

# Im Visier der Datendiebe

Straftaten im Internet: CDU-Bundestagesabgeordnete betroffen – Sogar Landesdatenschützerin hat's erwischt

VON GERRIT SPONHOLZ

**KREIS SEGEBERG.** Die CDU-Bundestagsabgeordnete Melanie Bernstein hat es schon erwischt, und selbst die oberste Datenschützerin des Landes Marit Hansen traf es: Sie wurden Opfer von Datenklau und Hackern. Auch aus dem Online-Portal der Kreisverwaltung Schleswig-Flensburg für die Anmeldung zu Hygienebelehrungen waren 837 personenbezogene Daten gestohlen worden, wie das „Flensburger Tageblatt“ schrieb.

Beim Kreis Segeberg und den 95 Städten und Kommunen war ein Hacker bislang nicht erfolgreich, berichten Sprecher auf SZ-Anfrage. Erwischt hat es allerdings, wenn auch in kleinerem Ausmaß, die CDU-Bundestagsabgeordnete Melanie Bernstein aus Wahlstedt. Sie berichtet, das Bundeskriminalamt habe ihr mitgeteilt, ihre Handynummer sei veröffentlicht worden. Sie nimmt es gelassen. „Aber diese hatte ich ja ohnehin schon publik gemacht, etwa in Flyern.“

## Mitarbeiter der Kreisverwaltung geschult

Der Hintergrund: Anfang des Jahres war bekannt geworden, dass ein Hacker Handynummern, Privatadressen, interne Nachrichten und Fotos von Prominenten und Politikern veröffentlicht hat. „Der Vorgang zeigt zweierlei“, warnt Bernstein. „Die Zersplitterung der behördlichen Aufgaben in der



Anfang des Jahres war bekannt geworden, dass ein Hacker Handynummern, Privatadressen, interne Nachrichten und Fotos von Prominenten und Politikern veröffentlicht hat. FOTO: OLIVER BERG

Cyber-Abwehr ist wenig effektiv. Wir müssen diesen Bereich deutlich verstärken: personell, technisch, aber vor allem organisatorisch.“ Als Vorbild nennt sie das „Gemeinsame Terrorismusabwehrzentrum“ in Berlin. Dort kooperieren die zuständigen Ämter und Dienste. „Zum anderen müssen wir selbst aber noch stärker darauf achten, welche Daten wir veröffentlichen, etwa in sozialen Medien, oder welche Passwörter wir verwenden.“

„Die Kreisverwaltung Segeberg ist durch das Landesnetz gegen einen Zugriff von außen etwa über eine Firewall abgeschirmt“, versichert Kreissprecherin Sylvia Janowski. „Beim Landesnetz handelt es sich um ein besonders geschütztes behördeninternes Netz, das im Auftrag des Landes durch den zentralen IT-Dienstleister Dataport betrieben wird.“

Sämtlicher ein- und ausgehender Datenverkehr fließt über dieses Netz. „Potenzial-

le Angriffe werden bei Dataport überwacht, protokolliert und abgewehrt.“ Außerdem seien alle PC-Arbeitsplätze und IT-Komponenten mit aktueller Virensoftware und aktuellen Betriebssystem ausgestattet. „Eine zentrale Monitoring-Software überwacht den jeweiligen Status der Geräte und warnt bei eventuellen Risiken.“ Für die kreiseigenen Rechenzentren gebe es einen besonderen Zugangsschutz nur für berechtigte Personen.

Mitarbeiter würden zur Datensicherheit sensibilisiert und geschult. „Und seit Mai 2018 hat der Kreis Segeberg einen IT-Sicherheitsbeauftragten und es gibt regelmäßige Sicherheitstests durch externe Dienstleister wie vor wenigen Tagen.“ Der Kreis will außerdem den IT-Bereich nach Regeln des Bundesamtes für Sicherheit in der Informationstechnik zertifizieren lassen. „Ein entsprechender Beschluss ist im Dezember 2018 durch die politischen Gremien des Kreises erfolgt.“

Marit Hansen, Landesbeauftragte für Datenschutz in Schleswig-Holstein, hat zwar noch keine offiziellen Beschwerden oder Hinweise aus dem Kreis Segeberg zu

Datenklau erhalten. Sie hält es aber „für ziemlich wahrscheinlich, dass Menschen aus dem Kreis Segeberg von einem der großen Datenschutzvorfälle der vergangenen Jahre betroffen waren“.

## ➔ Für die kreiseigenen Rechenzentren gibt es einen besonderen Zugangsschutz.

Angriffe durch Programme, die Server im Internet auf Sicherheitslücken abklopfen, „sind an der Tagesordnung“. Die Datenbank des Kreises bei Dataport hält Hansen für vermutlich gut gesichert. „Eine Garantie für hundertprozentige Sicherheit gibt es aber nicht.“

Sie selbst sei mal ausgespäht worden. „2013 war eine Email-Adresse betroffen, die anscheinend bei einem Anbieter durch einen Hackerangriff ausgespäht wurde.“

☀ Wer selbst testen möchte, ob die eigene Email-Adresse gehackt wurde, kann dies im Internet beim **Hasso-Plattner-Institut** prüfen unter der Adresse: <https://sec.hpi.de/ilc/search>.

## Sechs Tipps für den Datenschutz

- **Datensparsamkeit:** Wer freizügig mit seinen Daten umgeht, muss damit rechnen, dass sie im Netz an unerwünschter Stelle auftauchen. Deshalb: Daten, die gar nicht erst an- oder herausgegeben worden sind, können auch nicht gestohlen werden.
- **Datenkontrolle:** Um Missbrauch schnell eindämmen zu können, ist ständige Kontrolle und ein Überblick wichtig: Dazu gehört das regelmäßige Prüfen der Kontoauszüge ebenso wie die Recherche im Internet, welche Informationen über die eigene Person auffindbar sind.
- **Gute Passwörter:** Ein starkes Passwort hat zwölf oder mehr Stellen. Es besteht aus

Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

- **Passwortsicherheit:** Jedes Online-Konto braucht ein eigenes sicheres Passwort.
- **Zweifaktor-Authentifizierung:** Ein sicheres Passwort ist gut, ein zweiter Sicherheitscode ist besser. Genau das macht die Zweifaktor-Authentifizierung. So wird nach Eingabe des Passworts noch ein zweiter Code abgefragt.
- **Onlinespeicher:** Cloud-Dienste sind praktisch, bergen aber ein Datendiebstahl-Risiko. Vor allem sensible Daten sollten Nutzer deshalb nicht unverlüsselt in einem Onlinespeicher ablegen.


77 Eine Garantie für hundertprozentige Sicherheit gibt es aber nicht.

Marit Hansen, Landes-Datenschützerin