Behörden Spiegel
Juli 2019, Seite 28, www.behoerdenspiegel.de

Führungsaufgabe für Staat und Verwaltung

Freistaat Sachsen priorisiert die Informationssicherheit

(BS/Benjamin Stiebel) Die sächsische Landesregierung hat der Informationssicherheit einen Spitzenplatz auf ihrer politischen Agenda spendiert. Davon zeugt die Umressortierung des Aufgabenbereichs vom Innenministerium in die Staatskanzlei im letzten Jahr. Nun folgte die Verabschiedung eines eigenständigen IT-Sicherheitsgesetzes. Damit soll das Thema in allen Behörden zur Chefsache gemacht werden.

"Wir müssen das Thema Informationssicherheit als Führungsaufgabe verstehen. Dafür Bewusstsein zu schaffen, liegt mir besonders am Herzen." Das sagte *Thomas Popp* zur Eröffnung des zweiten IT-Sicherheitstags Sachsen, den die Sächsische Staatskanzlei in Zusammenarbeit mit dem Behörden Spiegel in Dresden veranstaltete.

Vor gut 200 Teilnehmern aus Landes- und Kommunalverwaltung sowie Wirtschaft und KRITIS-Betreibern betonte der Amtschef der Sächsischen Staatskanzlei und CIO des Freistaats: "Die Informationstechnik ist heute für die Verwaltung genauso wichtig, wenn nicht wichtiger, als klassische Arbeitsgrundlagen wie Gebäude oder Büromittel."

Eröffnete den IT-Sicherheitstag Sachsen: der Amtschef der Sächsischen Staatskanzlei und CIO des Freistaats Sachsen, Thomas Popp. Foto: BS/Stiebel

Souveränität im IT-Betrieb

Staat und Verwaltung müssten mehr Verantwortung für Entwicklung und Betrieb von sicherer Informationstechnik übernehmen. "Wir dürfen uns nicht nur auf Anbieter aus der Wirtschaft verlassen, sondern müssen selbst wieder Kompetenzen aufbauen", so *Popp.* In dem Zusammenhang kündigte der CIO auch einen Stellenzuwachs für den IT-Dienstleister des Freistaats, den "Staatsbetrieb Sächsische Informatik Dienste" (SID), an. "Wenn wir auf Grundlage von Gesetzen Daten von Bürgern und Unternehmen einholen, müssen wir auch in der Lage sein, diese Daten zu schützen."

Das kürzlich verabschiedete "Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen" gilt für alle Stellen, die an das Sächsische Verwaltungsnetz (SVN) oder das Kommunale Datennetz (KDN) angeschlossen sind. Geregelt werde die klare Verantwortung der Führungsebene für die Informationssicherheit. Zwar sähen bereits viele Führungskräfte in den Landesbehörden Digitalisierung und Informationssicherheit schon als Chefsache, so *Popp.* In der Vergangenheit hätten es sich aber auch einige noch zu leicht gemacht und das Thema der IT-Abteilung überlassen. Das sei jetzt nicht mehr möglich. *Popp:* "Es wird zum Beispiel eine jährliche Berichtspflicht geben. Damit kann sich keine Behördenleitung mehr damit herausreden, die Informationssicherheit habe nicht in ihrer Verantwortung gelegen."

Mit dem Gesetz werden außerdem Meldepflichten für öffentliche Stellen sowie die Befugnisse zur Analyse und Abwehr von Bedrohungen im Netzverkehr erweitert. "Die Gesetzesänderung war dringend notwendig", bekräftigte *Christoph Damm,* Leiter des beim SID angesiedelten Computer Emergency Response Teams des Freistaats (SAX.CERT). "Bisher hatten wir nur sehr eingeschränkte Möglichkeiten zur Log-Auswertung."

Im Frühjahr seien dem SAX.CERT 16 Fälle bekannt geworden, in denen infolge einer Infektion mit der Schadsoftware Emotet Landesdaten abgeflossen seien. Die Informationen darüber kamen aber überwiegend von externen Quellen, teils aus dem Ausland, so *Damm.* "Mit den neuen verbindlicheren Meldepflichten dürfte sich die Herangehensweise der Verantwortlichen ändern. So bekommen wir eine bessere Lageübersicht und können besser auf Vorfälle reagieren." Neuerdings ist das SAX.CERT auch offiziell für die Kommunen zuständig. Diese können sich nun Beratung sowie Dienstleistungen wie einen Warn- und Informationsdienst einholen.

Partnerschaften ausbauen

CIO *Popp* räumte aber ein, dass nicht alle Herausforderungen der Informationssicherheit allein auf Ebene der Landesverwaltung gestemmt werden könnten. Daher begrüßte er die Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnologie (BSI). Im Herbst letzten Jahres wurde bereits eine Absichtserklärung zur stärken Zusammenarbeit unterzeichnet. Seit Mai betreibe das BSI nun auch ein Verbindungsbüro für die Region Ost in Dresden als Ansprechstelle für Verwaltung und Unternehmen. Hier knüpfte BSI-Präsident *Arne Schönbohm* an. "Wir als nationale Cyber-Sicherheitsbehörde haben Fähigkeiten und Erfahrungen, die wir auch gerne den Ländern und Kommunen zur Verfügung stellen möchten." Gesetzliche Anpassungen vorausgesetzt, umfasse dies auch die Übernahme konkreter technischer Schutzmaßnahmen in den Lan-

desnetzen. Dabei gehe es nicht darum, den Partnern Angebote überzustülpen, stellte *Schönbohm* klar. "Je nach Interessenlage seitens des Landes diskutieren wir Möglichkeiten und entscheiden ganz individuell, in welchen Bereichen zusammengearbeitet wird." Möglich und mit Sachsen auch schon in die Wege geleitet seien Kooperationen zur Aus- und Fortbildung. Auch im Bereich der Mitarbeiter-Sensibilisierung und mit Beratung zu Sicherheitskonzepten stehe das BSI zur Verfügung. Bereits etabliert sei der Informationsaustausch über den Verwaltungs-CERT-Verbund. *Schönbohm* rief dazu auf, auch die Angebote der durch das BSI koordinierten Allianz für Cyber-Sicherheit noch stärker wahrzunehmen. "Hier tauschen die Teilnehmer kostenfrei Erfahrungen aus. Regelmäßig werden Whitepaper verteilt, wie zum Beispiel ein Leitfaden zur Sicherheit in Druckumgebungen." Gerade kleine und mittelständische Unternehmen hätten viel zu gewinnen, warb der BSI-Präsident.

Digitale Diskurse im Blick

(BS/stb) Souveräner Umgang im Digitalen endet nicht mit der Organisation von IT-Sicherheit. Der Staat sieht sich auch zunehmend mit den Folgen digitaler Technologien auf das gesellschaftliche Zusammenleben konfrontiert. So wird befürchtet, dass gezielte Desinformationskampagnen über Soziale Plattformen das Vertrauen der Bürger in Demokratie und Staat schwächen könnten. "Extremisten und staatliche Akteure verfolgen dieses Interesse und nutzen die Möglichkeiten, die Ihnen das Netz heute bietet", so Gordian Meyer-Plath, Präsident des sächsischen Landesamts für Verfassungsschutz, bei einer Diskussionsrunde auf dem IT-Sicherheitstag Sachsen. Das heute unter den Begriff "Fake News" gefasste Phänomen habe es im Grundsatz schon immer gegeben, ergänzte Oliver Schenk, Staatsminister für Bundes- und Europaangelegenheiten und Chef der Sächsischen Staatskanzlei. "Mit den heutigen digitalen Mitteln lassen sich Falschnachrichten aber viel schneller produzieren und je nach Intention breiter oder auch zielgerichteter verbreiten." Peter Welchering forderte daher, Plattformen wie Facebook als Medien wahrzunehmen und auch entsprechend zu regulieren: "Ich sehe hier ein klares Versagen beim Staat, der dabei zugesehen hat, wie sich am Datenschutz vorbei ein florierender, weltweiter Datenhandel entwickelt hat." Die gezielte Ansprache der Nutzer aufgrund von automatisiert erstellten Profilen sei die Voraussetzung für den Erfolg von Desinformationskampagnen, so der Journalist.

Immer wieder wird befürchtet, mit gezielten Fake News oder durch die Verbreitung massenhafter gefärbter Berichte könnten sogar Wahlergebnisse durch fremde Mächte beeinflusst werden. Dies sei am ehesten bei A-oder-B-Entscheidungen zu befürchten, wie man es beim Brexit-Votum oder der US-amerikanischen Präsidentenwahl gesehen habe, erklärte Meyer-Plath. "In Deutschland gibt es solche Konstellationen seltener, daher ist eine Beeinflussung viel schwieriger. Der Versuch wird aber trotzdem unternommen", so der Verfassungsschützer.

Beim Kampf gegen Fake News gebe es ein Problem: Eine Widerlegung falscher Darstellungen komme meist deutlich verzögert und generiere in der Regel weniger Aufmerksamkeit als die ursprüngliche Falschmeldung. "Das saubere Ausermitteln dauert naturgemäß leider länger, als einfach etwas ins Netz zu stellen", so Schenk. Innerhalb der Verwaltung müssten nun Kommunikationsabteilungen personell, aber auch mit zeitgemäßen digitalen Kompetenzen gestärkt werden, damit die neuen Kanäle sachgemäß bespielt werden könnten. "Wir müssen uns besser aufstellen, um irreführende Inhalte schneller erkennen und angemessen darauf reagieren können", forderte der Staatsminister. Besonders die Polizei sei hier gefragt, waren sich die Diskussionsteilnehmer einig. Wenn in Gefahrenlagen Gerüchte verbreitet würden, müsse schnell über die Sozialen Netzwerke Aufklärung betrieben werden. Dabei sei auch eine offensivere und transparente Kommunikation wünschenswert, wenn die Behörden noch kein umfassendes Lagebild hätten und einzelne Meldungen noch nicht bestätigen oder entkräften könnten.

Von links: Oliver Schenk, Uwe Proll (Moderator, Behörden Spiegel), Peter Welchering, Gordian Meyer-Plath

Foto: BS /Stiebel