

Kirkel

Krise kontrolliert bewältigt

[17.10.2025] Die saarländische Gemeinde Kirkel konnte einem Cyberangriff technisch erfolgreich begegnen – auch dank der Unterstützung umliegender Kommunen. Die offene Kommunikation mit der Öffentlichkeit trug ebenfalls zum kontrollierten Umgang mit dem Angriff bei.

Wie geht man als kleine Kommune mit einem Cyberangriff um? Dieser Frage musste sich die saarländische Gemeinde [Kirkel](#) (rund 10.000 Einwohner) Anfang dieses Jahres stellen, als ein Cyberangriff die Verwaltung lahmlegte. „Die Angreifer haben sich Zugriff auf die Systeme verschafft, Daten extrahiert und einen Ransomware-Angriff gestartet“, schildert Julian Gebhardt, Leiter der IT in der Gemeindeverwaltung Kirkel, das Szenario aus technischer Sicht. „Die Schutzmechanismen der Firewall haben gegriffen, und dies ist direkt bei den täglichen Kontrollen aufgefallen.“ Betroffen gewesen seien Domänen-Controller und File Server, so der IT-Chef.

Der Angriff zog eine ganze Reihe von Konsequenzen nach sich: Die Gemeinde wurde unmittelbar „vom Netz“ genommen und alle notwendigen Stellen über den Cyberangriff informiert – so die Zentrale Ansprechstelle Cybercrime (ZAC) beim saarländischen Landeskriminalamt und der Versicherungsträger der Gemeinde. Hier hatte man sich – eine Entscheidung mit Weitblick – schon frühzeitig gegen solche Angriffe versichert.

In der Folge wurden Spuren des Cyberangriffs sowohl von einem Team der ZAC als auch von der Versicherung gesichtet und sichergestellt. Im Anschluss erfolgte die Planung für einen kompletten Wiederaufbau der IT-Systeme und deren Wiederherstellung. Julian Gebhardt sagt mit Blick auf den Stand heute: „Alle IT-Systeme wurden gehärtet, alle festgestellten Lücken geschlossen.“ An ihrer Seite wusste die Gemeinde dabei mit der Firma HJP Datentechnik aus Kirkel einen verlässlichen Partner.

Kommunikation mit der Öffentlichkeit

Dass man recht schnell den technischen Folgen des Cyberangriffs erfolgreich begegnen konnte, habe auch an der Unterstützung umliegender Kommunen gelegen, macht Kirkels Bürgermeister Dominik Hochlenert deutlich. „Die kommunale Familie hat hier zusammengehalten.“

Der technische Aspekt des Cyberangriffs und dessen Folgen auf die Einsatzbereitschaft der Kirkeler Gemeindeverwaltung waren aber nur ein Teil der Geschichte. Konnte man im Rathaus schon sehr zügig wieder ein Höchstmaß an Arbeitsbereitschaft herstellen, wirkte der Cyberangriff aufgrund von entwendeten Daten nach. Vor allem, als die Hackergruppe nach einem ersten Hinweis im Darknet die Daten ohne weitere Vorwarnung veröffentlichte. Hatte schon der eigentliche Cyberangriff eine rechtskonforme Kommunikation mit der Öffentlichkeit erfordert, verschärfte sich die Situation durch den tatsächlichen Datenabfluss und dessen Veröffentlichung im Darknet weiter. In der Folge ging es darum, die Betroffenen – je nach Grad der Betroffenheit auf unterschiedlichen Wegen – rechtssicher zu informieren und die Pressearbeit im Wechsel zwischen aktiv und passiv zu steuern. Hier griff die Gemeinde auch auf die Unterstützung eines externen Kommunikationsspezialisten zurück.

Eben diese offene, aber immer anwaltlich begleitete Kommunikation, die auch vom externen Daten schutzbeauftragten unterstützt wurde, führte im Ergebnis zu einem gut kontrollierten Umgang mit dem Cyberangriff in der Öffentlichkeit.

Gegen Cyberangriffe versichert

Welches Fazit und welche Lehren zieht die Gemeinde Kirkel nun aus dem Vorfall, auch als Handlungshilfen für anderen Kommunen? „Es ist unerlässlich, eine entsprechende Versicherung gegen solche Cyberangriffe abzuschließen“, betont Bürgermeister Dominik Hochlenert. „Diese macht, gerade mit Blick auf den möglichen finanziellen Schaden, die Situation für eine Kommune handelbar. Auch ist es nötig, den engen Schulterschluss in der kommunalen Familie zu suchen – um hier auf Ressourcen zurückgreifen zu können, die man als kleine Kommune möglicherweise nicht hat.“ Und schließlich sei es unbedingt erforderlich, Notfallstrukturen zu schaffen, um möglichst schnell die Wiederherstellung der Arbeitsbereitschaft zu erreichen. Vorabplanungen für die Arbeit eines Krisenstabs gehörten hier ebenso zu den Aufgaben wie ein schlüssiges Kommunikationskonzept – sowohl nach innen als auch nach außen.

Gerade mit Blick auf die Innensituation einer Gemeinde unter der Last eines akuten Cyberangriffs macht Kirkels Bürgermeister Dominik Hochlenert zudem deutlich, dass es darum gehen müsse, in der Hochphase der Krisenbewältigung auch das Wohl der Mitarbeitenden im Blick zu haben – um Überbelastungssituationen und deren Folgen zu vermeiden.

()

Dieser Beitrag ist in der Ausgabe Oktober 2025 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Kirkel