Kein klarer Gesetzesentwurf für Vorfälle der Cyber-Sicherheit im Gesundheitswesen: Zeit für einen Gesundheitscheck

ENISA gibt Schlüsselempfehlungen bezüglich des Schutzes von eHealth-Diensten und Infrastrukturen heraus

Die potenzielle Auswirkung eines Ausfalls des Informationssystems eines Krankenhauses kann extrem sein. Ein Defekt oder der Ausfall medizinischer Geräte aufgrund von Remote-Hacking (z.B. via brachialer Kraft oder DoS-Angriffe) können beachtlich sein. Solche Vorfälle der Cyber-Sicherheit haben sich stark auf Gesundheitsdienstleistungen ausgewirkt, wo sie lebensbedrohliche Risiken mit sich bringen. Wichtig sind nicht nur die Auswirkungen auf den Patienten, sondern auch das Aufklären von Institutionen und Gesundheitssystemen zu Reputationsrisiken. Das Gesundheitswesen bewegt sich auf der politischen Agenda immer weiter nach oben und wird von den EU-Mitgliedsstaaten häufig als eine kritische Infrastruktur behandelt. ENISA hat mehr als 15 MS- und zwei EFTA-Staaten für eine Studie zusammengeführt, um die Maßnahmen der Politiker und des privaten Sektors zu identifizieren, die diese ergreifen sollten, um die Sicherheit und Flexibilität von eHealth-Systemen zu verbessern. Diese Studie fokussiert drei weit verbreitete echte Fälle, nämlich elektronische Patientenakten, nationale eHealth-Dienste (zum Beispiel ePrescription) und Cloud-Dienste, welche eHealth-Systeme unterstützen.

Der Geschäftsführer von ENISA, Udo Helmbrecht, kommentierte diesen Bericht: „Die Komplexität und Abhängigkeiten von eHealth-Systemen wachsen stetig. Das Dasein von Rechtschaffenheit und Vertraulichkeit von eHealth zu sichern ist eine Herausforderung für Anbieter und Begünstigte. ENISA strebt an, mit allen Stakeholdern zusammenzuarbeiten um die Sicherheit und Privatsphäre aller eHealth-Infrastrukturen und Dienste zu erweitern.“

Der Bericht empfiehlt, *inter alia*, dass:

- Nationale Verwaltungen der Cyber-Sicherheit sollten kritische Werte von eHealth erkennen und Risikobeurteilungen mit Blick auf mildernde Risiken austragen
- Politiker sollten grundlegende Richtlinien für Cyber-Sicherheit für eHealth-Infrastrukturen und Dienste vorstellen
- eHealth-Betreiber sollten zusammen mit Personen des öffentlichen Sektors einen Mechanismus zum Teilen von Informationen aufsetzen, um gute Kenntnisse und Praktiken bezüglich Gefahren und Schwachstellen weiterzugeben

Diese Befunde wurden durch eine hohe Anzahl an Experten aus dem privaten sowie öffentlichen Sektor in einem offenen Workshop[1] bestätigt, welcher zusammen mit der Europäischen Kommission am 30. Oktober 2015 organisiert wurde.

Neue Technologien, wie zum Beispiel Cloud Computing, Smart-Geräte und das Internet of Things, bieten bereits die Innovationen, die Laufwerke von eHealth benötigen. Während die Herausforderungen für Cyber-Sicherheit neben den Diensten in 2016 immer mehr wachsen, wird ENISA sich auf die Einführung von Cloud Computing durch Dienstleister des Gesundheitswesens konzentrieren und Analysen bezüglich Smart-Krankenhäusern austragen.

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2015/ehealth-workshop

Für den ganzen Bericht

Für technische Informationen: Dimitra Liveri, NIS Experte, Dimitra.liveri@enisa.europa.eu

Für Interviews und Presseanfragen kontaktieren Sie bitte **press@enisa.europa.eu, Tel.** +30 2814 409576