© UKSH GESELLSCHAFT FÜR IT SERVICES MBH

Abbildung 1:
Blick in einen Kaltgang eines TIER-III-Rechenzentrums

IT-Sicherheit und der FAKTOR MENSCH

Das Gesundheitswesen zählt zu den meistbedrohten Sektoren von Cyberkriminalität und die Angriffe auf die IT-Infrastrukturen von Kliniken nehmen zu. Doch was gilt es zu tun, um dort IT-Sicherheit zu gewährleisten? Ein ausführlicher Überblick.

TEXT: ARMIN WILL

Angriffe auf IT-Infrastrukturen im Gesundheitswesen werden immer häufiger.[1] Erstens weil die Infrastruktur möglichst frei zugänglich sein soll (Lieferanten- und Dienstleister-Wartungszugänge, Patiententerminals etc.), zweitens weil Angriffe mit vergleichsweise geringem Aufwand übers Internet möglich und weitestgehend anonym sind. Andererseits ist die Dienstleistung Krankenhaus nahezu vollständig von funktionierender IT-Infrastruktur abhängig. Maßnahmen zur Absicherung der Infrastrukturen sind daher zwingend.

Um die Wirksamkeit getroffener Schutzmaßnahmen an bereits identifizierten bzw. potenziell noch nicht bekannten Schwachstellen zu verifizieren, sind Penetrationstests eine etablierte Methode. Hierbei wird die IT-Infrastruktur auf Verwundbarkeiten überprüft und bewertet. Penetration Testing wird durch sogenannte Pen-Tester, die im Auftrag des IT-Infrastruktur-Betreibers versuchen, im laufenden Betrieb in die Computersysteme einzudringen, umgesetzt. Gelingt dies dem Pen-Tester, wird ein System bzw. die entsprechende Infrastrukturkomponente als unsicher eingestuft und es sollten umgehend geeignete und angemessene Maßnahmen eingeleitet werden, um das Gesamtsystem auf ein neues Sicherheitsniveau zu bringen. Eine Wiederholung des Tests dient der Validierung der getroffenen Maßnahmen.

Unberücksichtigt bei diesen Tests bleibt der Einfluss des Mitarbeiters, der mit den IT-Komponenten interagiert. Der Faktor Mensch und sein individuelles IT-Sicherheitsbewusstsein können mit technischen Penetrationstest nicht erfasst oder bewertet werden. Gerade aber das IT-Sicherheitsbewusstsein jedes Anwenders trägt, gegebenenfalls sogar entscheidend, zur IT-Sicherheit des Gesamtsystems bei. Unzureichendes Wissen um die eingesetzte Technologie, mögliche Gefahren und resultierende Folgeschäden bei IT-Infrastruktur-Anwendern stellen ein Risiko für die IT-Sicherheit dar. Dieses mangelnde IT-Sicherheitsbewusstsein machen sich Angreifer, zunehmend gezielt, zunutze. Trojanische Pferde und Social Engineering – insbesondere Phishing – sind prominente Beispiele, wie mangelhaftes IT-Sicherheitsbewusstsein eines Benutzers spezifisch ausgenutzt wird.

Bereits 2011 hat die Bundesregierung unter Federführung des Bundesinnenministeriums die Cybersicherheitsstrategie für Deutschland beschlossen.[2] In der Folge wurden etliche Maßnahmen zur Umsetzung der Strategie initiiert. Unter anderem wurden in neun Sektoren Kritische Infrastrukturen identifiziert, die sich durch das IT-Sicherheitsgesetz seit Dezember 2014 mit konkreten Anforderungen konfrontiert sehen.[3] Für einige Sektoren liegen die Kriterien zur Zuordnung von Betreibern zu den KRITIS vor, für den Sektor Gesundheit werden diese Kriterien aktuell definiert. Auch wenn bis zum Ende des Jahres nicht jedes Krankenhaus als KRITIS eingestuft wird: IT-Sicherheit gilt für alle.

Mit dem Förderprogramm „IT-Sicherheit für Kritische Infrastrukturen“[4] des Bundesministeriums für Bildung und Forschung (BMBF) werden gezielt sektorspezifische Anforderungen identifiziert, technische und organisatorische Konzepte entwickelt, um Kritische Infrastrukturen gegen Cybergefahren abzusichern.

Mit dem BMBF-Projekt ITS.APT (IT-Security Awareness Penetration Testing) wird am Universitätsklinikum Schleswig-Holstein (UKSH) der Fokus auf den Faktor Mensch als potenzielle Schwachstelle der IT-Infrastruktur gelenkt. Sowohl das Erfassen der individuellen IT-Security-Awareness wie auch – auf Basis der erhobenen Informationen gezielt zu fokussierende – Schulungen zur Stärkung des IT-Sicherheitsbewusstseins sowie anschließende Validierung der Schulungsmaßnahmen erfolgen im Rahmen von ITS.APT am UKSH.

»Der Faktor Mensch und sein individuelles Sicherheitsbewusstsein können mit einem technischen Penetrationstest nicht erfasst werden.«

Strukturen und Werkzeuge

Unternehmen der Gesundheitsbranche stützen sich bei der Erfüllung ihrer Kernaufgaben auf eine umfangreiche IT-Organisation und -Infrastruktur. Jedes Krankenhaus setzt dabei unterschiedliche Schwerpunkte und skaliert die IT-Strukturen entsprechend der Erfordernisse. In Grundzügen sind die nachfolgend skizzierten Elemente für ein funktionierendes Krankenhaus heute unverzichtbar. >

Kern einer funktionierenden IT-Infrastruktur sind Mitarbeiter. Ob diese nun durch das Krankenhaus selbst oder – wie zunehmend zu beobachten – von einer IT-Servicegesellschaft bereitgestellt werden, ist unerheblich. Entscheidend ist die Fachkompetenz der Mitarbeiter. Der Betrieb von Servern und Netzwerk, das Management von PC, Notebooks und mobilen Devices gehört in die Hände von Profis. Die Zeiten, als der Assistenzarzt der Fachabteilung den lokalen Server mal eben noch betreute, sind definitiv vorbei. Ein sicherer und verlässlicher IT-Einsatz über 24 Stunden am Tag an sieben Tagen in der Woche (24/7-Betrieb) muss an einem Krankenhaus (zumindest für die Kernsysteme) gewährleistet werden. Der kontinuierliche Betrieb der Systeme ist von kontinuierlicher Ausweitung der Anforderungen aus den klinischen und administrativen Bereichen flankiert. Immer umfangreicher sollen Daten erfasst und verarbeitet werden, Prozesse in einzelnen Bereichen, und übergreifend digital unterstützt werden. Insofern sind IT-Systeme in Krankenhäusern dynamische Systeme, die einem stetigen Weiterentwicklungsprozess unterliegen.

»IT-Systeme in Krankenhäusern sind dynamische Systeme, die einem stetigen Weiterentwicklungsprozess unterliegen.«

Die Anforderungen an Klinikrechenzentren sind nicht zu unterschätzen. Einerseits ist Ausfallsicherheit für den 24/7-Betrieb – zumindest für patientenkritische Systeme – sicherzustellen, andererseits eine recht große Skalierbarkeit einzuplanen, da mit zunehmender Laufzeit der Systeme sowohl Rechenleistung als auch Speicherplatzbedarf wachsen.

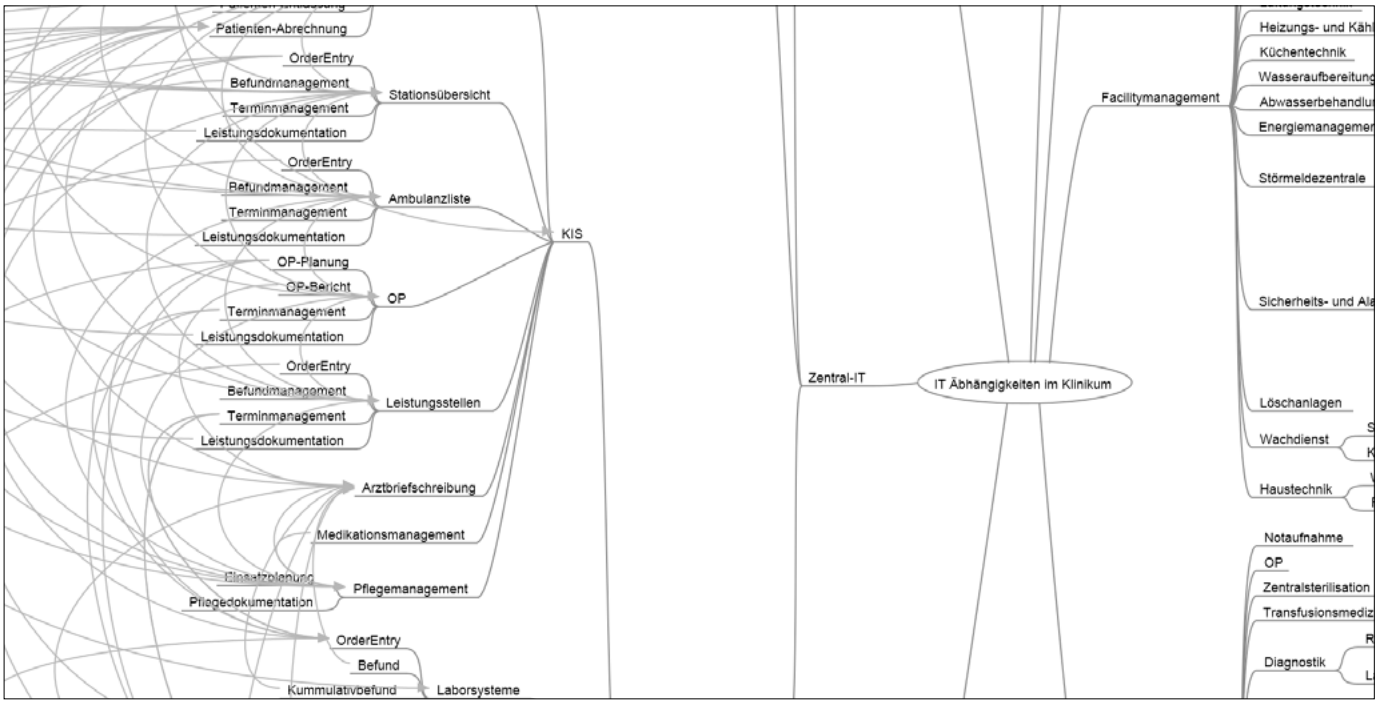
Ausfallsicherheit wird durch redundante Strukturen eines Rechenzentrums (RZ) erreicht. Mindestens zwei Serverräume in zwei unterschiedlichen Brandabschnitten sind idealerweise mittels redundanter Strom- und Klima-Installationen versorgt und über redundante Datenverbindungen gekoppelt. Unterbrechungsfreie Stromversorgung und gegebenenfalls eine eigene Notstromanlage sorgen für sichere Energiezufuhr. Umfassende Brandmelde-, Rauchabzugs- und Einbruchmeldeanlagen sowie gegebenenfalls erweiterter Hochwasserschutz ergänzen die strukturellen Sicherungsmaßnahmen für ein klinisches RZ. Ausfälle der Klinik-IT durch Störungen oder notwendige Wartungsarbeiten werden unter diesen Bedingungen weitestgehend vermieden, die Verfügbarkeit liegt bei 99,98 Prozent und Klinikbetreiber sollten für ihre Klinik-IT die Nutzung eines solchen TIER-III-Rechenzentrums anstreben.

Ein geflügeltes Wort in der Klinik-IT lautet „Storage ist nie genug da“. Insbesondere durch, im Vergleich zu anderen Bereichen, deutlich längere – für klinische Dokumente bis zu 30 Jahre – Aufbewahrungsfristen werden an die (Langzeit-)Speicher eines Klinik-RZ hohe Anforderungen gestellt. Ein abgestuftes Konzept umfasst neben einem zentralen Speichernetzwerk (Storage-Area-Network, SAN), verschiedene Network Attached Storage (NAS)-Systeme, revisionssichere Langzeitspeicher und kontinuierliche Back-ups. Das zu managende Storagevolumen eines Klinikums in der Größe des UKSH kommt schnell in PByte-Bereiche.

Neben der zentralen RZ-Struktur können im Einzelfall dezentrale Serverkomponenten notwendig sein, insbesondere bei daten- und kommunikationsintensiven Applikationen. In der Radiologie stellen z.B. MRT- und Röntgen-Serien enorme Anforderungen an die Netzwerk-Übertragungskapazität. Bei ausschließlich zentraler Speicherung kommt es gegebenenfalls schnell zu Engpässen. Ein dedizierter Server mit Kurzzeitspeicher (bis zu sechs Monate haben sich bewährt) kann die Latenzprobleme beim Aufruf der großen Datenmenge abfedern.

Neben zentralen Komponenten ist, je nach baulicher Struktur der Klinik unterschiedlich umfangreich ausgeprägt, eine – möglichst „alle Ecken“ abdeckende – Netzwerkinfrastruktur mit Router, Switches, Firewalls, Access-Points etc. durch die IT des Krankenhauses 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.

Kostengünstig und am besten skalierbar hat sich Virtualisierung



im Serverbereich inzwischen durchgesetzt, sodass im Allgemeinen die meisten Server als virtualisierte Server zentral gehostet werden. Ausnahmen stellen solche Geräte dar, bei denen spezifische, zwingend vorausgesetzte Hardwarekomponenten nicht transparent einer virtuellen Instanz zugewiesen werden können.

Schließlich muss die IT eines Krankenhauses auch die Endgeräte (Stationsarbeitsplätze) bis hin zu Geräten am Point-of-Care (POC), z.B. mobile Endgeräte, bereitstellen. Auch hierbei kann Virtualisierung die Anforderungen an die Endgeräte minimieren.

Wesentliche Anwendung eines Krankenhauses ist das zentrale Krankenhausinformationssystem (KIS). In der Kernarbeitszeit registriert das UKSH mehr als 3 000 parallele Sessions. Eine weitere wesentliche Komponente für den Krankenhausbetrieb ist das zentrale Enterprise-Resource-Planning (ERP). Der gesamte administrative Workflow außerhalb der Patientenversorgung wird hier abgewickelt. Es gibt Komplettlösungen, die sowohl klinische als auch administrative Prozesse abbilden. Selbst die größten Komplettpakete sind nicht in der Lage, alle – vor allem klinische – Anforderungen abzubilden. In vielen Kliniken, Ambulanzen und Instituten kommen daher spezifische klinische und administrative Spezialsysteme zum Einsatz, unter anderem Laborsysteme und klinische Fachsysteme. Sofern möglich werden diese auf zentralen Servern gehostet. In Ausnahmefällen müssen allerdings lokale Server betrieben werden.

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

Digitalisierung

Daten, sowohl administrativ als auch klinisch, sind zunehmend digital. Industrie 4.0, Buzzword der industriellen Produktion, greift in gleicher Weise – vielleicht noch tiefgehender – in der Gesundheitsbranche in vorhandene Prozesse ein und generiert neue, bisher nicht notwendige Arbeitsabläufe. Neben Patientendaten, Untersuchungs- und Therapiedaten sind Behandlungspfade und Workflows digital abgebildet oder zur Einsicht hinterlegt. In ausgewählten Bereichen ist bereits seit Längerem Prozesssteuerung implementiert (z.B. Laborstraßen, Sterilisation, Essensversorgung). Auch unmittelbar die Patientenversorgung betreffende Prozesssteuerung hält zunehmend Einzug in Kliniken. Kommissionierungsautomaten bereiten die Medikation jedes einzelnen Patienten tagesaktuell, vollautomatisch auf. Einsatzplanung von Personal und das Management der Materialflüsse, die Belegung der Operationseinheiten sowie die Einsatzplanung der diagnostischen Einrichtungen erfolgen digital. >

Abbildung 2: *Ausschnitt aus dem Beziehungsgeflecht einer Krankenhaus-IT-Landschaft*

»Zu den „Basisrisiken“ gesellen sich zunehmend Risiken aus Vernetzung und Digitalisierung.«

Die Werkzeuge sind nicht nur zunehmend IT-gestützt, sondern zunehmend untereinander vernetzt. Mit mobilen Endgeräten erfasste Vitalparameter werden über Schnittstellen in der zentralen, elektronischen Krankenakte dokumentiert. Die mobil erfassten Materialverbräuche finden Eingang in die Krankenakte und lösen in der Materialverwaltung entsprechende Verbuchungen, bei Bedarf automatisierte Nachbestellungen bei Hersteller bzw. 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 Behandlungsgerät zur Verfügung.

Ziel der Digitalisierung und Vernetzung ist die Optimierung der Behandlung des Patienten. Die transparente Bereitstellung notwendiger klinischer Daten am Ort des Geschehens sichert einen konsistenten Informationsstand. Die Verbesserung des Behandlungsworkflows durch IT-Einsatz kommt primär der Verbesserung der Behandlung des Einzelnen sowie dem beteiligten Mitarbeiter durch optimierte Arbeitsabläufe zugute. Unnötige Aktensuche, fehlende Informationen, Reduzierung des administrativen Aufwands ohne unmittelbaren Bezug zum Patienten helfen den Mitarbeitern, sich auf den Patienten zu konzentrieren.

Mit der Digitalisierung geht aber eine steigende Abhängigkeit von der digitalen Infrastruktur einher. Der Ausfall oder die Störung wesentlicher Komponenten der IT-Infrastruktur können erhebliche Auswirkungen – für Patienten eventuell letale Komplikationen – zur Folge haben. An einer Stelle falsch erfasste Informationen sind an allen anderen Stellen ebenfalls falsch und können fatale Folgen nach sich ziehen.

Mit steigender Komplexität der Vernetzung von Systemen und Daten gehen für den einzelnen Mitarbeiter Verständnis und Übersicht für Zusammenhänge verloren. Die Anteile einer Prozesskette und ihre Abhängigkeiten untereinander sind dem Einzelnen häufig nicht mehr transparent. Noch mehr geht das Verständnis und die Übersicht verloren, wenn verschiedene Prozessketten untereinander in Abhängigkeit stehen.

Dabei endet die Vernetzung bekanntermaßen nicht an der Krankenhausgrenze. Die Kommunikation mit den Kostenträgern, niedergelassenen Ärzten, Nachbehandlungseinrichtungen, Konsiliarii und zunehmend mit den Patienten selber, wird immer umfangreicher. Dabei werden die übertragenen Daten komplexer und sensibler (Datenschutz). Zu Wartungs- und Servicezwecken wird von Herstellern und Dienstleistern ein externer Zugang zur Krankenhaus-IT-Infrastruktur erwünscht, gefordert bzw. vorausgesetzt.

Im Ganzen ergibt sich ein nahezu unüberschaubares Geflecht von Beziehungen und Abhängigkeiten. Abbildung 2 gibt einen stark reduzierten Ausschnitt einer „Netzkarte“ einer Krankenhaus-IT-Landschaft wieder.

Bedrohungslage

Das komplexe System Krankenhaus braucht verlässliche Verfahren und Methoden zur Sicherung der Betriebsbereitschaft seiner IT-Infrastruktur und damit seiner Leistungsfähigkeit.

Verschiedenste Einflüsse können die Betriebsbereitschaft der IT-Infrastruktur gefährden: Stromausfall, Verbindungsstörungen / Unterbrechungen, Fehlfunktionen, Programmierfehler. Diesen „Basisrisiken“ kann mit bewährten Gegenmaßnahmen entgegengetreten bzw. vorgebeugt werden. TIER III RZ können mit entsprechender Notstromversorgung und redundanten Anbindungen Betriebsbereitschaftszeiten von 99,98 Prozent erzielen. Fehlfunktionen und Fehlbedienung kann durch Schulungen gezielt entgegengewirkt werden, Programmierfehler sind zwar nicht vermeidbar, können aber mit einem konsequenten Qualitätsmanagement bereits bei der Konzeption reduziert werden.

Doch wie sieht es mit Risiken aus, die sich durch die notwendige Vernetzung der IT-Infrastruktur mit dem Internet, mit Herstellern, Lieferanten etc. ergeben? Wie steht es mit Risiken bei Nutzung von Datenträgern mit Patienteninformationen, von Kollegen zugesandt oder vom Patienten mitgebracht?

Zu den Basisrisiken gesellen sich zunehmend Risiken aus Vernetzung und Digitalisierung. Was bedeutet Cyberkriminalität für die Krankenhaus-IT?

Für Angriffe auf die IT-Infrastrukturen im Gesundheitswesen sind die Voraussetzungen nahezu ideal. Fast ausnahmslos sind die Protagonisten der Gesundheitsversorgung gezwungen, elektronisch erreichbar zu sein. Seit Jahren erfolgt die Abrechnung

von Krankenhausleistungen vollständig per elektronischem Datenaustausch (§ 301). Zunehmend erwarten Dienstleister und Lieferanten Zugriff auf die von ihnen gelieferten Systeme zu Wartungs- und Servicezwecken, teilweise wird in Wartungsverträge freier Zugang gefordert, oder verlangt, dass Systeme „nach Hause telefonieren" bzw. Daten in die Cloud laden können. Zudem haben Krankenhäuser unter permanentem Konkurrenzdruck ein großes Interesse, in der Öffentlichkeit wahrgenommen zu werden, ihren Patienten Informationen über die angebotenen Dienstleistungen zur Verfügung zu stellen und betreiben umfangreiche Internetpräsenzen und Patientenportale. Solche Schnittstellen sind zwangsläufig nach außen, oft direkt im Internet, exponiert.

Der Aufwand für einen Cyberangriff über das Internet ist überschaubar. In einschlägigen Kreisen werden fertige Toolboxen für die Erstellung von Cyberangriffen angeboten. Im sogenannten Darknet können spezifisch angepasste Angriffe als Dienstleistung gebucht werden.[5] Angreifer bleiben dabei weitestgehend anonym. Im Vergleich zu physischen Angriffen vor Ort kann der Angreifer seine Identität über das Medium Internet leichter verschleiern. Ob Angriffe gezielt, seit 2015 zunehmend zu beobachten, oder im Rahmen massenhafter Cyberattacken erfolgen: Krankenhäuser müssen – im eigenen Interesse, vor allem zum Schutz ihrer Patienten – Vorkehrungen gegen durch Cyberattacken verursachte Systemausfälle treffen. Hierbei scheint Deutschland ein besonders lukratives Ziel zu sein. Laut einer aktuellen Studie des Kaspersky Lab stand Deutschland im Zeitraum zwischen April 2015 und März 2016 am stärksten unter Beschuss. So stieg der Anteil der angegriffenen Anwender um 35,65 Prozent gegenüber dem Vergleichszeitraum 2014-2015.[6] Zudem verdoppelte sich der Anteil der Attacken auf Unternehmen von 6,8 Prozent auf 13,13 Prozent.[7]

Obwohl die Schlagzeilen produzierende Ransomware Krankenhäuser nicht gezielt attackierte, muss doch konstatiert werden, dass 2015 >

die Zahl an Cyberangriffen auf das Gesundheitswesen gegenüber 2014 deutlich zugenommen hat. Hintergrund ist, dass medizinische Daten für Angreifer lukrativer sind als z.B. Kreditkartendaten. Während kompromittierte Kreditkartendaten schnell und effizient „neutralisiert" werden können, sind medizinische Informationen von Patienten meist permanent und in vielen Fällen nur schwer bzw. mit hohem Aufwand wiederherzustellen. Laut dem IBM X-Force Threat Intelligence Report 2016 müssen betroffene Organisationen für jeden kompromittierten Patientendatensatz 363 US-Dollar aufwenden, während durchschnittlich andere Arten von Datensätzen lediglich Kosten in Höhe von 154 US-Dollar nach sich ziehen. Dies spiegelt sich auch beim illegalen Handel gestohlener Daten wider: Während abgefischte Kreditkartennummern zu Schleuderpreisen verramscht werden, werden für gestohlene Patientendaten bis zu 50 US-Dollar pro Datensatz aufgerufen. Der Cybercrime-Markt orientiert sich um. Allein in den USA sind nach einer Studie des Ponemon Institute[8] Einrichtungen des Gesundheitswesens im Schnitt einmal pro Monat einer Cyberattacke ausgesetzt. Dabei geht es (noch) vornehmlich um Datendiebstahl, aber die Tatsache, dass etliche patientenversorgende Systeme ungenügend gegen Attacken abgesichert sind, lässt befürchten, dass konkrete Angriffe auf Patienten, zumindest als Drohkulisse, interessant werden.

Am 25.02.2016 zitierte die Ärzte-Zeitung eine Untersuchung der Firma Gemalto.[9] Nach Analyse von 1673 weltweiten öffentlich bekannt gewordenen Hackerangriffen wurden insgesamt über 700 Millionen Datensätze kompromittiert bzw. entwendet. Unternehmen des Gesundheitswesens waren zu 19 Prozent betroffen.

Auch wenn Krankenhäuser nicht gezielt Cyberattacken ausgesetzt sind, können bei einem erfolgreichen Angriff dennoch immense Kosten entstehen. So musste das Lukaskrankenhaus Neuss laut kma einen Schaden in Höhe von 1,7 Millionen Euro feststellen.[10] Auch wenn der Schaden durch das Nachholen der ausgefallenen Operationen auf rund 900 000 Euro reduziert werden konnte, wird doch deutlich: Erfolgreiche Cyberattacken verursachen immense Kosten. Solange bei Angriffen keine Patienten zu Schaden kommen, leidet die Reputation eines betroffenen Krankenhauses nur wenig, aber ausschließen, dass erfolgreiche Cyberangriffe zu Patientengefährdungen führen, kann niemand.

Schwachstellen

Vor dem Hintergrund dieser Bedrohungslage ist ein Krankenhaus gefordert, die Schwachstellen bei Betrieb und Nutzung von IT zu kennen und mit geeigneten Maßnahmen zu beheben bzw. abzusichern.

Nachfolgend sollen einige der bekanntesten potenziellen Schwachstellen betrachtet werden.

Organisation

Auch wenn das Krankenhaus seine IT nicht selbst betreibt, bleibt die Verantwortung für den Krankenhausbetrieb, gerade auch die Sicherstellung der Funktionsfähigkeit der IT als zentraler Komponente für die Erbringung der Dienstleistung Gesundheitsversorgung, in der Verantwortung der Geschäftsführung. Hat die Geschäftsführung jedoch keine IT-Sicherheitsziele definiert, sind die Verantwortlichen für Einhaltung und Erreichung der Ziele nicht klar bestimmt, liegt organisatorisches Versagen vor, das vor dem Hintergrund des IT-Sicherheitsgesetzes neben empfindlichen Bußgeldern auch Schadenersatzforderungen nach sich ziehen kann. Dementsprechend sollte die Geschäftsführung dafür sorgen, dass die zu beteiligenden Bereiche bzw. Personen mittels stringenter Prozessdefinitionen einerseits über eindeutige Verfahrensbeschreibungen und Handlungsanweisungen verfügen, andererseits die notwendigen Kompetenzen und Verantwortlichkeiten für alle transparent festgelegt sind. Ein dem wachsenden IT-Umfeld stetig anzupassendes Eskalations- und Risikomanagement sind zu etablieren und müssen Eingang in das Sicherheitskonzept finden. Nur bei gründlicher Analyse und Dokumentation können fehlende oder unzureichende Strukturen (Ansprechpartner und Zuständigkeiten, alternative Kommunikationswege, Vertretungsregelungen, Kompetenzlücken bzw. Konflikte, Eskalationspfade und Notfallpläne) identifiziert und zielgerichtet behoben werden.

Technik

Ein wesentlicher Teil bei Einführung und Durchführung eines IT-Sicherheitskonzeptes ist die ausführliche Bestandsaufnahme vorhandener Technik. Es ist erschreckend, wie viele veraltete, ungepatchte Systeme in Betrieb und vielfach auch im Netzwerk eingebunden sind. Die Gründe hierfür sind vielschichtig. Es gibt medizintechnische Systeme, die aufgrund von Zulassungsbestimmungen nicht ohne Weiteres mit einem Update versorgt werden dürfen. Wenn dies der Betreiber dennoch macht, riskiert er, das Gerät außerhalb der Zulassung zu betreiben und damit die vollständige

Verantwortung bei Fehlfunktion zu übernehmen, Stichwort Eigenherstellung. Neben veralteten Systemen (z.B. Windows XP) sind aber auch immer wieder fehlende Updates, nicht nur an PCs, anzutreffen, z.B. anfällige Firmware (z.B. Router). Weitere Schwachstellen werden durch fehlende Deinstallation nicht mehr genutzter Systeme und Programme eröffnet. Bei genutzten Programmen und Systemen sind immer wieder unzureichende Konfigurationen zu finden. Offene, nicht notwendige Ports, fehlender bzw. nicht aktueller Virenschutz, unregelmäßige und fehlende Firewall-Überprüfung und allzu oft einfache Adminpasswörter, unvollständige Rollen- und Profilzuordnung erleichtern Angreifern den Zutritt in IT-Systeme. Zudem ist die IT-Landschaft teilweise bereits so unübersichtlich, dass eventuell in dem einen oder anderen Büro ein seit Jahren zwar lokal genutzter, aber nicht gepflegter Server sein Dasein fristet. Aus der zunehmenden Digitalisierung der Prozesse ergibt sich eine erhöhte Komplexität der Vernetzung, mit neuen Wechselwirkungen und Abhängigkeiten. Multiple Komponenten mit unterschiedlichsten Sicherheitsmechanismen sind über mehrere Segmente miteinander vernetzt und es erfolgt häufig nur unzureichendes Monitoring genehmigter Zugriffe.

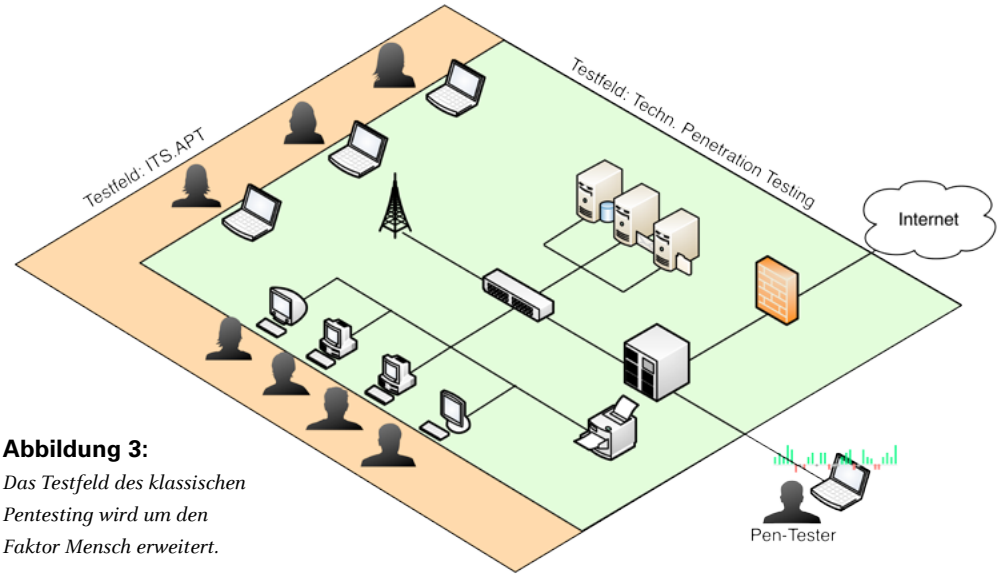


Abbildung 3:
Das Testfeld des klassischen Pentesting wird um den Faktor Mensch erweitert.

Mensch

Schließlich bleibt noch der vermeintlich größte Schwachpunkt bei der Einhaltung von IT-Sicherheit zu betrachten: die Schwachstelle Mensch.

Neben fehlendem Sicherheitsbewusstsein (Passwort unter der Tastatur, Zugangssharing, Verzicht auf Abmelden oder Sperren des Accounts) stellen das (blinde) Vertrauen in die Technik (Mail-Filter, Virenschutz, Firewall) und vor allem in die eigenen Fähigkeiten (Verzicht auf Verifikation, Verzicht auf regelmäßige Schulungen) häufig kritische IT-Sicherheitslücken dar.

Gezielt angegriffen werden menschliche „Schwächen" wie Hilfsbereitschaft, Mitgefühl, Neugierde, Suche nach Anerkennung und Glück etc. Mittels gezielter Mails und Internetseiten erfolgt das sogenannte Social Engineering, um für den Zugriff auf IT-Systeme notwendige Information zu erhalten. Hier sollte sich jeder Anwender bewusst sein, dass er vor einer solchen Attacke nicht gefeit ist. Niemand sollte sich einbilden, für Angreifer kein lohnendes Opfer zu sein: Auch wenn „nur" der Rechner des Pförtners kompromittiert wird, von dort in die gesamte IT-Landschaft ist es für einen Angreifer nur noch „ein Klick".

Gegenmaßnahmen

Bei aller Bedrohung und bei allen bestehenden oder potenziellen Schwachstellen sind Krankenhäuser aber nicht hilflos.

In verschiedenen Gesetzen, Verordnungen, Normen und Empfehlungen sind für Krankenhäuser Rahmenanforderungen definiert und – teilweise zwingend, teilweise mit empfehlendem Charakter – zur Verwendung bereitgestellt. Orientiert sich ein Krankenhaus bei der Etablierung seines IT-Sicherheitskonzeptes an den Empfehlungen des BSI-Grundschutzes nach ISO 2700x, etabliert ein Risikomanagement angelehnt an den Leitfaden Risikoanalyse Krankenhaus-IT, setzt die Anforderungen der DIN EN 80001-1 in seinem IT-Netz um, sind bereits viele kritische Schwachstellen adressiert. Wenn zudem Hersteller ihre IT-Komponenten und Systeme vermehrt einer „Common Criteria for Information Technology Security Evaluation" unterziehen und sich entsprechend zertifizieren lassen (Stichwort: Security by designe), kann weiterer Zugewinn an Cybersicherheit für die Betreiber dieser Komponenten gewonnen werden.

Der Einsatz von hochverfügbaren Komponenten, ein permanentes Monitoring des Systemzustands, regelmäßige Datensicherung und ausgefeilte Notfallpläne sind die Basis für den verantwortungsvollen Betrieb einer Krankenhaus-IT-Infrastruktur, eingebettet in ein effektives – möglichst schlankes – IT-Sicherheitskonzept. Den technischen Instrumentarien und organisatorischen

»IT-Systeme in Krankenhäusern sind dynamische Systeme, die einem stetigen Weiterentwicklungsprozess unterliegen.«

Maßnahmen müssen zwingend Mitarbeiter mit notwendiger Kompetenz zugeordnet werden. Dabei stehen ebenfalls Normen bzw. Standards zur Qualifizierung und Zertifizierung der Mitarbeiter zur Verfügung (z.B. ITIL). Allerdings steht hier meist nur der technische Mitarbeiter im Fokus. Dieser ist zwar an zentraler Stelle wesentlich, aber – mit Blick auf Cybersicherheit – durchaus nicht allein entscheidend.

Entscheidend ist die Awareness des normalen Anwenders, seine Sensitivität gegenüber potenziellen Bedrohungen und Risiken. 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 Mensch, als Anwender, im Fokus, da dieser die vermeintlich größte Schwachstelle des Systems darstellt.

Das Projekt ITS.APT

Gemeinsam mit Psychologen[11], Juristen[12], Datenschützern[13], einem IT-Sicherheitsdienstleister[14] und IT-Sicherheitsforschern[15] verfolgt das UKSH in dem vom BMBF geförderten Projekt ITS.APT drei Ziele. Es wird ein Testverfahren entwickelt, mit dessen Hilfe die IT-Security-Awareness von Anwendern ermittelt werden kann. Auf der Basis der Testergebnisse wird ein Schulungskonzept erstellt, welches die IT-Security-Awareness der Anwender verbessert und schließlich wird dieses Konzept am UKSH validiert.

Ausgangslage ist der klassische Pentest. Gute Pen-Tester unterziehen zunächst die getroffenen organisatorischen Maßnahmen einer differenzierten Prüfung und wenden sich anschließend der IT-Infrastruktur zu. Das Penetration Testing wird idealerweise durch externe Dienstleister vorgenommen, da es internen Überprüfungen häufig nicht gelingt, einen unabhängigen Blick „von außen“ zu bekommen. Die beim Pen-Test als unsicher eingestuften System- bzw. Infrastrukturkomponenten sollten umgehend mit angemessenen und geeigneten Maßnahmen auf ein höheres Sicherheitsniveau gebracht und das Ergebnis validiert werden.

Trotz aller technischen Raffinesse und persönlichen Erfahrung des Pen-Testers bleibt bei solchen Tests der Einfluss des mit den IT-Komponenten interagierenden Mitarbeiters unberücksichtigt. Das individuelle IT-Sicherheitsbewusstsein kann mit technischen Penetrationstests nicht erfasst oder bewertet werden. Das IT-Sicherheitsbewusstsein jedes Anwenders – nicht nur der IT-Mitarbeiter – trägt aber, ggf. sogar entscheidend, zur IT-Sicherheit des Gesamtsystems bei. Fehlendes Wissen über die eingesetzte Technologie, potentielle Gefahren und Folgeschäden stellen ein Risiko für die IT-Sicherheit dar.

Angreifer machen sich mangelndes IT-Sicherheitsbewusstsein auf vielfältige und differenzierte Weise zu Nutze. Bekannte Beispiele sind Trojanische Pferde und Social-Engineering – insbesondere Phishing – mit denen das mangelhaftes IT-Sicherheitsbewusstsein eines Benutzers gezielt ausgenutzt wird. Erstmals wissenschaftlich fundiert und abgesichert wird am UKSH mit ITS.APT der Fokus auf den Faktor Mensch als potentielle Schwachstelle der IT-Infrastruktur gelegt. Das Testfeld des klassischen Pentesting wird um den Faktor Mensch erweitert (Abbildung 3).

Auf der Basis einer fundierten Analyse bekannter Angriffsvektoren werden 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. Die Test-Teilnehmer werden anhand abstrakter Kriterien (Abteilung, Aufgabenbereich, Intensität der Computernutzung) ausgewählt, Reaktionsprotokolle nur anonymisiert bzw. pseudonymisiert erstellt. Die Ergebnisse lassen den Grad der Awareness ableiten und dienen der Konzeption gezielter Schulungsmaßnahmen zur Verbesserung der Awareness.

Die Beobachtung menschlichen Verhaltens mittels des skizzierten Testszenariums tangiert gleich mehrere gesetzlich geregelte Felder: Persönlichkeitsrecht, Arbeitsrecht, Haftungsrecht und den Datenschutz. Hier arbeitet das Projekt von Anfang an mit den lokalen Personalvertre-

tungen des UKSH und dem Datenschutzbeauftragten zusammen.

Fazit

IT-Sicherheit im Krankenhaus ist leistbar, auch wenn die Cyberkriminalität zunimmt. Organisatorische und technische Lösungen stehen zur Verfügung und müssen „nur noch" konsequent und effektiv im Tagesgeschäft umgesetzt werden. Dies erfordert zusätzliche Investitionen, einerseits in Technik, andererseits in Menschen. Krankenhausbudgets sehen derzeit hierfür keine Positionen vor. Hier bedarf es einer Anpassung der Krankenhausfinanzierung.

Nur qualifizierte Mitarbeiter sind in der Lage, die Konzepte und Techniken in der Praxis effektiv umzusetzen. Informierte und wachsame Mitarbeiter, mit geschulter Sensitivität für Risikosituationen und Bedrohungen durch Cyberangriffe können diesen angemessen begegnen. Das Bewusstsein einer latenten Bedrohungslage und Verwundbarkeit tragen wesentlich zur Sicherheit des gesamten IT-Systems bei. Der verantwortungsvolle Umgang mit IT-Komponenten unter kontinuierlicher Wachsamkeit jedes einzelnen Mitarbeiters können die Klinik-IT gegen Cyberangriffe härten. So werden informierte und sensibilisierte Mitarbeiter zur stärksten Waffe gegen Cyberangriffe und zu zentralen „Komponenten", um die Vulnerabilität einer IT-Infrastruktur zu verringern. ■

DR. ARMIN WILL

Stabsstelle Informationstechnologie
am Campus Lübeck des Universitätsklinikums Schleswig-Holstein

LITERATURVERZEICHNIS

1 Security Insider, Cyberkriminelle im Gesundheitswesen, 28.12.15 | Redakteur: Peter Schmitz, http://www.security-insider.de/cyberkriminelle-im-gesundheitswesen-a-516281/, zuletzt abgerufen: 07.01.2016

2 Cyber-Sicherheitsstrategie für Deutschland, Bundesministerium des Innern, Alt-Moabit 101, D 10559 Berlin

3 Bundesministerium des Innern, IT und Cybersicherheit, https://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/it-cybersicherheit_node.html, zuletzt abgerufen: 15.09.2016

4 Bundesministerium für Bildung und Forschung, Bekanntmachungen, https://www.bmbf.de/foerderungen/bekanntmachung-878.html, zuletzt abgerufen: 05.09.2016

5 Heise Security, Ronald Eikenberg: Online-Dienst erstellt maßgeschneiderte Krypto-Trojaner, https://www.heise.de/security/meldung/Online-Dienst-erstellt-massgeschneiderte-Krypto-Trojaner-2668860.html, veröffentlicht: 27.05.2015 16:06 Uhr, zuletzt abgerufen: 12.09.2016

6 KSN Report: Ransomware in 2014-2016, Kaspersky-Labs, Moskau, Juni 2016

7 ebenda

8 Ponemon Institute, Dr. Larry Ponemon: Healthcare organizations are in the cross hairs of cyber attackers, https://www.ponemon.org/blog/healthcare-organizations-are-in-the-cross-hairs-of-cyber-attackers, veröffentlicht: February 29, 2016, 12:00 am, zuletzt abgerufen: 15.09.2016

9 Ärzte Zeitung, Marco Hübner: Gesundheitssektor ist häufig Ziel von Hackern, http://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/905822/studie-gesundheitssektor-haeufig-ziel-hackern.html?sh=5&h=-966258025, veröffentlicht: 25.02.2016 06:46 Uhr, zuletzt abgerufen: 15.09.2016

10 kma-online, 900.000 Euro Gesamtschaden durch Cyberattacke, https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattacke-a-31629, Quelle: Guntram Doelfs, veröffentlicht: 24.06.2016 12:22 Uhr, zuletzt abgerufen: 15.09.2016

11 Universität Duisburg-Essen, Fachgebiet Allgemeine Psychologie: Kognition

12 Universität Münster, Institut für Informations-, Telekommunikations- und Medienrecht

13 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

14 Enno Rey Netzwerke GmbH

15 Universität Bonn, Institut für Informatik 4: Arbeitsgruppe IT-Sicherheit