Webinar

Schutz vor Cyber-Angriffen

[07.11.2023] Verwaltungen rücken immer stärker in den Fokus von Hacker-Angriffen. Gelingt ein solcher Angriff, können die Folgen verheerend sein. Wie sich Kommunen schützen können, damit beschäftigte sich jüngst ein Webinar aus der Reihe „Kommune21 im Gespräch“.

Herr Landrat Bauer, Kommunen gelten nicht als Betreiber Kritischer Infrastrukturen (KRITIS) und sind daher von den entsprechenden Verordnungen nicht betroffen. Die neue Bedrohungslage spricht aber doch sehr dafür, dass auch Kommunen KRITIS-Betreiber sind. Was bedeutet das für den Salzlandkreis?

Markus Bauer: Zur Rolle des Landrats gehört es, nicht erst darauf zu warten, bis er eine Aufgabe erhält – sei es schriftlich, als Verordnung oder als Gesetz. Es gibt Dinge, die im Management selbstverständlich sind. Sicherheit ist ein solcher Bereich. Als Kreis müssen wir in der Lage sein, die Daten und Informationen der Bevölkerung zu schützen.

Bei den Aufgaben eines Landrats denkt man nicht zuerst an IT-Sicherheit. Inwiefern betrifft Sie das Thema?

Bauer: Ich bin zwar kein IT-Fachmann, aber ich bin derjenige, der diesen Bereich organisiert. Wir trennen bei uns im Haus den Bereich IT, das Aufgabenfeld Informationen und Daten sowie das Thema Sicherheit. Als diejenigen, die diese drei Bereiche steuern, sagen wir, was wir brauchen. Diese Aufteilung erleichtert es mir, den gesamten Bereich zu leiten und Verantwortung zu übernehmen. So bin ich etwa dafür zuständig, den Kreistag oder die Gremien auf das Thema aufmerksam zu machen und Bedarf anzumelden. Langfristig ist es günstiger, in die IT-Sicherheit zu investieren, als darauf zu warten, dass ein Schaden entsteht. Das muss ein gemeinsames Grundverständnis werden. Sicherheit ist nicht nur Selbstschutz, sondern Schutz für die ganze Region.

Der Salzlandkreis grenzt an den Landkreis Anhalt-Bitterfeld. Wie ist es Ihnen ergangen, als Sie von dem Cyber-Angriff im Jahr 2021 erfahren haben?

Bauer: Natürlich hat uns der Angriff stark betroffen gemacht. Zugleich war er aber auch eine Bestätigung des Weges, den wir eingeschlagen haben; nämlich IT nicht mehr als isolierte Einheit zu betrachten, sondern in unterschiedliche Bereiche getrennt, aber miteinander verbunden aufzubauen.

Herr Petters, sind die Kommunen für das Thema IT-Sicherheit gewappnet?

René Petters: Die großen Kommunen haben das Thema inzwischen im Griff. Sie betreiben oft eigene Rechenzentren, haben eine gut aufgestellte Organisation und sind häufig zertifiziert. Heikel wird es hingegen bei den kleineren Gemeinden und Landkreisen. Strukturen zu schaffen und notwendige Maßnahmen umzusetzen, kostet viel Zeit und Ressourcen. Hier herrscht teilweise eine Überforderung: Weil man die Aufgaben nicht stemmen kann, klammert man sich an das Prinzip Hoffnung.

Herr Nitz, worauf müssen Kommunen beim Thema IT-Sicherheit besonders achten? Was sind die häufigsten Einfallstore?

Hendrik Nitz: Zunächst muss man die Intention des Angreifers kennen und wissen, wie ein Angriff funktioniert. Erst dann lassen sich in der Kommune Mechanismen etablieren, die einen wirksamen Schutz gewährleisten. Auskunft über die Intention des Angreifers erteilt das so genannte Mitre-Framework. Dieses umfasst drei Punkte: Sabotage, Doxing – also das Ausspähen von Informationen – und finanzieller Diebstahl. Letzteres war im Landkreis Anhalt-Bitterfeld der Fall, wo die Mitarbeitenden durch die Verschlüsselung ihrer Systeme keinen Zugriff mehr hatten. Beim anschließenden Aufbau eines Schutzes geht es dann erstens darum, das Ziel des Angreifers zu identifizieren, zweitens das Vorgehen des Angreifers zu erkennen. Welche Backdoors kann der Angreifer ausnutzen? Ist es ihm möglich eine eigene Software zu installieren, um die Herrschaft über die Systeme an sich zu reißen?

Herr Landrat Bauer, wie richten Sie sich ein, um Gefahren abzuwehren?

Bauer: Zunächst haben wir Resilienzanalysen durchgeführt. Dabei haben wir festgestellt, dass die IT mit ihren Facetten Netzwerk, Infrastruktur, Software und Hardware gut funktioniert. Ein weiterer Ansatzpunkt ist die Organisation. Im Ernstfall muss man wissen, was zu tun ist und wie man sofort reagieren kann. Um einen Schaden, wenn er denn entsteht, so gering wie möglich zu halten, müssen Organisationsstrukturen aufgebaut werden und Notfallpläne bereitstehen. Deshalb habe ich einen Chief Digital Officer (CDO) eingesetzt und die Stelle eines Chief Information Officer (CIO) geschaffen, um Verantwortlichkeiten zu verteilen und ein Sparring zwischen der direkten IT und der Strategie aufzubauen.

„Sicherheit ist nicht nur Selbstschutz, sondern Schutz für die ganze Region."
Herr Nitz, was versteht man unter einer Resilienzanalyse und inwiefern profitieren Kommunen davon?

Nitz: Eine Resilienzanalyse zeigt einer Kommune, wie gut sie aufgestellt ist. In einem ersten Schritt wird geschaut, welche Verwaltungsverfahren die Kommune den Bürgern bereitstellt und welche davon notwendig sind, um den Landkreis, die Stadt oder die Gemeinde zu organisieren. Im zweiten Schritt wird dann die IT, die diese Prozesse unterstützt, genauer unter die Lupe genommen. Hier kommt die Verfahrenskritikalität ins Spiel, die es zu bewerten gilt. Welche Daten sind besonders schützenswert? Welche Prozesse müssen zwingend bereitgestellt werden? Diese Fragen helfen dabei, die Business- und Verfahrenskritikalität festzulegen. Basierend auf diesen Erkenntnissen entscheidet man dann, wie die IT darunter aufgebaut sein muss. Hier gibt es viele Möglichkeiten und Richtlinien wie etwa ISO 27000 oder die Standardmaßnahmenkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI). Ein weiterer wichtiger Punkt ist der Umgang mit Notfällen. Am Ende einer Analyse weiß eine Kommune, wie sie aufgestellt ist, welche Verbesserungspotenziale sie hat und welche Punkte sie hinsichtlich der IT-Sicherheit priorisieren muss.

Herr Landrat Bauer, welche Schlüsse haben Sie aus der Resilienzanalyse im Salzlandkreis gezogen?

Bauer: Die Resilienzanalyse hat uns gezeigt, dass die Organisation aus der Strategie des Hauses heraus entwickelt werden muss. Daran arbeiten wir momentan. Ein weiterer wichtiger Punkt ist die interkommunale Zusammenarbeit. Es ist wichtig, dass sich die Kommunen gegenseitig die Hand reichen. Die Aufgaben, die eine Verwaltung rund um die Uhr zu leisten hat, ist mit den 20 bis 30 Mitarbeitenden, die ihr zur Verfügung stehen, kaum zu bewältigen. Wenn wir uns hingegen als kommunale Familie begreifen, stärken wir uns gegenseitig und die Sicherheit untereinander.

Herr Nitz, wie schätzen Sie die interkommunale Zusammenarbeit aus Sicht eines IT-Dienstleisters ein?

Nitz: Das kann ich nur begrüßen. Natürlich geht es erst einmal darum, bestimmte organisatorische Prozesse mit Informationssicherheit zu härten. Dabei ist es sinnvoll, standardisierte Prozesse, die sowohl

in kleinen Gemeinden als auch in größeren Landkreisen oder Städten ablaufen, zu vereinheitlichen. Das jeweilige Wissen über organisatorische Informationssicherheit sollte unbedingt geteilt werden.

Nach einer Resilienzanalyse müssen Maßnahmen umgesetzt werden. Was bedeutet das konkret aus technischer Sicht?

Nitz: Zunächst muss eine organisatorische Informationssicherheit aufgebaut werden. Dazu gehören ein Informationssicherheitsbeauftragter (ISB), ein Datenschutzbeauftragter (DSB) und ein organisatorischer Gesetzestext für die Verwaltung mit der Perspektive Informationssicherheit. Außerdem gibt es die IT-Abteilung, die sich um den sicheren Betrieb der Server und der Endgeräte kümmert. Hier empfehle ich immer, den Schwerpunkt auf ein gutes Service-Management zu legen. Anschließend stellt sich die Frage, wie das Ganze überwacht wird. Diese Aufgabe erledigt das Security Operation Center (SOC). Es beobachtet zum einen die IT und die Business- oder Verwaltungsprozesse. Zum anderen prüft es, welche Schwachstellen es gibt und ob diese ausnutzbar sind. Diese Aufgabe übernimmt das Security Incident und Event Management (SIEM). Dabei handelt es sich nicht um eine einzelne Software, sondern um ein Konglomerat aus unterschiedlichen Software-Instanzen, Systemen, Antivirus-Systemen, der Netzkommunikation, Stammdaten einer eigenen Configuration Management Database und einer Asset-Verwaltung. Schlägt das SIEM an, muss der Vorfall vom SOC analysiert werden. Liegt ein sicherheitsrelevantes Ereignis vor, informiert das SOC die IT-Abteilung mit einem Ticket und sagt, was zu tun ist. Mittlerweile setzt das SIEM aber auch Künstliche Intelligenz (KI) ein, um anormales Verhalten zu erkennen.

Herr Petters, welche IT-Sicherheitsdienstleistungen bietet GISA den Kommunen an?

Petters: An erster Stelle steht das Komplettpaket Full Managed IT-Security. Damit können die Kommunen ihre IT-Sicherheit komplett an uns auslagern. Zweitens unterstützen wir bei einer ersten Standortbestimmung. Hier führen wir eine Resilienzanalyse durch, um innerhalb weniger Tage mögliche Schwachstellen zu identifizieren. Und schließlich haben wir Angebote für Kommunen, die bereits genauer wissen, wo sie sich in ihren Betriebs- und Servicekonzepten verbessern müssen.

Herr Nitz, wir haben auch über organisatorische Informationssicherheit gesprochen. Was versteht man darunter und was ist dabei zu beachten?

Nitz: Das ist eine Pflicht, die jede Verwaltung neben der technischen Überwachung erfüllen muss. Wir empfehlen ganz klar, ein Informationssicherheitsmanagement-System zu etablieren. Das ist ein Regelwerk, das individuell auf die Verwaltungsprozesse und Fachverfahren abgestimmt ist und regelmäßig überwacht wird. Damit geht einher, dass Schutzbedarfsfeststellungen etabliert werden, und dass jedes in der Kommune oder im Land durchgeführte Projekt oder Vorhaben sicherheitstechnisch von einem Konzept begleitet wird. Außerdem umfasst es eine Risikoanalyse, die gezielte Maßnahmen beschreibt, mit denen sich Risiken und Gefährdungen ausschließen oder minimieren lassen. Wichtig sind auch Awareness-Schulungen der Mitarbeitenden. Sie müssen im Umgang mit Informationen geschult werden.

Herr Landrat Bauer, wie sehen Ihre Pläne und Strategien für die Digitalisierung und die IT-Sicherheit bis zum Jahr 2030 aus?

Bauer: In unserem Zukunftsstrategiepapier steht der Begriff Smart Region Salzlandkreis. Wir wollen den Bürgern zeigen, dass die Digitalisierung ein Werkzeug ist, mit dem wir uns verbessern und vieles einfacher machen können. Aber auch als Verwaltung wollen wir das Thema besetzen, weil es uns viele Abläufe erleichtert. Wie wichtig eine effiziente Kommunalverwaltung ist, hat sich in den vergangenen Jahren mit

der Corona-Pandemie, der Energiekrise und der Flüchtlingssituation mehr als deutlich gezeigt.

Herr Nitz, Herr Petters, wie unterstützt GISA die Kommunalverwaltungen? Was können Sie mit Blick in die Zukunft tun?

Petters: Über die Resilienzanalyse hinaus haben wir mit anderen Landkreisen Gespräche geführt, inwieweit Leistungen bei uns als Dienstleister in einem BSI-zertifizierten Rechenzentrum stattfinden können. Wir bieten an, Server und IT bei uns sicher aufzubewahren und nicht nur zu überwachen oder sicher unterzustellen. Das wäre eine Möglichkeit, noch einmal größer zu denken.

Nitz: Derzeit bereiten wir das Thema Private Cloud für Kommunen vor. Hier würden wir zum einen als Ansprechpartner fungieren, zum anderen hätten Kommunen die Sicherheit, dass sich ihre Informationen in einer Umgebung befinden, die sicherheitstechnischen Standards entspricht.
Herr Landrat Bauer, was raten Sie den Kommunen? Was sollte sofort in Angriff genommen werden, um ein Organisationsverschulden zu vermeiden?

Bauer: Die Resilienzanalyse war für uns ein erster wichtiger Schritt, um ein Werkzeug in die Hand zu bekommen. Außerdem ist es wichtig, sowohl die kommunalen Vertreter im Kreistag als auch die eigenen Mitarbeitenden für das Thema IT-Sicherheit zu gewinnen. Des Weiteren sollte man die IT nicht als isolierten Bereich betrachten und davon ausgehen, dass diese ihre Aufgaben aus eigener Kraft stemmt. Es empfiehlt sich, auch die Anwendungsbetreuer in die Fachdienste einzubinden und auf diesem Gebiet zu schulen. Man kennt das ja aus dem Büroalltag: Der Computer funktioniert nicht und man ruft bei der IT an. Bei einer Verwaltung mit 850 bis 1.000 Mitarbeitenden kann die IT das aber nicht mehr leisten. Hier muss ein Umdenken stattfinden. Wir versuchen derzeit, die Beschäftigten verstärkt in den Bereich IT einzuarbeiten. Es geht also nicht darum, neue Mitarbeitende zu gewinnen, sondern die Kompetenzen der vorhandenen zu schärfen. Verantwortung und Aufgaben zum Thema IT-Sicherheit müssen breiter aufgestellt, die erforderlichen Strukturen geschaffen und entsprechende Rollen stärker definiert werden, um organisatorische und fachliche Doppelstrukturen soweit möglich zu vermeiden – und damit das Gesamtsystem Kreisverwaltung für künftige Herausforderungen besser zu rüsten. Schließen möchte ich mit einem Plädoyer für den Austausch: Hier gibt es viele Möglichkeiten. Ich bin beispielsweise Mitglied in einem Innovationsring des Deutschen Landkreistags. Dort tauschen wir uns als Landräte regelmäßig untereinander aus – das tut gut, das kann ich nur empfehlen.

()

https://www.salzlandkreis.de

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Salzlandkreis, Resilienzanalyse, Kommune21 im Gespräch