Positionspapier des Bundesfachausschusses für Sicherheit

FREIE WÄHLER fordern Konsequenzen aus Berliner Hackerangriff: Deutschland braucht einen nationalen Schutzschirm für seine digitale Infrastruktur

Nach dem schweren Cyberangriff auf das Berliner Landesnetz und der inzwischen erfolgten Veröffentlichung der erbeuteten Daten im Darknet fordern die FREIE WÄHLER einen umfassenden Maßnahmenplan zum Schutz staatlicher IT-Infrastruktur.

Zur Stärkung der digitalen Resilienz setzen die FREIE WÄHLER auf einen 10-Punkte-Plan:

1. Kritische Behördennetze regelmäßig unabhängig testen

Bund, Länder und Kommunen müssen besonders schützenswerte IT-Systeme verpflichtend und regelmäßig durch unabhängige Experten auf Schwachstellen testen lassen. Dabei darf es nicht bei einer Prüfung von Konzepten und Dokumenten bleiben. Entscheidend ist, ob Systeme einem realistischen Angriff tatsächlich standhalten.

2. Verpflichtende Mehrfaktor-Authentifizierung

Für alle besonders sensiblen Verwaltungs- und Behördenzugänge muss eine starke Mehrfaktor-Authentifizierung verpflichtend sein. Ein gestohlenes Passwort darf nicht ausreichen, um sich Zugang zu staatlichen Systemen zu verschaffen.

3. Behördennetze konsequent segmentieren

Ein erfolgreicher Angriff auf einen Teil eines Behördennetzes darf nicht dazu führen, dass sich Angreifer anschließend innerhalb der gesamten Infrastruktur bewegen können. Deshalb müssen sensible Systeme technisch stärker voneinander getrennt und Zugriffsrechte nach dem Prinzip „so wenig wie möglich, so viel wie nötig“ vergeben werden.

4. Sicherheitslücken schneller schließen

Für kritische Sicherheitslücken in Behörden-IT müssen verbindliche Fristen zur Behebung gelten. Wir brauchen ein konsequentes Schwachstellenmanagement mit klaren Verantwortlichkeiten und nachvollziehbaren Eskalationsstufen.

5. Backups müssen im Ernstfall funktionieren

Jede kritische Behörde braucht regelmäßig getestete, vom produktiven Netzwerk getrennte und gegen Manipulation geschützte Backups. Ein Backup, das im Ernstfall nicht wiederhergestellt werden kann, ist kein ausreichendes Sicherheitskonzept.

6. Bund und Länder müssen Cyberabwehr enger verzahnen

Beim Berliner Angriff arbeiten unter anderem BSI, BKA, Bundesamt für Verfassungsschutz, Berliner Sicherheitsbehörden und weitere Stellen zusammen. Die Erkenntnisse werden im Gemeinsamen Cyberabwehrzentrum zusammengeführt. Diese Zusammenarbeit muss dauerhaft verbessert und institutionell gestärkt werden.

Wir brauchen einen echten nationalen Cyberlageverbund statt Zuständigkeitsdenken zwischen Bund, Ländern und Kommunen.

7. Kommunen dürfen bei der Cybersicherheit nicht allein gelassen werden

Gerade kleinere Kommunen verfügen häufig nicht über die personellen und finanziellen Ressourcen großer Behörden. Der Bund muss deshalb ein dauerhaftes Förderprogramm für kommunale Cybersicherheit schaffen – einschließlich Beratung, Notfallplanung, Schulungen und technischer Unterstützung.

8. Cyber-Notfallübungen verbindlich machen

Behörden müssen regelmäßig einen kompletten Cyberangriff simulieren.

Dabei muss praktisch getestet werden:

- Wie schnell wird ein Angriff erkannt?
- Wer übernimmt die Führung?
- Welche Systeme werden vom Netz getrennt?
- Wie werden Bürger informiert?
- Wie funktioniert die Wiederherstellung?
- Wie wird mit einem möglichen Datenabfluss umgegangen?

Ein Notfallplan, den niemand praktisch geübt hat, ist kein belastbarer Notfallplan.

9. Betroffene Bürger müssen schnell und konkret informiert werden

Wenn personenbezogene Daten abgeflossen sind, müssen Betroffene schnellstmöglich und verständlich darüber informiert werden, welche Daten konkret betroffen sein könnten und welche Schutzmaßnahmen sie ergreifen sollten. Die Bürger dürfen nicht darauf angewiesen sein, selbst im Internet nach Informationen über den möglichen Missbrauch ihrer Daten zu suchen.

10. Verantwortung und Aufarbeitung

Nach Abschluss der forensischen Untersuchungen muss transparent aufgearbeitet werden, wie der Angriff möglich war.