7. Interpellation von Patrick Siegenthaler vom 7. Juni 2023 "Kosten-Nutzen einer ISO27001-Zertifizierung im AFI Thurgau" (20/IN 46/519)

Beantwortung

Präsident: Die Antwort des Regierungsrates liegt schriftlich vor. Der Interpellant, Kantonsrat Patrick Siegenthaler, hat zuerst das Wort für eine kurze Erklärung, ob er mit der Beantwortung zufrieden ist.

Patrick Siegenthaler, Die Mitte/EVP: Die Schlagzeilen brechen nicht ab. Wir sprechen heute über ein sehr aktuelles und kritisches Thema. Der kantonale Führungsstab hat Cyberangriffe als eines der Hauptrisiken für die kantonale Verwaltung Thurgau definiert. Es vergeht kaum eine Woche, in welcher man nicht von Angriffen auf Schweizer Unternehmen oder Behörden und Verwaltungen liest. Kürzlich war beispielsweise gerade die Stadt Yverdon davon betroffen. Diejenigen von Ihnen, die heute schon die Thurgauer Zeitung gelesen haben, konnten darin von einem Angriff in der Privatwirtschaft, auf die Dieci AG, einen schweizweit bekannten Pizza-Kurier, vernehmen. Ich bedanke mich bei der Regierung für die Beantwortung der Interpellation. Mit der Antwort, geschätzter Ratspräsident, bin ich nur teilweise zufrieden. Man hat beim Amt für Informatik, was Informationssicherheit anbelangt, offenbar alles im Griff. Schön, wenn man das so sagen kann. Kürzlich konnten wir vernehmen, dass sechs Kantone gemeinsam ein sogenanntes Security Operations Center beschafft haben. Der Auftrag dafür wurde an die Swisscom vergeben für insgesamt 7.1 Mio. Franken. Die Swisscom wird also in den nächsten Jahren den Service in den Bereichen Security Information and Event Management (SIEM) und Security Operations Center (SOC) ("Security as a Service" von Swisscom) für die beteiligten Kantone bereitstellen. Damit soll die Resilienz der Kantone gegenüber Cyberangriffen gestärkt und sollen gemeinsame Synergien genutzt werden. Bei einem solchen Center handelt es sich um ein externes Team von IT-Sicherheitsexperten, welches die gesamte IT-Infrastruktur des Kantons rund um die Uhr überwacht. Ziel ist es, Cyber-Sicherheitsereignisse in Echtzeit zu erkennen und diesen so schnell und effektiv wie möglich entgegenzutreten. Somit alles gut? Nein, meine Damen und Herren, dem ist bei Weitem nicht so. Weshalb aber fordert diese Interpellation jetzt eine Zertifizierung mit der Analyse von Kosten und Nutzen? Das möchte ich dann gerne noch darlegen und beantrage deshalb Diskussion.

Abstimmung:
Diskussion wird mit 95:5 Stimmen bei 4 Enthaltungen beschlossen.

Patrick Siegenthaler, Die Mitte/EVP: Ich möchte nochmals diese Frage aufwerfen: Weshalb fordert diese Interpellation eine Analyse von Kosten und Nutzen einer Zertifizie-

rung? Denn ich höre sehr oft, Zertifizierungen würden keinen sonderlich guten Ruf geniessen. Eine Zertifizierung wie diese, nach ISO27001, sagt in erster Linie etwas darüber aus, wie oder wie sehr sich ein Unternehmen oder eine Verwaltung mit Aspekten der Informationssicherheit auseinandersetzt. Eine Zertifizierung an sich schafft nur sehr bedingt Sicherheit. Die zentrale Frage ist, wie Prozesse, Richtlinien und Best Practices im Alltag tatsächlich umgesetzt werden. Ein ISO-Zertifikat ist also in erster Linie ein Indikator dafür, dass sich die Organisation mit Fragen der Informationssicherheit beschäftigt. Eine Zertifizierung würde unmittelbar dafür sorgen, dass alle relevanten Aspekte systematisch, dauerhaft und prozessorientiert unter die Lupe genommen werden. Weshalb wehrt sich nun aber die Regierung gegen eine solche Zertifizierung? Weshalb wurde die Zertifizierung kürzlich sogar aufgegeben? Das wirft Fragen auf. In der Antwort der Regierung steht, dass aufgrund des Strategiewechsels beim Amt für Informatik kein Bedarf mehr für eine nach aussen wirkende Zertifizierung bestehe. Das primäre Ziel einer Zertifizierung ist jedoch nicht die Aussenwirkung. Dabei handelt es sich nicht um eine Marketingmassnahme, sondern es geht darum, zu gewährleisten, dass Organisation, Prozesse und Technologie auf eine nachhaltige und effektive Zielerreichung ausgerichtet sind. Wenn zum Leistungsauftrag des Amtes für Informatik (AFI) die Gewährleistung der Informationssicherheit zählt, dann muss die Erfüllung auch nachweislich erfolgen. Dieser Nachweis ist üblicherweise ein Bericht einer externen Stelle. Die in der Antwort genannten externen Prüfungen beziehen sich jedoch nur auf die Ebene der Technik und sind deshalb nicht ausreichend. Ich komme zurück zu diesem Security Operations Center. Auch “Security as a Service” von Swisscom zeigt eindrücklich, dass unter IT-Security wohl in erster Linie technische Massnahmen verstanden werden. Als ein weiteres Argument gegen eine externe Zertifizierung werden hohe Kosten ins Feld geführt. Meine Damen und Herren, ich habe heute eine gute Nachricht für Sie, insbesondere in dieser angespannten Finanzsituation. Die Angaben zu den Kosten sind hinsichtlich ISO-Audit massiv überhöht. Hier verschätzt man sich gewaltig – etwa um Faktor 10. Die Zertifizierungsstelle berechnet die Kosten in erster Linie basierend auf der Anzahl der Mitarbeitenden sowie auf der Komplexität der betriebenen Infrastruktur. Die Kosten für eine Zertifizierung und ein Überwachungsaudit dürften deshalb in ähnlicher Höhe liegen wie bei einem typischen Schweizer IT-KMU, bei ca. 15'000 Franken. Die Kosten werden hier mit rund 200'000 Franken viel zu hoch ausgewiesen. Weshalb solch ein Aufwand, wenn doch alles schon so gut wie bereit ist? Wenn tatsächlich jeweils so hohe Kosten für die Vorbereitung des Audits anfallen wie angegeben, dann ist das ein alarmierendes Zeichen, dass Organisation und Prozesse nicht wie in der Antwort beschrieben funktionieren. Heute wird in vielen öffentlichen Ausschreibungen, gerade auch kürzlich im Kanton Thurgau, verlangt, dass die Anbieter ISO27001-zertifiziert sind oder zumindest alle Richtlinien und Empfehlungen erfüllen. Die Frage ist jetzt: Weshalb geht der Kanton hier nicht mit einem guten Beispiel voran? Weshalb wehrt sich die Regierung gegen diese Zertifizierung? Das AFI wäre gut beraten, wenn es sich extern unabhängig bestätigen

liesse, dass es so gut ist, wie es selbst von sich annimmt und sich beschreibt. Auch wir hatten bei uns im Unternehmen, wie viele andere Firmen auch, das Gefühl gehabt, alles im Griff zu haben. Erst das umfassende Audit hat offensichtliche Schwachstellen zutage gebracht und hat uns dabei unterstützt, unsere IT-Sicherheit zu verbessern. Wenn wir heute nun von Ratskollegin Michèle Strähl-Obrist und vom Regierungsrat hören, dass nun die Gerichte digitalisiert werden, sehen wir: Die Digitalisierung ist noch lange nicht abgeschlossen. Wir sind mittendrin in diesem Prozess, und Informationssicherheit ist ein zentrales Thema. Ich komme zum Schluss: Eine Zertifizierung – das ist ganz wichtig – ist nicht die einzige Möglichkeit. Aus eigener Erfahrung handelt es sich für mich um den besten Weg. Da der Kanton noch nicht aufgestellt ist für interne Kontrollen, beispielsweise durch die Finanzkontrolle, ist es wohl aktuell die beste Option. Ich appelliere, geschätzter Regierungsrat, an die Verantwortung des Regierungsrates als Aufsichtsorgan. Unsere Regierungsrätinnen und Regierungsräte scheinen hier ihre Führungsrolle und die Verantwortung bezüglich der IT-Sicherheit noch nicht umfassend respektive ausreichend wahrzunehmen. Setzen Sie ein wirksames Controlling auf, bevor es zu spät ist.

Simon Vogel, GRÜNE: Im Namen der GRÜNE-Fraktion danke ich dem Interpellanten für die gestellten Fragen. Eine sichere und zuverlässige IT-Infrastruktur ist heute ein zentraler Teil jedes Unternehmens und auch jeder öffentlichen Verwaltung. Angriffe werden häufiger, und die IT-Verantwortlichen stehen vor grossen Herausforderungen. Die Beantwortung der Regierung zeigt: Diese Risiken sind dem Amt für Informatik bewusst. Es werden viele wichtige Massnahmen ergriffen, und die GRÜNE-Fraktion ist überzeugt, dass das AFI gute Arbeit leistet. Konkrete Einblicke können jedoch aus Sicherheitsgründen in der Beantwortung leider nicht gegeben werden. Dies ist in einem gewissen Masse verständlich, unterstreicht jedoch genau die Wichtigkeit von externen Kontrollen und Audits. Kern der Interpellation ist nun, ob diese externe Überprüfung im Rahmen der ISO27001-Norm offiziell zertifiziert werden soll. Diese Zertifizierung gibt eine gewisse Sicherheit, dass die notwendigen Normen eingehalten werden und dass diese auch regelmässig überprüft werden. Der Kanton Thurgau hat diesen Aufwand betrieben und über mehr als zehn Jahre diese Zertifizierung erhalten. Dies insbesondere, um gegenüber externen Kunden die Qualität der IT-Infrastruktur sicherzustellen. Mit der neuen Strategie und dem Wegfall dieser Kunden wurde nun auch die Zertifizierung nicht mehr verlängert. Das AFI hat jedoch auch 300'000 Kundinnen und Kunden, welche in Zukunft die IT-Systeme immer häufiger benutzen werden; und auch diese haben einen Anspruch darauf, dass die Sicherheit gewährleistet ist und dass diese regelmässig überprüft wird. Der Regierungsrat erwartet nicht, dass die Zertifizierung für die Einwohnerinnen und Einwohner des Kantons Thurgau bei der Benutzung dieser Dienste von entscheidender Bedeutung ist, womit er vermutlich auch recht hat. Jedoch vertrauen die Einwohnenden darauf, dass die Systeme sicher sind, und es liegt an uns als Parlament, hier genau hinzuschauen und eben für dieses Vertrauen zu sorgen. Für die GRÜNE-Fraktion ist es hier-

bei zentral, dass externe Überprüfungen stattfinden, welche eine neutrale Sichtweise geben und auch unangenehme Fragen stellen. Wird dies im Rahmen einer ISO-Zertifizierung gemacht, stellen wir sicher, dass die entsprechenden Standards eingehalten werden und dass die Sicherheit von einer unabhängigen Stelle verifiziert wird. Wenn bereits alles, wie in der Beantwortung angetönt, auf dem Niveau dieser ISO-Norm erfolgt, sollte sich auch der Aufwand in Grenzen halten. Es ist jedoch klar, dass eine solche Zertifizierung Aufwand und Kosten bedeutet. Gerade bei der Sicherheit der IT-Infrastruktur unseres Kantons muss es uns das wert sein. Die GRÜNE-Fraktion erwartet, dass der Regierungsrat die erneute Zertifizierung ernsthaft prüft und möglichst bald wieder über eine Einführung nachdenkt.

Celina Hug, GLP: Wohnadressen des Bundesrates, lahmgelegte Webseiten: 2023 war ein erfolgreiches Jahr für Hacker. Die Thurgauer Polizei half, eine der gefährlichsten russischen Ransomware-Banden zu stoppen. Cybercrime betrifft uns alle, mit verheerenden Auswirkungen auf Wirtschaft und Gesellschaft. Die GLP-Fraktion bedankt sich bei Ratskollege Patrick Siegenthaler für die Fragen. Die dynamische Verbreitung der Digitalisierung in allen Bereichen unserer Gesellschaft erfordert von der Politik eine Haltung bezüglich ihrer Auswirkungen, Chancen und Risiken. Wir von der GLP-Fraktion wollen die Chancen der Digitalisierung nutzen, um sie für unsere Umwelt, Wirtschaft und freie Gesellschaft positiv einzusetzen. Der Schutz kritischer Systeme und sensibler Informationen vor digitalen Angriffen ist für uns eine wichtige Grundlage. Wir schätzen es, dass sich der Regierungsrat dem Thema Informationssicherheit annimmt und diese hoch priorisiert. In seiner Antwort schreibt er, dass Cyberangriffe verheerende Auswirkungen auf Organisationen haben können. Es wird von Reputationsschäden und finanziellen Schäden gesprochen. Leider macht er dabei keine konkrete Aussage zur potenziellen Schadenshöhe. In der Privatindustrie verursacht ein erfolgreicher Hackerangriff auf ein Grossunternehmen einen durchschnittlichen wirtschaftlichen Schaden von rund 2 Mio. Franken. Im Juni 2023 konnte das AFI Cyberangriffe durch technische Massnahmen abwehren, und es wird uns dargelegt, dass die Technik "up to date" sei und dass die Mitarbeiter sensibilisiert seien. Doch ist das wirklich so, und reicht das aus? Der Regierungsrat führt aus, dass die Norm ein guter Ausgangspunkt und die Orientierung daran für jede IT-Betriebsorganisation sinnvoll sei. Man habe die Zertifizierung zwischen 2006 und 2019 jeweils insbesondere durchgeführt, um einen Fähigkeitsausweis gegenüber privaten Unternehmen zu haben, die man damals vermehrt akquirieren wollte. Ab 2020 sei diese Zertifizierung nicht mehr nötig. Man bediene nur noch die kantonale Verwaltung und Thurgauer Gemeinden. Man orientiere sich aber nach wie vor an den erreichten Standards. Diese Aussage erstaunt doch sehr. Wie man der Antwort der Regierung weiter entnehmen kann, sei der Aufwand enorm und der Ertrag dazu im Missverhältnis. Man bezeichnet die Zertifizierung sogar als Etikett nach aussen, die man jetzt nicht mehr brauche. Ich hoffe, die 13 Jahre waren kein Etikettenschwindel. Auf die Nutzungsakzep-

tanz der Onlineportale werde sich eine ISO-Zertifizierung, welche die Einhaltung des Sicherheitsstandards überprüft, nicht signifikant auswirken. Bei den Nutzern stünden andere Kriterien im Vordergrund. Das stimmt – die Benutzererfahrung hängt nicht von der Cybersicherheit ab; ausser in den Fällen, bei denen etwas Kriminelles geschieht. Es wird heute schlicht und einfach vorausgesetzt, dass die Cybersicherheit maximal ist. Die Rezertifizierungskosten von 200'000 Franken erscheinen uns sehr hoch. Das geht sicher noch günstiger. In Anbetracht der potenziellen Schäden durch Cyberangriffe sind diese Kosten verhältnismässig, zumal sich das jährliche Audit um die 50'000 Franken bewegt. Erpresser haben im Mai 2023 das Schulnetzwerk des Kantons Basel-Stadt angegriffen und grosse Mengen an teilweise heiklen Informationen veröffentlicht. Auch Angaben zu einzelnen Schülerinnen und Schülern schienen sich darunter zu befinden. Wann lesen wir eine solche Schlagzeile über den Kanton Thurgau? Cyberangriffe darf man nicht auf die leichte Schulter nehmen. Durch eine unabhängige Kontrolle von Standards könnten Schwachstellen entdeckt und eliminiert werden. Meist ist es gut, die Organisation mit anderen Augen zu sehen, eine zweite Meinung zu haben, auf Herz und Nieren geprüft zu werden. Die GLP-Fraktion würde es daher sehr begrüssen, wenn das AFI eine Rezertifizierung umsetzen und jährlich auditieren würde. Wir begrüssen es, wenn die Regierung in diese Richtung aktiv wird.

Linda Hess, SP und Gew.: In erster Linie auch von mir einen Dank für die ausführliche Beantwortung der Fragen. Dass die Mitarbeitenden des Kantons alles in ihrer Macht Stehende tun, um die IT-Security zu gewährleisten, freut mich, und im Grundsatz glaube ich ihnen das auch. Ich möchte hier nicht die gute und engagierte Arbeit aller in diesem Bereich kritisieren. Ich möchte aber, dass wir garantieren, dass die kantonalen Verwaltungen, die mit äusserst persönlichen Daten arbeiten, mit diesen so sicher wie möglich umgehen. Diese Daten geben wir Bürgerinnen und Bürger zum grössten Teil nicht freiwillig heraus, sondern von Gesetzes wegen. Wir haben da also keine Wahl. Meist ist die Herausgabe dieser Daten ja nicht optional; man ist verpflichtet. Und daher sind wir verpflichtet, für die Sicherheit dieser Daten zu garantieren. Irritiert hat mich die Beantwortung vor allem bezüglich zweier Punkte. Erstens: wie schon erwähnt, betreffend die hohen Kosten der Zertifizierung. Wenn der Kanton die Anforderungen bereits erfüllt, sind diese aus meiner Erfahrung – ich habe selbst schon solche Zertifizierungen durchgeführt – nicht so hoch wie dargestellt. Wenn diese Rechnung tatsächlich so hoch sein sollte, muss offensichtlich nachgebessert werden, und nicht nur in der Dokumentation. Zweitens: Die Antwort auf die Anfrage von Ratskollege Patrick Siegenthaler war zu erwarten: Natürlich kann man nicht konkrete Probleme im Bereich der IT-Security zugeben. Es ist aber eine Antwort ohne jegliche Selbstkritik. Ich habe lange genug im Bereich der IT-Security gearbeitet, um aufzuhorchen, wenn alles einfach nur gut läuft. Das ist der Hauptgrund, wieso ich und grossmehrheitlich auch die Fraktion SP und Gewerkschaften Sie bitten, die Zertifizierung erneut anzustreben. Wir können nicht konkret in diesen Be-

reich der Arbeit des Kantons Einsicht nehmen. Eine Zertifizierung garantiert uns aber, dass ein minimaler – und ich möchte hier betonen, die Zertifizierung ist ein minimaler – Standard eingehalten wird. Wir sind als Kantonsräte und Kantonsrätinnen verpflichtet, von der Regierung in diesem Bereich Sicherheit zu verlangen und diese auch zu kontrollieren. Das können wir aktuell nicht: Die Sicherheit der – noch einmal, um das zu betonen – äusserst persönlichen Daten der Einwohnerinnen und Einwohner des Kantons Thurgau garantieren. Wir bitten Sie daher, Ihre ablehnende Haltung der Zertifizierung gegenüber noch einmal zu überdenken.

Christian Caviezel, EDU/Aufrecht: Ich bedanke mich bei Ratskollege Patrick Siegenthaler, dieses Thema aufgenommen zu haben. Es ist wichtig, sich der Risiken bewusst zu sein und entsprechende Massnahmen zeitgemäss zu treffen. Eine ISO-Zertifizierung kann dienen, aber auch Ressourcen binden. Aktuell sind finanzielle und personelle Ressourcen ein knappes Gut. Wir sprechen von Fachkräftemangel und Kosteneinsparungen. Da gilt es, schlank und effizient zu sein. Es ist richtig, Aufwand und Ertrag abzuwägen. Eine hundertprozentige Sicherheit wird es jedoch nicht geben, und sich mit Zertifizierungen abzusichern, ist der falsche Ansatz. Die Fraktion EDU/Aufrecht sieht in einer weiteren Zertifizierung eher eine Massnahme, eine Scheinsicherheit zu erzeugen. Diese birgt die Gefahr, sich mit einem ausgewiesenen Qualitätssiegel eine Versicherung zu schaffen, welche bei einem Schadensfall vorgewiesen werden könnte; eine Versicherung, um Verantwortung abzuwälzen, anstatt diese persönlich mit Namen und Gesicht zu tragen. Es gilt, dem Fachpersonal Sorge zu tragen, dieses zu unterstützen bei der Kernaufgabe und nicht zu beschäftigen mit zusätzlichen Hürden. Es macht mehr Sinn, die vorhandene Energie in eine straffe, nahe Führung der Regierung zu investieren, das bestehende verantwortliche Fachpersonal zu stützen, anstatt es mit mehr Vorschriften und Reglementen zu beschäftigen. Das scheint zielführender. Die Fraktion EDU/Aufrecht appelliert daran, diese wichtigen Funktionen der führenden Mitarbeitenden weiter zu fördern und zu stärken, auch ohne Zertifizierung.

Raphael Stutz, SVP: Ratskollege Patrick Siegenthaler, ich bedanke mich für das Aufgreifen dieses Themas. Die Mitglieder der SVP-Fraktion haben einiges lernen dürfen. Ich muss ganz ehrlich sagen: Ich wusste bis zu dieser Interpellation nicht, dass es eine solche gibt. Die SVP-Fraktion hat das diskutiert und sieht eine Gefahr in der Cyberkriminalität respektive sieht ein Risiko im Internet und in den Netzwerken. Wir glauben aber auch, dass die Regierung sich ihrer Verantwortlichkeit bezüglich dieses Themas bewusst ist, weil der Schaden auf Kostenseite wie auch auf Vertrauensseite gegenüber den Kundinnen und Kunden, den Bürgerinnen und Bürgern immens sein kann. Wir sind aber nach erfolgter Diskussion zum Schluss gekommen, dass wir als SVP-Fraktion der Regierung vertrauen, dass sie die nötigen Instrumente und die Erfahrung in ihre Arbeit einfliessen lässt. Wir sind deshalb nicht davon überzeugt, dass wir diese Rezertifizierung brauchen.

Wir danken dem AFI, dass es dieser Diskussion zuhört und noch ein höheres Augenmerk auf diese Thematik setzt.

Sandra Stadler, Die Mitte/EVP: Vielen Dank dem Regierungsrat für die Beantwortung und herzlichen Dank unserem Fraktionskollegen Patrick Siegenthaler für das wichtige Thema, über das wir hier im Rat diskutieren können. Ich spreche im Namen der Fraktion Die Mitte/EVP. Cybersecurity, Datenschutz und Informationssicherheit sind heute zentrale Themen, gerade auch für eine öffentliche Verwaltung, die viele sensible Daten der Bürgerinnen und Bürger verarbeitet und speichert. Eine externe Überprüfung, nicht nur auf technischer Ebene, ist daher wichtig. Unseres Erachtens hat der Bürger ein Recht auf Transparenz, wofür die Verwaltung zum Schutz seiner Daten Verantwortung übernimmt. Ich selbst habe vor über 20 Jahren in einem Amt des Kantons Thurgau gearbeitet, das bereits dazumal, 2003, eine ISO-Zertifizierung eingeführt hat. Damals war ich eher der Meinung, dass das nicht verhältnismässig sei und dass man den externen Auditoren sowieso sagen kann, was man möchte. Heute bin ich etwas erfahrener und weiss, wie heikel der Umgang mit Personendaten ist. Zudem wissen wir leider alle, dass niemand mehr von Angriffen im digitalen Raum verschont bleibt. Bei Vorstandstätigkeiten oder in der Freiwilligenarbeit ist dies ein zentrales Thema. Ja, Fraktionskollege Patrick Siegenthaler stellt die richtige Frage: Warum wehrt sich die Regierung gegen eine solche Zertifizierung? Der Regierungsrat hat die Aufgabe, unsere Verwaltung zu führen und zu kontrollieren. Er trägt letztlich die Verantwortung. Ob er diese Verantwortung wahrnimmt, indem er das Amt zu einer Zertifizierung verpflichtet, oder indem er regelmässig einen Bericht der Finanzkontrolle über die IT-Sicherheit einfordert, ist dem Regierungsrat zu überlassen. Das ist für uns zweitrangig. Auch so kann eine externe Kontrolle sichergestellt werden. Aber haben wir in unserem Kanton auch die entsprechenden IT-Fachleute? Wir können uns gut vorstellen, dass dies aktuell noch nicht so ist, aber da könnte man ja aufrüsten.

René Walther, FDP: Die FDP-Fraktion bedankt sich beim Interpellanten für die gestellten spannenden Fragen zu einem aktuellen und sehr ernst zu nehmenden Thema. Genauso möchten wir uns auch bei der Regierung für die differenzierte Beantwortung bedanken. In meiner beruflichen Laufbahn konnte ich Erfahrungen im Prozessmanagement, und damit verbunden mit verschiedenen Zertifizierungssystemen im Bereich Maschinenbau, Umweltmanagement, IT etc., sammeln. Tatsächlich kann ein Zertifizierungsprozess im Zusammenhang mit der Einführung eines Qualitätssicherungssystems ein wertvoller Wegweiser sein, Prozesse systematisch und gezielt zu erfassen, zu dokumentieren, weiterzuentwickeln und Risiken zu reduzieren. Der nachhaltige Nutzen nach der Zertifizierung ist jedoch wesentlich davon abhängig, wie der Umgang mit den Prozessen in den kontinuierlichen Verbesserungsprozessen und eben in der Kultur der Unternehmung implementiert und verankert ist. Es stellt sich die Frage, ob das Ziel des

Handelns mehr dem Erhalt des Zertifikats oder eben der ernstgemeinten, stetigen Weiterentwicklung und Optimierung der Prozesse dient. Dies gilt übrigens aus meiner Sicht für die meisten Managementprozesse, wie zum Beispiel auch das interne Kontrollsystem einer Organisation. Formulare einmal pro Periode auszufüllen und quasi durch eine Proforma-Dokumentation festzuhalten, ist keine Garantie für fehler- und störungsfreie Verfahren und Abläufe. Aber klar: Regelmässig und seriös durchgeführte Audits oder Prozessüberprüfungen können das Risiko und Fehlerbewusstsein verbessern und helfen, Störungen zu vermeiden. Dies sollte aber in angemessenen Perioden und nicht nur zum Rezertifizierungs-Zeitpunkt erfolgen. Dazu ist nicht zwingend eine Rezertifizierung notwendig. Dies kann auch durchaus im Rahmen eines internen Kontrollsystems sichergestellt werden. Prozessmanagement ist nicht an Zertifikate, sondern an eine innere Überzeugung und ein entsprechend gelebtes Führungssystem gekoppelt. Unseres Erachtens konnte der Regierungsrat in seiner Beantwortung diese Überzeugung glaubhaft darlegen. Die FDP-Fraktion glaubt, dass die Ressourcen zurzeit gut in diesen laufenden Managementprozess investiert sind, was nicht heissen soll, dass zu gegebener Zeit eine Überprüfung und die Erneuerung des Qualitätsmanagement-Systems nicht prüfenswert wäre. Wir sehen zurzeit aber keinen Handlungsbedarf.

Regierungsrat Walter Schönholzer: Sie können mir glauben, der Regierungsrat nimmt die Abwehr von Cyberrisiken und die Datensicherheit sehr, sehr ernst. Es ist uns hundertprozentig bewusst, dass diese Sicherheit das höchste Gut ist im Umgang mit Daten unserer Bürgerinnen und Bürger. Unsere Digitalisierungsstrategie kann nur erfolgreich umgesetzt werden, wenn maximales Vertrauen der Bevölkerung in die Datensicherheit vorhanden ist. Aber ich bitte, und das steht ja schon in der Beantwortung, auch um Verständnis dafür, dass der Regierungsrat keine Details zu Sicherheitsvorkehrungen veröffentlichen kann, und ich werde es auch heute nicht tun. Wir haben schon früh, vor der Einreichung der Interpellation, dem Interpellanten angeboten, er könne sich mit den Verantwortlichen im AFI im Detail dazu austauschen, und er hat diese Gelegenheit auch genutzt. Weshalb dann diese Interpellation doch noch eingereicht wurde, weiss ich nicht so genau. Aber die Diskussion, die wir jetzt heute darüber führen können, die ist schon sehr wertvoll. In diesem Sinne danke ich Kantonsrat Patrick Siegenthaler aufrichtig dafür, dass er das gemacht hat. Aber, was die heutige Diskussion anbetrifft, könnte man ja jetzt meinen, dass ein solches Zertifikat ein Garant für die erfolgreiche Abwehr von Cyberattacken wäre. Meine Damen und Herren: Ich weiss, dass Sie auch wissen, dass dem nicht so ist. Niemand – keine Unternehmung, keine Organisation, ist vor einer erfolgreichen Attacke gefeit. Dies zeigen auch Beispiele, die Sie teilweise genannt haben. Und wenn jeweils wieder so eine Konferenz, wie zum Beispiel kürzlich jene auf dem Bürgenstock, stattfindet, dann explodieren die Angriffe. Gott sei Dank ist es unserem Amt für Informatik bisher gelungen, immer alle Attacken erfolgreich abzuwehren. Sie sehen also, unsere Fachleute im AFI sind intensiv auf diese Thematik fokussiert. Ich lade auch gerne

die Subkommission des Departements für Inneres und Volkswirtschaft (DIV) dazu ein, sich im Rahmen eines Ämterbesuches davon überzeugen zu lassen. Warum – das habe ich jetzt mehrfach gehört – wehrt sich dann der Regierungsrat gegen diese Zertifizierung? Ganz einfach: Weil wir nicht suggerieren wollen, dass dann alles gut wäre. Dem ist einfach nicht so. Die Herausforderungen sind derart komplex, dass wir uns entschieden haben, auch in diesem Bereich mit sechs Ostschweizer Kantonen intensiv zusammenzuarbeiten, mit ihnen gemeinsame Ausschreibungen und Vergaben zu machen. Der Interpellant hat es angesprochen: Der Auftrag ging an die Swisscom. Wir arbeiten auch mit dem Bund zusammen, weil kein Kanton, kein Amt und kein Mitarbeiter diese Thematik allein erfolgreich bearbeiten kann. Wir investieren auch sehr viel in die Sensibilisierung und Ausbildung unserer Mitarbeitenden, weil dort die grössten Risiken vorhanden sind. Die Einfallstore entstehen oft durch die unbedarfte Nutzung von E-Mails oder anderen elektronischen Daten, die dann dazu führt, dass solche Einfallstore zustande kommen. Wir haben es in der Beantwortung ausgeführt: Diese Zertifizierung ist ein Qualitätssiegel, das man vor allem dann braucht, wenn man Produkte vertreiben will. Dann ist es ein Gütesiegel. Das heisst jetzt aber nicht, dass der Kanton Thurgau hier lasch werden würde, sondern dieses Niveau, das wir damals erreicht haben, das halten wir hoch. Ob die Summen, die Kantonsrat Patrick Siegenthaler genannt hat, stimmen oder nicht – ich verlasse mich hier auf das, was wir aus der Erfahrung gelernt haben, und was meine Fachleute vom Amt für Informatik gezeigt haben. Ich verlasse mich darauf. Wir verkaufen unsere Software nicht mehr, wir haben aber unsere Prozesse in diesem Bereich im Griff. Es gibt aber immer wieder Weiterentwicklungen, die auch zu Investitionen seitens des Kantons führen; sei es eben in solche gemeinsamen Produkte, Projekte mit anderen Kantonen zur Cyber-Abwehr, sei es in die Beschaffung von entsprechenden personellen Ressourcen. Meine Damen und Herren, das kann ich Ihnen jetzt schon ankündigen: Sie werden in der Budgetdebatte dann Gelegenheit haben, sich darüber auszutauschen, ob es das jetzt wert ist oder nicht. Ich werde Sie dann gerne an die Diskussion heute erinnern. Aufwand und Ertrag für dieses Feigenblatt, wie es der Sprecher der Fraktion EDU/Aufrecht genannt hat, die stehen für den Regierungsrat in klarem Missverhältnis – daran hat sich bis heute nichts geändert.

Diskussion – **nicht weiter benützt.**

Präsident: Das Geschäft ist erledigt.