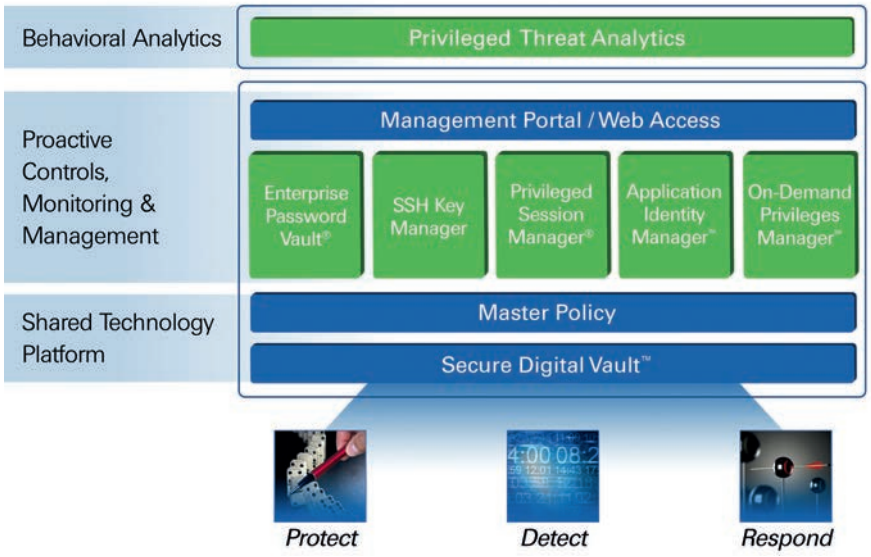
Zunehmende Vernetzung erhöht Risiko von Cyber-Attacken im Gesundheitswesen

Privilegien sicher schützen



Das Lösungsportfolio von CyberArk im Bereich Privileged Account Security im Überblick Bild: CyberArk

Der Umgang mit vertraulichen Krankenakten und Patientendaten gehört im Gesundheitswesen zum Tagesgeschäft. Datenschutz und Datensicherheit haben hier hohe Priorität. Eine zentrale Schwachstelle der IT-Sicherheit wird dabei allerdings oft vernachlässigt: privilegierte Nutzerkonten, wie sie Administratoren besitzen. Eine Lösung aus dem Bereich Privileged Account Security kann diese Sicherheitslücke zuverlässig schließen.

Die zunehmende Digitalisierung macht auch vor dem Gesundheitssystem nicht Halt. Diagnosen und Therapieformen werden heute in Krankenhäusern digital gespeichert, Laborberichte über das Internet übertragen und Krankenhäuser und -kassen kommunizieren digital miteinander. All das hat auch dazu geführt, dass die Gefahr eines Cyber-Angriffs und eines Diebstahls vertraulicher Informationen deutlich gestiegen ist.
Dass Institutionen im Gesundheitswesen dabei Standard-Sicherheitsvorkehrungen wie Firewall, Antivirenschutz oder Webfilter-Techniken treffen, sollte heute eine Selbstverständlichkeit sein. Doch dies ist keinesfalls ausreichend, wie die Vergangenheit mehrfach gezeigt hat. Mit immer ausgefeilteren Methoden, wie den aktuell häufig anzutreffenden zielgerichteten Web-Attacken (APTs – Advanced Persistent Threats), ist es heute relativ leicht, den Schutzwall gegen Angriffe von außen zu überwinden. Nahezu immer wurden in Fällen von Datensabotage oder -diebstahl privilegierte Nutzerkonten als Einfallstor genutzt. Mit ihren weitreichenden Rechten bergen sie prinzipiell für jedes Unternehmen, jede Behörde, aber auch jedes Krankenhaus eine erhebliche Sicherheitsgefahr. Der Grund: Über sie wird die gesamte IT-Umgebung mit Servern, Datenbanken und Netzwerkgeräten gesteuert und verwaltet.

Was tun, wenn der Angreifer schon im Netzwerk ist?

Es stellt sich folglich die Frage, wie die Sicherheit aufrechtzuerhalten ist, wenn der Angreifer den äußeren Schutzwall überwunden hat und sich bereits innerhalb des Netzwerkes befindet. Denn sobald er im Besitz privilegierter Zugangsdaten ist, kann er problemlos Ressourcen kontrollieren, Krankenhausinformationssysteme lahmlegen, Sicherheitssysteme ausschalten oder auf vertrauliche Daten zugreifen.
Im Gesundheitswesen betrifft das Sicherheitsrisiko dabei keineswegs nur die reine IT, sondern auch medizinische Geräte, die in die IT-Systemlandschaft integriert sind. Beispiele sind MRTs und CTs, Ultraschall- und Röntgengeräte oder Dialysemaschinen. Früher wurden solche Systeme noch getrennt von der IT betrieben, heute sind sie aber in immer stärkerem Maße mit der IT-Welt verknüpft – und damit, bedingt durch IT-Schwachstellen, auch leichter angreifbar.
Wenn aber die klassische Perimeter-Sicherheit prinzipbedingt heute keinen ausreichenden Schutz mehr vor externen Angriffen bietet, müssen die Systeme und Applikationen selbst in den Mittelpunkt der Sicherheitsstrategie rücken. Genau dies ist der Ansatz von Privileged-Account-

Best-Practice-Leitfaden für das Management privilegierter Nutzerkonten

1. Die wichtigsten Systeme, Anwendungen und Datenbanken und deren zugrunde liegenden privilegierten Konten ermitteln.
2. Die Personen bestimmen, die Zugriff auf privilegierte Konten haben sollen.
3. Richtlinien und Workflows für einen privilegierten Zugang zu den wichtigsten Systemen definieren.
4. Prozesse einrichten, die automatisch die Security-Richtlinien umsetzen.
5. Passwörter in einem virtuellen Tresor sichern.
6. Accounts und privilegierte Aktivitäten überwachen, mit Warnmeldungen, sobald die Richtlinien nicht eingehalten werden.

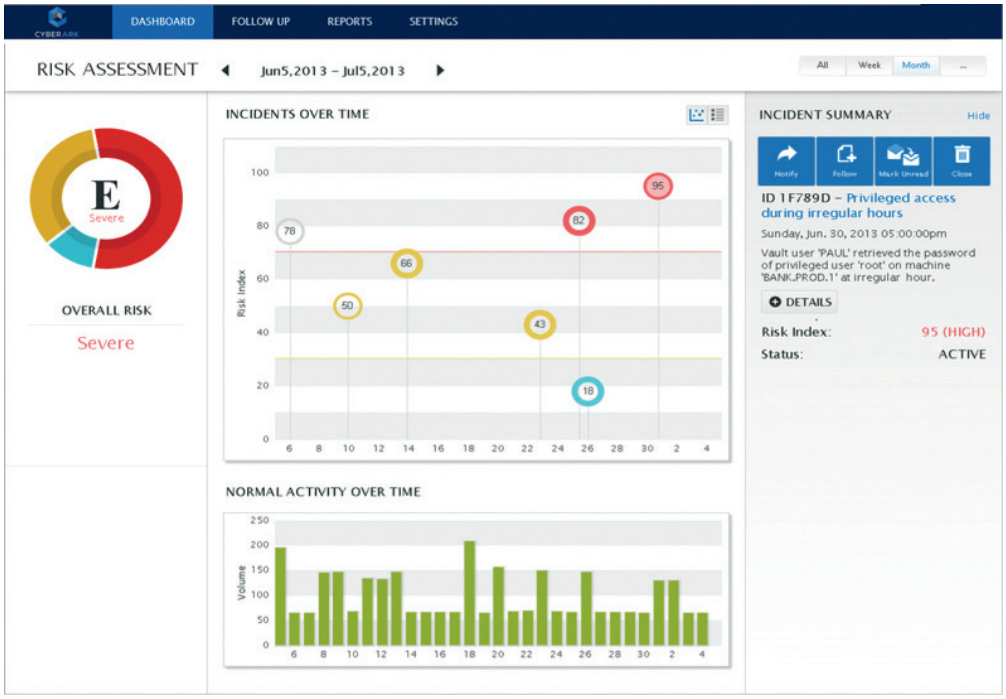
Security-Lösungen, mit denen privilegierte Zugriffe auf beliebige Zielsysteme zentral berechtigt, jederzeit kontrolliert und revisionssicher auditiert werden können. Immer mehr Unternehmen erkennen die Notwendigkeit einer solchen Lösung, wie das starke Wachstum dieses Marktsegmentes belegt.

Organisatorische Maßnahmen ergreifen

Vor der Implementierung sind aber zunächst organisatorische Maßnahmen zu ergreifen. Das betrifft vor allem das Rechte- und Rollenmanagement. Das heißt: In einem ersten Schritt muss – falls noch nicht geschehen – für privilegierte Administratoren-Accounts ein Berechtigungskonzept mit klar definierten Rollenmodellen erstellt werden. Durch das Rechtemanagement wird sichergestellt, dass die Administratoren nur Zugriff auf Daten inklusive Metadaten erhalten, die sie für die Durchführung ihrer Aufgaben benötigen. Dieses Rechtemanagement ist die Grundvoraussetzung für die Umsetzung einer rollenbasierten Zugriffskontrolle.
Die Realität sieht im Gesundheitswesen oft noch gänzlich anders aus. So ist es keine Seltenheit, dass in einem kleinen Krankenhaus jeder IT-Mitarbeiter mit Windows-Rechner gleichzeitig Domain-Administrator ist. Das ist allein schon unter datenschutzrechtlichen Aspekten extrem problematisch.
So heißt es etwa in der Anlage zu § 9, Satz 1 des Bundesdatenschutzgesetzes ganz klar: Es ist zu „gewährleisten, dass die zur Nutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).“

Privilegierte Nutzerkonten identifizieren und sichern

Bevor privilegierte und administrative Nutzerkonten gesichert werden, müssen sie zunächst identifiziert werden. Dies ist prinzipiell keine einfache Aufgabe. Eine typische Krankenhaus-IT-Umgebung besteht aus einer Vielzahl von Servern, Datenbanken und Netzwerkgeräten, die über persönliche, häufig aber auch generische, manchmal sogar lokale Admin-Konten gesteuert und verwaltet werden. Eine Privileged-Account-Security-Lösung sollte somit zunächst einmal die Möglichkeit bieten, diese Konten automatisch zu erkennen und zu analysieren – mit einer detaillierten Auswertung hinsichtlich Anzahl, Ort und Status.
Doch von welchen Konten gehen überhaupt die größten Gefahren aus? Hier sind eindeutig die von mehreren Personen genutzten Shared Accounts zu nennen, zum Beispiel Administratoren- und Dienste-Konten in Windows, Root-Konten in Unix/Linux und Administrator-Konten für Datenbanksysteme. Bei ihnen kann nicht kontrolliert werden, welcher Mitarbeiter ein Konto wann und wozu verwendet hat. Das heißt, eine revisionssichere Überprüfung der Verwendung bis auf die Personenebene ist nicht möglich.
Zur Sicherung von Nutzerkonten mit erweiterten Rechten sind heute verschiedene Lösungen auf dem Markt verfügbar. Bei der Auswahl sollte auf jeden Fall darauf geachtet werden, dass die Applikation neben einer regelmäßigen, automatischen Änderung aller Passwörter auch die Möglichkeit bietet, sämtliche Aktivitäten vollständig nachzuvollziehen. Mittels solcher Session-Protokolle kann dann nicht nur überprüft werden, wer Zugang zu vertraulichen Informationen hat, sondern auch, auf welche er zugreift und was er mit diesen Informationen macht. Dieser Punkt ist vor allem auch deshalb von Bedeutung, da viele Krankenhäuser nur über kleinere IT-Abteilungen verfügen und auf die Unterstützung externer IT-Provider angewiesen sind. Und auch auf die einzelnen medizinischen Geräte erfolgt in der Regel ein Remote-Zugriff durch den Hersteller.



Das CyberArk-Dashboard: Die grafische Darstellung von Vorfällen erleichtert eine schnelle Aufdeckung verdächtiger Verhaltensweisen. Bild: CyberArk

Christian Götz, Regional Professional Services Manager DACH bei CyberArk in Heilbronn: „An einer Privileged-Account-Security-Lösung, die einen gezielten Schutz privilegierter Nutzerkonten bietet, führt auch im Gesundheitswesen kein Weg vorbei." Bild: CyberArk

Konkret muss eine Sicherheitsapplikation drei Leistungsmerkmale bieten: Zugriffskontrolle, Überwachung und Reaktionsmöglichkeit. Grundvoraussetzung ist, dass sie eine Kontrollfunktion für die Verwendung von Passwörtern und den Zugriff auf Zielsysteme enthält. Zudem muss eine vollständige Überwachung der Nutzung privilegierter Konten gewährleistet sein. Nicht zuletzt sollte eine Privileged-Account-Security-Applikation natürlich auch eine sofortige Reaktion bei Sicherheitsvorfällen ermöglichen. Diese könnte auch den Entzug privilegierter Zugriffsberechtigungen oder das Beenden einer aktiven Verbindung beinhalten.

Echtzeit-Analytik bietet Sicherheitsplus

Eine zukunftsweisende Lösung bietet auch Echtzeit-Analytik und -Alarmierung bereits bei verdächtigen Aktivitäten im Zusammenhang mit privilegierten Konten. Das betrifft zum Beispiel abweichende Zugriffszeiten oder die ungewöhnliche Häufung von Zugriffen. Sicherheitsverantwortliche erhalten damit zielgerichtete Bedrohungsanalysen in Echtzeit, auf deren Basis sie auch auf laufende Angriffe reagieren können.

Alle Unternehmen, Behörden und Institutionen sind heute letztendlich den gleichen Cyber-Gefahren ausgesetzt. IT-Sicherheitslücken sollten deshalb mit State-of-the-Art-Lösungen zuverlässig geschlossen werden. Und das betrifft nicht zuletzt auch Nutzerkonten mit erweiterten Rechten. An einer Privileged-Account-Security-Lösung, die einen gezielten Schutz dieser Konten bietet, führt deshalb auch im Gesundheitswesen kein Weg vorbei. Nur damit ist eine generelle Erhöhung der Sicherheit und zuverlässige Erfüllung von Compliance-Anforderungen gegeben.

Christian Götz

Kontakt

CyberArk Deutschland
Ferdinand-Braun-Straße 8
74074 Heilbronn
Tel.: +49 7131 887353-0
dach@cyberark.com
www.cyberark.de

Das Gemeinschaftskrankenhaus Bonn zeigt, wie die Digitalisierung im Krankenhaus die Qualität der medizinischen Versorgung erhöht

Kabellos am Krankenbett

Mit etwa 200 Tablets hat das Gemeinschaftskrankenhaus Bonn die Grundlage dafür geschaffen, Papierakten ‚ad acta' legen zu können. Bilder: Deutsche Telekom

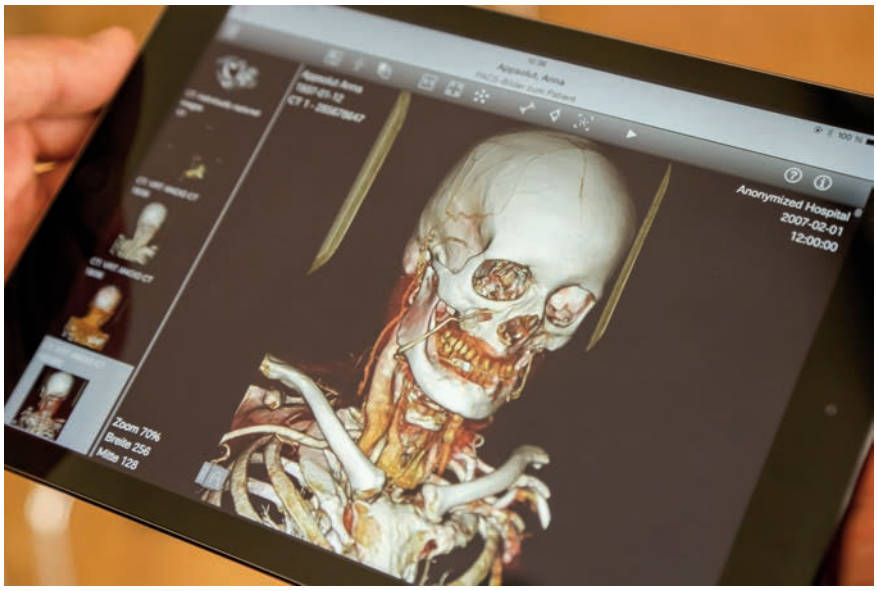
Aktenordner verbannen und auf Technik setzen: Die Ärzte und Pflegekräfte des Gemeinschaftskrankenhauses Bonn greifen auf aktuelle Befunde, Diagnosen oder Aufnahmen mit dem iPad zu. Dies ermöglicht ein effizienteres Arbeiten, erhöht die Qualität der Pflege und verbessert die Abrechenbarkeit von Leistungen.

Was Dr. Gesa Stöhr nicht im Kopf hat, hat sie auf dem Tablet. Röntgenbilder, Medikationen und sämtliche Befunde sieht die Assistenzärztin am Bonner Gemeinschaftskrankenhaus auf einem Bildschirm – überall abrufbar. „Ich kann direkt am Patientenbett alle relevanten Daten abrufen", sagt Dr. Stöhr. „Man hat zum Beispiel die Laborwerte direkt zur Hand und kann auf einer Art Zeitleiste nachsehen, wie sich der Wert nach und nach verändert hat." Durch den Einsatz von rund 200 Tablets und einer speziellen Software werden papierbasierte Patientenakten in Bonn überflüssig. Die Assistenzärztin greift per iPad mini von jedem Ort der Klinik aus auf das KIS iMedOne zu.

Mit der Digitalisierung der Patientendaten begegnet das Krankenhaus dem wirtschaftlichen Druck, unter dem das gesamte Gesundheitswesen steht. „Unser Ziel ist eine Kostenreduktion bei gleichzeitiger Qualitätssteigerung", erklärt Klaus-Werner Szesik, Kaufmännischer Direktor des Krankenhauses. „Dabei wollen wir die Chancen der Digitalisierung nutzen." Die Klinik im Herzen Bonns, die in die Modernisierung rund eine halbe Million Euro investiert hat, ist dem Großteil der Branche damit einen Schritt voraus. Andernorts, sagt Telekom-Vorstandschef Timotheus Höttges, besteht noch großer Nachholbedarf: „Ich bin aber davon überzeugt, dass das Krankenhauswesen in den kommenden fünf Jahren einen Sprung machen wird, was die Digitalisierung betrifft." Diese wird sich Höttges zufolge ohnehin flächendeckend ausbreiten: „Alles was digitalisierbar ist, wird digitalisiert."

Patienten akzeptieren das Tablet schnell

Die Technik erfährt indes sowohl bei Ärzten als auch bei Patienten großen Zuspruch. „Das Tablet wird schnell akzeptiert, weil selbst ältere Patienten die Vorteile erkennen", sagt Dr. Gesa Stöhr. So kann der Arzt



In der digitalen Akte können neben den Vital- und Laborwerten auch Inhalte aus dem PACS dargestellt werden. Mit der integrierten Kamera der Tablets lassen sich schnell Aufnahmen zur Wunddokumentation erstellen.

Die Mitarbeiter des Gemeinschaftskrankenhauses Bonn können mithilfe eines iPad mini von jedem Ort der Klinik aus auf das KIS iMedOne zugreifen.

Befunde, Krankheitsverläufe, aber auch Röntgenbilder bequem am Krankenbett abrufen und mit dem Patienten besprechen. „Untersuchungsergebnisse können dem Patienten sofort anschaulich demonstriert werden“, erklärt Dr. Jochen Textor, Ärztlicher Direktor und Chefarzt der Radiologie.
Ähnliche Erfahrungen hat auch Dr. Guido Trenn gemacht. Der Chefarzt der Inneren Medizin im Klinikum Bottrop nutzt die Software ebenfalls: „Wenn ich einem Patienten zum Beispiel den Befund einer Magenspiegelung vorstelle und ihm dabei ein Foto zeigen kann, wie sein Magen von innen aussieht, ist er in der Regel sehr interessiert und dankbar für die Information.“
Inzwischen setzen laut Telekom 35 Kliniken die Software für die mobile Datenerfassung per Tablet ein. In Bonn wurden im August 2015 die beiden letzten Stationen mit den Geräten ausgestattet, sodass die Vorarbeiten und die flächendeckende Umsetzung etwa ein Jahr in Anspruch genommen haben.
Rund 150 Ärzte und etwa 450 Pflegekräfte arbeiten nun mit dem iPad mini, das bequem in die Kitteltasche passt. In der Regel sind pro Station sechs Geräte im Einsatz, jeweils drei für das Pflegepersonal und für die Ärzte.

Kamera erlaubt schnelle Wunddokumentation

Die eingesetzte Software der Telekom deckt den kompletten Pflegeprozess ab. Mit einem Fingertipp wird die jeweilige Kategorie mit einem grünen Häkchen versehen. Zweimaliges Tippen hat ein rotes Häkchen zur Folge und bedeutet, dass die Maßnahme nicht nötig oder durchführbar war und daher nicht erbracht wurde.
Neben den Vitaldaten enthält die digitale Akte alle verfügbaren Informationen wie Labordaten. Sie lässt sich mit dem PACS verknüpfen, um Röntgenbilder auf dem iPad mini anzuzeigen. Mit der Kamera des Tablets ist zudem eine schnelle Wunddokumentation möglich.
Beim Anlegen neuer Datensätze wird festgelegt, welche Personen diese einsehen dürfen. Ändert ein Arzt die Medikation eines Patienten, ist die Information innerhalb weniger Sekunden zugänglich.
Denn die Daten fließen direkt in die digitale Patientenakte und sind dort für alle Beteiligten abrufbar. Jeder Mitarbeiter befindet sich daher immer auf dem neuesten Stand. Im Notfall ist so ein rascher Eingriff möglich. „Kommt zum Beispiel ein Notfallpatient in die Ambulanz, können seine Daten unmittelbar angesehen werden, ohne dass Akten oder Röntgenbilder umständlich gesucht und durchs ganze Haus getragen werden müssen“, sagt Dr. Jochen Textor.

Zweimonatige Testphase

Begonnen hatte die Umstellung im Bonner Gemeinschaftskrankenhaus im November 2014, als die Telekom zwei Stationen verschiedener Fachabteilungen mit der mobilen Visite ausstattete. „Nach einigen Verbesserungen in der zweimonatigen Testphase haben wir inzwischen eine Situation erreicht, in der wir klar profitieren“, berichtet Dr. Textor.
So hatte anfangs etwa die Infra-

Assistenzärztin Dr. Gesa Stöhr (re.) freut sich über die Möglichkeiten der digitalen Technik: „Man hat zum Beispiel die Laborwerte direkt zur Hand und kann auf einer Art Zeitleiste nachsehen, wie sich der Wert nach und nach verändert hat."

struktur des drahtlosen Netzwerks, worüber die verschlüsselten Daten zum Rechenzentrum übertragen werden, in einem Bonner Haus nicht die nötigte Leistungsfähigkeit. Der Engpass konnte durch den Austausch des WLANs und das Einrichten zusätzlicher Access Points behoben werden. Aufkommende Fragen betrafen nicht nur die Handhabung des IT-Systems, sondern durchleuchteten zudem die vorhandenen Abläufe auf den Stationen.
In einem Rhythmus von vier bis sechs Wochen wurden je zwei weitere Stationen in Betrieb genommen. Dabei verliefen die weiteren Umstellungen durch Schulung der Anwender und die Erfahrungen aus dem Testbetrieb ohne größere Vorkommnisse. Lediglich Spezifika verschiedener Fachabteilungen mussten geeignet umgesetzt werden.
Mit dem Einsatz der Tablets steigt die Effizienz der Arbeit: Ärzte sparen beim Nachschauen medizinischer Daten durchschnittlich rund eine Minute Zeit und verbringen zusätzliche eineinhalb Minuten beim Patienten. Dies ist das Ergebnis einer Studie der Charité in Berlin, bei der neun Neurologen über einen Zeitraum von 14 Wochen Visiten mit und ohne Tablets durchführten.

Für die Anordnung der Medikation hat das Bonner Krankenhaus ein Medikamenten-Informationssystem in die mobile App eingebunden. Dr. Textor zum Hintergrund: „80 Prozent der Behandlungsfehler im Krankenhaus passieren durch eine falsche Medikation. Die Ursachen liegen in Übertragungsfehlern oder weil Handschriften nicht gelesen werden können."

Fehlerfreie Medikation

Mit einem Blick auf das Tablet stehen dem Arzt nun detaillierte Informationen zur Medikation und den Wechselwirkungen der verordneten Medikamente zur Verfügung. Ist sich der Arzt bei der Medikation unsicher, führt er im Zweifel schnell einen Arzneimitteltherapie-Sicherheitscheck (AMTS) durch. „Mit dem elektronischen System sind Fehler künftig ausgeschlossen", ergänzt Dr. Textor. Die lückenlose Dokumentation lohnt sich nicht nur aus medizinischer Sicht, sondern auch finanziell. Vorteile ergeben sich zum Beispiel hinsichtlich der Abrechenbarkeit von Leistungen gegenüber der Krankenkasse. „Da kommt doch mehr zusammen, als man denkt", sagt Jürgen Remig, Chefarzt der Gefäßchirurgie am Bonner Gemeinschaftskrankenhaus. Das Krankenhaus profitiert darüber hinaus von einer verbesserten Hygiene: „Das Tablet kann desinfiziert werden; gegenüber der herkömmlichen Patientenakte ist das ein dicker Pluspunkt", betont Gesa Stöhr. Papier zu desinfizieren, ist bisher nicht möglich. Den Ärzten zufolge wird die Gefahr einer Übertragung von Keimen mit der neuen Lösung deutlich verringert.

Finanzieller Vorteil

Mit der Umstellung ihrer Arbeitsweise haben sich die Ärzte und Pflegekräfte inzwischen arrangiert. „Das System ist komplett alltagstauglich. Nur das Tippen ist etwas schwierig", sagt Gesa Stöhr. So dauert etwa die Eingabe von Freitext bei der Dokumentation auf einem mobilen Gerät mitunter länger als auf Papier. Die IT-Abteilung des Krankenhauses entwickelt daher gemeinsam mit den Medizinern Textbausteine, die die Eingabe künftig erleichtern sollen. Getestet wird zudem eine separate Tastatur. „Schön wäre auch eine Diktierfunktion", sagt Gesa Stöhr, deren Wunsch wohl nicht unerfüllt bleiben wird. In anderen Krankenhäusern ist diese bereits im Einsatz.
Die Entwicklung im Bonner Krankenhaus ist derweil auch Nachwuchskräften nicht entgangen, die mit mobilen Geräten aufgewachsen sind und großen Wert auf einen modernen Arbeitsplatz legen. Einige Zusagen von jungen Ärzten erhielt das Krankenhaus zuletzt auch deshalb, weil es mit dem iPad zeigen konnte, dass es über moderne Ausstattung verfügt und Wert auf innovative Arbeitsprozesse legt. ■

Kontakt

Deutsche Telekom Healthcare and Security Solutions GmbH
Magdalena Telec
Marketing Manager
Friedrich-Ebert-Allee 140
53113 Bonn
Tel.: +49 228 181-40551
magdalena.telec@t-systems.com
www.telekom-healthcare.com

Innovative Zutrittsorganisation sichert Gangelter Einrichtungen Maria Hilf

Neue Freiräume

Rund 2.000 elektronische blueSmart-Zylinder, neun Access Points und dreißig Standalone-Leser sichern den Komplex der Gangelter Einrichtungen. Auch die Schrankenanlage zum Parkplatz wurde umgerüstet.

Rund dreißig Gebäude umfasst der Komplex der Gangelter Einrichtungen Maria Hilf, der seine Wurzeln in einem Kloster aus der Gründerzeit hat. Psychisch-kranken, behinderten und alten Menschen wird hier geholfen. Die Zutrittsorganisation blueSmart von Winkhaus sichert die Bauten. Während sich damit für den Betreiber die Verwaltung der Liegenschaften deutlich vereinfacht hat, können sich die Bewohner über mehr Bewegungsfreiheit freuen.

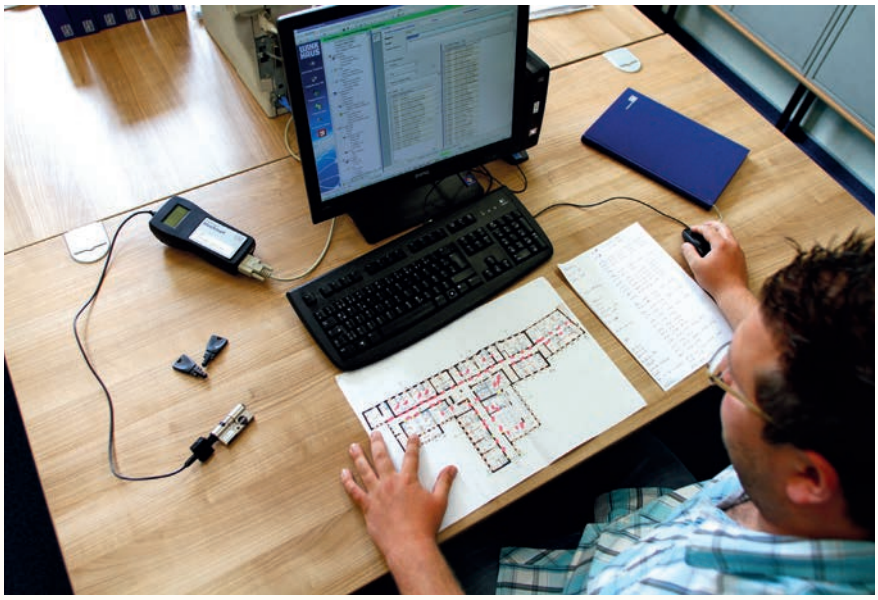
Schon 1869 lag den ersten Ordensschwestern das Wohl bedürftiger Menschen in Gangelt am Herzen. Noch heute sind ihre Leitlinien den 1.000 Mitarbeitern aus 42 Berufsgruppen präsent, die sich in der idyllischen Kleinstadt nahe der niederländischen Grenze für die Bewohner und Patienten engagieren. „Wir versorgen uns weitestgehend selbst. Neben einem kompletten landwirtschaftlichen Betrieb mit Maststall und Gemüseanbau betreiben wir auch eine eigene Metzgerei und eine Bäckerei“, berichtet Wirtschaftsleiter Patrick Berger. Sogar eine Reithalle gehört zum Komplex.

Bisher sicherten verschiedene mechanische und elektronische Schließanlagen die vielen Gebäude auf dem 87.000 m² großen Areal. Die bis zu zwanzig Jahre alten Anlagen entsprachen nicht mehr dem Stand der Zeit. Sie waren aufwändig in der Verwaltung und boten keine Möglichkeiten der Erweiterung – beispielsweise bei Neubauten.

Zukunftsorientierte Lösung für komplexe Aufgaben

Daher entschloss sich die Geschäftsführung, in eine zukunftsfähige Anlage zu investieren. „Für dieses Projekt bildeten wir eine Arbeitsgruppe, in der die Kollegen aus der Technik, der Personalabteilung und der Wirtschaftsleitung zusammenkamen“, erläutert Dieter Erfurth, Geschäftsführer der Trägergesellschaft Maria Hilf NRW gGmbH.
Um das optimale System zu finden, nahmen sie mithilfe eines beratenden Unternehmens den Markt unter die Lupe. „Winkhaus war einer der wenigen Anbieter, die aus unserer Sicht die Anforderungen an eine moderne, flexible und sichere elektronische Schließanlage erfüllen“, berichtet Patrick Berger, der das Projekt leitete. Denn blueSmart verknüpft die Vorteile von Offline- mit denen von Online-Lösungen. Dabei steigert das System die Effizienz elektronischer Schließsysteme und unterstützt den wirtschaftlichen Gebäudebetrieb, so der Hersteller.
Insbesondere die Möglichkeit eines virtuellen Netzwerks und die unkomplizierte Vergabe unterschiedlicher Schließrechte überzeugte das Team. So wurden die Gangelter Einrichtungen eines der ersten Projekte, bei denen blueSmart zum Einsatz kam.
Gerade in komplexen Strukturen wie in Gangelt zeigt die moderne Technologie ihre Stärken. Hoher Komfort und Flexibilität für den Anwender stehen im Fokus der neuartigen elektronischen Zutrittsorganisation. Einmalig, so der Hersteller, ist die Kombination aus passivem Schlüssel und elektronischem Schließsystem, das seine Daten mittels virtuellem Netzwerk kommuniziert. Informationen zwischen den elektronischen Zylindern überträgt das System schnell und kabellos über den batterielos arbeitenden Schlüssel.

Die Schließlösung wird mithilfe der Winkhaus-Software blueControl Professional zentral gesteuert. Die Organisationsstrukturen der Gebäude und Abteilungen können dabei direkt zur Berechtigung herangezogen werden. Änderungen werden in der Regel nicht mit dem Programmiergerät zu den Zylindern getragen, sondern beim regelmäßigen Aufbuchen am Access Point auf die Nutzerschlüssel programmiert. Der Daten- und Informationsaustausch zwischen Schlüssel und Zylinder geschieht bei der täglichen Verwendung des Schlüssels automatisch im Hintergrund, ohne dass der Anwender Kenntnis davon nimmt. Bei Bedarf kann das Schließsystem in bestehende Systeme wie Gebäudeleittechnik, Zeiterfassung oder Alarm- und Energiemanagement eingebunden werden. Mit diesen Vorteilen erfüllt es steigende Anforderungen an Bedienkomfort und Kosteneffizienz.



Vom zentralen Computer aus verwaltet Michael Heinrichs die Zutrittsberechtigungen. Der Datenaustausch innerhalb des Systems erfolgt kabellos im Rahmen der normalen Schlüsselnutzung. Der Schlüssel speichert auch Daten aus den Zylindern, wie den Zustand der Batterie. Schlüssel- und Zylinderdaten werden über den Access Point an den zentralen Server übertragen.

Datenaustausch in Rekordtempo

Im Gebäude arbeitet das Schließsystem mit einem virtuellen Netzwerk. Das funktioniert offline und drahtlos zwischen den installierten elektronischen Komponenten, die miteinander kommunizieren, Informationen verarbeiten und diese weitergeben. Im Gegensatz zu konventionellen Netzen entfallen aufwendige Verkabelungen, eine Vielzahl von Umsetzern oder störanfällige Funkstrecken.
Durch die Übertragung von Informationen im virtuellen Netzwerk entfällt der Aufwand für das manuelle Programmieren von Offline-Türkomponenten nahezu komplett.
So profitieren Verwalter und Nutzer von Schließanlagen vom Komfort von Online-Systemen, ohne auf die Vorteile von Offline-Lösungen verzichten zu müssen.
Die blueSmart-Zylinder haben die Abmaße mechanischer Zylinder, sodass beim Austauschen aufwändige Umbauten an den Türen entfallen.
Mit der modernen elektronischen Schließlösung können Schließanlagen mit bis zu 195.000 Zylindern und/oder Schlüsseln realisiert werden.
Dabei ist die blueSmart-Anlage schnell und unkompliziert installiert, denn nur der Access Point muss konventionell vernetzt werden, betont der Hersteller.
Lange Batteriestandzeiten ermöglichen auf Dauer den elektronischen Betrieb. Aus diesem Grund ist der Wartungsaufwand entsprechend gering. Der Ereignisspeicher auf den Schlüsseln und auch in den Zylindern ist deutlich größer als bisher: Es können zum Beispiel im Falle eines Diebstahls die letzten 2.000 Schließereignisse mit Datum und Uhrzeit im Zylinder ausgelesen werden.

Tatkräftige Unterstützung durch erfahrene Berater

Für die Realisierung des Projekts holte sich das Team Unterstützung von Praktikern. Der Sicherheitsspezialist Konnertz Schlüsselzentrale stand den Gangelter Einrichtungen bei der Konzeption, der Bedarfsermittlung und

Die elektronische Zutrittsorganisation blueSmart von Winkhaus bietet durch virtuelle Vernetzung dem Nutzer hohen Komfort und Flexibilität. Basiskomponenten sind der kompakte elektronische Zylinder, der elegante Schlüssel und der intelligente Aufbuchleser. Bild: Winkhaus

Der batterielos arbeitende blueSmart-Schlüssel trägt einen neuen, intelligenten Chip im Inneren eines IP68-tauglichen Kunststoffgehäuses. Mit ihm überträgt das System Informationen schnell und kabellos vom Access Point (li.) zu und zwischen den elektronischen Zylindern (Mitte) und den Standalone-Lesern (re.). Bilder: Winkhaus

der Erstellung der Schließpläne beratend zur Seite. Auch die Umrüstarbeiten, die die Einrichtungen selbst ausführten, begleitete das Unternehmen.
Bereits in der fünften Generation leiten die Brüder Dennis und Tino Konnertz den Familienbetrieb mit 85 Mitarbeitern und zwölf Niederlassungen. Schon lange arbeiten sie mit Schließanlagen von Winkhaus. Auch die neue Generation elektronischer Zutrittsorganisation aus Münster überzeugt sie: „blueSmart hat unsere hohen Erwartungen vollends erfüllt“, bestätigt Dennis Konnertz.
Heute sichern rund 2.200 elektronische blueSmart-Zylinder, neun Access Points und dreißig Standalone-Leser den Gangelter Komplex. Auch die Schrankenanlage zum Parkplatz wurde umgerüstet. Für die sensiblen psychiatrischen Bereiche entwickelte Winkhaus spezielle, von den Patienten nicht manipulierbare Zylinder.
Etwa 2.000 Schlüssel sind im Komplex im Einsatz, einige davon gehören den Bewohnern der verschiedenen Häuser. Für viele von ihnen brach mit der elektronischen Lösung eine neue Zeit an. Denn ihnen schenkt die innovative Technologie mehr Bewegungsfreiheit. Konnte ihnen in der Vergangenheit nicht ohne Weiteres ein eigener Schlüssel anvertraut werden, da die Gefahr des Verlusts bestand, sind sie nun stolze Inhaber eines blueSmart-Schlüssels.
Geht dieser doch einmal verloren, wird er nach 24 Stunden automatisch unbrauchbar oder kann vorher gesperrt werden. Die individuellen Schließrechte der Bewohner werden – ebenso wie die aus den Türkomponenten ausgelesenen Daten – temporär auf dem leistungsfähigen Chip im Inneren des stabilen Schlüsselgehäuses aus Kunststoff (IP 68) gespeichert.

Einfache Verwaltung der Schließanlage

Wird der Verlust eines Schlüssels gemeldet, kann er unmittelbar im zentralen Rechner gesperrt werden. Das übernimmt in Gangelt Michael Heinrichs – ebenso die Programmierungen der Schlüssel und die Installation der Zylinder. Eigentlich ist er Mitarbeiter der Personalabteilung. Doch sowohl die Hardware blueSmart als auch die Software blueControl Professional von Winkhaus ist so unkompliziert in der Handhabung, dass ihm die Verwaltung der kompletten Schließanlage bestens gelingt. Organisatorische Veränderungen und neue Nutzungskonzepte kann er mit wenigen Tastenklicks am zentralen PC sofort umsetzen. Zutrittsberechtigungen lassen sich zeitlich einschränken und Zutritte bei Bedarf durch ein elektronisches Protokoll nachvollziehen. Die vom Lösungsanbieter eigenentwickelte Software steuert das System.
„Unsere Bewohner und Mitarbeiter kommen mit den elektronischen Schlüsseln gut zurecht“, stellt Dieter Erfurth fest. Das liegt auch daran, dass der elektronische Schlüssel ähnlich genutzt wird wie ein mechanischer. Der Anwender steckt ihn in den Zylinder und dreht den Schlüssel. Daraufhin entsperrt der Zylinder die Tür. ■

Kontakt

Aug. Winkhaus GmbH & Co. KG
Irena Byrdy-Furmanczyk
August-Winkhaus-Straße 31
48291 Telgte
Tel.: +49 2504 921-657
Fax: +49 2504 921-429
irena.byrdy@winkhaus.de
www.winkhaus.de