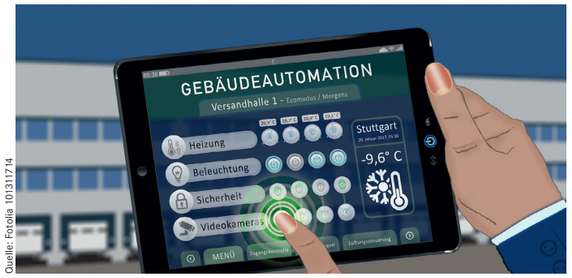
Blauäugiger Umgang mit der Gebäudeleittechnik

Die Vorstellung allein verbreitet Angst und Schrecken: In großen Industrieunternehmen stehen die Maschinen still, Versorgungsunternehmen können keinen Strom mehr liefern, Akkus können nicht mehr geladen werden, Server überhitzen infolge fehlender Kühlung, nichts funktioniert mehr.



Quelle: Fotolia 101311714

Mit der Vernetzung der Systeme gehen viele Vorteile einher. Doch auch die Gefahren sind mit ihr gestiegen.

So absurd es auf den ersten Blick scheint: All dies kann – so es denn jemand mit krimineller Energie darauf anlegt – innerhalb kürzester Zeit Realität werden: Heute noch, morgen oder erst später im Jahr. Warum begegnen also deutsche Unternehmen den teilweise gravierenden Sicherheitslücken in der Gebäudeleittechnik so gelassen und schauen blauäugig zu, wie sich die Situation stetig verschärft und die Risiken wachsen?

„Housten, wir haben ein Problem."

Der Frage nachgehend, woran es denn nun wirklich liegt, dass viele Unternehmen schlicht die Absicherung ihrer Gebäudeleittechnik verschlafen, lohnt ein Blick in die Historie. Nicht lange ist es her, da war die Gebäudeleittechnik (GLT) nämlich noch ein isoliertes System, das in den Kellern untergebracht war und anfangs keinerlei PC- oder Serversysteme benötigte. Seit deren Einführung wurde die GLT ausschließlich von Spezialisten betreut, die wiederum keinen IT-Fokus mitbrachten. Alles in allem waren ja auch nur simple IT-Systeme erforderlich, bei denen schon eine Kennworteingabe eine merkliche Hürde für ihre Akzeptanz darstellte – was sich nicht zuletzt in praxi in Form von auf den Monitor geklebten Kennwort-Postits zeigte.
Getreu dem Motto „Never change a running system" wurden beispielsweise Updates als unkalkulierbares Risiko eingestuft, für die sich in der Regel niemand verantwortlich fühlte. Vielmehr wurde die Fernwartung als risikolose Innovation angesehen und entsprechende Zugänge wenig umsichtig an alle Errichter verteilt. Irgendwann, als GLT-Informationen auch an anderer Stelle erforderlich waren, wurde die GLT einfach mit der restlichen IT verbunden.Inzwischen ist also aus dem einst übersichtlichen Funktionalitätenumfang ein hoch komplexes System unterschiedlichster Komponenten geworden, das in seiner Detailtiefe und in seiner Angreifbarkeit allerdings unterschätzt wird. Darin liegt auch der Hauptgrund, warum die GLT nicht längst ein wichtiger Baustein in sicherheitsstrategisch ausgelegten Konzepten ist. Und das, obwohl die Gebäudeleittechnik mit den inzwischen selbstverständlich gewordenen technischen Möglichkeiten längst Einfluss auf den Wert einer Immobilie nimmt.
Den Eigentümern und Investoren ist in der Regel schon bewusst, dass ausfallende GLT-Komponenten zu Mieterwechseln oder gar zu Haftungsklagen führen können. Zunächst einmal ist also (wie so oft im Leben) die Erkenntnis, dass die GLT als solche viel zu lange ein Schattendasein führte, der entscheidende erste Schritt, sie künftig sicherer zu gestalten.

GLT ist Teil der IT

Nach der Erkenntnis, dass überhaupt etwas getan werden muss, hakt es in weiten Teilen auch an der thematischen Einordnung der GLT. Viele Fachverantwortliche sehen sie nach wie vor als autarke Haustechnik, was sie schon lange nicht mehr ist. Diese Fehleinschätzung führt aber in der Regel dazu, dass die Vielschichtigkeit der GLT und ihre Einflussfaktoren völlig unbeachtet bleiben. Dass das so ist, nimmt früh seinen Anfang: Bereits im Zuge der Planung einer Liegenschaft spielen in den seltensten Fällen GLT-Themen und deren Absicherung eine Rolle.
Umso weiter wird dann der Weg hin zu der Wahrnehmung sein, dass die GLT zwingend Teil der „normalen" IT ist und damit auch so behandelt werden muss. Essentiell für die IT sind beispielsweise Zustandsmeldungen aus der GLT, die für die Gesamtsicherheit in einer Organisation wesentlich sein können. Sie müssen zudem an den unterschiedlichsten Orten innerhalb und außerhalb der Immobilie verfügbar gemacht werden.
Parallel dazu gelten die Modifikation und Steuerung der GLT-Systeme auch dezentral inzwischen längst als unverzichtbar. So funktionieren beispielsweise Wartung und Notfallunterstützung heute nur noch über den Fernzugriff effizient. All jene Merkmale decken sich mit denen klassischer IT Systeme, so dass sich die GLT nicht mehr wesentlich von der Office- und Produktions-IT unterscheidet. Um also nicht eines Tages bei Kerzenschein den Büroalltag zu beschließen, bedarf es dringend eines sach- und fachgerechten Zusammenspiels und ebensolcher Schutzmaßnahmen beider Bausteine: GLT und IT.

Ein Maßnahmenorchester muss her

Ein dritter wesentlicher Fehler liegt in der Tatsache begründet, dass viele Organisationen – wenn sie erkannt haben, dass sie etwas tun müssen und dass GLT und IT zusammen betrachtet werden müssen – auf Insellösungen setzen, die jedoch nicht helfen (können). Sie scheinen aber vielen Entscheidern das gute Gefühl zu geben, das Richtige zu tun. Dieses Gefühl trügt. Denn: Insellösungen können unmöglich die Antwort auf die Absicherung hochkomplexer Systeme sein. Im Gegenteil: Sie tragen mitunter noch zusätzlich zu ihrer Unübersichtlichkeit bei und sorgen somit für neue Gefahren.
Bewährt hat sich hingegen die strukturierte und noch vor Baubeginn startende Diskussion, wie die GLT eingebettet in die Gesamt-IT sicher gestaltet und damit vor externen Manipulationen und Angriffen geschützt werden kann. Die daraus resultierenden Konzepte gilt es genau zu dokumentieren und allen Beteiligten zugänglich zu machen, damit kontinuierliche Abgleiche des einst festgelegten Soll-Status mit dem Ist-Zustand erfolgen können.
Ein wesentlicher Punkt in einem möglichen Maßnahmenorchester muss also die möglichst frühe zeitliche Einordnung des Themas GLT-Sicherheit und die Einführung prozessualer Kontrollmechanismen sein. Darüber hinaus sollten Organisationen ihre Mitarbeiter hinsichtlich des Themas „Angriffsziel GLT" regelmäßig weiterbilden, damit die Sensibilität dafür insgesamt wächst. Daneben sind viele weitere Schritte notwendig. Ganz am Ende des Maßnahmenkatalogs stehen jedenfalls erst technische Lösungen, deren Einführung zusätzlich prozessunterstützend und risikominimierend wirkt.

Anforderungen an externe Dienstleister

Im Zuge der Maßnahmenorchestrierung spielt der FM-Dienstleister in der Regel eine nachrangige Rolle. die dennoch nicht zu unterschätzen ist. Zum Zuge kommt er in der Regel erst, wenn in neuen Immobilien die Strukturen und Systeme längst definiert und auch in Betrieb genommen wurden. Folglich können die externen FM-Experten kaum noch oder gar keinen Einfluss auf die Architektur nehmen. Zudem wechselt der Dienstleister im Lebenszyklus einer Immobilie häufiger, so dass sich immer wieder neue Mitarbeiter mit den Systemen auseinandersetzen müssen. Daher ist eine dauerhafte Aufgabenübertragung im Bereich IT, IT-Sicherheit oder IT-Wartung auf diesen nicht sinnvoll. Vielmehr lohnt es sich aus Betreiberperspektive hier die Expertise von IT-Spezialisten heranzuziehen.
Der FM-Dienstleister sollte als reiner Anwender fungieren, dem allenfalls klar definierte und überprüfbare Teilaufgaben übertragen werden – gleichwohl können Schulungen und eine ausreichende Sensibilisierung für das Thema IT-Sicherheit nicht schaden. Aus IT-Perspektive spannend sind FM-Beratungshäuser, die eine Schnittstelle zum IT-Fachwissen vorweisen können. Sie sind gefordert, ihre Kunden nicht nur im Bereich Property Management, sondern eben auch im Bereich IT-Zukunftsorientierung auf Kurs zu halten. Alternativ dazu können Immobilienbetreiber die erforderlichen Kompetenzen unterschiedlicher Dienstleister bündeln, müssen dann aber die entsprechend höheren Abstimmungsaufwände schultern.

Fazit

Die Sorge vor dem GLT-Supergau ist groß – und sie ist leider berechtigt. Tagtäglich verzeichnen Organisationen Angriffe auf ihre IT-Systeme, deren Verbindung mit der GLT aus Tätersicht ein willkommenes Einfallstor formt. Aus der einst nahezu autark arbeitenden Gebäudeleittechnik ist längst ein mit der Unternehmens-IT komplex verwobenes Gesamtsystem geworden. Dies zu erkennen ist ein erster wichtiger Schritt. Danach zu handeln müssen viele noch lernen.

Der Autor
Stefan Schaffner, CEO, ProFM Facility und Project Management GmbH

Nachgefragt

Herr Schaffner, die Gebäudeleittechnik in ihrer Funktion als mögliches Angriffsziel wird gemeinhin unterschätzt. Woran liegt das Ihrer Meinung nach?
Schaffner: In erster Linie fehlt in den meisten Häusern die Erkenntnis, dass hier eine reale Gefahr droht. Dass das allerdings tatsächlich so ist, stellen die meisten dann leider viel zu spät fest. Beispielsweise genau dann, wenn das Kind schon im Brunnen liegt und die Produktionsanlagen stillstehen müssen.

Wie oft kommt denn so ein Supergau tatsächlich vor und warum liest man dazu nicht häufiger in den Medien?
Schaffner: Das kommt öfter vor, als viele denken. In der Regel wird mindestens jedes zweite Unternehmen einmal im Jahr Opfer eines externen Angriffs auf die Gebäudeleittechnik – was allerdings aus Image- und auch aus Sicherheitsgründen gern verschwiegen wird. Darum liest man dazu auch wenig bis gar nichts in der Presse.

Woran liegt es, dass beispielsweise Industrieunternehmen oder auch andere Branchen diese Gefahren bewusst übersehen?
Schaffner: In unserer täglichen Arbeit erleben wir immer wieder, dass zum Beispiel die GLT-Verantwortlichen mit uns gemeinsam das erste Mal den IT-Leiter kennenlernen. Jeder Einzelne ist sich der Gefahren durchaus bewusst, aber in großen Konzernen sind die Strukturen oft nicht gegeben, dass diese beiden regelmäßig miteinander kommunizieren und sich abstimmen, geschweige denn klare Verantwortlichkeiten vergeben werden. Darüber hinaus ist es auch extrem schwierig, die GLT im Nachhinein – also mitten in der Betriebsphase – in sichere Fahrwasser zu bringen. Dafür bedarf es tiefer Expertise, die mitunter von außen eingekauft werden muss. Darum raten wir immer wieder im Rahmen von Neubauvorhaben, wirklich frühzeitig, am besten noch in der Planungsphase, die GLT und ihre Absicherung sowie alle dazu erforderlichen Prozesse zu thematisieren und zu dokumentieren.