Autor
Jürgen Kretschmer, Beauftragter für Informationssicherheit der SAKD

Veröffentlichungen
Sachsenlandkurier 03/21: Digitale Verwaltung, Informationssicherheit, September 2021
Homepage der SAKD: https://www.sakd.de/ozg_informationssicherheit.html, Oktober 2021

Informationssicherheit bei der Umsetzung des Online-Zugangs-Gesetz - OZG durch sächsische Kommunen

Das OZG verpflichtet Bund, Länder und Kommunen, bis Ende 2022 ihre „Verwaltungsleistungen auch elektronisch über Verwaltungsportale anzubieten“. Von den im OZG-Leistungskatalog[1)] aus Sicht des BMI erfassten und aufgrund regionaler Besonderheiten hinzukommenden Leistungen sind durch sächsische Kommunen ca. 540 Leistungen entsprechend elektronisch abzubilden.
Im Hinblick auf die Terminsetzung und das bisherige Tempo im E-Government wird mit dem OZG[2)] ein sehr ehrgeiziges Ziel formuliert.

Für kommunale Behörden stellt sich hier natürlich die Frage, wie sie ihren Anteil an dieser Mammutaufgabe erfüllen können, ohne dabei die Schutzziele der Informationssicherheit zu vernachlässigen.
Und gerade denen, welche sich bisher in diesen Dingen auf einen Dienstleister verlassen haben, wird unter Umständen gerade bewusst, dass sie auf diese Herausforderung angesichts des absehbar inhomogeneren Umfelds ungenügend vorbereitet sind.

Wie also sollte man aus Sicht einer kommunalen Behörde vorgehen?
Im Folgenden soll auf die bestehenden Normierungen in Form von Gesetzen und technischen Richtlinien und den momentanen Umsetzungsstand und dem sich daraus ergebenden Handlungsbedarf sowie auf die Bestandteile des Informationsverbundes einer Online-Anwendung und die Schutzziele der Informationssicherheit eingegangen werden.
Über den aktuellen Stand hinaus gehende Betrachtungen können als Anregung einer perspektivischen Entwicklung verstanden werden.

Verantwortung gegenüber Bürgern und Unternehmen

Egal ob der Verwaltungskunde über das Serviceportal Amt24 des Freistaates Sachsen oder die Homepage der Behörde auf das Online-Angebot der Verwaltungsleistung gelangt und unter welcher Internet-Adresse das Angebot zur Verfügung gestellt wird, als verantwortlich, also quasi Vertragspartner, muss immer die kommunale Behörde erkennbar sein (Angabe eines Impressums). Welche weiteren Dienstleister zur Erbringung der Leistung von der Behörde einbezogen werden, interessiert den Kunden in aller Regel nicht.
Insofern ist die Behörde vor dem Kunden auch für alle Aspekte der Informationssicherheit verantwortlich. Im Verhältnis mit etwaigen Dienstleistern teilt sie sich natürlich diese Verantwortung mit diesen.

Grundvoraussetzung

Die Verantwortung für die Informationssicherheit in einer Behörde trägt immer die Behördenleitung. Da diese umfangreiche Aufgaben hat und das Thema spezielle Kenntnisse erfordert, sollte sie die Zuständigkeit für Informationssicherheit delegieren. Das Sächsische Informationssicherheitsgesetz[3)] enthält hier eine SOLL-Vorschrift zur Bestellung eines Beauftragten für Informationssicherheit – BfIS für

Träger der kommunalen Selbstverwaltung.
Es muss eine Stelle geben, welche sich kümmert und als Ansprechpartner zur Verfügung steht. IT-Kenntnisse sind für diese Stelle zwar hilfreich. Wichtiger jedoch sind Kenntnisse, wie man ein System zum Management der Informationssicherheit – ISMS aufbaut und kontinuierlich verbessert.
Sich darauf zu verlassen, die IT würde das wie gehabt mit erledigen, könnte ins Leere laufen. Bei der kompletten Abbildung von Online-Anwendungen bei Dienstleistern ist die eigene IT, insbesondere wenn sie als Outsourcing organisiert ist, unter Umständen gar nicht beteiligt. Auch ergeben sich durch eine weitere Online-Anwendung keine neuen Anforderungen an das eigene Netz.
Bei kleinen Verwaltungen kann es am Ende durch die zusätzliche Benennung eines BfIS vorkommen, dass sich bei dem betreffenden Mitarbeiter mehrere inhomogene Aufgaben ansammeln, welche aufgrund der Breite der nötigen Kenntnisse schwer handhabbar sind. Abhilfe kann hier die Beauftragung eines externen Dienstleisters schaffen.

Der zu betrachtende Informationsverbund

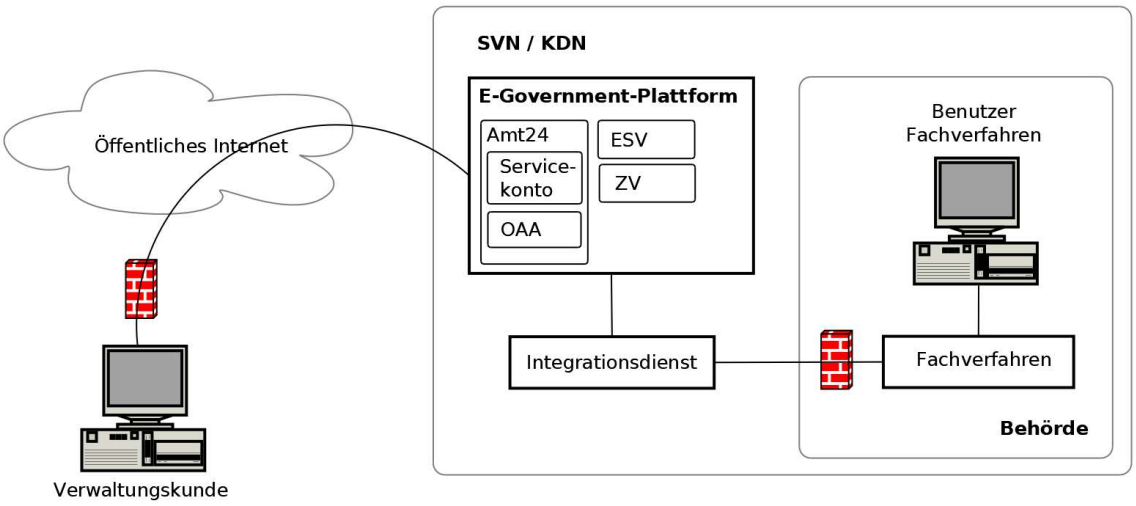
Reichte es noch vor wenigen Jahren aus, durch ein Web-Frontend ein Fachverfahren für Verwaltungskunden im Internet verfügbar zu machen, ist heute die Vernetzung spezialisierter Komponenten und die Verwendung offener standardisierter Datenformate und Übertragungstechnologien im Sinne einer verteilten Anwendung das Mittel der Wahl.

Nur so können, trotz einer zunehmenden Anzahl von Online-Anwendungen, Datenbestände konsistent gehalten werden und die benötigten Ressourcen zur Entwicklung und zum Betrieb der Komponenten sichergestellt werden.

Die kommunale Behörde sollte sich also als Erstes einen Überblick der für eine Online-Anwendung nötigen Anwendungen und der damit verbundenen Dienstleister verschaffen.

Der für die Informationssicherheit zu betrachtende Informationsverbund bestand bisher in der Regel aus den eigenen Diensten und Fachverfahren, dem eigenen Netz mit Servern und Arbeitsplätzen und dem Netzübergang zum KDN oder öffentlichen Internet. Oft wurde/n zusätzlich ein oder mehrere Fachverfahren in einem externen Rechenzentrum betrieben.

Bei den Online-Anwendungen zur Umsetzung des OZG kommen nun zusätzlich die Bausteine der sächsischen Referenzarchitektur zur Umsetzung des OZG und die Ausstattung des Verwaltungskunden zum Tragen.



Grafik typischer Informationsverbund schematisch

Die Ausstattung des Verwaltungskunden

Üblicherweise greift der Verwaltungskunde von seinem PC oder Mobilendgerät über sein LAN/WLAN oder ein öffentliches WLAN und das öffentliche Internet auf das Onlineangebot der Verwaltung zu. Diese angreifbaren Komponenten kommen also zum Informationsverbund hinzu, sind jedoch durch die Behörde wenig beeinflussbar. Sie sollte zwar versuchen den Verwaltungskunden auf seinen Teil der Verantwortung durch zum Beispiel sichere Verwahrung von Passworten und regelmäßige Updates hinzuweisen, das zu kontrollieren oder gar zu sanktionieren wird aber kaum möglich sein.
Die Anstrengungen zur Verbesserung der Informationssicherheit müssen sich deshalb auf die eigene Einflusssphäre und damit auch die der vertraglich gebundenen Dienstleister konzentrieren.

Das eigene Hoheitsgebiet

Die meisten Behörden kommunizierten auch vor OZG elektronisch mit Bürgern, Unternehmen und anderen Behörden, meistens per E-Mail. Die Kommunikationspartner waren persönlich bekannt oder die Authentizität konnte aus dem Kontext ganz gut beurteilt werden.
Mit Online-Anwendungen wird unstrukturierte E-Mail zur Vermeidung von Medienbrüchen durch Online-Antragsassistenten und standardisierte Datenübertragung abgelöst.

Der Ersatz der E-Mail verschafft hier einen deutlichen Sicherheitsgewinn, dient sie doch oft als Einfallstor für Schadsoftware.

Andererseits verstärkt sich die Kommunikation mit dem als unsicher geltenden öffentlichen Internet und den Verwaltungskunden. Die Behörde wird sichtbarer und könnte damit die Aufmerksamkeit potenzieller Angreifer auf sich ziehen.
Neue Zugriffsmöglichkeiten bieten neue Angriffsfläche.
Spätestens jetzt sollten also grundsätzliche Anforderungen der Informationssicherheit an das eigene Netz und die damit verbundenen Arbeitsplätze und Server erfüllt werden.
Das Bundesamt für Informationssicherheit – BSI bietet hier eine Reihe von Publikationen[4)] an, in denen es auf so grundlegende Maßnahmen wie z.B.:

- Verwendung von privaten IP-Adressen im LAN (NAT),

- Segmentierung des LAN,
- Verschlüsselung im WLAN,
- Absicherung des Internet (resp. KDN)-Übergangs mit Firewall/Sicherheitsgateway,
- Viren- und SPAM-Schutz durch Application Level Gateway,
- Verschlüsselung von Datenträgern,
- Datensicherung und
- Sichere Client- und Serverkonfiguration

detailliert eingeht.
Sehr aktuell ist auch die Veröffentlichung zum Schutz vor Ransomware[5)], welche zahlreiche Maßnahmen noch einmal aufgreift.

Die Basiskomponenten der sächsischen E-Government-Plattform

Einen wesentlichen Anteil am Informationsverbund haben die Basiskomponenten der sächsischen E-Government-Plattform und dort insbesondere das Servicekonto und die Online-Antrags-Assistenten – OAA des Amt24.
Die seit 2014 in diesem Zusammenhang zwischen dem Freistaat Sachsen und den sächsischen kommunalen Spitzenverbänden fortgeschriebene Mitnutzungsvereinbarung[6)] stellt in Bezug auf die Informationssicherheit die Anforderung einer „sicheren und datenschutzgerechten elektronischen Abwicklung und Integration von Verwaltungsverfahren“. Der Freistaat erbringt u.a. „technische und organisatorische Maßnahmen des Datenschutzes und der Informationssicherheit“.
Im Übrigen regelt die Vereinbarung die Modalitäten zur kommunalen Beteiligung bei der Weiterentwicklung der Plattform und Finanzierung.
Demnach sind durch die pauschal über den sächsischen Finanzausgleich getragene Beteiligung der Kommunen alle Kosten abgedeckt, außer es handelt sich um Weiterentwicklungskosten, welche allein durch die Kommunen veranlasst sind.

Im Folgenden ist der Freistaat Sachsen, ggfs. vertreten durch den Staatsbetrieb Sächsische Informatik Dienste – SID als OZG-Dienstleister zu sehen.

Einbindung der OZG-Dienstleister

Die Besonderheit bei den Online-Anwendungen zur Umsetzung des OZG, insbesondere wenn man die zentralen Dienste der sächsischen Rechenzentrumsdienstleister nutzt, wird darin liegen, dass ein Großteil der Verarbeitungstätigkeit außerhalb des eigenen Netzes durchgeführt wird.
Dieser Anteil wird also durch die Behörde bei den Dienstleistern eingekauft. Je nachdem auf wie viele Komponenten sich die zugrunde liegende Anwendung verteilt, können das auch mehrere Dienstleister sein.
Eine durch die SAKD als koordinierende Stelle für sächsische Kommunen zur Verfügung gestellte Aufstellung der Komponenten und Dienstleister je Online-Anwendung sollte hier Transparenz schaffen.

Die Anforderungen an die Informationssicherheit werden also in Verträgen verankert. Insbesondere kleine Kommunen werden Schwierigkeiten haben, ihre entsprechenden Vorstellungen zu formulieren und bei mehreren Dienstleistern eine Abgrenzung zu treffen.

Hier sollten die Dienstleister durch Musterverträge unterstützen und darin gegenüber den Kunden zusichern, dass alle gesetzlichen und auch sonst nötigen Anforderungen durch organisatorische Maßnahmen und technische Maßnahmen nach dem Stand der Technik erfüllt sind.

Es sind Regelungen zu treffen über die Verantwortung

- der Behörde (z.B. Sicherheit des Benutzergerätes, Verantwortung der Benutzer),
- der Behörde und des Dienstleisters (z.B. Datensicherung, Verschlüsselung, Einhaltung von Richtlinien, Umgang mit Vorfällen) und
- des Dienstleisters (z.B. Organisation der Informationssicherheit).

Die Bündelung von allen nötigen Dienstleistungen in einem Vertragspaket bei einem Anbieter vereinfacht die Entscheidung bei der beauftragenden Behörde zusätzlich und minimiert dort den Aufwand.
Die dafür nötigen Vorarbeiten zahlen sich letztlich auch in einem transparenten und effizienten Vertrieb für die Anbieter aus.

Die Musterverträge sollten auf für bestimmte Größenklassen typische Schutzbedarfsniveaus eingehen. Unbenommen kann natürlich jede Kommune zu einer abweichenden Beurteilung kommen. Sollte hier ein höherer Schutzbedarf ermittelt werden, muss das dann individuell vereinbart werden.
Da beim Dienstleister die Schutzbedarfe vieler Kunden zusammen kommen, muss durch den Kumulationseffekt bei dessen Komponenten zwangsläufig ein höherer Schutzbedarf abgebildet werden.

Verwendung einer standardisierten Methodik

Zum gemeinsamen Verständnis sollte in den Verträgen als Methodik zur Verbesserung der Informationssicherheit ein Standard vereinbart werden.
Etabliert hat sich hier unter anderem der BSI-Standard 200-2[7)] „IT-Grundschutz-Methodik“

Neben den Begriffsdefinitionen werden in diesem Standard unter anderem beschrieben:

- die Initiierung und Organisation des Sicherheitsprozesses
- die Erstellung einer Sicherheitskonzeption
- die Anwendung der BSI-Bausteine (Anforderungen, Gefährdungen, Maßnahmen)

Ins Detail gehen zum Beispiel Anforderungen im Baustein OPS.2.2 - Cloud-Nutzung zu[8)]:

- Planung Einbindung und Migration des Dienstes,
- Vertragsgestaltung mit dem Cloud-Diensteanbieter,
- Aufrechterhaltung und Betrieb,
- Notfallvorsorge,
- Beendigung und Wechsel des Anbieters und
- Datensicherung.

Im Dialog zwischen Behörde und Dienstleister sollte es sehr hilfreich sein, sich auf diese standardisierte Vorgehensweise zu beziehen.

Durch die Verwendung eines Standards und die daraus resultierende Möglichkeit, sich die Einhaltung durch einen zertifizierten Auditor bestätigen zu lassen, kann der Anbieter das Vertrauen seiner Kunden in seine Leistungsfähigkeit stärken.
Die reine Möglichkeit für die Kunden, ein eigenes Audit vorzunehmen, würde wohl aus Ressourcengründen von den Wenigsten genutzt werden.

Schutzziele der Informationssicherheit

Verfügbarkeit

Dem Slogan von Amt24 „Zu Hause aufs Amt“ folgend, sollte dieses auch zu Zeiten zur Verfügung stehen, an denen viele Menschen zu Hause sind.
Die Mitnutzungsvereinbarung teilt die Komponenten der E-Government-Plattform bestimmten Serviceklassen zu. Die im Kontext OZG besonders relevanten Basiskomponenten Amt24, Servicekonto, Elektronische Signatur und Verschlüsselung – ESV und Zahlungsverkehr – ZV werden nach der Sächsischen E-Government-Gesetz-Durchführungsverordnung[9)] mit einem Betriebsregime „24/7“ und einer maximalen Ausfallzeit von 10,8 Stunden/Monat betrieben.
Entsprechende Service-Level-Agreements – SLA müssen mit allen anderen Dienstleistern geschlossen werden. Bezüglich der Verfügbarkeit sind weitere Vereinbarungen zu Reaktions- und Wiederherstellungszeiten, Verantwortung für Backups und Benachrichtigungsmodalitäten erforderlich.

Die von den Kommunen im Kontext OZG angebotenen Online-Anwendungen werden in der Regel durch die Zusammenarbeit von verschiedenen Komponenten realisiert und sind somit verteilte Anwendungen.
Die Betrachtung jeder Komponente in den einzelnen SLA‘s sichert das Schutzziel aus Gesamtsicht somit nicht ab. Ein komponentenübergreifenden Monitoring der Vorgänge durch eine übergeordnete Instanz anhand einer eindeutigen Vorgangs-ID könnte die Einschätzung der Verfügbarkeit verbessern.
Dabei sollten die gesammelten Daten mit einem hinterlegten SOLL-Prozess abgeglichen werden, um auf diese Weise den Status einzelner Vorgänge und ein Gesamtbild der Verfügbarkeit der beteiligten Komponenten zeitnah festzustellen und darzustellen. Die einzelne Kommune erhält den Zugriff auf ihren Teil des Systems. Kritische Zustände wie z.B. eine nahende Genehmigungsfiktion bei einzelnen Vorgängen oder sich stauende Vorgänge könnten von der übergeordneten Instanz oder der Kommune zeitnah erkannt werden.

Integrität

Für die Sicherstellung der Ende-zu-Ende-Integrität der Daten bei einer elektronischen Übertragung hat sich das Verfahren der digitalen Signatur etabliert. Der Sender verschlüsselt mit seinem privaten Schlüssel den Hash-Wert der zu übertragenden Daten und der Empfänger entschlüsselt den Hashwert mit dem öffentlichen Schlüssel des Senders, prüft die Gültigkeit des Senderzertifikats und vergleicht die Hash-Werte[10)].
Sind die Prüfungen erfolgreich, kann der Empfänger sicher sein, dass der Sender authentisch und die Nachricht unverändert ist.

Bei einer Übertragung von Antragsdaten vom Amt24 über den Integrationsdienst bis zum Fachverfahren kann momentan nicht davon ausgegangen werden, dass alle Komponenten dieses Verfahren unterstützen. Hinzu kommt, dass die Daten im Integrationsdienst unter Umständen transformiert werden. Die Wahrung der Integrität bei der Übertragung ist also nur abschnittsweise möglich. Anstelle der Personenzertifikate der Verwaltungskunden kommen Organisationszertifikate der Betreiber der Komponenten zum Einsatz.
Die Prozesse zur Einrichtung und Erneuerung dieser Zertifikate müssen besonders sicher gestaltet sein. Die Integrität in den Komponenten ist durch eine hohe Qualität der Software in Verbindung mit einer sorgfältigen Konfiguration und entsprechender Dokumentation und Tests zu gewährleisten.

Vertraulichkeit

Voraussetzung ist ein sicheres Anmeldeverfahren für Verwaltungskunden, Behördenmitarbeiter und alle anderen am Übertragungsweg Beteiligten und eine

geregelte Rechtevergabe.
Die Verschwiegenheitspflicht der Administratoren ist obligatorisch. Eine Sicherheitsüberprüfung könnte in Erwägung gezogen werden. Besser wäre eine durchgehende Verschlüsselung, welche aber aus oben genannten Gründen oft nicht möglich sein wird.

Authentizität

Hier geht es momentan vornehmlich um die Authentizität des Verwaltungskunden. Die Behörde möchte sicher sein, dass der Verwaltungskunde jener ist, als welcher er sich ausgibt. Es kann eine Motivation, sei sie destruktiver Natur oder zur Erlangung eines Vorteils, zu Manipulationsversuchen durch den Kunden unterstellt werden.

Die Gefahr, die Authentizität der anderen Beteiligten zu manipulieren, erscheint bei einer professionellen Implementierung im SVN/KDN gering.

Am Beginn der Authentizität steht auch hier ein angemessenes Anmeldeverfahren. Für jedes Verfahren muss das erforderliche Vertrauensniveau ermittelt werden. Zur ersten Einschätzung bietet das Bundesministerium des Innern, für Bau und Heimat auf seiner OZG-Informationsplattform[11)] ein Praxistool Vertrauensniveau an. Im Tool wird sowohl auf Aspekte des Datenschutzes als auch der Informationssicherheit eingegangen.

Amt24 bietet momentan die Anmeldung mittels Name und Passwort und eID-Funktion des Personalausweises bzw. des elektronischen Aufenthaltstitels an (elektronischer Identitätsnachweis).
Eine Nutzung des Anmeldeverfahrens der elektronischen Steuererklärung – ELSTER ist geplant.
Bei der Anmeldung mit Name und Passwort kann nach der BSI-Richtlinie TR 03107-1[12)] maximal das Vertrauensniveau „normal“ erreicht werden. Amt24 prüft die Inhaberschaft einer zugehörigen E-Mail-Adresse durch eine Bestätigungsmail mit Aktivierungslink. Hier kommt es darauf an, wie der E-Mail-Anbieter die Identität der zugehörigen Person geprüft hat.
Die Einen bieten anonyme Wegwerf-Adressen, die Anderen senden zur Aktivierung einen Brief an die Postadresse. Da die Kommune die Qualität der Identitätsprüfung nicht kennt, bleibt ihr im Zweifelsfall nur eine eigene nachgelagerte Prüfung.
Mit ELSTER kann unter Verwendung eines Softwarezertifikates das Vertrauensniveau „substanziell“ erreicht werden.
Der elektronische Identitätsnachweis erreicht das Niveau „hoch“, wird jedoch momentan von den Verwaltungskunden nicht im erhofften Maße genutzt.

Das Sicherheitsziel Authentizität betreffend ist auch die Vorgabe in §11a Sächsisches E-Government-Gesetz[13)] relevant, wonach das Serviceportal Amt24 „die Verwendung des für das jeweilige Verwaltungsverfahren erforderlichen Vertrauensniveaus ermöglichen muss“ und die „besonderen Anforderungen der einzelnen Verwaltungsleistungen an die Identifizierung ihrer Nutzer zu berücksichtigen sind“.
Im Portalverbund nach §1 OZG soll es bis Ende 2022 allen Nutzern möglich sein, mit einem Servicekonto alle Verwaltungsverfahren der Landesportale und des Bundesportales zu nutzen und sich dabei nur einmal anmelden zu müssen (Single Sign On - SSO). Wird das Verfahren nicht vom Heimatportal angeboten, erhält das entfernte Portal eine Zusicherung über die Authentisierung des Verwaltungskunden mit einem bestimmten Vertrauensniveau.

Nichtabstreitbarkeit / Zurechenbarkeit

Auf den Nachweis der Autorenschaft und die momentan einzugehenden Kompromisse wurde schon in den Abschnitten *Integrität* und *Authentizität* eingegangen.
Zur Bestätigung des Versandes und des Empfangs von Nachrichten bietet sich der Standard „Online Services Computer Interface“ – OSCI[14)] an. Mit diesem ist es möglich Inhalts- und Nutzungsdaten getrennt zu verschlüsseln und zu signieren.
Im Sinne der Schutzziele werden die Zeitpunkte der Kommunikation protokolliert und den Beteiligten bestätigt.

Auf Anforderung können auch kryptografische Zeitstempel generiert werden.Diese Protokolldaten nach den gesetzlich vorgeschriebener Aufbewahrungsfristen beweiswerterhaltend elektronisch zu speichern sollte vorerst den Online-Anwendungen mit sehr hohem Schutzbedarf vorbehalten bleiben, zieht der Anspruch auf Beweiswerterhaltung doch eine Reihe von Folgemaßnahmen nach sich.
Nähere Anforderungen beschreibt die BSI Richtlinie TR 03125 - TR-ESOR[15)].

Fazit

Die Ausführungen zeigen, dass die Umsetzung des OZG die Betrachtung vieler, zum Teil auch komplexer, Facetten erfordert. Dies ist nur arbeitsteilig möglich, wobei sich jede Seite auf die Arbeit der Anderen verlassen können muss.

An Stellen, wo nach heutigem Stand kein 100%iger Schutz zu erreichen ist, muss das verbleibende Risiko abgeschätzt und ggfs. getragen werden.
Wer welchen Anteil am Risiko tragen muss, wird nicht zuletzt die zukünftige Rechtssprechung entscheiden. Die Bewertung, ob die elektronische Welt gleichwertig oder besser als die Papierwelt ist, wird sich oft an Indizien orientieren.
Wobei auch die Papierwelt ihre Schwächen hat. Man denke nur bei der Authentizität an die Prüfbarkeit einer Unterschrift, vor allem wen sie per Fax eingegangen ist.
Ein für die Verwaltung oder den Verwaltungskunden untragbares Risiko darf nicht eingegangen werden.

Zur weiteren Qualifizierung der Risikoabschätzung sollten die Erfahrungen des aktuellen Umsetzungsstandes zu technischen und organisatorischen Aspekten und konkreten Gefährdungen und Manipulationsversuchen gesammelt und analysiert werden.
Diese Erfahrungen sind im Sinne eines kontinuierlichen Verbesserungsprozesses in weiteren Umsetzungsstufen zu berücksichtigen.
Denn für alles, was nicht absehbar ist, gilt nicht nur in der Informationssicherheit das Motto:

„Aus Erfahrung lernen“

Verweise

[1] BMI-OZG-Leistungskatalog
https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-leistungen/info-leistungen-node.htm

[2] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen
http://www.gesetze-im-internet.de/ozg/index.html

[3] REVOSax - Sächsisches Informationssicherheitsgesetz
https://revosax.sachsen.de/vorschrift/18349

[4] Reihe der Veröffentlichungen zur Internet-Sicherheit – ISi-Reihe
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/ISI-Reihe/isi-reihe_node.html

[5] Ransomware: Bedrohungslage, Prävention & Reaktion 2021
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf

[6] Sächsische E-Government-Plattform – Mitnutzungsvereinbarung (SVN/KDN-Extranet)
https://www.extranet.egovernment.sachsen.de/download/20191223_Kommunale_Mitnutzungsvereinbarung.pdf

[7] BSI-Standard 200-2 „IT-Grundschutz-Methodik“
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html

[8] BSI Baustein OPS.2.2: Cloud-Nutzung
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2020.pdf

[9] Sächsische E-Government-Gesetz-Durchführungsverordnung
https://www.revosax.sachsen.de/vorschrift/17103-Saechsische-E-Government-Gesetz-Durchfuehrungsverordnung

[10] Wikipedia-Artikel Elektronische Signatur
https://de.wikipedia.org/wiki/Elektronische_Signatur

[11] BMI OZG-Informationsplattform
https://vn-check.ozg-umsetzung.de/index.php/96979

[12] BSI-Richtlinie TR 03107-1
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

[13] Sächsisches E-Government-Gesetz
https://www.revosax.sachsen.de/vorschrift/14070-Saechsisches-E-Government-Gesetz#p11a

[14] Online Services Computer Interface“ – OSCI-Transport Spezifikation
https://www.itzbund.de/DE/itloesungen/standardloesungen/xoev/oscixoevbezugsstelle/oscixoevbezugsstelle_node.html

[15] BSI Richtlinie TR 03125 - TR-ESOR
Beweiswerterhaltung kryptographisch signierter Dokumente
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1_2_1.pdf