Brandschutz ist in den Einrichtungen etabliert, doch gezielte Notfallübungen für den Fall von Cyberangriffen? Sie sind ähnlich brenzlig wie Feuer, das in Windeseile Werte zerstören kann.

Bild **dpa/pa, Hans Wiedl**

Der Knackpunkt

Soziale Organisationen sind ein zunehmend beliebtes Ziel von Cyberangriffen – vor allem wegen der Fülle an besonders sensiblen, personenbezogenen Daten. Wie es um IT-Sicherheit im sozialen Bereich steht und wie sich die Caritas besser schützen kann, zeigt ein Blick auf die jüngsten Vorfälle.

Text **Thomas Althammer**

Die Bedrohung durch Cyberangriffe auf Unternehmen und Organisationen ist nicht mehr wegzudiskutieren. In den vergangenen zwölf Monaten waren deutschlandweit 81 Prozent aller Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen, meldet der Branchenverband Bitkom. Der durch digitale Angriffe verursachte Schaden sei damit um 29 Prozent gestiegen und liege auf einem neuen Rekordhoch in Höhe von über 223 Milliarden Euro. Diese Angriffe richten sich zunehmend auch gegen Wohlfahrtsverbände wie Caritas, Diakonie und andere soziale Einrichtungen, die selten über die gleichen Sicherheitsressourcen wie große Unternehmen verfügen. Aber: Im Rahmen der eigenen Mittel und Möglichkeiten in Cybersicherheit zu investieren, ist besser, als abzuwarten. »

„In den vergangenen zwölf Monaten waren 81 Prozent der Unternehmen betroffen“

Quelle: **Bundeskriminalamt: Bundeslagebild Cybercrime 2023**

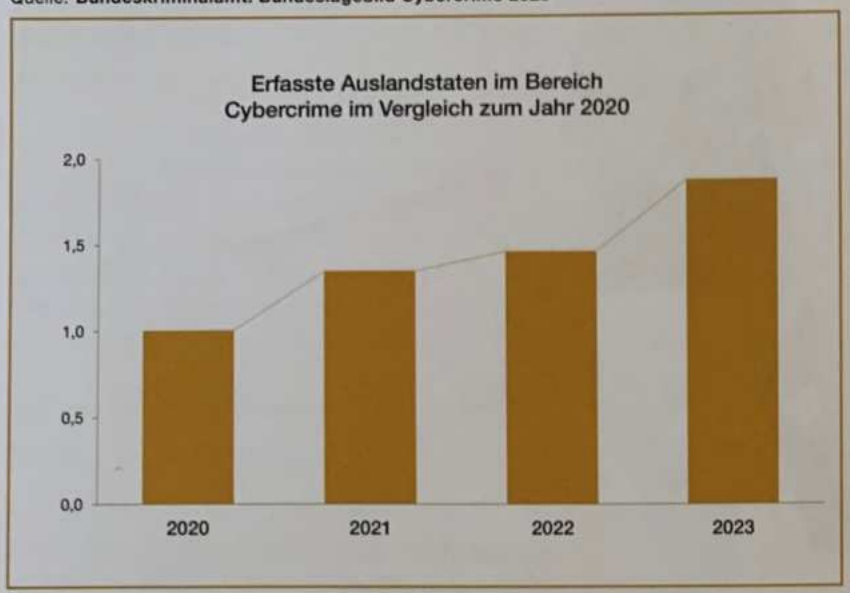

Abbildung: In den Jahren 2020 bis 2023 hat sich die Fallzahl der erfassten Auslandstaten im Bereich Cybercrime beinahe verdoppelt. Im Vergleich zu 2022 ist die Zahl 2023 um 28 Prozent gestiegen.

Wer auf die Bedrohungslage durch Cyberkriminelle mit einem reflexartigen „Bei uns gibt es nichts zu holen" reagiert, irrt: Denn wer die Fälle beobachtet, erkennt einen alarmierenden Trend von Cyberangriffen im Gesundheits- und Sozialbereich, der durch neue KI-Technologien künftig noch befeuert werden wird. Allein im Frühjahr 2024 waren dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zufolge die Universitätsklinik Mainz, die Zentrale der Katholischen Jugendfürsorge der Diözese Augsburg und die Kassenärztliche Vereinigung Hessen von Cyberkriminalität betroffen.

Soziale Einrichtungen rücken in den Fokus von Cyberkriminellen

Die Ziele der Cyberkriminellen sind in der Regel, an sensible Daten zu gelangen, Firmennetzwerke zu infiltrieren, lahmzulegen und Geld zu erpressen oder Identitäten zu stehlen. Hacker nutzen die Unachtsamkeit oder Unwissenheit der Nutzenden, dringen durch Schlupflöcher in veralteter Hard- und Software ein, identifizieren neue Schwachstellen in aktueller Software oder nutzen Lücken, die dem Software-Betreiber noch nicht bekannt sind (sogenannte Zero Day Exploits), und spähen gezielt Personen aus.

Cyberkriminelle sind dabei in der Regel keine nerdigen Einzelpersonen, sondern hochprofessionelle Täter(-gruppen). Sie verfügen über enorme Ressourcen, immer neue Angriffsstrategien zu entwickeln und diese auszuführen. Die vom Bundeskriminalamt festgestellten Inlandsdelikte verharren nach einem Höhepunkt 2021 auf weiterhin hohem Niveau (2023 knapp 135.000 Fälle). Die Delikte, bei denen die Täter im Ausland sitzen, steigen allerdings stetig (siehe Abbildung).

Wohlfahrtsverbände und soziale Einrichtungen warten gleich mit mehreren attraktiven Gründen auf, die Potenzial für Cyberangriffe bieten:

Erstens verfügen soziale Organisationen über eine hohe Dichte an besonders sensiblen, persönlichen Daten. Um eine vollumfängliche Versorgung und Pflege der Kundinnen und Kunden zu gewährleisten, werden schließlich viele Daten erhoben, verarbeitet und gespeichert. Nicht nur Namen und Wohnort, auch medizinische Daten, Kontoinformationen oder Sozialversicherungsnummern. Beim bereits erwähnten Angriff auf die Katholische Jugendfürsorge der Diözese Augsburg wurden beispielsweise sensible Daten von mehr als 20 Krankenhäusern und sozialen Einrichtungen gestohlen, wie der bayerische Rundfunk meldete. Zu den entwendeten Informationen gehörten Personaldaten, Finanzdaten sowie Patienten- und Gesundheitsdaten.

Zweitens haben soziale Einrichtungen häufiger nur geringe Ressourcen für Informationstechnologie. Aufgrund dieser schmalen Budgets arbeiten soziale Einrichtungen in der Regel nicht auf Systemen, die dem neuesten Stand der Technik entsprechen. Erschwerend kommt hinzu, dass Systeme mitunter nicht oder zu spät aktualisiert werden, Konfigurationslücken aufweisen sowie nicht voneinander abgegrenzt sind. Dadurch können sie zu einem Einfallstor werden. Bei einem Angriff auf den katholischen Sozialdienstleister SKM in Düsseldorf wurden 2022 durch eingeschleuste Schadsoftware Teile der Daten verschlüsselt und kopiert, hieß es seinerzeit in einer Stellungnahme. Dass nötige Sicherheitsstrategien nicht oder zu spät umgesetzt werden, liegt unter anderem an einer unzureichenden Refinanzierung zum Beispiel im Rahmen von Pflegesatzverhandlungen. Die Mittel für IT und Cybersecurity bei Sozialunternehmen sind schlicht zu knapp bemessen.

Drittens erschweren die gängigen Bedingungen der Sozialwirtschaft einheitliche Sicherheitsstandards. Dezentrale Strukturen, die Fülle an Systemen und Fachanwendungen und die zunehmende Vernetzung mit externen Playern sorgen dafür, dass es eine Vielzahl an virtuellen Verflechtungen mit Partnern, Einrichtungen und Zulieferern gibt. Vor einem Hackerangriff erfolgt in der Regel eine strukturierte Informationserhebung: über die Organisation, die Zielperson, das Netz-

werk und vieles mehr. Wenn sich Angreifende unbemerkt innerhalb des Netzwerks bewegen und (vernetzte) Systeme und Daten angreifen können, spricht man von lateralen Bewegungen. Das bedeutet, dass ein Zugriff auf ein IT-System auch den Zugang zu verknüpften Systemen ermöglichen kann – mit potenziell katastrophalen Folgen für Netzwerke. Beim Cyberangriff gegen die Caritas der Erzdiözese München-Freising im Jahr 2022 (mehr dazu ab Seite 15 in diesem Heft) waren Medienberichten zufolge mehr als 350 Dienste und Einrichtungen mit etwa 10.000 Mitarbeitenden betroffen. Der Schaden belief sich auf 23 Millionen Euro.

Viertens scheint es immer noch an der Sensibilität für die Bedrohungslage zu fehlen. Die rasante Digitalisierung in allen Branchen geht in der Sozialwirtschaft traditionell langsamer voran. Denn im Zentrum der Arbeit sozialer Einrichtungen steht der Mensch. Aber: Ist der Umgang mit Technologie bei Mitarbeitenden nicht geschult und sind Bedrohungsszenarien wie Malware, Phishing oder Identitätsklau nicht bekannt, ist der Mensch das schwächste Glied in der Kette. Auch in technikaffineren Wirtschaftssektoren sehen 66 Prozent der befragten Firmen der KPMG-Studie „e-Crime in der Deutschen Wirtschaft 2024" zufolge ein mangelndes

Cybersicherheit

Cyber-Feuerwehr für Mitglieder im Caritasverband

Seit dem 1. November 2024 bietet das Caritas-Netzwerk IT allen Mitgliedern des Deutschen Caritasverbands den IT-Sicherheitsservice „Incident & Response" an – als Cyber-Feuerwehr in Notfällen. Denn: Cyberattacken sind in der modernen und vernetzten Welt eine große Bedrohung für das Überleben von Organisationen.

Was bedeutet „Incident & Response"?

Ähnlich wie die Feuerwehr im Ernstfall sofort eingreifen muss, um im Brandfall Schlimmeres zu verhindern, bietet der „Incident & Response"-Service eine schnelle und professionelle Reaktion bei IT-Sicherheitsnotfällen. Mit einer Hotline und bis zu 100 Stunden Expertenhilfe pro Vorfall unterstützt der gemeinsame Dienstleister SVA betroffene Organisationen sehr zeitnah, um mögliche Schäden zu minimieren und zu helfen, sich in einer entsprechenden Notsituation richtig zu verhalten.

Der Dienst im Überblick

- **24/7-Hotline: Das SVA-Expertenteam ist rund um die Uhr erreichbar – sieben Tage die Woche, 24 Stunden am Tag.**
- **Optimal vorbereitet: Gemeinsam führt SVA die Kunden in einem professionellen Onboarding in die Unterstützung ein, so dass diese alle technischen und organisatorischen Maßnahmen vorbereiten können, die für eine effektive Unterstützung im Notfall benötigt werden. So liegen in einer Notsituation bereits alle wichtigen Informationen bereit.**
- **Kosteneffizient: Für Mitglieder im Caritas-Netzwerk IT kostet der Service nur einen Euro brutto pro Vollzeitäquivalent und Monat. Nichtmitglieder (aus dem Caritas-Bereich) zahlen 1,50 Euro pro Vollzeitäquivalent und Monat.**

Erfolgreicher Start im Oktober 2023

Seit Oktober 2023 haben bereits zahlreiche Mitglieder im Caritas-Netzwerk IT vom „Incident & Response"-Service profitiert und sind erfolgreich durch IT-Krisen gekommen.

» **Mehr erfahren: Bei Interesse oder weiteren Fragen wenden Sie sich bitte an: Gerhard Müller, E-Mail: gerhard.mueller@caritas-netzwerk-it.de** Gerhard Müller, *Community-Manager im Caritas-Netzwerk IT*

Sicherheitsverständnis ihrer Mitarbeitenden als großes Risiko.

Die langfristigen Folgen eines Cyberangriffs sind nicht nur finanzieller Natur. Soziale Einrichtungen haben bei solchen Vorfällen auch mit Vertrauensverlusten der Klient:innen zu rechnen. Darüber hinaus kann die Arbeitsfähigkeit betroffener Organisationen stark eingeschränkt werden. Die Notwendigkeit einer robusten Cybersicherheitsstrategie wird daher immer dringlicher. Auch vor dem Hintergrund weiterer gesetzlicher Rahmenbedingungen.

Umsetzung rechtlicher Bedingungen belastet Budgets zusätzlich

Neue gesetzliche Rahmenbedingungen im Zusammenhang mit der fortschreitenden Digitalisierung treffen auch die Sozialwirtschaft. Als rechtliche Grundlage hat die Sozialwirtschaft dabei vor allem diese Gesetze zu berücksichtigen: die Datenschutz-Grundverordnung (DSGVO) in Verbindung mit dem Bundesdatenschutzgesetz (BDSG) beziehungsweise die kirchlichen Datenschutzgesetze für Einrichtungen von Diakonie und Caritas. Alle Gesetze stammen aus einer Zeit, als KI und Maschinelles Lernen noch nicht so weit verbreitet waren und in der heutigen Form zur Verfügung standen.

Da aber gerade diese Technologie das Potenzial hat, Prozesse zu beschleunigen, um gerade im Fachkräftemangel für Entlastung zu sorgen, braucht es neue Regelungen. Die jüngst verabschiedete KI-Verordnung (Ai Act) der Europäischen Union ist daher zukünftig parallel zu den bekannten Datenschutzgesetzen anzuwenden, was Auswirkungen auf die Rechte von Betroffenen hat.

Daneben sind Gesundheitsdatennutzungsgesetz (GDNG), das Hinweisgeberschutzgesetz (HinSchG), das Lieferkettensorgfaltspflichtengesetz (LkSG) und die Umsetzung der europäischen „Network und Information Security Directive 2" (NIS-2) in nationales Recht zu beachten. Hoher bürokratischer und finanzieller Mehraufwand droht, der vielfach nicht finanziert ist.

So können sich soziale Organisationen schützen

Geringe Budgets und Fachkräftemangel sind Fakt. Trotzdem lohnt es sich, Cybersicherheit auf die Agenda zu heben und Maßnahmen zu priorisieren. Dafür müssen soziale Organisationen sich zunächst fragen: Welche Systeme müssen besonders geschützt werden und haben ein hohes Risiko, von außen angegriffen zu werden? Ressourcen sollten zuerst zum Schutz der kritischen Systeme mit sensiblen Daten investiert werden, um die Auswirkungen eines Angriffs zu minimieren. Erst danach folgen budgetabhängig alle weiteren Anwendungen.

Damit ein leckgeschlagenes Schiff nicht unmittelbar untergeht, werden im Schiffsbau Schotten eingezogen, die geschlossen werden können, um die betroffenen Bereiche so zu isolieren, dass der Schaden begrenzt wird. Dieses Prinzip sollten soziale Organisationen auch bei IT-Systemen berücksichtigen, da so bei Schadensereignissen die anderen Systemkomponenten nicht mit betroffen sind. Diese Segmentierung von Netzwerken bedeutet, dass einzelne Systeme und Bereiche voneinander getrennt betrieben werden und Freigaben untereinander auf ein Mindestmaß beschränkt sind. Konkret ist das eine Abkehr vom Prinzip „Stadtmauer", hin zu mehreren dezentralen Schutzsystemen. Gelingt ein Angriff in einem Bereich oder einer Einrichtung, soll ein leichter Übersprung auf andere Unternehmensbereiche verhindert werden. Bei einer Ransomware-Attacke sind somit nicht alle IT-Systeme gleichzeitig angreifbar und das Schadensmaß wird reduziert. Dabei gilt es immer abzuwägen, dass Sicherheitshürden die Arbeit und den Komfort für Nutzerinnen und Nutzer nicht zu sehr einschränken.

Regelmäßige Schulungen zu Cybersicherheit sind entscheidend, um auf gängige Bedrohungslagen wie Malware, Phishing und das Ausspähen von Personen aufmerksam zu machen. Deshalb sollten soziale Organisationen ihr Personal als „Human Firewall" stärken. Wenn Sicherheitsbewusstsein und Sicherheitskultur gefördert werden, können Einrichtungen ihre Resilienz gegenüber Cyberbedrohungen deutlich erhöhen. Im Hinblick auf den Umgang mit Anwendungen, die auf Künstlicher Intelligenz basieren, verschreibt die Europäische Union Organisationen, die diese Technologie nutzen, über den Ai Act die Pflicht, Kompetenzen bei den eigenen Mitarbeitenden aufzubauen (Artikel 4 KI-Verordnung). NIS-2 schreibt Pflichtschulungen für die Geschäftsführung vor.

Neben einer allgemeinem Sensibilisierung brauchen soziale Organisationen auch klare Regeln. Eindeutige Richtlinien beispielsweise geben Mitarbeitenden die notwendige Orientierung und Sicherheit. Damit einhergehen sollte, dass eine offene Kommunikation

„Soziale Einrichtungen müssen bei Cyberangriffen auch mit Vertrauensverlust rechnen"

gefördert wird. Fehler sind menschlich, und gut organisierte Angriffe sind nicht immer abzuwehren. Kommt es zu einem Fehler, etwa wenn Zugangsdaten fälschlicherweise preisgegeben wurden, sollte den Mitarbeitenden Unterstützung bei der Beseitigung angeboten werden. Denn nur so lassen sich Angriffe wirklich aufdecken.

Neben klaren Regeln hilft es auch, ein übliches Vorgehen als „Best Practice" zu etablieren. Verwendete Software beispielsweise sollte regelmäßig aktualisiert werden, um Sicherheitslücken zu schließen. Dazu ist es wichtig, sich einen Überblick über die verwendeten Systeme in der eigenen Organisation zu verschaffen – auch und gerade über sogenannte Schatten-IT, also Software, die ohne Wissen von Verantwortlichen implementiert wurde. Verantwortlichkeiten und Fristen zur Aktualisierung von Systemen müssen klar geregelt sein.

Zu guter Letzt sollten sich soziale Organisationen ernsthaft mit dem Worst Case auseinandersetzen. Denn es ist nicht die Frage, ob ein Cyberangriff passiert, sondern wann. Sozialunternehmen sollten davon ausgehen, dass es früher oder später Sicherheitsvorfälle geben wird. Es muss sowohl um die Stärkung der Verteidigungslinien als auch um das Notfallmanagement gehen. Dazu gehört beispielsweise eine regelmäßige gründliche Überprüfung von Backups mit einem vollständigen Test auf Wiederherstellbarkeit. Durch die Simulation von Ausfällen kann so ein Ernstfall durchgespielt werden.

Schutz vor Cyberkriminalität

Handlungsempfehlungen für soziale Organisationen

1. Risiken bewerten, Prioritäten setzen
Welche Systeme haben ein hohes Risiko? Eine Priorisierung auf dieser Grundlage definiert, welche Systeme besonders und daher als Erstes geschützt werden.

2. Netzwerke segmentieren
Indem einzelne IT-Systemkomponenten voneinander getrennt werden, kann bei Attacken der Schaden auf einzelne Bereiche begrenzt werden. Andere Systeme bleiben dann idealerweise unberührt.

3. Mitarbeitende sensibilisieren und schulen
Regelmäßige Schulungen zu Cybersicherheit stärken das Sicherheitsbewusstsein und helfen, Bedrohungen wie Phishing und Malware abzuwehren. Der Aufbau von Kompetenzen ist auch bei KI-basierten Anwendungen Pflicht.

4. Richtlinien erstellen
Klare Richtlinien bieten Orientierung und Sicherheit. Offene Kommunikation bei Fehlern ermöglicht es, Sicherheitsvorfälle schneller aufzudecken.

5. Best Practices implementieren
Regelmäßige Software-Updates schließen Sicherheitslücken. Die Verantwortung und die Fristen für Updates sollten festgelegt und als Best Practice etabliert sein.

6. Auf den Ernstfall vorbereiten
Vorbereitung auf Cyberangriffe durch Notfallmanagement, regelmäßige Backup-Tests und Angriffs-Simulationen verbessern die Resilienz.

7. Zusammenarbeit mit externen Partnern
Angesichts steigender Cyberbedrohungen werden gezielte Investitionen in Informationssicherheit notwendig. Dafür brauchen soziale Organisationen starke Partnerschaften.

Soziale Organisationen brauchen starke Partner

Soziale Einrichtungen stehen vor der Entscheidung, ihre begrenzten finanziellen Mittel klug einzusetzen. Langfristig wird klar: Es wird immer wichtiger, in Cyber- und Informationssicherheit zu investieren. Diese Investitionen sind angesichts der steigenden Anzahl von Cyberangriffen auf Wohlfahrtsverbände entscheidend, um Arbeitsfähigkeit und Existenz sozialer Organisationen zu sichern.

Auf die stetig steigende Bedrohung durch Cybercrime müssen Unternehmen und Organisationen aus allen Branchen Antworten finden. Diese können aber nicht lauten, dass möglichst auf digitale Anwendungen verzichtet wird. In einer digitalen, vernetzten Welt wäre das fatal. Es ist Zeit für proaktives Handeln und gezielte Investitionen, um die Resilienz sozialer Organisationen deutlich zu erhöhen.

Thomas Althammer
Geschäftsführer Althammer & Kill GmbH & Co. KG
E-Mail: ta@althammer-kill.de