Man wollte nur mal schnell seine Lohnabrechnung herunterladen. Ein paar Klicks, ein PDF, fertig – so die Vorstellung. Was man stattdessen bekommt, ist ein bürokratisch-technisches Hindernisrennen aus gesperrten Konten, nicht funktionierenden Apps, Zwei-Faktor-Hürden und digitalem Frust. Willkommen im deutschen Alltag 2025, wo die Digitalisierung nicht vereinfacht, sondern verkompliziert. Was nach „mehr Sicherheit“ klingt, ist in Wirklichkeit ein neuer Zwangspfad. Eine politische Regulierung wäre dringend nötig. Von **Günther Burbach**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/250820-Digitale-Sackgassen-NDS.mp3

Podcast: Play in new window | Download

Der Einstieg beginnt oft harmlos. Der Arbeitgeber übergibt die Verwaltung der Lohnabrechnungen an einen großen Anbieter wie DATEV, für Unternehmen eine standardisierte Lösung, für die Angestellten jedoch eine digitale Zumutung. Wer seine Abrechnung einsehen will, muss sich dort registrieren, ein Konto erstellen und künftig über App-basierte Authentifizierungsverfahren anmelden. Doch sobald man dieses System länger nicht nutzt, beginnt das Dilemma: Die Zugangsdaten sind nicht mehr aktuell, das Passwort läuft ab oder der Authentifizierungscode wird auf ein Handy gesendet, das längst ersetzt oder zurückgesetzt wurde.

Das allein wäre schon ärgerlich. Aber die eigentliche Absurdität beginnt, wenn man versucht, das Konto neu zu aktivieren oder zu ersetzen. Denn die Mailadresse, mit der man sich damals registriert hat, ist weiterhin fest mit dem Konto verknüpft. Ein neues Konto lässt sich nicht erstellen, da die Adresse „schon vergeben“ ist, das alte Konto aber bleibt unerreichbar, weil der Zugriffscode nicht mehr generiert wird. Eine echte digitale Sackgasse: kein Zugang, kein Zurück, keine Hilfe. Wer versucht, den Support zu kontaktieren, wird oft an den Arbeitgeber verwiesen. Der wiederum hat keinen Zugriff auf die persönlichen Zugangsdaten, das System ist technisch „sauber getrennt“. Für den Betroffenen bedeutet das: Er hat zwar ein Konto, aber keinerlei Möglichkeit, es zu nutzen.

Viele greifen in ihrer Verzweiflung zu Apps aus dem Store, die vermeintlich den Zugang erleichtern sollen, etwa sogenannte Authenticator-Apps. Doch hier lauert

die nächste Falle: Der Markt ist überschwemmt von dubiosen Klon-Apps, die aussehen wie das Original, aber bereits beim Öffnen ein kostenpflichtiges Abo aktivieren. Und während man sich durch Nutzungsbedingungen klickt, in der Hoffnung, irgendwo den rettenden QR-Code-Scan starten zu können, läuft im Hintergrund bereits der Abrechnungsprozess. Man zahlt und bekommt dennoch keinen Zugang.

Es ist ein technisches System, das vorgibt, sicher und effizient zu sein, in Wahrheit aber viele Menschen ausschließt, frustriert und in Abo-Fallen treibt. Und das alles, nur weil sie ihr eigenes Gehalt sehen wollen.

Ein geschlossenes System mit offener Flanke

DATEV ist kein kleines Start-up mit wilden Ideen, sondern ein etablierter IT-Dienstleister, der in Deutschland eine marktbeherrschende Rolle bei der Abwicklung von Lohnabrechnungen, Steuerdaten und Buchhaltung einnimmt. Rund 2,5 Millionen Arbeitnehmer greifen über das DATEV-System auf ihre Entgeltabrechnungen zu, oder besser gesagt: sollten darauf zugreifen können. Denn in der Praxis erleben viele das Gegenteil.

Der Zugang erfolgt in der Regel über das sogenannte DATEV Arbeitnehmer-Online-Portal, das mit einer Kombination aus Benutzername, Passwort und – besonders wichtig – einem zweiten Sicherheitsfaktor gesichert ist. Und dieser zweite Faktor ist fast immer eine App-basierte Authentifizierung**,** etwa über die DATEV SmartLogin-App oder über externe Tools wie den Google Authenticator. Was nach „mehr Sicherheit“ klingt, ist in Wirklichkeit ein neuer Zwangspfad**,** der gerade diejenigen ausschließt, die sich nicht täglich mit digitalen Sicherheitsprotokollen beschäftigen.

Zwar ist es theoretisch möglich, die App schon bei der Einrichtung des Zugangs zu installieren und mit dem Konto zu verknüpfen. Doch praktisch gesehen, bedeutet das: Wer einmal sein Smartphone wechselt, zurücksetzt, die App löscht oder den Code verliert, muss den gesamten Prozess neu starten, inklusive Einladung durch den Arbeitgeber oder Rücksetzung über den DATEV-Support. Das wäre kein Problem, wenn die Benutzerführung klar, die Hilfe erreichbar und das System fehlertolerant wäre. Doch genau hier liegt das strukturelle Versagen: Wer einen Schritt nicht korrekt ausführt, oder schlicht nicht mehr nachvollziehen kann, welche Schritte vor zwei Jahren nötig waren, steht erneut vor der digitalen Mauer.

Die Unfähigkeit, bestehende Mailadressen einem neuen Konto zuzuordnen oder ein

temporäres Login zu generieren, ist dabei keine technische Notwendigkeit, sondern eine bewusste Systementscheidung. In den Geschäftsbedingungen steht zwar viel über Datenschutz und Sicherheit, aber fast nichts über Nutzerfreundlichkeit oder Wiederherstellbarkeit des Zugangs**.** Der Staat schweigt dazu. Dabei wäre gerade hier politische Regulierung dringend nötig, schließlich handelt es sich nicht um Luxusfunktionen, sondern um den Zugang zu zentralen Arbeits- und Steuerdaten.

Und als wäre das nicht genug, geraten viele Nutzer zusätzlich in die Falle der sogenannten Authenticator-Apps, insbesondere bei Android. Wer versehentlich die falsche App aus dem Google Play Store lädt, landet mitunter bei Anbietern, die täuschend echt aussehen, aber versteckte Abos enthalten. Die Apps versprechen „schnellen Zugang zu Ihren sicheren Codes“, doch sobald man sie öffnet, erscheint ein Bildschirm mit AGBs und „kostenlosem Testzeitraum“, der sich stillschweigend in ein Monatsabo für 7 bis 15 Euro verwandelt. Wer nicht rechtzeitig kündigt, zahlt, oft über Monate hinweg, für eine App, die nicht einmal funktioniert oder gar keinen Bezug zum eigentlichen Dienst hat.

So geraten viele Menschen in ein doppeltes Netz: auf der einen Seite der digitale Zugriffszwang über Apps wie DATEV SmartLogin, auf der anderen Seite eine App-Ökonomie, die Unsicherheit systematisch in Geld umwandelt. Und am Ende steht ein ernüchternder Befund: Wer seine Abrechnung sehen will, muss nicht nur technisch versiert sein, sondern auch noch die Fallen der Plattformökonomie erkennen, vermeiden und rechtzeitig kündigen.

Was ist das für ein System, das den Zugang zu den eigenen Daten so erschwert, dass es am Ende wie digitale Erpressung wirkt?

Digitale Unfreiheit – Wie der Staat mit seiner Verantwortung umgeht

Die Situation, wie sie Millionen Arbeitnehmer mit Systemen wie DATEV erleben, ist kein Einzelfall. Sie ist Teil eines größeren Trends: der technokratischen Entmündigung im Namen der Digitalisierung. Offiziell heißt es, alles werde einfacher, schneller, effizienter. Tatsächlich wird vieles komplizierter, unübersichtlicher und exklusiver. Wer nicht Schritt hält mit den technischen Anforderungen, oder wer sich schlicht weigert, jedes Update, jede App, jedes Identifikationsverfahren kritiklos mitzumachen, wird zunehmend ausgesperrt.

Dabei ist das nicht nur ein Problem einzelner Anbieter wie DATEV. Es ist die Folge politischer Versäumnisse und eines Digitalverständnisses, das auf Zwang statt auf

Wahlfreiheit setzt**.** Die Bundesregierung und viele Landesregierungen preisen seit Jahren die sogenannte „digitale Verwaltung“, fördern Plattformlösungen und verlangen elektronische Nachweise, von Elster bis eRezept, von De-Mail bis Steuer-ID. Doch sie überlassen die konkrete Umsetzung weitgehend privaten Anbietern, deren Systeme oft auf maximaler Absicherung, nicht aber auf praktischer Zugänglichkeit beruhen. Wer außen vor bleibt, hat Pech gehabt.

Was fehlt, ist eine digitale Ethik, die den Menschen nicht nur als Datensatz, sondern als Subjekt begreift, mit Rechten, Bedürfnissen und Begrenzungen. Nicht jeder hat ein Smartphone. Nicht jeder will dutzende Apps auf dem Gerät. Nicht jeder versteht, was ein „zweiter Faktor“ ist, wie man QR-Codes sichert oder was passiert, wenn ein Authenticator verloren geht. Und selbst wenn man all das weiß, es bleibt dabei: Es darf keine Pflicht zur App geben, wenn es um elementare Verwaltungs- oder Arbeitsdaten geht.

Was wäre so schwer daran, einen einfachen Zugang über Benutzername, Passwort und eine temporäre SMS-TAN anzubieten, zumindest als alternative Option? Was hindert Arbeitgeber daran, analoge Abrechnungen auf Wunsch wieder zur Verfügung zu stellen? Warum dürfen zentrale Systeme wie DATEV nur noch über App-Strukturen funktionieren, obwohl die Risiken (Datenverlust, Gerätewechsel, Abhängigkeit von Drittanbietern) allseits bekannt sind?

Die Antwort ist bitter: Weil es niemanden interessiert, solange die Prozesse intern effizient und revisionssicher sind. Der Aufwand für die Betroffenen, Zeit, Nerven, im schlimmsten Fall auch Geld, wird externalisiert. Das ist digitale Bürokratie in Reinform: technisch korrekt, formal sauber, aber praktisch unzumutbar.

Besonders bezeichnend ist, wie sehr die Systeme auf Eindeutigkeit bestehen und damit ihre eigene Unbeweglichkeit produzieren. Wer seine E-Mail-Adresse einmal registriert hat, kann sie oft kein zweites Mal nutzen, selbst wenn das alte Konto nicht mehr erreichbar ist. Das System erkennt die Mail als „vergeben“, weigert sich aber gleichzeitig, eine Wiederherstellung ohne den ursprünglichen Authentifizierungsfaktor zuzulassen. Das ist, als würde ein Türschloss den alten Schlüssel verlangen, aber keinen Ersatzschlüssel akzeptieren und trotzdem jede neue Tür mit „dieser Schlüssel gehört schon jemandem“ blockieren.

Gerade in einer Zeit, in der Menschen ohnehin mit steigender Komplexität, Informationsüberflutung und digitaler Unsicherheit kämpfen, ist es brandgefährlich, solche Zugangssysteme ohne Not zu verengen. Die Botschaft an die Bürger lautet

am Ende: Du kommst nur rein, wenn du das Spiel mitspielst, inklusive aller Risiken, Drittanbieter-Apps, Kosten und technischer Anforderungen. Und wenn nicht? Dann bleibt dir der Zugang zu deinen eigenen Dokumenten eben verwehrt.

Resümee: Digitale Effizienz auf Kosten der Menschenwürde

Wir sind längst mittendrin, in einer Zeit, in der Technik nicht mehr nur Hilfsmittel ist, sondern zur Pflicht erhoben wird. Wer heute auf seine eigenen Daten zugreifen will, wird zu digitalen Verhaltensmustern gezwungen, die mit Alltagstauglichkeit oft nichts mehr zu tun haben. Man braucht ein Smartphone, eine bestimmte App, eine registrierte Mailadresse, stabile Internetverbindung, die richtige Uhrzeit, ein korrektes Backup, nur um ein PDF zu öffnen, das früher per Post kam.

Und das ist keine Schwarzmalerei, sondern gelebte Realität. Wer solche Systeme entwirft, prüft sie oft nur unter Idealbedingungen, mit IT-Fachleuten, die tagtäglich mit Authentifizierung, Geräten, Passwörtern und digitalen Zertifikaten arbeiten. Die Wirklichkeit draußen sieht anders aus. Dort stehen Menschen, die zwei bis drei Mal im Jahr ihre Lohnabrechnung brauchen. Menschen, die keinen Nerv dafür haben, sich durch verschachtelte Wiederherstellungsprozesse und App-Zwänge zu klicken. Menschen, die vielleicht kein aktuelles Smartphone besitzen oder schlicht kein Vertrauen mehr in diese digitalen Ketten haben.

Natürlich ist es für Arbeitgeber günstiger, Lohnabrechnungen nicht mehr auszudrucken. Aber die Folge ist eine neue Form der digitalen Entkoppelung. Viele Arbeitnehmer schauen sich ihre Abrechnung monatelang gar nicht mehr an, aus Frust, aus Bequemlichkeit oder weil sie sich vom System ausgeschlossen fühlen. Und wenn sie die Abrechnung dann doch einmal brauchen, zum Beispiel für einen Mietvertrag, ein Bankgespräch oder das Finanzamt, dann beginnt der Spießrutenlauf. Das Konto ist gesperrt, der Zugangscode ungültig, die App verloren. Der Weg zur eigenen Gehaltsabrechnung wird zur Tortur.

Wenn das die Zukunft der digitalen Verwaltung ist, dann Gute Nacht. Denn was wir hier sehen, ist nicht technische Modernisierung, sondern ein schleichender Rückzug des Servicegedankens. Statt barrierefreier Zugänge für alle entsteht ein Netz aus App-Zwang, Passwortfallen und Zugriffsverweigerung. Statt echter Digitalisierung erleben wir digitale Bürokratie in Reinkultur, effizient für die einen, entmündigend für die anderen.

Es ist höchste Zeit, umzudenken: Wer digitale Systeme einführt, muss sie zuerst mit

den unerfahrensten Nutzern testen, nicht mit IT-Fachleuten. Es braucht analoge Alternativen, barrierefreie Notzugänge und ein digitales System, das dem Menschen dient, nicht umgekehrt. Denn wenn selbst der Zugriff auf die eigene Lohnabrechnung zur Hürde wird, dann hat die Digitalisierung ihren Zweck verfehlt.

Quellenangaben:

- Nutzerzahlen bei DATEV „Arbeitnehmer online“ (2024, Handwerksblatt)
- Offizielle DATEV-Pressemitteilung zu Wachstum und Cloud-Plattformen (2024)
- Wikipedia-Artikel zu DATEV eG (Struktur, Marktstellung, Kritik)
- Warnung vor bösartigen Authenticator-Apps im Google Play Store (heise online, 2023)
- Onlinezugangsgesetz (OZG) – gesetzlicher Rahmen der digitalen Verwaltung (Wikipedia)
- Welt.de über das Scheitern der deutschen Digitalisierungsstrategie (11 % Zielerreichung, 2023)

Titelbild: Alliance Images / Shutterstock