27.07.2025 BDC|News

Mehr Sicherheit in der Chirurgie?

Ralph Lorenz

BERICHT VON DER 9. GEMEINSAMEN FRÜHJAHRSTAGUNG ANC UND BDC – BRANDENBURG UND BERLIN AM 24. MAI 2025, KV BRANDENBURG POTSDAM

Im Rahmen der 9. Gemeinsamen Frühjahrstagung haben die Veranstalter und Organisatoren der ANC und des BDC|Brandenburg und BDC|Berlin zunächst im politischen Teil der Veranstaltung Sicherheitsaspekte und die zunehmende Digitalisierung zum Thema gemacht.

Cyberkriminalität im digitalen Gesundheitswesen: Herausforderung für Kliniken und Praxen

Im ersten Vortrag beleuchtete Herr Dipl.-Ing. Frank Engelking (Abb. 1, 2), Informationssicherheitsbeauftragter an der Medizinischen Universität Cottbus Carl Thiem, eindrücklich die Bedrohung durch Cyberkriminalität.

Die politisch vorangetriebene Digitalisierung des Gesundheitswesens nimmt mit beeindruckender Geschwindigkeit Fahrt auf. Elektronische Patientenakten, vernetzte Medizingeräte und automatisierte Abläufe versprechen Effizienz und Fortschritt – doch mit dieser Entwicklung gehen auch neue Risiken einher. Insbesondere die Informationssicherheit steht zunehmend im Fokus.

Cyberangriffe: Keine Frage des Ob, sondern des Wann

Engelking machte deutlich: Die Gefahr durch Cyberangriffe ist allgegenwärtig. Krankenhäuser und Praxen müssen sich nicht fragen, ob ein Angriff erfolgt, sondern wann. Die häufigsten Szenarien sind dabei der direkte Diebstahl sensibler Daten oder deren Verschlüsselung, gefolgt von Lösegeldforderungen – oft in Form von Kryptowährungen wie Bitcoin. Neben dem potenziellen Datenverlust droht auch der komplette Ausfall der IT-Infrastruktur, wodurch die Patientenversorgung massiv beeinträchtigt werden kann.

In erschütternden Beispielen zeigte Engelking die reale Bedrohung auf. So etwa der Fall des Universitätsklinikums Düsseldorf im Jahr 2020, bei dem ein Cyberangriff tragischerweise eine Todesfolge nach sich zog. Cyberkriminelle nehmen dabei nicht nur Krankenhäuser selbst ins Visier, sondern auch deren IT-Dienstleister oder sogar einzelne Medizingeräte, die über Schnittstellen angreifbar sind.

Schwachstellen: E-Mail, USB-Sticks & veraltete Systeme

Einfallstore für Schadsoftware sind oft alltägliche Mittel: Phishing-Mails mit infizierten Anhängen oder präparierte USB-Sticks, die unbemerkt einen Schadcode ins System schleusen. Besonders gefährlich ist dabei, dass dieser Code häufig über Wochen oder gar Monate unentdeckt bleibt. Laut Engelking fallen immer noch rund 20 % der Empfänger von Phishing-Mails auf diese Täuschungen herein – ein alarmierender Wert.

Abb. 1: Dipl.-Ing. Frank Engelking

Dabei sind moderne Krankenhäuser längst komplex vernetzte Systeme – sogenannte „Smart Hospitals“. Ein solcher Betrieb ohne digitale Infrastruktur ist heute kaum noch vorstellbar. Doch genau hier liegt auch die Krux: Die Lebensdauer von IT-Komponenten und Medizingeräten ist begrenzt – meist auf fünf Jahre. Betriebssysteme wie Windows werden nach etwa zehn Jahren nicht mehr mit Sicherheitsupdates versorgt, was ihre Anfälligkeit für Angriffe drastisch erhöht.

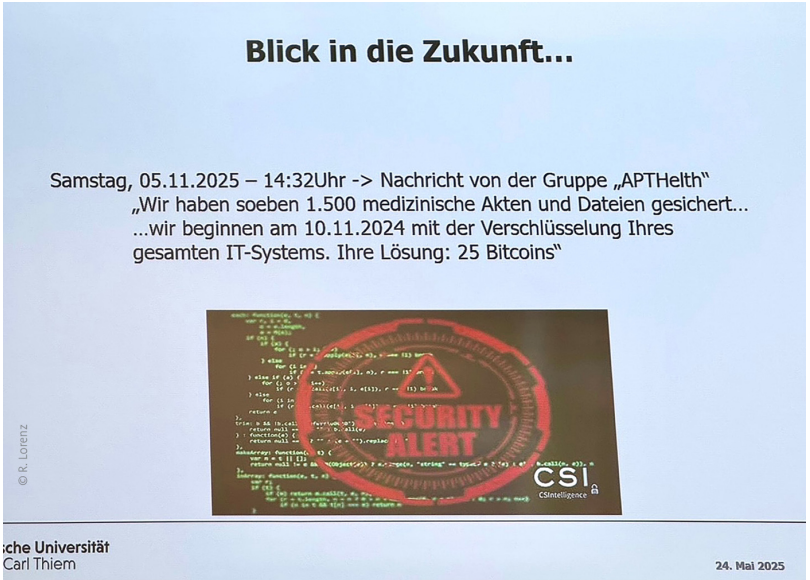

Abb. 2: Screenshot Vortrag von F. Engelkin

Enorme Schäden – und wenig Transparenz

Die Auswirkungen von Cyberangriffen sind vielfältig: Neben dem unmittelbaren finanziellen Schaden – etwa durch Betriebsausfälle oder Lösegeldforderungen – steht oft auch die Frage im Raum, ob der Klinik- oder Praxisbetrieb überhaupt weitergeführt werden kann. Wie viele Einrichtungen tatsächlich Lösegeld zahlen, bleibt in vielen Fällen im Verborgenen. „Es wird nicht darüber gesprochen – alles bleibt streng vertraulich", so Engelking. Seine klare Empfehlung: Niemals zahlen. Denn Erpresser wüssten genau, wo die Schmerzgrenzen der Betroffenen liegen.

Prävention: Sicherheit kostet – aber lohnt sich

Zur Prävention rät Engelking zunächst zu einer engen Abstimmung mit den eigenen IT-Dienstleistern. Cyberversicherungen können ergänzend sinnvoll sein – für eine Praxis kostet eine solche Police zwischen 500 und 2500 Euro jährlich. Darüber hinaus sind jedoch technische Schutzmaßnahmen unerlässlich: Firewalls, regelmäßige Backups, Systeme zur Angriffserkennung und die Überwachung von Kommunikationsstrukturen im Netzwerk.

Nicht zu unterschätzen sei auch das Nutzerverhalten: Passwörter sollten regelmäßig – etwa alle drei bis sechs Monate – geändert werden. Wichtig sei dabei weniger die Frequenz, sondern die Sensibilisierung der Mitarbeitenden für IT-Sicherheit. Denn: Sicherheit kostet Geld – aber ein erfolgreicher Angriff kann weitaus teurer werden.

Fazit

Die Digitalisierung bringt enorme Chancen für das Gesundheitswesen – aber auch ebenso große Herausforderungen. Cyberkriminalität ist keine abstrakte Bedrohung, sondern ein reales Risiko, das Krankenhäuser und Praxen mit aller Ernsthaftigkeit angehen müssen. Nur durch technische Schutzmaßnahmen, geschultes Personal und eine vorausschauende Sicherheitsstrategie: lässt sich sicherstellen, dass aus der Digitalisierung kein Desaster wird.

Die elektronische Patientenakte (ePA): Zwischen Testphase und flächendeckendem Rollout

In einem zweiten Vortrag referierte Frau Tina Peters, Sachgebietsleiterin IT in der Arztpraxis von der Kassenärztlichen Vereinigung Brandenburg (Abb. 3) über die elektronische Patientenakte ePA.

Abb. 3.: Ina Peters

Die Digitalisierung im deutschen Gesundheitswesen erreicht mit der elektronischen Patientenakte (ePA) eine neue Etappe. Seit dem 15. Januar 2025 läuft die erweiterte Testphase in ausgewählten Regionen: Hamburg, Franken und Nordrhein-Westfalen. Rund 250 Praxen und Institutionen beteiligen sich an diesem Pilotprojekt, dessen Ziel es ist, die ePA als zentrales digitales Element in der Patientenversorgung zu etablieren.

70 Millionen Datensätze wurden bereits verschlüsselt

Trotz der noch freiwilligen Nutzung seit dem offiziellen Start des freiwilligen Rollouts am 29. April 2025 wurden bereits 70 Millionen Patientendaten verschlüsselt. Die Anbieterstruktur ist dabei klar verteilt: Das Unternehmen Rise/BITMARK deckt rund ein Drittel des Marktes ab, während IBM mit zwei Dritteln Marktanteil den Löwenanteil stellt.

Abb. 4: Prof. Hartwig Riediger und Dr. Ralf Greese im Gespräch

Die Daten in der ePA sind verschlüsselt und nicht direkt für Krankenkassen zugänglich. Auch beim Zugriff durch medizinisches Fachpersonal gibt es klare Regelungen: Nur mit ausdrücklicher Einwilligung der Patienten dürfen Inhalte eingesehen werden. Das System arbeitet nach dem „Opt-out"-Prinzip, was bedeutet: Wer keine ePA wünscht, muss aktiv widersprechen. Für Kinder und Jugendliche unter 15 Jahren besteht keine Übermittlungspflicht.

Erste Funktionen verfügbar – Alltagstauglichkeit noch nicht erreicht

Zwar liegen mittlerweile erste positive Rückmeldungen aus den Testregionen vor, doch in der breiten Praxis gilt die ePA noch nicht als alltagstauglich. Viele Arztpraxen berichten von technischer Unsicherheit, unvollständigen Updates und noch nicht freigegebenen Systemen.

Kernstück der ePA ist derzeit die elektronische Medikationsliste (eML). Diese zeigt nicht nur, welche Medikamente ärztlich verordnet wurden, sondern dokumentiert auch die tatsächliche Einlösung der Rezepte. Damit bietet sie einen besseren Überblick über die tatsächliche Medikation eines Patienten. Ab dem Jahr 2026 soll zudem der elektronische Medikationsplan (eMP) eingeführt werden.

Weitere Funktionen sind bereits integriert, darunter elektronische Arztbriefe und Abrechnungsdaten. Auch privatversicherte Patienten – derzeit bei sechs privaten Krankenkassen – können optional eine ePA nutzen.

Sicherheit: Zwischen Gutachten und Kritik

Die Sicherheit der ePA wurde am 10. Oktober 2024 durch das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) im Rahmen eines abschließenden Gutachtens überprüft. Das Ergebnis fiel differenziert aus: Während die Kernmechanismen als sicher bewertet wurden, bestehen noch Lücken bei einzelnen Schnittstellen und in der Systemintegration in den Praxen.

Der Chaos Computer Club (CCC) hatte bereits am 27. Dezember 2004 potenzielle Angriffsszenarien öffentlich gemacht. Besonders kritisch wurden dabei Zugriffsmöglichkeiten über die Telematikinfrastruktur und mögliche Umgehungen von Sperrmechanismen, etwa durch kompromittierte Praxisausweise, bewertet.

Abb. 5: Dr. Stefan Kaiser

Ausblick: Verpflichtender Rollout ab Oktober 2025

Ab dem 01. Oktober 2025 soll die ePA verpflichtend für alle gesetzlich Versicherten eingeführt werden. Allerdings ist der Einfluss der Kassenärztlichen Vereinigungen (KV) auf die praktische Umsetzung begrenzt. Ob und in welcher Form es zu Sanktionen bei Nichtteilnahme kommen wird, ist derzeit noch nicht abschließend geklärt.

In Brandenburg wurden zunächst Referenzpraxen eingerichtet, um die Einführung zu begleiten und Probleme frühzeitig zu identifizieren. Ein umfassendes Update zur ePA ist abrufbar, jedoch sind noch nicht alle Systeme freigegeben oder vollständig getestet. Auch die Pflegeeinrichtungen sollen künftig angebunden werden – aktuell ist das aber noch nicht umgesetzt.

Informationsangebote und Unterstützung

Für medizinisches Personal gibt es mittlerweile eine Vielzahl an Informationsplattformen und Unterstützungsangeboten, die Praxen bei der Einführung der ePA begleiten. Dennoch bleibt der Erfolg der digitalen Patientenakte stark von der praktischen Integration in den medizinischen Alltag abhängig – und von der Akzeptanz der Nutzer, sowohl auf Seiten der Patientinnen und Patienten als auch des Fachpersonals.

Im Fachteil der Frühjahrstagung 2025 referierten Prof. Dr. Hartwig Riediger aus der Klinik für Allgemein- und Viszeralchirurgie des Vivantes Klinikum Humboldt und Dr. Stefan Kaiser (Abb. 5) aus der Chirurgischen Praxis Kleinmachnow über eine aktuelle Kontroverse in der Hernienchirurgie: Die Rektusdiastase und Nabelhernie aus Sicht der Klinik und Praxis.

In einem weiteren Vortrag gab Dr. Fred Gätcke aus dem KMG Klinikum Nordbrandenburg, Zentrum für Unfall-, Handchirurgie und Orthopädie aus Kyritz, einen interessanten Einblick in die Endoprothetik an der Hand.

Es entstand eine angeregte Diskussion der Teilnehmer mit den Referenten. Alles in allem war es dadurch eine überaus gelungene Veranstaltung, auch wenn die Teilnehmerzahl der Frühjahrstagung 2025 leider unter unseren Erwartungen blieb.

Lorenz R: Mehr Sicherheit in der Chirurgie? Passion Chirurgie. 2025 Juli/August; 15(07/08): Artikel 04_02.

Autor des Artikels

Dr. med. Ralph Lorenz

1. Vorsitzender des BDC LV|Berlin
Havelklinik Berlin
3+CHIRURGEN
Klosterstr. 34/35
13581 Berlin
> kontaktieren