Wie Hacker das Land lahmlegten

Illustration: Standard

Der Einsatz von Erpressungssoftware ist in der Pandemie immer lukrativer geworden. Für Kärntens Landesregierung bedeutet dies, dass kritische Zahlungen wie Beihilfen plötzlich nicht mehr automatisiert überwiesen werden können.

Muzayen Al-Youssef und Walter Müller

Als die Kärntner Landesregierung Anfang vergangener Woche per Livestream vor die Medien trat, um Fragen zum Hackerangriff auf die Kärntner Landesverwaltung zu beantworten, waren jene Hacker, die dafür verantwortlich sind, offenbar selbst anwesend. Sie drohten im Chat: Entweder zahlt Kärnten Lösegeld – fünf Millionen US-Dollar in Form von Kryptowährungen –, oder die Daten werden publiziert.

Das Land ist der Forderung nicht gefolgt. Nun tauchen häppchenweise Daten im Netz auf. An den Folgen arbeiten die IT-Experten des Landes mithilfe externer Experten nunmehr seit mehr als zwei Wochen praktisch rund um die Uhr. Mehrere zehntausend Personendaten waren bei dem Cyberangriff zumindest eingesehen worden: 80.000 Stammdatenblätter von Niederlassungs- und Aufenthaltsbewilligungen seit 1999, 4000 Kontaktdaten des Veranstaltungsmanagements und knapp 200 Gigabyte Daten aus internem Schriftverkehr von Regierungsmitgliedern und Mitarbeitern.

Angriff wie aus Lehrbuch

Alles begann – wie so oft – mit einer E-Mail. Ein Unternehmen habe ein Angebot, hieß es darin. Sie sah allen bisherigen E-Mails des vermeintlichen Absenders so ähnlich, dass jemand in der Kärntner Landesverwaltung sie ohne Bedenken öffnete. In Wahrheit handelte es sich um eine Phishing-Mail – eine Nachricht, die bewusst dem Aussehen einer E-Mail des vorgegaukelten Versenders nachempfunden wird. Tatsächlich ist sie mit einer Schadsoftware infiziert, die das Ziel hat, Zugriff auf das IT-System zu erlangen.

Für den Angriff verantwortlich, zeigte sich die Hackergruppe Black Cat. Kärnten ist bei weitem nicht ihr einziges Opfer: Auf ihrer Webseite prahlt die Gruppe, die wohl aus Russland stammt, etwa mit Angriffen auf andere Lokalregierungen weltweit sowie auch auf Konzerne aus verschiedensten Branchen. Ihr Geschäft mit Erpressungssoftware ist während der Pandemie immer lukrativer geworden. Und mit einem unbedachten Klick der Beamten war den Hackern der erste Schritt gelungen. Sie drangen in die IT-Systeme des Landes ein, verschlüsselten sie – und kommunizierten ihre Motive: Sie wollen Geld, sonst bleibt der Landesverwaltung künftig der Zugriff verwehrt.

Doch häufig reicht die Zahlung solchen Gruppierungen dann doch nicht. Also machte sich die Kärntner Landesregierung daran, den Angriff abzuwehren und ältere Back-ups der Systeme einzuspielen. Dabei hielt die Landesregierung sich anfangs zu den Hintergründen bedeckt. So wurde etwa zunächst ein Datendiebstahl dementiert, später wieder bestätigt. Wie ein Sprecher sagt, würden täglich Sicherungen erstellt. Allerdings brauche es Zeit, die IT-Infrastruktur wiederherzustellen. Diese war heruntergefahren worden, um zu verhindern, dass die Hacker in die Systeme eingreifen. Eine Person, die öfter mit solchen Angriffen konfrontiert ist, sagt, dass es Fälle gibt, in denen die Rückkehr zum Status quo Monate dauert.

Besonders kritisch ist die Situation allerdings für jene, die von den Diensten der Landesregierung finanziell abhängig sind. Betroffen von der Lahmlegung der Systeme waren zum Teil auch Landeszahlungen. Das Land verwaltet etwa Wohnbeihilfen, die Gehälter in der Landesverwaltung, aber auch die Grundversorgung für Geflüchtete in Kärnten. Ein Landessprecher betont, dass die meisten Zahlungen rasch oder leicht verzögert organisiert werden konnten. Sie erfolgten Anfang des Monats manuell. Die Systeme für eine automatisierte Zahlung stehen noch still.

Bei der Grundversorgung gab es hingegen andauernde Verzögerungen. Die Zahlungen soll nunmehr am Montag erfolgen. Das Geld werde nicht vollständig vom Land Kärnten zur Verfügung gestellt, weswegen eine Abstimmung erforderlich gewesen sei, sagt der Sprecher. Zudem sei eine andere Software im Einsatz als bei anderen staatlichen Geldern. „Pässe werden jetzt zum Beispiel außerhalb der Amtszeit ausgestellt, um ausgefallene Termine nachzuholen“, fügt er hinzu.

Dreifache Erpressung

Auch das Schulverwaltungsprogramm des Landes, das benötigt wird, um Zeugnisse auszustellen, ist derzeit lahmgelegt.

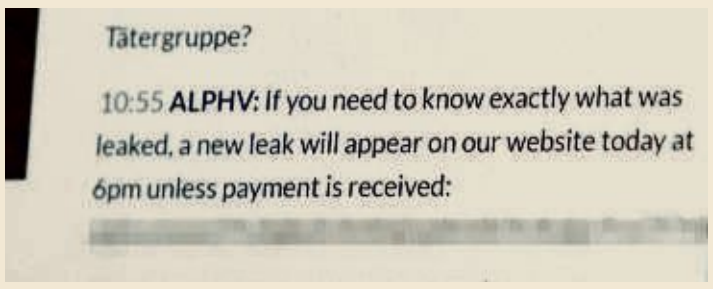

Foto: APA / Gert Eggenberger

Die Hackergruppe schleuste sich zu Beginn der Woche in den Live-Chat einer Pressekonferenz des Landes ein.

Die Rückkehr in die Normalität wird weiter erschwert, weil Black Cat auf eine Methode setzt, die sich besonders im vergangenen Jahr unter Erpressungssoftwaregruppen etabliert hat: die sogenannte „Triple Extortion“. Dabei belassen die Hacker es nicht dabei, bloß bestehende Daten zu verschlüsseln. Gleichzeitig setzen sie auf DDoS-Attacken: IT-Systeme werden durch eine hohe Anzahl an Zugriffen gezielt so überlastet, dass sie stillstehen.

Die Website des Amts der Kärntner Landesregierung werde seit dem Online-Gehen laufend mittels „Überlastungsangriffen“ attackiert, bestätigte ein Sprecher des Landespressedienstes am Wochenende. „Unsere nach Stand der Technik gesetzten Maßnahmen wehren diese Angriffe effektiv und erfolgreich ab, sodass die Services weiterhin verfügbar bleiben“, sagte der Sprecher.

Black Cats dritte Waffe sind die Daten selbst. Die Hacker drohen damit, alles, was sie erbeutet haben, online zu veröffentlichen. Im Netz kursieren derzeit zahlreiche derartige Datensätze, darunter etwa auch Reisepassausschnitte. Das Land Kärnten gab lange Zeit an, dass es sich bei den bisher geleakten Daten ausschließlich um Daten der Belegschaft in der Verwaltung handle.

Am Freitag räumte man dann ein, dass Stammdaten von tausenden Personen aufgetaucht seien, darunter von Politikern, aber auch von Bürgern. Man könne nicht garantieren, dass keine weiteren Daten veröffentlicht werden. Die forensischen Analysen seien noch im Gange. Seit dieser Woche gibt es für besorgte Personen eine eigene Hotline, bei der sie sich zum Thema informieren können – nicht aber darüber, ob sie betroffen sind. Eine gesonderte Nachricht an Betroffene soll noch folgen. Die Datenschutzbehörde bestätigt, dass die Meldung eines Datenvorfalls bei ihr eingelangt sei und derzeit ergänzt werde.

Unter den geleakten Informationen findet sich unter anderem auch ein Ausschnitt des Reisepasses eines Kindes. Auf Nachfrage beim Land Kärnten heißt es, dass es sich dabei um einen Verwandten eines Beamten handeln dürfte. Dieser habe das Bild wohl zu Privatzwecken auf seinem Arbeitsrechner gespeichert.

Und jetzt?

Doch was bedeuten die Leaks nun für jene, die betroffen sind? „Gerade wenn viele Daten bekannt sind, muss man mit Konsequenzen rechnen, von Identitätsdiebstahl bis hin zur Erpressung“, sagt Thomas Lohninger von der Datenschutz-NGO Epicenter Works. Betroffene können wenig gegen die Publikation tun: Erst wenn Daten missbraucht werden, können sie das anzeigen. Derzeit wird vor dem EuGH zu Schadenersatzforderungen aufgrund von Datenlecks prozessiert, allerdings sind Urteile noch anhängig.

„ Es hilft nicht, dass es für die öffentliche Hand nicht die Gefahr einer Strafe für den Verlust personenbezogener Daten gibt“, sagt Lohninger. Österreich sei nicht gut vorbereitet in Sachen IT-Sicherheit.

Der Datenschützer empfiehlt, verstärkt in die Prävention von Angriffen zu investieren. „Dazu zählt eine sichere Architektur, Schulung von Mitarbeitenden und, wo immer es möglich ist, Datenminimierung walten zu lassen“, erklärt er. Das heißt: Personenbezogene Daten, die nicht gespeichert werden, könnten auch nicht entwendet werden. Wenn es zu einem Angriff kommt, sei eine offene Kommunikation wichtig. „Leider hat das Land Kärnten mit seiner Informationspolitik eine ehrliche Aufarbeitung verhindert. Das verheißt nichts Gutes für künftige Angriffsversuche“, kritisiert Lohninger.

Bürgerinnen und Bürgern legt er nahe, nur die notwendigsten Infos mit Firmen und Behörden zu teilen. Als Einzelperson sei es allerdings kaum möglich, sich gegen Behörden oder den Arbeitgeber zu wehren.

Kommentar Seite 20