Veranstaltungsrückblick

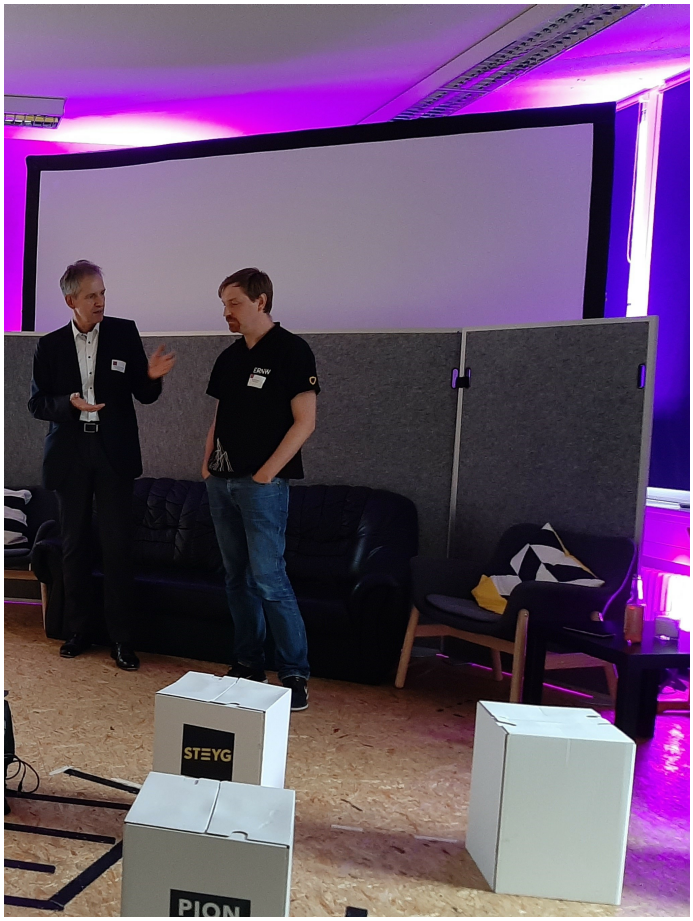
Digitale Gesundheit 360° – Datensicherheit in der digitalen Gesundheitswelt

Auf der zweiten Veranstaltung der Reihe Digitale Gesundheit 360° des Vereins DG-BW Digitale Gesundheit Baden-Württemberg e.V. drehte sich dieses Mal alles um Sicherheit in der Praxis- und Klinik-IT. Welche Sicherheitslücken es gibt und wie diese entstehen können, diskutierten Experten aus verschiedenen Bereichen der Gesundheitsversorgung am 24. September 2019 in Stuttgart.

Dass Datensicherheit in Kliniken erst genommen werden muss, weiß man spätestens, seit Anfang 2016 ein Trojaner das Neusser Lukaskrankenhaus lahm legte. Und wie es mit dem Datenschutz um elektronische Gesundheitsakten (eGA) bestellt ist, zeigten Sicherheitsexperten Ende 2018 am Beispiel der eGA vivy. Mit dem Thema „Datenschutz und Datensicherheit im Krankenhaus und im Datenaustausch mit Praxen" der zweiten Veranstaltung der Reihe „Digitale Gesundheit 360°" wurde daher ein Nerv sowohl bei Patientenvertretern wie auch bei Ärzten und Krankenhaus-IT getroffen.

„Wir wollen diese Themen kontrovers diskutieren", sagt Prof. Dr. Mark Dominik Alscher, Vorsitzender des Vorstands des Vereins DG-BW Digitale Gesundheit Baden-Württemberg e.V. in seiner Begrüßung. „Datenpannen passieren, umgekehrt muss man sehen, an welcher Stelle Entwicklungen durch hohe Sicherheitsstandards ausgebremst werden", so Alscher.

Gut durchdachtes Sicherheitssystem



Den Einstieg machte Florian Grunow, IT-Sicherheitsexperte der Heidelberger ERNW Enno Rey Netzwerke GmbH, mit seinem Keynote-Vortrag. Der Sicherheitsexperte beleuchtet zunächst die von der gematik GmbH konzipierte Telematikinfrastruktur und die dazugehörenden Funktionen, die elektronische Gesundheitskarte (eGK) und die elektronischen Patientenakten (ePA). Dabei spricht er positiv über die hohen Sicherheitsspezifikationen, die die gematik für den Konnektor, der die IT-Systeme medizinischer Einrichtungen mit der Telematikinfrastruktur verbindet, festgelegt hat. Isoliert betrachtet sei das Sicherheitssystem hier gut durchdacht. Grunow sieht jedoch ein Problem bei der Wartung der Konnektoren. Ferner stellten die sogenannten elektronischen Gesundheitsakten (eGA) ein Sicherheitsrisiko dar, da diese häufig sehr schnell und auch mit Sicherheitslücken auf den Markt gekommen waren.

Für Kliniken sieht er jedoch ein Sicherheitsrisiko in sogenannter Ransomware. Die auch Verschlüsselungstrojaner genannte Schadsoftware ermöglicht Dritten den Zugriff auf die Computer der Klinik. Infiziert werden die Computer dabei zum Beispiel über E-Mail-Anhänge. Die Ransomware verschlüsselt das befallene System. Cyberkriminelle fordern im Anschluss Lösegeld für die Entschlüsselung. Mittlerweile sind die Schadsoftwaren für die Kliniken zu einem Problem geworden. So waren zum Beispiel im Juli 2019 von der Trägergesellschaft Süd-West des Deutschen Roten Kreuzes 13 Krankenhäuser betroffen (1). Dabei gehe es immer um

Prof. Dr. Mark Dominik Alscher begrüßt Florian Grunow, ERNW Enno Rey Netzwerke GmbH, zu seinem Keynote-Vortrag.
© DG-BW, Foto: Dr. Ariane Pott

Geld, also die Erpressung der Kliniken, die ohne das Computersystem nicht weiterarbeiten können. Denn obwohl aus der Sicht eines jeden einzelnen Patienten die Daten der Patientenakte ein sehr schützenswertes Gut seien, haben diese auf dem Schwarzmarkt in Deutschland nur einen geringen monetären Wert.

In IT-Sicherheit investieren

Ein weiteres Problem in der Sicherheit entstehe durch fehlendes Know-How, zum einen auf der Seite der Hersteller von Medizingeräten. So ist bei modernen Medizingeräten zum Beispiel eine Online-Wartung möglich. Doch die damit einhergehende hohe Komplexität des Systems steigere auch die Angriffsfläche, die sich für Hacker biete. Hier sieht Grunow die Hersteller der Medizinprodukte in der Pflicht, diese Sicherheitslücken zu schließen. Dass Kliniken für Sicherheits-Updates bezahlen müssen, sei völlig undenkbar. Die Botschaft am Ende des Vortrags ist klar: „Investieren Sie in einem vernünftigen Ausmaß in Sicherheits-IT!“

Security ist wie Müll rausbringen

In der Runde diskutieren Bärbel Handlos, Dr. Lennart Jahnke, Markus Koffner, Florian Grunow und Prof. Mark Dominik Alscher (v.l.n.r.) über die Sicherheit im digitalen Gesundheitswesen.
© DG-BW, Foto: Dr. Ariane Pott

Die anschließende Diskussionsrunde gemeinsam mit den Experten Bärbel Handlos, Geschäftsführerin des Gesundheitstreffpunkts Mannheim, Dr. Lennart Jahnke, Geschäftsbereichsleiter IT am Universitäts-Herzzentrum Freiburg - Bad Krozingen, und Markus Koffner, Leiter für regionales Vertragswesen Techniker Krankenkasse, zeigt, dass Sicherheitsmaßnahmen zwar nicht hoch im Kurs stehen, aber dennoch notwendig sind. Patientenvertreterin Handlos sieht die fehlenden Sicherheitsmaßnahmen auch als Resultat einer erforderlichen Wirtschaftlichkeit der Krankenhäuser. Ferner seien eine Ausbildung und Sensibilisierung des Personals ein weiterer wichtiger Schritt. Medizininformatiker Lennart Jahnke sieht auch ein Problem in fehlendem Know-how, allerdings bei den Medizinprodukteherstellern. Denn diese hätten als Ingenieure nicht die Erfahrung mit IT-Themen.

Jahnke und Alscher machen aber deutlich, dass Betreiber Kritischer Infrastrukturen seit 30. Juni 2017 den Regelungen des IT-Sicherheitsgesetzes unterliegen. Dazu gehören neben den ursprünglichen Bereichen Energie, Informationstechnik und Telekommunikation sowie Ernährung und Wasser auch der Sektor Gesundheit. In der sogenannten KRITIS (Kritische Infrastruktur)-Verordnung werden die KRITIS-Betreiber verpflichtet, die von ihnen benötigte IT nach dem Stand der Technik abzusichern und mindestens alle zwei Jahre überprüfen zu lassen. Um die entsprechenden Standards zu erreichen, stellt das Land Baden-Württemberg im Rahmen des Krankenhausstrukturfonds 120 Millionen Euro zur Verfügung, die auch Vorhaben zur IT-Sicherheit beinhalten. Zusätzlich kommen 10 Millionen Euro im Rahmen der Digitalisierung der Krankenhäuser hinzu. Jedoch seien die Mittel für die IT-Sicherheit immer sehr knapp. Markus Koffner weiß, welchen Fokus die Krankenkassen als Körperschaft des Öffentlichen Rechts auf die IT-Sicherheit legen. Dennoch sieht er ein Problem bei der Konzeption der IT-Sicherheit in den Kliniken, ein roter Faden fehle häufig. Man müsse die IT-Sicherheit mehr in die Digitalisierung mit einbeziehen, fasst Moderator Alscher die Diskussion zusammen, auch wenn man schon eine gute Grundlage mit den KRITIS-Vorgaben habe: „Security ist leider nicht fancy“, so der Mediziner. Der IT-Sicherheitsexperte bringt es auf den Punkt: „ Security ist wie Müll rausbringen“. Keiner will es machen, aber falls es nicht passiert, hat man große Probleme.

Der Verein Digitale Gesundheit Baden-Württemberg ist Veranstalter von „Digitale Gesundheit 360°“. © DG-BW, Foto: Dr. Ariane Pott

Auch die Koordinierungsstelle Telemedizin Baden-Württemberg war bei der Veranstaltung vertreten. © DG-BW, Foto: Dr. Ariane Pott

Florian Grunow erklärt, welche Möglichkeiten Hacker haben, um Schadsoftware in Krankenhäuser zu schleusen. © DG-BW, Foto: Dr. Ariane Pott

Fachbeitrag

10.10.2019
Ariane Pott

Weitere Informationen

DG-BW Digitale Gesundheit Baden-Württemberg e.V.
Geschäftsstelle
Theodor-Kutzer-Ufer 1-3
68167 Mannheim
Tel.: +49 (0)621/383-8190
E-Mail: info(at)digitale-gesundheit-bw.de

- Digitale Gesundheit Baden-Württemberg

Der Fachbeitrag ist Teil folgender Dossiers

Data-Mining: Neue Chancen für Medizin und Gesundheit

Big Data – das große Versprechen der neuen digitalisierten Welt

Veranstaltung: Digitale Gesundheit 360°

Hier finden Sie das Video zu der Veranstaltung Digitale Gesundheit 360° - Datenschutz und Datensicherheit im Krankenhaus und im Datenaustausch mit Praxen. © DG-BW