



Rede

„Ausbau der IT-Infrastruktur: Fokus auf die Sicherheit!“

Christian Amsinck

Alternierender Vorsitzender des Vorstandes der Deutschen
Rentenversicherung Bund

Vertreterversammlung
der Deutschen Rentenversicherung Bund
in Freiburg am 21. Juni 2022

[Einleitung]

Meine sehr geehrten Damen und Herren,

nach über zwei Jahren des Austausches vornehmlich über Videokonferenzen freue ich mich sehr, dass wir uns endlich wieder in Präsenz begegnen.

Lassen Sie uns heute ausgiebig die Möglichkeiten zur gemeinsamen Diskussion und zum Austausch nutzen – ich freue mich darauf.

Mit Freiburg gibt es zudem kaum einen schöneren Ort in Deutschland, um hier symbolisch den Startknopf für künftig wieder mehr Präsenzveranstaltungen zu drücken – eine gute Wahl.

Auch für mein heutiges Thema kann die Stadt Freiburg als eine gute Referenz dienen. Denn: Freiburg war sich frühzeitig bewusst, dass das Thema Digitalisierung sehr komplex und umfangreich sein wird.

Mit ihrer Digitalstrategie "FREIBURG. DIGITAL. GESTALTEN." setzt die Stadt bis zum Jahr 2025 den Rahmen für die Digitalisierung in der Verwaltung, und alle hierfür notwendigen Aufgaben sind seit 2019 in einem Fachamt für Digitales und IT – kurz DIGIT – gebündelt.

Ganz ähnlich geht im Grunde auch die DRV Bund vor. Welche Herausforderungen sich dabei ergeben und mit welchen Themen wir uns als Selbstverwaltung zukünftig noch stärker auseinandersetzen müssen, das möchte ich Ihnen in den kommenden Minuten aufzeigen.

[Fortschritt der Informationstechnik]

Meine sehr geehrten Damen und Herren,

der rasante Fortschritt im Bereich der Informationstechnik verändert unsere Gewohnheiten im Beruflichen wie im Privaten in vielfältiger, oft auch sprunghafter Weise.

Besprechungen finden zunehmend digital statt,

Haushaltsgeräte werden mit dem Internet vernetzt. All dies erleichtert unseren Alltag.

Die Vorteile können aber auch Nachteile mit sich bringen, denn digital vernetzte Systeme sind angreifbar.

Wir als DRV Bund sind uns der Herausforderungen der zunehmenden Digitalisierung – bezogen auf die Informationssicherheit – seit langem bewusst. Eine umfassende Cyber-Resilienz ist heute wichtiger denn je.

Als Dienstleister sind wir zudem Teil der kritischen Infrastruktur, mit wichtiger Bedeutung für das Gemeinwesen. Wir verarbeiten und speichern Daten in Rechenzentren, versorgen die Bevölkerung mit Rentenzahlungen und bieten datenbasierte Auskunftsservices an. All dieses muss zu 100 Prozent sicher erfolgen.

Deshalb schreibt der Gesetzgeber für Betreiber von Kritischen Infrastrukturen – und damit auch für die DRV Bund – alle zwei Jahre die Durchführung von so genannten KRITIS-Audits vor.

Bei der heutigen Entwicklungsgeschwindigkeit der Technologie im Bereich Cyber-Security ein notwendiges Zeitintervall, um Schäden an der IT – von innen wie von außen – zu vermeiden.

Angriffsflächen auf die IT-Infrastruktur vermeiden – das hat die DRV Bund auch gleich zu Beginn der Covid-19-Pandemie getan. Wir haben schnell dafür gesorgt, dass unsere Mitarbeitenden mit besonders abgesicherten Notebooks oder so genannten Nano-PCs von Zuhause arbeiten konnten. Nur dies hat es uns ermöglicht, angemessene Sicherheitsstands für die Informationstechnik zu gewährleisten, wie sie auch am Arbeitsplatz im Büro gegeben sind.

Meine Damen und Herren,

selbstverständlich nicht nur wir, sondern alle verantwortlichen Akteure und Institutionen in der Bundesrepublik haben ein großes Interesse daran, ihre IT-Systeme und IT-Infrastruktur zukünftig entsprechend dem Stand der Technik abzusichern.

Denn in Summe überwiegt ganz klar der Nutzen, der Mehrwert der Digitalisierung – und der muss geschützt werden.

[Digitalisierungsprojekte der Bundesregierung und der EU-KOM]

Nicht nur deshalb spielt das Thema Digitalisierung im Koalitionsvertrag der neuen Bundesregierung die dominante Rolle.

Gleich im ersten Kapitel werden die Vereinbarungen für das Feld „Moderner Staat, digitaler Aufbruch und Innovationen“ festgelegt. Insgesamt 226 mal kommt das Wort „digital“ im Vertrag vor, „Klima“ 198 mal.

So ist die digitalpolitische To-Do-Liste der Bundesregierung recht lang: Cloud-Strategie, digitale Identitäten, Registermodernisierung, Infrastrukturausbau, Interoperabilität, Digitalpakt 2.0, Cybersicherheit, OZG 2.0 sind nur einige der zahlreichen Projekte, von denen viele

auch Schnittmengen mit den Aufgaben und Pflichten der DRV Bund haben.

- Zum Beispiel wird von der Koalition auch ein Digitalcheck, der die digitale Tauglichkeit von Gesetzen sicherstellen soll, gefordert. Während dieser auf Bundesebene noch diskutiert wird, hat die DRV Bund bereits Ihren eigenen Digitalcheck erarbeitet und pilotiert.
- Zudem trägt die DRV mit dem Ausbau und der Modernisierung der Online-Dienste zu einer erfolgreichen Umsetzung des Onlinezugangsgesetzes [OZG] bei.
- Das im Koalitionsvertrag hervorgehobene „Once Only Prinzip“ soll Bürgerinnen davon entlasten, Ihre Daten von einer Verwaltung zur Nächsten zu tragen. Dazu hat die DRV Bund bereits vor einem Jahr das Projekt „DRV Once Only Ready“ initiiert. Wir untersuchen unsere Geschäftsprozesse systematisch darauf, wo heute noch manuelle Nachweise zukünftig durch automatisierten Datenaustausch wegfallen können.

[Deutsche Rentenversicherung Bund]

Wie aber ordnet sich nun die Deutsche

Rentenversicherung Bund ganz konkret in dieses weite

Feld der Digitalisierung und Cybersicherheit ein?

Nun, im Prinzip ganz einfach. Denn – wie erwähnt – nahezu jedes der von mir gerade aufgeführten Themen, hat eine Schnittmenge zu den Aufgaben und Pflichten der Rentenversicherung.

Mit dem Ausbau der Online-Dienste werden wir zudem neue, zukunftsfähige Services einführen und mit der Digitalisierung der Verwaltung Geschäftsprozesse effizienter gestalten. Eine störungsfreie eigene und sichere IT-Infrastruktur sowie der sichere Austausch mit anderen digitalen Schnittstellen – unter Erfüllung der gestiegenen IT-Sicherheitsanforderungen – ist hierfür zwingende Voraussetzung.

[Gemeinsame Rechenzentrum DRV]

Damit uns dies zukünftig weiterhin gelingt, errichten wir bis 2024 das Gemeinsame Rechenzentrum der Deutschen Rentenversicherung. Hier werden künftig alle Daten gemeinsam gespeichert und verwaltet. Dieser Schritt, ein Gemeinsames Rechenzentrum zu schaffen, war rückblickend eine notwendige und sehr wichtige Initiative der Selbstverwaltung.

Für diese neue Grundsatz- und Querschnittsaufgabe sind inzwischen die rechtlichen Grundlagen gelegt und die Abteilung 0900 in der DRV Bund gegründet worden. Diese ist mit dem Aufbau und dem zukünftigen Betrieb des Gemeinsamen Rechenzentrums betraut. In diesem Zusammenhang war auch die Etablierung des Steuerungsgremiums ein wichtiger Schritt. Dieses koordiniert und bündelt die Interessen aller Beteiligten hinsichtlich des Rechenzentrums.

Denn: Mit dem Gemeinsamen Rechenzentrum wird erstmalig für alle 16 Träger eine übergreifende und einheitliche IT-Infrastruktur für das Leistungssystem der Rentenversicherung geschaffen.

Dieses befindet sich an den Standorten Berlin und Würzburg, in zwei miteinander gekoppelten Rechenzentren. Jeder der zwei Standorte ist vor Ort redundant abgesichert.

Hinzukommt eine Absicherung zwischen den Standorten, die sog. Georedundanz. Bei einem Totalausfall eines der beiden Rechenzentren kann damit auf den zweiten Standort geschwenkt werden.

Zudem verbleiben alle Sozialversicherungsdaten fest in den Händen der DRV und verlassen das Gebiet der Bundesrepublik nicht.

Damit schlussendlich eine optimale Integration des Gemeinsamen Rechenzentrums in die Trägerlandschaft gelingt, werden wir uns als Selbstverwaltung zudem noch mit einer weiteren Satzungsänderung befassen.

Denn die Bündelung der Aufgabenerfüllung in einem gemeinsamen Rechenzentrum hat den großen Vorteil, dass durch eine zentrale IT-Sicherheit, die besten Voraussetzungen geschaffen werden, um einen hohen Standard an Sicherheit zu erreichen und erfolgreich IT-Angriffe und die daraus resultierenden Schäden abzuwehren.

Auch wenn Cyberangriffe nahezu täglich erfolgen, konnte die Deutsche Rentenversicherung bisher alle potenziell schwerwiegenden IT-Angriffe abwehren. Das liegt vor allem auch daran, dass wir einen zentralen Internetzugang betreiben, der hoch abgesichert und ebenfalls geo-redundant betrieben wird.

Zu beobachten ist aber, dass die Angriffe an Quantität und Qualität stetig zunehmen. Daher gilt es – auch mit Hilfe des Gemeinsamen Rechenzentrums – die Sicherheitsstrukturen engmaschiger zu knüpfen, um auf zukünftige Bedrohungsszenarien vorbereitet und bei einem Risikoeintritt handlungsfähig zu sein und mögliche Schäden zu begrenzen.

Die Digitalisierung von Services und Verwaltung erfordert nicht nur eine gute Absicherung gegen Cyberattacken mittels einheitlicher IT-Infrastruktur. Sie erfordert auch die ständige Härtung der internen Systeme mittels Sicherheitskonzepten und deren Überwachung. Verantwortlich hierfür ist Herr Dr. Stegmann und sein Team als IT-Sicherheitsbeauftragter der DRV und der DRV Bund.

Nach den zurückliegenden zwei Jahren intensiver Arbeit, folgt nun die Schaffung der notwendigen Bedingungen für die künftige Migration der Trägerdaten in das Gemeinsame Rechenzentrum. Momentan wird intensiv an der Umzugsplanung für alle Träger gearbeitet und der Aufbau der neuen IT-Infrastruktur vorbereitet.

Technisch gesehen hat die Deutsche Rentenversicherung dann die Grundlage dafür geschaffen, die anstehenden Herausforderungen im Bereich der Digitalisierung und IT-Sicherheit erfolgreich zu meistern.

Neben den benannten Fortschritten für die IT-Sicherheit profitieren die Träger der Deutschen Rentenversicherung auch von weiteren Verbesserungen durch ein Gemeinsames Rechenzentrum.

So werden dringend benötigte IT-Personalressourcen für weitere Digitalisierungsvorhaben freigesetzt, die andererseits mit dem Betrieb der IT-Infrastruktur beschäftigt wären.

Auf Basis einer erstmalig einheitlichen Infrastruktur durch das Rechenzentrum können zudem vereinfacht trägerübergreifende Entwicklungsprojekte durchgeführt werden.

Das gemeinsame Rechenzentrum legt damit auch die Basis für die Arbeiten im Rahmen der Modernisierung von rvSystem innerhalb des Multiprojektes rvEvolution.

[rvEvolution]

Mit dem trägerübergreifenden Multiprojekt rvEvolution sorgen wir bis 2026 für eine Modernisierung unseres aktuellen Kernsystems rvSystem.

Die aktuell angestoßenen Maßnahmen für die Prozessoptimierungen und die digitale Transformation werden hier bestmöglich integriert – ebenso unsere Onlinedienste für unsere Versicherten.

Wir wollen mit dem neuen System folgende vier Ziele erreichen:

1. Das wir unseren Kunden künftig personalisierte Angebote schnell, sicher und digital zur Verfügung stellen können.
2. Das wir künftig noch stärker automatisierte Geschäftsprozesse aufsetzen können, um die Kolleginnen und Kollegen in der Sachbearbeitung bestmöglich zu entlasten.
3. Das wir die Anforderungen unserer Versicherten sowie Rentnerinnen und Rentner und die der Politik künftig noch flexibler und schneller umsetzen können.
4. Dass das künftige Programmsystem für unsere Mitarbeitenden intuitiv zu bedienen ist und sie bestmöglich bei der Arbeit unterstützt.

Das ist eine Mammutaufgabe, für die wir die Unterstützung der gesamten DRV benötigen. Gelingt uns dies, macht auch diese Maßnahme uns – die DRV, als Teil der kritischen Infrastruktur – ein Stück weit sicherer.

[Folgen des Angriffskriegs auf die Ukraine]

Meine Damen und Herren,

neben den allgemeinen Herausforderungen bzgl. der Informationssicherheit, müssen wir nun auch mit den Auswirkungen des Angriffskrieges Russlands auf die Ukraine umgehen. Dies betrifft nicht nur verstärkte Cyber-Angriffe in Deutschland, die Russland zugeordnet werden können, sondern weitere ganz unterschiedliche Themen, über die ich Sie abschließend noch informieren möchte.

So ist zum Beispiel eine Einschränkung der Energieversorgung der DRV Bund sehr wahrscheinlich.

Gerade Ostdeutschland und insbesondere Berlin-Brandenburg ist momentan bei raffinierten Erdölprodukten

noch stark von russischen Importen abhängig. Denn die für Berlin-Brandenburg hauptversorgende Raffinerie Schwedt bezieht bisher ausschließlich russisches Erdöl. Sie muss nun sehr schnell auf andere Bezugsquellen umgestellt werden. Dies war auch Thema der Ost-Ministerpräsidentenkonferenz am vergangenen Montag, gemeinsam mit Bundeskanzler Scholz.

Das DRV Bund-Notfallmanagement hat für solch einen Versorgungsengpass oder -ausfall einen Notfallplan erstellt. Bei regelmäßigen Übungen beziehungsweise Tests wird dieser Notfallplan jeweils an die neuesten Entwicklungen angepasst.

Eine größere Herausforderung könnte ebenso die Papierversorgung werden. Etwa 80 Prozent der Industrie zur Herstellung des bei uns benötigten Papiers sind in der Ukraine angesiedelt. Momentan steigen die Preise, Lieferunterbrechungen und -ausfälle sind wahrscheinlich.

Das beschränkt vor allem die Bestellmenge beim Papier, welches z. B. für das Verschicken der Rentenbescheide benötigt wird.

Die DRV Bund stockt aktuell ihren Lagerbestand auf und sucht zudem gemeinsam mit den Datenschutz-Behörden, anderen SV-Trägern und den Ministerien nach Lösungen, wie gültige Bescheide sicher an die Versicherten digital verschickt werden können.

Alle diese Themen und noch weitere mehr, werden in der DRV Bund durch einen extra dafür eingerichteten Arbeitsstab Ukraine koordiniert, der bereits wenige Tage nach Kriegsbeginn eingesetzt wurde.

[Schluss]

Meine Damen und Herren,

die Digitalisierung mit all ihren Vorzügen wird weiter voranschreiten. Das ist gut so. Sollten wir dabei aber die Informationssicherheit vernachlässigen, werden wir niemals das volle Potenzial der Digitalisierung ausnutzen können.

Deshalb: **Digitalisierung braucht Sicherheit**. Für die Deutsche Rentenversicherung mit ihren millionenfachen Rentenkonten ist dies Auftrag, Anspruch und Verantwortung zugleich. Informationssicherheit hat Vorrang, sie ist die Grundlage all unserer Digitalisierungsprojekte.

Wer digital und digital-sicher gut aufgestellt ist, kommt besser durch Krisen. Gerade im öffentlichen Sektor ist eine sichere Digitalisierung praktizierte Krisenvorsorge.

Nehmen wir also das diesjährige Motto des vom BSI ausgerichteten Deutschen IT-Sicherheitskongresses wörtlich: „**Cyber-Sicherheit ist Chefinnen- und**

Chefsache“. Die Selbstverwaltung und das Direktorium der DRV Bund stehen hier in der Verantwortung.

Vielen Dank!