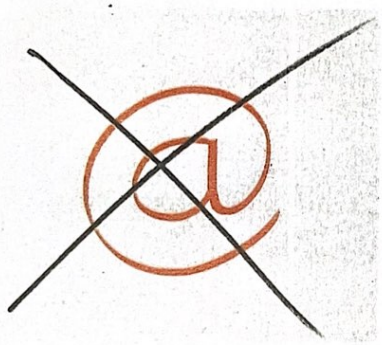
Sozialcourage 1 | 2023

Bei uns eingetroffen am 3.3.2023

Eine Cyberkrise, die Chancen bietet

Cyberattacken auf karitative Einrichtungen häufen sich, die Kriminellen werden immer professioneller. Auch den Caritasverband für München und Oberbayern traf es, ein Hackerangriff hat dessen IT-Infrastruktur außer Gefecht gesetzt – vorübergehend.



Text – Bettina Bäumlisberger

Es geschah mitten hinein in die letzten Vorbereitungen für den Festakt anlässlich des 100-jährigen Bestehens des Caritasverbands der Erzdiözese München und Freising e. V.: Cyberkriminelle legten die zentrale IT-Infrastruktur lahm. Kommunikation, Planung und Dokumentation waren erheblich eingeschränkt. Der Betrieb der 350 Dienste und Einrichtungen lief trotz der IT-Großstörung weiter, die Prozesse wurden gesichert. Die Behebung des weitreichenden Schadens führte allerdings zu einer vorübergehenden Umstellung auf analogen Betrieb.

Hochprofessionelle, kriminelle Angreifer hatten sich Ende August 2022 über einen Link in einer E-Mail mit einem Virus Zugang zu Servern und Netzwerk des Caritasverbands verschafft. Mithilfe eines Trojaners konnten sich die Kriminellen zwei Wochen im IT-Haus der Caritas umschauen, Systeme ausspähen, Daten stehlen und verschlüsseln. Erst am 10. September, einem Samstag, hinterließen die Cyber-Kriminellen auf einem Caritas-Server eine Nachricht mit einer hohen Lösegeldforderung. Sofort wurde das IT-Haus verriegelt, damit nichts und niemand mehr hineinkommt. Aber es kamen dann auch keine Daten mehr heraus. Alles, was über das Caritas-Netzwerk, mit Caritas-Software, auf einem Dienst-Rechner und zentral über Server erarbeitet, erledigt und abgespeichert worden war, war nicht mehr zugänglich.

Der Caritas-Vorstand etablierte einen Krisenstab und erstattete Anzeige. Externe Cyber-Spezialisten und Beamte der Ermittlungsbehörden kamen als Berater an Bord. Der Vorstand des Caritasverbands München-Freising entschied sich gegen die Zahlung des Lösegeldes, weil es im rechtsfreien Raum der Organisierten Kriminalität keine Verbindlichkeit und schon gar keine Garantie gibt, dass die Cyberkriminellen die Daten anschließend nicht doch noch in die Öffentlichkeit streuen. Öffentlichkeit, Klienten und Partner wurden über die Medien, Briefe, Telefonate und die Webseite informiert, die nicht gehackt worden war. FAQ (Frequently Asked Questions) wurden rasch auf die Webseite gestellt.

Den eigentlichen Betrieb konnte der Angriff nicht zum Stillstand bringen. Die Kerntätigkeit der Caritas ist analog, nicht digital: Dienst am Menschen eben. An erster Stelle stand stets, die karitative Arbeit für die uns anvertrauten Menschen in den Altenheimen, in den Kitas und Werkstätten sowie in der Sozialberatung aufrecht zu erhalten. Schwierig genug – ohne Computer, ohne Datenleitungen, anfangs teilweise ohne Telefon und Drucker. In der stationären und ambulanten Pflege konnte zum Glück auf analoge Papier-Dokumentationen zurückgegriffen werden. Zudem war es in den ersten Wochen nach dem Angriff wichtig, betriebswirtschaftliche Prozesse wie in der Finanzbuchhaltung wieder aufzubauen, um die Liquidität zu wahren.

„Die Caritas ist auch in der Krise stark, das lehrt ihre 100-jährige Geschichte. Und keine Krise, die nicht auch eine Chance bietet: So beschleunigen wir aktuell unseren digitalen Transformationsprozess. Wir stellen nicht einfach nur unsere alte IT-Struktur wieder her, sondern wir bauen ein neues, modernes und zukunftsfähiges, robustes und sichereres IT-Haus auf", so Caritasdirektor Prof. Hermann Sollfrank. Und wir sind auch schon eingezogen. Alle ca. 5.000 Mitarbeitenden, die schon vor der Cyberattacke einen persönlichen E-Mail-Account hatten, sind wieder mit einen Caritas-eigenen E-Mail-Konto versorgt. Einziger Unterschied: Die Adressen enden nun auf @caritasmuenchen.org, nicht mehr auf .de.

Ein erster großer Meilenstein im Wiederaufbau der IT-Umgebung. Doch es bleibt noch viel zu tun. So müssen alle Endgeräte und Daten gereinigt werden, d. h. sie werden „gewaschen" und neu installiert. Zudem müssen Anwendungen und Programme angebunden, Schnittstellen definiert werden. Priorität beim Aufbau der alternativen IT-Infrastruktur hat, uns künftig vor weiteren Cyberangriffen zu schützen. Natürlich war auch bisher der Standard unserer IT-Sicherheit hoch, aber auch die Fähigkeiten der Angreifer sind groß. Daher sind neben technischen Schutzsystemen auch Schulungen für die Mitarbeitenden wichtig. Sie müssen wissen, wie sie mit verdächtigen E-Mails oder Dateien umgehen sollen. Entscheidend im Kampf gegen die Cyberkriminalität sind Sensibilisierung und Aufmerksamkeit.