Schnell auf **Hackerattacken reagieren**

Hacker spähten Anfang 2022 personenbezogene Daten aus, die das Internationale Komitee vom Roten Kreuz für seinen Suchdienst gespeichert hatte. Das DRK rüstete nach dem **Cyberangriff** auf.

Das Internationale Komitee vom Roten Kreuz (IKRK) war Anfang 2022 Opfer eines massiven Hackerangriffs, der auch den Suchdienst des DRK sowie Hunderttausende Schutzbedürftige weltweit getroffen hat. Mit dem DRK-Suchdienst unterstützen wir seit über 150 Jahren gemeinsam mit dem IKRK und 191 weiteren Nationalen Rotkreuz- und Rothalbmond-Gesellschaften Menschen, die durch bewaffnete Konflikte, Katastrophen, Flucht, Vertreibung oder Migration von ihren Nächsten getrennt wurden. Die Zusammenarbeit dieses internationalen Suchdienst-Netzwerks hilft dabei, Angehörige wieder miteinander in Kontakt zu bringen und Familien zu vereinen. Dabei ist es unerlässlich, die persönlichen Daten vermisster Personen und ihrer suchenden Angehörigen zu erheben und zu verarbeiten.

515 000 Hilfesuchende betroffen

Im Januar 2022 stellte ein externer Anbieter von Servern des IKRK in der Schweiz einen gezielten Cyberangriff fest. Unbekannte hatten sich unberechtigt Zugang zu wichtigen, vom IKRK gehosteten IT-Anwendungen verschafft, die das internationale Suchdienst-Netzwerk zur Erfüllung seiner Aufgaben nutzt. So wurden personenbezogene Daten von mehr als 515 000 Hilfesuchenden weltweit ausgespäht, die etwa 60 Rotkreuz- und Rothalbmond-Gesellschaften zu Suchdienstzwecken dort gespeichert hatten. Etwa 62 000 stammten vom DRK-Suchdienst. Die Daten gehören vermissten Menschen, deren suchenden Angehörigen, voneinander getrennten Familien und weiteren Personen, die von der Rotkreuz- und Rothalbmond-Bewegung unterstützt werden, zum Beispiel Menschen in Haft. Außerdem extrahierten die Hacker auch Zugangsdaten von Mitarbeitenden des DRK-Suchdienstes auf allen Verbandsebenen.

Unmittelbar nach Bekanntwerden des Angriffs haben das IKRK und die betroffenen Rotkreuz- und Rothalbmond-Gesellschaften zusammen mit Datenschutz- und IT-Experten reagiert. Wir haben alle betroffenen Systeme des IKRK unverzüglich abgeschaltet, um einen weitergehenden unbefugten Zugriff auf die Daten zu verhindern. Wichtige Elemente der Suchdienst-Infrastruktur, wie die Website www.tracetheface.org, waren daraufhin monatelang offline. Wir haben mögliche Risiken für die Rechte und Freiheiten betroffener Personen analysiert, um geeignete Maßnahmen zur Abwendung etwaiger Schäden für diesen Personenkreis zu entwickeln. Darüber hinaus haben wir unsere internen Systeme, die nicht mit denen des IKRK verbunden waren, zusätzlich vor unberechtigtem Zugriff gesichert.

Die Betroffenen haben wir gemäß Artikel 34 der Datenschutz-Grundverordnung (DSG VO) soweit möglich per Brief und darüber hinaus auch öffentlich auf der Suchdienst-Website über den Vorfall informiert. Wir haben die Informationen für die Betroffenen in zwölf Sprachen sowie zusätzlich in leichter Sprache veröffentlicht und aktualisieren sie stetig. Grundlage waren die Mitteilungen des IKRK. In den DRK-Suchdienst-Beratungsstellen bundesweit stehen Ansprechpersonen bereit, um Fragen von betroffenen Klientinnen und Klienten zu beantworten und bei Bedarf an die Datenschutzbeauftragte des DRK-Suchdienstes weiterzuleiten. Auch den Bundesbeauftragten für Datenschutz und Informationsfreiheit haben wir umgehend konsultiert. Schließlich beauftragte das IKRK ein spezialisiertes IT-Sicherheitsunternehmen, den Vorfall zu untersuchen und die digitalen Systeme zukünftig noch besser abzusichern.

Die Hackerattacke hat große Betroffenheit in der gesamten Rotkreuz- und Rothalbmond-Bewegung ausgelöst. Der Schutz von persönlichen Details über sensible Ereignisse, die uns Hilfesuchende in der Beratung anvertrauen, ist essenziell für unsere Arbeit. Deshalb bemühen wir uns darum, unsere digitalen Systeme stets auf dem aktuellen Stand der Technik zu halten und so vor einem unbefugten Zugriff Dritter zu schützen. Mit Verhaltensregeln für den Umgang mit diesen Informationen bauen wir zusätzlich Vertrauen auf. Wir informieren die Hilfesuchenden transparent über unseren Umgang mit personenbezogenen Daten und über ihre Rechte zum Schutz dieser Daten. Hierzu nutzen wir zum Beispiel ein mehrsprachiges Video sowie Zeichnungen, die den Suchdienst-Mitarbeitenden die Erklärung erleichtern. Dieses Informationsangebot wird ergänzt um mehrsprachige Hinweisblätter zum Datenschutz. Auch online sind die Datenschutzgrundsätze für Suchdienst-Mitarbeitende einsehbar.

Dialog für besseren Schutz

Die Motive für den Cyberangriff sind bis heute ebenso wenig bekannt wie die dafür Verantwortlichen. Die Hacker haben die gestohlenen Daten weder manipuliert noch gelöscht und nach aktuellem Kenntnisstand bislang nicht veröffentlicht. Der bestmögliche Schutz der Schutzbedürftigen hinter diesen Daten bleibt unsere oberste Priorität. So setzt sich die Rotkreuz- und Rothalbmond-Bewegung gemeinsam mit anderen unparteiischen humanitären Organisationen weltweit für einen besseren Schutz humanitärer Daten ein, etwa mit den Datenschutzverhaltensregeln ‚Restoring Family Links' von 2015. Die neue Resolution ‚Safeguarding Humanitarian Data' von 2022 des Delegiertenrats zielt darauf ab, mit allen Teilen der Rotkreuz- und Rothalbmond-Bewegung in den Dialog mit Staaten und anderen Akteuren zu treten. Dies soll sicherstellen, dass unparteiische humanitäre Organisationen online genauso geschützt sind wie offline. Das Rote Kreuz wird alles daransetzen, das Vertrauen der Schutzbedürftigen zu stärken, um sie in Zukunft weiter unterstützen zu können.

Iris Mitsostergios
ist Referentin in der Suchdienst-Leitstelle im DRK-Generalsekretariat.
iris.mitsostergios@drk.de
Frauke Weber
ist Suchdienst-Datenschutzbeauftragte des DRK.
frauke.weber@drk.de

Sofortmaßnahmen für den Ernstfall

- betroffene Systeme abschalten, um weiteren Zugriff zu verhindern
- noch nicht betroffene Systeme abtrennen und sichern
- Schäden und Folgerisiken analysieren und gezielte Maßnahmen entwickeln
- Betroffene des Datenleaks sowie zuständige Behörden informieren

„Das Thema Lösegeld **ist sehr heiß diskutiert.“**

Sozialunternehmen können gegen Hackerschäden eine **Versicherung** abschließen. Was versicherbar ist und wie viel der neue Schutz kostet, erklärt Frank Schultz vom Versicherungsmakler Ecclesia.

Hackerangriffe auf Einrichtungen der Sozialwirtschaft, darunter viele Krankenhäuser, häufen sich. Wie hoch ist die jährliche Schadenssumme für die Branche?

Unsere Zahlen decken sich im Wesentlichen mit den Daten, die der Gesamtverband der Deutschen Versicherungswirtschaft veröffentlicht. Der Verband zählte deutschlandweit im Jahr 2021 rund 3700 Schäden durch Hackerangriffe. Dafür leisteten Versicherer rund 137 Millionen Euro. Das ist fast dreimal so viel wie 2020. Zahlen für die Sozialwirtschaft lassen sich nicht nennen, da Cyberschäden Bestandteil unterschiedlicher Versicherungen sein können.

Frank Schultz
arbeitet im Produktmanagement bei Ecclesia und ist TÜV-zertifizierter Fachberater für Cyber-Risiken.
info@ecclesia-gruppe.de

Welche Schäden eines Hackerangriffs sind versicherbar?

Bei einem erfolgreichen Hackerangriff haben Unternehmen keinen Zugriff mehr auf ihre Daten, da diese oft vollständig verschlüsselt worden sind. Ein ambulanter Pflegedienst hat beispielsweise in so einem Fall keinen Zugriff mehr auf Patientendaten und kann die Menschen nicht mehr vernünftig versorgen. Das ist der klassische Betriebsunterbrechungsschaden. Das heißt, es können keine Erlöse erwirtschaftet werden, aber die Kosten laufen weiter. Das ist mit Abstand bei allen Schadensfällen die größte Kostenposition, die versicherbar ist. Unternehmen brauchen nach einem Angriff auch Experten, die Geld kosten. Sie schauen, wie die Täter ins System gekommen und welche Bereiche betroffen sind. Ein großer Aufwand ist dann auch, die Daten und die Infrastruktur wiederherzustellen. Für all das bietet die Cyberversicherung Bausteine.

Was ist nicht versicherbar?

Unsere speziell konzipierten Absicherungskonzepte basieren auf einer umfassenden Absicherung der möglichen finanziellen Risiken. Nicht zu versichern sind letztlich nur Daten und Programme, die sich im Arbeitsspeicher des Computers befinden sowie Daten, für die keine Nutzungsberechtigung vorliegen oder nicht betriebsfertige Programme. Auch vorhersehbare Schäden, zum Beispiel durch geplante Abschaltungen, sind nicht zu versichern.

Ersetzt eine Cyberversicherung auch an Hacker gezahltes Lösegeld?

Das lässt sich nicht einfach mit Ja oder Nein beantworten. Das Thema Lösegeld ist sehr heiß diskutiert. Anfangs enthielten nahezu alle Versicherungen einen Baustein, der Lösegeld übernommen hat. Das setzte aber erhebliche Anreize für Hacker, denen man das Geld ja quasi gleich direkt