E-book

Kybernetische Sicherheit und digitale Identität für Krankenhäuser und medizinische Einrichtungen

ProID

Kybernetische Sicherheit und digitale Identität für Krankenhäuser und medizinische Einrichtungen

Wir haben diese Broschüre als unterstützendes Material für IT-Manager und Führungskräfte in Krankenhäusern und medizinischen Einrichtungen erstellt, die sich mit der digitalen Sicherheit ihrer Organisation und ihrer Mitarbeiter befassen.

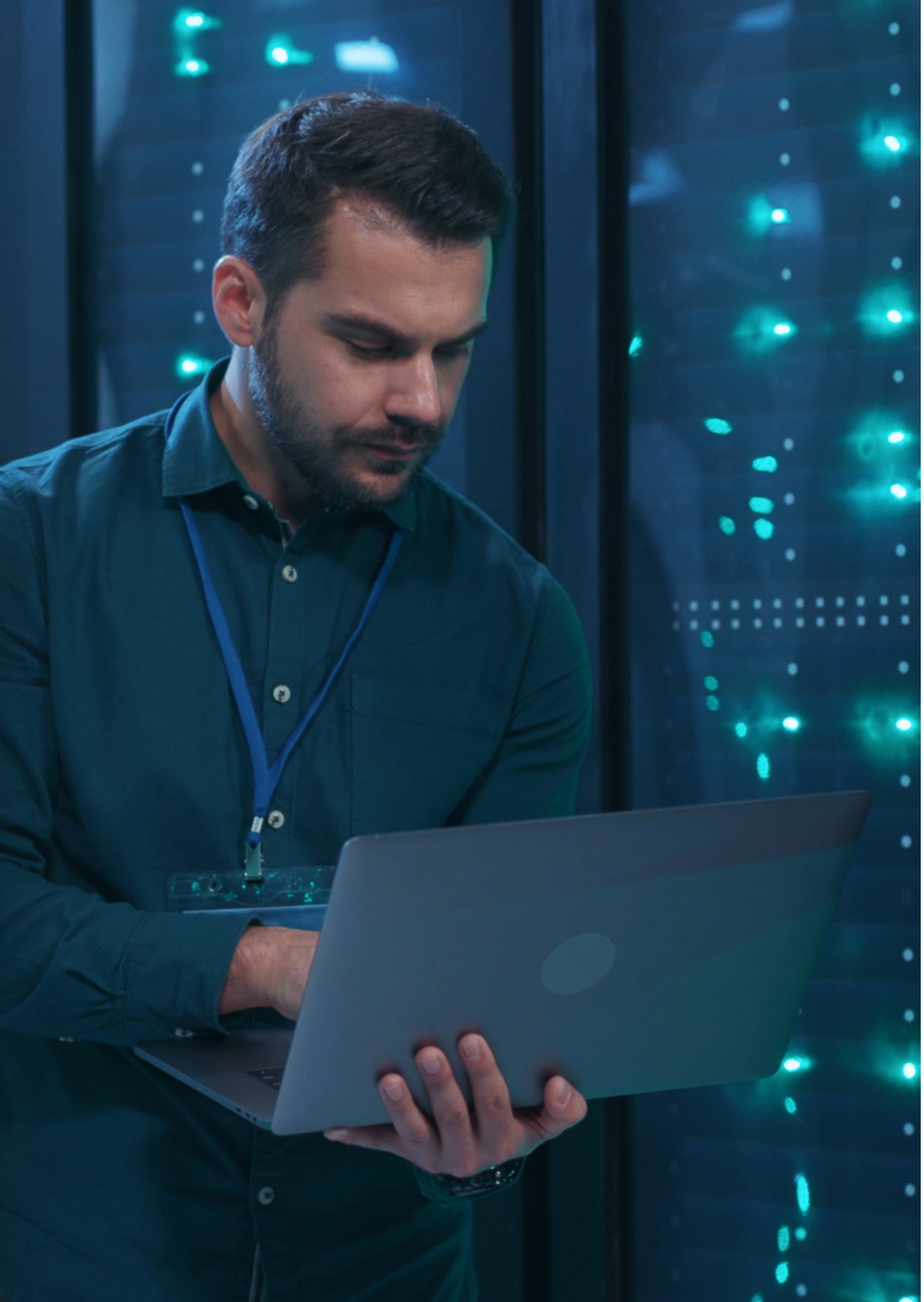
Wir sind spezialisiert auf die Einführung moderner Kryptographie, den Aufbau von PKI und die Entwicklung von Instrumenten für eine sichere, mehrstufige Anmeldung. Diese Broschüre befasst sich mit diesen Themen.

Wir haben bereits Dutzende von Implementierungen in Organisationen unterschiedlichster Größe und Art durchgeführt – in regionalen und Fakultätskrankenhäuser, Polikliniken und privaten Arztpraxen. In diesem Dokument finden Sie Erkenntnisse, die Ihnen in der Praxis helfen werden.

Kybernetische Sicherheit als Grundvoraussetzung für den Krankenhausbetrieb

In den letzten Jahren wurden wir Zeugen von Dutzenden Hackerangriffen auf verschiedene Organisationen und wichtige Behörden. Leider waren die Folgen für den Gesundheitssektor am deutlichsten, wo sie den normalen Betrieb ganzer Krankenhäuser gestört oder sogar lahmgelegt haben.

Beispielsweise entstand bei einem kybernetischen Angriff auf die Fakultätsklinik in Brünnein Schaden in Höhe von mehreren zehn Millionen Kronen, und einige Teile der Klinik waren mehr als einen Monat lang nicht funktionsfähig. Die gleiche Situation ereignete sich im Rudolf-und-Stefanie-Krankenhaus in Benešov und in vielen anderen Einrichtungen. Die Frage der Sicherheit medizinischer Einrichtungen und ihrer sensiblen Daten wurde somit zum Thema einer breiten Debatte, nicht nur unter IT-Experten.



Es gibt viele Gründen für solche fatalen Auswirkungen, die häufigsten sind jedoch:

- Anhaltende personelle und finanzielle Unterausstattung der IT in medizinischen Einrichtungen
- Die Annahme, dass „uns das nicht betrifft“
- Die Annahme, dass ein möglicher Angriff den Krankenhausbetrieb nicht beeinträchtigen kann

Leider ist das Gegenteil der Fall. Angriffe sind oft nicht auf eine bestimmte Organisation ausgerichtet, sondern erfolgen flächenhaft und automatisiert.

Die Kernaufgaben von IT-Managern im Gesundheitswesen

1. Sicherstellung eines reibungslosen und sicheren Ablaufs der digitalen Transformation
2. Schutz von Patientendaten und sensiblen Daten
3. Sicherstellung des unterbrechungsfreien Betriebs Ihrer Einrichtung
4. Reaktionsfähigkeit auf mögliche Bedrohungen und Angriffe
5. Überblick über den Status der betriebenen Systeme und Sicherstellung kontinuierlicher Aktualisierungen
6. Sicherstellung der Konformität mit gesetzlichen Vorschriften
7. Einrichtung geeigneter Mechanismen im Risikomanagement

Digitalisiertes Krankenhaus

Im Gesundheitswesen findet, wie in allen anderen Bereichen auch, eine rasante digitale Transformation statt. Der Großteil der medizinischen Dokumentation, Laborergebnisse und Kommunikation ist bereits vollständig digitalisiert. Das bedeutet, dass jede Unterbrechung dieses Informationsflusses zu einem Ausfall des gesamten Betriebs führt.

Auch die Arbeitsweise der Verwaltung und die Arbeitsgewohnheiten der Mitarbeiter haben sich verändert, insbesondere während der Coronavirus--Pandemie. In vielen Positionen wurde Remote-Arbeit oder die Beschäftigung von Teilzeitkräften eingeführt.

Europäische Richtlinie NIS 2

Auf die kritische Situation reagiert auch die Gesetzgebung, vor allem die neue europäische Richtlinie NIS 2. Diese führt eine völlig neue Strategie zur Bekämpfung der kybernetischen Kriminalität ein und wird für alle EU-Staaten verbindlich sein. Sie legt sehr strenge Regeln für den Umgang mit kybernetischer Sicherheit fest und definiert, wie Organisationen damit umgehen müssen.

Die neue Richtlinie gilt für alle Krankenhäuser, Heilhäuser und medizinischen Einrichtungen in der Tschechischen Republik.

Neben Prozessen und obligatorischen Schulungen muss auch die Einführung einer ganzen Reihe technischer Maßnahmen sichergestellt werden. Die neue Richtlinie wird als novelliertes Gesetz über kybernetische Sicherheit in das tschechische Recht übernommen.

Die häufigsten Fehler im Bereich der kybernetischen Sicherheit der Krankenhäusern

In unseren Projekten stoßen wir auf eine ganze Reihe von Problemen und Mängeln, mit denen die IT-Manager von medizinischen Einrichtungen bei der Gewährleistung der kybernetischen Sicherheit konfrontiert sind.

Sicherheitsmanagement (Security Governance)

- Kybernetische Sicherheit wird nur „auf dem Papier" in Form von Berichten oder Meldungen behandelt, nicht durch die praktische Einführung der erforderlichen Prozesse
- Es ist kein Budget für die erforderlichen Maßnahmen vorgesehen
- Fehlende Strategie und unzureichende Unterstützung von der Gesellschaftsführung
- Es gibt keine definierte Struktur für das Management, die Durchführung und die Kontrolle im Bereich der kybernetischen Sicherheit.
- Es gibt keine festgelegte Verantwortung für die Identifizierung und Erfassung vonAktiven
- Es wurde keine Risikoanalyse und kein Notfallplan für den Fall eines Systemausfalls erstellt
- Es wurden keine Regeln und Verantwortlichkeiten für die Umsetzung der aus der Risikoanalyse resultierenden Maßnahmen festgelegt
- Unzureichende oder fehlende Sicherheitsdokumentation
- Keine Schulungen im Bereich Informationssicherheit
- Es sind keine Sicherheitsrichtlinien definiert

Sicherheitsmaßnahmen (Security operations)

- Fehlende Überwachung der Netzwerksicherheit und der Endgeräte
- Fehlende Protokollierung
- Fehlende Zwei-Faktor-Authentifizierung für Computer und Systeme
- Unsystematische Lösung von Zwischenfällen
- Fehlende Topologie, Segmentierung, Portlisten
- Fehlende Prozesse zur Regelung der Kontinuität des Betriebs
- Unklares und informelles Verfahren zur Datensicherung, fehlendes Testen von Backups bei der Wiederherstellung

Personelle Absicherung der Sicherheit

- Es sind keine klaren Verantwortlichkeiten und Kompetenzen definiert
- Die Unternehmensleituqng unterschätzt die möglichen Risiken von kybernetischen Angriffen
- Es fehlt ein dedizierter CISO (Chief Information Security Officer)
- Die Unabhängigkeit des kybernetischen Sicherheitsmanagements vom IT-Management der Organisation ist nicht gewährleistet
- Die Rolle des CISO ist auf die technische Überwachung beschränkt (die meist von einem IT-Techniker der Organisation wahrgenommen wird)
- Die Mitarbeiter und das Management werden nicht im Bereich kybernetische Risiken geschult

Das schwächste Glied? Der Mitarbeiter

Es ist eine traurige Tatsache, dass 80 % aller erfolgreichen Angriffe darauf zurückzuführen sind, dass die Anmeldedaten von Mitarbeitern in den Kernsystemen des Krankenhauses durchgebrochen wurden. Über ihre Konten (oder die Konten der Administratoren) können Angreifer am einfachsten in die Systeme eindringen und diese kontrollieren.

Die Situation wird dadurch begünstigt, dass die meisten Benutzer sehr schwache Passwörter vom Typ Wörterbuch (admin123 usw.) verwenden, die sie zudem für alle Dienste, einschließlich privater Dienste, verwenden. Die schlimmste Variante ist dann das Einbrechen in privilegierte Administratorkonten, die in der Regel Zugriff auf alle Systeme und Schnittstellen haben.

Workforce Identity als Schutzschild für die Organisation

Die Verteidigung gegen diese Art von Angriffen ist Aufgabe des IT-Bereichs Workforce Identity, also der Arbeitsidentität. Dieser Bereich umfasst alle Vorgänge, mit denen Mitarbeiter bei ihren täglichen Tätigkeiten konfrontiert sind, beispielsweise die Anmeldung an Unternehmenssystemen, Computern oder Administrator-Schnittstellen.

Dies wird durch ein System digitaler Zertifikate ermöglicht, die innerhalb der PKI-Infrastruktur (Public Key Infrastructure) gespeichert sind und von einer Zertifizierungsstelle (CA) verwaltet werden. Die Mitarbeiter werden dann mit Tools für eine sichere, mehrstufige Authentifizierung für alle internen Systeme, Computer oder VPNs ausgestattet.

Die Einführung einer PKI innerhalb einer Organisation bedeutet die Einführung einer robusten Kryptografie, die sensible Daten und die Identität der Benutzer durch ein System aus öffentlichen und privaten Schlüsseln schützt und fortgeschrittene kryptografische Vorgänge wie die Erstellung elektronischer Signaturen ermöglicht.

Das digitale Ökosystem eines Krankenhauses aus der Sicht des Personals

Fakultäts- oder Kreiskrankenhäuser in der Tschechischen Republik haben in der Regel 10.000 Mitarbeiter. Hinzu kommen eine hohe Fluktuation und eine Reihe von externen Mitarbeitern, Studenten oder Vertragsärzten, die nicht mitgezählt werden, aber Zugang zu allen Kernsystemen haben. Aus der Perspektive der Mitarbeiterstruktur sprechen wir also von folgenden Grundgruppen.

Ärzte und Forschungsmitarbeiter

Die digitale Identität eines Arztes besteht aus mehreren grundlegenden Szenarien, die abgedeckt und gesichert werden müssen. In der Tschechischen Republik wird häufig auch die Arbeit externer Spezialisten in Anspruch genommen, die Teil verschiedener Forschungsprojekte sind.

Die häufigsten Prozesse, mit denen sie konfrontiert sind, sind:

- Die Anmeldung am Arbeitscomputer
- Die Unterzeichnung von eRezepten, eKrankmeldungen und eVerschreibungen
- Sicherer Empfang und Versand von Untersuchungsergebnissen
- Sicherer Zugriff auf medizinische Unterlagen
- Der Zugriff auf das Informationssystem des Krankenhauses
- Die Identifizierung in kontaktlosen Systemen

Lösung zur Gewährleistung der Identität und Sicherheit:

- Die Chipkarten und USB-Token mit der Funktion für elektronische Signatur und mehrstufige Anmeldung in die Systeme des Krankenhauses
- Die Verschlüsselung der Kommunikation und der versendeten Dokumente mit empfohlenen Algorithmen (RSA, ECC)
- Ein Modul für die einfache Eingabe des QPins (qualifizierter PIN für die Unterzeichnung von eRezepten und anderen elektronischen Dokumenten)

Medizinisches Personal und Laboranten

Das übliche medizinische Personal hat sehr ähnliche Arbeitssituationen, die gesichert werden müssen. Im Vergleich zu Ärzten müssen sie sich zwar nicht mit elektronischen Signaturen befassen, benötigen jedoch ein einfaches Tool, um sich an gemeinsam genutzten Computern anzumelden, auf die Schnittstellen medizinischer Geräte zuzugreifen oder Türen zu öffnen und Aufzüge zu steuern.

Die häufigsten Prozesse, mit denen sie konfrontiert sind, sind:

- Visuelle Identifizierung (multifunktionaler Ausweis)
- Der Zugang zu den Räumlichkeiten, der Türöffnung, der Steuerung von Aufzügen
- Die Anmeldung an einem gemeinsam genutzten Computer unter Ihrer ID
- Der Zugang zu medizinischen Unterlagen
- Der Zugang zum Informationssystem des Krankenhauses
- Die Versiegelung/Unterzeichnung von Laborergebnissen.

Unsere Lösung zur Gewährleistung der Identität und Sicherheit:

- Die Chipkarten als Ausweis mit der Signatur- und der Anmeldefunktion
- Kontaktlose Funktionen – Öffnen von Drehkreuzen, Türen, Aufzügen
- Die Anbindung an Anwesenheitslisten oder die Bezahlung von Mittagessen
- Elektronischer Siegel zum massenhaften Versiegeln von Laborproben
- Elektronische Versiegelung von Ausdrucken medizinischer Geräte (Mammographiegerät, Röntgengerät…)

Management/Externe Mitarbeiter/Backoffice

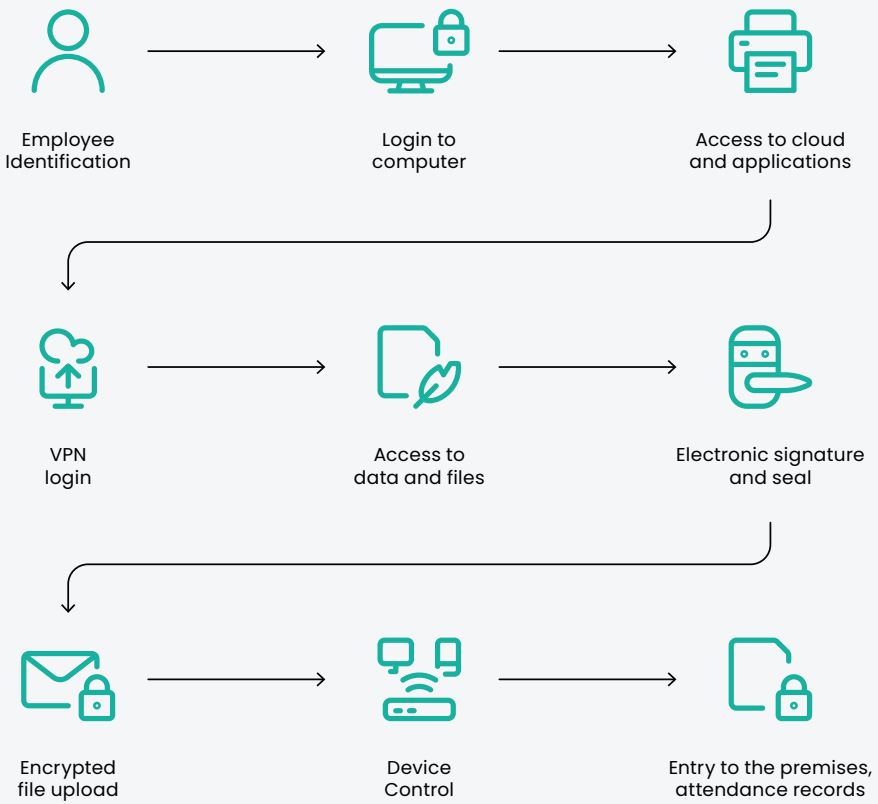
In jeder medizinischen Einrichtung gibt es eine Reihe von Positionen und Aufgaben, die nicht zum Gesundheitswesen gehören, ohne deren Erfüllung die Organisation jedoch nicht funktionieren könnte. Im Allgemeinen handelt es sich vor allem um alle Verwaltungsmitarbeiter und Externisten. Neben der Sicherstellung der üblichen wirtschaftlichen und betrieblichen Abläufe gewährleisten sie die Kommunikation mit Behörden und Versicherungen und leisten Unterstützung bei Förderanträgen und Forschungsprojekten.

Die häufigsten Prozesse, mit denen sie konfrontiert werden, sind:

- Sicherung der Kommunikation mit Gerichten und Sozialbehörden
- Bearbeitung von Dokumenten für die Krankenkassen
- Zugriff auf das Informationssystem des Krankenhauses und auf die Abrechnungsprogramme
- Bearbeitung von den Förder- und Projektunterlagen
- Onboarding neuer Mitarbeiter (bis zu Dutzende pro Monat)

Unsere Lösung zur Gewährleistung der Identität und Sicherheit:

- Verschlüsselte VPN-Verbindung für die Fernarbeit
- Die Instrumente für die mehrstufige Anmeldung in den Systemen des
- Krankenhauses
- Die Erleichterung der Arbeit mit qualifizierten Zertifikaten
- Automatische Benachrichtigungen beim Ablauf von Zertifikaten und deren schnelle Erneuerung
- Elektronische Signatur, Siegel und Zeitstempel als Fernservice



IT-Administratoren der Organisation

Die Rolle der IT-Administratoren im Krankenhausbetrieb ist äußerst komplex. Sie sind für den gesamten Betrieb des Netzwerks im Krankenhaus verantwortlich, einschließlich der Wartung von Computern, Druckern, Servern und Kabeln. Sie sind personell und finanziell unterbesetzt und verfügen nur über begrenzte finanzielle und zeitliche Kapazitäten für die Umsetzung komplexer IT-Projekte. Dennoch müssen sie sich auch um die digitale Identität und Sicherheit ihrer Mitarbeiter kümmern.

Die häufigsten Prozesse, mit denen sie konfrontiert werden, sind:

- Sicherer Zugriff auf Administratorkonsolen
- Sicherer Zugriff auf VPN und Remote-Desktops
- Massenoperationen für Mitarbeiter und Zertifikate
- Umfassende Überwachung ausgestellter Zertifikate und digitaler Schlüssel
- Möglichkeit der sofortigen Ungültigmachung von Zertifikaten
- Die Übertragung von Routinetätigkeiten an HR/Backoffice.

Unsere Lösungen zur Gewährleistung der Identität und Sicherheit:

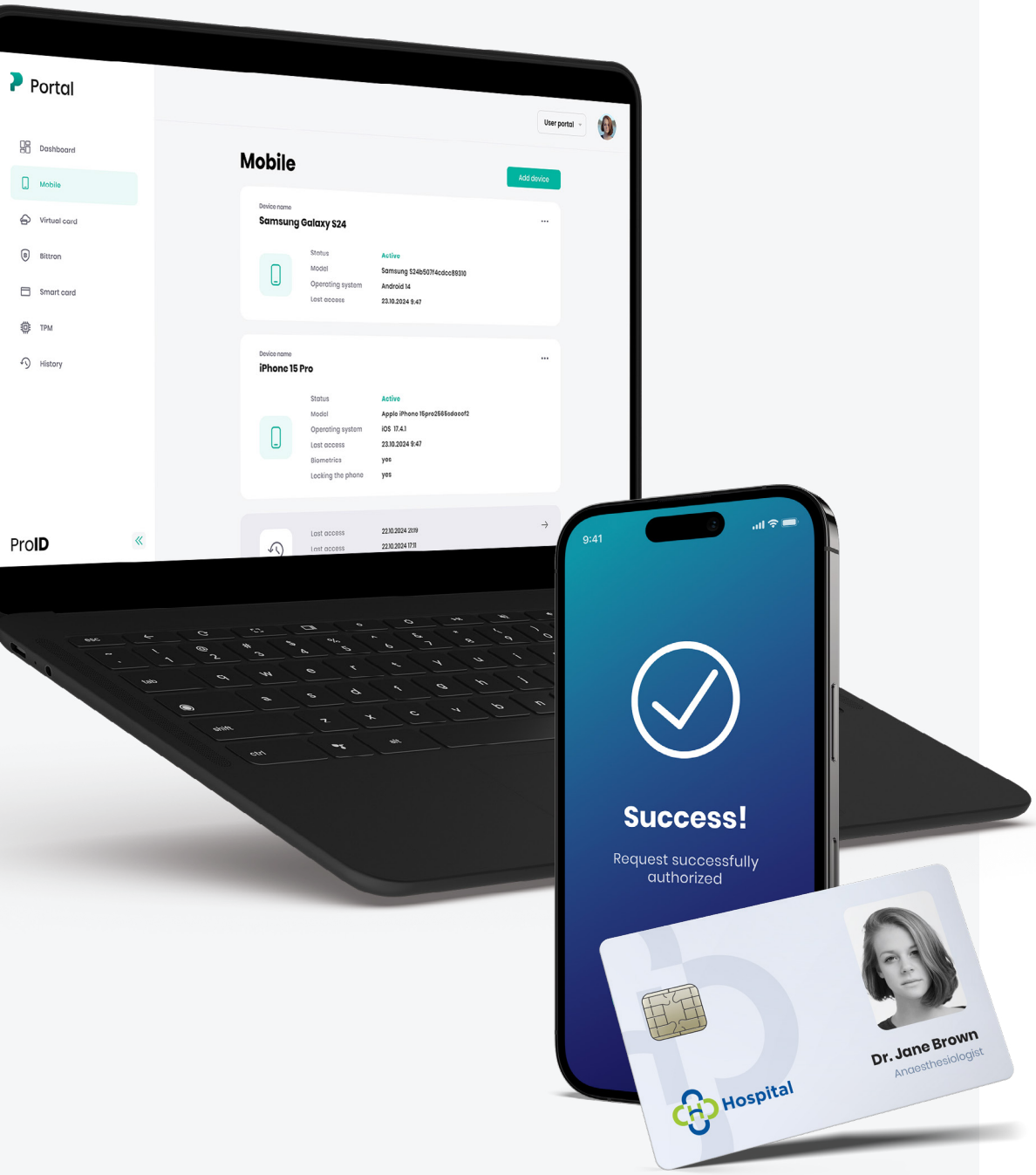
- Die Instrumente für die passwortlose Anmeldung an der Admin-Oberfläche
- Die Module für Data Mining, Backups und Operationen in der Echtzeit
- Ein Modulset zur Automatisierung der Arbeit mit Zertifikaten und Schlüsseln

Wie kann die logische Sicherheit des medizinischen Personals und der Kranken-hausmitarbeiter gewährleistet werden?

Die Lösung ist klar: Einführung einer modernen **Workforce Identity,** also einer Arbeitsidentität (logische Identität), innerhalb der medizinischen Einrichtung. Dieser Prozess muss jedoch nicht kompliziert sein:

- Die Krankenhäuser verwenden bereits HW-Tools (ProID-Chipkarten oder andere).
- Sie lösen damit jedoch nicht die logische Sicherheit (Anmeldung an Systemen,
- Computern usw.) – sie werden entweder für kontaktlose Funktionen oder für elektronische Signaturen verwendet.
- Dabei ist die Erweiterung der Funktionen einfach – es müssen lediglich die erforderlichen SW-Module und Zertifikate hinzugefügt werden.

Es handelt sich also um eine Ergänzung der Funktionen von bereits üblichen Tools. Das medizinische Personal muss nicht aufwendig auf neue Lösungen umsteigen, sondern kann weiterhin das gewohnte System nutzen. Darüber hinaus lassen sich so enorme Kosten einsparen.



Verfügbare Tools und Lösungen für Workforce Identity innerhalb des Krankenhauses

Die ProID-Chipkarten

Mit dem Kontaktchip der ProID-Hybridkarten können Sie eine qualifizierte elektronische Signatur erstellen oder sich in die Systeme des Krankenhauses einloggen. Der kontaktlose Chip kann für übliche Tätigkeiten verwendet werden, beispielsweise für die Anwesenheitserfassung, zum Öffnen von Türen, zur Steuerung von Aufzügen usw. Wenn die Karte mit den persönlichen Daten und einem Foto des Inhabers bedruckt wird, kann sie auch zur visuellen Identifizierung dienen.

ProID Mobile - die Authentifizierung per Handy

Die mobile Anwendung ProID funktioniert genauso sicher wie die Anmeldung bei Bankkonten auf dem Mobiltelefon. Sie können sich mit biometrischen Daten (Fingerabdruck oder Face ID) oder einer PIN bei Ihrem Computer, Dutzenden von Anwendungen oder VPN anmelden. Die Methode funktioniert passwortlos.

Die Domänen-PKI und Zertifizierungsstelle

Der Aufbau von Zertifizierungsstellen für die Verteilung digitaler Zertifikate ist ein fester Bestandteil der meisten Projekte. In Krankenhäusern bauen wir meist eine separate Stamm-CA mit einer anschließenden zweistufigen Hierarchie für Benutzer und Infrastrukturkomponenten auf. Wir liefern auch die komplette Notfall-, Betriebs- und Sicherheitsdokumentation.

Qualifiziertes elektronisches Siegel ProID QSeal

Es eignet sich für das massenhafte Versiegeln von Laborproben – es ermöglicht die Erstellung von bis zu 1700 Siegeln pro Stunde. Es handelt sich um eine sichere Lösung in Form eines USB-Tokens, der an einen Server in Ihrer Organisation angeschlossen wird. Es wird ein einmaliger Festpreis gezahlt, das anschließende Versiegeln ist kostenlos.

Module für die Verwaltung digitaler Zertifikate

Wir bieten Dutzende von Zusatzmodulen für die Automatisierung komplexer Prozesse mit Karten und Zertifikaten. Die Verwaltung des Lebenszyklus und die automatische Erneuerung von Zertifikaten sind so einfach, dass auch weniger erfahrene Benutzer damit zurechtkommen.

Für die Ärzte haben wir ein Modul zur Speicherung von QPINs und zur einfachen Signatur von eRezepten in Übereinstimmung mit der QSCD-Zertifizierung und der eIDAS-Verordnung entwickelt.

Unsere Dienstleistungen für Sie Womit wir Ihnen gerne helfen

- Die Durchführung einer PKI-Überprüfung, gegebenenfalls kontrollierte Abschaltung und Aufbau einer neuen PKI
- Die Implementierung empfohlener Änderungen
- Die Einführung von Tools für die sichere Anmeldung und Identitätsprüfung von Benutzern und Administratoren
- Die Einhaltung der Empfehlungen vertrauenswürdiger Behörden, die korrekte Verwendung von kryptografischen Schlüsseln und digitalen Zertifikaten
- Die Überprüfung von Sicherheitsplänen und -richtlinien

ProID solutions by MONET+

Wir sind ein tschechisches Softwareunternehmen mit 25 Jahren Tradition. Zu unseren Kunden zählen öffentliche Einrichtungen und private Unternehmen aller Größen und Branchen. Unser Team besteht aus fast 300 Experten aus der ganzen Tschechischen Republik. Im Rahmen der Produktplattform ProID entwickeln wir fortschrittliche Tools für Firmenkunden, die eine sichere (verschlüsselte) Anmeldung an Unternehmenssystemen, Computern und VPNs ermöglichen.

Außerdem entwickeln wir Tools für sichere elektronische Signaturen und elektronische Siegel. Unsere Lösungen erfüllen die Kriterien des Gesetzes über kybernetische Sicherheit und gewährleisten den Schutz personenbezogener Daten gemäß der EU-Verordnung DSGVO und der eIDAS-Verordnung.

ProID

Erfahren Sie mehr unter www.proid.tech