nach ISO27001 zertifiziert ist gehostet.
Die Daten werden regelmäßig auf ein externes Laufwerk gesichert

5.3.1 Ergebnis

Das Elevision 4.0 **erreicht**, für FR3, den Security Level SL-C2

5.4 FR4 Datenvertraulichkeit SL-T1

Das Elevision 4.0 speichert außer der email Adresse keinen Personenbezogenen Daten.

5.4.1 Ergebnis

Das Elevision 4.0 **erreicht**, für FR4, mindestens den Security Level SL-C2

5.5 FR5 Eingeschränkter Datenfluss SL-T1

Die Datenverbindung zur Aufzugssteuerung findet, bei GSM, über einen VPN Kanal statt
Die Verbindung von Webbrowser zu Webserver ist TSL verschlüsselt.

5.5.1 Ergebnis

Das Elevision 4.0 **erreicht**, für FR5, mindestens den Security Level SL-C2

5.6 FR6 Rechtzeitige Reaktion auf Ereignisse SL-T1

Elevision 4.0 wird per „Grafana“ überwacht und gemonitort.
Zusätzlich werden Ereignisse im Systemlog aufgezeichnet.

5.6.1 Ergebnis

Das Elevision 4.0 **erreicht**, für FR6, mindestens den Security Level SL-C2

5.7 FR7 Ressourcenverfügbarkeit SL-T2

Elevision 4.0 wird per Grafana überwacht und gemonitort.
Der Server wird auf Speicherverfügbarkeit überwacht und bei Bedarf aufgerüstete

5.7.1 Ergebnis

Das Elevision 4.0 **erreicht**, für FR7, mindestens den Security Level SL-C2

6 Gesamtübersicht

Herstellererklärung Cybersicherheit bezogen auf:

TRBS 1115-1
ISO8102-20
IEC62443-4

17.03.2024

Gesamtergebnis:

Produkt	FR1 / SL-T	FR2 / SL-T	FR3 / SL-T	FR4 / SL-T	FR5 / SL-T	FR6 / SL-T	FR7 / SL-T	Grundsätzliche Anforderungen aus der ISO8102-20 erfüllt*
Elevision 4.0	3	3	2	2	2	2	2	**JA**

Die „Herstellererklärung Cybersicherheit – Elevision 4.0 NEW LIFT“ ist unter dem Link https://www.newlift.de/downloads.html - „Bescheinigungen / Zertifikate“ abrufbar.

NEW LIFT Neue elektronische Wege Steuerungsbau GmbH
Lochhamer Schlag 8
82166 Gräfelfing

* Es sind die Voraussetzungen für die Teilergebnisse des jeweiligen Produktes zu beachten!