Thurgau

Der Regierungsrat des Kantons Thurgau an den Grossen Rat

GRG Nr.	20	IN 46	519

Frauenfeld, 12. Dezember 2023

708

Interpellation von Patrick Siegenthaler vom 7. Juni 2023 „Kosten-Nutzen einer ISO27001-Zertifizierung im AFI Thurgau“

Beantwortung

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Angriffe auf Informations- und Kommunikationsstrukturen staatlicher Akteure, Unternehmen und Einzelpersonen nehmen zu. Die Professionalisierung einer eigentlichen Hackerindustrie, deren Akteure Sicherheitslücken vor den Herstellern oder Entwicklern entdecken (sog. „Zero-Day-Exploits“), sowie fehlende Daten zu Angriffszahlen und Schadenskosten erschweren die Einschätzung der Gefahren. Cyberangriffe haben potenziell verheerende Auswirkungen auf Organisationen, einschliesslich Datenverlust, Betriebsunterbrechungen und den damit einhergehenden Schäden finanzieller Natur sowie der Reputation.

Der Regierungsrat nimmt das Thema der Informationssicherheit sehr ernst und hat diverse Massnahmen ergriffen (siehe insbesondere auch die Beantwortung der Frage 7). Gleichzeitig bittet er um Verständnis, dass aus Sicherheitsgründen nicht auf Einzelheiten zu den Sicherheitsvorkehrungen eingegangen werden kann.

Frage 1

Cyberrisiken werden vom Amt für Informatik (AFI) aus verschiedenen Quellen identifiziert. Generelle und akute Cyberrisiken werden durch die Teilnahme des Chief Information Security Officer (CISO) am wöchentlichen Cyberbriefing des nationalen Zentrums für Cybersicherheit (NCSC) und im engen Austausch mit den umliegenden Kantonen erfasst. Ist dies angezeigt, werden präventive Abwehrmassnahmen eingeleitet.

Direkt adressierte Risikomeldungen von Herstellern werden vom CISO zusammen mit der Einheit IT-Security-Operations des AFI auf Relevanz geprüft und gegebenenfalls durch technische Spezialistinnen und Spezialisten die notwendigen Schritte eingeleitet. Ist für eine gemeldete Sicherheitslücke seitens Hersteller keine Lösung verfügbar, wird das Risiko mit anderen Massnahmen mitigiert. Das können angepasste Firewalleinstel-

lungen sein, die Isolation in einer eigenen Netzwerkzone oder im Extremfall die komplette Trennung des betroffenen Systems vom Netzwerk.

Die Einheit IT-Security-Operations des AFI ist mit der permanenten Überwachung der IT-Infrastruktur und des Datenverkehrs auf den Netzwerkstrecken betraut. Mithilfe moderner Monitoringsysteme werden Anomalien automatisch identifiziert, in einer Überwachungskonsole in Echtzeit angezeigt und nach bestimmten Kriterien eine Alarmierung der relevanten Personen ausgelöst. Je nach Kritikalität der Alarmierung analysiert das zuständige Team gemeinsam mit dem CISO die Situation. Wenn nötig werden Sofortmassnahmen eingeleitet, und – sollte es die Situation erfordern – wird ein formeller „Major Incident“ ausgelöst. Aus Sicherheitsgründen kann nicht im Detail auf die einzelnen Schritte eingegangen werden.

Weiter führt das AFI periodische IT-Security-Assessments mit externen Spezialistinnen und Spezialisten durch. Dabei werden u.a. einzelne Systeme oder Netzwerkzonen auf ihre Angreifbarkeit überprüft. Feststellungen werden kategorisiert, priorisiert und in einem Massnahmenkatalog festgehalten. Um die systematische Bearbeitung der Massnahmen sicherzustellen, ist ein so genanntes Incident-Management-Tool im Einsatz.

Die Nutzerinnen und Nutzer sowie die AFI-Mitarbeiterinnen und AFI-Mitarbeiter im Besonderen werden durch regelmässige Informationen des CISO in der AFI-Geschäftsleitung, das „AFI Info“, Online-Informationsveranstaltungen und Schulungen darauf sensibilisiert, allfällige Sicherheitsvorfälle sofort an den Servicedesk zu melden. Dieser leitet die gemeldeten Fälle umgehend an das IT-Security-Operations-Team weiter, das eine Einschätzung über zu treffende Massnahmen vornimmt. Alle gemeldeten Risiken und Sicherheitsvorfälle sowie die Massnahmen dazu werden vom CISO gesammelt. Dieser führt ein entsprechendes Inventar und überprüft dieses laufend mit der Risikoeinschätzung des NCSC sowie im regelmässigen Austausch mit den Verantwortlichen aus anderen Kantonen. Daraus leitet der CISO den kurz-, mittel- und längerfristigen Handlungsbedarf ab. Über zu treffende Massnahmen entscheidet grundsätzlich die AFI-Geschäftsleitung, der CISO verfügt aber auch über die Kompetenz, im Bedarfsfall eigenständig Sofortmassnahmen anzuordnen.

Das AFI investiert viel in die Prävention. Im Einzelnen sind folgende Massnahmen zu nennen:

– Die Software auf sämtlichen Systemen wird ständig auf dem aktuellen Stand gehalten.
– Die vom AFI vorgegebene Projektmethodik berücksichtigt die Anforderungen an die Sicherheit in jeder Phase.
– Datenträger von ausgemusterter Hardware werden konsequent vernichtet.
– Wird der Betrieb eines Systems an einen externen Auftragnehmer übergeben, wird dessen Sicherheits-Zertifizierung auf die Erfüllung der Sicherheitsanforderungen des AFI geprüft und es werden vertragliche Regelungen in Bezug auf Datensicherheit und Datenschutz vereinbart.

Weitere Sicherheitsmassnahmen sind Zutrittskontrollen, die Aufzeichnung sämtlicher Zugriffe, der Einsatz vorgeschalteter Sicherheitssysteme, diverse Prüfprozesse und ein

ausgereiftes Backup-Konzept. Siehe hierzu auch die Beantwortung der Frage 1 der Einfachen Anfrage „Ist die kantonale Verwaltung gegen Cyberrisiken gerüstet?“ vom 1. März 2023 (GR 20/EA 191/468).

Frage 2

ISO 27001 ist ein international anerkannter Standard für Informationssicherheitsmanagement. Der Hauptzweck von ISO 27001 besteht darin, Organisationen dabei zu helfen, ein effektives Informationssicherheitsmanagementsystem (ISMS) zu etablieren, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

Mit der Einführung erhält ein Unternehmen einen systematischen Leitfaden, um die eigenen Informationssysteme zur Unterstützung der Geschäftsprozesse zu planen, umzusetzen, zu überwachen und stetig zu verbessern. Die Norm konzentriert sich dabei auf die systematische Untersuchung der Sicherheitsrisiken und die Berücksichtigung von Bedrohungen und Auswirkungen, bevor sie zur Implementierung von Kontrollen zur Risikominderung übergeht. So gesehen ist ISO 27001 ein guter Ausgangspunkt und die Orientierung daran für jede IT-Betriebsorganisation sinnvoll.

Die Zertifizierung bietet insbesondere dann einen Zusatznutzen, wenn ein Qualitätsnachweis erbracht werden muss, um beispielsweise Neukunden anzuwerben oder sich am Markt gegenüber der Konkurrenz zu differenzieren. Das AFI hatte zwischen 2006 und 2019 die Strategie verfolgt, auch ausserhalb der Kantonalen Verwaltung Thurgau (KVTG) öffentlich-rechtliche Kunden zu gewinnen. In diesem Rahmen liess sich das AFI 2009 für die ISO-Normen 9001 und 27001 zertifizieren.

Mit der neuen strategischen Ausrichtung 2020 und der damit verbundenen Konzentration auf die KVTG und die Politischen Gemeinden im Kanton ist eine Zertifizierung aus Sicht des Regierungsrates nicht mehr notwendig. In der Konsequenz wurden die Zertifikate 2021 bewusst nicht mehr erneuert. Das AFI orientiert sich aber weiterhin eng an den Normen ISO 27001 und 9001 sowie an weiteren Sicherheitsrahmenwerken wie beispielsweise dem Cyber Security Framework des amerikanischen National Institute of Standards and Technology (NIST CSF).

Das Ziel ist es, den durch die vormalige Zertifizierung erreichten Qualitätsstandard zu halten. Für die Sicherstellung dieser Zielerreichung ist AFI-intern der CISO zuständig.

Frage 3

Das AFI war wie erwähnt bis 2021 zertifiziert nach ISO 27001 sowie 9001 und weiss deshalb aus eigener Erfahrung, dass die Zertifizierung sowie die jährlichen Rezertifizierungen und die entsprechenden internen und externen Audits mit einem enormen administrativen Aufwand verbunden sind. Die Ressourcen, die für die Dauer einer Rezertifizierung im Betrieb fehlen, können unter Umständen dazu führen, dass wichtige Themen – gerade auch solche aus dem ISO-Portfolio – nicht mehr seriös behandelt werden können. Aufwand und Ertrag stehen dann in einem klaren Missverhältnis.

Die ISO-Zertifizierungen dienen zur Repräsentation auf dem Markt als gut strukturiertes und prozessorientiertes Unternehmen mit hohem Qualitätsstandard und somit haupt-

sächlich als Etikette gegen aussen. Dies steht für das AFI nicht im Vordergrund. Eine inhaltliche Orientierung an der Norm ergibt hingegen keine Nachteile.

Frage 4

Der Regierungsrat ist überzeugt, dass sich eine erneute ISO-Zertifizierung nicht signifikant auf die Nutzungsakzeptanz der künftigen Thurgauer Online-Services auswirken würde. Das zeigt sich auch im Umgang der Benutzerinnen und Benutzer mit anderen Portalen. Der grösste Teil der Bevölkerung nutzt beispielsweise Online-Banking-Services oder Social-Media-Plattformen, ohne zu hinterfragen, welche Normen oder Standards die Anbieter einhalten. Für die Akzeptanz sind Faktoren wie die Verfügbarkeit, die Stabilität, das eigentliche Angebot an Dienstleistungen und die nutzerfreundliche Bedienerführung wichtiger.

Frage 5

Die Zertifizierung für ISO 9001 und ISO 27001 hat das AFI in den Jahren 2008 und 2009 insgesamt rund Fr. 470'000 gekostet. Darin enthalten sind die internen Aufwände inkl. Schulungen, die externe Beratung und die Kosten für die Einführung einer Software für die revisionssichere Ablage der für die Zertifizierung notwendigen Dokumentationen. Da sich das AFI weiterhin an den Normen orientiert, würden bei einer erneuten Zertifizierung weniger Kosten entstehen. Eine erneute Zertifizierung würde gemäss Schätzung des AFI Kosten in der Höhe von gegen Fr. 200'000 verursachen.

Frage 6

Die Kosten der Audits für Überprüfungen und die Rezertifizierung sowie die Anpassungen an die überarbeiteten Normen betrugen in der Vergangenheit pro Jahr rund Fr. 50'000. Insbesondere aufgrund der Teuerung der letzten zwei Jahre dürfte dies mittlerweile teurer sein.

Frage 7

Der Regierungsrat hat in diesem Zusammenhang bereits eine ganze Reihe von Massnahmen veranlasst. Eine professionelle Organisation im AFI als interner Dienstleister, gefestigte Prozesse, moderne Technologien, gut ausgebildetes Personal sowie die Sensibilisierung auf allen Stufen sind dabei oberstes Ziel. Für die Handlungsfelder „Schützen und Erkennen“ sowie „Reagieren und Wiederherstellen“ sind unter anderem folgende Massnahmen eingeleitet worden:

Schützen und Erkennen

Das kantonale Datennetz, in dem alle IT-Systeme betrieben werden und sämtliche internen Benutzerinnen und Benutzer angeschlossen sind, ist auf professionellen Standards und einer State-of-the-art-Netzwerkarchitektur folgend aufgebaut (Netzwerk-Zonenkonzept). Eine moderne High-End-Firewall-Infrastruktur schützt und überwacht permanent den gesamten ein- und ausgehenden Datenverkehr. Diese wird durch das IT-Security-Operations-Team betrieben, das bei Bedarf interveniert und die notwendigen Prozesse einleitet.

Ein automatisiertes und durch künstliche Intelligenz (KI) gestütztes Cyber-Threat-Managementsystem löste den klassischen Virenscanner ab. Dieses wurde neben sämtlichen Clients auch flächendeckend auf der Server-Infrastruktur ausgerollt. Zudem läuft in Kooperation mit weiteren Ostschweizer Kantonen eine Ausschreibung mit dem Ziel, die Dienste eines professionellen „Security Information and Event Management“ (SIEM) sowie „Security Operations Center“ (SOC) zu integrieren.[1]

Das Personal des AFI wird laufend aus- und weitergebildet, und das AFI arbeitet eng mit spezialisierten Unternehmen zusammen, die unter anderem periodische Security Assessments durchführen. Diese Assessments werden durch das AFI selbst initiiert, die Resultate und Massnahmenvorschläge im Detail festgehalten und mit den Spezialistinnen und Spezialisten diskutiert. Ausserdem führt die Finanzkontrolle seit 2022 auch selbständig IT-Audits durch, die jeweils mit den betroffenen Spezialistinnen und Spezialisten des AFI sowie der Amtsleitung besprochen werden.

Reagieren und Wiederherstellen

Im Falle einer Attacke greifen strukturierte Abläufe zur Detektion, Isolation und Neutralisierung befallener IT-Systeme, auf die aus Sicherheitsgründen nicht näher eingegangen werden kann. In einer ersten Phase wird AFI-intern vorgegangen, danach werden externe Spezialistinnen und Spezialisten beigezogen.

Damit sind interne und externe Überwachungsinstrumente implementiert, die den Mehrwert einer erneuten ISO-Zertifizierung stark relativieren. Zudem gilt zu beachten, dass eine solche Zertifizierung keinen Schutz vor Cyberangriffen garantieren kann.

Der Präsident des Regierungsrates

Der Staatsschreiber

[1] https://www.inside-it.ch/ostschweizer-kantone-buendeln-ihre-kraefte-fuer-it-sicherheit-20231004.