Cybersicherheit für Gebäudetechnik

Zwölf essenzielle Maßnahmen

Cybersicherheit ist längst ein unverzichtbarer Bestandteil der Unternehmens-IT sowie der Industrie 4.0. Die Teile der IT, die in modernen Gebäuden zum Einsatz kommen, erfahren hingegen meist noch nicht den nötigen Schutz gegen Angriffe aus dem Cyberraum – die diesbezügliche Risikolage für Gebäude- und Sicherheitstechnik wird noch immer häufig unterschätzt und oft nicht ausreichend beachtet.

Von Werner Metterhausen, Bonn

Mittlerweile gleichen Gebäude- und Sicherheitstechnik in ihrer Komplexität und in ihrer Durchdringung mit Informationstechnik durchaus fortschrittlichen Produktionsanlagen. Ein Bürogebäude mit Baujahr 2021 ist beispielsweise nur noch dann nutzbar, wenn die IT, welche die Funktionalität und die Sicherheit des Gebäudes steuert und überwacht, einwandfrei funktioniert: Angefangen bei der Lüftung und Heizung über Zutrittskontrolle und Videotechnik bis hin zur Brandmeldeanlage wird eine Menge „klassischer" Technik in immer engerem Zusammenwirken mit IT zum Betrieb des Gebäudes erforderlich. Diese Mischung aus Gebäude- und Informations-Technik zur Betriebsführung eines Gebäudes – hier im Weiteren als „Operational Technology" (OT) bezeichnet – erfordert ein ebenso hohes Maß an Cybersicherheit wie die klassische IT oder die Industrie 4.0.

Um zu einer Vorstellung zu kommen, wie sich diese OT schützen lässt, darf man sich von der Industrie 4.0 inspirieren lassen: Dort wird die Musterarchitektur für die IT zur Messung, Steuerung und Überwachung der industriellen Technik durch die sogenannte Purdue-Referenz-Architektur beschrieben (vgl. etwa Wikipedia oder [1]). Obwohl sie über die Jahre in verschiedenen Variationen stetig erneuert wurde, ist die fünfschichtige Purdue-Einteilung informationstechnischer Systeme im industriellen Umfeld im Grunde immer noch gültig:

_____ Schicht 0 bilden die *Sensoren und Aktoren,* welche physische Prozesse messen und steuern. Ein einfaches System an dieser Stelle wäre ein Temperaturfühler, ein komplexes etwa ein Schweißroboter.

_____ Schicht 1 umfasst die zugehörigen *Steuerungs- und Regelsysteme,* oft mit speziellen Protokollen wie KNX, BACnet oder Modbus – gekoppelt mit den Geräten der Schicht 0 und untereinander.

_____ Schicht 2 enthält die *Bedienebene:* Sie kann ein Display an einem Gerät oder einer Anlage sein oder auch ein PC, der wiederum mit einem oder vielen Geräten der Schicht 1 verbunden ist.

_____ Schicht 3 ist die *Gebäudeautomation oder Betriebssteuerung,* in der durch Zusammenführung und übergeordnete Kontrolle der einzelnen Systeme Workflows entstehen.

_____ Schicht 4 schließlich ist die „normale" *Unternehmens-IT:* Hier werden beispielsweise Materialflüsse für den Zulauf und Ablauf der Produktion durch ein Enterprise-Ressource-Planning-(ERP)-System gesteuert oder die finanzielle Seite einer Produktion verfolgt.

Dieses Modell kann man 1 zu 1 auf den aktuellen Stand der Gebäude-OT übertragen, wie in Tabelle 1 veranschaulicht.

Empfehlungen aus der Praxis

Die von zur Mühlen'sche GmbH (VZM) adressiert das Problemfeld „Cybersicherheit der Gebäude-OT" seit Jahren im Rahmen ihrer Arbeit mit Bauherren und Betreibern und hat dabei die im Folgenden aufgeführten zwölf essenziellen Maßnahmen identifiziert. Diese sind bei Bau und Betrieb unabdingbar zu betrachten und umzusetzen, um für die immer komplexer und angreifbarer werdende Betriebs-, Steuerungs- und Sicherheitstechnik eines Gebäudes ein angemessenes Maß an Cybersicherheit zu schaffen und zu erhalten.

Zuständigkeit für OT in den richtigen Händen

So wie sich ein Brandschutzbeauftragter von Anfang an um den Schutz von Gesundheit und Leben aller

Menschen im zukünftigen Gebäude Gedanken macht und die Planung begleitet und bewertet, so muss sich ebenso frühzeitig ein Mensch mit passender Vorbildung Gedanken um die Cybersicherheit von Haus und Technik machen. Häufig muss man dazu in der zuständigen Abteilung „Facility-Management" zunächst (oder endlich) Wissen zu diesem Thema aufbauen.

Physische Sicherheit der OT

Komponenten der OT müssen sicher stationiert sein – das heißt: Sie werden in gesicherten Räumen unter IT-tauglichen Bedingungen betrieben. Vor allem muss die Elektroversorgung der Geräte den Ansprüchen der Technik und Funktion, die sie steuern, entsprechen. Gefahrenmeldeanlagen müssen etwa auch einen lang andauernden Stromausfall ohne funktionale Einschränkung überstehen – redundante Versorgungsstränge für Strom und Daten stellen sicher, dass ein punktueller Schaden keine wichtigen Funktionen im gesamten Gebäude gravierend stört oder ausfallen lässt.

OT-Sicherheitsarchitektur/ Netztrennung

Von Beginn an muss eine Netzarchitektur für das OT-Netz geschaffen werden: Einerseits beachtet sie das Schadenpotenzial der OT und vor allem der durch die OT gesteuerten und überwachten Anlagen, andererseits macht sie die Anforderungen und Wünsche an den Betrieb realisierbar.

Die Architektur für das OT-Netz ist ausgehend von einer Risikobetrachtung mit Blick auf die Technik, die im Gebäude zum Einsatz kommt oder kommen soll, und mit Blick auf die Anforderungen an Betrieb und Nutzung der Gebäudetechnik (und damit der Gebäude-OT) zu entwickeln.

Dieses OT-Netz ist ein virtuelles oder physisches Netz und läuft getrennt von der „normalen" IT. Auch in sich sollte man es durch Kontrolle (Firewalls) und Überwachung (Monitoring) in Schutzzonen untergliedern. So lässt sich etwa eine weniger bedeutsame „offene" Gebäude-OT (z. B. Präsentations- und Veranstaltungstechnik) von der wirklich kritischen OT (z. B. Zutrittskontrolle, Einbruchmeldeanlage) abschotten.

Inventarisierung der OT-Konfiguration

Ein Problem, das alle dem Autor bekannten Gebäude mit ihrer OT aufweisen, ist das Fehlen einer brauchbaren Dokumentation. Weder zur Errichtung und erst recht nicht mehr im laufenden Betrieb werden die Komponenten so detailliert dokumentiert, dass grundlegende Abläufe des Betriebs der Systeme möglich wären – etwa eine systematische Identifikation und Behebung (oder zumindest Entschärfung) von Schwachstellen. Ein ausreichend detailliertes Inventar von Hard- und Software ist jedoch die Grundlage aller Bemühungen um die Cybersicherheit!

Lieferanten und Dienstleister verpflichten und einbinden

Je stärker der Glaube daran ist, dass das eigene OT-Netz von allen anderen Netzen und vor allem vom Internet abgeschottet ist, desto argloser wird oft zugelassen, dass Wartungstechniker sich mit dem mitgebrachten Notebook per USB in das Netzwerk einklinken – und von Fernwartungszugängen des Lieferanten ist oftmals wenig mehr bekannt als deren Existenz. Richtig (und wichtig) wäre es hingegen, in Verträge mit Dritten explizite Vorgaben aufzunehmen, wie diese Zugriff auf „ihre" Technik erhalten.

Betriebssichere Konfiguration der OT herstellen und testen

Die ersten Schritte hin zu einem sicheren IT/OT-Betrieb bestehen darin, Standardeinstellungen wie Passwörter zu ändern und nicht benötigte Dienste dauerhaft zu deaktivieren.

Darüber hinaus muss es zum Bestandteil der Abnahme des Gebäudes samt seiner Gebäude- und Sicherheitstechnik werden, durch Kontrollen und Testwerkzeuge festzustellen, dass keine vermeidbaren Schwachstellen und Sicherheitslücken aus der Errichtung übrigbleiben. Diese erste „sichere" Konfiguration der OT ist detailliert zu dokumentieren und zu speichern – inklusive aller zum Betrieb erforderlichen Daten und Informationen und vorzugsweise in einer Konfigurationsdatenbank.

Tabelle 1: Anwendung der Purdue-Referenz-Architektur auf Gebäude-OT (nach wme/ TeMedia)

Internet	**mobile Geräte, Cloud-Services et cetera**
Level 4	Geschäftsprozesse („klassische" IT): Verwaltung, Betriebswirtschaft, ERP, CAFM, BIM Netzprotokolle: IP
Datenaustausch	**kontrollierte Grenze zwischen IT und OT**
Level 3	Betriebssteuerung – Workstations, Server (z. B. Zutrittskontrolle, Einbruchmeldezentrale etc.) Netzprotokolle: IP
Level 2	Bedienung – Touchpanel, Browser, PC-Anwendung Netzprotokolle: IP
Level 1	Gerätesteuerung – spezielle Steuereinheiten (z. B. Türensteuerung) Netzprotokolle: IP (TCP/UDP), BACnet/IP
Level 0	Geräte und Anlagen mit OT-Schnittstelle – Sensoren, Aktoren und I/O-Systeme (z. B. Kartenleser) Netzprotokolle: Modbus, KNX, LoRaWAN

Sicherer OT-Betrieb

Mindestanforderung an einen sicheren Betrieb ist die Fähigkeit, Ereignisse rechtzeitig zu bemerken und zu bewerten. Fast alle Geräte und Anwendungen protokollieren intern (Logging) und es gibt bewährte Lösungen, um übergreifend das Zusammenwirken einzelner Komponenten zu beobachten (Monitoring). Solche Instrumente müssen zielgerichtet eingesetzt werden.

Zum Zweiten sind jegliche Änderungen, die der Betrieb mit sich bringt, kontrolliert durchzuführen und auch zu dokumentieren. Dieser Change-Management-Prozess ist die einzige Chance, die Dokumentation aller Komponenten aktuell zu halten oder – gröber ausgedrückt – den Durchblick bei der üblicherweise komplexen OT-Informationstechnik zu behalten.

Backup und Restore

Ein heikles Thema ist immer die Datensicherung: Während es bei „normalen" Bestandteilen der Gebäude-OT wie PCs und Servern noch offenkundig sein mag, was wie oft gesichert werden muss, ist das bei Anlagenteilen wie Prozessrechnern oder der Firmware irgendwelcher Komponenten überhaupt nicht klar. Unklar ist häufig nicht nur das „Wie oft?" bei der nötigen Frequenz einer Datensicherung, sondern vor allem das „Wie?" bei einer Rücksicherung: Die Wiederherstellung eines Verzeichnisses oder einer virtuellen Maschine ist eher einfach. Die Wiederherstellung einer Anlagensteuerung muss hingegen nicht nur gut dokumentiert sein, sondern sogar geübt werden, damit sie auch im Notfall funktioniert.

Threat-Intelligence und Malware-Abwehr

Cybersicherheit befasst sich mit dem Schutz vor Angriffen auf bekannte Schwachstellen. Damit diese Schwachstellen nicht nur den Angreifern, sondern auch den Verteidigern bekannt sind, muss sich jemand mit Informationsquellen zum Thema befassen! Auf Grundlage der eigenen Bestandsdokumentation ist zu verfolgen, ob neue Schwachstellen in eingesetzten Produkten bekannt werden und welche Gegenmaßnahmen für die eigene OT-Landschaft möglich und wirksam sind.

Geringere Bedeutung sollte nach Einschätzung des Autors hingegen der immer noch beliebten Anti-Viren-(AV)-Software zugebilligt werden: Ein Verzicht auf Windows-PC und -Server mit ihrer überkomplexen Active-Directory-Infrastruktur und ein gut strukturiertes OT-Netz mit nachvollziehbaren Übergängen zwischen Teilnetzen sind letztlich wirksamer als ein oft nur vermeintlicher Schutz durch AV-Software.

Benutzermanagement und Authentifizierung

Zugriff auf Anwendungen im OT-Netz stellen oft auch den direkten Zugriff auf die Steuerung von Anlagen und Geräten dar. Selbstverständlich muss organisatorisch geregelt und technisch umgesetzt werden, wer (ggf. wann) was bedienen darf. Das gilt für den Zugriff vor Ort und erst recht für den Zugriff aus der Ferne (Remote-Access).

Praktisch finden sich allerorten noch immer Sammelaccounts für jeden, der gerade einmal etwas nachsehen muss, Anmeldungen als „administrator" mit dem Kennwort „123456" und aus dem Internet erreichbare Remote-Desktops in unklarer Konfiguration. Derlei unzeitgemäße „Arbeitserleichterungen" sollten dringend bereinigt und zumindest organisatorisch (besser auch technisch) gebannt werden.

Obsoleszenz-Management

Die Sorge um die Lebens- oder Nutzungsdauer von Produkten und Leistungen ist ein Thema, das die klassische IT nur am Rande beschäftigt. Die OT jedoch, also die IT rund um „konventionelle" Technik, hat viel kürzere Lebenszyklen als die Gebäude- und Sicherheitstechnik selbst, die mit und von der OT überwacht und gesteuert wird – das gilt für sichtbare und noch mehr für unsichtbare, in Geräten und Anlagen eingebaute Teile.

Die Verfügbarkeit von Technik und Informationen ist über den gesamten Lebenszyklus hinweg sicherzustellen: angefangen beim vertraglich vereinbarten, vom Lieferanten garantierten Support bis zu einem festgeschriebenen Zeitpunkt, über die darauf folgende „Updatefähigkeit" eines Produkts bis hin zu Mitarbeiter:inne:n, die wichtiges Wissen nicht mit in den wohlverdienten Ruhestand nehmen dürfen.

Tests und Audits

„Vertrauen ist gut, Kontrolle ist besser", sagte ein Mensch, dem man wahrlich nicht vertrauen konnte. Dennoch: Sei es der Bestand an Hard- und Software, irgendwelche Schutzmechanismen und Konfigurationen oder die Liste der berechtigten Benutzer – all das muss regelmäßig geprüft werden! Nur so lässt sich ein angestrebtes Niveau an Sicherheit halten oder gar verbessern. ■

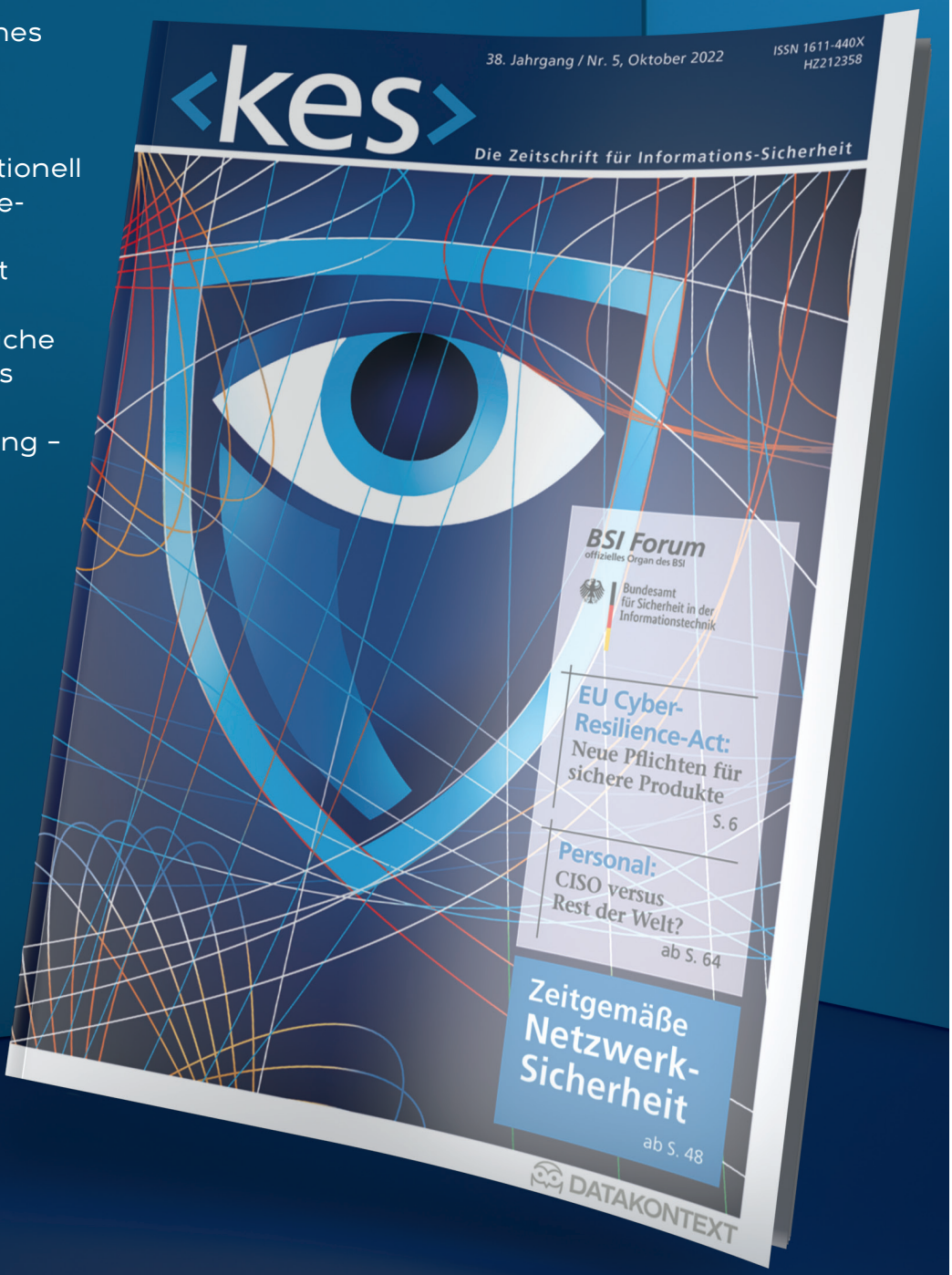
Dipl.-Inf. Werner Metterhausen (ISO-27001-Lead-Auditor) ist Sicherheitsberater bei VZM mit den Spezialgebieten RZ-Zertifizierung, Datenschutz und Informationssicherheit.

Literatur

[1] Stephen Mathezer, The Purdue Model and Best Practices for Secure ICS Architectures, in: Introduction to ICS Security Part 2, SANS Blog, Juli 2021, www.sans.org/blog/introduction-to-ics-security-part-2/

Need to know für CISO & Co.

- <kes> liefert strategisches Wissen für Security-Verantwortliche
- <kes> informiert redaktionell unabhängig zu Management und Technik der Informations-Sicherheit
- <kes> enthält das amtliche Organ des Bundesamts für Sicherheit in der Informationsverarbeitung - BSI-Forum
- <kes> kostet im Jahr weniger als zwei Beraterstunden



<kes>
Die Zeitschrift für Informations-Sicherheit

Für 159,00 € jährlich (inkl. MwSt. und Versandkosten) erhalten Sie alle zwei Monate eine gedruckte Ausgabe und für bis zu fünf Mitarbeiter am belieferten Standort Online-Zugriff auf alle aktuellen Beiträge sowie das <kes>-Archiv.

Online bestellen: datakontext.com/kes
oder per Mail: abo@kes.de

DATAKONTEXT