Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Bericht des Rechnungshofes

Register im Hauptverband der österreichischen Sozialversicherungsträger; Follow–up–Überprüfung

Reihe BUND 2017/39

IMPRESSUM

Herausgeber: Rechnungshof
1031 Wien,
Dampfschiffstraße 2
http://www.rechnungshof.gv.at

Redaktion und Grafik: Rechnungshof
Herausgegeben: Wien, im Oktober 2017

AUSKÜNFTE

Rechnungshof
Telefon (+43 1) 711 71 - 8644
Fax (+43 1) 712 49 17
E-Mail presse@rechnungshof.gv.at

facebook/RechnungshofAT
Twitter: @RHSprecher

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
ASVG	Allgemeines Sozialversicherungsgesetz, BGBl. Nr. 189/1955 i.d.g.F.
BKA	Bundeskanzleramt
BMASK	Bundesministerium für Arbeit, Soziales und Konsumentenschutz
BMI	Bundesministerium für Inneres
bspw.	beispielsweise
bzw.	beziehungsweise
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSO	Chief Security Officer
GZ	Geschäftszahl
i.d.(g.)F.	in der (geltenden) Fassung
inkl.	inklusive
IT	Informationstechnologie
RH	Rechnungshof
SBBG	Sozialbetrugsbekämpfungsgesetz, BGBl. I Nr. 113/2015
SV	Sozialversicherung
TZ	Textzahl(en)
u.a.	und andere(n)m
Z	Ziffer
z.B.	zum Beispiel

Wirkungsbereich

Bundesministerium für Arbeit, Soziales und Konsumentenschutz

Register im Hauptverband der österreichischen Sozialversicherungsträger; Follow–up–Überprüfung

Kurzfassung

Prüfungsziel

Der RH überprüfte von September bis November 2016 beim BMASK und beim Hauptverband der österreichischen Sozialversicherungsträger die Umsetzung der Empfehlungen, die er bei einer vorangegangenen Gebarungsüberprüfung zum Thema „Register im Hauptverband der österreichischen Sozialversicherungsträger“ abgegeben hatte. Der in der Reihe Bund 2014/8 veröffentlichte Bericht wird in der Folge als Vorbericht bezeichnet. Zur Verstärkung der Wirkung seiner Empfehlungen hatte der RH im Jahr 2015 deren Umsetzungsstand beim BMASK und beim Hauptverband der österreichischen Sozialversicherungsträger nachgefragt. Das Ergebnis dieses Nachfrageverfahrens hatte er in seinem Bericht Reihe Bund 2015/18 veröffentlicht. Der überprüfte Zeitraum der nunmehrigen Follow–up–Überprüfung umfasste die Jahre 2014 bis 2016. Das BMASK setzte von fünf Empfehlungen vier vollständig und eine teilweise um; der Hauptverband der österreichischen Sozialversicherungsträger setzte von acht Empfehlungen vier vollständig und vier teilweise um. **(TZ 1**, **TZ 11**)

Früherkennung von Sozialbetrug durch Scheinfirmen

Das Sozialbetrugsbekämpfungsgesetz sowie die Änderung des Allgemeinen Sozialversicherungsgesetzes legten nunmehr fest, dass Daten über natürliche und juristische Personen verarbeitet werden sollten, wenn sich Anhaltspunkte für das Vorliegen von Sozialbetrug ergaben. Weiters wurden die Krankenversicherungsträger dazu verpflichtet, eine Risiko– und Auffälligkeitsanalyse im Dienstgeberbereich zur Ergreifung von Maßnahmen gegen Versicherungsmissbrauch durchzuführen. (**TZ 2**, **TZ 3**)

Cyber Sicherheitsstrategie der Sozialversicherungsträger

Der Hauptverband entwickelte Regelungen zur Cyber Sicherheitsstrategie für den Bereich der Sozialversicherung. Ebenso wurde ein Sozialversicherungs CERT (Computer Emergency Response Team) gegründet, an der Erstellung des Sicherheitsgesamtbildes der Sozialversicherung gearbeitet und von der Trägerkonferenz eine Sicherheitsrichtlinie zum Krisenmanagement beschlossen. (**TZ 5**, **TZ 6**, **TZ 7**, **TZ 8**, **TZ 10**)

Das Gremium der Sicherheitsverantwortlichen erarbeitete Sicherungs– und Schutzstandards, für die allerdings noch keine verbindliche Kontrolle eingerichtet war. (**TZ 9**)

Kenndaten

Register im Hauptverband der österreichischen Sozialversicherungsträger	
Bezeichnung des Registers	**Rechtsgrundlagen**
Zentrale Partnerverwaltung (ZPV)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Zentrale Versicherungsdatei (ZVD)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Zugriffsprotokolle der Online–Verarbeitung des Hauptverbandes (ZUP)	Datenschutzgesetz 2000 i.d.g.F.
Berechtigungssystem für Standardprodukte (BERE)	Datenschutzgesetz 2000 i.d.g.F.
Dokumentation des österreichischen Sozialversicherungsrechts (SozDok)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Amtliche Verlautbarungen (AVI)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Honorarordnungsverwaltung (HONO)	Bundesgesetz über die Dokumentation im Gesundheitswesen i.d.g.F.
	Verordnung zum Gesundheitsdokumentationsgesetz vom 30. Juni 2010
Betriebliche (Mitarbeiter–) Vorsorge im Hauptverband (BMV)	Betriebliches Mitarbeiter– und Selbständigenvorsorgegesetz – BMSVB
Erstattungskodex Basisdatenbank (EKO–BDB)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Elektronisches Pensionskonto (ePK)	Allgemeines Pensionsgesetz i.d.g.F.
Zentraler Patientenindex Z–PI	ELGA–Gesetz (Gesundheitstelematikgesetz 2012)
Leistungsinformation für Versicherte (LIVE)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
	Gewerbliches Sozialversicherungsgesetz i.d.g.F.
	Bauern–Sozialversicherungsgesetz i.d.g.F.
	Beamten–Kranken– und Unfallversicherungsgesetz i.d.g.F.
Familienbeihilfedatenbank (FB)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
	Gewerbliches Sozialversicherungsgesetz i.d.g.F.
	Bauern–Sozialversicherungsgesetz i.d.g.F.
	Familienlastenausgleichsgesetz 1967 i.d.g.F.
e–card–Konsultationssystem (KONS)	Allgemeines Sozialversicherungsgesetz i.d.g.F.
Anspruchsdatenbank (ANSP)	Allgemeines Sozialversicherungsgesetz i.d.g.F.

Quelle: Hauptverband der österreichischen Sozialversicherungsträger

Prüfungsablauf und –gegenstand

1 (1) Der RH überprüfte von September bis November 2016 beim BMASK und beim Hauptverband der österreichischen Sozialversicherungsträger (**Hauptverband**) die Umsetzung der Empfehlungen zu den zwei Schwerpunkten „Früherkennung von Sozialbetrug durch Scheinfirmen“ und „Cyber Sicherheitsstrategie der Sozialversicherungsträger“, die er bei einer vorangegangenen Gebarungsüberprüfung zum Thema „Register im Hauptverband der österreichischen Sozialversicherungsträger“

abgegeben hatte. Der in der Reihe Bund 2014/8 veröffentlichte Bericht wird in der Folge als Vorbericht bezeichnet.

(2) Der RH hatte zur Verstärkung der Wirkung seiner Empfehlungen im Jahr 2015 deren Umsetzungsstand beim BMASK und dem Hauptverband nachgefragt. Das Ergebnis dieses Nachfrageverfahrens hatte er in seinem Bericht Reihe Bund 2015/18 veröffentlicht.

(3) Der überprüfte Zeitraum der nunmehrigen Follow–up–Überprüfung umfasste die Jahre 2014 bis 2016.

(4) Zu dem im März 2017 übermittelten Prüfungsergebnis nahmen der Hauptverband und das BMASK im April 2017 Stellung. Der Hauptverband teilte in seiner Stellungnahme mit, dass er bestrebt sei, die Anregungen des RH bei seiner weiteren Vorgangsweise zu berücksichtigen. Das BMASK verwies in seiner Stellungnahme darauf, dass die an das Ministerium gerichtete Empfehlung in Umsetzung sei, aufgrund der Größe des Projektes und des damit verbundenen zeitlichen und organisatorischen Aufwands jedoch noch nicht abgeschlossen werden konnte. Eine Gegenäußerung des RH war daher nicht erforderlich.

Früherkennung von Scheinfirmen

2.1 (1) Der RH hatte dem BMASK und dem Hauptverband in seinem Vorbericht (TZ 10) empfohlen, mögliche Indikatoren bezüglich Aktivierung einer Scheinfirma zu definieren und die Register der Sozialversicherung auf diese – unter Beachtung des Datenschutzes und der rechtlichen Rahmenbedingungen – automationsunterstützt auszuwerten.

(2) Im Nachfrageverfahren hatten das BMASK und der Hauptverband darauf hingewiesen, dass diese Empfehlung mit dem Inkrafttreten des Sozialbetrugsbekämpfungsgesetzes (**SBBG**) per 1. Jänner 2016 sowie mit einer Änderung des Allgemeinen Sozialversicherungsgesetzes (§ 42b **ASVG**) umgesetzt sei.

(3) Der RH stellte nunmehr fest, dass gemäß SBBG bzw. Änderung des ASVG eine Sozialbetrugsdatenbank zum Zweck der Erfassung und erleichterten Ermittlung von Sozialbetrugsfällen zu führen war. Darin waren die Daten über natürliche und juristische Personen bei Anhaltspunkten über das Vorliegen von Sozialbetrug zu verarbeiten. Weiters wurden die Krankenversicherungsträger dazu verpflichtet, eine Risiko– und Auffälligkeitsanalyse im Dienstgeberbereich zur Ergreifung von Maßnahmen gegen Versicherungsmissbrauch durchzuführen. Dabei war unter Verwendung von bestimmten Versicherungs– und Dienstgeberdaten insbesondere nach Indikatoren (Daten) für

– Schwarzarbeitsverdacht,

– Scheinanmeldungen,

– Versichertenströme,

– Dienstgeberzusammenhänge,

– Insolvenzgefahr sowie

– Melde– und Beitragszahlungsverhalten

zu prüfen. Die Oberösterreichische Gebietskrankenkasse hatte als Kompetenzzentrum diese automatisationsunterstützten Analysen zu verknüpfen und die Ergebnisse allen beteiligten Stellen[1] zur Verfügung zu stellen.

2.2 Das BMASK und der Hauptverband setzten die Empfehlung des RH um, weil die entsprechenden Bundesgesetze Indikatoren (Daten) hinsichtlich Scheinfirmen definierten und eine automatisationsunterstützte Auswertung durch die Oberösterreichische Gebietskrankenkasse als Kompetenzzentrum dieser Analysen festlegten.

3.1 (1) Der RH hatte dem BMASK und dem Hauptverband in seinem Vorbericht (TZ 11) empfohlen, die von Expertinnen bzw. Experten zur Früherkennung von geplantem Sozialbetrug (Scheinfirma) definierten Indikatoren (Daten) zeitgerecht in die Register einzutragen und notwendigenfalls einen diesbezüglichen Gesetzesvorschlag an den Gesetzgeber heranzutragen.

(2) Im Nachfrageverfahren hatten das BMASK und der Hauptverband mitgeteilt, dass diese Empfehlung mit dem Inkrafttreten (per 1. Jänner 2016) des SBBG sowie mit einer Änderung des ASVG (§ 42b ASVG) umgesetzt sei.

(3) Der RH stellte nunmehr fest, dass auf Grundlage des SBBG bzw. der Änderung des ASVG Risiko– und Auffälligkeitsanalysen über Daten im Dienstgeberbereich von den Sozialversicherungsträgern durchgeführt wurden. Das SBBG verpflichtete die Kooperations–[2] und Informationsstellen[3] außerdem zu einer möglichst frühzeitigen Meldung bei Verdacht auf Sozialbetrug.

---

[1] Krankenversicherungsträger, Abgabenbehörden des Bundes, Hauptverband

[2] Finanzstraf– und Abgabenbehörden des Bundes, Krankenversicherungsträger, Bauarbeiter–Urlaubs– und Abfertigungskasse, Insolvenz–Entgelt–Fonds–Service GmbH und Sicherheitsbehörden

[3] Bezirksverwaltungsbehörden, die Gewerbebehörden, Arbeitsinspektion und Arbeitsmarktservice

3.2 Das BMASK und der Hauptverband setzten die Empfehlung des RH um, weil die entsprechenden Bundesgesetze Indikatoren (Daten) zur Früherkennung von geplantem Sozialbetrug definierten und eine möglichst frühzeitige Meldung sowie die Erfassung in einer Sozialbetrugsdatenbank bei Verdacht auf Sozialbetrug festlegten.

Gesetzliche Regelung zur zentralen Umsetzung einer Cyber Sicherheitsstrategie

4.1 (1) Der RH hatte dem BMASK in seinem Vorbericht (TZ 13) empfohlen, eine gesetzliche Regelung zur zentralen Umsetzung einer Cyber Sicherheitsstrategie in der Sozialversicherung an den Gesetzgeber heranzutragen.

(2) Im Nachfrageverfahren hatte das BMASK vorgebracht, dass diese Empfehlung inhaltlich auf Basis der bestehenden Gesetzeslage und Struktur bereits weitgehend umgesetzt sei. Da die Arbeiten des Hauptverbands gemeinsam mit den Sozialversicherungsträgern an der Umsetzung einer Cyber Sicherheitsstrategie für den gesamten Bereich der österreichischen Sozialversicherung bereits weit fortgeschritten waren, bestünde nicht mehr die Notwendigkeit einer gesetzlichen Regelung.

(3) Der RH stellte nunmehr fest, dass der Hauptverband auf Grundlage seiner diesbezüglichen Kompetenz[4] für den Bereich der Sozialversicherung Richtlinien bzw. Regelungen zur Cyber Sicherheitsstrategie[5] entwickelte. Für die Umsetzung und Weiterentwicklung dieser Strategie war ein sozialversicherungsweites Gremium verantwortlich, das sich aus den jeweiligen Sicherheitsverantwortlichen (CISO bzw. CSO) der einzelnen Sozialversicherungsträger zusammensetzte.

4.2 Der RH wertete seine Empfehlung an das BMASK als umgesetzt, weil der Hauptverband bereits auf Basis der bestehenden Kompetenz verbindliche inhaltliche Richtlinien bzw. Regelungen zur zentralen Umsetzung einer Cyber Sicherheitsstrategie in der Sozialversicherung entwickelte.

[4] § 31 Abs. 5 Z 4 ASVG

[5] Informationssicherheitsstrategie der österreichischen Sozialversicherung (Entwurf), SV–Sicherheitsrichtlinie 2016, Mobile Device Management/Strategie (Entwurf), Handbuch Zugriffskontrolle (Entwurf)

Umfassende Cyber Sicherheitsstrategie für den Sozialversicherungsbereich

5.1 (1) Der RH hatte dem BMASK und dem Hauptverband in seinem Vorbericht (TZ 3 und 12) empfohlen, zur Abwehr und Bewältigung von Cyber Sicherheitsvorfällen eine umfassende Sicherheitsstrategie für den Sozialversicherungsbereich zu erarbeiten und umzusetzen.

(2) Im Nachfrageverfahren hatten das BMASK und der Hauptverband darauf hingewiesen, dass diese Empfehlung durch die Entwicklung einer umfassenden Cyber Sicherheitsstrategie, der Einrichtung eines Sicherheitsverantwortlichen und des gemeinsamen beratenden Gremiums dieser Sicherheitsverantwortlichen aller Sozialversicherungsträger sowie einzelner Strategieentwicklungen (z.B. Mobile Secure–Management) umgesetzt sei.

(3) Der RH stellte nunmehr fest, dass der Hauptverband Regelungen zu einer Cyber Sicherheitsstrategie für den Bereich der Sozialversicherung teilweise entwickelte. So wurden die SV–Sicherheitsrichtlinie sowie Konzepte bspw. zur Informationssicherheitsstrategie der österreichischen Sozialversicherung, zur Zugriffskontrolle und zum Mobile Device Management ausgearbeitet. Für die Umsetzung und Weiterentwicklung dieser Strategie war ein sozialversicherungsweites Gremium verantwortlich, das die Umsetzung der Sicherheitsstrategie bereits einleitete (siehe **TZ 9**).

5.2 Der RH wertete seine Empfehlung an das BMASK und den Hauptverband als teilweise umgesetzt, weil die Ausarbeitung der Regelungen zur Cyber Sicherheitsstrategie in der Sozialversicherung und deren Umsetzung noch nicht abgeschlossen war.

Der RH hielt daher seine Empfehlung aufrecht, zur Abwehr und Bewältigung von Cyber Sicherheitsvorfällen eine umfassende Sicherheitsstrategie für den Sozialversicherungsbereich zu erarbeiten und umzusetzen.

Einrichtung eines Sozialversicherungs CERT

6.1 (1) Der RH hatte dem BMASK und dem Hauptverband in seinem Vorbericht (TZ 15) empfohlen, zur operativen Bearbeitung der Cyber Sicherheitsbereiche in der Sozialversicherung ein Sozialversicherungs CERT (Computer Emergency Response Team) im Rahmen der Zielsteuerung einzurichten und in Abstimmung mit dem BMASK der Trägerkonferenz zur Beschlussfassung vorzulegen.

(2) Im Nachfrageverfahren hatten das BMASK und der Hauptverband mitgeteilt, dass die Trägerkonferenz am 7. Oktober 2014 beschlossen habe, ein Sozialversicherungs CERT zu gründen. Seit Mitte 2015 sei dieses CERT operativ im Einsatz und unterstütze den Hauptverband, die Sozialversicherungsträger, die IT–Services der Sozialversicherung GmbH, die Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. und die SVD Büromanagement GmbH und stünde auch in enger Verbindung mit dem Government CERT. Eine Teilnahme am CERT Verbund des BKA werde angestrebt.

(3) Der RH stellte nunmehr fest, dass die Aufgaben des Sozialversicherungs CERT mittlerweile ausgebaut wurden und dieses nun auch Mitglied des CERT Verbunds des BKA war.

6.2 Das BMASK und der Hauptverband setzten die Empfehlung des RH um, weil ein Sozialversicherungs CERT etabliert wurde, das zwischenzeitlich auch dem CERT Verbund des BKA angehörte.

Prioritäre Aufarbeitung der Cyber Sicherheitsinhalte und verbindliche Umsetzung

7.1 (1) Der RH hatte dem Hauptverband in seinem Vorbericht (TZ 14) empfohlen, die Inhalte der Cyber Sicherheit nach Priorität gereiht aufzuarbeiten und verbindlich umzusetzen.

(2) Im Nachfrageverfahren hatte der Hauptverband mitgeteilt, dass im Rahmen des sozialversicherungsweiten Gremiums der jeweiligen Sicherheitsverantwortlichen (CISO bzw. CSO) der einzelnen Sozialversicherungsträger ein Informationssicherheitsgesamtbild der Sozialversicherung erstellt werde. Auf Basis der dabei erkannten Handlungsfelder würden mögliche Verbesserungen der Gesamtsicht ausgearbeitet und in Folge verbindlich umgesetzt.

(3) Der RH stellte nunmehr fest, dass an der Erstellung eines risikoorientierten Sicherheitsgesamtbildes der Sozialversicherung gearbeitet wurde. Weitere prioritäre Maßnahmen zur Hebung der Gesamtsicherheit waren für das Jahr 2017 geplant. So wurden Arbeitsgruppen zu Themenbereichen wie bspw. der sozialversicherungsweiten Informationssicherheitsstrategie, dem sozialversicherungsweiten Sicherheitsgesamtbild, dem sicheren Datenaustausch oder dem Identitätsmanagement beauftragt (siehe **TZ 9**).

7.2 Der RH wertete seine Empfehlung an den Hauptverband als teilweise umgesetzt, weil an der Erstellung des Sicherheitsgesamtbildes der Sozialversicherung gearbei-

tet wurde, aber weitere prioritäre Maßnahmen zur Hebung der Gesamtsicherheit noch ausständig waren.

Der RH hielt daher seine Empfehlung aufrecht, die Inhalte der Cyber Sicherheit umfassend und nach Priorität gereiht aufzuarbeiten und verbindlich umzusetzen.

Einrichtung eines Krisenmanagements

8.1 (1) Der RH hatte dem Hauptverband in seinem Vorbericht (TZ 16) empfohlen, ein Krisenmanagement für die Sozialversicherung einzurichten. Dieses hätte die Risikoanalysen durchzuführen, Kontinuitätspläne zu entwickeln und Krisenübungen abzuhalten.

(2) Laut Mitteilung des Hauptverbands im Nachfrageverfahren habe er auf Basis einer Richtlinie des BMI („Richtlinie für das Führen im Katastropheneinsatz“) im Jahr 2014 ein Krisenmanagement etabliert und bereits zwei Krisenübungen durchgeführt. Eine weitere Krisenübung sei geplant. Bei den einzelnen Sozialversicherungsträgern sei ebenfalls ein Krisenmanagement eingerichtet und es seien Krisenübungen geplant bzw. würden solche durchgeführt.

(3) Der RH stellte nunmehr fest, dass der Hauptverband im Zuge des Krisenmanagements Kontinuitätspläne entwarf und Krisenübungen abhielt.[6] Die Trägerkonferenz der Sozialversicherung verabschiedete die „Sicherheitsrichtlinie für die gesetzliche Sozialversicherung“ (SV–Sicherheitsrichtlinie 2016 – SV–SR 2016) und setzte diese am 1. Juli 2016 in Kraft.

Diese Richtlinie beinhaltete Festlegungen zur Bewältigung von Störfällen, Notfällen und sozialversicherungsweiten Krisen und sah vor, dass der Hauptverband und alle Sozialversicherungsträger bis Mitte 2017 ein Konzept zur Bewältigung von lokalen Krisen zu erstellen, aktuell zu halten und zu üben hatten. Außerdem waren dadurch der Hauptverband und jeder einzelne Sozialversicherungsträger dazu verpflichtet, bis Ende 2018 an mindestens einer organisationsübergreifenden Übung teilzunehmen.

Ein Risikomanagement war im Aufbau. Für das Jahr 2017 war die Durchführung umfangreicher Risikoanalysen geplant.

8.2 Der RH wertete seine Empfehlung an den Hauptverband als teilweise umgesetzt, weil der Hauptverband bereits ein Krisenmanagement einrichtete und Krisenübun-

[6] Hauptverband: 19.12.2014, 27.02.2015, 25.09.2015; SV–weit: 1.12.2016

gen durchführte, aber der SV–weite Kontinuitätsplan erst als Entwurf vorlag und das Risikomanagement noch im Aufbau war.

Der RH hielt daher seine Empfehlung aufrecht, ein Krisenmanagement für die Sozialversicherung einzurichten. Dieses hätte die Risikoanalysen durchzuführen, die Kontinuitätspläne weiterzuentwickeln und Krisenübungen abzuhalten.

Sicherungs– und Schutzstandards mit verbindlicher Kontrolle

9.1 (1) Der RH hatte dem Hauptverband in seinem Vorbericht (TZ 3 und 17) empfohlen, Sicherungs– und Schutzstandards für die Einrichtungen der Sozialversicherung vorzusehen, dem jeweiligen Aufgabengebiet und den verwendeten Daten anzupassen und dessen verbindliche Kontrolle einzurichten.

(2) Im Nachfrageverfahren hatte der Hauptverband mitgeteilt, dass eine ständige Arbeitsgruppe der Verantwortlichen für Informationssicherheit aus dem Hauptverband, den Sozialversicherungsträgern, der IT–Services der Sozialversicherung GmbH, der Sozialversicherungs–Chipkarten Betriebs– und Errichtungsgesellschaft m.b.H. und der SVD Büromanagement GmbH gegründet sei, um u.a.

- sich mit Bedrohungen und Gegenmaßnahmen zur allgemeinen Computersicherheit und Cyber Sicherheit zu befassen,
- Informationssicherheitsrisiken zu dokumentieren, zu beurteilen und den Entscheidungsgremien präventive Maßnahmen vorzuschlagen,
- für Informationsaustausch zu sorgen,
- Erfahrungen aus Informationssicherheitsvorfällen zu beachten,
- Vorschläge für trägerübergreifende Prozesse zu Themen der Informationssicherheit zu erarbeiten,
- Mindeststandards für Informationssicherheit vorzuschlagen

und der Trägerkonferenz hierüber entsprechend zu berichten.

(3) Der RH stellte nunmehr fest, dass die ständig eingerichtete Arbeitsgruppe der Verantwortlichen für Informationssicherheit (CISOs) mehrere Sitzungen pro Jahr abhielt und Arbeitsgruppen mit folgenden Themen beauftragt hatte:

- Krisenvorsorge,
- sozialversicherungsweite Informationssicherheitsstrategie,
- Hebung des Informationssicherheitsbewusstseins (Awareness),
- sicherer Datenaustausch,
- Identitiy Management (Identitätsmanagement) und
- sozialversicherungsweites Sicherheitsgesamtbild.

Eine weitere Arbeitsgruppe zur Erarbeitung von Empfehlungen zur Software–Robustheit war in Gründung.

Für die Sicherungs– und Schutzstandards richtete der Hauptverband allerdings noch keine verbindliche Kontrolle ein.

9.2 Der RH wertete seine Empfehlung an den Hauptverband als teilweise umgesetzt, weil der Hauptverband zwar eine ständige Arbeitsgruppe zur Befassung mit Sicherungs– und Schutzstandards etablierte und weitere Arbeitsgruppen für die Erarbeitung konkreter Verbesserungsvorschläge hinsichtlich Informationssicherheit beauftragte, jedoch eine verbindliche Kontrolle der Sicherungs– und Schutzstandards noch fehlte.

Der RH hielt daher seine Empfehlung aufrecht, eine verbindliche Kontrolle der Sicherungs– und Schutzstandards einzurichten.

Meldepflicht bei Cyber Sicherheitsvorfällen

10.1 (1) Der RH hatte dem Hauptverband in seinem Vorbericht (TZ 18) empfohlen, eine verbindliche Meldepflicht bei Cyber Sicherheitsvorfällen vorzusehen. Die Bewertung bzw. Einstufung des jeweiligen IT–Sicherheitsvorfalls sollte den Sicherheitsfachleuten des Sozialversicherungs CERT vorbehalten sein. Anhand definierter Strukturen und Prozesse wären alle potenziell gefährdeten Einrichtungen der Sozialversicherung zu informieren und entsprechende Maßnahmen zu empfehlen.

(2) Das BMASK und der Hauptverband hatten im Nachfrageverfahren mitgeteilt, dass das seit Mitte 2015 operative Sozialversicherungs CERT als zentrale Meldestelle für Informationssicherheitsvorfälle fungiere und bei der Schadensbehebung unterstütze. Weiters sammle es Sicherheitswarnungen, prüfe deren Relevanz für die Sozialversicherung und warne die potenziell betroffenen Organisationen.

(3) Der RH stellte nunmehr fest, dass der Hauptverband und alle Sozialversicherungsträger gemäß § 5 Abs. 1 SV–Sicherheitsrichtlinie 2016 Krisen an das Sozialversicherungs CERT zu melden hatten.[7] Die Organisationen der Sozialversicherung meldeten auch Cyber Sicherheitsvorfälle gemäß einem Beschluss des sozialversicherungsweiten Gremiums der jeweiligen Sicherheitsverantwortlichen an das Sozialversicherungs CERT. Dieses prüfte die Sicherheitsvorfälle auf deren Relevanz und warnte die potenziell betroffenen Organisationen.

10.2 Der Hauptverband setzte die Empfehlung des RH um, weil im Krisenfall eine Meldepflicht an das Sozialversicherungs CERT bestand. Weiters wurden auch Cyber Sicherheitsvorfälle von den Organisationen der Sozialversicherung gemeldet, auf deren Relevanz für die Sozialversicherung geprüft und die potenziell betroffenen Organisationen gewarnt.

[7] § 5 Abs. 1 der SV–Sicherheitsrichtlinie 2016 tritt mit 1. Juli 2017 in Kraft

Schlussempfehlungen

11 Der RH stellte fest, dass das BMASK von fünf an das Ressort gerichteten überprüften Empfehlungen des RH vier vollständig und eine teilweise umgesetzt hatte. Der Hauptverband der österreichischen Sozialversicherungsträger setzte von acht an ihn gerichteten, vom RH überprüften Empfehlungen vier vollständig und vier teilweise um.

Umsetzungsgrad der Empfehlungen des Vorberichts Reihe Bund 2014/8			
TZ	**Vorbericht**	**Follow–up–Überprüfung**	
	Empfehlungsinhalt	**TZ**	**Umsetzungsgrad**
BMASK			
13	Hinwirken auf gesetzliche Regelung zur zentralen Umsetzung einer Cyber Sicherheitsstrategie in der Sozialversicherung	4	**umgesetzt**
BMASK und Hauptverband der österreichischen Sozialversicherungsträger			
10	Definition von Indikatoren bezüglich Aktivierung einer Scheinfirma und Auswertung der Register der Sozialversicherung auf deren Basis	2	**umgesetzt**
11	zeitgerechter Eintrag der für Sozialbetrug definierten Indikatoren in die Register	3	**umgesetzt**
3, 12	Erarbeitung und Umsetzung einer Cyber Sicherheitsstrategie für den Sozialversicherungsbereich	5	**teilweise umgesetzt**
15	Einrichtung eines Sozialversicherungs CERT zur operativen Bearbeitung der Cyber Sicherheitsbereiche in der Sozialversicherung	6	**umgesetzt**
Hauptverband der österreichischen Sozialversicherungsträger			
14	verbindliche Umsetzung der Inhalte der Cyber Sicherheit nach Priorität	7	**teilweise umgesetzt**
16	Einrichtung eines Krisenmanagements für die Sozialversicherung mit Risikoanalysen, Kontinuitätsplänen und Krisenübungen	8	**teilweise umgesetzt**
3, 17	aufgabenangepasste Sicherungs– und Schutzstandards für die Einrichtungen der Sozialversicherung inklusive verbindlicher Kontrolle	9	**teilweise umgesetzt**
18	verbindliche Meldepflicht bei Cyber Sicherheitsvorfällen für alle Einrichtungen der Sozialversicherung; Bewertung der IT–Sicherheitsvorfälle nur durch Sicherheitsfachleute des Sozialversicherungs CERT	10	**umgesetzt**

Anknüpfend an den Vorbericht hob der RH folgende Empfehlungen hervor:

BMASK und Hauptverband der österreichischen Sozialversicherungsträger

(1) Zur Abwehr und Bewältigung von Cyber Sicherheitsvorfällen wäre eine umfassende Sicherheitsstrategie für den Sozialversicherungsbereich zu erarbeiten und umzusetzen. (**TZ 5**)

Hauptverband der österreichischen Sozialversicherungsträger

(2) Die Inhalte der Cyber Sicherheit wären umfassend und nach Priorität gereiht aufzuarbeiten und verbindlich umzusetzen. (TZ 7)

(3) Ein Krisenmanagement für die Sozialversicherung wäre einzurichten. Dieses hätte die Risikoanalysen durchzuführen, Kontinuitätspläne weiterzuentwickeln und Krisenübungen abzuhalten. (TZ 8)

(4) Eine verbindliche Kontrolle für Sicherungs– und Schutzstandards wäre einzurichten. (TZ 9)

Rechnungshof Österreich

Wien, im Oktober 2017
Die Präsidentin:

Dr. Margit Kraker