MEMO

Postbus 154
3990 DD Houten

Tel: 030 – 290 1623
Fax: 084 – 210 4325

Email: info@sbcl.nl

Onderwerp: Cyberbeveiliging voor bestaande liften
Kenmerk: 25-042
Datum: 19 september 2025

SBCL wil dat bestaande liften (ook wel (lift)installaties genoemd) in gebouwen goed bestand zijn tegen cyber aanvallen (hierna: cybersecurity).
De bij dit document behorende quick-scan kan hieraan bijdragen.
Bij de bouw van nieuwe liften wordt al rekening gehouden met de beveiliging tegen cyber aanvallen.

Cybersecurity is belangrijk omdat het de digitale systemen, instelgegevens en netwerken van o.a. liften beschermt tegen aanvallen, schade en ongeoorloofde toegang.
Als het gaat om cyberbeveiliging zijn eigenaren van liften nog onvoldoende doordrongen van de gevaren die er zijn voor hun liften.
Een lift die verbonden is, of verbonden kan worden met het internet of waarvan de software met een tool of vaste verbinding benaderbaar is, kan door een kwaadwillend persoon worden beïnvloed. Het is om die reden van belang te kijken naar cybersecurity.
Het is aan te bevelen dat liften door maatregelen van de lift-installateur tegen cyberdreigingen worden beschermd. Dat is in Nederland nog niet wettelijk verplicht. In bijv. Duitsland worden liften al wel periodiek getoetst op cybersecurity-maatregelen.

De belangrijkste redenen waarom cybersecurity bij liften cruciaal is, zijn:

<u>Voorkomen van inbreuk op veiligheid</u>
- Inbreuk op instellingen of veiligheidssysteem van de lift, kan ongecontroleerde liftbeweging veroorzaken met letsel of dood tot gevolg
- Inbreuk op liftsysteem kan uitval van veiligheidssysteem veroorzaken
- Lift kan worden gebruikt als niet geoorloofde toegang tot gebouwsystemen

<u>Voorkomen van schade aan -systemen- van derden</u>
- Lift kan worden gebruikt als niet-geoorloofde toegang tot gebouwsystemen (GBS, beveiliging etc.)
- Overname van liftbesturing om liftgebruik te beïnvloeden

<u>Voorkomen van financiële schade</u>
- Uitval van de lift, mensen kunnen hun bestemming niet of moeilijk bereiken
- Uitval van de lift, operatie kan komen stil te vallen;
- Gevaar van aansprakelijkheid als de lift wordt gebruikt als niet geoorloofde toegang tot gebouwsystemen

De eigenaar van de lift en/of de onderhoud partij zal in staat moeten zijn om de beoordeling op cybersecurity uit te (laten) voeren. Het is een lastige opgave waarvoor je niet alleen bekend moet zijn met lifttechnologie, maar ook met cybersecurity- en liftnormen.

Beoordeling van cybersecurity in de lift
De beoordeling van cybersecurity maatregelen in liften en/of liftsystemen kan starten met een risicobeoordeling. Op basis daarvan kunnen maatregelen worden genomen.

Procedure van een risicobeoordeling

1. Identificeer en vermeld de interfaces van de componenten van de lift die kunnen worden gecompromitteerd. Dit betekent dat diegene die kijkt naar de risico's van cybersecurity, in zijn proces naar de volgende componenten moet kijken:
    - Connectiviteitsystemen (noodoproepsysteem, spreek luister verbinding (SVL), afstandbewaking, koppeling gebouw beheer systeem)
    - Beveiligingsrelevante connectiviteitssystemen
    - Andere IT/OT componenten, indien digitaal en cyberrelevant bescherming behoevend (zie ISO 8102-20)
    - PESSRAL-componenten

2. Evalueer of het onderdeel dat kan worden getroffen door een cyberaanval een zodanige functie heeft dat er een kritieke toestand kan ontstaan.
   Voorbeeld: Tweerichtingscommunicatiesysteem of noodoproepsysteem:
    - De de-activering vertegenwoordigt al een kritieke bedrijfstoestand, als een opgeslotene geen hulp kan inschakelen.
    - Mogelijke toegang op afstand via een externe besturingssysteem interface is iets wat niet uit te sluiten is.
3. Controleer of er componenten zijn, met name veiligheidsvoorzieningen, die opzettelijk kunnen worden uitgeschakeld, geactiveerd of waarvan de parameters kunnen worden gewijzigd.
4. Inventariseer technische documentatie van het liftsysteem (informatie van de fabrikant, bijv. uit de gebruiksaanwijzing, certificaten met betrekking tot cybersecurity van de gebruikte componenten, ondersteunende dienstverleners)
5. Definieer en documenteer maatregelen.
   De maatregelen worden uitgevoerd na de risicobeoordeling door de lift-installateur. Waar kunt u als lift-installateur informatie vinden over de componenten die risico lopen en wat zijn mogelijke maatregelen?

Mogelijke maatregelen

De volgende maatregelen zijn mogelijk (niet limitatief):

- Vermindering van onvoldoende beveiligde interfaces naar de buitenwereld
- Hardware-interfaces die niet nodig zijn voor het veilig functioneren van de lift, blokkeren of extra beveiligen.
- Mechanische toegangsbeperkingen invoeren voor operatorinterfaces en bekabelde interfaces zoals:
  - Mechanische barrières (gesloten machinekamers, besturingskasten (MRL) gesloten houden)
  - Toegewezen autorisatieniveaus in het besturingssysteem voor bijv. bediening, onderhoud en reparatie
  - Noodzakelijke interfaces met toegang op afstand (bijv. noodoproep-systeem/onderhoud op afstand) kunnen worden beschermd door firewalls en wachtwoorden
  - W-LAN / Bluetooth-interfaces alleen activeren voor onderhoud en reparatie voor de periode waarin dit nodig is.

Schema: *voorbeelden van besturingen, risicovolle interfaces en de mogelijke maatregelen om ze te beveiligen*

<table>
<tr><th colspan="2">Ontwerp van de liftbesturing</th><th>Besturing</th><th>Overige componenten bijv. PessRal</th><th>Mogelijke maatregelen</th></tr>
<tr><td colspan="2">Netwerk Interfaces</td><td>Spreekluisterverbindingen
Toegang op afstand mogelijk in de besturing (onderhoud/ monitoring)</td><td>-</td><td>Firewall/ wachtwoord</td></tr>
<tr><td rowspan="5">Hardware en gebruiker interfaces</td><td rowspan="3">Vaste bedrading</td><td>RS232</td><td>USB</td><td rowspan="3">Interface afsluiten door kast of machinekamer op slot te houden. Toegang beperken.</td></tr>
<tr><td>USB</td><td>LAN</td></tr>
<tr><td>LAN, CAN open</td><td>CAN open</td></tr>
<tr><td rowspan="3">Draadloos</td><td>W-LAN</td><td>-</td><td rowspan="3">Interface alleen actief tijdens onderhoud en beschermen met firewall/wachtwoord</td></tr>
<tr><td>Bluetooth</td><td>-</td></tr>
<tr><td>Overige draadloze verbindingen</td><td>-</td></tr>
</table>

Deskundige hulp is belangrijk

Er moet rekening mee worden gehouden dat de fabriekscertificaten voor afzonderlijke componenten niet zonder meer voldoende zijn als bewijs voor het complete systeem.
Deze afzonderlijke certificaten kunnen worden opgenomen in de documentatie van de lift-installateur als basis voor de risicobeoordeling en functioneren als startpunt voor de RI&E-analyse op cybersecurity.
Na analyse en uitvoeren van cybersecurity maatregelen kan er een penetratietest worden uitgevoerd.

Quick scan Cybersecurity voor liften

Fabrieksnummer:
Apparatuurnummer

Onderdeel *	Resultaat Quick Check cybersecurity		
1 Toegang tot het systeem Onbevoegden hebben toegang tot het liftbesturingssysteem/de machinekamer.	☐	NEE, er is geen potentieel gevaar geïdentificeerd.	
	☐	JA, een aanval op of storing van het systeem/onderdeel is mogelijk. Er moet een uitgebreide gevarenbeoordeling worden uitgevoerd en de daaruit voortvloeiende maatregelen moeten worden opgevolgd.	
2 Besturings-Technologie A Er zijn draadloze interfaces naar digitale liftonderdelen beschikbaar.	☐	NEE, er is geen potentieel gevaar geïdentificeerd.	
	☐	JA, een aanval op of storing van het systeem/onderdeel is mogelijk. Er moet een uitgebreide gevarenbeoordeling worden uitgevoerd en de daaruit voortvloeiende maatregelen moeten worden opgevolgd.	
3 Besturings-Technologie B Er zijn fysieke interfaces voor het programmeren van digitale liftonderdelen met externe apparaten beschikbaar. Deze zijn onvoldoende beveiligd.	☐	NEE, er is geen potentieel gevaar geïdentificeerd.	
	☐	JA, een aanval op of storing van het systeem/onderdeel is mogelijk. Er moet een uitgebreide gevarenbeoordeling worden uitgevoerd en de daaruit voortvloeiende maatregelen moeten worden opgevolgd.	
4 Systeem voor noodoproepen op afstand Er is een interface tussen SLV en de liftbesturing beschikbaar.	☐	NEE, er is geen potentieel gevaar geïdentificeerd.	
	☐	JA, een aanval op of storing van het systeem/onderdeel is mogelijk. Er moet een uitgebreide gevarenbeoordeling worden uitgevoerd en de daaruit voortvloeiende maatregelen moeten worden opgevolgd.	
5 Systeem voor bewaking op afstand Er is geen certificaat van de fabrikant beschikbaar.	☐	NEE, er is geen gevaar geïdentificeerd of er is geen systeem voor bewaking op afstand beschikbaar.	
	☐	JA, een aanval op of storing van het systeem/onderdeel is mogelijk. Er moet een uitgebreide gevarenbeoordeling worden uitgevoerd en de daaruit voortvloeiende maatregelen moeten worden opgevolgd.	
Samenvatting	☐	Er zijn geen gevaren geïdentificeerd met betrekking tot de onderzochte onderdelen. Er zijn momenteel geen verdere maatregelen vereist.	
	☐	Er is ten minste één onderdeel met een verhoogd risico op interferentie van buitenaf. Een aanval of storing van het systeem/onderdeel is mogelijk. Er moet een uitgebreide gevarenbeoordeling worden uitgevoerd en de daaruit voortvloeiende maatregelen moeten worden opgevolgd.	

Toelichting op de Quick-scan

Onderdeel 1
Het gaat hier om de fysiek toegang, bijv. doordat de sleutel van de machinekamer naast de lift hangt.

Onderdeel 2 A
Draadloze interfaces. Denk hierbij bijv. aan WLAN, Bluetooth, etc.

Onderdeel 3 B
Fysieke interfaces:
Denk hierbij bijv. aan USB, RS232, etc.

Onderdeel 4
SLV = spreekluisterverbinding

Onderdeel 5
Geen bijzonderheden