Digitale Risiken sind Auftragsrisiken

IT-Modernisierungstrends wirken sich auf den Auftrag der Behörden aus

Von Bundesbehörden (ob nun Zivilbehörden, Verteidigungs- oder Geheimdienste) bis zu staatlichen und kommunalen Behörden nutzen Organisationen zunehmend die digitale Transformation, um ihren Wählern besser zu dienen, das Heimatland zu schützen, die Bürger mit Daten zu vernetzen und die Effizienz ihrer Behörde zu steigern.

Diese digitale Transformation ist kein über-Nacht-Phänomen. Sie begann mit den Gesetzen der 1990er Jahre (Clinger-Cohen Act von 1996)[1], die CIOs auf Behördenebene mit dem Management und der Umsetzung der IT-Modernisierung beauftragten. Das wurde im E-Government Act von 2002[2] fortgeführt, der die Internetnutzung für eine verbesserte Einbeziehung der Bürger an der Regierung fördert. Darauf folgte der Federal Information Security Modernization Act of 2002 (FISMA), der die Implementierung angemessener Sicherheitsmaßnahmen im Rahmen der behördenweiten Transformation gewährleistet. In jüngerer Zeit haben Richtlinien und Standards wie Cloud First[3] und Cloud Smart[4] Organisationen dazu veranlasst, die digitale Transformation in Behörden schnell voranzutreiben. Darüber hinaus haben Durchführungsverordnungen (Executive Orders) die Cyberagenda für die Administration skizziert. Durch all diese Veränderungen stehen IT- und Sicherheitsexperten der Behörden vor der Herausforderung, sicherzustellen, dass die Systeme und Daten sicher sind und sensible Behörden- und Bürgerdaten geschützt werden, während sie für die Stakeholder offen und transparent bleiben.

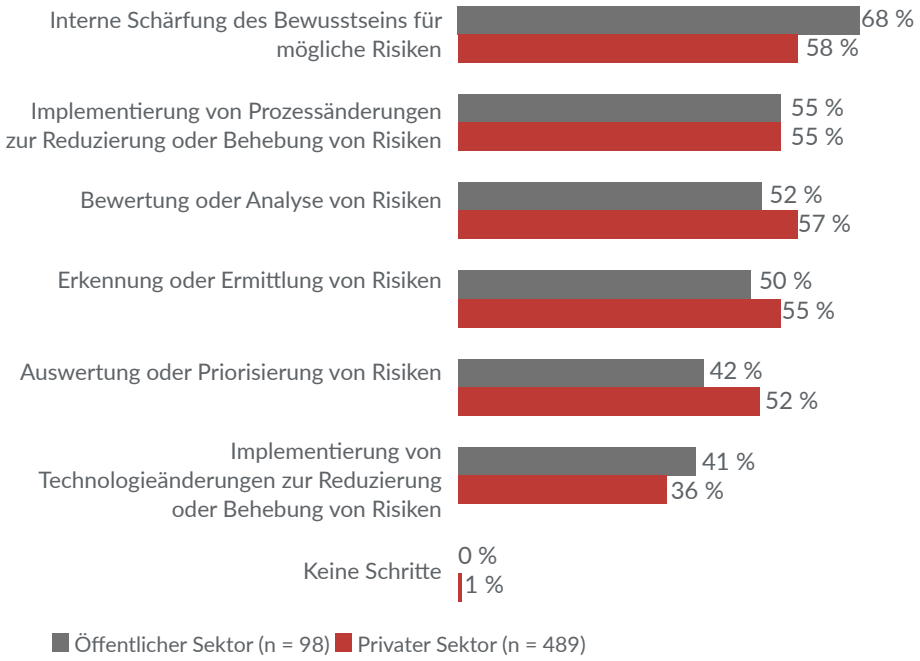
Sowohl eigenständig als auch in Zusammenarbeit mit anderen Organisationen (öffentlich und privat) verfolgen Regierungsorganisationen die digitale Transformation, um Auftragsergebnisse für Bürger zu erzielen, und sehen sich einem gewissen Maß an Potenzial für erhöhte Risiken gegenüber, die sich auf den Auftrag auswirken könnten. Da Behörden und ihre Partner daran arbeiten, die Behörden durch Online- und mobile Erfahrungen besser zugänglich zu machen, besteht auch die Gefahr, dass diese Aktivitäten den Betrieb sowie die Daten für Cyberangriffe anfälliger machen – ob von externen Akteuren wie z. B Staaten, Aktivisten und unzufriedene Bürger, die Chaos stiften wollen, oder durch Insiderbedrohungen von Behördenmitarbeitern. Mögliche Folgen können erhebliche Auswirkungen haben:

- Bedrohungen für die nationale Sicherheit
- Unterbrechungen im öffentlichen Dienst, bei Versorgungsbetrieben und im Gesundheitswesen
- Datenschutzverletzungen, Sicherheitsverletzungen und die Exposition von Millionen personenbezogener und finanzieller Daten der Bürger für Kriminelle im Dark Web
- „Leaks“ von vertraulichen Informationen mit dem Potenzial für internationale oder nationale Wellen der Empörung, Auswirkungen auf den wirtschaftlichen Handel und Gefährdung der Streitkräfte
- Wahlmanipulation mit nachfolgender Untergrabung des Vertrauens der Wähler in rechtmäßige Wahlen

Da Behörden und ihre Partner daran arbeiten, die Behörden durch Online- und mobile Erfahrungen besser zugänglich zu machen, besteht auch die Gefahr, dass diese Aktivitäten den Betrieb sowie die Daten für Cyberangriffe anfälliger machen.

Organisationen im öffentlichen Sektor sind sich der ernsten Natur digitaler Risiken sehr bewusst und ergreifen Maßnahmen, um diese zu mindern. Laut den Ergebnissen der RSA Digital Risk Study, die im 2019 RSA Digital Risk Report enthalten ist, gaben 68 % der Befragten im öffentlichen Sektor an, dass sie Maßnahmen ergreifen, um intern das Bewusstsein für die potenziellen Risiken der digitalen Transformation zu schärfen; im privaten Sektor waren es hingegen nur 58 % der Unternehmen. Das deutet darauf hin, dass Organisationen im öffentlichen Sektor die Unternehmen im privaten Sektor überflügeln, wenn es darum geht, die Mitarbeiter über die Risiken zu informieren und zu erklären, wie sie sich selbst sowie Behördendaten und -systeme vor böswilligen Akteuren schützen können.

Unternommene Schritte für das digitale Risikomanagement



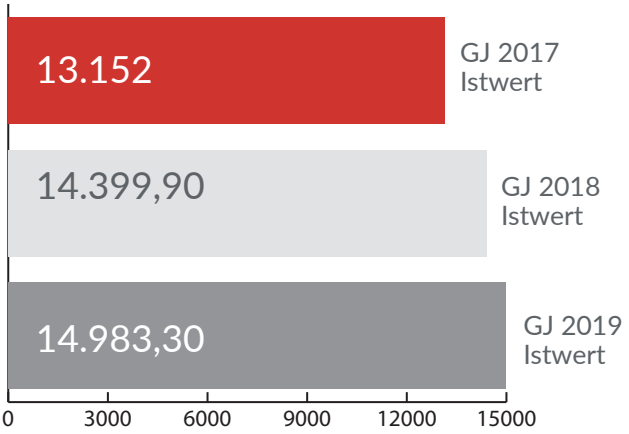
Laut den Ergebnissen der RSA Digital Risk Study, die im 2019 RSA Digital Risk Report enthalten ist, gaben 68 % der Befragten im öffentlichen Sektor an, dass sie Maßnahmen ergreifen, um intern das Bewusstsein für die potenziellen Risiken der digitalen Transformation zu schärfen; im privaten Sektor waren es hingegen nur 58 % der Unternehmen.

Zudem nannten die Befragten im öffentlichen Sektor drei Hauptbereiche digitaler Risiken, über die sie sich in den nächsten zwei Jahren am meisten Sorgen machen und die behoben werden müssen: Risiken von Cyberangriffen, Datenschutzrisiken und dynamische Mitarbeiterrisiken.

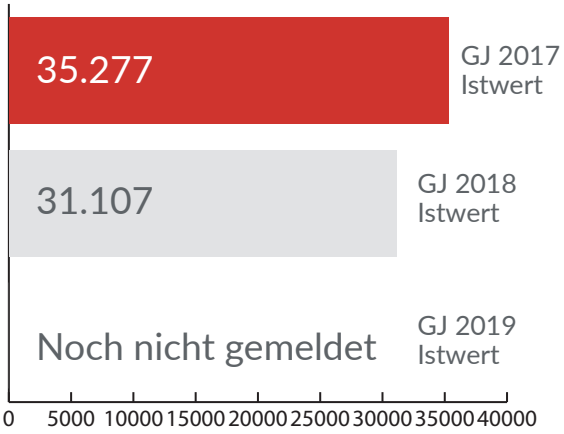
Risiken von Cyberangriffen

Die Minderung von Cyberangriffen war laut der RSA Digital Risk Study in den letzten beiden Jahren das oberste Ziel für das Risikomanagement im öffentlichen Sektor. Wie wichtig das Management dieser Risiken ist, wird im „FISMA FY 2018 Annual Report to Congress“ vom US Government Accountability Office (GAO) untermauert. Dieser Bericht hebt deutliche Fortschritte beim Management der Risiken von Cyberangriffen hervor, z. B. einen Rückgang der Cybersicherheits-Incidents um 12 % im Vergleich zum vorherigen Geschäftsjahr (35.277 im GJ 2017). Der Bericht unterstreicht jedoch auch die Tatsache, dass es im GJ 2018 immer noch 31.107 Cybersicherheits-Incidents gab.[5] Dies zeigt, dass die Bundesbehörden vor der großen Herausforderung stehen, ihre Informationen und Systeme vor böswilligen Akteuren schützen zu müssen. Damit werden die Herausforderungen der Cybersicherheit zu einem „Problem mit hohem Risiko“ (High-Risk Issue) für die US-Bundesregierung.[6] In einem neueren GAO-Bericht wird die „Sicherstellung der Cybersicherheit der Nation“ als einer von neun Bereichen mit hohem Risiko aufgeführt, die besonders im Fokus von Exekutive und Kongress stehen.[7]

Finanzmittel der Behörden für Cybersicherheit (in Millionen USD)



Gemäß FISMA gemeldete Cyber-Incidents



Quelle: https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf

Bundesbehörden sind keineswegs die einzigen Organisationen im öffentlichen Sektor, die derzeit mit Herausforderungen im Bereich der Cybersicherheit konfrontiert sind. Anfang des Jahres waren in Texas 22 Kommunen einer Flut von Ransomware-Angriffen ausgesetzt – etwa zur gleichen Zeit wurden Datennetzwerke in Baltimore, das von den Gerichten verwendete System in Georgia und ein County in Utah ebenfalls angegriffen.[8] Es besteht die begründete Annahme, dass kleinere Behörden deutlich anfälliger für Angriffe dieser Art sind als Bundesbehörden: Angreifer sehen, dass dort weniger Ressourcen für Investitionen in Cybersicherheit vorhanden sind. Da die Anzahl bei vielen Angriffsarten zunimmt[9], ergreifen Staaten und lokale Behörden Maßnahmen. Beispielsweise bieten Staaten wie Texas neben weiteren Tools und Support auch Services für Cybersicherheit und Managed Security Services (MSS) in Zusammenarbeit mit privaten Anbietern an, um lokalen Behörden und öffentlichen Einrichtungen kostengünstigen Zugriff auf Sicherheitstools, Monitoring und Erkennung zu ermöglichen.[10] Darüber hinaus führen Staaten und lokale Behörden mehr Schulungen durch, um die Mitarbeiter anhand von Best Practices zu informieren, wie sie ihr Bewusstsein zur Cybersicherheit schärfen können. Einfache Schulungen, wie z. B. die Aufklärung von Nutzern über Phishing-E-Mails, deren Erkennung und die Reaktion darauf, können dazu beitragen, potenzielle Bedrohungen zu erkennen und ähnliche Phishing-Angriffe zu verhindern.

Organisationen im öffentlichen Sektor verbessern weiterhin ihre allgemeine Cybersicherheitsstrategie und kämpfen gleichzeitig mit Budget- und Ressourcenbeschränkungen. Regierungsbehörden übernehmen gängige Frameworks für Cybersicherheit, wie z. B. NIST (National Institute of Standards and Technology) und CSF (Cyber Security Framework), die sich auf Technologie, Mitarbeiter und Prozesse konzentrieren, um Cyberangriffe zu identifizieren, zu erkennen, davor zu schützen, auf diese zu reagieren und danach wiederherzustellen. Unternehmen verfolgen einen risikobasierten Ansatz und nutzen Automatisierung und Advanced-Threat-Erkennung, um die wichtigsten Bedrohungen zu priorisieren. Außerdem implementieren und verbessern Sicherheitsverantwortliche in allen Behörden die grundlegenden Sicherheitsmaßnahmen – z. B. Multifaktor-Authentifizierung, Identitäts-Governance und Lebenszyklusmanagement – und stellen so sicher, dass nur Befugte auf Behördeninformationen zugreifen können.

Sicherheitsverantwortliche implementieren und verbessern in allen Behörden die grundlegenden Sicherheitsmaßnahmen – z. B. Multifaktor-Authentifizierung, Identitäts-Governance und Lebenszyklusmanagement – und stellen so sicher, dass nur Befugte auf Behördeninformationen zugreifen können.

Dynamische Mitarbeiterrisiken

Die Lage der Mitarbeiter im öffentlichen Dienst von heute hat sich dramatisch verändert. Nicht nur die Demografie der Behördenmitarbeiter entwickelt sich nun, da mehr Millennials im öffentlichen Dienst beschäftigt sind, weiter, sondern die Behörden sind auch weiterhin von zahlreichen Contractors und deren Beiträgen zur Unterstützung ihres Auftrags abhängig. Wie im privaten Sektor führen auch Organisationen im öffentlichen Sektor mehr digitale Technologien ein, um den Mitarbeitern zu helfen, produktiver und effizienter zu werden und die Ziele ihres Auftrags zu erreichen. Das stellt jedoch eine Herausforderung für die Verantwortlichen des behördlichen Sicherheits- und Risikomanagements dar. Sie müssen ein Gleichgewicht zwischen einem offenen und reibungslosen geräte-, plattform- und Cloud-übergreifenden Informationsfluss für die unterschiedlichen Mitarbeiter und den Sicherheitsanweisungen und Ressourcenkontrolle, die zum Schutz der Daten von Bürgern und Behörden erforderlich sind, herstellen.

Diese Herausforderung wird durch behördliche Auflagen und durch Verfügungen von Behörden und der Exekutive verstärkt, denn diese stellen zusätzliche Anforderungen an die Behörden, um eine Zugriffs- und Identitätssicherung in der gesamten Umgebung des öffentlichen Sektors zu erreichen. Auch die Richtlinien für das Management dieses Gleichgewichts verändern sich. Die Regierung hat bereits seit Jahren Programme für Insiderbedrohungen, doch hat sich die Definition der Insiderbedrohung geändert. Da immer mehr Behördendaten auf Mobilgeräten und in der Cloud gespeichert werden, kann sich auch ein sorgloser, jedoch nicht böswilliger Mitarbeiter oder Contractor als Schwachstelle erweisen. Ein von der Behörde gestelltes Laptop im Bus zu vergessen, eine PIV-Karte zur Verifizierung der eigenen Identität zu verlegen oder Daten, die sich auf einem von der Behörde zur Verfügung gestellten Gerät befinden, auf ein privates oder ein anderes Gerät zu übertragen, um eine Aufgabe zu beenden – das alles sind reale Risiken. Und sogar einfache Fehler können zu Datenverlusten führen. Organisationen im öffentlichen Sektor setzen auf Schulung und Bewusstsein, um dieses Problem zu lösen. Wie bereits erwähnt kam der RSA Digital Risk Report zu dem Ergebnis, dass Organisationen im öffentlichen Sektor im Vergleich zu Unternehmen im privaten Sektor mehr leisten, um das Bewusstsein dieser digitalen Risiken bei den Mitarbeitern zu schärfen. Kontinuierliche Wachsamkeit und Schulung sind entscheidend, um sicherzustellen, dass alle Arbeitnehmer im öffentlichen Dienst sowie die Contractors die Verantwortung für die Sicherheit von Behördendaten und -ressourcen übernehmen.

Und schließlich werden die Tools, die Sicherheitsverantwortliche der Behörde für die Steigerung der Mitarbeiterproduktivität bereitstellen, ebenfalls weiterentwickelt. Die Verantwortlichen wollen die herkömmlichen Zugriffskontrollen (CAC/PIV) ergänzen und andere Kontrollen wie z. B. die Multifaktor-Authentifizierung, Mobile Push, Biometrie usw. einsetzen, die moderne Authentifizierungsansätze verwenden, um den Zugriff zu vereinfachen. Dadurch werden die Prozesse für den Mitarbeiterzugriff optimiert und gleichzeitig wird sichergestellt, dass die Zugriffskontrolle für jedes System gewährleistet ist. Durch die Nutzung risikobasierter Analysen im Back-End lässt sich unangemessener Zugriff mittels neuer Methoden, die keine Einschränkungen für die Mitarbeiter darstellen, überwachen und erkennen.

Regierungsorganisationen arbeiten beständig daran, Datenschutzrisiken durch verbesserte Zugriffskontrollen zu beheben, um eine bessere Sichtbarkeit darüber zu erhalten, wer Zugriff auf Daten hat und was die Nutzer damit tun. Auch Richtlinien für das Datenmanagement werden weiterentwickelt, um den Datenschutz für Mitarbeiter und Bürger zu gewährleisten.

Datenschutzrisiken

Der Datenschutz ist für alle ein wichtiges Thema. Zwar stehen Sicherheitsverletzungen in der kommerziellen Welt mehr in den Schlagzeilen, dennoch sind Organisationen im öffentlichen Sektor nicht immun. Laut 2019 Verizon Data Breach Investigations Report treten im öffentlichen Sektor 16 % der Datenschutzverletzungen auf, das ist nahezu derselbe Prozentsatz wie im Gesundheitswesen.[11] The National Law Review beschreibt die Datenschutzrisiken im öffentlichen Sektor als „wenig diskutierte" Risiken, die nun in den Vordergrund rücken. Insbesondere angesichts der Datenschutzverletzung beim Office of Personnel Management (OPM) im Jahr 2019, bei dem personenbezogene Daten in Millionen Datensätzen mit Hintergrundermittlungen und Personalakten exponiert wurden.[12]

Die Schwerte der OPM-Datenschutzverletzung ist eine ernüchternde Erinnerung daran, wie viele personenbezogene Daten in Behördensystemen gefährdet sind. Abgesehen von den Millionen Menschen, die für die Bundesregierung arbeiten oder sich dort bewerben, gibt es viele weitere Millionen, deren Daten sich in behördlichen Systemen befinden. Regierungsorganisationen haben den Auftrag, ihren Wählern zu dienen. Der Schutz der Bürgerdaten und die Gewährleistung, dass diese nur für beabsichtigte Zwecke verwendet werden, tragen somit dazu bei, das Vertrauen zu erfüllen, das die Bürger in Behörden und Regierung setzen. Dies ist von entscheidender Wichtigkeit, um den Erfolg dieses Auftrags zu gewährleisten.

Die gute Nachricht ist, dass Regierungsorganisationen beständig daran arbeiten, Datenschutzrisiken durch verbesserte Zugriffskontrollen zu beheben, um eine bessere Sichtbarkeit darüber zu erhalten, wer Zugriff auf Daten hat und was die Nutzer damit tun. Auch Richtlinien für das Datenmanagement werden weiterentwickelt, um den Datenschutz für Mitarbeiter und Bürger zu gewährleisten. Beispielsweise hat die US-Bundessteuerbehörde (Internal Revenue Service, IRS) ein Programm eingeführt, das die Verwendung der Sozialversicherungsnummer zur Authentifizierung der Steuerzahler minimiert.[13] Und es wird erwartet, dass das NIST in Kürze ein Framework für Datenschutz vorstellt, das nicht nur von Behörden, sondern auch von Unternehmen im privaten Sektor als Modell verwendet werden kann – wie das derzeit vorhandene NIST CSF.[14]

Fazit

Die heutigen Regierungsorganisationen modernisieren weiterhin, wie sie Services für die Wähler bereitstellen und Auftragsergebnisse mit Technologie erbringen. Wie die RSA Digital Risk Study verdeutlicht, ist das Management von Risiken im Zusammenhang mit der digitalen Transformation oberstes Ziel für Sicherheitsverantwortliche in den Behörden. Doch da die digitale Transformation zunehmend die Arbeit der Behörden definiert, bedeutet das auch digitale Risiken. Und es geht nicht nur um die drei hier besprochenen Risiken, sondern auch um Risiken in Bezug auf Bestimmungen, Abläufe usw., die sich auf die Aufträge der Behörden auswirken. Die Einsätze für die Behörden sind wohl höher – und die Herausforderungen größer. Aber nicht in Frage gestellt wird die Notwendigkeit, die Risiken der digitalen Transformation zu managen. Organisationen im öffentlichen Sektor, die sich mit der digitalen Transformation beschäftigen, sind sich dessen bewusst. Gemäß der RSA Digital Risk Study ist der öffentliche Sektor dem privaten Sektor weit voraus, wenn es darum geht, das Bewusstsein für digitale Risiken zu schärfen. Bei der Bewertung, Priorisierung und Behebung von Aspekten dieser Risiken ist jedoch noch viel Fortschritt nötig, um den Auftragserfolg zu gewährleisten.[15]

Der öffentliche Sektor ist dem privaten Sektor weit voraus, wenn es darum geht, das Bewusstsein für digitale Risiken zu schärfen. Bei der Bewertung, Priorisierung und Behebung von Aspekten dieser Risiken ist jedoch noch viel Fortschritt nötig, um den Auftragserfolg zu gewährleisten.

Digitale Risiken betreffen alle
Wir helfen Ihnen, sie zu beherrschen

Mit den Lösungen von RSA® Business-Driven Security™ können Unternehmen einen einheitlichen Ansatz für das Management digitaler Risiken nutzen, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Aktionen basiert. Dank der Lösungen für schnelle Erkennung und Reaktion, Nutzerzugriffskontrolle, Verbraucherschutz und integriertes Risikomanagement können RSA-Kunden erfolgreich sein und sich kontinuierlich an Transformationsänderungen anpassen.

Finden Sie heraus, wie Sie in einer dynamischen, hochriskanten Welt erfolgreich sein können. Besuchen Sie RSA.com/de-de.

1 „Information Technology Management Reform Act of 1996“, Wikipedia: The Free Encyclopedia, Wikimedia Foundation, Inc., 19. Februar 2019, 19:45 Uhr, https://en.wikipedia.org/wiki/Information_Technology_Management_Reform_Act_of_1996 (aufgerufen am 10. Oktober 2019)

2 „E-Government Act of 2002“, Wikipedia: The Free Encyclopedia, Wikimedia Foundation, Inc., 18. April 2019, 14:00 Uhr, https://en.wikipedia.org/wiki/E-Government_Act_of_2002 (aufgerufen am 10. Oktober 2019)

3 „OMB announces ‘cloud first’ policy for agencies“, Federal News Network, https://www.federalnewsnetwork.com/technology-main/2010/11/omb-announces-lsquocloud-firstrsquo-policy-for-agencies/ (23. November 2010)

4 „From Cloud First to Cloud Smart“, Federal Cloud Computing Strategy, https://cloud.cio.gov (aufgerufen am 10. Oktober 2019)

5 „Federal Information Security Modernization Act of 2014: Annual Report to Congress“, https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf (Fiscal Year 2018)

6 „Key Issues: Cybersecurity Challenges Facing the Nation—High Risk Issue“, U.S. Government Accountability Office, https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary (aufgerufen am 10. Oktober 2019)

7 „High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas“, U.S Government Accountability Office, https://www.gao.gov/products/GAO-19-157sp#summary (06. März 2019)

8 „22 Texas Towns Hit With Ransomware Attack In ‘New Front’ Of Cyberassault“, National Public Radio, https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault (20. August 2019)

9 Allen Kim, „In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks“, CNN, https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html (08. Oktober 2019)

10 „Cyberdefense for Texas State Government“, Fiscal Notes: A Review of the Texas Economy from the Office of Glenn Hegar, Texas Comptroller of Public Accounts https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php (März 2019)

11 „2019 Data Breach Investigations Report“, Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (Mai 2019)

12 Kristin Ann Shepard, „Data Privacy Exposure Hits the Public Sector“, The National Law Review, https://www.natlawreview.com/article/data-privacy-exposure-hits-public-sector-lessons-opm-data-breach-class-action (13. August 2019)

13 „What are we doing to protect taxpayer privacy?“ IRS, https://www.irs.gov/privacy-disclosure/what-are-we-doing-to-protect-taxpayer-privacy (18. Oktober 2019)

14 Alex Hickey, „Government takes baby steps in data privacy with NIST framework, bill discussions“, CIO Dive, https://www.ciodive.com/news/government-takes-baby-steps-in-data-privacy-with-nist-framework-bill-discu-1/550084/ (12. März 2019)

15 „RSA Digital Risk Study“, RSA Digital Risk Report, 1. Edition, https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf (September 2019)