Vom Stationsaccount zur digitalen Identität

Norman Lüttgerding, Leiter IT Ruppiner Kliniken Neuruppin
Stefan Zorn, Geschäftsführer imatics Software GmbH / Projektleiter IAM Ruppiner Kliniken

Health-IT-Talk Berlin/Brandenburg, 01. April 2019

Ruppiner Kliniken / Pro Klinik Holding

- Schwerpunktversorger im Land Brandenburg
- Trägerklinik der Medizinischen Hochschule Brandenburg
- 820 Betten
- 2.500 Mitarbeiter
- 22 Kliniken
- 4 MVZ
- 27.000 vollstationäre Fälle
- 120.000 ambulante Fälle

RUPPINER KLINIKEN
Hochschulklinikum der MHB

MHB MEDIZINISCHE HOCHSCHULE BRANDENBURG

imatics Software GmbH

- Healthcare Consulting zu Digitalisierungsthemen
- Führungskräfte- und Mitarbeitercoaching
- Prozessmanagement
- Projektmanagement
- Softwareauswahl
- Organisation und Neuausrichtung IT-Abteilung
- IT-Strategie
- → Identity- und Access-Management

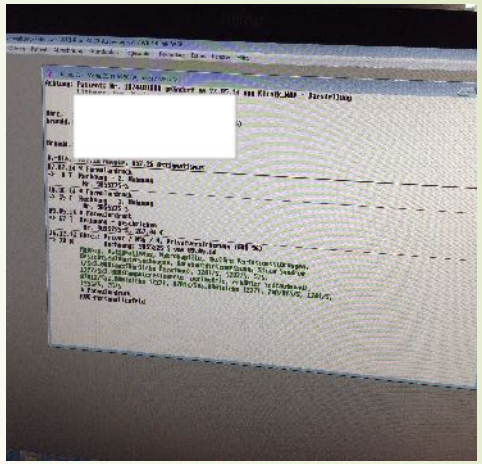
imatics
...moving ideas

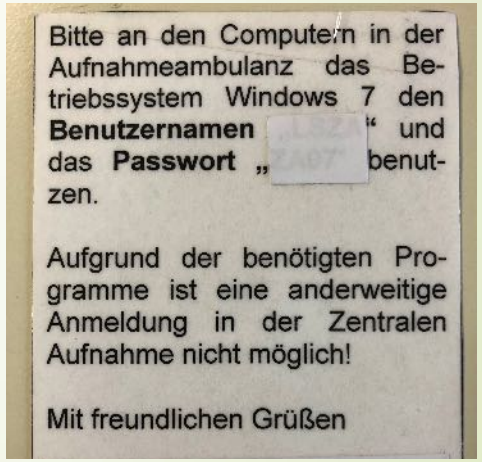
Datenschutzanforderungen gestern und heute

- Diverse Datenschutzverordnungen
  - BDSG
  - BSI
  - LKG
  - DSGVO
  - KRITIS
- Die Luft für einen „entspannten Umgang“ mit Datenschutzthemen wird langsam dünn
- Neue IT-Systeme im Zuge der Digitalisierung stehen den häufig üblichen Gemeinschaftszugängen diametral entgegen

Datenschutz im Klinikalltag

- Unsensibler Umgang mit Login-Daten
  - Freizügiger und unreflektierter Zugang mit Login-Daten
  - Post-It, „123456; hallo123; …“
- **Alle mit Einem – Eins für Alle**: Stationsaccounts
  - Keine Nachvollziehbarkeit, niemand weiß, wer wann was gemacht hat
- Offene Bildschirme
  - Patienten und Besucher können Patientendaten auf den angeschalteten Bildschirmen sehen (geht mit Papier auch ganz gut…)
- Datenschutz und Datensicherheit auf Stationen im Alltag nicht präsent





Initiatoren und Motivatoren für IAM

- Wirtschaftsprüfer, Audits
- Qualitätsmanagement
- Unternehmensstrategie
- Compliance
- Einführung neuer IT-Systeme
  - Medikation
  - PMS/EPA
- Lizenzkosten für „Userleichen“

Konsequenzen im Arbeitsalltag

- Häufig fehlende AD-Unterstützung
- „Login-Mania“
  - Einzel-Logins pro Applikation
  - Jeweils mit unterschiedlichen Passwort-Policies
- Komfort trifft auf Sicherheit
- Hoher Zeitverlust durch andauerndes An- und Abmelden
- Ohne technische Hilfestellung wird so etwas nicht akzeptiert → Es gibt immer einen Weg drumherum…

Los geht‘s...? → Weg von...

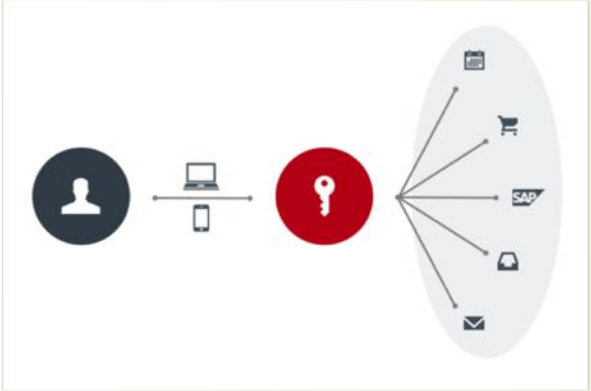
- Historisch gewachsene Rollen und Gruppen
  - Passen häufig nicht mehr zu aktuellen Strukturen
  - Werden z.T. nicht mehr benutzt
- Einzelberechtigungen
  - Sowohl auf Filesystem- als auch auf Applikationsebene → Unbeherrschbar!
- Stationsaccounts
- Nicht existierende bzw. konsequente Pflege von Berechtigungsänderungen
- Userleichen

Los geht‘s! → Hin zu…

- Aufgeräumtes und aktuelles Directory
  - Inkl. Prozesse zur Bewahrung dieses Zustands
- Klare Policies für Benamungen und Passwörter
  - Einheitlich, Bereichs- und Systemübergreifend
- Definierte Prozesse
  - …und „Leben“ Selbiger…
- „Audit2Go“
  - Jederzeitige Auskunftsfähigkeit für QM, Wirtschaftsprüfer, Prozessoptimierungen

Phase 1: IAM & SSO

- Vereinheitlichung von Benutzeraccounts
- Entlastung Mitarbeiter bei Login-Mania durch SSO
- Datenschutzkonforme, komfortable Infrastruktur
  - Automatisches Ausblenden von Bildschirminhalten
  - Automatisches Logout
  - Mitnahme des Arbeitsplatzes durch Virtual Desktop
  - Two Phase Commit (2PC)



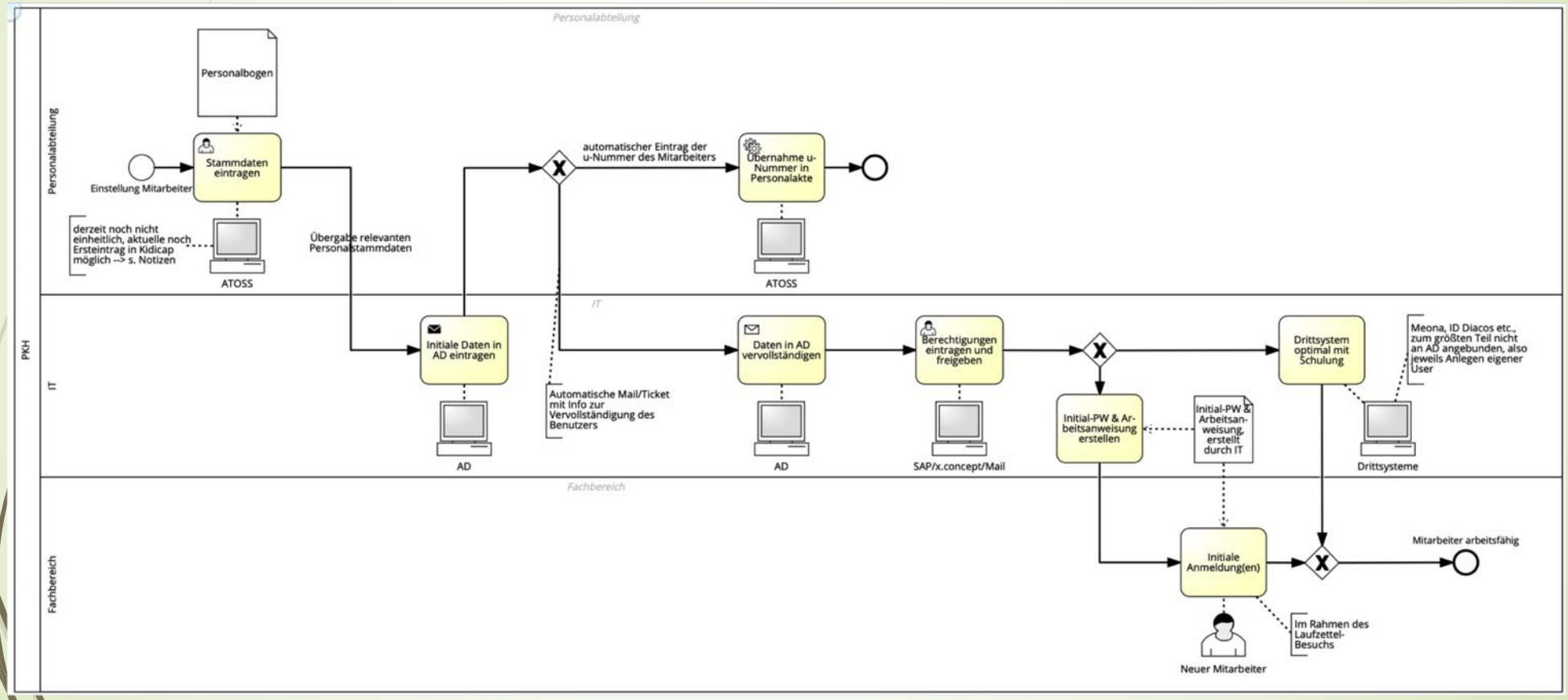
Phase 2: Access-Management

- Zentralisierte, teilautomatisierte Verwaltung von Zugriffsrechten
- Passwortmanagement
  - Automatische Passwort-Vergabe in Drittapplikationen inkl. Passwort-Updates, alles unter Berücksichtigung der jeweiligen Passwort-Policies
- User muss sich nur noch Windows-Login merken
- Transparente Berechtigungsvergabe
  - Die richtigen Rechte zur richtigen Zeit am richtigen Ort in der richtigen Applikation
- Helpdesk-Aufwand für vergessene Passwörter gehen gegen 0
- Sehr aufwendiges Projekt (viel Orga)

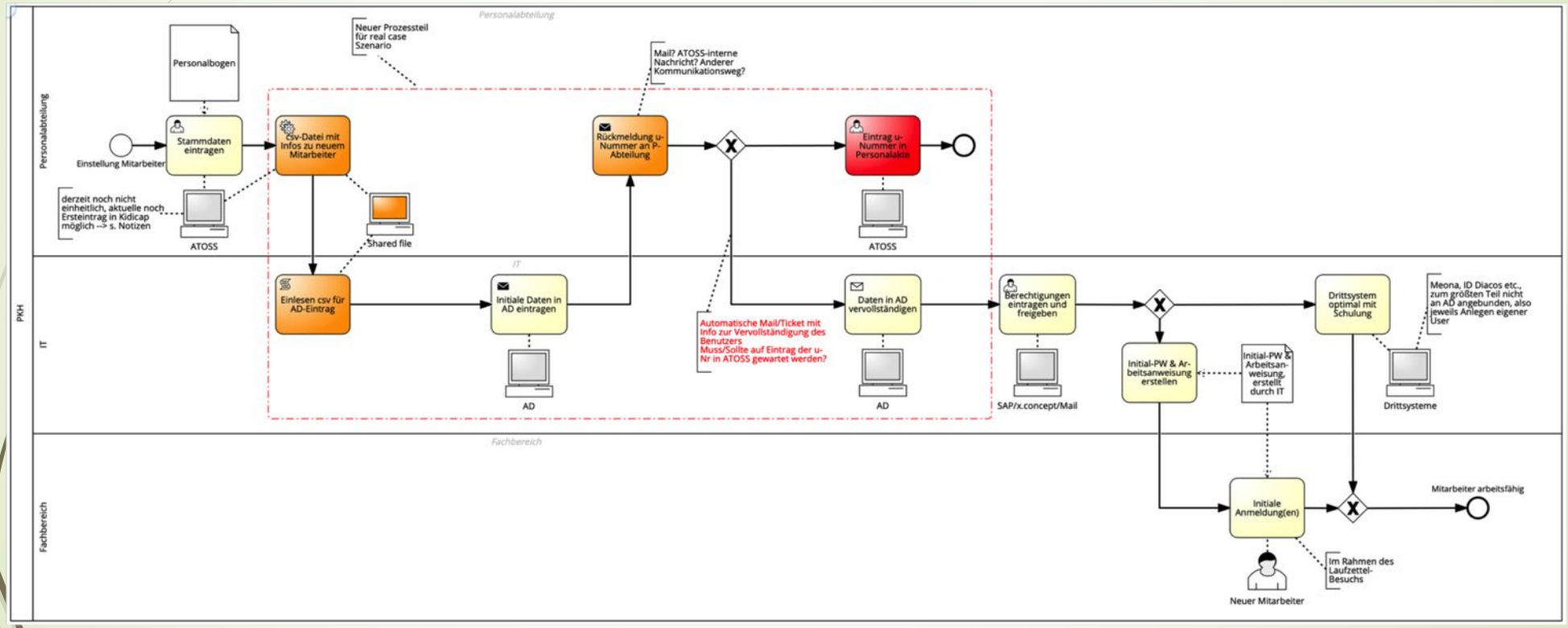
Datenquellen und Datenqualität

- HR ist Dreh- und Angelpunkt → Zentrale Stelle für Mitarbeiterbewegungen
- Integration HR-System in Infrastruktur
- Datenschutzdiskussion mit HR-Abteilung
  - Diskussionen zum Thema Datenschutzrelevanz von z.B. der Personalnummer, Datenminimierung bei der Datenübergabe etc. (Betriebsrat, Personalrat, Datenschützer) werden kommen…
- Einheitliche Nomenklaturen mit Clearingstelle in der IT-Abteilung
  - Voraussetzungen: IT-gestützte und integrierte HR; Klinikweit einheitliche Stellenbeschreibungen (und entsprechende Berechtigungen); Vereinbarung von klaren Nomenklaturen im Schnittstellenbereich, idealerweise gestützt und geschützt vom HR-System; Implementierung einer „Clearing"-Stelle in IT;
- Ergebnis: Sofortige Verfügbarkeit der richtigen IT-Ressourcen mit maximaler Transparenz

Access-Management mit HR-Integration



Access-Management ohne HR-Integration



Aufsetzen eines IAM-Projektes

- Virtual Desktop insbesondere für stationären Bereich zentral
  - Ausnahmen: Nicht-VDI-fähige Arbeitsplätze, Funktionsarbeitsplätze, ggfs. Verwaltungsarbeitsplätze
- Tokenbasiertes Login
- Projektverantwortung in IT-Abteilung
- Schritt 1: Proof of Concept
  - Ergebnisprognose: Die Abteilung will das System nicht mehr hergeben ☺
- Schritt 2: Pilotierung
  - Station mit allen beteiligten Berufsgruppen ist optimal für das „Innenmarketing“, allerdings auch die aufwendigste Variante
- Schritt 3: Sukzessive Einführung

Change → in diesem Fall mal anders

- Rechtliche Rahmenbedingungen sind so wie sie sind
  - Die Rahmenbedingungen sind so wie sie sind und fallen nicht negativ auf die IT zurück
- IT unterstützt spürbar bei der täglichen Arbeit
  - Die IT hilft und unterstützt bei einem solchen Projekt sofort spürbar in der täglichen Arbeit
- Initiale User waren sofort begeistert und überzeugt
- Nach Abschluss PoC wollte die Station die Technologie nicht mehr hergeben!
- Kritische Stimmen gibt es auch...

Kommunikation, Kommunikation, Kommunikation, Kommunikation

- mit Bereichsleitern
- intensiv mit Pilotkunden mit Individualbetreuung
- mit Pflege und ärztlichem Personal
- Monitoranhefter
- Längerer Text auf Startbildschirm
- Seite im Intranet
- Direkter Durchgriff auf Projektmitarbeiter via Helpdesk mit "Codewort" in Initialphase

Learnings und Erfahrungen

Sensibilierung für das Compliance-Thema im Allgemeinen mit dem Angebot einer Lösung "zieht“

Regelmäßige Kommunikation mit Leitungsebene

Vorher Kommunikationswege für verschiedene Zielgruppen definieren (Auslagen, Intranet, Mails etc.)

Einbinden möglichst unterschiedlicher Akteure in der Pilotphase

Möglichst vollständige Erfassung kritischer bzw. nicht integrierbarer Systeme (und Lösungen dafür finden)

Vielen Dank!

Norman Lüttgerding, n.luettgerding@pro-klinik-holding.de

Stefan Zorn, s.zorn@imatics.de, 0175/1658151