www.facility-manager.de ISSN: 0947-0026 € 11,– SFr. 18,– B 13382 F

Der Facility Manager

Mit Stellenmarkt auf S. 6

März 2018
Heft 3, Jahrgang 25

Gebäude und Anlagen
besser planen, bauen, bewirtschaften

Light + Building
Human Centric Lightning • Gebäude-automation • IT-Sicherheit • Big Data 20

Bild: Jakub Jirsák.stock.adobe.com

IT-SICHERHEIT IN GEBÄUDEN

Ungeschützte Gebäudeleittechnik hat gravierende Folgen

Die Digitalisierung lässt die Herausforderungen für Bauherren und Betreiber wachsen. Aber die Angst vor Hackerangriffen auf die Gebäudeautomation ist angesichts der Konsequenzen noch viel zu klein.

Die Gebäudeleittechnik (GLT) nimmt einen wichtigen und steigenden Einfluss auf den Wert einer Immobilie. Investoren wissen längst um die Bedeutung ausfallender Komponenten, die zu häufigen Mieterwechseln und – schlimmer noch – zu Haftungsklagen führen können. Sie erwarten, dass hier eine bestmögliche Vorsorge getroffen wird. Konkret ist das vor allem die Konzeption von Präventionsmaßnahmen, die neue Cyberrisiken eindämmen helfen.

Die GLT als Angriffspunkt zu identifizieren, fällt indes den Tätern deutlich leichter als den Opfern. Den meisten Immobilienbetreibern fehlt das Problembewusstsein. Die Konsequenzen von Sicherheitslücken zeigen einfache Beispiele auf: Geht das fremdgesteuerte Licht in einem Bürogebäude aus, muss das gesamte Gebäude evakuiert werden. Schaltet die Kühlung der Serversysteme ab, wird in der Fabrik die Produktion bald stillstehen, denn die IT-Komponenten schalten sich bei Überhitzung selbstständig ab. Bei außer Gefecht gesetzten Zutrittsbarrieren weiß schließlich niemand mehr, wer sich im Firmengebäude befindet und auf welche Rechner er zugreift.

Auf diese Risiken wird in der Öffentlichkeit fast nie aufmerksam gemacht, denn es droht Imageverlust gegenüber Geschäftspartnern. Außerdem will niemand potenzielle Täter auf Schwachstellen aufmerksam machen. Doch mit der geringen allgemeinen Wahrnehmung steigt die Gefahr, dass weitere GLT-Systeme nur schwach oder gar nicht gesichert installiert werden. Damit wächst die Angriffsfläche für Täter. In dieser Situation tut Umdenken not. Entscheider müssen weg von der Devise „GLT muss funktionieren, mehr nicht", hin zu „damit GLT funktioniert, müssen wir sie schützen".

Von zentraler Bedeutung für die GLT-Sicherheit sind die Fragen:

- Wie können wir verhindern, dass interne oder externe Täter die GLT und damit den Geschäftsbetrieb lahmlegen?
- Was passiert im Havariefall?
- Haben wir eine gute Dokumentationsgrundlage, um im Notfall schnell reagieren zu können?

Ursachen aufdecken

Um die GLT perspektivisch sicher aufzustellen, muss das Umdenken nicht nur in den Köpfen der Fachverantwortlichen stattfinden. Wer die GLT als unliebsame Mitläuferin der Haustechnik betrachtet, kann die Vielschichtigkeit des Themas nicht erkennen. Deshalb verwundert es auch nicht, wenn die Abnahme selbst in großen Immobilien oftmals im Panikmodus verläuft. Der für die Abnahme Verantwortliche sollte die folgenden Fragen beantworten können:

- Von wo aus wird die GLT von wem und warum gesteuert?
- Wer hat wie intern und extern Zugriff?
- Wo ist das alles dokumentiert?
- Sind die Dokumentationen vollständig?
- Wo und wie erfolgt die Datensicherung?
- Welche Prozesse sind für Serviceeinsätze definiert und wie wird auch im Servicefall die Sicherheit gewahrt?

Dass bereits in der Planungs- und Vertragsphase versäumt wird, diese Fragen zu klären und zu dokumentieren, ist eine der wesentlichen Ursachen für die später mit entsprechend hohem Aufwand zu lösenden Probleme bei der Absicherung der GLT. Zwar ist das den meisten Fachverantwortlichen wohl bekannt, doch sind die Entscheidungen zu oben genannten Fragen in den komplexen Strukturen großer Unternehmen nur schwer herbeizuführen. Das notwendige Umdenken wird dann oft nur durch die Begleitung durch externe Kompetenzträger möglich. Das Ziel ist der grundsätzlich andere Umgang mit der GLT von Beginn an. Und das Schlagwort „Big Data" steht für die Brisanz dieses Vorhabens. Hier stellt die GLT eine wichtige Quelle von Status- und Zustandsinformationen dar. Daten zu Anwesenheiten, Raumtemperaturen, CO_2-Werten und vieles mehr bilden die Grundlage für die Steigerung der Energieeffizienz. Ebenso essenziell sind die Zustandsmeldungen aus der GLT für die Gesamtsicherheit einer Organisation. Sie liefern in Korrelation mit weiteren Daten aus dem Unternehmen wichtige Informationen für die Sicherstellung der (IT-)Security.

Big Data ist also der Schlüssel für Verbesserungen der Energieeffizienz, des Komforts und der Sicherheit. Dazu müssen

Bild: Monet.stock.adobe.com

Mit der GLT und IT intelligent verknüpfte Zutrittskontroll-Systeme erhöhen die Sicherheit und liefern Ansätze für die energieeffiziente Gebäudetechnik.

Bild: lassedesignen - fotolia.com

Einordnen statt ignorieren

Die Gebäudeautomation und die Gebäudeleittechnik sind traditionell Bereiche, die aufgrund ihrer fachlichen Nähe zur Immobilie dem Immobilienbetrieb, dem Facility Management oder dem Werksschutz zugeordnet werden. Die haben in der Regel wenig bis gar keine Berührungspunkte zur klassischen IT-Abteilung in Unternehmen. Vielmehr herrscht meist ein Klima von Desinteresse oder gar gegenseitigem Misstrauen. In der Folge kennt die für die Office- und Produktions-IT zuständige IT-Abteilung die Anforderungen und Strukturen der GLT-Systeme nicht. Oft weist sie jegliche Verantwortung für die GLT von sich.

Dass die GLT eine Insel in der Immobilie formt, die zwar mit IT betrieben wird, aber keine Anbindung an die klassische IT hat, ist ein ebenso üblicher wie gefährlicher Trugschluss. Der Austausch von Informationen zwischen Office-Systemen und der GLT ist für maximale Energieeffizienz obligatorisch und nimmt zu. Weil Angriffe auf GLT-Systeme unmittelbaren Einfluss auf den Betrieb der klassischen IT-Systeme (Serverkühlung, Zutrittsregelung etc.) haben, ist ihre Sicherheit auf eine Stufe mit der Office- und Produktions-IT zu heben. Firewalls, Anti-Viren-Systeme, Mehrfaktor-Authentisierung, Patch-Management usw. sind uneingeschränkt auf die IT-Ebene der GLT anzuwenden und das Monitoring der IT-Systeme muss auch die GLT-Systeme umfassen. Das heißt aber auch, dass sich die GLT-Verantwortlichen in den Unternehmen den Regularien der IT-Sicherheit unterordnen.

Bild: ProFM

Stefan Schaffner ist CEO der ProFM Facility und Project Management GmbH.

die zur Verfügung gestellten Daten allerdings zwingend drei Voraussetzungen erfüllen:

- Sie müssen sicher sein vor Ausspähung und Manipulation,
- zeitnah vorliegen und
- in ihrer Erhebung und Verarbeitung valide sein.

Nur kombinierte Maßnahmen schaffen Sicherheit

Um die eigene GLT sicher zu gestalten, sollten die Fachverantwortlichen früh agieren. Am besten noch vor der eigentlichen Bauplanungsphase. Wie jede Office- oder Produktions-IT hat auch die GLT in ihrem Kern ein IT-System. Dementsprechend wird sie auch so geplant, umgesetzt und gewartet. Die immer engere Kopplung an andere IT-Strukturen und externe Schnittstellen erfordert, dass die GLT als gleichwertiger Baustein in der gesamten IT-Architektur behandelt wird. Folglich muss das IT-Sicherheitskonzept der GLT auch in der Planung und in den Verträgen adäquat vertreten sein.

Wie bei allen anderen Projekten auch, bedarf es einer durchgehenden Dokumentation von Soll- und Ist-Zustand, damit aus dem Plan auch Realität wird. Im Rahmen der Abnahme der GLT ist deshalb neben rein funktionalen Tests auch die Einhaltung des IT-Sicherheitskonzeptes zu prüfen. Im Havariefall gilt es, das GLT-System zeitnah wiederherzustellen. Das kann nur gelingen, wenn neben einer validierten und regelmäßigen Sicherung der GLT-Daten und GLT-Systeme (Back-up) eine umfassende und stets aktualisierte Dokumentation vorliegt. Szenarien für einen raschen Recovery-Prozess sind festzulegen.

Fortwährende Fortbildung

Eine Organisation ist gut beraten, ihre Aus- und Weiterbildungsangebote rund um das Thema „GLT vor Angreifern schützen" zu erweitern. Einmalige Schulungen können das allerdings nicht leisten. Eine regelmäßige Weiterbildung ist notwendig, denn die Angreifer und ihre Methoden entwickeln sich stetig weiter. Für die fachverantwortlichen Mitarbeiter in den Unternehmen gilt es, Schritt zu halten. Im täglichen Betrieb ist die Sensibilisierung des beauftragten FM-Dienstleisters unabdingbar. Da Sicherheitslücken in der GLT Schäden erwarten lassen, die deut-

Bild: Dukes.stock.adobe.com

Die Frage nach der geeigneten Software stellt sich erst nach der unternehmensspezifischen Definition der Datensicherheits- und -sicherungsstrukturen.

lich mehr als nur Komfortverlust bedeuten, empfiehlt es sich, von Anfang an einen verantwortlichen Mitarbeiter zu benennen.

Viel Sicherheit lässt sich durch die intelligente Verknüpfung der Office-IT mit der GLT erzielen. Beispielsweise stellt ein Ausweis, mit dem sich der Mitarbeiter nur dann am PC anmelden kann, wenn er zuvor eine bestimmte Tür passiert hat, sicher, dass kein unbefugter Externer Zugriff auf den PC hat. Das bedarf natürlich geeigneter Schnittstellen zwischen Office-IT (PC) und GLT (Tür).

Die Bildung und Weiterentwicklung von Netzen bedarf allerdings der Vorüberlegungen: Wenn GLT und Office-IT Hand in Hand agieren, darf ein System das andere bei Angriffen nicht kompromittieren. Eine Aufteilung in zwei Schutzbereiche und die Einleitung der jeweils dazu passenden Maßnahmen erweisen sich in der Praxis als sinnvoll:

Die GLT-Ebene: IP-basierte Kommunikation und Feldbusprotokolle sind zu unterscheiden. Bei IP lassen sich weitgehend mit der Office-IT vergleichbare Schutzmaßnahmen (Firewall, VLAN usw.) anwenden. Bei den Feldbusprotokollen hängen die erforderlichen Schutzmaßnahmen von den eingesetzten Systemen ab.

Die IT-Ebene: Hier ist der Einsatz der in Office- und Produktions-IT verwendeten Maßnahmen in Firewalls, VLANs und Netzsegmentierung gegenüber Serversystemen zu unterscheiden. Letztere schützen durch sichere Kennwörter (oder 2-Faktor-Authentisierung), ein enges Monitoring, zeitnahes Patchen, ein Rollen- und Rechtekonzept sowie optional durch den Einsatz von Systemen für das Security Information and Event Management (SIEM).

Wer also glaubt, nur auf Basis der eingesetzten GLT-Softwarelösungen Abhilfe gegen Sicherheitslücken zu schaffen, springt zu kurz. Die wirksamen Weichen lassen sich nur in einer abgesicherten Infrastruktur auf der IT-Ebene stellen.

Softwarelösungen: Ausnahmsweise nachrangig

In der Praxis folgt beim Versuch, die GLT sicherer zu machen, schnell der Ruf nach einer geeigneten Software. Wenn die Anwendung dann in der Regel nicht (sofort) den erhofften Nutzen erzielt, liegt es jedoch selten an der Software. Vielmehr haben die Organisationen meist die oben benannten Hausaufgaben nicht erledigt. Der Mix aus den unterschiedlichen Maßnahmen macht's! Fragen wie: „Wo sind die Sicherungen im System zu platzieren?" oder „Sollten Sicherheitslösungen besser extern aufgesetzt sein?" haben erst nach der vollständigen Umsetzung des skizzierten Maßnahmenbündels ihren Platz auf der Tagesordnung. Als Ausblick auf lösungsrelevante Parameter seien im Folgenden dennoch die wichtigsten Eckdaten benannt.

Die Gebäudeautomation setzt bereits heute vielerorts auf moderne IT-Systeme. Folglich müssen hier dieselben Sicherheitsregeln gelten wie für die Office-IT – das sind zum Beispiel regelmäßig wechselnde, ausreichend differenzierte Passwörter. Zu jeder Zeit muss klar sein, wer, mit welchen Rechten ausgestattet, auf die GLT-Systeme zugreifen kann und darf. Nicht zuletzt ist festzulegen, wie mit externen Fachkräften und Auftragnehmern umgegangen wird. Transparenz, Nachvollziehbarkeit und Sicherheit sind die Schlüsselworte.

Kein Weg führt an einer geschützten GLT vorbei

Die GLT ist bereits heute ein wesentliches Gut einer Immobilie. Und diese Entwicklung verschärft sich: GLT avanciert mit „Smart Building"-Konzepten zur Schlüsselkomponente für Mehrwert. Energieeffizienz durch intelligente Steuerung funktioniert aber nur mit einer einsatzbereiten und zukunftsorientierten GLT. Es führt also kein Weg daran vorbei, sich mit der sicheren und geschützten GLT frühzeitig auseinanderzusetzen. Die Anforderungen sind klar zu kennen und zu formulieren. Wer hier Wissenslücken hat, ist bestens beraten, diese mithilfe externer Kompetenzträger zu schließen.

Red. Bearbeitung: Detlef Hinderer