Digital? Aber sicher!

Cybersecurity für Life Sciences Unternehmen

Die Life Sciences-Branche denkt bei der digitalen Transformation vor allem an die Optimierung von Prozessen. Die Kehrseite davon: Mit wachsendem Datenstrom haben jedoch auch die potenziellen Sicherheitsrisiken zugenommen. Als wichtiges Rückgrat der Wirtschaft ist die Life Sciences-Industrie ein attraktives Angriffsziel für Hacker. Werden Produktionsprozesse jedoch gestört oder gar lahmgelegt, gerät die Versorgungssicherheit mit Wirkstoffen und Medikamenten ins Wanken. Das muss – und kann – verhindert werden: mit einem Cybersecurity-Konzept, das Schwachstellen aufdeckt und eliminiert.

Klaus Dederichs

Die häufigsten Schwachstellen finden sich oft an der gleichen Stelle, und zwar unabhängig vom jeweiligen Unternehmen. Ganz vorne auf der Liste der kritischen Punkte stehen z.B. die technische Gebäudeausrüstung und die Gebäudeautomation. Wer sich hier Zugriff verschafft, kann die Luftmengen, Temperatur- oder Feuchtewerte ganz einfach verändern – mit verheerenden Folgen für die GMP- und FDA-Regularien. Und es ist nicht nur die Software, die Risiken birgt. In vielen Gebäuden sind die Gebäudeautomationsregelungssysteme mit ihren Schaltschränken oft in Technikzentralen ohne jegliche Zugangssicherung verbaut sind. Segmentierten IT-Netze fehlen, und sichere Passwörter sind in der Regel ebenfalls nur unzureichend vergeben. Die Zugangsports zu den Gebäudeautomationssysteme sind meist offen für externe Zugänge, ebenso wie aktive Netzwerkkomponenten der Gebäudeautomation. So greift das interne oder das externe Facility Management oft remote über angeschlossener „Fritz!Boxen“ auf die Gebäudeautomation und Aufzugsanlagen zu. Die unternehmenseigene IT kennt diese Zugänge und aktiven Komponenten der Gebäudeautomation oftmals nicht. Sicherheits-Updates werden somit nicht kontinuierlich umgesetzt bzw. sind aufgrund des Alters der IT Komponenten nicht mehr verfügbar. Die Produktionsprozesse sind damit leicht manipulierbar. Dringen Hacker über Remote-Zugänge (Wartungszugänge der Dienstleister) in die Gebäudeautomationssysteme der Gebäude ein, besteht zudem die Gefahr, in Schutzgeldforderungen von Kriminellen einbezogen zu werden. Eine Gefahr, die in Zukunft noch steigen wird und vielen Unternehmen bereits eine Menge Geld und Reputationsverluste gekostet hat. Der Cyber War 2.0 verursachte im Jahr 2022 mehr als 203 Mrd. EUR weltweit (BITKOM) und das ist erst der Anfang.

Cybersecurity für Neubau und Bestand

Sicher begegnen lässt sich diesen Drohszenarien nur, wenn die Digitalisierungsstrategie auch den Datenschutz integriert. Und zwar von Anfang an. „Data protection by default“ lautet hier der Grundsatz, an dem alle Digitalisierungsbausteine ausgerichtet werden sollten. Zusammen mit dem IT-Dienstleister ComConsult hat das auf Bau und Immobilien spezialisierte Beratungsunternehmen Drees & Sommer daher eine Cybersecurity-Strategie für Gebäude und Produktion entwickelt, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Februar 2022 als Cybersecurity-Standard durch ComConsult entwickeln lies. Dieser ist für alle neu errichteten Gebäude und Anlagen zumindest im Öffentlichen Bereich verbindlich und bildet gleichzeitig eine fundierte Basis, auf der sich Cybersecurity auch für den Bestand optimieren und sicherstellen lässt. Ziel der Strategie ist es, zunächst alle eigenen Schwachpunkte in Erfahrung zu bringen, um sie im Anschluss sicher zu eliminieren.

Die Gefahr aufdecken – mit Penetrationstests…

Wer Sicherheitslücken verhindern möchte, sollte daher am besten schon während der Planungsphase eines Gebäudes Sicherheitsanforderungen an Soft- und Hardware berücksichtigen. Noch bevor ein digitales Gebäude in Betrieb genommen wird, müssen alle Hardware- und Software-Applikationen in einem Testcenter zudem einem sogenannten Penetrationstest unterzogen werden. Um Sicherheitslücken zu entdecken, werden alle Systembestandteile und Anwendungen mit Mitteln und Methoden konfrontiert, die Hacker anwenden würden, um unautorisiert in das System

einzudringen. Der Penetrationstest ermittelt die Empfindlichkeit des zu testenden Systems gegen derartige Angriffe und wird auch für Bestandsanlagen und -immobilien eingesetzt, um deren Betrieb sicherer zu machen und Cyberrisiken zu eliminieren. Damit lässt sich genau feststellen, wie empfindlich ein System ist und welche Schutzmaßnahmen daraus abgeleitet werden müssen.

…und Digital Ready Checks

Bei Bestandsimmobilien hilft zusätzlich ein Digital Ready- und Cybersecurity Check, potenzielle Gefahren zu definieren. Beim sogenannten Digital Ready- und Cybersecurity Check werden Produktionsgebäude und sonstige Liegenschaften wie Verwaltungsgebäude, Logistik und Versorgungsgebäude auf Herz und Nieren geprüft, was die IT-Infrastrukturen, Konnektivität, Cybersecurity und die technische Infrastruktur angeht. Daraus lassen sich die Schwachstellen der Infrastruktur darstellen, um daraus eine Sicherheitsstrategie und Optimierungsmaßnahmen abzuleiten, die in das gesamte Sicherheitskonzept des Standortes, der Gebäude und Liegenschaften integriert werden muss. Ein Cybersecurity-Konzept umfasst zudem nicht nur digitale Maßnahmen wie Firewalls, Segmentierung der Netze, Regelung zu Softwarteupdates etc. sondern auch die physischen und personelle Vorkehrungen, um einen sicheren Betrieb (Digital Operation) zu gewährleisten. Wer glaubt ein Sicherheitskonzept zu erstellen und dann ist alles in „trockenen Tüchern“ der irrt. Cybersecurity benötigt eine entsprechenden Organisationsstruktur im Unternehmen, die auch an Dienstleister ausgegliedert werden kann, da Cybersecurity eine 365 Tage/24 h professionelle Expertenbegleitung benötigt.

Bauliche Anforderungen an digitalisierte Gebäude – Customized Smart Building (CSB)

Digitale, intelligente und nachhaltige Gebäude unterscheiden sich von herkömmlichen Gebäuden in deren grundsätzlichen Konzeption. Die unterschiedlichen technischen Systeme werden mittels offen Schnittstellen (Open API´s) miteinander verbunden. Die Vernetzung übernimmt ein sogenanntes Gehirn (Brain). Das Vorbild des Menschen mit Gehirn, Rückgrat, Sinnesorganen beschreibt die Konzeption eines CSB recht gut. Es kann durch eine sogenannte „Digital Readiness“ heutige und zukünftige IoT Sensorik einfach integrieren. Im Mittelpunkt des CSB stehen die Mehrwerte für die Nutzer und Dienstleister in der Produktion und die damit verbundenen Optimierung der Prozesse, die Optimierung des Betriebs (CREM) und die Verbesserungen im Bereich der CO_2-Emissionen und der ESG Anforderungen etc..

Schutz personenbezogener Daten

Datenschutz steht bei Gebäuden an erster Stelle und muss daher auch von Anfang an Bestandteil jeder Digitalisierungsstrategie sein. Der Grundsatz „Data protection by design“ stellt dabei sicher, dass die Persönlichkeitsrechte aller Nutzer im Sinne der EU-Datenschutz-Grundverordnung

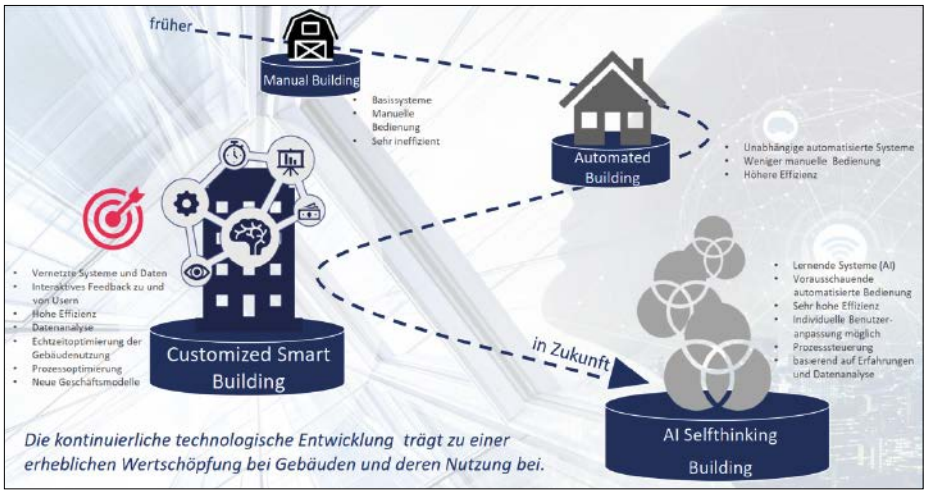

Abb. 1: Selfthinking Building

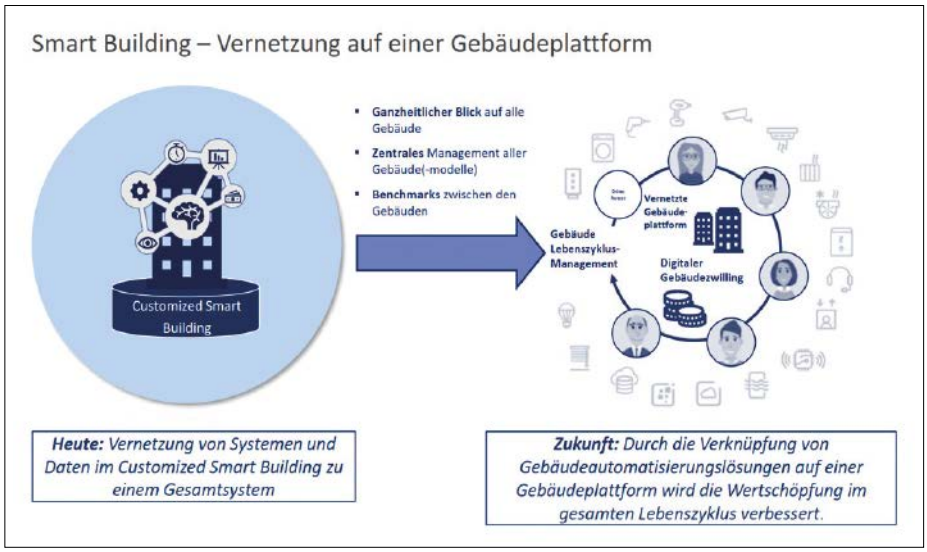

Abb. 2: Vernetzung Gebäudeplattform © Drees & Sommer

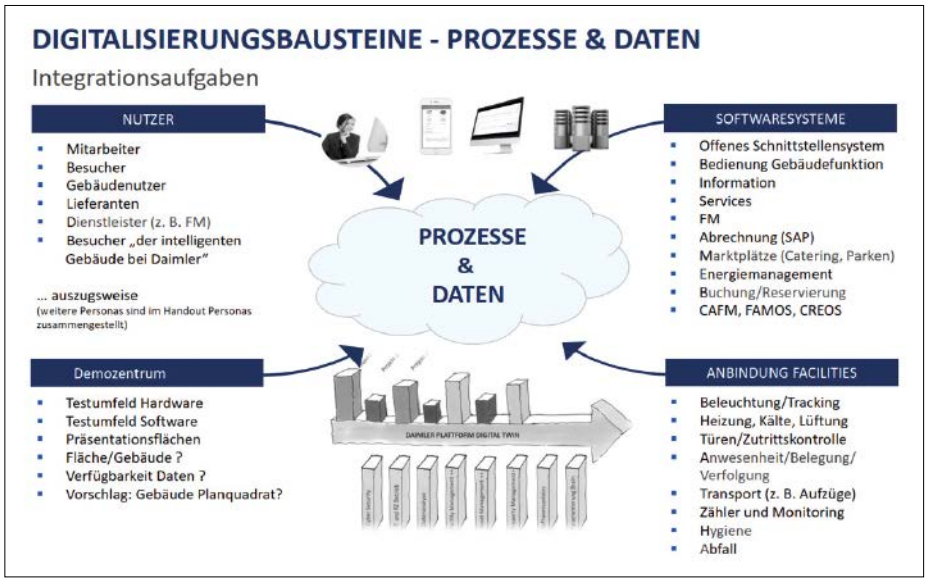

Abb. 3: Digitalisierungsbausteine © Drees & Sommer

und des deutschen Rechts (DSGVO) geschützt sind. Ein Smartes Gebäude sammelt die Betriebsdaten wie den Wasserverbrauch, Stromverbrauch, Kälte- und Wärmeverbrauch etc.. Solche Daten sind in der weiteren Verarbeitung völlig unkritisch und tragen dazu bei, den Betrieb eines Gebäudes zu optimieren. Gleichzeitig können Sensoren jedoch auch Informationen erfassen, aus denen sich Rückschlüsse auf individuelle Verhaltensmuster gewinnen lassen. Der Schutz dieser personenbezogenen Daten erfordert zusätzliche Maßnahmen, beispielsweise Anonymisierung oder Pseudonymisierung und die strikte Trennung zwischen Personendaten und Sensordaten in unterschiedlichen Datenbanken.

Schutz vor internem Datendiebstahl

Da für Datendiebstahl, Industriespionage oder digitale Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen auch die eigenen Mitarbeitenden verantwortlich sein können, sind für diesen Part der Cybersecurity mehrere Sicherheitsmaßnahmen notwendig – angefangen von der Benennung eines Datenschutzverantwortlichen über die Systemkonfiguration von Anlagen bis hin zur Gebäudeautomation. Dem Datenschutzbeauftragten fällt dabei die Kontrollfunktion zu. Seine Aufgabe ist es, fortwährend die Systeme und erhobenen Daten zu überprüfen und gegebenenfalls auf Verstöße zu reagieren. Während er somit eine menschliche Kontrollfunktion im Betriebsablauf übernimmt, müssen Hersteller von Anlagensystemen deren DSGVO Konformität von Vornherein nachweisen. Bei einer steigenden Anzahl der Nutzung von Cloud-Diensten im Gebäude und einer hohen Anzahl von IoT-Produkten aus dem asiatischen und amerikanischen Raum ist das eine große Herausforderung für die Zukunft. Nach der DSGVO müssen Daten zwingend in Europa gehostet werden. Mit „Data protection by design" in der frühen Planungsphase ist sie umsetzbar.

Von der Firewall…

Über jene Maßnahmen hinaus kommen im Sinne der Cybersecurity auch digitale Applikationen zum Einsatz. Ihre Aufgabe ist es vor allem, den täglichen Betrieb vor Hackerangriffen oder sonstiger Cyber-Kriminalität abzusichern. Neben Firewalls, Antivirus-Software und regelmäßigen Software-Updates empfiehlt sich insbesondere die Unterteilung des IT-Systems in Netzwerksegmente und einer ständigen Sicherheitsüberwachung der Systeme. Um IT-Ausfälle zu vermeiden, wird dafür ein redundantes IT-Netzwerk mit entsprechenden Servern und Storage-System im und außerhalb des Gebäudes aufgebaut. Dabei müssen die Zugriffsrechte klar geregelt sein.

…bis zum plattformübergreifenden System

Gleichzeitig ist es wichtig, sich nicht von proprietären Systemen abhängig zu machen. Wer künftig erfolgreich sein will, muss in Systemen und Cloud-Plattformen denken – das gilt auch für Gebäudeautomation. Als Betriebssystem der Immobilie muss die Gebäudeautomation eine grenzenlose Einbindung sämtlicher Gewerke ermöglichen – und das möglichst anbieteroffen. Denn bislang basiert die Gebäudetechnik/Haustechnik vorrangig auf proprietären Systemen. Das heißt: herstellereigene Systeme, in dem nur ein einziger Hersteller Komponenten dieses Systems anbietet, die nicht vernetzbar sind. Das führt zu einer hohen Abhängigkeit und zahlreichen Insellösungen. In Zukunft müssen vermehrt offene Systeme eingesetzt werden, die von vielen Herstellern unterstützt werden: Ihre Komponenten sind „interoperabel" und können miteinander in einer Anlage kommunizieren. Zu diesem Zweck muss eine Strategie erarbeitet werden, die eine einfache, effiziente und nachhaltige Einbindung von in und um das Gebäude befindlichen „Dingen" über Protokolle und Bussysteme erlaubt: die Systemarchitektur des Gebäudes mit einer integrierten Cybersecurity und DSGVO Strategie.

AUTOREN

Klaus Dederichs,
Partner und Head of ICT, Drees & Sommer

Stefan Göstl,
Head of Life Sciences & Chemicals,
Drees & Sommer

KONTAKT

Stefan Göstl
Drees & Sommer SE, München
Tel.: +49 89 1498 - 160
chemicals@dreso.com
www.dreso.com