Cyberattacken – wie bedroht sind unsere Kommunen?
Beitrag: Julia Cruschwitz, Carolin Haentjes
Kamera: Dirk Meinhardt, Alexander Rott, Ulf Wogenstein
Schnitt: Tobias Hohensee

Wolmirstedt in der Nähe von Magdeburg. Im Rathaus macht man sich Gedanken um die Cyber-Sicherheit der Stadtverwaltung, möchte besser gegen Angriffe gewappnet sein. Deshalb wird digital aufgerüstet, erklärt der stellvertretende Bürgermeister Marko Kohlrausch.

Marko Kohlrausch, stellvertr. Bürgermeister Wolmirstedt, parteilos
Ja, das ist jetzt unser Museum, könnte man fast sagen. Also ist jetzt nicht so, dass wir das extra zusammengestellt haben, um hier ein schönes Bild, ein altes Bild zu zeigen, sondern das hier ist die Technik, mit der wir vor kurzem noch gearbeitet haben.
Reporterin: Das kenne ich noch aus meiner Studienzeit.

Nach jahrelanger Vernachlässigung hat die Stadt Wolmirstedt rund 140.000 Euro für neue Hardware in die Hand genommen. Corona war ein Auslöser, weil viel mehr digital ablief. Dazu kamen immer mehr Stadtverwaltungen, die durch Cyber-Attacken lahmgelegt wurden, wie das nahe Bitterfeld. Auch hier hat man Angst vor so einem Angriff.

Marko Kohlrausch, stellvertr. Bürgermeister Wolmirstedt, parteilos
Das sind ja Daten, persönliche Daten, intime Daten, die dann verloren gehen. Im Kassenbereich, wenn ich ihr Konto dort irgendwo registriert habe, möchten Sie auch nicht, dass das irgendjemand drittes sieht. Also das sind sensible Daten, die wir hier verarbeiten. Und das ist schon, denke ich mal ein Super-GAU, wenn das nach draußen geht.

Die Pflege der Software und die Cyber-Sicherheit kosten nochmal rund 100.000 Euro pro Jahr. Darum kümmern sich nun externe Dienstleister - vor allem die Firma von Marco Langhof.

Marco Langhof, Unternehmer und IT-Sicherheitsexperte
Hier sind wir jetzt im Server Raum. Wenn man sich das hier anschaut, dann haben wir hier die eigentliche Servertechnik. Eigentlich ist das hier das Herz des Ganzen.

Der Unternehmer sieht gerade bei kleinen Kommunen häufig sehr große Sicherheitslücken. Er meint, seit dem Ukraine-Krieg gäbe es insgesamt mehr Angriffsversuche, auch auf

Kommunen. Vor allem durch automatisierte Schadsoftware, die nach Schwachstellen suche und dort andocke.

Marco Langhof, Unternehmer und IT-Sicherheitsexperte
Wir sehen eine Verschiebung der Angriffsmethodik, was das Ziel hat, das Vertrauen von Bürgern in den Staat zu erschüttern. Das ist tatsächlich eine Sache. Also der Staat ist nicht vertrauenswürdig. Auch das, was gesagt wird, ist vielleicht nicht vertrauenswürdig. Und tatsächlich, andere Länder dahin zu bringen, sich eher mit sich selbst zu beschäftigen, als zum Beispiel Hilfe zu leisten.

So könnte der weltpolitische Konflikt in kleine Kommunen getragen werden. Ihre oft schlecht gesicherten IT-Strukturen sind ideale Ziele. Stellen also Cyber-Angriffe auf Kommunen ein ernstzunehmendes Sicherheitsproblem dar?

Der bisher schwerwiegendste Angriff trifft den Landkreis Anhalt-Bitterfeld im vergangenen Juni. Dort wird der erste Cyber-Katastrophenfall Deutschlands ausgerufen. Alle 160 Software-Programme sind betroffen, 900 Rechner müssen vom Netz. Eine Gruppe namens „Pay or Grief“ fordert Lösegeld in Kryptowährung. Dokumente aus dem Innersten der Kreisverwaltung werden veröffentlicht. Der Schaden beträgt zwei Millionen Euro.

In Bitterfeld kämpft man heute noch mit den Folgen. In der Kfz-Zulassungsstelle stapeln sich tausende unbearbeitete Aufträge. Nur rund ein Drittel der Verwaltungsrechner sind wieder im IT-Netz integriert.

Die Bundestagsabgeordnete der Linken, Anke Domscheit-Berg warnt schon lange, dass die Cyber-Sicherheit in Deutschland viele Lücken hat. Besonders kleinere und ärmere Kommunen seien schlecht aufgestellt.

Anke Domscheit-Berg, MdB, Die Linke.
Bitterfeld war, glaube ich, eine wichtige Warnung für alle anderen Kommunen. Außerdem ist es so, dass sehr viele Kommunen ja ähnliche Software benutzen, dass sie manchmal sogar den gleichen IT-Dienstleister teilen. Und wenn da ähnliche Softwareprodukte verwendet werden, dann kann natürlich auch eine bestimmte Schadsoftware die gleichen Programme in unterschiedlichen Kommunen attackieren. Das heißt, wir können auch in eine Situation kommen, wo nicht eine Kommune, sondern 100 oder 1.000 betroffen sind. Und dann wird das gleich ein Flächenbrand.

Ein Flächenbrand, der kritische Infrastruktur in größeren Teilen Deutschlands lahmlegen könnte. Dazu gehören Bereiche wie Strom- oder Wasserversorgung, auch Kommunen fallen darunter.

Mit dem BSI-Gesetz möchte das Bundesamt für Sicherheit in der Informationstechnik - kurz BSI - die kritische Infrastruktur vor Cyber-Angriffen schützen. Merkwürdig nur: Kommunen werden nicht im BSI-Gesetz erwähnt. Weil Vorgaben durch eine Bundesbehörde in das Selbstbestimmungsrecht der Kommunen eingreifen würden.

Anke Domscheit-Berg, MdB, Die Linke.
Ich glaube, dass die Kommunen unbedingt explizit im BSI-Gesetz erfasst werden müssen, damit für sie auch ganz konkrete Anforderungen gelten. Zum Beispiel, dass sie bestimmte Mindestanforderungen an IT-Sicherheit erfüllen müssen, dass sie den Basis-IT-Grundschutz erfüllen müssen, dass sie eine externe Prüfung vielleicht alle zwei Jahre vorweisen müssen. Das würde den Grad an IT-Sicherheit enorm erhöhen.

Der Bereich der „Gefahrenabwehr“ allerdings liegt bei den Ländern. Dafür sollen sie sogenannte CERTs etablieren: “Cyber Emergency Response Teams”, also eine Art Cyber-Feuerwehr, die Wache hält, im Notfall eingreift.

Wir sind in Sachsen. In Dresden sitzt das Cyber-Sicherheitsnotfallteam des Freistaates, das Sax.CERT. Der Landes-Beauftragte für Informationssicherheit, Jörg Steinig, zeigt uns das Lagezentrum.

Jörg Steinig:
Wir haben jeden Tag so zwischen 20 und 30 Schwachstellen, die erkannt werden. Und regelmäßig nutzen dann unsere Kommunen oder auch die Landesverwaltungen den Dienst, den das Notfallteam hier anbietet.

Sachsen hat ein Informations-Sicherheitsgesetz. Darin sind Standards für die Kommunen festgelegt, was die Cyber-Sicherheit betrifft. Außerdem werden kostenlose Schulungen für Mitarbeitende in Verwaltungen angeboten. Alle Attacken auf sächsische Kommunalverwaltungen konnten bisher abgewehrt werden. Doch Angriffe auf kommunale Eigenbetriebe in Sachsen gab es durchaus, sowie auf die Stadtwerke Pirna oder die Stadtreinigung Leipzig. Denn Eigenbetriebe wiederum sind nicht an das sächsische kommunale Datennetz angeschlossen.

Sachsen-Anhalt dagegen hat gar kein eigenes CERT. Gemeinsam mit Schleswig-Holstein, Hamburg und Bremen gehört es zum das CERT Nord. Nur vier Personen arbeiten direkt im CERT Nord für alle diese Länder. Erstaunlich wenige.

Wir fragen im Digitalministerium Sachsen-Anhalt nach. Und erfahren: Hier gibt es auch nach dem Katastrophenfall von Bitterfeld kein IT-Sicherheitsgesetz und keine speziellen Angebote für Kommunen. Man fühle sich nicht zuständig, Zitat: “Grundsätzlich fallen Fragen der IT-Sicherheit in die originäre Zuständigkeit der jeweiligen Kommune.”
Ministerium für Infrastruktur und Digitales Sachsen-Anhalt

Auf eigene Initiative hat die Stadt Wolmirstedt daher den IT-Unternehmer Marco Langhof engagiert. Dank der Investition fühlt man sich in Wolmirstedt nun sicherer vor einem Cyber-Angriff – doch gut unterstützt vom Land oder Bund überhaupt nicht.