RheinlandPfalz
MINISTERIUM FÜR
WISSENSCHAFT
UND GESUNDHEIT

Ministerium für Wissenschaft und Gesundheit
Postfach 32 20 | 55022 Mainz

[redacted]

Mittlere Bleiche 61
55116 Mainz
Telefon 06131 16-0
Telefax 06131 16-2997
poststelle@mwg.rlp.de
www.mwg.rlp.de

10. Januar 2024

Per elektronischer Kommunikation

Mein Aktenzeichen	Ihr Schreiben vom	Ansprechpartner/-in / E-Mail	Telefon / Fax
[redacted] Bitte immer angeben!	14.11.2023 u. 12.12.2023 - #292235	[redacted]	[redacted]

Ihre Anfrage nach dem Landestransparenzgesetz

Sehr [redacted],

ich bestätige den Empfang Ihrer E-Mail-Eingabe vom 14.11.2023 - #292235 nach dem Landestransparenzgesetz (LTranspG), mit der Sie Auskunft über bekannte Informationen und schriftliche Aufzeichnungen über bekannte Sicherheitslücken der Software „Health“ der Firma Mikroprojekt GmbH im Kontext des Digitalisierungsprojektes in Rheinland-Pfalz erbitten, sowie Ihre ergänzende E-Mail vom 12.12.2023.

Ihre Anfrage wird als Antrag nach §§ 2 Abs. 2, 11 Landestransparenzgesetz (LTranspG) behandelt.

Insoweit gab es insbesondere mehrere Anfragen von Zeit Online an die Herstellerfirma der Software, den Landesbeauftragten für den Datenschutz und die Informationssicherheit sowie das Ministerium für Wissenschaft und Gesundheit.
Nachstehend sind die hierzu vorliegenden Anfragen und Antworten zusammengefasst dargestellt.
Weitere Anfragen von Zeit Online und Antworten sind hier nicht bekannt.

1. Anfrage Zeit-Online an die Mikroprojekt GmbH und entsprechende Antwort

Sehr geehrte…,,

vielen Dank für Ihre konkreten Fragen zum Einsatz unserer Software mikropro health in Rheinland-Pfalz und der Möglichkeit, sie in kurzer Form zu erläutern.

Die Software wurde über die letzten Jahrzehnte mit Kommunen aus unterschiedlichsten Bundesländern entwickelt und an deren Bedürfnisse konsequent angepasst. health ist eine .NET Desktop-Anwendung und ist nur aus dem behördlichen Netzwerk zu erreichen. Es handelt sich daher nicht um eine Web-Applikation wie Luca oder Sormas.

Zu Punkt 1:
"Unter anderem sind laut den uns vorliegenden Informationen das Login und das Passwort für die Datenbank-Konfiguration (Initialisierungsdatei) direkt im Code enthalten, also hartkodiert. Ist das korrekt? Wenn ja, warum sind Login und Passwort hartcodiert? Halten Sie das für ein Sicherheitsproblem?
Wenn nein, warum nicht?"

Zum erstmaligen Einrichten eines Clients kann über eine hartkodierte Benutzer-Passwort-Kombination ein Tool zur Konfiguration der Datenbankverbindung aufgerufen werden. Nach Einrichten einer validen Verbindung kann dann ein eigenes Passwort frei vergeben werden. Das hartkodierte Passwort kann dann nicht mehr verwendet werden. Deswegen sehen wir das nicht als Sicherheitsproblem.

Zu Punkt 2:
"Zudem scheint die Rechteverwaltung nicht konsequent umsetzbar zu sein: So haben wir Hinweise, dass selbst Nutzer, denen alle Berechtigungen entzogen sind, weiterhin einige Informationen sehen können – beispielsweise welche Bürgerinnen mit dem sozialpsychiatrischen Dienst zu tun haben. Ist das korrekt? Wenn ja, handelt es sich dabei um eine Beschränkung der Software oder um eine Vorgabe der Softwarenutzer?"

Diese Aussage ist so nicht korrekt. Über unsere Rollen- und Rechteverwaltung lassen sich die einzelnen Fachbereiche im Gesundheitsamt trennen. Das Rechtesystem ist kumulativ, so dass ein Benutzer über alle Rechte aus den Benutzergruppen verfügt, denen er zugeordnet ist. Die Administratoren der jeweiligen Ämter sind für dies Rechtevergabe eigenverantwortlich zuständig.
Bei entsprechender Rechtevergabe ist für einen Benutzer ein Bezug zu einem anderen Vorgangsgrund eines Klienten nicht sichtbar.

Zu Punkt3:
"Die von Mikropro genutzte Datenbank lässt laut den uns vorliegenden Informationen beliebige SQL-Abfragen zu, unabhängig davon, ob die entsprechenden Nutzer und Nutzerinnen zu solchen Abfragen berechtigt sind.
Halten Sie das für ein Sicherheitsproblem? Wenn nein, warum nicht?"

Zur besseren Wartung und Fehleranalyse gibt es einen SQL-Editor, über den Abfragen in der verbundenen Datenbank ausgeführt werden können. Diese Funktion ist für den Support und die Administration gedacht und durch entsprechende Berechtigungen abgesichert. Damit haben nur Benutzer Zugriff auf dieses Tool, die entsprechende Rechte dazu haben. Die Vergabe liegt eigenverantwortlich bei den lokalen Administratoren. Hierin sehen wir kein Sicherheitsproblem, da die Rechte, den SQL-Editor zu verwenden durch die lokalen Administratoren entsprechend gesetzt werden können.

Zu Punkt 4:
Passwörter der Nutzer und Nutzerinnen werden bei bestimmten Anwendungen im Klartext gespeichert und nicht verschlüsselt, ist das korrekt? Halten Sie das für ein Sicherheitsproblem? Wenn nein, warum nicht?

Das stimmt so nicht. Per Installation durch den lokalen Administrator können die Passwörter der Mitarbeiter mit der Technik AES-256 verschlüsselt werden.
Damit sind sie dann nicht mehr im Klartext lesbar.

Zu Punkt 5:
"Die Software Mikropro Health wird demnach mit einem Standardaccount für Administratoren ausgeliefert, der mit immer demselben Standardpasswort gesichert ist. Ist das korrekt? Halten Sie das für ein Sicherheitsproblem?
Wenn nein, warum nicht?"

Es ist korrekt, dass unsere Software mit einem Standardaccount für Administratoren ausgeliefert wird um damit die Ersteinrichtung von weiteren Benutzern vorzunehmen. Diese Vorgehensweise ist auch in anderen Softwareprodukten so üblich. Die lokalen Administratoren sind dazu angehalten diesen Account anschließend zu löschen oder inaktiv zu setzen.
Bei dieser Vorgehensweise sollte das kein Sicherheitsproblem sein.

Zu Punkt 6:
"Die Mikroprojekt GmbH beziehungsweise Ihre Support-Mitarbeiter haben Zugriff auf die gesamte Datenbank der Gesundheitsämter, wenn diese zur Fehlersuche an die Mikroprojekt GmbH übermittelt wird – was laut unseren Informationen Praxis ist. Wie stellen Sie sicher, dass diese Daten nicht missbraucht werden?"

Wie bereits oben beschrieben, haben wir zur Wartung und Fehleranalyse in der Datenbank entsprechende Tools, die wir vor Ort oder per Fernwartung verwenden können. Bei komplexen Sachverhalten kann es aber dazu kommen, dass wir die Datenbank selbst zur Analyse benötigen. Unsere Verträge mit unseren Kunden, aber auch mit unseren Mitarbeitern, regeln den Umgang mit diesen Daten. Die Daten werden prinzipiell nur an zuständigen Mitarbeiter bei uns übermittelt. Es ist für uns selbstverständlich, dass neben der verschlüsselten Übertragung (zzgl. Abspeichern in einem speziell verschlüsselten Veracrypt-Container), die Daten nur für den notwendigen Zweck betrachtet und im Anschluss unverzüglich wieder gelöscht werden. Der Umgang mit Daten wird auch regelmäßig in internen Meetings besprochen, auch um auf die Sensibilität der Daten nochmals hinzuweisen. Datenschutzrechtlich sind wir in einem solchen Fall Auftragsverarbeiter im Sinne von Art. 28 DSGVO. Eine entsprechende Vereinbarung zur Auftragsverarbeitung wird zwischen uns und dem Kunden geschlossen.

Zu Punkt 7:
"Ist Ihr Unternehmen für die Verarbeitung solcher Daten durch das BSI zertifiziert? Wenn ja, in welchem Umfang?"

Nein, eine BSI-Zertifizierung haben wir nicht, wir beachten aber bei unserer Programmierung stets die Richtlinien des BSI und ziehen externe Datenschützer beratend hinzu. Wir sind uns unserer Verantwortung bei der Entwicklung unserer Software gerade im Bereich Gesundheit bewusst. Aus diesem Grund werden noch in diesem Jahr oder Anfang nächsten Jahres unsere Software einem Pentest inkl. Code-Review unterziehen.

Wir hoffen, dass Ihnen diese Antworten weiterhelfen, die wir in der Kürze der uns zur Verfügung stehenden Zeit verfasst haben.

Mit freundlichen Grüßen aus Kaiserslautern

-----Ursprüngliche Nachricht-----
Von: @zeit.de]
Gesendet: Dienstag, 31. Oktober 2023 08:20
An: health@mikroprojekt.de; software@mikroprojekt.de
Cc: …….
Betreff: EILT: Statement zu Sicherheitslücken in Ihrer Software

Sehr geehrte Damen und Herren,

uns liegen Informationen vor, aus denen hervorgeht, dass die Gesundheitsämter in Rheinland-Pfalz Software Ihres Unternehmens Mikroprojekt GmbH nutzen und weiter nutzen sollen. Unseren Informationen zufolge gibt es in Mikropro Health einige Sicherheitslücken und potentielle Einfallstore für Unbefugte. Für unseren aktuellen Artikel für Zeit Online haben wir dazu einige Fragen. Bitte beantworten Sie diese bis Donnerstag, 2.11., 11 Uhr.

Unter anderem sind laut den uns vorliegenden Informationen das Login und das Passwort für die Datenbank-Konfiguration (Initialisierungsdatei) direkt im Code enthalten, also hartkodiert. Ist das korrekt? Wenn ja, warum sind Login und Passwort hardcodiert? Halten Sie das für ein Sicherheitsproblem? Wenn nein, warum nicht?
Zudem scheint die Rechteverwaltung nicht konsequent umsetzbar zu sein: So haben wir Hinweise, dass selbst Nutzer, denen alle Berechtigungen entzogen sind, weiterhin einige Informationen sehen können – beispielsweise welche Bürgerinnen mit dem sozialpsychiatrischen Dienst zu tun haben. Ist das korrekt? Wenn ja, handelt es sich dabei um eine Beschränkung der Software oder um eine Vorgabe der Softwarenutzer?

Die von Mikropro genutzte Datenbank lässt laut den uns vorliegenden Informationen beliebige SQL-Abfragen zu, unabhängig davon, ob die entsprechenden Nutzer und Nutzerinnen zu solchen Abfragen berechtigt sind.
Halten Sie das für ein Sicherheitsproblem? Wenn nein, warum nicht?

Passwörter der Nutzer und Nutzerinnen werden bei bestimmten Anwendungen im Klartext gespeichert und nicht verschlüsselt, ist das korrekt? Halten Sie das für ein Sicherheitsproblem? Wenn nein, warum nicht?

Die Software Mikropro Health wird demnach mit einem Standardaccount für Administratoren ausgeliefert, der mit immer demselben Standardpasswort gesichert ist. Ist das korrekt? Halten Sie das für ein Sicherheitsproblem?
Wenn nein, warum nicht?

Die Mikroprojekt GmbH beziehungsweise Ihre Support-Mitarbeiter haben Zugriff auf die gesamte Datenbank der Gesundheitsämter, wenn diese zur Fehlersuche an die Mikroprojekt GmbH übermittelt wird – was laut unseren Informationen Praxis ist. Wie stellen Sie sicher, dass diese Daten nicht missbraucht werden?

Ist Ihr Unternehmen für die Verarbeitung solcher Daten durch das BSI zertifiziert? Wenn ja, in welchem Umfang?

Wir erbitten eine schriftliche Stellungnahme bis Donnerstag, 2.11., 11 Uhr.

Beste Grüße
ZEIT ONLINE

2. Anfrage Zeit-Online an den Landesbeauftragten für den Datenschutz und die Informationssicherheit RLP und entsprechender Antwortentwurf

Antwortentwurf
Sehr geehrte..,

vielen Dank für Ihre o.g. Anfrage, die ich folgendermaßen beantworte:

Vorbemerkung:
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) bot dem Ministerium für Wissenschaft und Gesundheit Rheinland-Pfalz (MWG) frühzeitig an, das aus Bundesmitteln getragene Projekt „Einheitliche EDV-Plattform für den ÖGD in Rheinland-Pfalz“ mit Projektlaufzeit vom 4. Quartal 2022 bis 3. Quartal 2024 im Rahmen seiner personellen Ressourcen beratend zu begleiten. Aufgrund dessen informiert das MWG fortlaufend den LfDI über den aktuellen Projektstand. Auf Initiative des LfDI wurde im Projekt eine zusätzliche Arbeitsgruppe zur Umsetzung datenschutzrechtlicher Vorgaben geschaffen, die insbesondere kommunale Datenschutzbeauftragte integrierte. Darüber hinaus fanden in der Vergangenheit einzelne anlassbezogene Gespräche zwischen MWG und LfDI statt, die allerdings kaum die von Ihrer Anfrage umfassten Inhalte betrafen.
Grundsätzlich gilt: Der LfDI begrüßt Vorhaben zur Digitalisierung des Gesundheitswesens, wenn sie mit dem Datenschutzrecht vereinbar sind. Gesundheitsdaten gehören zur Kategorie der besonders sensiblen personenbezogenen Daten und müssen besonders geschützt werden.

Im Zusammenhang mit dem o.g. Projekt besteht die vorrangige Rolle des LfDI darin, das MWG als primär Projektverantwortlichem zu datenschutzrechtlichen Inhalten strategisch zu beraten. Dabei ging es bislang vor allem um allgemeine Fragen zur Prozessarchitektur und der Zuordnung datenschutzrechtlicher Verantwortlichkeiten im Zusammenspiel der verschiedenen Stellen des öffentlichen Gesundheitsdienstes. Selbstverständlich war und ist es dabei das Ziel unserer Behörde, auf die umfassende Einhaltung der Regelungen der Datenschutz-Grundverordnung und insbesondere der geltenden Vorgaben zum lückenlosen Schutz der Gesundheitsdaten bei der Digitalisierung des öffentlichen Gesundheitsdienstes in Rheinland-Pfalz hinzuwirken. Bitte beachten Sie, dass sich die Beratungstätigkeit des LfDI dabei ausschließlich auf die Ausgestaltung und Fortentwicklung des o.g. Projekts bezog. Die datenschutzrechtliche Konformität des regulären, gegenwärtig schon stattfindenden Einsatzes von Softwares zu Verwaltungszwecken in allen insgesamt 24 rheinland-pfälzischen Gesundheitsämtern war ausdrücklich nicht Teil der Beratung und damit auch nicht Gegenstand an den LfDI gerichteter Anfragen. Generell gilt, dass die einzelnen Kreisverwaltungen, bei denen Gesundheitsämter angebunden sind, für die Umsetzung der datenschutzrechtlichen Vorgaben und insbesondere für die Sicherstellung der hierzu erforderlichen technisch-organisatorischen Maßnahmen zur Datensicherheit verantwortlich sind.

Sollten sich aus Ihrer Recherche oder aus anderen Hinweisen Anhaltspunkte für datenschutzrechtliche Defizite bei einem oder mehreren meiner Aufsicht unterliegenden Gesundheitsämtern ergeben, so wird der LfDI dem nachgehen.

Zu Ihren Fragen nehme ich wie folgt Stellung:

1. *Unter anderem ist laut den vorliegenden Informationen das Passwort für die Datenbank-Konfiguration direkt im Code enthalten. Ist das im Sinne des Datenschutzes ein Problem? Wenn nein, warum nicht?*

   Für den Umgang mit Passwörtern verweist der LfDI auf den IT-Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI). Das BSI erarbeitet praxisorientierte Mindeststandards und zielgruppengerechte Handlungsempfehlungen zur IT- und Internet-Sicherheit, um Verantwortliche und Anwender bei der Vermeidung von Risiken zu unterstützen.

   Es gelten die allgemeingültigen Anforderungen des BSI, die Empfehlungen u.a. zur Komplexität und zum Wechseln von Passwörtern machen und die bei der von Ihnen geschilderten Vorgehensweise möglicherweise nicht durchsetzbar wären. Welche Auswirkungen dies im konkreten Szenario auf die Sicherheit und Vertraulichkeit der in einer solchen Datenbank gespeicherten Daten hätte, kann aufgrund der Unkenntnis weiterer Details nicht bewertet werden.

2. *Zudem scheint in Mikropro Health die Rechteverwaltung nicht konsequent umsetzbar zu sein: So können selbst Nutzer, denen alle Berechtigungen entzogen sind, weiterhin einige Informationen sehen – beispielsweise welche Bürgerinnen mit dem sozialpsychiatrischen Dienst zu tun haben.*
   Ist diese Information, dass ein namentlich identifizierbarer Mensch schwere psychosoziale Probleme hat, nach Ihrer Einschätzung besonders schützenswert in dem Sinne, dass andere

Fachbereiche der Gesundheitsämter darauf keinen Zugriff haben sollten?

Bislang verfügt der LfDI über keine Kenntnisse zu den von Ihnen dargestellten Defiziten bei der Rechteverwaltung in der Anwendung Mikropro Health. Bitte beachten Sie, dass jede Kreisverwaltung selbst als datenschutzrechtlich Verantwortlicher die hierzu bestehenden datenschutzrechtlichen Vorgaben umzusetzen hat.

Datenschutzrechtlich unterliegen Angaben über die Gesundheit natürlicher Personen als besondere Kategorien personenbezogener Daten grundsätzlich einem qualifizierten Schutz. Dementsprechend gilt nach Art. 9 Abs. 1 EU Datenschutz-Grundverordnung (DS-GVO) für diese Daten zunächst ein generelles Verarbeitungsverbot, das nur unter den Voraussetzungen des Art. 9 Abs. 2 DS-GVO aufgehoben werden kann. Bereichsspezifische Regelungen wie z.B. das Landesgesetz über den öffentlichen Gesundheitsdienst (ÖGdG) oder das Landesgesetz über Hilfen bei psychischen Erkrankungen (PsychKHG) tragen diesem Schutzbedarf Rechnung. Die o.g. Verantwortlichen haben diese Vorgaben bei der Gewährung von Zugriffsrechten auf Gesundheitsdaten auch innerhalb eines Gesundheitsamtes umzusetzen.

3. *Daten des Sozialpsychiatrischen Dienstes sollen unseren Informationen nach grundsätzlich nicht in eine gesonderte Datenbank ausgelagert und damit einem höheren Schutzniveau unterworfen werden. Ist das Ihrer Meinung nach gerechtfertigt, oder liegt darin – unter Berücksichtigung des unter 2. erwähnten Punktes – ein potenzieller Datenschutzverstoß?*

   Maßgeblich für die Verarbeitung personenbezogener Daten im Sozialpsychiatrischen Dienst eines Gesundheitsamtes sind insbesondere die datenschutzrechtlichen Regelungen im ÖGdG (§ 11) und PsychKHG (§ 32). Nach § 11 Abs. 6 ÖGdG haben die Behörden des öffentlichen Gesundheitsdienstes die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Beachtung der geltenden Datenschutzbestimmungen zu gewährleisten. Die innerbehördliche Organisation ist so zu gestalten, dass Geheimhaltungspflichten, insbesondere die ärztliche Schweigepflicht, gewahrt werden können.

   Den dargestellten Regelungen ist im Ergebnis nicht zu entnehmen, dass Daten des Sozialpsychiatrischen Dienstes einen höheren Schutzbedarf haben als andere ebenfalls in die Kategorie besonderer personenbezogener Daten fallende, noch in einer gesonderten Datenbank auszulagern sind. Die datenschutzrechtlich verfolgten Ziele können auch durch alternative technische und organisatorische Vorkehrungen erreicht werden.

4. *Zudem soll zur Fehlersuche stets die gesamte Datenbank an die Mikroprojekt GmbH übermittelt werden – womit die dortigen Support-Mitarbeiter Zugriff auf die Gesundheitsdaten der Bürgerinnen und Bürger bekommen. Gibt es entsprechende Verträge zur Auftragsdatenverarbeitung und sind diese nach Ihrer Meinung ausreichend? Wurde die Mikroprojekt GmbH für die Verarbeitung solcher Daten durch Ihre Behörde zertifiziert?*

   Der LfDI hat weder Kenntnis vom geschilderten Sachverhalt noch vom Inhalt etwaiger Verträge zwischen einzelnen Gesundheitsämtern und der Mikroprojekt GmbH. Der LfDI geht zunächst davon aus, dass im Falle der Notwendigkeit eines Auftragsverarbeitungsvertrages ein solcher regelmäßig auch vorliegt.

Die Mikroprojekt GmbH wurde nicht durch den LfDI zertifiziert. Ich weise darauf hin, dass eine Zertifizierung nach Maßgabe der DS-GVO keine Voraussetzung für die Rechtmäßigkeit einer Datenverarbeitung ist.

Im Allgemeinen ist eine Übermittlung von Datenbeständen oder ein Fernzugriff auf diese zu Zwecken der Fehlersuche durch einen Dienstleister grundsätzlich denkbar. Voraussetzung hierfür ist neben der Erforderlichkeit der Datenbereitstellung für die o.g. Zwecke die Einhaltung datenschutzrechtlicher Schutzmaßnahmen auf Basis entsprechender vertraglicher Grundlagen.

Laut den uns vorliegenden Informationen wurden die Verantwortlichen ebenso wie Ihr Büro auf die datenschutzrechtlichen Probleme mehrfach hingewiesen. Dazu haben wir folgende Fragen:

5. *Sehen sie in den Softwarelücken und administrativen Entscheidungen Probleme für den Datenschutz?*
   - *Wenn ja, welche?*
   - *Wenn nein, warum nicht?*

   Dem LfDI liegen weder Anhaltspunkte noch konkrete Informationen zu etwaigen „Softwarelücken“ in den in rheinlandpfälzischen Gesundheitsämtern eingesetzten Produkten der Mikropro GmbH vor. Deshalb ist eine konkrete Bewertung leider nicht möglich. Es gelten die bereits dargestellten Anforderungen der DS-GVO und der o.g. bereichsspezifischen Regelungen an die Verarbeitung besonderer Kategorien personenbezogener Daten.

6. *Haben Sie etwaige datenschutzrechtliche Bedenken gegen die in Rheinland-Pfalz geplante Umsetzung der Digitalisierungsstrategie für die Gesundheitsämter geäußert?*
   - *Wenn ja, wann und wem gegenüber?*
   - *Wenn nein, warum nicht?*

   Bislang hatte der LfDI im Rahmen seiner Begleitung des o.g. Projekts keinen Grund, datenschutzrechtliche Bedenken gegen die Digitalisierungsstrategie der Landesregierung zu äußern. Nach dem bisherigen Kenntnisstand und aufgrund des offenen Dialogs mit dem federführenden Ressort bestand zu keinem Zeitpunkt Anlass zur Annahme, dass die Umsetzung der datenschutzrechtlichen Vorgaben in diesem Zusammenhang keine Priorität habe. Im Gegenteil, mit der zu Projektbeginn auf Anregung des LfDI installierten Arbeitsgruppe zum Datenschutz wurde seitens der Projektverantwortlichen ein besonderes Augenmerk auf die effektive Sicherstellung des Datenschutzes auch in einem digitalisierten öffentlichen Gesundheitsdienst in Rheinland-Pfalz gelegt.

   Der LfDI wird auch künftig die weiteren Projektschritte im Rahmen der ihm zur Verfügung stehenden Ressourcen beratend begleiten und zugleich Hinweisen auf Defizite bei der Verarbeitung von Gesundheitsdaten in den seiner Aufsichtszuständigkeit unterliegenden Gesundheitsämtern konsequent nachgehen.

3. Anfrage Zeit-Online an das Ministerium für Wissenschaft und Gesundheit RLP und entsprechender Antwortentwurf

Antwortentwurf:

Sehr geehrte…..,

vielen Dank für Ihre o.g. Anfrage, die ich folgendermaßen beantworte:

Rheinland-Pfalz nimmt im Einvernehmen mit den Gesundheitsämtern, die den Kreisverwaltungen der Landkreise angegliedert sind, an einem vom Bund und der EU geförderten Projekt „Förderung von Maßnahmen zur Steigerung und Weiterentwicklung des digitalen Reifegrades des öffentlichen Gesundheitsdienstes in Deutschland“ teil, welches eine Projektlaufzeit bis zum 30. September 2024 hat.

Wesentliches Ziel dieses Projektes ist es eine einheitliche Software, einheitliche Arbeitsweisen und auch Sicherheitsstandards und Datenschutzregelungen in allen Gesundheitsämtern zu erreichen.

Aus einer Bestandsaufnahme bei den Gesundheitsämtern ergab sich, dass zwar alle die Software der Mikroprojekt GmbH nutzten, aber in verschiedenen Versionen, unterschiedlichen Modulen und unterschiedlichen Ausprägungen. Im Vorfeld des Projektes haben sich die Gesundheitsämter auf eine Vereinheitlichung auf Basis der bestehenden Software ausgesprochen.

Die Durchführung des Projektes erfolgt unter Beteiligung einer externen Beratungsfirma und läuft dabei grundsätzlich in folgenden Phasen ab.

1. Erstellung eines Fach- und Realisierungskonzeptes unter Beteiligung der Gesundheitsämter für die definierten 11 Fachbereiche (Standard RLP).
2. Abnahme der Fach- und Realisierungskonzepte durch die Projektgruppe innerhalb der Projektorganisation.
3. Umsetzung der Fach- und Realisierungskonzepte durch den Softwarehersteller
4. Zurverfügungstellung der jeweils abgenommenen Software und der Standardkonfiguration an die Gesundheitsämter durch die Service- und Leitstelle mittels LDI-Safe. (Die Gesundheitsdaten von Personen verbleiben dabei bei den jeweiligen Gesundheitsämtern.)

Dabei werden auch zu den je jeweiligen Themenbereiche auch die Aspekte des Datenschutzes, z.B. Löschfristen betrachtet und rund 15 % des Projektaufwandes sind für den Bereich von IT-Sicherheitsmaßnahmen und die Erstellung von IT-Sicherheitskonzepten eingeplant.

In der Projektumsetzung wurde von einer externen IT-Beratungsfirma unter anderem eine Bestandsaufnahme von möglichen Sicherheitsrisiken erstellt. Diese werden im Rahmen der Projektdurchführung beachtet und minimiert bzw. abgestellt. Die hierfür erforderliche Zusammenarbeit zwischen den Beteiligten insbesondere Softwarehersteller, Datenschutz- und IT-Sicherheitsbeauftragten ist durch gemeinsame Arbeitsgruppen sichergestellt.

Allen Gesundheitsämtern und dem Softwarehersteller ist darüber hinaus die Möglichkeit eröffnet worden innerhalb des Projektes einen Penetrationstest durchzuführen mit dem Ziel möglichen Schwachstellen und Risiken entgegenzuwirken, um spätestens zum Projektende die IT-Sicherheit und den Datenschutz für alle auf einem optimalen Niveau zu erreichen.

-----Ursprüngliche Nachricht-----
Von: ...@zeit.de>
Gesendet: Dienstag, 31. Oktober 2023 07:57
An: Pressepostfach (MWG) <presse@mwg.rlp.de>; Poststelle (BM und MWG) <poststelle@mwg.rlp.de>
Cc: ….
Betreff: EILT: Stellungnahme zu Sicherheitslücken in Software der Gesundheitsämter in RLP

Sehr geehrte Damen und Herren,

uns liegen Informationen vor, aus denen hervorgeht, dass die Gesundheitsämter in Rheinland-Pfalz Software der Mikroprojekt GmbH nutzen, die einige Sicherheitslücken und potentielle Einfallstore für Unbefugte aufweist.

Unter anderem sind laut den uns vorliegenden Informationen das Login und das Passwort für die Datenbank-Konfiguration direkt im Code enthalten, was dazu führen kann, dass Unbefugte auf Daten zugreifen, neue User anlegen und Rechte vergeben können.

Zudem scheint die Rechteverwaltung nicht konsequent umsetzbar zu sein: So können selbst Nutzer, denen alle Berechtigungen entzogen sind, weiterhin einige Informationen einsehen – beispielsweise welche Bürgerinnen mit dem sozialpsychiatrischen Dienst zu tun haben.

Besonders schützenswerte Daten des Sozialpsychiatrischen Dienstes sollen unseren Informationen nach auch nicht in eine gesonderte Datenbank ausgelagert und damit einem höheren Schutzniveau unterworfen werden.

Laut den uns vorliegenden Informationen wird also von den Gesundheitsämtern in Rheinland-Pfalz eine Software eingesetzt, die sowohl unsicher ist als auch datenschutzrechtlich bedenklich. Schließlich schreibt die DSGVO für Gesundheitsdaten einen besonders hohen Schutzbedarf vor. Sowohl auf die Sicherheitsprobleme als auch auf die datenschutzrechtlichen Probleme wurden Sie als verantwortliche Stelle laut der uns vorliegenden Informationen mehrfach hingewiesen.

Wie wir erfahren haben, soll der Einsatz von Mikropro-Software im Rahmen der Digitalisierungsstrategie des Bundes für die Gesundheitsämter (Pakt für den öffentlichen Gesundheitsdienst) noch ausgebaut werden. Wie begründen Sie das?

Nach unseren Informationen planen Sie auch eine dezentrale Struktur, jedes Gesundheitsamt soll seine Instanz von Mikropro selbst hosten und verwalten. Warum haben Sie sich gegen eine zentrale und damit leichter administrierbare und besser sicherbare Verwaltung von Mikropro entschieden?

Für unseren aktuellen Artikel für Zeit Online erbitten wir zu diesen Punkten eine schriftliche Stellungnahme bis zum 2.11., 11 Uhr.

Darüber hinaus haben wir dazu die folgenden Fragen:

Haben Sie andere – beispielsweise cloudbasierte – Softwarelösungen für die Gesundheitsämter erwogen?

Wenn ja, mit welchen Argumenten haben Sie sich für die bestehende entschieden?

Wenn nein, warum nicht?

Wann sind Ihnen die Probleme zur IT-Sicherheit in Mikropro Health und seinen Modulen bekannt geworden?

Welche Maßnahmen haben Sie geplant, um diesen Problemen zu begegnen?

Wenn Sie keine geplant haben, warum nicht? Welche Gründe sprechen dagegen?

Wir benötigen Ihre Antwort bis Donnerstag, 11 Uhr, damit wir sie in unserem Artikel berücksichtigen können.

Vielen Dank und beste Grüße
ZEIT ONLINE

Kosten gemäß § 24 LTranspG werden nicht erhoben.

Sie haben die Möglichkeit, den Landesbeauftragten für die Informationsfreiheit anzurufen (§ 12 Abs. 4 Satz 6 LTranspG).

Sollte diese Antwort veröffentlicht werden, möchte ich Sie mit Hinweis auf die Datenschutz-Grundverordnung darum bitten, personenbezogene Daten unkenntlich zu machen.

Rechtsbehelfsbelehrung

Gegen diese Entscheidung kann innerhalb eines Monats nach Bekanntgabe Widerspruch beim Ministerium für Wissenschaft und Gesundheit, Mittlere Bleiche 61, 55116

Mainz schriftlich, in elektronischer Form nach § 3 a Abs. 2 des Verwaltungsverfahrensgesetzes oder zur Niederschrift erhoben werden.

Mit freundlichen Grüßen
Im Auftrag

[redacted]