14.03.2026 11:22:18 BfB Schenefeld <info@bfb-schenefeld.de>:

Sehr geehrte Frau Bürgermeisterin,

sehr geehrte Damen und Herren,

bezugnehmend auf die Vorlage VO/100/799/26 für den Hauptausschuss am 17.03.2026, Tagesordnungspunkt 10, erlauben wir uns Ihnen hiermit die im Anhang befindliche Information zu übermitteln.

Ziel dabei ist, uns alle in die Lage zu versetzen, politische Beschlüsse in Ausschüssen basierend auf Fakten zu treffen und alle auf einen gemeinsamen objektiven Kenntnisstand zu bringen.

Wir hoffen mit dem übermittelten Dokument eine konstruktive Meinungsbildung im Sinne der Transparenz zu fördern.

Mit besten Grüßen,

Eure BfB Schenefeld

OParl-Abschaltung: Warum das Sicherheitsargument nicht trägt (zur Vorlage: VO/100/799/26)

(Hinweis: Jegliche Fachbegriffe werden im Anhang erläutert!)

1. Was am 12. Januar passiert ist

Betrugs-E-Mails wurden im Namen der Bürgermeisterin Christiane Küchenhof an Ratsmitglieder versandt. Absender war eine Hotmail-Adresse. Inhalt: klassisches Social Engineering (CEO-Fraud). Der Büroleitende Beamte Melf Kayser hat die Betroffenen gewarnt.

Die Verwaltung hat daraufhin die OParl-Schnittstelle ad-hoc ohne belegbaren und konkreten Nachweis für die Ursächlichkeit abgeschaltet und beantragt nun im Hauptausschuss am 16.03. die formelle Aufhebung des OParl-Beschlusses von 2025. Die Begründung: Der Datenmissbrauch sei „mit hoher Wahrscheinlichkeit durch die Maschinenlesbarkeit der Allris-Daten und somit mithilfe der OParl-Schnittstelle ermöglicht“ worden.

2. Was OParl tatsächlich liefert

Eine Analyse der über OParl abrufbaren Daten ergibt:

- 221 Personen im ALLRIS-Datenbestand
- Davon 57 mit E-Mail-Adresse, 56 mit Telefonnummer
- Die E-Mails sind überwiegend private Adressen der Ratsmitglieder (gmx.de, outlook.de, gmail.com, Partei-Adressen)
- Verwaltungsmitarbeiter (Kayser, Arwers, Bothing, Esmann u.a.) erscheinen im ALLRIS, aber fast alle ohne Kontaktdaten

Entscheidend: Exakt dieselben 221 Personen mit denselben Kontaktdaten sind über das öffentliche ALLRIS-Webinterface (sitzungsdienst-schenefeld.de) abrufbar. OParl liefert keine zusätzlichen Daten. OParl ist lediglich ein anderes Ausgabeformat (JSON statt HTML) für identische Inhalte.

3. Zwei getrennte Datenquellen

Die Verwaltungsvorlage VO/100/799/26 unterscheidet nicht zwischen zwei unterschiedlichen Datenbeständen:

	Webseite der Stadt	ALLRIS / OParl
Inhalt	89 Verwaltungsmitarbeiter	221 Personen (Politiker, Gremien, Presse)
E-Mails	@stadt-schenefeld.de (dienstlich)	Überwiegend private Adressen (gmx, outlook, gmail)
Telefon	Dienstliche Durchwahlen	Private Nummern / Mobilnummern
Quelle	ionas-CMS / ZuFiSH	ALLRIS (cc e-gov)
OParl?	Nein, nicht beteiligt	OParl = JSON-Ausgabe desselben ALLRIS-Inhalts
Automatisiert auslesbar?	Ja, die Seite ist technisch in wenigen Minuten auslesbar	Ja, über sitzungsdienst-schenefeld.de in wenigen Minuten, auch ohne OParl

	Video-Demonstration 1 hier anschauen: https://t1p.de/bfb6	**Video-Demonstration 2 hier anschauen:** https://t1p.de/bfb10

Technischer Befund:

Zwei kurze technische Tests zeigen, dass zum einen die öffentlich zugängliche Ansprechpartner-Seite der Stadt (https://www.stadt-schenefeld.de/service/von-a-bis-z/ansprechpartner-innen/) ganz ohne OParl automatisiert ausgelesen werden kann. Dabei lassen sich 89 Mitarbeiter mit vollständigen Kontaktdaten (Name, Telefon, Fax, E-Mail, Position, Aufgabengebiet und Abteilung) in wenigen Minuten extrahieren. Zum anderen können auch Namen und Emailadressen aus dem ALLRIS ausgelesen werden. OParl wird in keinem dieser Beispiele verwendet. Dies zeigt, dass Maschinenlesbarkeit kein neues Risiko darstellt, sondern eine Eigenschaft jeder modernen Webseite ist.

Dasselbe ist technisch möglich für jede andere Kommune, die das CMS ionas einsetzt (bundesweit über 500) und auch das ALLRIS. Die Standardisierung beider Systeme macht einen solchen Zugriff einfacher, nicht schwerer.

4. Wie E-Mail-Spoofing funktioniert

Der Vorfall war ein klassischer CEO-Fraud (https://de.wikipedia.org/wiki/CEO_Fraud). Der Ablauf läuft in zeitlich entkoppelten Phasen ab, typischerweise durch verschiedene Akteure:

Phase 1: Adress-Harvesting (automatisiert)

Spezialisierte Crawler sammeln E-Mail-Adressen von Webseiten, Google, LinkedIn und Presseartikeln. Massenhaft und automatisiert. Die Ergebnisse werden in Datenbanken aggregiert und im Darknet weiterverkauft. OParl ist dafür nicht nötig: Die städtische Webseite und das ALLRIS-Webinterface liefern dieselben Daten.

Phase 2: Infrastruktur (andere Akteure)

Die Käufer der Adressdaten nutzen kompromittierte SMTP-Server oder Bulletproof-Hosting im Ausland. Das SMTP-Protokoll prüft Absenderangaben nicht von sich aus. Ohne korrekte SPF-, DKIM- und DMARC-Konfiguration kann jeder Absenderadressen fälschen.

Phase 3: Social Engineering (gezielt)

Mit öffentlich verfügbaren Organigramm-Daten konstruiert der Angreifer glaubwürdige Szenarien. Im konkreten Fall wurde eine Hotmail-Adresse im Namen der Bürgermeisterin verwendet.

Entscheidend:

Wer sofortige Kausalität zwischen OParl und dem Angriff herstellt, hat nicht verstanden, wie die heutige Bedrohungslandschaft funktioniert. Harvesting, Infrastruktur und Angriff sind zeitlich und personell entkoppelt.

5. Das Standardisierungsargument

Das CMS ionas (Hersteller: Chamäleon AG, Montabaur) wird bundesweit von über 500 Kommunen eingesetzt. In Schleswig-Holstein werden die Instanzen bei Dataport gehostet. Das ALLRIS-Ratsinformationssystem (cc e-gov, Hamburg) wird von nahezu allen norddeutschen Kommunen genutzt.

Beide Systeme verwenden standardisierte Datenstrukturen. Ein Scraper, der für Schenefeld funktioniert, funktioniert mit minimalen Anpassungen für jede andere Kommune. Wenn die Argumentation der Vorlage konsequent angewendet würde, müssten alle norddeutschen Kommunen:

- Ihre Webseiten-Ansprechpartnerverzeichnisse abschalten
- ALLRIS abschalten (dort stehen ebenfalls Namen und E-Mails)
- Ratsmitgliederseiten löschen
- Mailadressen und Telefonnummern entfernen

Die Vorlage selbst widerlegt sich: „Die bisherigen öffentlichen Allris-Daten bleiben unverändert auf der städtischen Homepage veröffentlicht."

6. Zusammenfassung

> *Wer OParl abschaltet und sagt „wir haben das Problem behoben", wiegt die Organisation in falscher Sicherheit und verhindert möglicherweise, dass die tatsächlich wirksamen Maßnahmen ergriffen werden. Das ist schlimmer als nichts zu tun, denn es bindet Aufmerksamkeit und Ressourcen an der falschen Stelle.*

Der Fachbegriff: „Security Theater" (Bruce Schneier). Maßnahmen, die das Gefühl von Sicherheit erzeugen, ohne tatsächlich Sicherheit zu schaffen.

BfB-Position:

Wir widersprechen nicht aus Prinzip, sondern auf Basis überprüfbarer technischer Fakten. Jede Behauptung in diesem Dokument ist durch eigene Tests oder öffentlich zugängliche Quellen belegbar. Wir sind bereit, die Verwaltung bei der Umsetzung tatsächlich wirksamer Sicherheitsmaßnahmen zu unterstützen.

Glossar: Fachbegriffe einfach erklärt

Begriff	Erklärung
Scraping (Web Scraping)	Das automatisierte Auslesen von Inhalten einer Webseite durch ein Computerprogramm. Vergleichbar mit dem Abschreiben einer öffentlichen Telefonbuch-Seite, nur schneller. Der Browser selbst ist im Grunde auch ein Scraper, er zeigt die Daten nur hübscher an.
Harvesting (E-Mail-Harvesting)	Das systematische Sammeln von E-Mail-Adressen aus öffentlichen Quellen (Webseiten, Suchmaschinen, soziale Netzwerke). Geschieht automatisiert und massenhaft. Die gesammelten Adressen werden oft weiterverkauft.
Phishing	Betrugsversuch per E-Mail (oder Telefon), bei dem der Angreifer eine falsche Identität vortäuscht, um Informationen, Zugangsdaten oder Geld zu erlangen. Der Name leitet sich von „Fischen nach Passwörtern“ ab.
Spoofing (E-Mail-Spoofing)	Das Fälschen des Absenders einer E-Mail. Da das E-Mail-Protokoll (SMTP) den Absender nicht automatisch prüft, kann jeder einen beliebigen Absendernamen angeben. Vergleichbar mit einem Brief, auf dessen Umschlag ein falscher Absender steht.
CEO-Fraud	Eine Sonderform des Phishing, bei der sich der Angreifer als Vorgesetzter ausgibt (z.B. Bürgermeister/in) und Mitarbeiter zu Handlungen auffordert. Im konkreten Fall: E-Mails im Namen der Bürgermeisterin von einer Hotmail-Adresse.
SMTP	Simple Mail Transfer Protocol. Das technische Regelwerk, nach dem E-Mails im Internet versendet werden. Stammt aus den 1980er Jahren und enthält keine eingebaute Absenderprüfung.
SPF / DKIM / DMARC	Drei ergänzende Sicherheitsmechanismen für E-Mail. Sie ermöglichen es, gefälschte Absender zu erkennen und abzuweisen. Vergleichbar mit einem Siegel auf einem Brief, das bestätigt, dass der Brief wirklich vom angegebenen Absender stammt.
OParl	Offene Schnittstelle für Ratsinformationssysteme. Ein deutschlandweiter Standard, der es ermöglicht, öffentliche parlamentarische Daten (Sitzungen, Beschlüsse, Gremien, Personen) maschinenlesbar abzurufen. OParl liefert ausschliesslich Daten, die bereits öffentlich im Ratsinformationssystem sichtbar sind.
ALLRIS	Ein Ratsinformationssystem der Firma cc e-gov (Hamburg). Wird von nahezu allen norddeutschen Kommunen eingesetzt. Enthält Sitzungstermine, Beschlussvorlagen, Gremien und Personendaten (Ratsmitglieder). Zu erreichen unter sitzungsdienst-schenefeld.de.
ionas / CMS	Content-Management-System der Chamäleon AG (Montabaur). Wird für den Internetauftritt der Stadt Schenefeld verwendet (stadt-schenefeld.de). CMS = System zur Pflege von Webseite-Inhalten. Bundesweit bei über 500 Kommunen im Einsatz.
ZuFiSH	Zuständigkeitsfinder Schleswig-Holstein. Zentrale Landesdatenbank mit Organisationsstrukturen, Mitarbeitern und Zuständigkeiten aller SH-Kommunen. Betrieben vom Land Schleswig-Holstein.
Dataport	IT-Dienstleister der öffentlichen Verwaltung in Norddeutschland. Betreibt die Server-Infrastruktur, auf der u.a. die Webseiten der SH-Kommunen laufen. Nicht der Hersteller der Software, sondern der Hosting-Partner.
Darknet	Ein Teil des Internets, der nur über spezielle Software erreichbar ist und Anonymität bietet. Wird u.a. für den Handel mit gestohlenen Daten, E-Mail-Adresslisten und Zugangsdaten genutzt.
Security Theater	Begriff des IT-Sicherheitsexperten Bruce Schneier. Bezeichnet Sicherheitsmassnahmen, die das Gefühl von Sicherheit erzeugen, ohne tatsächlich Sicherheit zu schaffen. Bekanntes Beispiel: Schuhe ausziehen am Flughafen.
Maschinenlesbarkeit	Die Eigenschaft von Daten, von Computerprogrammen verarbeitet werden zu können. Jede Webseite ist technisch maschinenlesbar, eine API wie OParl macht es lediglich strukturierter. Vergleich: Eine Bibliothek mit Katalog (API) vs. ohne Katalog (Webseite). Die Bücher (Daten) sind dieselben.