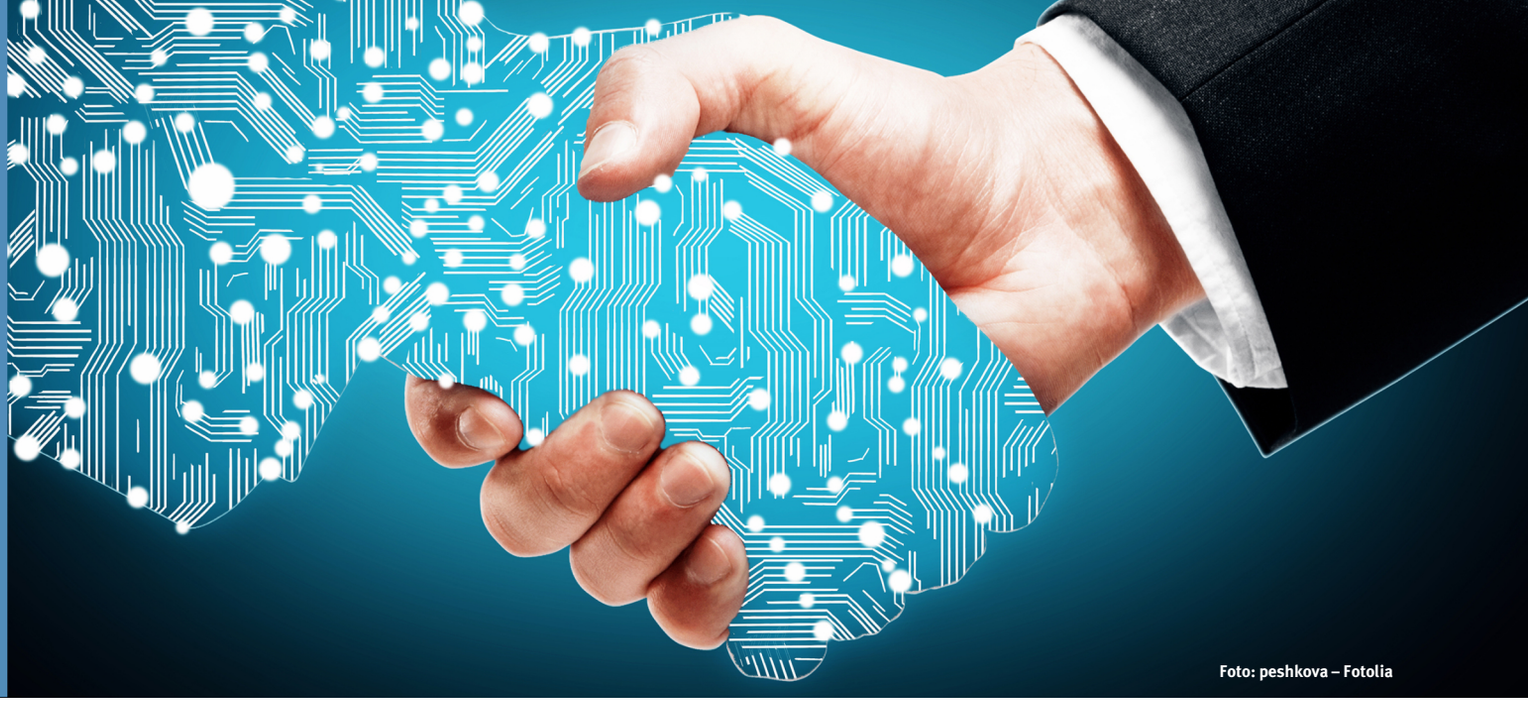

Foto: peshkova – Fotolia

Auf den Menschen kommt es an

IT-Sicherheit im Krankenhaus am Beispiel des UKSH

Mit geringem Aufwand und weitgehend anonym erfolgen immer häufiger Angriffe auf IT-Infrastrukturen im Gesundheitswesen. Gleichzeitig ist die „Dienstleistung Krankenhaus" nahezu vollständig von einer funktionierenden IT-Infrastruktur abhängig. Die Wirksamkeit getroffener Schutzmaßnahmen an identifizierten beziehungsweise potenziellen Schwachstellen kann mit Penetrationstests ermittelt werden. Hierbei wird die IT-Infrastruktur auf Verwundbarkeit überprüft und bewertet. Unberücksichtigt bei diesen Tests bleibt der Einfluss des Mitarbeiters, der mit den IT-Komponenten interagiert. Gerade aber das IT-Sicherheitsbewusstsein jedes Anwenders trägt oftmals entscheidend zur IT-Sicherheit des Gesamtsystems bei.

Unternehmen der Gesundheitsbranche, so auch das Universitätsklinikum Schleswig-Holstein (UKSH), stützen sich bei der Erfüllung ihrer Kernaufgaben auf eine umfangreiche IT-Organisation und -Infrastruktur. Nachfolgende Konzepte und Lösungen des UKSH sind für ein funktionierendes Krankenhaus heute unverzichtbar. Jedes Krankenhaus setzt dabei unterschiedliche Schwerpunkte und skaliert die IT-Strukturen entsprechend seiner Erfordernisse.

Kern einer funktionierenden IT sind die Mitarbeiter, sowohl Anwender als auch IT-Administratoren. Ob die IT-Mitarbeiter im Krankenhaus selbst, oder – wie am UKSH – in einer IT-Servicegesellschaft wirken, ist unerheblich. Entscheidend ist die Fachkompetenz der IT-Mitarbeiter. Der Betrieb von Servern und Netzwerk, das Management von PC, Notebooks und mobilen Devices gehört in die Hände von Profis. Ein sicherer und verlässlicher 24/7-Betrieb, zumindest der IT-Kernsysteme, muss an einem Krankenhaus gewährleistet werden. Der kontinuierliche Betrieb ist von zunehmenden Anforderungen aus klinischen und administrativen Bereichen flankiert. Immer umfangreicher sollen administrative und medizinische Daten erfasst und verarbeitet und Prozesse in einzelnen Bereichen, sowie übergreifend digital unterstützt werden. Insofern sind IT-Systeme in Krankenhäusern dynamische Systeme in stetigem Weiterentwicklungsprozess mit hoher Innovationsrate.

Zwei wesentliche Anforderungen werden an Klinikrechenzentren gestellt. Einerseits ist Ausfallsicherheit für patientenkritische Systeme im 24/7-Betrieb sicherzustellen, andererseits eine große Skalierbarkeit einzuplanen, die dem wachsenden Rechenleistungs- und Speicherplatzbedarf gerecht wird.

Ausfallsicherheit erreicht das UKSH durch redundante Strukturen. Die IT des UKSH betreibt ein zentrales TIER-III-Rechenzentrum. Zwei Serverräume in unterschiedlichen Brandabschnitten, sind mittels redundanter Strom- und Klima-Installationen versorgt und über redundante Datenverbindungen gekoppelt. Unterbrechungsfreie Stromversorgung und eine Notstromanlage sorgen für sichere Energiezufuhr. Umfassende Brandmelde-, Rauchabzugs- und Einbruchmeldeanlage sowie ein erweiterter Hochwasserschutz ergänzen die strukturellen Sicherungsmaßnahmen. Ausfälle der Klinik-IT durch Störungen oder während notwendiger Wartungsarbeiten können weitgehend vermieden werden, eine Verfügbarkeit von 99,98 % ist möglich. In einem anderen Gebäude sichert ein Desaster-Rechenzentrum zusätzlich den kontinuierlichen Betrieb. Zur Reduzierung von Latenzzeit-

problemen betreibt die IT des UKSH ein weiteres dezentrales Rechenzentrum in Kiel. Datenintensive Applikationen wie zum Beispiel die Anzeige von Röntgen- oder MRT-Serien laufen hierdurch performant. Neben der zentralen Rechenzentrum-Struktur werden am UKSH dezentrale Serverkomponenten nur noch für wenige klinische Spezialsysteme betrieben.

Alle zentral zu betreibenden Server werden, kostengünstig und bestens skalierbar, am UKSH durch eine Virtualisierungslösung gehostet, aktuell bereits über 800. Ausnahmen stellen solche Systeme dar, bei denen spezifische, zwingend vorausgesetzte Hardwarekomponenten nicht transparent einer virtuellen Instanz zugewiesen werden können.

An die (Langzeit-)Speicher eines Klinik-Rechenzentrum stellen sich erhöhte Anforderungen, für klinische Dokumente gilt eine bis zu 30 Jahre lange Aufbewahrungsfrist. Das UKSH begegnet diesen mit einem abgestuften Konzept, welches neben einem zentralen Speichernetzwerk (Storage-Area-Network, SAN), revisionssichere Langzeitspeicher und kontinuierliche Backups umfasst. Das zu managende Storagevolumen eines Klinikums der Größe des UKSH mit 500.000 Patienten und 13.000 Mitarbeitern erreicht so schnell PByte-Bereiche.

Neben zentralen Komponenten ist eine – möglichst „alle Ecken“ abdeckende – Netzwerkinfrastruktur mit Router, Switches, Firewalls, Accesspoints etc. durch die IT des Krankenhauses, am UKSH weit über 1.200 Komponenten, zu betreiben. Besonderes Augenmerk gilt dabei den Bereichen der Klinik, wo neben der „normalen“ Klinik-IT auch Geräte und Systeme aus dem Geltungsbereich der Medizinprodukte-Betreiberverordnung (MPBetreibV) in die Netzstruktur eingebunden werden. Hier sind durch die DIN EN 80001-1 besondere Sicherungsmaßnahmen notwendig. Eine enge Abstimmung mit der Medizintechnik ist zwingend.

Schließlich muss die IT eines Krankenhauses auch die Endgeräte (Stationsarbeitsplätze) bis hin zu Geräten am Point-of-Care (POC), zum Beispiel mobile Endgeräte, bereitstellen. Am UKSH werden derzeit über 6.000 PC- und weitere 600 mobile Arbeitsplätze, 2500 Drucker und circa 11.000 Telefone durch die IT betreut. Hinzu kommen vermehrt mobile Geräte aus dem „smart“-Bereich.

Wesentliche Anwendung eines Krankenhauses ist das zentrale Krankenhaus Informationssystem (KIS). In der Kernarbeitszeit registriert das UKSH mehr als 4.500 parallele Sessions. Weitere wesentliche Komponente für den Krankenhausbetrieb ist das zentrale Enterprise-Resource-Planning (ERP). Der gesamte administrative Workflow außerhalb der Patientenversorgung wird am UKSH in dieser Komponente abgewickelt. In einigen klinischen Bereichen sind spezifische medizinische Spezialsysteme erforderlich. Unter anderem Laborsysteme und klinische Fachsysteme zum Beispiel für die Pathologie. Sofern möglich werden diese am UKSH ebenfalls auf zentralen Servern gehostet.

Je größer die Zahl der notwendigen Systeme, desto komplexer die Vernetzung untereinander. Grundsätzlich ist die direkte Anbindung einzelner Systeme untereinander möglich, aber gegebenenfalls nicht mehr mit vertretbarem Aufwand zu betreuen. Der Einsatz eines zentralen Kommunikationsservers und die Nutzung gemeinsamer Verzeichnisdienste ermöglichen am UKSH den umfassenden Datenaustausch zwischen den vernetzten Systemen unter bestmöglicher Datensparsamkeit und -sicherheit.

Digitalisierung und ihre Folgen

Industrie 4.0, eigentlich die industrielle Produktion fokussierend, dringt in gleicher Weise in die Gesundheitsbranche ein und verändert vorhandene Prozesse und generiert neue Arbeitsabläufe. Neben Patientendaten, Untersuchungs- und Therapiedaten sind Behandlungspfade und Workflows digital abzubilden. In ausgewählten klinischen und administrativen Bereichen ist Prozesssteuerung bereits seit Längerem implementiert (z.B. Laborstraßen, Sterilisation, Essensversorgung). Am UKSH hält zunehmend unmittelbar die Patientenversorgung betreffende Prozesssteuerung Einzug. Ein Kommissionierungsautomat wird noch in 2017 die Medikation jedes einzelnen Patienten tagesaktuell, vollautomatisch aufbereiten. Die Einsatzplanung von Personal und das Management der Materialflüsse, die Belegung der Operationseinheiten sowie die Einsatzplanung der diagnostischen Einrichtungen erfolgen am UKSH digital.

Die Werkzeuge sind nicht nur zunehmend IT-gestützt, sondern verstärkt auch miteinander vernetzt. Über mobile Visitenwagen kann direkt über Schnittstellen in der zentralen, elektronischen Krankenakte dokumentiert werden. Mit Barcode-Scannern erfasste Materialverbräuche finden Eingang in die Krankenakte und lösen in der Materialverwaltung die Verbuchung

Uta Knöchel
Leiterin der
Stabsstelle Informationstechnologie
Campus Kiel und Lübeck
Universitätsklinikum Schleswig-Holstein

Dr. Armin Will
Stabsstelle Informationstechnologie
Campus Kiel und Lübeck
Universitätsklinikum Schleswig-Holstein

und bei Bedarf automatisiert die Nachbestellung bei Hersteller beziehungsweise Lieferant aus. Mit der online-Buchung einer Untersuchung oder Operation werden relevante Patienteninformationen (z.B. Allergien, Risikofaktoren, wesentliche Medikationen) übermittelt. Untersucher und Behandler stehen die Informationen der elektronischen Krankenakte unmittelbar am Behandlungssystem zur Verfügung. ▶

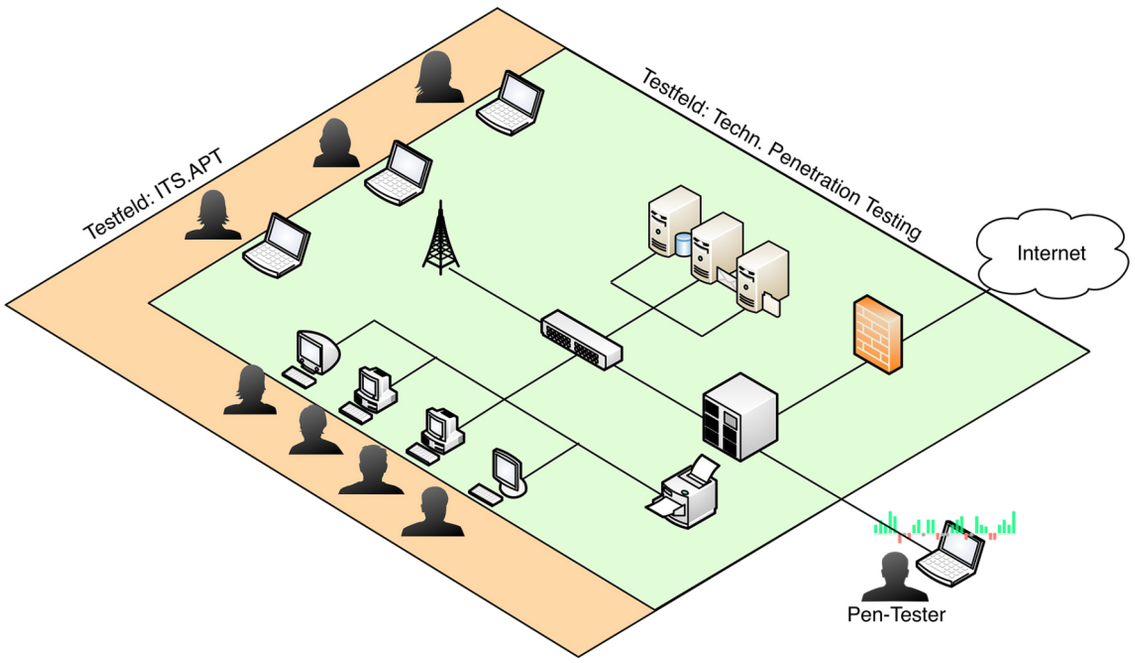

Abb.: Das Testfeld des klassischen Pentesting wird am UKSH um den Faktor Mensch erweitert.

Quelle: ITS.APT, Universität Bonn

Die transparente Bereitstellung notwendiger klinischer Daten am Ort des Geschehens sichert einen konsistenten Informationsstand. Die Verbesserung des Behandlungsworkflows kommt primär der Verbesserung der Behandlung des Einzelnen aber auch dem beteiligten Mitarbeiter zugute. Unnötige Aktensuche, fehlende Informationen, Reduzierung des administrativen Aufwands helfen den Mitarbeitern, sich auf den Patienten zu konzentrieren.

Mit der Digitalisierung einher geht eine steigende Abhängigkeit von der digitalen Infrastruktur. Der Ausfall oder die Störung wesentlicher Komponenten können erhebliche Auswirkungen – für Patienten eventuell letale Komplikationen – zur Folge haben. Zentral falsch erfasste Informationen sind an allen Stellen falsch und können fatale Auswirkungen haben. Mit steigender Komplexität der Vernetzung von Systemen und Daten können für den einzelnen Mitarbeiter Verständnis und Übersicht für die Struktur einer Prozesskette und die wechselseitigen Abhängigkeiten verschränkter Prozesse verloren gehen. Die Kommunikation mit Kostenträgern, niedergelassenen Ärzten, Nachbehandlungseinrichtungen, Konsiliarii und zunehmend mit Patienten überschreitet zudem die Krankenhausgrenzen. Die übertragenen Daten werden mehr, komplexer und sensibler (Datenschutz). Externe Zugänge zur Krankenhaus-IT zu Wartungs- und Servicezwecken werden von Herstellern und Dienstleistern vorausgesetzt.

Bedrohungslage

Das komplexe System Krankenhaus muss zur Sicherung seiner Betriebsbereitschaft verschiedensten Einflüssen begegnen. Den „Basis“-Risiken Stromausfall, Verbindungsstörungen/-Unterbrechungen und Fehlfunktionen beugt das UKSH mit seinem TIER-III-Rechenzentrum vor. Fehlfunktionen und Fehlbedienung werden durch Schulungen gezielt entgegengewirkt. Neben den „Basis“-Risiken werden zunehmend Risiken aus Vernetzung und Digitalisierung relevant: Die Krankenhaus-IT muss vor Cybergefahren geschützt werden.

Angriffe auf die Krankenhaus-IT erfolgen inzwischen täglich. 2015 stieg der Anteil um rund 36 % und hat sich – insbesondere durch Ransomware-Attacken in Deutschland – 2016 nochmals verdoppelt. Die Prognosen aller Beobachter der Szene rechnen für 2017 mit einer weiteren Steigerung und vor allem gezielteren Attacken auf einzelne Unternehmen. Ein erfolgreicher Angriff, ob nun als gezielte Cyberattacke oder als Kollateraleffekt einer Ransomwarewelle, kann immense Kosten auslösen. Das Anfang 2016 von einer Ransomware betroffene Lukaskrankenhaus Neuss bezifferte den Schaden auf rund 1,7 Millionen Euro. Solange durch Cyberangriffe keine Patienten zu Schaden kommen, leidet die Reputation eines betroffenen Krankenhauses nur wenig. Allerdings müssen wir uns bewusst sein, dass jeder Cyberangriff auch Patientengefährdung in Kauf nimmt.

Gegenmaßnahmen

Vor dem Hintergrund dieser Bedrohungslage ist jedes Krankenhaus gefordert, die Schwachstellen bei Betrieb und Nutzung von IT zu kennen und mit geeigneten Maßnahmen zu beheben beziehungsweise abzusichern. So hat sich das UKSH bei der Etablierung seines IT-Sicherheitskonzeptes an den Empfehlungen des BSI-Grundschutzes nach ISO 27001 orientiert. Es wurde ein Risikomanagement, angelehnt an den Leitfaden Risikoanalyse Krankenhaus-IT,

etabliert und bei der zunehmenden Anbindung von Medizingeräten werden die Anforderungen der DIN EN 80001-1 berücksichtigt. Das UKSH fordert von Herstellern von IT-Komponenten beziehungsweise IT–Systemen in Ausschreibungen eine Zertifizierung gemäß Common Criteria for Information Technology Security Evaluation (Stichwort: Security by design).

Generell ist eine ausführliche Bestandsaufnahme der vorhandenen IT-Infrastruktur am Anfang der Durchführung des IT-Sicherheitskonzeptes zu empfehlen und mittels eines kontinuierlichen Dokumentations- und Validierungsprozesses fortzuführen. Augenmerk ist dabei nicht nur auf das Vorhandensein von Komponenten, sondern auch auf die jeweils aktuelle Konfiguration und Nutzung zu legen. Komponenten und Funktionen sind auf ihre Notwendigkeit zu prüfen und zum Beispiel nicht benutze Ports zu schließen, ungenutzte Software zu deinstallieren und nicht notwendige Netzwerkdosen zu deaktivieren. Eine zentrale Dokumentation der Komponenten, ihrer jeweiligen Konfiguration und Funktionalitäten ermöglicht es, den Überblick zu behalten. Die Protokollierung von Zugriffen auf die Systeme gewährleistet die Nachverfolgbarkeit von Änderungen.

Der Einsatz von hochverfügbaren Komponenten, das permanente Monitoring des Systemzustands, regelmäßige Datensicherung und ausgefeilte Notfallpläne sind die Basis für den verantwortungsvollen Betrieb der IT am UKSH. Den technischen Instrumentarien und organisatorischen Maßnahmen sind zwingend Mitarbeiter mit der notwendigen Kompetenz zuzuordnen. Dabei können Normen beziehungsweise Standards zur Qualifizierung und Zertifizierung der technischen Mitarbeiter (z.B. ITIL) Rahmenbedingungen schaffen.

Entscheidend ist aber auch die Awareness des normalen Anwenders, seine Sensitivität gegenüber potenziellen Bedrohungen und Risiken. Mangelndem Sicherheitsbewusstsein (Passwort unter der Tastatur, Zugangssharing, Verzicht auf Abmelden oder Sperren des Accounts) ist durch Schulungen gezielt entgegen zu wirken. Das Bewusstsein der latenten Verwundbarkeit – gerade auch hinter der vermeintlich sicheren Firewall – ist zu schärfen, die Kenntnis über die aktuelle Bedrohungslage zu verbessern und bei jedem Anwender eine kontinuierliche Wachsamkeit zu erzeugen.

Vonseiten der Angreifer steht zunehmend der Anwender im Fokus, da dieser die vermeintlich größte Schwachstelle des Systems darstellt. Gezielt werden menschliche Eigenschaften wie Hilfsbereitschaft, Mitgefühl, Neugierde, Suche nach Anerkennung und Glück etc. angegriffen. Mittels gezielter Mails und Internetseiten erfolgt Sozial Engineering, um für den Zugriff auf IT-Systeme notwendige Information zu erhalten. Gemeinsam mit Psychologen, Juristen, Datenschützern, einem IT-Sicherheitsdienstleister und IT-Sicherheitsforschern führt das UKSH das vom BMBF geförderten Projekt ITS.APT durch. Hier wird ein Test-Verfahren entwickelt, mit dessen Hilfe die IT-Security-Awareness von Anwendern ermittelt werden kann (▶ Abb.). Auf Basis der Testergebnisse wird ein Schulungskonzept erstellt, welches die IT-Security-Awareness der Anwender verbessert und schließlich am UKSH validiert. Ausgangslage ist der klassische Schwachstellentest (Penetration Test), der zwar die organisatorischen Konzepte und die zugrunde liegende Infrastruktur adressiert, aber den Einfluss des mit den IT-Komponenten interagierenden Mitarbeiters nicht berücksichtigen kann. Das individuelle IT-Sicherheitsbewusstsein kann mit technischen Penetrationstests nicht erfasst oder bewertet werden. Erstmals wissenschaftlich fundiert und abgesichert wird am UKSH mit ITS.APT der Fokus auf den Anwender als potenzielle Schwachstelle gelegt. Das Testfeld des klassischen Penetrationtesting wird um den Faktor Mensch erweitert.

Auf der Basis einer fundierten Analyse bekannter Angriffsvektoren wurden Artefakte identifiziert, die mit Angriffen einhergehen und durch Menschen wahrnehmbar sind. Ausgewählte Mitarbeiter werden mit diesen Artefakten während ihrer normalen Tätigkeit am PC konfrontiert und ihre Reaktion auf die Artefakte dokumentiert. Aus den Ergebnissen der anonymisierten beziehungsweise pseudonymisierten Reaktionsprotokolle lassen sich der Grad der Awareness ableiten und gezielte Schulungsmaßnahmen zur Verbesserung konzipieren.

Fazit

IT-Sicherheit im Krankenhaus ist auch bei zunehmender Cyberkriminalität leistbar. Organisatorische und technische Lösungen stehen zur Verfügung, müssen jedoch konsequent und effektiv im Tagesgeschäft umgesetzt werden. Dies erfordert zusätzliche Investitionen, einerseits in Technik andererseits in Menschen. Krankenhausbudgets müssen hierfür entsprechende Positionen vorsehen. Nur qualifizierte Mitarbeiter sind in der Lage, die Konzepte und Techniken in der Praxis effektiv umzusetzen. Informierte Mitarbeiter, mit geschulter Sensitivität für Risikosituationen und Bedrohungen durch Cyber-Angriffe können diesen angemessen begegnen. Das Bewusstsein einer latenten Bedrohungslage und Verwundbarkeit tragen, der verantwortungsvolle Umgang mit IT-Komponenten unter kontinuierlicher Wachsamkeit jedes einzelnen Mitarbeiters können die Klinik-IT gegen Cyber-Angriffe härten. Somit werden informierte und sensibilisierte Mitarbeiter zur stärksten Waffe gegen Cyberangriffe und zu zentralen „Komponenten“ um die Vulnerabilität einer IT-Infrastruktur zu verringern. ■

Uta Knöchel
Dr. Armin Will

Stabsstelle Informationstechnologie
Universitätsklinikum Schleswig-Holstein
Ratzeburger Allee 160
23538 Lübeck

Uta.Knoechel@uksh.de
Armin.Will@uksh.de