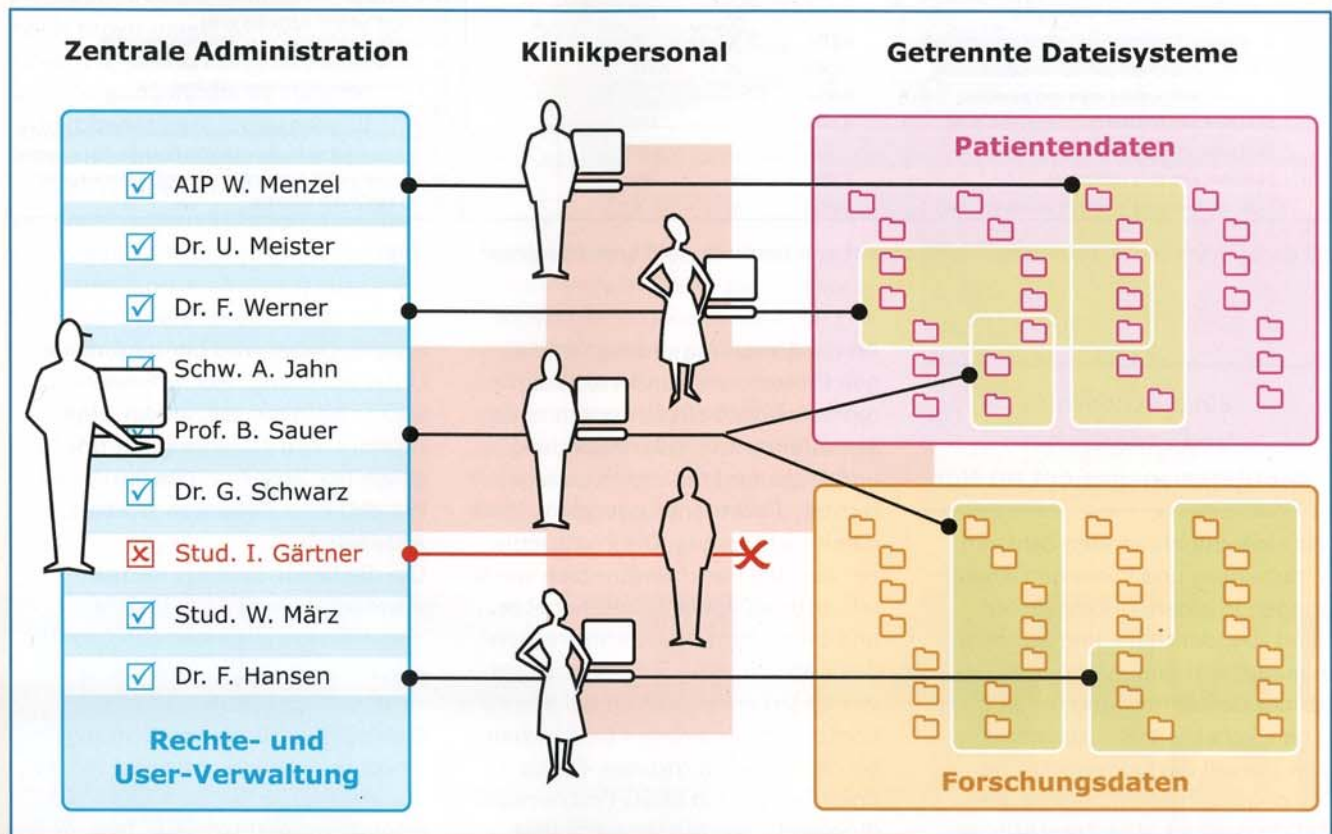


Identitätsmanagement regelt den Zugriff auf Patienten- und Forschungsdaten in Krankenhäusern

Patient Krankenhaus: Operation IT-Rechte



In Krankenhäusern und Forschungseinrichtungen ist die Überwachung der Zugangsberechtigungen auf IT-Ebene besonders wichtig und heikel.

BILDER: ECUNET

Das Thema Rechtevergabe wird im Krankenhaus ganz oben diskutiert. Eine ‚Therapie‘ in vier Stufen, wie sie ein Dienstleister vorschlägt, soll Ordnung im IT-Rechte-Chaos schaffen, betriebliche Sicherheitsprobleme lösen und Krankenhäuser dabei unterstützen, kosteneffizient zu arbeiten.

Internationale Studien bestätigen: Gesicherter Zugriff auf Patienten- und Forschungsdaten steht in Krankenhäusern ganz oben auf der Agenda der IT-Administratoren. Für eine zeitnahe Betreuung von Patienten ist vor allem der schnelle Zugang zu den Patientendaten entscheidend. Dieser ist aber gleich-

zeitig eine große Sicherheitslücke: Für 62 Prozent der Befragten einer US-Studie im Healthcare-Umfeld¹ stellt der unbefugte Zugriff auf Patientendaten das größte Sicherheitsproblem dar. 53 Prozent der Befragten wenden zwischen 11 und 40 Prozent ihrer Zeit für Compliance-Fragen auf. 54 Prozent der Befragten verfügen bereits über ein System zur Bereitstellung von Benutzerkonten in ihrer Systemumgebung oder wollen ein solches einführen. Auch in Deutschland hängen IT-Rechte in Krankenhäusern am Tropf: Um den Überblick zu behalten und Rechtssicherheit zu garantieren, müssen sowohl Patienten- als auch Forschungsdaten um-

fassend geschützt werden. Krankenhäuser und Unikliniken stehen dabei vor der IT-Herausforderung, dem zuständigen Klinikpersonal benötigte Daten zugänglich zu machen und gleichzeitig dafür Sorge zu tragen, dass nur berechtigte Personen Einblick erhalten.

¹ Imprivata Studie: Befragt wurden IT-Entscheidungsträger von Healthcare-Unternehmen in verschiedenen Teilen der USA (Februar/März 2009). www.imprivata.com/stuff/contentmgr/files/2/1c6b3966676339a140dfdcdbe11b64f/miscdocs/2009_identity_management_trends_in_healthcare_survey_research_brief_final_april_2009.pdf

Berechtigungs-Analyse

Scan Summary Report

Scope: C:\Users

Name	Percentage	Set directly	Value
1. Scanned folders	-	-	2.360
2. Scanned permissions	-	-	16.235
3. Permissions after resolved group memberships	-	-	202.549
4. Users authorized in scanned folders	-	-	25
5. Groups authorized in scanned folders	-	-	20
6. Relation of groups to users	-	-	0,80
7. Folders with 'everyone' permissions *	9,75%	75	230
8. Folders with 'everyone full control' permissions *	0,21%	2	5
9. Folders with non-group/single user permissions *	95,04%	23	2.243
10. Folders with just one single user permission	0,00%	0	0
11. Folders with non-inherited permissions (FSN)	4,24%	-	100
12. Relation of FSNs to users	-	-	4,00
13. Folders with deny permissions	2,92%	69	69
14. Folders exceeding maximum path length (255) *	0,00%	-	0

Mit cMatrix Reporting für Dateisysteme werden bestehende Forschungs- und Patientennetzwerke geröntgt.

Ein durchdachtes und verlässliches Identitätsmanagement tut Not

Mit einer zunehmenden Zahl von Mitarbeitern und klinischen Anwendungen in einem Unternehmen spielt das Identitäts- und Zugangsmanagement eine wichtige Rolle bei der Gewährleistung der betrieblichen Sicherheit. Hinzu kommt, dass überall dort, wo eine hohe Personalfuktuation besteht, die Gefahr groß ist, dass Berechtigungen auf Dokumente und Ordner in Dateisystemen nicht entsprechend verändert oder gelöscht werden. Dies gilt für Krankenhäuser im Allgemeinen und Unikliniken im Besonderen. Denn einerseits müssen sie Patientendaten für Schwestern, Ärzte, Ärzte im Praktikum, Oberärzte, Gastprofessoren oder Professoren schnell und sicher vorhalten. Andererseits müssen sie aber auch kritische Informationen wie beispielsweise Forschungsdaten vor unberechtigtem Zugriff schützen. Darum trennen Krankenhäuser sensible Patienten- und wertvolle Forschungsdaten strikt durch demilitarisierte Zonen. Dieses Vorgehen führt jedoch zu erhöhten Betriebs- und Supportaufwendungen in der IT: Administratoren müssen zwei komplett getrennte Netze verwalten.

An der Forschung sind neben einigen Professoren Hunderte Studenten beteiligt. Deshalb kommt es bei Semesterwechsel oder zu Anfang und Ende der Studienzeit zu regelrechten ‚Rechteentzugsorgien‘. Doch damit nicht genug: Die Protagonisten aus den Forschungsnetzen wechseln oftmals in die Patientennetze und umgekehrt, ohne entsprechenden Rechteentzug. Als Resultat entstehen Sicherheitslücken bei den Patientendaten sowie ein Rechtechaos bei den Forschungsdaten. Dieser Compliance- und BDSG-Problematik (Bundesdatenschutzgesetz) lässt sich mithilfe einer vierstufigen, methodischen ‚Rechte-Therapie‘ entgegenwirken.

Vierstufige Rechte-Therapie

Eine Ist-Analyse bringt zunächst Licht ins Rechtedunkel auf beiden Seiten – für Forschungs- und Patientennetze. Hilfreich ist dabei der Einsatz einer Softwarelösung wie beispielsweise cMatrix Reporting für Dateisysteme von econet. Sie deckt nicht nur beträchtliche Sicherheitsverstöße und Rechtevergehen auf, sondern liefert auch Kennzahlen zur Bewertung dieser Risiken und zum Aufwand deren Behebung. Im zweiten Schritt werden für beide Netze separate Soll-Konzepte für die standardisierte Verwaltung von Dateisystemen und Berechtigungen

erstellt. Dabei wird die zukünftige Unterscheidung, wer wo welche Rechte besitzen soll, an der organisatorischen Zugehörigkeit festgemacht – Forschung (Institut, Projekt) oder Patienten (Station, Abteilung).

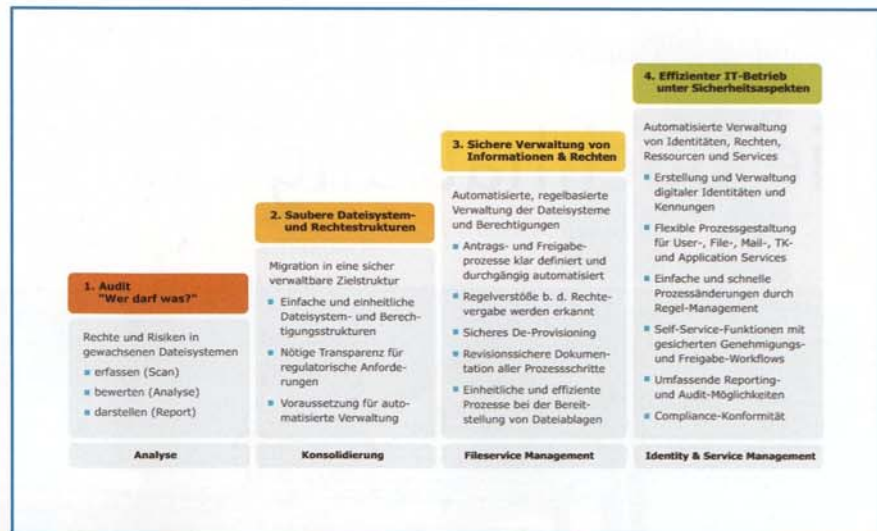
Um die bevorstehende Rechtsstandardisierung schnell, sicher und effizient umsetzen zu können, müssen dann zuerst manuell die strukturellen Mängel des alten Dateisystems, beispielsweise verschachtelte Shares, beseitigt werden. Die eigentliche Rechtemigration erfolgt automatisch, vom Tool gestützt.

Danach werden die Regeln des Soll-Konzepts in das Regelwerk einer Software wie cMatrix for Fileservice-Management und das Dateisystem übertragen. Damit besitzen nun beide Netze eine saubere, weil zentral verwaltete Struktur. Die zentrale Verwaltung und die kontrollierte Rechtevergabe über Genehmigungs-Workflows ermöglichen im späteren Betrieb den Erhalt der sauberen Datenbasis.

Durch automatisierte Prozesse Kosten sparen

Die finalen Schritte zum zentralen Management von Identitäten und Rechten sind der automatisierte Import der Userdaten beider Netze in das Identitätsmanagementsystem

sowie die Zuordnung von Metadaten wie Gebäude oder verantwortlicher Oberarzt zur organisatorischen Rolle samt den daran geknüpften Berechtigungen. Ab diesem Zeitpunkt können neue Mitarbeiter in den Systemen angelegt werden und mit Active Directory-Services, Mail-Services oder Application-Services versorgt, das heißt provisioniert werden. Dies geschieht automatisiert und mit den Berechtigungen, die sie für ihre Arbeit benötigen. Entsprechend können beim Weggang von Mitarbeitern deren sämtliche Berechtigungen mit einer Aktion von einer zentralen Stelle aus gesperrt werden. Die Investition in eine prozessorientierte Unternehmenssoftware für das Identity- und Servicemanagement unterstützt Krankenhäuser dabei, die wichtigsten Prozesse bei der Verwaltung von IT-Rechten und -Services sicherer und effizienter abzuwickeln. Vor allem die unüberschaubaren



Ein Vierstufenplan regelt die Wissensweitergabe in Krankenhäusern und Forschungseinrichtungen.

Deprovisioning-Prozesse lassen sich so von zentraler Stelle aus und automatisiert durchführen. Indem sie Prozesse transparenter und compliancekonform gestalten, beweisen Kliniken nicht nur mehr Verantwortung, sondern sparen auch Kosten durch die automatisierte Erbringung und Verwaltung von Services. ■

Kontakt

econet AG
 Martin Sauter
 Kaiser-Ludwig-Platz 5
 80336 München
 Tel.: 0 89 / 5 14 51-0
 martin.sauter@econet.de
 www.econet.de