

In ähnlicher Form veröffentlicht in LANline

Thema: Gebäudeautomation: Netzwerksicherheit

Angriff auf Gebäudeautomation: So gelingt effektiver Schutz

Autor: Stefan Schaffner, Geschäftsführung, ProFM Facility & Project Management GmbH

IT-Sicherheit spielt auch in Gebäuden eine entscheidende Rolle. Immerhin ist aus modernen Immobilien Stand heute die IT-gestützte Gebäudeautomation nicht mehr wegzudenken. Diese gilt es folglich mit allen Mitteln zu schützen. Anderenfalls drohen Chaos und wirtschaftliche Ausfälle – unter Umständen sogar eine ernst zu nehmende Gefahr für Leib und Leben.

Ohne Vernetzung geht es nicht mehr

Sowohl der Mieterwunsch, das Streben nach Komfort- und Effizienzsteigerungen als auch gesetzliche Anforderungen verstärken die Notwendigkeit, GA Systeme mit den übrigen Systemen im Gebäude zu vernetzen. Gemeint sind hier zum Beispiel auch Zugangskontrollsysteme oder Videoüberwachungssysteme, die mit den Anwendungen für die Office-IT und Produktions-IT zusammen wachsen sollen. Dieses Zusammenspiel birgt allerdings einige Gefahren. Beispielsweise ist die Office-IT auf die Verbindung mit weiteren internen und externen Systemen ausgelegt. Es gibt zahlreiche Maßnahmen und Systeme, die einen Schutz nach außen hin ermöglichen. Die Office-IT ist seit mehr als 20 Jahren mit dem Internet verbunden – folglich sind entsprechende Prozesse und Tools vorhanden. Bei der Gebäudeautomation bzw. der Gebäudeleittechnik ist IT in Form von PC-Systemen und Servern in der GA erst seit etwa 15 Jahren intensiver im Einsatz. Bislang waren diese Systeme oft weder mit dem Internet noch mit der restlichen IT verbunden. Schutzmechanismen waren aus Sicht der Entwickler auch nicht notwendig oder sinnvoll.

Gebäudeleittechnik ist angreifbar

Historisch bedingt treffen in der GA/GLT also als weitgehend ungeschützte Systeme auf eine komplexe Office-IT-Welt. Prozesse, die den Fokus insgesamt auf Sicherheit gegen Angriffe von extern *und* intern legen, sind nur wenige vorhanden. Mechanismen und Tools, die innerhalb der Office-IT für Sicherheit sorgen, lassen sich in der GA/GLT Welt nicht oder nur eingeschränkt einsetzen. Die eingesetzten GA/GLT-Softwarelösungen sind zudem teilweise nicht auf den aktuellen Betriebssystemen einsetzbar. Firewalls und andere Tools konterkarieren die Funktionen und lassen sich nicht oder nur mit viel KnowHow für diesen Einsatzzweck anpassen. Ungenügender Schutz lässt hingegen neue Angriffsvektoren entstehen. Angriffe, die etwa über die Office-IT zur GA kommen, können nicht kompensiert werden. Anders herum steht auch außer Frage, dass Angriffe auf die GA negative Auswirkungen auf die Office-IT haben können. Sabotage-Angriffe könnten folglich gezielt auf die GA/GLT stattfinden. Die Folgen sind weitreichend und erstrecken sich über teilweise erheblichen wirtschaftlichen Schaden bis hin zu beispielsweise herabfallenden Fahrstühlen mit Personenschaden oder Lüftungen, die sauerstoffarme Luft in die Räume pumpen.

Praxisbewährte Schutzmaßnahmen

Grundlage für die Installation geeigneter Schutzmaßnahmen ist den Erfahrungen der ProFM-Berater folgend zunächst einmal eine genaue Analyse aller in der GA/GLT eingesetzter Systeme sowie die konsequente Umsetzung eines Patchmanagements für alle IT Systeme in der GLT. Darüber hinaus sollten alle IT-Sicherheitskriterien bei Ausschreibungen in das Leistungsverzeichnis aufgenommen werden. Die Absicherung der eingesetzten IT Systeme erfordert zudem den Einsatz geeigneter Tools, beispielsweise von Gateways (Middleware). Mit der Lösungsintegration allein ist es jedoch nicht getan. Vielmehr bedarf es auch stimmiger Prozessabläufe und engagierten Mitarbeitern, die für die neuen Systeme geschult und im Sinne der GLT-Sicherheit weitergebildet werden. Damit im Laufe des Gebäudebetriebes keine Sicherheitslücken aufkommen, empfiehlt sich zudem ein kontrollierter Zu-



gang zu GA/GLT-Systemen und eine frühzeitige Prävention. So ziehen Betreiber die GLT-Netze beispielsweise bereits in der Planungsphase von Gebäuden als gleichberechtigte IT-Netze und IT-Systeme ein. Grundsätzlich gilt es nämlich, die Anforderungen der GLT bei der Konzeption und Architektur der gesamten IT zu berücksichtigen. Dabei sollten natürlich auch notwendige Informationsübergänge zwischen einzelnen Systemen der GA/GLT und der restlichen IT Beachtung finden. Im Zuge dessen spielen auch Normen und Vorschriften, die bereits heute im Bereich der GA bestehen (z.B VDI 3814), eine entscheidende Rolle.

Fazit

In Zeiten, wo die Vernetzung von IT auf nahezu allen Ebenen Anwendung findet, ist es auch für Immobilieneigentümer notwendig, rechtzeitig Vorsorge zu treffen. Immerhin ist die Gebäudeleittechnik als Teilelement der Gebäudeautomation spätestens seit ihrem Zusammenspiel mit der Office-IT angreifbar geworden. Im Sinne präventiver Schutzmaßnahmen gehen Betreiber nun dazu über, bereits in der Planungsphase Schutzziele festzulegen und deren dauerhafte Einhaltung zu überwachen. Nicht zuletzt aus rechtlichen Gründen (z.B. Betreiberpflichten) sind sie dazu sogar verpflichtet.