

**Offener Brief des IKRK Generaldirektors Robert Mardini und des  
DRK Generalsekretärs Christian Reuter**

---

**Deutsches Rotes Kreuz e.V.**

**Vorstand**

Carstennstraße 58  
12205 Berlin  
Tel. +49 30 85404-0  
www.DRK.de  
Generalsekretaer@DRK.de

Durchwahl  
030 85404-274  
Fax  
030 85404-474

**Präsidentin**  
Gerda Hasselfeldt

**Vorsitzender des Vorstands**  
Christian Reuter

Berlin, 31.01.2022

**Die Daten der Schwächsten der Welt zu hacken ist ein Skandal**

Der jüngste Cyberangriff auf die Daten von 515.000 Menschen im Bereich der humanitären Hilfe war ein Affront gegen die Menschlichkeit und eine Gefährdung derjenigen, die bereits unter den Auswirkungen von Krieg und Katastrophen leiden.

Dazu gehören Menschen, die durch Konflikte, Migration und Naturkatastrophen von ihren Familien getrennt wurden, vermisste Personen und ihre Familien sowie Inhaftierte. Diese Daten stammten von Menschen weltweit, die ihre privaten Informationen einem humanitären Netzwerk anvertraut hatten, dessen Hilfe sie dringend benötigten.

Diese Verantwortung haben wir nicht leichtgenommen. Das IKRK ist sich schon lange der Gefahr bewusst, dass unsere Daten eines Tages Ziel eines Angriffs sein könnten. Aufgrund der zunehmenden Bedrohung durch Angriffe auf die Cybersicherheit haben wir in den letzten Jahren eine Vielzahl von Verbesserungen vorgenommen und mit bewährten Partnern zusammengearbeitet, um hohe Standards für den Datenschutz und die Systeme zu gewährleisten.

Dieser Angriff zeigt jedoch, dass diese Systeme gegen ausgeklügelte Cyber-Operationen nicht immun sind. Und ebenso wie humanitäre Helfer nicht von Konfliktparteien ins Visier genommen werden sollten, sind auch humanitäre Daten zu respektieren und nur für humanitäre Zwecke zu verwenden.

Ein Cyberangriff bedeutet oft Gewinneinbußen oder die Offenlegung von Kreditkartendaten. In diesem Fall könnten diese Daten dazu verwendet werden, extrem schutzbedürftigen Personen, einschließlich unbegleiteter Kinder, Schaden zuzufügen. Dieser Angriff verletzt ihre Privatsphäre, ihre Sicherheit und ihr Recht auf humanitären Schutz und Hilfe.

Der Angriff hat auch die Fähigkeit unseres globalen Netzwerks beeinträchtigt, vermisste Personen zu finden und Familien wieder zusammenzuführen. Ein aktuelles Beispiel ist der jüngste Vulkanausbruch und die durch den Tsunami ausgelöste Überflutung im pazifischen Inselstaat Tonga. Unsere Aufgabe, besorgten Familien und vermissten Personen zu helfen, wurde erschwert. Das gilt auch für unsere Sucharbeit in Konfliktgebieten, z. B. für vor der Gewalt fliehende Menschen in Afghanistan.

Etwa 60 nationale Rotkreuz- und Rothalbmondgesellschaften haben derzeit keinen Zugang zu den Daten, die sie in dieses globale System eingespeist haben, und können deshalb nicht auf die Akten von Migranten zugreifen, die vor Konflikten, Katastrophen oder extremer Hungersnot fliehen. Glücklicherweise wurden bei dem Angriff keine Daten gelöscht. Unsere Teams arbeiten an der Einrichtung von Übergangssystemen, die uns die Fortsetzung dieser wichtigen Arbeit ermöglichen.

Was uns heute am traurigsten stimmt, ist die Gefahr, das Vertrauen der Menschen zu verlieren, die unsere Hilfe brauchen, und das privat und vertraulich. Wir suchen nach Wegen, um Personen, auf deren Daten möglicherweise zugegriffen wurde, zu informieren und die Schritte zu erläutern, die wir unternehmen, um ihre Daten in Zukunft zu schützen.

Dieser Vorfall ist der jüngste in einem besorgniserregenden Trend, bei dem Krankenhäuser und humanitäre Einrichtungen in den letzten Jahren zum Ziel von Angriffen auf die Cybersicherheit wurden. Cyberangriffe richteten sich auf medizinische Einrichtungen in Ländern wie Frankreich, Spanien, Thailand, der Tschechischen Republik, Südafrika und den Vereinigten Staaten. Aufgrund dieser Angriffe kann es dazu kommen, dass Operationen verschoben und kritische Patienten an andere Orte verlegt werden müssen. Angriffe haben die Analyse von COVID-19-Tests verzögert.

Gemeinsam müssen wir uns klar positionieren: Cyberoperationen und Angriffe auf medizinische Einrichtungen, humanitäre Daten und Organisationen sind gefährlich, inakzeptabel und rechtswidrig.

Die Rotkreuz- und Rothalbmondbewegung strebt danach, das Beste zu sein, was die Menschheit zu bieten hat. Wir helfen Menschen in den schlimmsten Situationen und bewahren ihre Würde. Dieser Angriff beschädigt die wichtige Arbeit, zu der wir alle einen Beitrag leisten.

Und an die Menschen, deren Daten gehackt wurden: Wir wissen, dass Sie uns persönliche Informationen und Details über traumatische Ereignisse in Ihrem Leben anvertraut haben. Sie sollen wissen, dass wir unser Möglichstes tun, um die von uns angebotenen Dienstleistungen weltweit wiederherzustellen. Wir werden alles daransetzen, Ihr Vertrauen zu stärken, damit wir Sie auch in Zukunft weiter unterstützen können.

**Robert Mardini**  
Generaldirektor  
Internationales Komitee vom Roten Kreuz

**Christian Reuter**  
Generalsekretär  
Deutsches Rotes Kreuz e.V.