



Statement der DGK zur aktuellen Tatort-Folge „Kammerflimmern“

Der am 28.09. ausgestrahlte *Tatort* hat mit einem sehr zugespitzten Szenario gespielt: Implantierbare Defibrillatoren, die bei Personen mit einer Gefährdung durch einen plötzlichen Herztod durch bösartige Rhythmusstörungen eingesetzt werden, wurden gezielt gehackt bzw. manipuliert und wurden so zur tödlichen Gefahr für Patientinnen und Patienten. Die Deutsche Gesellschaft für Kardiologie – Herz- und Kreislaufforschung e. V. (DGK), versteht, dass eine solche Darstellung Ängste auslösen kann – gerade bei Menschen, die selbst ein Herzimplantat tragen.

Als Fachgesellschaft möchten wir klarstellen:

- Implantierbare Defibrillatoren sind sichere und lebensrettende Medizinprodukte. Sie werden weltweit millionenfach eingesetzt und retten täglich viele Leben. Allein in Deutschland werden jährlich etwa 20.000 (Stand: 2022) ICD-Eingriffe durchgeführt.
- Die im Film gezeigte Manipulation ist ein extrem überspitzt dargestelltes Szenario. In der Realität gelten strenge europäische und internationale Sicherheitsstandards für Medizinprodukte. Die Systeme sind so konzipiert, dass ein Fremdzugriff nahezu auszuschließen ist und bisher auch noch nie berichtet wurde.
- Cybersicherheit ist ein ernstzunehmendes Thema. Hersteller und Zulassungsbehörden arbeiten kontinuierlich daran, Geräte maximal gegen Fremdzugriffe abzusichern und entsprechende Schutzmechanismen weiterzuentwickeln.

Wir begrüßen, dass der Tatort die Aufmerksamkeit auf die zunehmende Bedeutung von IT-Sicherheit im Gesundheitswesen lenkt, gleichzeitig möchten wir betonen: Patientinnen und Patienten können Defibrillatoren vertrauen. Die Nutzen-Risiko-Bilanz ist eindeutig: Die Geräte retten Leben und sind sicher.

Prof. Dr. David Duncker, Leiter des Hannover Herzrhythmus Centrums an der Klinik für Kardiologie und Angiologie der Medizinischen Hochschule Hannover, Mitglied des Nukleus der Arbeitsgruppe Elektrophysiologie und Rhythmologie (AGEP) der Deutschen Gesellschaft für Kardiologie sowie e-Cardiology-Experte, ordnet ein: „In der Realität ist das Risiko eines gezielten Hackerangriffs auf implantierbare Defibrillatoren – kurz ICDs – sehr unwahrscheinlich. Die Systeme sind durch mehrere Sicherheitsmechanismen geschützt, erfordern einen direkten physischen oder äußerst spezifischen digitalen Zugang, und die Hersteller arbeiten kontinuierlich an der Weiterentwicklung und Aktualisierung der Sicherheitssysteme.“

Fazit: Während Cybersicherheit im medizinischen Bereich zurecht zunehmende Aufmerksamkeit erhält, besteht für Trägerinnen und Träger von Herzimplantaten kein Grund zur Sorge. Die bestehenden Schutzmechanismen und regulatorischen Anforderungen bieten einen hohen Sicherheitsstandard.



DGK.
Deutsche Gesellschaft für Kardiologie
– Herz- und Kreislaufforschung e.V.

Grafenberger Allee 100
40237 Düsseldorf
Tel +49 (0) 211 600 692 – 150
Fax +49 (0) 211 600 692 – 10
E-Mail presse@dgk.org
Web Herzmedizin.de

Mehr Einordnung zur Cybersicherheit bei Herzimplantaten gibt Prof. Duncker im [Interview](#) auf dem Informationsportal Herzmedizin.de.

Medienkontakt:

Deutsche Gesellschaft für Kardiologie
Pressesprecher: Prof. Dr. Michael Böhm (Homburg/Saar)
Pressestelle: Jill Graw, Tel.: 0211 600 692 967
presse@dgk.org

Über die DGK:

Die Deutsche Gesellschaft für Kardiologie – Herz- und Kreislaufforschung e. V. (DGK) mit Sitz in Düsseldorf ist eine gemeinnützige, wissenschaftlich-medizinische Fachgesellschaft mit knapp 13.000 Mitgliedern. Sie ist die älteste und größte kardiologische Gesellschaft in Europa. Ihr Ziel ist die Förderung der Wissenschaft auf dem Gebiet der kardiovaskulären Erkrankungen, die Ausrichtung von Tagungen, die Aus-, Weiter- und Fortbildung ihrer Mitglieder und die Erstellung von Leitlinien. Weitreichende Informationen für Ärztinnen und Ärzte sowie medizinisches Fachpersonal, aber auch für Nicht-Medizinerinnen und Nicht-Mediziner stellt die DGK auf Herzmedizin.de zur Verfügung.