



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Informationssicherheit in der Gebäudeautomation

*Mangelhafte Dokumentation und Betrieb von undokumentierten
Fernwartungszugängen*

CSW-Nr. 2023-222993-1031, Version 1.0, 04.04.2023

IT-Bedrohungslage*: 1 / Grau

Sachverhalt

In einem Feldtest des BSI wurden branchenspezifische IT-Sicherheitsprobleme im Gebäudemanagement (GM) und der Gebäudeautomation (GA) festgestellt. Auch in diesem Bereich hat die Digitalisierung in den letzten Jahren und Jahrzehnt stark zugenommen. Die GA automatisiert gewerksübergreifend die einzelnen Gewerke der technischen Gebäudeausrüstung (TGA). Die einzelnen TGA-Gewerke, wie Brandmeldeanlagen (BMA), Löschanlagen, Rauchabsauganlagen (RAS) und Sprachalarmierungsanlagen, Fluchttürensteuerung und Zutrittssysteme, werden zunehmend über die GA vernetzt, visualisiert und gesteuert. Für das Errichten, Warten und Betreiben der Systeme sind meist externe Unternehmen verantwortlich, welche über die erforderlichen fachspezifischen Errichter-Akkreditierungen und Qualifikationen verfügen.

Das GM, sowie die Komponenten, Systeme und Anwendungen der GA und TGA sind oft nicht oder nur eingeschränkt im Informationssicherheitsmanagement (ISMS) einer Organisation berücksichtigt. Dies spiegelt sich wieder in

1. keinen oder unzureichenden Vorgaben und Prozessen zur IT-Sicherheit im Gebäudemanagement (GM) beim Planen, Errichten, Betrieb und Warten,
2. unvollständige oder fehlende Betrachtung von Abhängigkeiten kritischer Geschäftsprozesse von Gebäudefunktionen,
3. fehlenden Sicherheitskonzepten für die GA und die einzelnen TGA-Gewerke,
4. kein oder unzureichendes Überprüfen von bestehenden technischen und organisatorischen IT-Sicherheitsmaßnahmen.

Aus den fehlenden Vorgaben resultieren unter Anderem:

- Unvollständige und veraltete Dokumentation für GM, GA und TGA.
 - › Änderungen, Erweiterungen und Anpassungen (auch durch Dienstleister) werden nicht erfasst.
 - › Das Unternehmen macht sich abhängig von einzelnen Dienstleistern.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.

2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.

3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.

4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

- Unzureichende vertragliche Regelungen zwischen dem Unternehmen und dem Dienstleister. Die Verantwortlichkeiten sind nicht eindeutig festgelegt.
- Ein koordiniertes Patchmanagement findet nicht statt. Geräte erhalten keine notwendigen Sicherheitsupdates oder nutzen veraltete unsichere Protokolle.
- Zur Wartung und Entstörung der GA und TGA werden vom Dienstleister unzureichend gesicherte Fernwartungszugänge in der Organisationsinfrastruktur etabliert oder sogar undokumentierte Fernwartungszugänge genutzt.

Bewertung

Das GM und deren eingesetzte GA und TGA stellen essentiell wichtige Funktionen für das Funktionieren einer Organisation bereit. Störungen reichen von Komforteinschränkungen, wenn Beleuchtung oder Klimatisierung der Büros beeinträchtigt ist, bis hin zu gefährlichen Situationen, die Menschenleben gefährden können. Ein Beispiel für den letzteren Fall stellt das Zusammenspiel von Fluchttüren, Brandmeldeanlage und Zutrittsmanagement dar. Auf der einen Seite müssen im Brandfall die Türen geöffnet werden, auf der anderen Seiten dürfen die Fluchttüren nicht unberechtigt geöffnet werden. Wenn ein Angreifer diese Steuerungen manipuliert, öffnen sich die Türen im Notfall ggf. nicht oder sie können unberechtigt geöffnet werden. Wenn solche Zwangsläufigkeiten über zentrale Systeme der GA gesteuert werden, besteht für diese ein erhöhter Schutzbedarf, um Manipulationen und weiteren Schaden zu verhindern.

Eine initiale Infektion von IT-Infrastrukturen mit Schadsoftware erfolgt in den meisten Fällen über Büroarbeitsplätze. Besteht eine Verbindung zwischen einem infizierten Büroarbeitsplatz und der GA, ist meist aufgrund der beschriebenen Probleme (wie z. B. fehlendes Patchmanagement) eine Ausbreitung von Schadsoftware und ein weiteres Eindringen eines Angreifers nicht mehr zu verhindern.

Auch unzureichend abgesicherte Fernwartungszugänge können durch unberechtigten oder nicht autorisierten Zugriff als Einfallstor für Schadsoftware missbraucht werden.

Vor diesem Hintergrund sind die gefundenen Mängel als kritisch zu bewerten. Ungeschützte oder unsichere Teile der GA oder TGA gefährden nicht nur ihre jeweilige Funktion. Sie können das Gesamtsystem und sogar die gesamte Organisation für Angriffe verwundbar machen. Auch wenn aktuell noch keine gravierenden Vorfälle zu beobachten sind, besteht dringender Handlungsbedarf. Aufgrund der Vielzahl an Komponenten und dem komplexen Zusammenwirken der einzelnen Gewerke ist eine organisationsübergreifende Integration der GA und TGA in ein ISMS erforderlich.

Maßnahmen

Organisationen sollten prüfen, welche Regelungen zur IT-Sicherheit für das GM, die GA und TGA vorhanden sind. Langfristig sind entsprechende Konzepte zu erstellen.

Beim Erfassen des IST-Zustands ist eine enge kooperative Zusammenarbeit zwischen IT-Sicherheitsbeauftragten und den Verantwortlichen für das GM erforderlich. Es sollte ein offener und kooperativer Austausch erfolgen, um mit den Herausforderungen bei dem Betrieb von Bestandsanlagen umzugehen und angemessene Lösungen zu erarbeiten. Dabei sollte auf die Sicherheitsrisiken für die gesamte Organisation sensibilisiert werden.

Erste Maßnahmen sollten sich auf die Erfassung und Absicherung aller Fernwartungszugänge beziehen, um diese bezüglich deren Kritikalität bewerten zu können. Gleiches gilt für Netzwerkübergänge von Systemen der GA und TGA in die IT-Infrastruktur. Hier sollten alle notwendigen Kommunikationsbeziehungen erfasst und auf das betrieblich Notwendigste reduziert werden.

Danach kann der Abgleich des IST-Zustand schrittweise erweitert werden, indem alle Geräte im Netzplan erfasst und mit der vorhandenen Dokumentationen abgeglichen werden. Hierbei ist es notwendig, die Dokumente mit den Gegebenheiten in der Schaltschränken vor Ort abzugleichen und ggf. die Dokumentation zu aktualisieren.

Erst mit der Erfassung aller Geräte kann die GA in das Risikomanagement des ISMS integriert und mit der Absicherungen der einzelnen Systeme begonnen, sowie Regelungen mit Dienstleistern getroffen oder angepasst werden.

Links

[1] INF.13 Technisches Gebäudemanagement, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2022/10_INF_Infrastruktur/INF_13_Technisches_Gebaeudemanagement_Edition_2022.pdf

[2] INF.14 Gebäudeautomation, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_14_Gebaeudeautomation_Edition_2023.pdf

[3] IND.3.2 Fernwartung im industriellen Umfeld https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompodium_Einzel_PDFs_2023/08_IND_Industrielle_IT/IND_3_2_Fernwartung_im_industriellen_Umfeld_Edition_2023.pdf

[4] ICS-Security-Kompodium https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompodium_pdf