Bundesamt
für Soziale Sicherung

Bundesamt für Soziale Sicherung, Friedrich-Ebert-Allee 38, 53113 Bonn

Alle bundesunmittelbaren Sozialversicherungsträger
- ausschließlich per E-Mail -

nachrichtlich:

Alle Verbände der bundesunmittelbaren Sozialversicherungsträger, Aufsichtsbehörden der Länder, Bundesministerium für Gesundheit, Bundesministerium Arbeit und Soziales

Friedrich-Ebert-Allee 38, 53113 Bonn
Tel. +49 1517 0257396
Referat 116
bearbeitet von:
Joel Vogt
referat116@bas.bund.de
www.bundesamtsozialesicherung.de

Bonn, 20. September 2023

GZ: 116 – 1010801#00002#0007

(bei Antwort bitte angeben)

Informationstechnik im Aufsichtsbereich – hier: Umgang mit IT-Sicherheitsvorfällen

Sehr geehrte Damen und Herren,

in der letzten Zeit ist es vermehrt zu IT-Sicherheitsvorfällen gekommen, von denen Sozialversicherungsträger betroffen waren. Hierbei verstehen wir unter einem IT-Sicherheitsvorfall eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit Ihrer informationstechnischen Systeme, Komponenten oder Prozesse aufgrund eines Cyberangriffs, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von Ihnen betriebenen Infrastrukturen und angebotenen Leistungen geführt haben.

In der Folge führten die Sicherheitsvorfälle unter anderem dazu, dass die betroffenen Sozialversicherungsträger teilweise über einen längeren Zeitraum weder telefonisch noch elektronisch mit ihren Versicherten und dem Bundesamt für Soziale Sicherung (BAS) kommunizieren konnten. Sozialversicherungsträger tragen eine hohe Verantwortung für den Schutz von Sozialdaten aber auch für die Verfügbarkeit der Systeme, mit denen die Funktionsfähigkeit der Sozialen Sicherungssysteme sichergestellt werden. Sind die Vertraulichkeit der Sozialdaten und/oder die Verfügbarkeit der Systeme beeinträchtigt, wirkt sich dies nicht nur auf die Versicherten und den eigenen Geschäftsbetrieb aus, sondern auch auf das BAS. Zum einen stehen wir als Rechtsaufsichtsbehörde für die Öffentlichkeit und die Versicherten als Ansprechpartner zur Verfügung. Zum anderen müssen wir aber auch in Bezug auf unsere eigenen Verwaltungsaufgaben (RSA, diverse Fonds, Datenaustauschverfahren) handeln und Sicherheitsmaßnahmen prüfen. Daher

ist für das BAS eine schnelle Information durch die Sozialversicherungsträger zu einem bestehenden IT-Sicherheitsvorfall von großer Bedeutung.

Um für das Gesamtsystem der sozialen Sicherung die bestmögliche Krisenfestigkeit zu erzielen und damit wir als Rechtsaufsichtsbehörde und Verwaltungsbehörde unsere Aufgaben ordnungsgemäß wahrnehmen können, bitten wir, Folgendes zu beachten und in Ihren Maßnahmenplan aufzunehmen bzw. an uns zu übersenden:

1. Meldung eines IT-Sicherheitsvorfalls mit erheblicher Störung der Verfügbarkeit von Systemen und Leistungen

Bitte melden Sie **IT-Sicherheitsvorfälle aufgrund eines Cyberangriffs,** die zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von Ihnen betriebenen Infrastrukturen und angebotenen Leistungen führen oder führen können, unverzüglich dem BAS. Sollte der Vorfall an einem Wochenende oder an einem gesetzlichen Feiertag auftreten, bitten wir um eine Meldung bis zum Beginn des nächsten Werktags.

Für eine Meldung wenden Sie sich bitte an folgende E-Mail-Adresse:
E-Mail: Informationssicherheit@bas.bund.de

Kommunizieren Sie mit uns nur verschlüsselt über E-Mail. Nähere Informationen stehen auf unserer Internetseite.[1] Bitte verwenden Sie bei der E-Mail-Kommunikation das Nur-Text (plain text) Format und für Dateianhänge das PDF-Format.

Ist dieser Kommunikationskanal kompromittiert, nutzen Sie bitte folgende Telefonnummer: **+49 228 619-2222**
Die Servicezeiten für diese Rufnummer sind Montag bis Donnerstag 9 bis 15 Uhr, Freitag 9 bis 14 Uhr. Bitte unterlassen Sie eine Nutzung dieses Kontakts zu anderen Zwecken.

Wir bitten Sie, die Ihnen bekannten **Informationen zum IT-Sicherheitsvorfall so genau wie möglich anzugeben (z. B. Art, Zeitpunkt, Ausmaß und Ursache des Vorfalls, Auswirkungen auf die Verfügbarkeit von Diensten und Services gegenüber Versicherten, sowie Maßnahmen die bereits ergriffen wurden)**. Bitte benennen Sie die für den konkreten Vorfall bestehenden **Ansprechpartner mit entsprechenden Kontaktdaten**, die sicher funktionieren.

[1] https://www.bundesamtsozialesicherung.de/de/bundesamt-fuer-soziale-sicherung/kontakt/e-mail-verschluesselung/ > Dort: S/MIME Domain Key

Bitte beachten Sie, dass diese Meldung an das BAS Ihre Meldepflichten gegenüber dem BAS nach § 83a SGB X und gegenüber anderen Behörden wie dem BfDI und dem BSI unberührt lässt. Wir verweisen darüber hinaus in Bezug auf das Vorgehen bei einem IT-Sicherheitsvorfall auf die Informationen des BSI[2].

2. Kontaktdaten im Krisenfall

Soweit im Rahmen des IT-Sicherheitsvorfalls auch die üblichen Kontaktkanäle gestört sind, weichen die Sozialversicherungsträger auf alternative, vom eigenen System losgelöste Kontaktmöglichkeiten aus. Hierbei weisen wir Sie auf § 35 Abs. 1 Satz 1 SGB I (Sozialgeheimnis) und Art. 5 Abs. 1 lit. f DSGVO hin. Danach dürfen personenbezogene Daten nur in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Zum Schutz der Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten müssen öffentliche E-Mail-Diensteanbieter die Anforderungen der Technischen Richtlinie TR-03108 des Bundesamts für Sicherheit in der Informationstechnik einhalten. Sie als Träger der Sozialversicherung und Verantwortliche müssen sich davon überzeugen, dass die Anbieter öffentlicher E-Mail-Dienste hinreichende Garantien für die Einhaltung der Anforderungen der DSGVO und insbesondere der genannten Technischen Richtlinie bieten. Dies schließt auch die sichere Anbindung eigener Systeme und Endgeräte an die Diensteanbieter ein. Im Einzelnen weisen wir auf die Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021 hin[3].

Wir empfehlen Ihnen daher, alternative Kontaktmöglichkeiten bereits im Rahmen der Vorbereitung auf einen IT-Sicherheitsvorfall zu etablieren und diese in Ihre Notfall- und Krisenkommunikationspläne aufzunehmen.

3. Austausch von Notfallnummern

---

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html und
https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/service-fuer-kritis-betreiber_node.htmlhttps://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/unternehmen-und-organisationen_node.html und
https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/service-fuer-kritis-betreiber_node.html

[3] https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf

Im Falle eines IT-Sicherheitsvorfalls ist für uns eine schnelle Kontaktaufnahme mit Ihrem IT-Sicherheitsbeauftragten von großer Bedeutung. Wir bitten Sie daher bereits jetzt, um Übersendung der Kontaktdaten Ihres IT-Sicherheitsbeauftragten als auch um die Mitteilung der Notfallrufnummer/-n, unter der wir Sie im Bedarfsfall erreichen können der Form halber bis **zum 31. Oktober 2023**.

Telefonnummer: +49 228 619-1935
E-Mail: pg-adv2@bas.bund.de

Bitte kommunizieren Sie mit uns nur verschlüsselt über E-Mail. Nähere Informationen stehen auf unserer Internetseite.[4] Bitte verwenden Sie bei der E-Mail-Kommunikation das Nur-Text (plain text) Format und für Dateianhänge das PDF-Format.

4. Vorlage Ihres Kommunikationsplans für Notfälle

Verschiedene fachliche Anforderungen zielen auf die Erarbeitung eines Notfall- und Krisenkommunikationsplans ab (u. a. BSI-Standard 200-4, Kapitel 5.7). Ein Notfall- und Krisenkommunikationsplan sollte Standard bei jedem Träger sein. Bitte übermitteln Sie uns bis zum **31. Oktober 2023** eine Kopie Ihres Notfalls- und Krisenkommunikationsplans. **Soweit mit unserem Haus bereits eine andere Frist zur Übersendung der Unterlagen vereinbart wurde, hat diese weiterhin bestand. Die vorstehende Frist ist für Sie dann gegenstandslos.** Hintergrund dieser Bitte sind auch Beauftragungen externer Auftragsverarbeiter im Bereich der Leistungs- und Beitragssysteme, die im Krisenfall zu berücksichtigen sind. Bitte wenden Sie sich hierfür an:

Telefonnummer: +49 228 619-1935
E-Mail: pg-adv2@bas.bund.de

Bitte kommunizieren Sie mit uns nur verschlüsselt über E-Mail. Nähere Informationen stehen auf unserer Internetseite.[5] Bitte verwenden Sie bei der E-Mail-Kommunikation das Nur-Text (plain text) Format und für Dateianhänge das PDF-Format.

[4] https://www.bundesamtsozialesicherung.de/de/bundesamt-fuer-soziale-sicherung/kontakt/e-mail-verschluesselung/
[5] https://www.bundesamtsozialesicherung.de/de/bundesamt-fuer-soziale-sicherung/kontakt/e-mail-verschluesselung/

Sollten Sie Fragen haben oder eine Frist nicht einhalten können, bitten wir Sie, uns über die im Briefkopf genannten Möglichkeiten zu kontaktieren.

Die Herausforderung, die Krisenfestigkeit der Sozialen Sicherungssysteme gerade vor dem Hintergrund der voranschreitenden Digitalisierung sicherzustellen, kann nur gemeinsam gelingen. Wir bedanken uns für Ihre Unterstützung und Kooperation.

Mit freundlichen Grüßen

Im Auftrag
Romy Bromen