



Kleine Anfrage

des Abgeordneten Dr. Bernd Buchholz (FDP)

und Antwort

der Landesregierung – Der Minister und Chef der Staatskanzlei

Datenschutz im Rahmen der Umstellung auf Open Source

1. Wurden bereits Datenschutzverletzungen im Rahmen der Umstellung der Landesverwaltung auf „Open Source“ gemeldet? Wenn ja, wie viele, durch wen, wann konkret und welche Art von Verstoß wurde gemeldet?

Antwort:

In Drucksache 20/5107 wurde über einen Vorfall am 06.08. berichtet. Auf die dortigen Ausführungen wird verwiesen.

Am 17.9. wurde durch das MLLEV ein Vorfall gemeldet, der das mögliche Auslesen von Passwörtern betrifft, wenn den Vorgaben des Sperrens des Arbeitsplatz-PCs beim Verlassen des Platzes nicht regelhaft nachkommen wird. Sollte dies arbeitsplatzbezogen auf Grundlage einer individuelle Risikoabschätzung als relevante Gefährdung eingeschätzt werden, kann zusätzlich ein Masterpasswort vergeben werden.

Am 25.9. wurde ein Vorfall durch das LVermGeo gemeldet, der eine durch Nutzer falsch gesetzte Funktionspostfachberechtigung betrifft. Hierzu wurde inzwischen eine zusätzliche Kontrollfunktion eingerichtet, die sicherstellt, dass die im bestehenden Verzeichnisdienst vergebenen Berechtigungen regelmäßig überprüft werden. Dies war bislang kein Standard ist nun aber Dank des neuen E-Mail Systems möglich.

2. Wie viele E-Mails wurden bislang fehlerzugestellt und in welcher Weise werden diese durch die Landesregierung erfasst?

Antwort:

Wenn unter Fehlerzustellung ein Versand an einen falschen Empfänger verstanden wird, der nicht auf einen menschlichen Fehler beim Eintippen der E-Mail-Adresse o.ä. zurückzuführen ist, dann sind keine solchen Ereignisse bekannt. Für die am 06.08. aufgetretene Fehlerzuordnung von E-Mails wird zur Beantwortung dieser Frage auf Drucksache 20/5107 sowie auf den beigefügten Abschlussbericht von Dataport zum Sicherheitsvorfall verwiesen. Auch hier kann ausweislich des Berichts von keiner Fehlerzustellung im o.g. Sinne gesprochen werden.

3. Wer wurde bei Fehlerzustellungen von E-Mails jeweils durch wen benachrichtigt und innerhalb welchen Zeitraums erfolgte die Benachrichtigung?

Antwort:

Siehe Antwort zu 2.

4. Ergreift die Landesregierung initiativ Maßnahmen, um das konkrete Ausmaß der Fehlerzustellungen zu ermitteln? Wenn ja, welche? Wenn nein, warum nicht?

Antwort:

Siehe Antwort zu 2.

5. Welche konkreten Konsequenzen hat die Fehlerzustellung vertraulicher Inhalte? Bitte erläutern.

Antwort:

Siehe Antwort zu 2.

6. Sind der Landesregierung Fälle bekannt, in denen Inhalte verloren gingen? Wenn ja, wie viele und welche Maßnahmen ergreift die Landesregierung, um diese wiederherzustellen? Bitte aufschlüsseln nach der betroffenen Behörde und dem Zeitpunkt.

Antwort:

Nein. In den Fällen, in denen vermeintliche E-Mail-Verluste mitgeteilt wurden, konnten diese Mails sichtbar gemacht werden. So wurde bspw. in einem Fall ein Filter in der Ansicht des Posteingangs gesetzt, in anderen Fällen wurde die E-Mail bereits in einem anderen Ordner abgelegt.

1 Ausgangslage

Dataport stellt im Auftrag der Landesverwaltung Schleswig-Holstein die Behörden von der Bürokommunikationssoftware MS Exchange auf Open-Xchange um. Die vorhandenen Daten der Postfächer werden dabei im Rahmen einer Migration übernommen.

Die Migration der Landesverwaltung SH ist die erste dieser Art, die bei Dataport beauftragt wurde.

Diese Umstellung/Migration erfolgt behördenweise und in Chargen von je 200 Postfächern.

Die Migration der Postfächer wird Ende September 2025 abgeschlossen sein. Bisher hat Dataport ca. 11.000 Postfächer umgestellt.

Die Umstellung erfolgt in zwei Phasen:

- Erstmigration der Daten der letzten sieben Tage (ohne Zugriff auf die Postfächer)
- Nachmigration aller Daten älter als sieben Tage (mit Zugriff auf die Postfächer).

Jeweils nach erfolgter Migration werden die Behörden informiert. Auf einer „Fortschrittsseite“ kann der Fortgang der Migration verfolgt werden.

Eine Skizze des Migrationsprozesses ist der Anlage 1 zu entnehmen.

Alle technischen Migrationsschritte werden automatisiert in Log-Dateien protokolliert, so dass das Geschehen von den Berechtigten nachvollzogen und ggf. ausgewertet werden kann.

Das eingesetzte Personal ist im Umgang mit dem Vorgehen und den Systemen geschult und hat die erforderliche IT-Qualifikation. Microsoft-zertifizierte Mitarbeitende oder Mitarbeitende der Hersteller Univention und Open-Xchange werden bei Bedarf hinzugezogen.

2 Sachverhalt

Am 6.8. 2025, 17.45 Uhr wurden Nachmigrationen über Nacht für folgende Behörden angestoßen:

- Finanzamt Lübeck
- Finanzamt Plön
- Ministerium für Inneres

Am 7.8. um 7.05 Uhr wurde festgestellt, dass die Postfächer einer migrierten Behörde E-Mails aus einer anderen migrierten Behörde enthielten. Im Rahmen einer Nachmigration wurde „Konto A“ aus MS Exchange nicht in „Konto A“ von Open-Xchange migriert, sondern in „Konto B“. Von diesem Fehler waren 790 Konten betroffen.

3 Sofort-Maßnahmen nach Bekanntwerden des Problems

- Die Postfächer in den betroffenen Behörden wurden sofort gesperrt.
- Das ZIT und das AIT wurden umgehend informiert.
- Es wurde ein Sicherheitsvorfall gemeldet.
- Die bereits angestoßene Migration des Finanzamtes Stormarn wurde abgebrochen.
- Weitere geplante Migrationen wurden ausgesetzt.
- Der Hersteller Open-Xchange wurde eingebunden.

4 Fehleranalyse

Die Migration erfolgt durch Kopie des Kontos aus Exchange in ein .tmp-Konto und von dort in das Konto unter Open-Xchange. Bezugsdaten sind dabei die Mailadresse und die eindeutige ID des AD (Activ Directories).

Die Kopier- und Migrationsvorgänge erfolgen in mehreren Chargen. Diese Chargen werden parallel abgearbeitet.

Grundlage für die Migration sind sogenannte Chargen-Listen. Das ist eine Tabelle, in denen der Account-Name des .tmp-Kontos der eindeutigen AD-ID zugeordnet wird, um mit dieser ID den Account in das Open-Xchange-Konto zu übertragen.

Das .tmp Konto wird erzeugt um die downtime (Ausfallzeit) für die Anwendenden so gering wie möglich zu halten. Hierzu wird ein „virtueller Mailuser“ .tmp erstellt um das Routing von der heutigen Microsoft Umgebung auf die neu OX zu realisieren.

Bei der Nachmigration werden diese einzelnen Chargenlisten aus der Erstmigration in einer Tabelle zusammengefasst, damit diese in der Nacht ohne händisches Anstarten einzelner Jobs automatisch durchlaufen kann.

Beim Zusammenkopieren dieser einzelnen Chargenlisten ist es zu einem Sortierfehler gekommen. Die Sortierung der Spalte „Accountname“ erfolgte ohne die Funktion „auch die Bezugsspalten sortieren/Markierung erweitern“, so dass die eindeutige AD-ID nicht mit der passenden Mailadresse sortiert wurde. So wurden Mailadressen beim Übertragen in das Open-Xchange-Konto falschen AD-IDs zugeordnet.

Dieser Fehler ist auf menschliches Versagen zurückzuführen. Es besteht die begründete Vermutung, dass die mit dieser Aufgabe betraute Person wegen der Vielzahl der anstehenden Aufgaben und zeitlichen Gegebenheiten überfordert war.

Das zur Absicherung und Qualitätssicherung vorgesehene Vier-Augen-Prinzip wurde hier offensichtlich nicht durchgeführt.

Es liegen keine Erkenntnisse vor, die ein vorsätzliches Handeln vermuten lassen.

Eine Veränderung der erprobten Migrationsskripte hat nicht stattgefunden!

Der ausführende Dienstleister hat dazu folgende Aussage getroffen:

„Sollte sich nachweislich herausstellen, dass der Fehler durch einen unserer Mitarbeitenden verursacht wurde, möchten wir betonen, dass kein vorsätzliches Fehlverhalten vorliegt. Sollte ein menschlicher Fehler ursächlich sein, so ist es denkbar, dass dieser auf die hohe Arbeitsbelastung, unter anderem durch projektbedingte Überstunden und regelmäßig über zehnstündige Arbeitstage zurückzuführen ist. In solchen Konstellationen können erfahrungsgemäß

Konzentrationsschwächen auftreten, was möglicherweise zu einem Flüchtigkeitsfehler geführt haben könnte.

Unsere eingesetzten Mitarbeitenden sind sicherheitsüberprüft und verfügen über umfangreiche Erfahrung in der Administration von Open-Source-Infrastrukturen. Sie arbeiten stets nach bestem Wissen und Gewissen sowie mit hoher Sorgfalt.“

5 Maßnahmen zur Behebung der falschen Kontenzuordnungen

Ein Datenverlust für die aktiven Konten liegt nicht vor.

Für die drei betroffenen Behörden wurden folgende Maßnahmen eingeleitet:

- Reaktivierung des MS Exchange Postfachs
- Überführung der seit Migrationsbeginn eingegangenen E-Mails im Postfach von Open-Xchange in das MS Exchange Postfach
- Überführung der aufgelaufenen E-Mails in das MS Exchange Postfach seit der Deaktivierung nach Überführung der Konten.

Damit sind die drei Behörden seit dem 8.8.2025 ca. 14.15 Uhr ohne Datenverlust wieder arbeitsfähig. Die während der Maßnahme zwischengespeicherten E-Mails wurden nach und nach abgearbeitet und stehen seit dem 8.8.2025 ca. 17.30 Uhr wieder zur Verfügung.

Das Finanzamt Stormarn ist seit dem 8.8. wieder auf das Ausgangssystem MS Exchange zurückgesetzt.

6 Maßnahmen zur zukünftigen Fehlervermeidung

Nach einer eingehenden Analyse der Fehlerquelle sind die organisatorischen und technischen Maßnahmen zur zukünftigen Fehlervermeidung gehärtet worden.

Es wurde ein Makro entwickelt, welches die Zuordnungen Mailadresse und AD-ID aus der Chargenliste der Erstmigration mit der Mailadresse und AD-ID aus der Chargenliste für die Nachmigration vergleicht und Abweichungen farblich darstellt (Integrations-Check in die relevanten Zuordnungstabellen per Makro).

Darüber hinaus wurden folgende Maßnahmen ergriffen:

- Erstellung der Chargenlisten nur für eine Behörde. Keine Zusammenfassung mehrerer Behörden in einer Liste, so dass es keine Zuweisung von Mails an fremde Behörden geben kann.
- Strikte Einhaltung des Vier-Augenprinzips in der Erstellung der Zuordnungstabellen
- Zusätzliche Qualitätssicherung der Zuordnungstabelle durch zwei Mitarbeitende.

Generell erfolgen bei weiteren Verbesserungen am Prozess intensive Tests in der QS-Umgebung.

7 Weiteres Vorgehen

Bis zur Freigabe durch das ZIT erfolgten keine weiteren Migrationen. Die Migrationen der drei Behörden und der ausstehenden Behörden werden neu geplant. Ziel ist die Einhaltung des 30.9.2025 als Migrationsende.

Weitere Fragen des AIT und des Landespolizeiamtes zur Migration werden in der Anlage 2 beantwortet.