Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

16.02. 2022

Cyberangriff auf das IKRK: Bekanntgabe der Ergebnisse unserer Analyse

Von PPS

Cyberangriff auf das IKRK: Bekanntgabe der Ergebnisse unserer Analyse

(Genf)(PPS) Offener Brief von Robert Mardini, Generaldirektor des Internationalen Komitees vom Roten Kreuz (IKRK), nach der Entdeckung eines Cyberangriffs Mitte Januar auf Server des IKRK, auf denen Daten im Zusammenhang mit dem Programm der Rotkreuz- und Rothalbmondbewegung zur Zusammenführung getrennter Familien gespeichert sind.

Vor einem Monat haben wir beim Internationalen Komitee vom Roten Kreuz (IKRK) festgestellt, dass Server mit personenbezogenen Daten von über 515 000 Menschen weltweit gehackt wurden.

Unsere Teams haben alles in ihrer Macht Stehende getan, um zu verstehen, wie dieser Angriff passieren konnte, welche Auswirkungen er hat, wie wir unsere Sicherheitssysteme verbessern können und wie wir Fakten zu dieser für die uns zum Schutz und zur Unterstützung anvertrauten Menschen bedauerlichen Situation kommunizieren können.

Es ist unsere Verantwortung als humanitäre Organisation, die ihren Partnern und den Menschen, für die sie sich einsetzt, rechenschaftspflichtig ist, alles zu diesem inakzeptablen Angriff zu teilen.

Heute möchten wir im Rahmen unseres entschiedenen Engagements für die Menschen, die wir schützen und unterstützen wollen, weitere Informationen zu

diesem Angriff teilen. Auf diese Art bemühen wir uns, das ununterbrochene Vertrauen der Menschen zu gewinnen.

Lassen Sie mich zunächst eine Tatsache unterstreichen: Es war ein ausgeklügelter Cyberangriff – eine kriminelle Handlung - auf sensible humanitäre Daten. Wir wissen, dass es sich um einen zielgerichteten Angriff gehandelt hat, weil die Angreifer einen Code geschaffen haben, der nur zur Ausführung auf den betroffenen IKRK-Servern entwickelt wurde – eine Technik, von der wir glauben, dass sie entwickelt wurde, um die Aktivitäten der Hacker vor einer Erkennung und vor anschliessenden kriminaltechnischen Untersuchungen abzuschirmen.

Die Angreifer sich eine Schwachstelle zunutze gemacht, die hat keines unser Cyberabwehrsysteme entdeckt hat, und, nachdem sie in unser Netzwerk eingedrungen sind, haben sie Techniken eingesetzt, mit denen sie sich selbst als legitime Nutzer ausgeben konnten. Als dieses Eindringen entdeckt wurde, haben wir umgehend entsprechende Änderungen an einigen unserer Prozesse und Werkezuge vorgenommen und beschleunigen die Umsetzung der bereits geplanten Massnahmen im Rahmen unseres Programms zur Verbesserung der Cybersicherheit.

Es ist keine angenehme Aufgabe, solche Informationen bekanntzugeben, aber ich bin davon überzeugt, dass wir nur durch Transparenz mit Blick auf die Herausforderungen von den Angreifern lernen und unsere Richtlinien und Praktiken verbessern können.

Wir arbeiten eng mit unseren Partnern in den Nationalen Rotkreuz- und Rothalbmondgesellschaften weltweit an Massnahmen zusammen, wie wir die Menschen, deren Daten gehackt wurden, bestmöglich informieren. Die oberste Priorität ist derzeit, mögliche Risiken, die sie möglicherweise zu befürchten haben, abzufedern. Wir tun dies anhand von Telefonanrufen, Hotlines, öffentlichen Bekanntmachungen, Briefen und in einigen Fällen im Rahmen von persönlichen Besuchen in abgelegenen Gegenden.

Zu den Betroffenen gehören vermisste Personen und ihre Familien, Inhaftierte und andere Personen, die infolge von bewaffneten Konflikten, Naturkatastrophen oder Migration Leistungen von der Rotkreuz- und Rothalbmondbewegung erhalten. Wir haben es geschafft, sicherzustellen, dass die wichtige Arbeit zur Auffindung vermisster Angehöriger fortgesetzt werden konnte, wenngleich auf minimalem Niveau und mit Low-Tech-Lösungen (beispielsweise unter Einsatz einfacher Tabellen),

während wir daran arbeiten, die umfassenden Leistungen mit verbesserten Sicherheitsfunktionen wiederherzustellen.

Die Arbeit im Rahmen von Naturkatastrophen und an den Frontlinien birgt echte Risiken. Der neutrale und unparteiliche Ansatz der Bewegung ist entscheidend, um unsere Arbeit sicher durchführen zu können. Wir haben Kontakt mit Regierungsbehörden und bewaffneten Gruppierungen, um die Gefahren für das Personal und die Freiwilligen der Bewegung, medizinische Einrichtungen, Fahrzeuge und andere Sachwerte zu minimieren. Wir verfolgen in der digitalen Welt denselben Ansatz wie in der realen Welt – und wir dürfen weder in der einen, noch in der anderen zum Ziel werden.

Es ist unsere Hoffnung, dass dieser Angriff auf die Daten bedürftiger Menschen als Katalysator für einen Wandel dient. Wir werden nun unsere Kontakte mit Regierungen und nicht-staatlichen Akteuren intensivieren, um ausdrücklich zu verlangen, dass der Schutz des humanitären Auftrags der Rotkreuz- und Rothalbmondbewegung sich auch auf unsere Daten und unsere Infrastruktur erstreckt. Wir sind davon überzeugt, dass es entscheidend ist, einen echten Konsens zu erreichen – in Worten und Taten -, wonach humanitäre Daten nie angegriffen werden dürfen.

Lassen Sie mich zum Abschluss den Menschen, die wir unterstützen, und unseren Partnern in der Rotkreuz- und Rothalbmondbewegung, die uns ihre Daten anvertrauen, Folgendes sagen: Ich bedauere zutiefst, dass Ihre Daten bei diesem inakzeptablen Angriff kompromittiert wurden. Ich verspreche Ihnen, dass wir alles in unserer Macht Stehende tun werden, um den Schutz unserer Daten heute und künftig zu verbessern, und – was noch entscheidender ist – uns für den Schutz humanitärer Einsätze in der digitalen Welt einzusetzen.

Pressekontakt:

International Committee of the Red Cross
avenue de la Paix 19
1202 Geneva

Ewan Watson, IKRK Genf (Englisch, Französisch, Spanisch), ewatson @ icrc.org
Jason Straziuso, IKRK Genf (Englisch), jstraziuso @ icrc.org
Crystal Wells, IKRK Genf (Englisch), cwells @ icrc.org

Kategorie
IT & Software & Neue Medien