Thurgau

Der Regierungsrat des Kantons Thurgau an den Grossen Rat

GRG Nr.	20	EA 191	468

Frauenfeld, 18. April 2023
225

Einfache Anfrage von Patrick Siegenthaler vom 1. März 2023 „Ist die kantonale Verwaltung gegen Cyberrisiken gerüstet?“

Beantwortung

Sehr geehrte Frau Präsidentin
Sehr geehrte Damen und Herren

Der „Bereitschaftsgrad gegen einen Cyberangriff“ ist nur schwer messbar. Der Regierungsrat bittet sodann um Verständnis, dass aus Sicherheitsgründen keine detaillierten Angaben zum Abwehrdispositiv und zur allgemeinen Maturität der IT-Security der Kantonalen Verwaltung Thurgau (KVTG) gemacht werden können.

Frage 1

In der KVTG werden betreffend Informationssicherheit bei den IT-System sämtliche gängigen Standards angewendet. Bereits die Bauten der Rechenzentren unterliegen Standards, die sich über die gesamte Infrastruktur (Netzwerk, Datenbanken, Betriebssysteme etc.) bis hin zu den Applikationsarchitekturen erstrecken.

Es wird grosser Wert auf physische und systemtechnische Zugangsbeschränkungen gelegt und immer das „Need-to-know“-Prinzip angewendet. Das bedeutet, dass nur derjenige Personenkreis physischen Zugang zu den Rechenzentren erhält, der auch tatsächlich Arbeiten darin ausführen muss. Der Zutritt zur physischen IT-Infrastruktur wird separat überwacht und ist generell nur einem stark eingeschränkten Personenkreis möglich. Zudem werden sämtliche Zutritte registriert. Analog verhält es sich mit den systemtechnischen Zugriffen. Es sind verschiedene Stufen von Logins zu durchlaufen, und über granulare Berechtigungskonzepte wird sichergestellt, dass nur berechtigten Personen der Zugang auf die Systeme ermöglicht wird. Ausserdem werden die Zugriffe auf sensitive Systeme im Detail aufgezeichnet. Sämtliche Fernwartungszugriffe von Drittfirmen sind nur über separate Authentisierungs- und Autorisierungsmechanismen möglich und werden ebenfalls aufgezeichnet.

Zum Schutz der Daten und sensitiven Systeme sind in den Rechenzentren der KVTG professionelle IT-Systeme aus dem High-End-Sektor im Einsatz. So werden zum Beispiel für die Netzwerkzonierung Produkte wie die „Palo Alto Security Operating Platform“ verwendet. Die Systeme sind in einem Netzwerkverbund mit verschiedenen Netzwerkzonen eingebettet und auf zwei physische Standorte verteilt. Zum Schutz gegen Datenverlust ist ein dreistufiges Backup-Konzept im Einsatz, wobei unterschiedliche Technologien für Speichermedien zum Einsatz kommen.

Jedes neu aufzusetzende System durchläuft einen detaillierten Prüfprozess bezüglich Architektur und IT-Sicherheit. Relevante Angaben werden im Rahmen eines standardisierten Informationssicherheits- und Datenschutzkonzeptes (ISDS-Konzept) dokumentiert. Insgesamt ist die Informationssicherheit der beiden kantonalen Rechenzentren vergleichbar mit derjenigen in anderen, auch grösseren Kantonen.

Frage 2

Das Amt für Informatik (AFI) ist zwar wie die meisten anderen verwaltungsinternen kantonalen IT-Dienstleister nicht ISO-zertifiziert, orientiert sich aber eng an den Standards ISO27001 und ISO9001. Die Finanzkontrolle führt regelmässige IT-Audits durch. Zudem arbeitet das AFI für periodische IT-Security-Assessments mit externen Spezialisten zusammen. Dabei werden beispielsweise einzelne Systeme oder Netzwerkzonen auf ihre Angreifbarkeit überprüft. Aus Sicherheitsgründen können hierzu keine näheren Angaben gemacht werden.

Die Einheit IT-Security Operations des AFI ist mit der permanenten Überwachung der gesamten IT-Infrastruktur und des Datenverkehrs auf den Netzwerkstrecken betraut. Mittels moderner Monitoringsysteme werden Anomalien automatisch erkannt, in einer Überwachungskonsole in Echtzeit angezeigt und nach bestimmten Kriterien eine Alarmierung der relevanten Personen ausgelöst.

Das AFI verfügt weiter über einen IT-Sicherheitsbeauftragten (Chief Information Security Officer [CISO]), der die gesamte IT-Landschaft laufend auf Unsicherheiten überprüft und Weisungsbefugnis über sämtliche operativen Einheiten des AFI hat. Der CISO ist in engem Austausch mit dem National Cyber Security Center (NCSC) des Bundes, über das laufend Informationen bezüglich Bedrohungsszenarien und entsprechender Abwehrstrategien ausgetauscht werden. Sodann bestehen enge Kontakte mit den CISO der umliegenden Kantone.

Frage 3

Es werden periodische Phishing-Kampagnen durchgeführt, letztmals im Herbst 2022. Zurzeit läuft eine Security-Awareness-Kampagne, in deren Rahmen sämtliche Mitarbeiterinnen und Mitarbeiter der KVTG aufgefordert werden, verschiedene E-Learning-Module zur Sensibilisierung für ICT-Security zu durchlaufen. Das AFI arbeitet auch in diesem Bereich mit externen Spezialisten zusammen, um sich stetig weiterzuentwickeln.

Frage 4

Der Kantonale Führungsstab (KFS) hat Cyberangriffe als eines der Hauptrisiken für die KVTG definiert und die entsprechende Dokumentation kürzlich vollständig überarbeitet. Gestützt darauf hat das AFI konkrete Massnahmen festgelegt und diese in ihrer Strategie in einzelnen Handlungsfeldern zusammengefasst. Im Einzelnen sind dies u.a. folgende Massnahmen:

– Informationssicherheit: Stärkung der Sensibilisierung mittels einer Schutzbedarfsanalyse, dem Aufbau eines ICT-Security-Informationsportals sowie einer ICT-Sensibilisierungskampagne.
– Ausbau des Sicherheitsbetriebs: Cyber-Security-Incident–Response–Service, Security–Assessment und daraus abgeleitete Massnahmen sowie Stärkung des Sicherheitsdispositives mit einem externen Security Operation Center.

Frage 5

Nein. Der Regierungsrat beurteilt den Nutzen einer solchen Versicherung für die KVTG als verhältnismässig klein. Im Gegensatz zur Privatwirtschaft wäre die Verwaltung bei einem Cyberangriff wohl weniger mit unmittelbaren wirtschaftlichen Schäden konfrontiert. Im Vordergrund stehen dagegen Reputationsschäden und die zeitliche Verzögerung im Zusammenhang mit der Wiederherstellung der betroffenen Bereiche, die beide nicht durch eine Versicherung gedeckt werden können.

Die Präsidentin des Regierungsrates

Der Staatsschreiber