Schleswig-Holsteinischer Landtag
Umdruck 16/2644

ULD · Postfach 71 16 · 24171 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200
Aktenzeichen:
LD5 –

Innen- u. Rechtsausschuss
des Schleswig-Holsteinischen Landtags
Vorsitzender Herr MdL Werner Kalinka
Postfach 7121
24171 Kiel

Kiel, 28. November 2007

Sicherheitslücken beim Datenschutz im internen Netz von Dataport mit Auswirkungen auf personenbezogene Daten schleswig-holsteinischer Behörden
Sitzung des Innen- und Rechtsausschusses am 28. November 2007, TOP 1,
Ihre Einladung vom 21.11.2007, L 215
Schreiben der FDP-Landtagsfraktion vom 16.11.2007, LT-Umdruck 16/2603

Sehr geehrter Herr Kalinka,
sehr geehrte Damen und Herren Abgeordnete,

mit dem in der Bezugszeile genannten Schreiben beantragte die FDP zum im Betreff genannten Thema eine Behandlung im Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtags, wozu Sie mich freundlicherweise einladen. Ergänzend zu meinen mündlichen Darlegungen sende ich Ihnen in der Anlage eine Darstellung der Sicherheitsprobleme im Netz von Dataport aus Sicht des ULD mit der Bitte um Kenntnisnahme.

Für Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

gez.
Dr. Thilo Weichert

Anlage: - 1 -

Sicherheitsprobleme im Behördennetz der FHH

Auswirkungen auf Schleswig-Holstein

Sachstandsdarstellung des
Unabhängigen Landeszentrums für Datenschutz
Schleswig-Holstein

Zusammenfassung

Der Hamburgische Datenbeauftragte hat im Rahmen einer Prüfung des von den Behörden in Hamburg genutzten Netzwerk (kurz: FHH-Net) eine Reihe von gravierenden Schwachstellen festgestellt, die es einem internen Angreifer mit Zugang zum FHH-Net ermöglichen können, unbefugt auf personenbezogene Daten von schleswig-holsteinischen Kunden bei Dataport zuzugreifen. Bei den festgestellten Schwachstellen handelt es sich um Sicherheitsvorfälle.

Ursache ist zum einen eine mangelhafte Durch- und Umsetzung datenschutzrechtlicher Vorgaben im Bereich der Administration bei Dataport. Zum anderen beruhen die festgestellten Mängel – soweit sie Dataport und Schleswig-Holstein betreffen – auf dem Umstand, dass das interne Datennetz von Dataport auf dem FHH-Net aufsetzt und von diesem sicherheitstechnisch nicht ausreichend separiert ist. Auf diese Weise „erbt“ das interne Datennetz von Dataport konzeptionelle Schwächen des FHH-Net.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat die Ergebnisse und Bewertungen des Prüfberichts nachvollzogen und durch eigene Untersuchungen vor Ort ergänzt. Zusätzlich werden vom Datenschutz- und Sicherheitsmanagement von Dataport weitere Untersuchungen in Abstimmung mit dem ULD durchgeführt.

Das ULD teilt die Einschätzung des Hamburgischen Kollegen über die offensichtlichen Fehler bei der Administration sowie den konzeptionellen Schwachstellen des internen Hausnetzes von Dataport. Die datenschutzrechtliche und sicherheitstechnische Bewertung des FHH-Net liegt in der Zuständigkeit des Hamburgischen Datenschutzbeauftragten.

Das ULD konzentriert sich derzeit auf die Kontrolle und Bewertung der vom Sicherheitsmanagement Dataport nach Kenntnis des Prüfberichts veranlassten Sofortmaßnahmen. Darüber hinaus hat das ULD seine Beratung angeboten, mit welchen Maßnahmen die festgestellten Schwachstellen zur Vermeidung von weiteren Sicherheitsvorfällen behoben werden können.

Auswirkungen auf Schleswig-Holstein?

Nicht stattgefunden hat ein direkter Zugriff aus dem FHH-Net auf schleswig-holsteinische Fachverfahren und die dort verarbeiteten personenbezogenen Daten. Ein solcher Zugriff hätte über das Landesnetz Schleswig-Holstein erfolgen müssen, welches jedoch im Unterschied zum FHH-Net deutlich strikter aufgeteilt und damit deutlich stärker kontrolliert ist.

Durch die strikte Aufteilung des Landesnetzes Schleswig-Holstein werden die Auswirkungen eines Sicherheitsvorfalles deutlich begrenzt. Die Kontrollmechanismen des Landesnetzes stellen sicher, dass nur solche Verbindungen möglich sind, die von den jeweiligen Kommunikationspartnern beantragt und genehmigt sind. Zudem können die an das Landesnetz angeschlossenen Teilnehmer die sie betreffenden Einstellungen jederzeit und eigenständig kontrollieren.

Aus dem FHH-Net konnte jedoch auf die Bürokommunikations-Umgebung bei Dataport

zugegriffen werden. Aufgrund einer zu offenen Berechtigungsvergabe war ein Zugriff auf die dataport-interne Dateiablage möglich. Auf der internen Dateiablage waren sicherheitskritische Dokumente und personenbezogene Daten in großer Menge einsehbar. Sicherheitsmaßnahmen wie bspw. eine Verschlüsselung von Dateiablagen oder eine minimalisierte Vergabe von Rechten für den Zugriff auf diese Ablagen waren nicht getroffen worden.

Der Hamburgische Datenschutzbeauftragte hat insbesondere festgestellt, dass Zugriffe auf Datenbank-Abzüge des Fachverfahren Permis sowie Berichte aus INPOL-SH möglich waren. Zusätzlich konnte auf Geoinformationsdaten sowie Schriftwechsel mit schleswig-holsteinischen Behörden zugegriffen werden.

Welche Schritte hat das ULD bisher ergriffen?

Das ULD überprüft derzeit die von Dataport getroffenen Sofortmaßnahmen. Ergänzende Prüfungen sind vorgesehen insbesondere zur Vergabe administrativer Berechtigungen sind vorgesehen.

Das ULD hat darüber hinaus bei Dataport eine vollständige Dokumentation der Zugriffsmöglichkeiten aus dem FHH-Net in das Landesnetz Schleswig-Holstein angefordert.

Das ULD prüft derzeit zusätzlich, ob aus dem FHH-Net über eine Manipulation der administrativen Arbeitsplätze bei Dataport ein administrativer Zugriff auf Fachverfahren der schleswig-holsteinischen Verwaltung überhaupt möglich ist.

Das ULD hat bei seinen stichprobenartigen Kontrollen nicht hinreichend geschützte Sicherheitskonzepte, Kundenkommunikationen, Designdokumente und personenbezogene Daten in der internen Ablage von Dataport gefunden. Das Sicherheitsmanagement bei Dataport ist vom ULD aufgefordert worden, diese Daten aus der Ablage zu löschen bzw. soweit eine Speicherung erforderlich ist durch zusätzliche Sicherheitsmaßnahmen zu schützen bzw..

Das ULD hat von Dataport eine vollständige Dokumentation der aktuell vergebenen Zugriffsberechtigungen und genutzten Ablageziele angefordert. Diese Dokumentation wird von Dataport derzeit mit Unterstützung eines externen Dienstleisters automatisiert erstellt.

Auf Basis dieser sehr umfangreichen Dokumentation wird das ULD prüfen, ob auch auf andere, aus schleswig-holsteinischen Verfahren abgeleitete Daten bei Dataport unbefugt zugegriffen werden kann.

Konkreter Handlungsbedarf

Aus Sicherheitsgründen ist es nach dem Stand der Technik unumgänglich, dass das interne Datennetz des Dienstleisters Dataport aus dem FHH-Net herausgelöst wird. Das ULD wird den Prozess der Trennung des Dataport internen Netzes aus dem FHH-Net beratend begleiten.

Dataport muss seine interne Dateiablage stärker absichern. Für Daten mit hohem Schutzbedarf ist zusätzlich eine Verschlüsselung einzuführen, um diese dem systembedingten Zugriff von Administratoren bei Dataport zu entziehen. Für alle Datenablagen sind die vergebenen Zugriffsrechte zu überarbeiten und auf die zwingend notwendigen Zugriffsmöglichkeiten zu beschränken.