ZEIT ONLINE

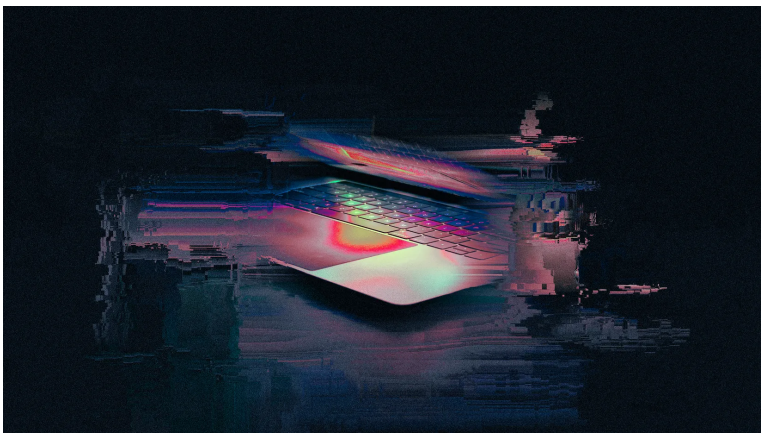
Erpressung im Internet

Der Staat als Beute

Mehr als 100 Behörden und öffentliche Einrichtungen wurden mit Ransomware angegriffen, einige zahlten gar Lösegeld. Koordinierte Hilfe des Staates aber gibt es nicht.

Von **Kai Biermann**

29. Juni 2021, 6:14 Uhr / 75 Kommentare /



© [M] Felix Burchardt, Martin Sanchez/unsplash.com

Im März sind die Computer der Stadtverwaltung Angermünde "abgebrannt". So bezeichnet es der Bürgermeister der Brandenburger Gemeinde, Frederik Bewer. Unbekannte hatten sich in das Computernetz der Stadtverwaltung gehackt und große Teile davon verschlüsselt. Einwohnermeldeamt, Standesamt und Grünflächenamt waren nicht mehr arbeitsfähig. Heiraten oder einen neuen Pass beantragen? Wochenlang unmöglich. Erst jetzt, vier Monate später, kann beispielsweise das Meldeamt wieder Bürgerinnen und Bürger empfangen.

Angriffe mit sogenannter Ransomware, bei der die Täter alle Daten der Betroffenen verschlüsseln und anschließend Lösegeld für den Entschlüsselungscode verlangen, sind zu einer Pandemie geworden. Weltweit erpressen Dutzende dieser Banden Lösegelder in Milliardenhöhe. Das trifft nicht nur Privatleute und Unternehmen, die Täter schrecken auch nicht davor zurück, Krankenhäuser, Schulen oder Polizeibehörden anzugreifen.

Mindestens 100 deutsche Ämter, Regierungsstellen, landeseigene Kliniken, Stadtverwaltungen und Gerichte sind in den vergangenen sechs Jahren von Ransomware-Banden attackiert worden. In den meisten Fällen ist es den Tätern dabei gelungen, in die IT-Systeme der Institutionen und öffentlichen

Ransomware

Daten als Geiseln

Ransomware

Die Lösegeld-GmbH

[https://www.zeit.de/digital/internet/2021-06/ransomware-netwalker-schadsoftware-erpressung-fbi-kriminalitaet]

Cyberkriminalität

US-Ermittler finden Lösegeld nach Pipeline-Hackerangriff

[https://www.zeit.de/politik/ausland/2021-06/hackerangriff-usa-pipeline-colonial-loesegeld-fbi-ermittler-bitcoin]

Hackerangriffe

"Ich sehe eine größere Gefahr bei Krankenhäusern"

[https://www.zeit.de/digital/internet/2021-02/hackerangriffe-bsi-arne-schoenbohm-cybersicherheit-krankenhaeuser-dirk-haeger]

Einrichtungen einzudringen und Daten zu verschlüsseln, sodass die Mitarbeiter und Mitarbeiterinnen keinen Zugriff mehr darauf hatten. Das ergibt eine Umfrage des Bayerischen Rundfunks und von ZEIT ONLINE unter allen Bundesländern. Demnach wurden beispielsweise in Sachsen-Anhalt seit 2015 mindestens 20 landeseigene Institutionen angegriffen, darunter der Landtag, Landesministerien, Krankenhäuser und Polizeidienststellen. In Mecklenburg-Vorpommern traf es mindestens 17 öffentliche Einrichtungen, darunter eine Landtagsfraktion, in Hamburg 15, in Schleswig-Holstein acht und in Sachsen sieben. Thüringen erfasst solche Angriffe erst seit dem Jahr 2019 und hat seitdem 13 Attacken auf Behörden und öffentliche Institutionen registriert.

"Gelegentlich Behörden unter den Opfern"

Diese Angaben geben allerdings nur einen groben Überblick, sehr wahrscheinlich ist die Gesamtzahl erheblich höher. Denn offenbar weiß keine Stelle in Deutschland genau, wie viele solche Ransomware-Angriffe auf staatliche Strukturen es gibt. So haben Berlin und Nordrhein-Westfalen gar keine Angaben dazu gemacht, niemand erfasst dort entsprechende Erpressungsversuche. Berlins Innensenat schrieb, es seien "gelegentlich auch Behörden und öffentliche Einrichtungen unter den Opfern", belastbare Zahlen aber habe man nicht. Baden-Württemberg antwortete, es habe eine "niedrige zweistellige" Zahl von Angriffen auf Kommunen gegeben, ohne das zu konkretisieren. Auch Nordrhein-Westfalen machte keine weitergehenden Angaben: "In NRW waren in den vergangenen Jahren unter anderem Schulen

und Krankenhäuser von Ransomware-Angriffen betroffen. Ein herausragendes Beispiel ist der Ransomware-Angriff auf das Uniklinikum Düsseldorf im Jahr 2020."

Die Regierung in den USA sieht Ransomware-Angriffe inzwischen als eine ernste Bedrohung der nationalen Sicherheit. FBI-Direktor Christopher Wray sagte dem *Wall Street Journal* [https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003], die Herausforderung sei vergleichbar mit der nach den Terroranschlägen des 11. September 2001. Doch obwohl solche Erpresser auch hierzulande seit Jahren Unternehmen und diverse staatliche Institutionen terrorisieren, gibt es in Deutschland keine gemeinsame Strategie, um etwas dagegen zu unternehmen. Dabei hat das Bundeskriminalamt Ransomware in seinem *Bundeslagebild Cybercrime 2020* [https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020] als "die Bedrohung für öffentliche Einrichtungen und Wirtschaftsunternehmen" beschrieben und das "die" in dem Satz unterstrichen. Doch es gibt, wie die Antworten der Bundesländer zeigen, nicht einmal den Versuch, sich einen Eindruck über die Größe des Problems zu verschaffen.

Im Bereich Cybercrime bestehe für Betroffene keine Meldepflicht gegenüber staatlichen Stellen, das gelte auch für Ransomware, antwortet das Bundesinnenministerium auf entsprechende Fragen. Daher existiere keine solche Statistik auf Bundesebene. "Den Betroffenen steht es frei, bei den zuständigen Strafverfolgungsbehörden Strafanzeige zu erstatten." Lediglich Behörden des Bundes müssten Ransomware-Angriffe beim BSI melden, dem Bundesamt für Sicherheit in der Informationstechnik. "In diesem Zusammenhang liegen BSI (*sic!*) keine Meldungen vor."

Kaum Täter ermittelt

Koordinierte Gegenwehr erscheint angesichts mangelnder Informationen schwierig. Das Bundesinnenministerium schreibt zur staatlichen Antwort auf diese Bedrohung lediglich, Erpressungen mit Ransomware seien schwere Straftaten. "Es ist Aufgabe der Strafverfolgungsbehörden, darauf geeignet zu reagieren", und man habe keine Hinweise darauf, "dass die Strafverfolgungsbehörden diese Straftaten nicht mit der notwendigen Priorität behandeln". Gleichzeitig aber gelingt es deutschen Strafverfolgern so gut wie nie, Erpresserinnen zu identifizieren, geschweige denn zu verhaften und Lösegelder zurückzuholen. Selbstverständlich schalten alle öffentlichen Einrichtungen sofort die Polizei ein, werden sie attackiert. Die kommt auch, doch die Beamten und Beamtinnen haben selten mehr als den Rat, kein Lösegeld zu bezahlen.

KAI BIERMANN

Redakteur im Ressort Investigative Recherche und Daten von ZEIT und ZEIT ONLINE

Das Problem trifft vor allem einen öffentlichen Bereich hart: die Kommunen. Das Grundgesetz sichert Gemeinden zu, ihre Belange selbst gestalten zu dürfen. Doch diese sinnvolle kommunale Selbstverwaltung gerät bei international agierenden Kriminellen schnell an ihre Grenzen.

Es bedeutet, dass Gemeinden wie Angermünde, immerhin eine Stadt mit 13.000 Einwohnern, auf sich allein gestellt sind. "Es gibt kein organisiertes System, das eine Kommune in Anspruch nehmen kann", sagt Bürgermeister Bewer. "Wir haben uns die Hilfe zusammengesucht und aus eigenen Mitteln finanziert." Die Folgekosten eines Angriffs sind erheblich, Angermünde musste die komplette Computerinfrastruktur neu aufbauen. Glücklicherweise gelang es, die meisten Daten zu retten. Mit den Erpressern verhandelt habe man nicht, sagt Bewer.

"Das ist kritisch, egal, ob wir zur kritischen Infrastruktur gehören"

Doch mit einer neuen Infrastruktur allein ist es nicht getan. In Angermünde beispielsweise fehlen die Daten aus dem Einwohnermeldeamt von mehreren Tagen. Damit aber komme die Bundesdruckerei nicht klar, sagt Bewer. "Was sind die notwendigen Schritte, wenn eine Kommune crasht? Darüber müssten sich die Behörden Gedanken machen", sagte er. Finanzielle Hilfe erwartet Bewer nicht, aber Informationen, was nach einem solchen Vorfall alles zu tun sei, wären sehr sinnvoll.

Es gibt eine Behörde, deren Aufgabe es ist, staatlichen Stellen beim Schutz und der Sicherung ihrer IT zu helfen, zumindest auf Bundesebene. Auf den Seiten des BSI gibt es zahlreiche Empfehlungen dazu. Aber dort steht auch der Satz: "Aufgrund ihrer Vielzahl können für Kommunen keine individuellen Beratungen angeboten werden." Städte und Gemeinden gehören auch nicht zur kritischen Infrastruktur – also zu jenen Bereichen des öffentlichen Lebens, die für den Staat und die Bürgerinnen und Bürger lebensnotwendig sind.

"Wenn so etwas passiert, was uns passiert ist, dann ist das kritisch, egal, ob wir zur kritischen Infrastruktur gehören", sagt Bewer. Angermünde hat daher zusammen mit anderen Brandenburger Gemeinden eine Art Selbsthilfegruppe gegründet. Der Zweckverband Digitale Kommunen Brandenburg (Dikom) [https://www.dikom-bb.de/] will bei Ransomware-Angriffen und anderen Vorfällen dieser Art erster Ansprechpartner sein. Vor allem gehe es darum, Erfahrungen betroffener Orte zu sammeln und anderen weiterzugeben.

Lösegeld aus Steuermitteln

So etwas gibt es jedoch nicht in jedem Bundesland. Die Zusammenarbeit von Kommunen und Landesbehörden im Bereich der Prävention könne durchaus noch weiter verbessert werden, schreibt der Städte- und Gemeindebund auf Anfrage dazu. Das BSI als Bundesbehörde sei kein direkter Ansprechpartner der Kommunen. "Die Länder sind hier aufgerufen, mit eigenen Landesämtern die Kommunen zu unterstützen."

Das klappt offensichtlich unterschiedlich gut. Manche Betroffene wissen sich nicht anders zu helfen, als Lösegeld an die Kriminellen zu zahlen – aus Steuermitteln. Das Staatstheater Stuttgart beispielsweise, das 2019 Opfer einer Ransomware-Attacke wurde [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2], soll 15.000 Euro bezahlt haben, wie lokale Medien berichteten. Die Hoffnung hinter solchen Zahlungen: dass die Täter ihr Versprechen halten und den Entschlüsselungscode herausrücken. Doch eine Garantie dafür gibt es nicht. Landeskriminalämter und BKA raten daher davon ab, auch, um die kriminelle Infrastruktur nicht noch zu fördern.

Wie viele weitere Opfer gezahlt haben und um welche Summen es geht, bleibt unklar. Mehrere Bundesländer, darunter Bayern, Nordrhein-Westfalen und Berlin, lassen in ihren Antworten offen, ob und wie viele Kommunen oder Behörden Lösegeld überwiesen haben.

Man dürfe die Städte und Gemeinden beim Thema Digitalisierung und IT nicht alleinlassen, sagt Bürgermeister Bewer. Es brauche Geld, vor allem aber Beratung und Know-how. "Man kann die Kosten für eine aktuelle IT-Infrastruktur nicht vermeiden. Entweder man baut seine IT geplant neu auf oder man tut es ungeplant – nach einem solchen Angriff." Bezahlen aber müssten alle irgendwann.