Behördensoftware 1995 Check: Sicherheit auf dem Prüfstand

Category: Opinion
geschrieben von Tobias Hager | 11. August 2025

Behördensoftware 1995 Check: Sicherheit auf dem Prüfstand

Du glaubst, deine Daten sind bei deutschen Behörden sicherer als Goldreserven im Tresor? Willkommen im Jahr 2024 – und willkommen zu einer schonungslosen Bestandsaufnahme von Behördensoftware, die teilweise noch aus der Zeit stammt, als Windows 95 und Faxgeräte als Hightech galten. In diesem Artikel zerlegen wir gnadenlos, wie es um die IT-Sicherheit, Datenschutz und technische Basis in deutschen Amtsstuben wirklich steht. Wer jetzt noch an digitale Souveränität glaubt, sollte besser weiterlesen – oder gleich den Stecker ziehen.

- Behördensoftware 1995: Warum Technik von gestern heute zum Sicherheitsrisiko wird
- Die größten Schwachstellen alter Verwaltungssoftware – von ungepatchten Systemen bis zu Klartext-Passwörtern
- Warum deutsche Behörden IT-Modernisierung verschlafen – und was das für Bürger bedeutet
- Cyberangriffe, Ransomware & Datenleaks: Die tickende Zeitbombe in öffentlichen IT-Infrastrukturen
- Rechtliche Vorgaben vs. technische Realität: Wo Datenschutz auf Legacy-Systeme trifft
- Wie Behörden ihre Software sichern könnten – und warum sie es selten tun
- Schritt-für-Schritt-Analyse: So prüfst du, ob eine Behördensoftware sicher ist (Spoiler: Meistens nicht)
- Die wichtigsten Tools und Methoden für Security Audits von Altsystemen
- Warum Digitalisierung ohne Security nur ein teures Placebo ist
- Der Weg aus der Legacy-Hölle: Was Politik, Verwaltung und IT wirklich ändern müssten

Es klingt wie ein schlechter Witz, ist aber bittere Realität: Während Deutschland über Digitalisierung debattiert, laufen in unzähligen Behörden noch Software-Systeme, die schon Y2K-Panik ausgelöst haben. Behördensoftware 1995 – das steht sinnbildlich für IT-Architekturen, die seit Jahrzehnten nicht grundlegend erneuert wurden. Und genau das ist der Grund, warum deutsche Amtsstuben heute nicht nur Innovations-, sondern auch Sicherheitswüsten sind. Die Folgen? Angriffe, Datenverluste, Datenschutzskandale. Doch warum hält sich dieser technische Muff so hartnäckig – und warum ist der Weg in die Moderne so schwer?

Die Wahrheit ist unbequem: Behörden kaufen keine Software wie Start-ups, sie entwickeln und beschaffen nach Regeln, deren Ursprung ungefähr so alt ist wie Netscape Navigator. Das Ergebnis: Legacy-Software, Patchwork-Infrastrukturen, fehlende Sicherheitsupdates und ein digitaler Flickenteppich, der Hacker magisch anzieht. Wer wissen will, warum die nächste Cyberattacke auf eine deutsche Behörde nur eine Frage der Zeit ist, sollte sich die folgenden Zeilen genau anschauen. Willkommen zum Sicherheits-Check der Behörden-IT, Version 1995.

Behördensoftware 1995: Die Anatomie eines IT-Sicherheitsrisikos

Fangen wir mit den Basics an: Was ist eigentlich Behördensoftware 1995? Damit meinen wir nicht nur Programme, die im Jahr 1995 entwickelt wurden, sondern eine ganze Generation von Verwaltungsanwendungen, die auf veralteten Technologien basieren. Gemeint sind Softwarelösungen, die auf Windows NT, veralteten UNIX-Derivaten oder sogar Mainframes laufen, bei denen die Bedienoberfläche maximal an eine bessere Tabellenkalkulation erinnert. Diese

Lösungen sind das Rückgrat vieler Amtsstuben – und das ist genau das Problem.

Der Hauptgrund für den anhaltenden Einsatz solcher Systeme ist die schiere Trägheit öffentlicher IT-Prozesse. Software, die Jahrzehnte überdauert, wurde oft maßgeschneidert entwickelt, ist tief in die Arbeitsabläufe integriert und wird von Generationen von Sachbearbeitern wie ein Heiligtum behandelt. Eine Migration auf moderne Systeme? Zu teuer, zu riskant, zu kompliziert. Also bleibt alles beim Alten – und die Sicherheitslücken wachsen mit jedem Jahr.

Technisch gesehen sind diese Systeme ein Albtraum: Fehlende Verschlüsselung, Klartext-Passwörter in Konfigurationsdateien, proprietäre Protokolle ohne Authentifizierung und ein Patchmanagement, das oft aus dem Prinzip “Never touch a running system” besteht. Die Folge: Angriffe, die in der kommerziellen IT längst abgewehrt oder automatisiert verhindert werden, führen bei Behörden regelmäßig zu Ausfällen, Datenverlusten und – im schlimmsten Fall – zu Datenabflüssen, die Bürger direkt betreffen.

Ein weiteres Problem: Diese Software läuft häufig auf Hardware, die längst vom Hersteller abgekündigt wurde. Sicherheitsupdates? Fehlanzeige. Support? Gibt’s nur noch auf dem Papier oder zu Preisen, bei denen jeder IT-Dienstleister in Tränen ausbricht. Das ist die Realität hinter “Behördensoftware 1995” – und damit das Einfallstor für jede denkbare Attacke.

Sicherheitslücken und Schwachstellen: Wo Behörden-IT wirklich brennt

Wer glaubt, dass Behörden-IT wenigstens hinter dicken Firewalls sicher ist, irrt. Die Realität sieht so aus: Offene Ports ins öffentliche Netz, Remote-Desktop-Zugänge ohne Zwei-Faktor-Authentisierung, File-Server mit SMBv1-Protokoll und Passwörtern wie “Dienststelle2020” – das ist keine Übertreibung, sondern Alltag in vielen Kommunen, Landes- und Bundesbehörden.

Ein Klassiker: Ungepatchte Windows-Systeme, die noch auf Versionen wie Windows 7 oder gar XP laufen. Jeder Exploit, der in den letzten 10 Jahren durch die Medien geisterte, funktioniert hier noch wie am ersten Tag. EternalBlue? Läuft. WannaCry? Kein Problem – im Gegenteil, es ist oft nur eine Frage der Zeit, bis der nächste Verschlüsselungstrojaner eine komplette Behörde lahmlegt.

Doch es sind nicht nur die Betriebssysteme. Auch die eigentliche Behördensoftware ist voller Schwachstellen: SQL-Injection-Lücken in Altanwendungen, unverschlüsselte Datenbanken, Debug-Interfaces mit Standardpasswörtern und selbstgebastelte Authentisierung, die mit aktuellen Security-Standards ungefähr so viel gemein hat wie ein Faxgerät mit 5G. Und das alles oft in Systemen, die sensible Daten von Millionen Bürgern enthalten – von Steuerdaten über Gesundheitsinformationen bis zu polizeilichen

Ermittlungsakten.

- Häufigste Schwachstellen in Behördensoftware 1995:
  - Fehlende Transportverschlüsselung (kein HTTPS, kein VPN)
  - Hartcodierte Passwörter in Skripten und Konfigurationsdateien
  - Ungepatchte Drittanbieter-Bibliotheken und veraltete Frameworks
  - Offene Netzwerkdienste ohne Zugriffsbeschränkung
  - Fehlende oder fehlerhafte Protokollierung und Monitoring

Die Liste ließe sich endlos fortsetzen. Fakt ist: In den wenigsten Fällen gibt es ein dediziertes Security-Team, das systematisch Schwachstellen sucht und schließt. Vielmehr verlässt man sich auf die Hoffnung, dass "schon nichts passieren wird". Ein Trugschluss, der angesichts der Angriffsfläche fatal ist.

IT-Modernisierung verschlafen: Warum sich bei Behörden (fast) nichts ändert

Warum also verharren Behörden so hartnäckig in der Legacy-Hölle? Die Antwort ist so deutsch wie ernüchternd: Bürokratie, Vergaberecht, Ressourcenmangel und eine Risikoaversion, die ihresgleichen sucht. Wer schon einmal versucht hat, einen neuen Drucker in einer Behörde zu beschaffen, weiß, dass selbst kleinste IT-Investitionen durch endlose Gremien, Ausschreibungen und Prüfungen geschleust werden müssen. Bei Software ist es noch schlimmer.

Hinzu kommt: Viele Behörden verfügen schlichtweg nicht über das Personal, um IT-Projekte zu stemmen, die über die Einführung eines neuen E-Mail-Clients hinausgehen. Interne IT-Abteilungen sind häufig chronisch unterbesetzt, der Altersdurchschnitt hoch, das Know-how über moderne Technologien gering. Externe Berater werden zwar geholt – aber oft nur, um bestehende Systeme irgendwie am Leben zu halten, nicht um Innovationen voranzutreiben.

Das Ergebnis ist eine Abwärtsspirale: Je älter die Systeme, desto teurer und riskanter wird eine Migration. Also schiebt man die Entscheidung immer weiter auf, hofft auf politische Initiativen ("Digitalisierungspakt!") und investiert in Workarounds statt in echte Modernisierung. Die Folge: Die Kluft zwischen technischer Realität und politischem Anspruch wird immer größer – und damit auch das Sicherheitsrisiko.

Und noch ein Faktor: Die Angst vor Fehlern. Wer heute in einer Behörde ein Projekt anstößt, das später scheitert, muss mit öffentlicher Schelte, politischer Verantwortung und im schlimmsten Fall persönlichen Konsequenzen rechnen. Da ist es bequemer, auf Nummer sicher zu gehen – auch wenn das bedeutet, das Risiko auf Millionen von Bürgern abzuwälzen.

Angriffsvektor Behörde: Cybercrime, Ransomware und Datenschutzpannen

Wer auf Sicherheitslücken und veraltete Software setzt, lädt Cyberkriminelle geradezu ein. Die letzten Jahre sind ein einziges Mahnmal: Von Kommunen, die nach Ransomware-Angriffen tagelang offline waren, über gehackte Gesundheitsämter bis zu spektakulären Datenlecks im Justizbereich – die Liste der Vorfälle ist lang und wird jedes Jahr länger.

Ransomware-Angriffe sind dabei nur die Spitze des Eisbergs. Viel gefährlicher sind gezielte Attacken auf sensible Datenbestände, bei denen Angreifer unbemerkt jahrelang Daten abziehen. Gerade Mainframe-basierte Systeme, die niemand mehr wirklich versteht oder regelmäßig überprüft, sind ein Paradies für professionelle Hacker. Und: Viele Behörden merken erst Monate später, dass sie Opfer eines Angriffs wurden – wenn überhaupt.

Aber auch klassische Fehler sorgen für Schlagzeilen: Fehlkonfigurierte Cloud-Speicher, E-Mails mit personenbezogenen Daten an falsche Empfänger, USB-Sticks mit sensiblen Daten, die in der Kantine liegen bleiben. Die DSGVO mag hohe Bußgelder androhen – in der Praxis herrscht oft das Prinzip Hoffnung. Das Resultat: Bürgerdaten sind in der deutschen Verwaltung alles andere als sicher.

Die Angriffsflächen sind dabei so vielfältig wie die IT-Landschaft selbst:

- Direkte Angriffe auf ungepatchte Server und Endgeräte
- Social Engineering gegen überforderte Mitarbeiter
- Phishing-Kampagnen, die auf fehlende Security Awareness treffen
- Insider-Bedrohungen durch unzufriedene oder nachlässige Beschäftigte

Jede dieser Schwachstellen ist nicht nur ein technisches, sondern auch ein gesellschaftliches Problem. Denn sie untergräbt das Vertrauen in den Staat als Hüter sensibler Daten.

Security-Audit der Legacy-IT: Schritt-für-Schritt-Anleitung

Die gute Nachricht: Es gibt bewährte Methoden, um die Sicherheit von Behördensoftware 1995 systematisch zu überprüfen. Die schlechte Nachricht: Sie werden selten konsequent angewendet. Wer wissen will, wie ein echter Security-Audit für Legacy-Systeme aussieht, sollte sich an folgende Schritte halten:

- Systeminventur: Vollständige Erfassung aller eingesetzten Systeme, Versionen, Schnittstellen und Zugänge. Dokumentation ist Pflicht!

- Patchlevel-Prüfung: Analyse aller installierten Softwarestände. Gibt es Sicherheitsupdates? Werden sie eingespielt? Gibt es einen Update-Prozess?
- Netzwerkanalyse: Welche Ports und Dienste sind nach außen offen? Gibt es Remote-Zugänge? Wer hat Zugriffsrechte?
- Authentisierung & Passwortmanagement: Werden Passwörter regelmäßig geändert? Gibt es Zwei-Faktor-Authentisierung? Wie werden Passwörter gespeichert?
- Protokollierung & Monitoring: Werden Zugriffe und Änderungen geloggt? Gibt es ein zentrales Monitoring für Anomalien?
- Penetrationstests: Externe Experten simulieren echte Angriffe auf die Systeme. Werden Schwachstellen gefunden, müssen sie dokumentiert und zeitnah geschlossen werden.
- Awareness-Training: Mitarbeiter müssen regelmäßig auf aktuelle Bedrohungen, Phishing und Social Engineering geschult werden.

Wer diese Liste gewissenhaft abarbeitet, erlebt oft böse Überraschungen: Admin-Accounts mit Standardpasswörtern, offene RDP-Ports, SQL-Injection-Lücken oder unverschlüsselte Datenübertragungen. Die Faustregel: Je älter das System, desto größer das Risiko.

Tools und Methoden für den Sicherheits-Check: Was wirklich hilft

Ein Security-Audit lebt von den richtigen Werkzeugen. Die Klassiker aus der kommerziellen IT funktionieren auch bei Behörden – sofern sie überhaupt eingesetzt werden dürfen. Hier einige der wichtigsten Tools für den Check von Behördensoftware 1995:

- Nmap: Der Standard für Port- und Netzwerkscans. Findet offene Dienste und unsichere Konfigurationen in Sekunden.
- Nessus/OpenVAS: Vulnerability Scanner, die bekannte Schwachstellen in Betriebssystemen und Anwendungen erkennen. Perfekt für Legacy-Systeme mit hohem Risiko.
- Metasploit: Framework für Penetrationstests – mit Modulen für Exploits, die gerade bei alten Windows- oder UNIX-Systemen noch erschreckend gut funktionieren.
- Wireshark: Netzwerk-Sniffer, der unverschlüsselte Übertragungen und verdächtigen Traffic sichtbar macht.
- Sysinternals Suite: Microsoft-Tools für tiefgehende Systemanalysen auf Windows-Basis – extrem hilfreich, um versteckte Prozesse oder Rootkits zu finden.
- Logfile-Analyse: Unverzichtbar, um verdächtige Aktivitäten, fehlende Updates oder fehlerhafte Konfigurationen zu erkennen.

Wichtig: Viele Behörden scheuen den Einsatz solcher Tools aus Angst vor “Störung des Betriebs”. Das ist verständlich – aber genau das Problem. Wer

Sicherheit will, muss die Komfortzone verlassen und Unangenehmes offenlegen.

Der Weg aus der Legacy-Hölle: Was wirklich passieren muss

Die Diskussion um sichere Behördensoftware ist alt – geändert hat sich wenig. Dabei liegen die Lösungen auf der Hand: Konsequente Migration auf moderne, wartbare Systeme mit regelmäßigen Updates, zertifizierte Sicherheitsarchitekturen und echtes Security-Monitoring. Dazu gehören nicht nur technische Maßnahmen, sondern auch organisatorische Änderungen: IT-Personal aufstocken, Beschaffungsprozesse beschleunigen und Security als Daueraufgabe begreifen.

Ein radikaler Schnitt ist nötig: Legacy-Systeme müssen raus, auch wenn es kurzfristig teuer und unbequem ist. Wer immer noch glaubt, dass “weiter so” reicht, unterschätzt die Dynamik von Cyberbedrohungen und das Ausmaß gesellschaftlicher Schäden bei Datenverlusten. Es braucht politischen Willen, klare Vorgaben und endlich Budgets, die nicht für Hochglanz-Broschüren, sondern für sichere und funktionale IT ausgegeben werden.

Was einzelne Behörden tun können? Sofort alle Systeme inventarisieren, Schwachstellen dokumentieren und kurzfristig absichern, was möglich ist. Parallel Modernisierungsprojekte starten – mit echtem Projektmanagement, festen Deadlines und klarer Verantwortung. Der Verweis auf “fehlende Ressourcen” zählt nicht mehr – die Risiken sind zu groß.

Fazit: Sicherheit als Voraussetzung für echte Digitalisierung

Wer heute über digitale Verwaltung redet, muss zuerst über Sicherheit reden. Behördensoftware von 1995 ist keine technische Marotte, sondern ein massives Risiko für Bürger, Staat und Gesellschaft. Die Zeit der Ausreden ist vorbei – jede weitere Verzögerung macht die Angriffsfläche größer und die Schäden teurer.

Was bleibt? Die Erkenntnis, dass echte Digitalisierung ohne sichere, moderne IT-Infrastrukturen nichts als teures Placebo ist. Behörden müssen raus aus der Legacy-Hölle, rein in die technische Realität von 2024. Das ist unbequem, komplex und kostet Geld – aber alles andere ist verantwortungslos. Wer den Sicherheits-Check jetzt nicht besteht, wird ihn nie wieder bestehen. Willkommen in der echten Welt. Willkommen bei 404.