Von: Joachim Lindenberg <[redacted]@lindenberg.one>
Gesendet: Montag, 19. Juni 2023 13:51
An: [redacted]@bfdi.bund.de; POSTSTELLE@bfdi.bund.de
Betreff: AW: Anhörung Az. 16-206 II#1228
Anlagen: Testergebnis für bmi.bund.de (bfinv.de, bmi.bund.de) (6,39 KB); Testergebnis für bfinv.de (4,02 KB); Offener Brief zu Sicherheitsfragen an den Bundesbeauftragten für den Date... (110 KB); 2023-05-31 19_17_43-BundID-Sicherheitsfragen.png; AW: Sicherheit der Verarbeitung (Artikel 32 DSGVO) im Verwaltungsportal (617 KB)

Sehr geehrter [redacted], sehr geehrte Damen und Herren,

vielen Dank für Ihre Schreiben vom 01.06.2023 und 06.06.2023. Ich glaube nicht, dass sich die Telefonnotiz auf eine mögliche Akteneinsicht des BMIs in die Akte beim BfDI bezieht. Das BMI hat selbstverständlich als Beteiligte im Verfahren ein Akteneinsichtsrecht, das muss ganz sicher nicht erst besprochen werden, und als Rechtsgrundlage dafür dient das VwVfG und nicht das IFG. Wenn die Telefonnotiz so unklar ist, dann darf ich in Zukunft daran zweifeln, dass der BfDI die Grundsätze ordnungsgemäßer Aktenführung und insbesondere den Anspruch der Nachvollziehbarkeit beachtet.

Dass ich keinen Anspruch auf die Beschaffung von irgendwelchen Akten habe ist mir klar. Aber ich habe Anspruch darauf, dass der BfDI sich mit meiner Datenschutzbeschwerde ernsthaft befasst. In Anbetracht der Tatsache, dass Sie bisher nur relativ nichtssagende und nachweislich teilweise falsche Stellungnahmen des BMIs angefordert und wiedergegeben haben ist die bisherige Tätigkeit des BfDI in meinen Augen unzureichend. Ich darf deswegen falsch schreiben, denn die Bund-ID erfüllt noch nicht einmal die mehrfach erwähnte Anforderung NET.1.1.A7. Emails werden ohne obligatorische Transportverschlüsselung im Sinne der Orientierungshilfe Emailverschlüsselung der Datenschutzkonferenz übermittelt und können von einem aktiven Angreifer mitgelesen oder umgeleitet werden. Die entsprechenden Testergebnisse (eines vom März 2022, eines Mai 2023) füge ich bei. ITZ Bund – Betreiber des verwendeten Emailservers – ist zertifiziert? Aber ganz offensichtlich ohne NET.1.1.A7? Oder hat der Auditor das übersehen?

Dieses Problem hat ganz offensichtlich auch der vom BMI erwähnte Penetrationstester nicht gefunden, denn nach Angaben des BMI soll der ja einmal im Jahr die Sicherheit prüfend und gewährleisten. Nein, daran dass Penetrationstests alle Sicherheitsprobleme finden glaube ich nicht. Ich glaube an geeignete Sicherheitskonzepte, und dass das BMI keine obligatorische Transportverschlüsselung, dafür aber unsichere und überflüssige Sicherheitsfragen verwendet, deutet für mich klar darauf hin, dass man kein in der Softwareentwicklung kein ausreichendes Wissen über Sicherheit und auch kein taugliches Sicherheitskonzept hat. Eine Kopie meines offenen Briefs an den BfDI darf ich beifügen. Desweiteren füge ich einen Screendump bei, der die Fragen bei Bund-ID zeigt, und fast alle Antworten sind bei vielen Betroffenen trivial zu ermitteln. Sicherheit kann man so nicht erreichen. Und überflüssig, weil man sowohl ein Emailkonto nutzen muss und damit ein Passwort-Rücksetzen ohne Sicherheitsfragen anbieten könnte. Sogar wenn man das Konto mit eID anlegt und nach Anmeldung mit eID ohne Eingabe der Sicherheitsfragen das Passwort ändern kann werden Sicherheitsfragen erzwungen. Die Sicherheitsfragen sind also bei Anlage mit eID unnötig und verstoßen damit gegen die Datensparsamkeit, bei Anlage mit Email + Passwort sind sie inhärent unsicher. Ich darf mir daher analog zur Beschwerde von Christina Franke in 11-103 II#7156 Beschwerde wegen der Verwendung von unsicheren und unnötigen Sicherheitsfragen einlegen. Aber der BfDI ist m.W. noch nie gegen das Unterschreiten des Stand-der-Technik oder des gesunden Menschenverstands aktiv geworden, von NET.1.1.A7 vielleicht abgesehen, und Anbetracht des Bescheid vom 28.03.2023 zu Beschwerde 24-191 II#5163 „Es besteht keine datenschutzrechtliche Verpflichtung, … einen maximalen Sicherheitsstandard zu implementierten. … Ein etwaiges Abweichen von meinen Empfehlungen .. begründet noch keinen Verstoß gegen die DSGVO.“ erwarte ich eigentlich, dass Sie jede Beschwerde ablehnen und sich damit mitschuldig machen, dass Deutschland miserabel im Bereich Sicherheit ist.

Das BMI behauptet auch, „die Speicherlösung ist verschlüsselt." Sie selbst zitieren weitere Teile von SYS.1.8.A23 „Verschlüsselung auf dem Transportweg auch bei Replikationen und Backup-Traffic relevant ist" – keine Aussage dazu. In Anbetracht der Tatsache, dass man auch behauptet die Kommunikation sei entsprechend NET.1.1.A7 verschlüsselt und diese Aussage nachweislich falsch ist, darf ich Wahrheitsgehalt und Wert dieser Aussage bezweifeln, denn selbst wenn tatsächlich irgendwie verschlüsselt wird, selbst dann habe ich eine Vorstellung davon, welche untauglichen Varianten im Einsatz sein können – einige davon bei Dataport und anderen Behörden erlebt, und einige davon sind anscheinend auch Standard im Grundschutzumfeld, wenn auch erkennbar schlechte Standards.

Zurück zur Beschaffung von Akten: ich habe das BMI selbst um Einsicht in das Sicherheitskonzept gebeten, die entsprechende Email füge ich ebenfalls bei. Das BMI hat bis heute nicht geantwortet, ich darf daher eine weitere Beschwerde gegen das BMI wegen Verstoß gegen Artikel 5 Abs. 2 DSGVO einreichen. Inzwischen hat sogar ein Gericht festgestellt, dass Geheimhaltung ein Zeichen für Unsicherheit ist, sehr schön aufbereitet von Dominic Deuber und Michael Keuchen in "Anonymisierung von Gerichtsentscheidungen im Lichte der IT-Sicherheit", Multimedia und Recht (MMR) Nr. 5/2023. Wenn das BMI Angst vor einer Veröffentlichung hat, dann nur weil das Sicherheitskonzept löchrig ist. Pikant auch, dass das BMI schreibt, dass die „Sicherheitskonzeption, insbesondere die Risikoanalyse, regelmäßig unter Einbeziehung des BSI überprüft wird" – davon dass Mängel beseitigt werden steht da nichts. Der Hinweis auf 21-506-1 II#2896 sei mir erlaubt – da werden bestimmt schneller neue Löcher geschaffen als alte geschlossen.

Der BfDI ist unabhängige Aufsicht mit Untersuchungsbefugnissen aus Artikel 58 DSGVO und einem Durchsetzungsauftrag in Artikel 57 DSGVO. Unter einer Untersuchung verstehe ich mehr, als nur die Stellungnahmen der Verantwortlichen einzuholen und dann weitgehend wörtlich wiederzugeben. Ich sehe nicht, dass der BfDI seinem Auftrag gerecht wird, wenn man die Beschwerden Betroffener konsequent bis auf unvermeidliches ablehnt statt dem Datenschutz zum Durchbruch zu verhelfen, und auch nicht wenn man sich keine eigene Meinung zu Artikel 32 oder dem Grundschutz bildet. Die Presse hat anlässlich des 5. Jahrestags der DSGVO auch in vielen Publikationen ein enormes Durchsetzungsdefizit festgestellt. Oder wir alle werden uns nicht wundern, wenn jede Woche eine weitere Behörde oder Organisation als gehackt in den Nachrichten auftaucht.

Auch wenn ich eigentlich digital-Enthusiast bin: wie gut, dass im Umgang mit Behörden vieles immer noch „analog" geht.

Mit freundlichen Grüßen
Joachim Lindenberg

Von: Joachim Lindenberg <[redacted]@lindenberg.one>
Gesendet: Freitag, 26. Mai 2023 14:38
An: POSTSTELLE@bfdi.bund.de
Betreff: Anhörung Az. 16-206 II#1228

Sehr geehrter [redacted], sehr geehrte Damen und Herren,

vielen Dank für Ihr Schreiben vom 24.05.2023 und 12.04.2023. Auch in diesem Verfahren darf ich Sie zunächst bitten, mir vor einer Stellungnahme etwaige neuere Schriftwechsel mit dem BMI, BSI, oder ITZ Bund in dieser Sache, die mir noch nicht vorliegen, in Kopie zuzusenden – gerne auch per Email mittels qualifizierter Transportverschlüsselung. Insbesondere möchte ich auch wissen, ob das BMI wie in der Aktennotiz vom 24.05.2022 erwähnt bereit ist, Einsicht in das Sicherheitskonzept zu geben. Meine nochmals beigefügte Email – auch in der Untätigkeitsklage erwähnt – hat es bis zu meiner letzten Auskunft wohl wegen der fehlenden 8 oder weil Referat 11 mit im Boot war nicht in die richtige Akte geschafft.

Vielen Dank und viele Grüße
Joachim Lindenberg

Lindenberg Software

Von: Lindenberg Email Test Service <emailtest@lindenberg.one>
Gesendet: Freitag, 26. Mai 2023 23:05
An: noreply@bmi.bund.de
Cc: emailtest@lindenberg.one
Betreff: Testergebnis für bmi.bund.de (bfinv.de, bmi.bund.de)

Verbindungshistorie:
26.05.2023 20:35:56 - 20:36:06 (lxmxext2.bfinv.de/lxmxext2.bfinv.de/80.245.147.31/ITZBUND-NET-1, ITZBUND-NET-BN, Germany -> Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Spf:Pass Signatures:None
26.05.2023 20:57:42 - 20:57:47 (lxmxext2.bfinv.de/lxmxext2.bfinv.de/80.245.147.31/ITZBUND-NET-1, ITZBUND-NET-BN, Germany -> Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Spf:Pass Signatures:None
26.05.2023 21:21:09 - 21:21:15 (lxmxext2.bfinv.de/lxmxext2.bfinv.de/80.245.147.31/ITZBUND-NET-1, ITZBUND-NET-BN, Germany -> Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Spf:Pass Signatures:None
26.05.2023 22:02:15 - 22:02:21 (lxmxext2.bfinv.de/lxmxext2.bfinv.de/80.245.147.31/ITZBUND-NET-1, ITZBUND-NET-BN, Germany -> Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Spf:Pass Signatures:None
26.05.2023 22:21:03 - 22:21:08 (lxmxext2.bfinv.de/lxmxext2.bfinv.de/80.245.147.31/ITZBUND-NET-1, ITZBUND-NET-BN, Germany -> Server 2, verschlüsselt, Mail):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Spf:Pass Signatures:None
26.05.2023 23:04:36 - 23:04:41 (lxmxext2.bfinv.de/lxmxext2.bfinv.de/80.245.147.31/ITZBUND-NET-1, ITZBUND-NET-BN, Germany -> Server 2, verschlüsselt, Acked):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Spf:Pass Signatures:None

Analyse Senden von Email
Ihr Mailserver verwendet kein SNI, also auch kein RFC 7672 oder RFC 8461, und akzeptiert dann vermutlich auch beliebige Zertifikate beim Senden (nicht gut).
Ihr Mailserver hat eine Mail (FROM/RCPT/DATA) ohne Verschlüsselung (STARTTLS) übertragen. Selbst wenn er RFC 7672 oder RFC 8461 verwenden sollte, erzwingt er keine Verschlüsselung (nicht gut, aber leider normal).
Ihr Mailserver unterstützt DKIM nicht (nicht gut).
Ihr Mailserver verwendet DMARC ohne auch SPF und DKIM zu verwenden - das kann dazu führen, dass Nachrichten zurückgewiesen werden (nicht gut).

Analyse Empfangen von Email
Die Domäne bmi.bund.de @ Provider bund.de verwendet DNSSEC für MX-Records (gut).
Die Domäne bmi.bund.de @ Provider bund.de verwendet DNSSEC für A-Records (gut).
Die Domäne bmi.bund.de @ Provider bund.de verwendet DNSSEC für TLSA-Records (gut).
Die Domäne bmi.bund.de @ Provider bund.de verwendet STARTTLS (gut).
Die Domäne bmi.bund.de @ Provider bund.de verwendet gültige Zertifikate (gut).
Die Domäne bmi.bund.de @ Provider bund.de unterstützt die qualifizierte Transportverschlüsselung (gut).
Die Domäne bmi.bund.de @ Provider bund.de unterstützt RFC 7672 SMTP-DANE (sehr gut).
Die Domäne bmi.bund.de @ Provider bund.de unterstützt nicht RFC 8461 MTA-STS (nicht gut).

Mehr Informationen ggfs. auf https://blog.lindenberg.one/EmailSicherheitsTest#bmi.bund.de

Lindenberg Software

Von: Lindenberg Email Test Service <noreply@lindenberg.one>
Gesendet: Montag, 7. März 2022 22:53
An: emailtest@lindenberg.one
Betreff: Testergebnis für bfinv.de

Verbindungshistorie:
07.03.2022 16:17:06 - 16:17:10 (Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Signatures:None
07.03.2022 16:32:29 - 16:32:32 (Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Signatures:None
07.03.2022 17:11:43 - 17:11:46 (Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Signatures:None
07.03.2022 17:44:00 - 17:44:03 (Server 2, nicht verschlüsselt, None):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Signatures:None
07.03.2022 18:06:07 - 18:06:16 (Server 2, verschlüsselt, Mail):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Signatures:None
07.03.2022 18:33:30 - 18:33:34 (Server 2, verschlüsselt, Acked):
From: <n***y@bmi.bund.de> To: <nr@et.lindenberg.one> Signatures:None

Ihr Mailserver verwendet kein SNI, also auch kein RFC 7672, und akzeptiert dann vermutlich auch beliebige Zertifikate beim Senden (nicht gut).
Ihr Mailserver hat eine Mail (FROM/RCPT/DATA) ohne Verschlüsselung (STARTTLS) übertragen. Selbst wenn er RFC 7672 verwenden sollte, erzwingt er keine Verschlüsselung (nicht gut, aber leider normal).

Die Domäne bfinv.de verwendet kein DNSSEC für MX-Records (nicht gut).
Die Domäne bfinv.de verwendet kein DNSSEC für A-Records (nicht gut).
Die Domäne bfinv.de verwendet kein DNSSEC für TLSA-Records (nicht gut).
Die Domäne bfinv.de verwendet STARTTLS (gut).
Die Domäne bfinv.de verwendet gültige Zertifikate (gut).
Die Domäne bfinv.de unterstützt keine qualifizierte Transportverschlüsselung/RFC 7672 STARTTLS/DANE (nicht gut).

Mehr Informationen ggfs. auf https://blog.lindenberg.one/EmailSicherheitsTest#bfinv.de

Lindenberg Software

Von: Joachim Lindenberg <[redacted]@lindenberg.one>
Gesendet: Montag, 3. April 2023 18:29
An: PRESSESTELLE@bfdi.bund.de
Betreff: Offener Brief zu Sicherheitsfragen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
Anlagen: Offener Brief zu Sicherheitsfragen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.pdf

Sehr geehrter Herr Professor Kelber,
ich darf Ihnen eine Kopie meines offenen Briefs zusenden.
Mit freundlichen Grüßen
Joachim Lindenberg

Offener Brief zu Sicherheitsfragen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Sehr geehrter Herr Professor Kelber,

im 31. Tätigkeitsbericht für das Jahr 2022 schreiben Sie auf Seite 84 im Abschnitt 8.13:

> *Dies bedeutet für die Bürgerinnen und Bürger auf der anderen Seite, dass sie die Zugriffsinformationen zu ihrem Konto wie beispielsweise auch ihren Haustürschlüssel nicht „verlegen" sollten. Sonst droht auch hier die Gefahr, sich „auszusperren".*
>
> — *31. Tätigkeitsbericht, Seite 84*

Soweit richtig.

> *Ebenfalls als ungünstig kann sich erweisen, wenn man für die alternativ vorgesehenen Sicherheitsabfragen – vielleicht sogar „zur Sicherheit" – falsche Angaben macht, an die man sich dann später nicht mehr erinnern kann.*
>
> — *31. Tätigkeitsbericht, Seite 84*

Der hier implizierten Empfehlung, richtige Angaben zu machen, muss ich widersprechen und darf Wikipedia zitieren:

> *Eine Sicherheitsfrage ist eine Authentifizierungsmethode, die häufig als zusätzlicher Sicherheits-Layer sowie zur Wiederherstellung von vergessenen Passwörtern eingesetzt wird. Es handelt sich um ein gemeinsames Geheimnis.*
>
> *Eine typische Sicherheitsfrage ist zum Beispiel: „Wie lautet der Mädchenname Ihrer Mutter?"*
>
> *Es wird bemängelt, dass die in Sicherheitsfragen abgefragten Fakten meist öffentlich zugänglich sind und daher von Hackern leichter herausgefunden werden können als Passwörter. Manche Benutzer sind sich dessen bewusst und erfinden absichtlich falsche Antworten, die sie dann aber oft vergessen und somit das Konzept der Sicherheitsfrage ad absurdum führen.*
>
> — *Sicherheitsfrage (Wikipedia)*

Genau, das Konzept ist absurd. Aus einem meiner eigenen Artikel darf ich zitieren:

> *Das grundsätzliche Problem bei Sicherheitsfragen ist, dass die richtige Antwort in fast allen Fällen nicht nur dem Benutzer sondern auch vielen anderen bekannt ist, oder über öffentliche Quellen wie z.B. Telefonbuch, Social Media, oder über Social-Engineering ermittelbar ist. Wikipedia zitiert Josh Levins In What City Did You Honeymoon? And other monstrously stupid bank security questions. Josh Levin ist natürlich nicht der einzige, der von Sicherheitsfragen abrät. Auch das NIST, OWASP, und Bruce Schneier (2005) raten eindeutig von Sicherheitsfragen ab. OWASP zitiert dabei auch Studien von Microsoft (2009) und Google (2015), die klar zeigen, dass Sicherheitsfragen nicht funktionieren. Sicherheitsfragen entsprechen also schon einige Zeit nicht dem Stand der Technik. …*
>
> *Werden Sicherheitsfragen verwendet, dann sollte man als Benutzer falsche Antworten eingeben – z.B. generierte Passwörter des Passwortmanagers – und sie dann auch am besten dort aufbewahren für den Fall, dass sie wirklich irgendwann zum Einsatz kommen sollten. Leider erschweren einige Verwender das dadurch, dass die Eingaben validiert werden und damit der Zufall begrenzt wird.*
>
> — *Sicherheit? Nein Unsinn!*

Auf die Gefahr, den einen oder anderen Leser vorübergehend abzuhängen: Christina Franke hat sich in ihren Beschwerden zu den Verwaltungsportalen auch gegen Sicherheitsfragen gewandt. Die typische Antwort der Behörden und Aufsichten war, das findet ja nur auf niedrigem Vertrauensniveau statt. Das Bundesamt für Sicherheit schrieb mir:

> *Da es sich laut dem verlinkten Text offenkundig um eine Basisregistrierung – also kein Vertrauensniveau nach eIDAS-Verordnung – handelt, wäre eine Absicherung des Zugangs zu einem derartigen Account mit Hilfe einer Sicherheitsabfrage bspw. bei einem vergessenen Passwort nicht unüblich.*
>
> *Diese Vorgehensweise wird im Übrigen nach unsere Kenntnis noch bei vielen vergleichbar niedrigschwelligen privatwirtschaftlichen Angeboten gewählt (z.B. Wiederherstellung des Zugangs zu Freemail-Postfächern)*
>
> — *Email des Bundesamt für Sicherheit vom 26.10.2022*

Email und niedriges Vertrauensniveau? Sie Herr Professor Kelber schreiben:

> *Vielfach speichern Bürgerinnen und Bürger in ihrem E-Mail-Konto viele E-Mails, aus denen sich zahllose persönliche Informationen und Querverbindungen ergeben.*
>
> — *31. Tätigkeitsbericht, Seite 84*

Das interpretiere ich nicht gerade als niedriges Vertrauensniveau oder niedrigen Schutzbedarf. Und nach meinen Beobachtungen versteht der normale Anwender im digitalen Leben weder den Sinn unterschiedlicher Vertrauensniveaus noch kann er mit Sicherheitsfragen umgehen – und hier werden sich die oben abgehängten Leser wiederfinden.

Ich halte es für wünschenswert, Sicherheitsfragen abzuschaffen. Sie und alle Datenschutzaufsichten können dazu einen Beitrag leisten, in dem Sie auf Abschaffung drängen. Solange das nicht stattgefunden hat halte ich es für richtig, Anwendern zu empfehlen, sich die falschen Antworten genau wie Passwörter zu merken und für den Schutz von beidem sichere Verfahren – Passwortmanager und Datensicherung – zu verwenden. Ich halte es für unverantwortlich, Anwendern zu empfehlen, richtige Antworten zu oft trivial zu ermittelnden Angaben zu machen.

Ich würde mich freuen, wenn Sie hier einen Beitrag zur digitalen Grundausbildung leisten würden. Auch dazu schreiben Sie richtig:

> *Wirksamer Datenschutz setzt damit auch entsprechende Digitalkompetenzen bei allen Akteuren sowie ein Bewusstsein für den Schutz der eigenen Daten voraus. Hier werde ich mich weiterhin sowohl für einfache und verständliche aber sichere Systeme als auch für ein breiteres Datenschutzbewusstsein einsetzen.*
>
> — *31. Tätigkeitsbericht, Seite 84*

Lassen Sie den Worten bitte Taten folgen. Anregungen dazu finden Sie positiv auf Digitale Selbstverteidigung und auf den dort verlinkten Seiten, Negativbeispiele auf Sicherheit? Nein Unsinn.

Vielen Dank und viele Grüße

Joachim Lindenberg

Veröffentlicht am 03.04.2023

Sicherheitsfrage*

bitte wählen

In welcher Stadt haben sich Ihre Eltern kennengelernt?
Wie lautet der Name Ihres ersten Haustiers?
Wie lautet der Mädchenname Ihrer Mutter?
Wie lautet der Name Ihres ersten Arbeitgebers?

Lindenberg Software

Von: Joachim Lindenberg <[redacted]@lindenberg.one>
Gesendet: Freitag, 18. November 2022 15:16
An: bds@bmi.bund.de; datenschutz@im.bwl.de; datenschutzbeauftragter@stmd.bayern.de; behdsb@seninnds.berlin.de; poststelle@zit-bb.brandenburg.de; datenschutzbeauftragter@finanzen.bremen.de; itd-dsb@sk.hamburg.de; datenschutz@stk.hessen.de; Datenschutz@im.mv-regierung.de; datenschutzbeauftragter@mi.niedersachsen.de; poststelle@mhkbg.nrw.de; datenschutz@mastd.rlp.de; datenschutz@sk.sachsen.de; datenschutz-mid@sachsen-anhalt.de; DSB-ZIT@melund.landsh.de; TLRZ-Datenschutzbeauftragter@tlrz.thueringen.de
Cc: 'Christina Franke'
Betreff: AW: Sicherheit der Verarbeitung (Artikel 32 DSGVO) im Verwaltungsportal
Anlagen: Presseausweis.pdf

Sehr geehrte Damen und Herren,

dieser Aufforderung und Anfrage will ich mich als selbst betroffener Nutzer und als Pressevertreter (Presseausweis anbei) anschließen.

Vielen Dank und viele Grüße
Joachim Lindenberg

Von: Christina Franke <frankechristina@[redacted]>
Gesendet: Donnerstag, 17. November 2022 17:32
An: bds@bmi.bund.de; datenschutz@im.bwl.de; datenschutzbeauftragter@stmd.bayern.de; behdsb@seninnds.berlin.de; poststelle@zit-bb.brandenburg.de; datenschutzbeauftragter@finanzen.bremen.de; itd-dsb@sk.hamburg.de; datenschutz@stk.hessen.de; Datenschutz@im.mv-regierung.de; datenschutzbeauftragter@mi.niedersachsen.de; poststelle@mhkbg.nrw.de; datenschutz@mastd.rlp.de; datenschutz@sk.sachsen.de; datenschutz-mid@sachsen-anhalt.de; DSB-ZIT@melund.landsh.de; TLRZ-Datenschutzbeauftragter@tlrz.thueringen.de
Cc: Joachim Lindenberg <journalismus@lindenberg.one>
Betreff: Sicherheit der Verarbeitung (Artikel 32 DSGVO) im Verwaltungsportal

Sehr geehrte Damen und Herren,

einige von Ihnen haben mir eine Auskunft geschickt, bei anderen warte ich noch darauf. Leider bleiben auch bei denen, die mir Auskunft zu meiner Beschwerde gegeben haben, viele Fragen offen, auch weil die jeweiligen Aufsichten Ihnen relevante Fragen gar nicht gestellt haben. Daher bitte ich Sie, mir die folgenden Dokumente und Nachweise der Sicherheit der Verarbeitung im jeweiligen Verwaltungsportal/Serviceportal oder wie auch immer Sie Ihr Portal zum OZG nennen zur Verfügung zu stellen:

1. Schutzbedarfsfeststellungen und Datenschutzfolgenabschätzungen soweit vorhanden.

2. Sicherheitskonzepte, inbesondere auch alle Dokumente, die die folgenden Fragen beantworten:

- wird bei der Speicherung der Daten konsequent verschlüsselt und wenn ja, wie? gilt dies auch für Infrastrukturkomponenten wie virtueller Speicher, Virenscanner, Router, Firewall, etc.? wie wird dabei Schlüsselmanagement realisiert?

- werden Daten bei der Übertragung innerhalb des Rechenzentrums oder bei der Weitergabe an Dritte verschlüsselt und wenn ja, wie? Gibt es davon Ausnahmen?
- wie werden Komponenten (gegenseitig) authentisiert/authentifiziert? Als unterscheidbare Komponente betrachte ich zumindest alles was über irgendein Netzwerk kommuniziert, unabhängig davon ob das Netzwerk öffentlich oder privat ist.
- wird VMware ESXi verwendet (zur Sicherheit davon siehe https://blog.lindenberg.one/BundesamtUnsicherheit#vmware)?
- können Administratoren aus einem WLAN zugreifen und falls ja, welche Art der Authentifizierung wird verwendet um das Eduroam-Problem zu vermeiden (siehe https://blog.lindenberg.one/BundesamtUnsicherheit#eduroam)?
- werden Web-Application-Firewalls eingesetzt, und wenn ja, mit welchen Filterregeln?
- falls Sicherheitsfragen verwendet werden, werden die entsprechenden OWASP-Empfehlungen dazu (https://cheatsheetseries.owasp.org/cheatsheets/Choosing_and_Using_Security_Questions_Cheat_Sheet.html) eingehalten?
- welche Sicherheitsanforderungen haben Sie für die Software oder andere Komponenten im Zusammenhang mit BSI Grundschutz APP.6 A2/APP.7 A4 definiert?

3. In welchen Abständen finden Änderungen an Diensten statt? wie und in welchen Zeitabständen wird die Einhaltung des Sicherheitskonzepts bzw. der Sicherheitsanforderungen überprüft, insbesondere auch, aber nicht nur, bei Zulieferungen? Wurden bereits Penetrationstests oder Webchecks (u.a. nach §2 IT-Sicherheitsverordnung Portalverbund) durchgeführt und mit welchem Ergebnis?

4. welche TOMs haben Sie mit Auftragsverarbeitern vereinbart und wie beantwortet der Auftragsverarbeiter die Fragen 1 bis 3 einschließlich Unterpunkte?

5. existiert eine Eigenerklärung nach §2 Absatz 12 IT-Sicherheitsverordnung Portalverbund? Bitte mitschicken.

Um der Umwelt das unnötige Bedrucken oder Kopieren von Papier zu ersparen bitte ich Sie, ale Dokumente auf CD oder DVD zur Verfügung zu stellen.

Vorsorglich will ich anführen, dass ein Sicherheitskonzept das auf Geheimhaltung beruht in der Fachwelt als unsicher angesehen wird, weil nur öffentliche Begutachtung Sicherheitsmängel aufdeckbar macht. Auch kann ein Angreifer aus den Mängeln und Wahlmöglichkeiten im Grundschutz sehr leicht ableiten, welche Angriffe erfolgsversprechend sein können.

Als Inhaberin eines Servicekontos in Ihrem jeweiligen Verwaltungsportal bin ich Betroffene im Sinne der DSGVO. Damit trifft Sie als Verantwortliche die Beweislast aus Artikel 5 II i.V.m. Artikel 5 I lit. f für die Sicherheit der Verarbeitung nach Artikel 32 DSGVO. Diese Beweislast besteht nicht nur gegenüber der Aufsicht, sondern nach dem Urteil des Bundesverwaltungsgericht vom 02.03.2022, BVerwG 6 C 7.20, Rn. 50 und dem Urteil des Europäischen Gerichtshofs vom 24. Februar 2022 C-175/20, Rn. 77 auch gebenüber betroffenen Personen.

Mit freundlichen Grüßen
Christina Franke