EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung der Informatiksicherheit der sedex-Plattform

Bundesamt für Statistik

EFK-22657 | inkl. Stellungnahme | 13. März 2023

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	317.22657
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Mit Nennung der männlichen Funktionsbezeichnung ist in diesem Bericht, sofern nicht anders gekennzeichnet, immer auch die weibliche Form gemeint.

Inhaltsverzeichnis

Das Wesentliche in Kürze **4**

1 Auftrag und Vorgehen **8**

1.1 Ausgangslage 8

1.2 Prüfungsziel und -fragen 8

1.3 Prüfungsumfang und -grundsätze 8

1.4 Unterlagen und Auskunftserteilung 9

1.5 Schlussbesprechung 9

2 Informationssicherheit bei sedex **10**

2.1 Angemessene Informationssicherheit bei sedex 11

2.2 Fehlendes Ausnahmenmanagement 11

2.3 Unklare Vorgaben zur Verfügbarkeit der sedex-Plattform 12

2.4 Externe Sicherheitsüberprüfungen sollten häufiger durchgeführt werden 13

2.5 Unvollständige Sicherheitsdokumentation 14

2.6 Fehlendes Code-Signing des sedex-Clients für Unix-basierte Systeme 15

2.7 Keine Ankündigung von neuen Client-Versionen 16

2.8 Unklarer Auftrag an die sedex-Abteilung als BFS-interner Leistungserbringer 17

Anhang 1: Abkürzungen **18**

Anhang 2: Glossar **19**

Prüfung der Informatiksicherheit der sedex-Plattform
Bundesamt für Statistik

Das Wesentliche in Kürze

sedex steht für «secure data exchange» und ist eine Dienstleistung des Bundesamts für Statistik (BFS). Die Plattform ist für den sicheren Datenaustausch zwischen Fachapplikationen von Organisationseinheiten der öffentlichen Verwaltung konzipiert.

sedex wurde im Rahmen der Modernisierung der Volkszählung aufgebaut, um die Statistiklieferungen der kommunalen Einwohnerdienste und der Personenregister des Bundes an das BFS sicherzustellen. Seit Inbetriebnahme Mitte 2008 hat sich sedex auch Teilnehmern ausserhalb der Registerharmonisierung und der Statistik geöffnet. Heute wird sedex von über 8000 Teilnehmern der Organisationseinheiten in über 80 Domänen eingesetzt. Teilnehmer sind bundesinterne Organisationen (v. a. Bundesämter) sowie zugelassene bundesexterne Organisationen (Kantone, Gemeinden, Dritte). Im Jahr 2022 wurden ca. 28,6 Millionen Meldungen via sedex übermittelt.

Da damit sensitive Daten ausgetauscht werden, musste die Plattform von Beginn an hohen Anforderungen an die Vertraulichkeit, Verfügbarkeit, Integrität sowie an die Nachvollziehbarkeit genügen. Dazu setzt sedex moderne Verschlüsselungsverfahren sowie Sicherheitszertifikate der Swiss Government PKI ein.

sedex besteht aus den zwei Teilsystemen sedex-Plattform und sedex espace. Die sedex-Plattform ermöglicht den sicheren Datenaustausch und besteht aus einem zentralen sedex Server und bei den Teilnehmern installierten sedex-Clients (Client-Server-System). Serviceerbringer ist das BFS. Leistungserbringer ist das Bundesamt für Informatik und Telekommunikation (BIT), welches für den Betrieb und die Entwicklung der Plattform zuständig ist. sedex escpace ist ein Web-basiertes Kundenportal und ermöglicht die Administration der Teilnehmer und der dazugehörigen Dienste sowie das Monitoring der erbrachten Services. Serviceerbringer ist wiederum das BFS. Der Leistungserbringer von sedex espace ist eine externe Firma.

Die Eidgenössische Finanzkontrolle (EFK) prüfte beim BFS und den Leistungserbringern die Informationssicherheitsmechanismen und -prozesse, die Kontrollen auf technischer und organisatorischer Ebene sowie das Lifecycle-Management.

Die sedex-Plattform verfügt über angemessene Sicherheitsmechanismen, um ihre Aufgaben zu erfüllen. Die vorhandenen Sicherheitsmassnahmen und -funktionen sind ausführlich dokumentiert. Positiv ist auch das vorausschauende Lifecycle-Management zu bewerten. Der sedex Service wird laufend weiterentwickelt, um neuen Anforderungen gerecht zu werden. Bei der Entwicklung hat die Sicherheit einen hohen Stellenwert.

Trotzdem hat die Prüfung noch Optimierungspotenzial ergeben:

Unklare Anforderungen zur Verfügbarkeit der sedex-Plattform

Die für die sedex-Plattform relevanten Informationssicherheitsdokumente enthalten widersprüchliche Anforderungen zur geforderten Verfügbarkeit. Weiter ist es fraglich, ob die geforderten Verfügbarkeitswerte mit den aktuell definierten Massnahmen tatsächlich

erreicht werden können. Das BFS soll die Verfügbarkeitsanforderungen der sedex-Plattform ganzheitlich prüfen und klar festlegen. Anschliessend sollen dem Schutzbedarf entsprechende Massnahmen definiert werden, um die Verfügbarkeit gemäss den Anforderungen sicherstellen zu können.

Notwendigkeit häufigerer externer Sicherheitsüberprüfungen

Die Sicherheit der sedex-Plattform und von sedex espace wird mittels externer Audits überprüft. Die Empfehlungen dieser Sicherheitsüberprüfungen wurden jeweils aufgenommen und umgesetzt. Zur Häufigkeit dieser Überprüfungen gibt es jedoch widersprüchliche Vorgaben und die letzte fand im 2020 statt. Die sedex-Plattform weist einen erhöhten Schutzbedarf bezüglich Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit auf. Weiter ist sedex espace aus dem Internet erreichbar und daher exponiert. Das BFS soll daher die Häufigkeit der externen Sicherheitsüberprüfungen eindeutig regeln. Aus Sicht der EFK sind Überprüfungen alle ein bis zwei Jahre angemessen.

Generelle Stellungnahme des BFS

Die Sicherheitsprüfung von sedex durch die EFK fand in vertrauensvollem und transparentem Rahmen statt. Das BFS bestätigt, dass die dargestellten Beschreibungen und Prozesse vollständig den Gegebenheiten entsprechen und bedankt sich für die professionelle Durchführung. Die im Bericht genannten Empfehlungen sind willkommen und werden entsprechend der weiteren Planung umgesetzt.

Generelle Stellungnahme des BIT

In Zusammenarbeit mit den Verwaltungseinheiten erachtet das BIT Backup-Restore-Tests als eine wichtige Möglichkeit, die Wiederherstellung von Applikationen für den Notfall zu üben. Sämtliche Applikationen werden vom RZ Bern nach Frauenfeld migriert, so auch Sedex. Im neuen Rechenzentrum werden möglicherweise einige Komponenten nicht mehr zur Verfügung stehen. Deshalb ist ein Backup-Restore-Test erst nach der Migration ins neue Rechenzentrum nach Frauenfeld geplant.

Das BIT sieht die Notwendigkeit, Installationspakete zu signieren. Deshalb werden ab dem nächsten Release Installationspakete Unix für den Sedex-Client signiert.

1 Auftrag und Vorgehen

1.1 Ausgangslage

sedex steht für «secure data exchange» und ist eine Dienstleistung des Bundesamts für Statistik (BFS). Die Plattform ist für den sicheren asynchronen und nachvollziehbaren Datenaustausch zwischen Fachapplikationen von Organisationseinheiten konzipiert.

Der Datenaustausch via sedex wird in Domänen geregelt in welchen die Domäneninhaber die entsprechenden Teilnehmer berechtigen und die erlaubten Meldungstypen definieren. Ein sedex-Teilnehmer ist einer Organisationseinheit zugeordnet. Jeder Teilnehmer ist Mitglied einer sedex-Domäne und erhält eine eindeutige, adressierbare Identität.

Danach wird der Teilnehmer durch den Domäneninhaber für bestimmte Meldungstypen autorisiert und kann, wenn der Sender und der Empfänger für dieselben Meldungstypen freigeschaltet wurden, die Daten verschlüsselt austauschen.

1.2 Prüfungsziel und -fragen

Mit der Prüfung soll dem BFS aufgezeigt werden, ob die vorhanden Informationssicherheitsmassnahmen und -Prozesse von sedex den Anforderungen des Bundes und dem definierten Schutzbedarf entsprechen und in welchen Bereichen noch Verbesserungsbedarf besteht.

Die Prüffragen lauteten:

1. Verfügt die sedex-Plattform über ausreichende Sicherheitsmechanismen und -prozesse, um ihre Aufgabe zu erfüllen?
2. Ist im operativen Betrieb sichergestellt, dass das Portal die hohen Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit erfüllt?
3. Wird die Betriebssicherheit mittels Kontrollen auf technischer und organisatorischer Ebene kontinuierlich und proaktiv überwacht und werden allfällige Korrekturmassnahmen zeitnah eingeleitet?
4. Ist durch ein vorausschauendes Lifecycle-Management eine dauerhaft effektive und effiziente Zugriffs- und Betriebssicherheit gewährleistet?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung konzentrierte sich auf die zwei Schutzobjekte sedex-Plattform und sedex espace. Sie erfolgte anhand der Cyberrisikenverordnung (CyRV)[1], dem IT-Grundschutz[2] der Bundesverwaltung sowie dem Secure Software Development Framework des National Institute of Standards and Technology (NIST)[3].

[1] https://www.fedlex.admin.ch/eli/cc/2020/416/de
[2] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/grundschutz.html
[3] https://csrc.nist.gov/publications/detail/sp/800-218/final

Die Prüfung wurde von Christian Brunner (Revisionsleiter) vom 31. Oktober bis 18. November 2022 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Das Revisionsteam wurde durch eine externe Firma unterstützt. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der Eidgenössischen Finanzkontrolle (EFK) vom BFS, dem Bundesamt für Informatik und Telekommunikation (BIT) sowie den externen Leistungserbringern umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 15. Februar 2023 statt. Teilgenommen haben von Seiten BFS die Vizedirektorin und der Dienstchef und Applikationsverantwortliche sedex. Seitens BIT die Compliance Officerin und Seitens EFK die zuständige Mandatsleiterin, der zuständige Fachbereichsleiter und der Revisionsleiter.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung der Amtsleitung bzw. dem Generalsekretariat des BFS obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

[redacted]

[redacted]

Fachbereichsleiter

Prüfungsexperte

2 Informationssicherheit bei sedex

sedex besteht aus den zwei Teilsystemen sedex-Plattform und sedex espace. Die sedex-Plattform besteht aus einem zentralen sedex Server und bei den Teilnehmern installierten sedex Clients (Client-Server-System). Serviceerbringer ist das BFS. Leistungserbringer ist das BIT, welches für den Betrieb und die Entwicklung der Plattform zuständig ist. sedex verwendet für den End-to-End verschlüsselten Transport das Produkt Governikus der deutschen Firma Governikus KG[4].

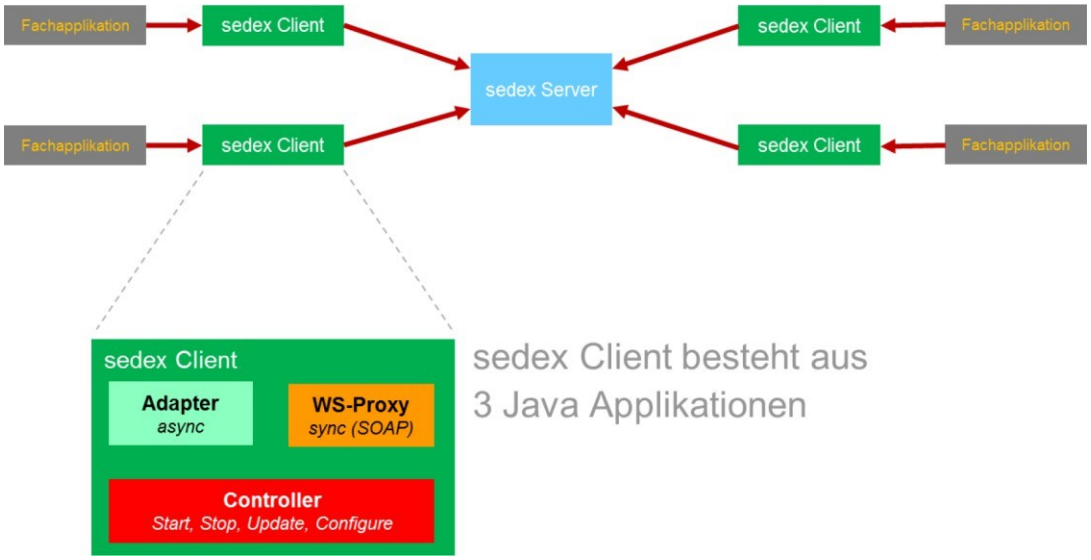

Abbildung 1: Kommunikation zwischen sedex-Client und Server (Quelle BFS)

sedex espace ist ein Web-basiertes Kundenportal auf SharePoint Basis und ermöglicht die Administration der Teilnehmer und der dazugehörigen Dienste sowie das Monitoring der erbrachten Services. Serviceerbringer ist wiederum das BFS. Der Leistungserbringer von sedex espace ist die Firma Boss Info AG[5], welche für die SharePoint Plattform und die Datenbank zuständig ist. Diese bezieht ihrerseits die Server als «Platform as a Service» als Leistungsbezüger von der Firma BEGASOFT[6] welche diese aufsetzt und deren Betrieb sicherstellt. sedex espace soll ab Mitte 2023 durch eine neue Kundenplattform abgelöst werden. Bis zu diesem Zeitpunkt wird sedex espace durch die Boss Info AG weiterbetrieben. Dies wurde mittels eines Übergangsvertrages geregelt.

Datenaustausch zwischen sedex-Plattform und sedex espace

Es findet kein automatisierter Datenaustausch zwischen der sedex-Plattform und sedex espace statt. Der Austausch der Daten erfolgt mittels einer im BIT entwickelten Hilfsapplikation, welche diese mittels sedex-Meldungen sicher und nachvollziehbar an sedex espace übermittelt. Die Daten werden anschliessend manuell in sedex espace importiert. Um Daten zwischen sedex espace und der sedex-Plattform auszutauschen wird ebenfalls diese Schnittstelle verwendet. Die Daten werden auch hier von den Administratoren manuell in die sedex-Plattform importiert.

[4] https://www.governikus.de/
[5] https://www.bossinfo.com/
[6] https://www.begasoft.ch/

2.1 Angemessene Informationssicherheit bei sedex

Die Plattform ist hochverfügbar und für den sicheren automatischen Datenaustausch konzipiert.

Die sedex-Plattform verfügt über angemessene Sicherheitsmechanismen, um ihre Aufgaben zu erfüllen. Die vorhandenen Sicherheitsmassnahmen und -funktionen sind ausführlich dokumentiert. Es werden externe Sicherheitsaudits durchgeführt und die daraus resultierenden Empfehlungen werden zeitnah umgesetzt.

Der sedex Service wird laufend weiterentwickelt, um neuen Anforderungen gerecht zu werden. Bei der Entwicklung hat die Sicherheit einen hohen Stellenwert. So finden diverse Tests und Überprüfungen im Rahmen der Entwicklung statt. Vorhandene Abhängigkeiten sind erkannt (z. B. Governikus und SharePoint) und werden aktiv gemanagt. Im Bereich der Kundenplattform werden neue Lösungen ohne Abhängigkeit zu SharePoint angestrebt.

Beurteilung

Das BFS ist sich der Wichtigkeit der Informationssicherheit bei der sedex-Plattform bewusst und hat angemessene Massnahmen getroffen. Sicherheit ist Teil der täglichen Arbeit sowie der Prozesse und wird stetig verbessert.

Die Weiterentwicklung nimmt einen hohen Stellenwert ein. Besonders positiv ist das vorausschauende Lifecycle-Management zu bewerten. Dabei wird auch nach Möglichkeiten gesucht, um bestehende Abhängigkeiten zu verringern und nachhaltige Lösungen zu entwickeln und zu implementieren.

2.2 Fehlendes Ausnahmenmanagement

Sowohl bei der sedex-Plattform als auch bei sedex espace gibt es Ausnahmen hinsichtlich des IT-Grundschutzes. Bei der sedex-Plattform ist die Ausnahme direkt im Nachweis zum IT-Grundschutz dokumentiert. Bei sedex espace sind die Ausnahmen im Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) aufgeführt.

Eine Ausnahme besteht dann, wenn eine oder mehrere Anforderungen des IT-Grundschutzes nicht oder nur teilweise erfüllt werden können. Ausnahmen müssen gemäss Art. 11 Abs. 1 lit. f CyRV beantragt und bewilligt werden. Ausnahmebewilligungen sind immer befristet und beinhalten geplante Massnahmen zur Risikoreduktion.

Die Ausnahmen bei sedex werden durch das BFS nicht aktiv überwacht. Es fehlt eine Übersicht zu den bestehenden Ausnahmen, deren Gültigkeiten und über die Massnahmen zur Risikoreduktion. Weiter findet kein Tracking der definierten Massnahmen statt, so dass unklar ist, ob diese auch umgesetzt werden.

Das BFS ist sich dessen bewusst und will das Management von Ausnahmen im Rahmen des sich im Aufbau befindenden Informationssicherheitsmanagementsystems (ISMS) adressieren.

Beurteilung

Das BFS sollte rasch ein Ausnahmenmanagement aufbauen, welches regelt, wie Ausnahmen überprüft, genehmigt und überwacht werden. Ein solches Verfahren soll es ermöglichen, eine fundierte Entscheidung darüber zu treffen, ob eine Ausnahme gewährt werden soll. Grundlage für die Entscheidung sind die mit der Ausnahme verbundenen Risiken und vorhandenen Alternativen. Gleichzeitig ist mit dem Ausnahmenmanagement sichergestellt, dass definierte Massnahmen zur Risikoreduktion umgesetzt werden.

Das Vorhaben des BFS zum Aufbau eines ISMS ist zielführend. Das Management von Ausnahmen ist sinnvollerweise Bestandteil davon.

Empfehlung 1 (Priorität 2)

Die EFK empfiehlt dem BFS im Rahmen des Aufbaus des ISMS das Ausnahmenmanagement für die sedex-Plattform und sedex espace zu regeln und bereits bestehende Ausnahmen und daraus resultierende Massnahmen aufzuarbeiten und zu verfolgen.

Die Empfehlung ist akzeptiert.

Stellungnahme des BFS

Die Empfehlung ist akzeptiert. Sie wird bei der Einführung des Informationssicherheitsgesetzes (ISG) im Rahmen des ISMS adressiert (2023–2024).

Eine der beiden bei sedex vorhandenen Ausnahmen wird zukünftig obsolet werden (Schnittstelle sedex zu sedex espace via letzte Meile).

Bei der anderen Feststellung handelt es sich nicht um eine Ausnahme im Sinne des P035 Prozesses des Bundes, eher um eine Umsetzung der im IT-Grundschutz festgelegten Zugriffsmatrix, welche für die Authentifizierung von Partnersystemen vorgesehen ist. Aus diesem Grund wurde vom NCSC auch keine Befristung für diesen Zugriff vorgesehen.

2.3 Unklare Vorgaben zur Verfügbarkeit der sedex-Plattform

Die für die sedex-Plattform relevanten Informationssicherheitsdokumente enthalten widersprüchliche Anforderungen hinsichtlich der geforderten Verfügbarkeit von sedex:

- Gemäss Schutzbedarfsanalyse beträgt die maximal zulässige Ausfalldauer der sedex-Plattform 8 Stunden (Verfügbarkeitsklasse 2). Die Servicezeiten sind als 24/7 angegeben, wobei bereits in der Schutzbedarfsanalyse darauf hingewiesen wird, dass diese Betriebszeiten nur für die BIT-Infrastruktur nicht aber für die Applikation selbst gelten.
- In der Business Impact Analyse der sedex-Plattform ist ein Recovery Time Objective (RTO - maximal tolerierbare Ausfallzeit) von weniger als 1 Tag definiert. Das Recovery Point Objective (RPO – maximal tolerierbarer Datenverlust) ist mit 4 Stunden vorgegeben. Dabei wird aber bereits ein Unterbruch von mehr als 2 Stunden als Gefährdung für die Geschäftsfortführung angesehen.
- Das Notfallkonzept geht nicht auf die in der Business Impact Analyse definierten RPO sowie RTO ein und beschreibt keine konkreten Massnahmen, wie die Systeme wiederhergestellt werden. Hinsichtlich der Massnahmen ist lediglich erwähnt, dass der sedex Service Manager die erforderlichen Massnahmen einleitet und das BIT die technischen Massnahmen ergreift.
- Die Dienstleistungsvereinbarung des BFS mit dem BIT für sedex legt fest, dass der 3rd Level Support durch das sedex Entwicklungsteam erfolgt und für dieses keine garantierte Reaktionszeiten gelten (siehe erster Punkt zur Schutzbedarfsanalyse).
- Gemäss ISDS-Konzept ist der Datenbankserver als einzige Infrastrukturkomponente der Server-Seite nicht redundant ausgeführt. Ein Restore der Datenbank sowie das Aufsetzen eines neuen Servers wird im ISDS-Konzept mit max. 4 Stunden veranschlagt. Bisher wurden noch keine Restoretests der Datenbank durchgeführt. Es ist nicht sichergestellt, dass der Restore in maximal 4 Stunden durchgeführt werden kann.

Weiter weisen gewisse Services, welche auf sedex aufbauen (z. B. GEVER Bund), eine höhere Verfügbarkeitsklasse auf. Durch die Restorezeiten von sedex ist auch die Verfügbarkeit dieser Services gefährdet.

Beurteilung

Die in den erwähnten Dokumenten aufgeführten Anforderungen an die Verfügbarkeit der sedex-Plattform sind widersprüchlich. Damit ist nicht klar, welche Verfügbarkeitswerte der Service tatsächlich im täglichen Betrieb erreichen soll.

Weiter ist fraglich, ob die geforderten Verfügbarkeitswerte mit den aktuell definierten Massnahmen tatsächlich erreicht werden können. Folgende Risiken können sich negativ auf die Verfügbarkeit auswirken:

- Ausfall des nichtredundanten Datenbank-Servers
- Betriebsunterbrechender Incident ausserhalb der Bürozeiten, dessen Behebung die Mithilfe des sedex Entwickler-Teams benötigt (3rd Level Support)

Zudem ist abzuklären, ob die Kunden, deren Applikationen höhere Verfügbarkeitsklassen haben, sich der Thematik bewusst sind und entsprechende Massnahmen definiert haben.

Zwar führt das Notfallkonzept gewisse Auslöseereignisse und Szenarien auf, enthält aber keine Angaben, welche Massnahmen beim Eintreten eines dieser Szenarien ergriffen werden sollen.

Wenn keine Restoretests durchgeführt werden kann nicht mit Sicherheit festgestellt werden, wie lange die Wiederherstellung tatsächlich benötigen würde.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem BFS, die Verfügbarkeitsanforderung der sedex-Plattform ganzheitlich zu überprüfen, klar zu definieren und allfällig notwendige Massnahmen zu deren Sicherstellung umzusetzen.

Die Empfehlung ist akzeptiert.

Stellungnahme des BFS

Das BFS wird die Verfügbarkeitsanforderungen prüfen, die Dokumente 2023 konsolidieren und mit dem BIT Restoretests planen.

2.4 Externe Sicherheitsüberprüfungen sollten häufiger durchgeführt werden

Die Sicherheit der sedex-Plattform und von sedex espace wird mittels externer technischer Audits überprüft. Gemäss dem sedex Organisationshandbuch sollen die Sicherheitsüberprüfungen ungefähr alle zwei Jahre durch einen unabhängigen externen Experten stattfinden. Das ISDS-Konzept hingegen führt auf, dass Security Audits ca. alle 5 Jahre durchgeführt werden. Die letzte externe Überprüfung von sedex fand 2020 statt. Die Empfehlungen dieser Sicherheitsüberprüfung wurden aufgenommen und umgesetzt. Die nächste Überprüfung ist für 2023 budgetiert.

Beurteilung

Die Notwendigkeit und der Mehrwert von externen technischen Sicherheitsüberprüfungen sind durch das BFS erkannt und die empfohlenen Massnahmen der letzten Überprüfung wurden umgesetzt.

Externe Sicherheitsüberprüfungen sollten insbesondere in Abhängigkeit des Schutzbedarfs, interner und externer Vorgaben sowie der Informationssicherheitsrisiken geplant und durchgeführt werden. Die sedex-Plattform weist einen erhöhten Schutzbedarf auf und wird von einer sehr grossen Anzahl Teilnehmer genutzt. Weiter ist sedex espace aus dem Internet erreichbar und daher exponiert. Die Häufigkeit der Überprüfungen sollte in den internen Vorgaben (Organisationshandbuch und ISDS-Konzept) identisch sein.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt dem BFS, externe Sicherheitsüberprüfungen der sedex-Plattform und von sedex espace alle ein bis zwei Jahre durchzuführen.

Die Empfehlung ist akzeptiert.

Stellungnahme des BFS

Die ursprünglich für 2024 geplante externe Sicherheitsprüfung wird auf 2023 vorverschoben und danach alle ein bis zwei Jahre durchgeführt.

2.5 Unvollständige Sicherheitsdokumentation

Für sedex gelten die Vorgaben der CyRV. Folglich müssen die erforderlichen Sicherheitsdokumentationen erstellt werden. Für beide Schutzobjekte liegen die von der CyRV geforderten Sicherheitsdokumentationen vor.

sedex-Plattform

Die Sicherheitsdokumentation der sedex-Plattform ist – mit Ausnahme des Notfall-Konzepts (siehe Kapitel 2.3) – inhaltlich sauber und schlüssig erarbeitet und weist einen qualitativ hochwertigen Stand auf.

sedex espace

Die Sicherheitsdokumentation von sedex espace ist zwar vollständig – im Sinne, dass sämtliche geforderten Dokumente vorhanden sind – jedoch weisen diese inhaltlich einige Unstimmigkeiten auf:

- IT-Grundschutz: Es werden diverse Anforderungen des IT-Grundschutzes nicht oder nur teilweise erfüllt. So werden bespielweise im Gegensatz zu den Angaben im Grundschutz keine Restore Tests von Backups durchgeführt und es bestehen diesbezüglich keine abgestimmten Vorgehensweisen zwischen Leistungserbringer und -bezüger. Weiter sind Anforderungen fälschlicherweise als «nicht anwendbar» definiert (bspw. Synchronisierung der Systemzeit). Schliesslich ist die Umsetzungsbeschreibung bei gewissen Anforderungen unvollständig.
- ISDS-Konzept: Bei der im ISDS-Konzept abgebildeten Kommunikationsmatrix handelt es sich um jene der sedex-Plattform und nicht von sedex espace. Weiter besteht ein Widerspruch zur Schutzbedarfsanalyse: Gemäss Schutzbedarfsanalyse beinhaltet das Schutzobjekt keine Personendaten, während gemäss ISDS-Konzept Personendaten bearbeitet werden. Aussagen sind teilweise nicht mit den Lieferanten abgestimmt und die Lieferanten sind bei der Umsetzung von im Konzept definierten Massnahmen (bspw. Berechtigungskonzept) nicht involviert. Weiter sind gewisse Massnahmen (Log-Management) technisch durch die Lieferanten umsetzbar – im Gegensatz zu den Aussagen im ISDS-Konzept.

Beurteilung

Bei der Sicherheitsdokumentation handelt es sich um Dokumente, die das System selbst und seine sicherheitsrelevanten Bestandteile und Funktionen beschreiben. Die Dokumente bieten einen Überblick über das System und helfen Administratoren und weiteren Beteiligten, die sicherheitsrelevanten Konfigurationen und Funktionen initial zu definieren und anschliessend im Betrieb aufrecht zu erhalten und zu verbessern. Die Sicherheitsdokumentation sollte daher stets inhaltlich korrekt, vollständig und aktuell sein. Dies ist auch explizit in den IT-Grundschutzanforderungen so festgehalten.

Um sedex espace abzulösen wird bis Ende 2023 ein Konzept und ein Umsetzungsplan erstellt. Da es zum Zeitpunkt der Prüfung noch nicht klar ist, wann die neue Plattform eingeführt wird sollte das vorhandene Dokument zeitnah aktualisiert werden.

Empfehlung 4 (Priorität 2)

Die EFK empfiehlt dem BFS die Sicherheitsdokumente von sedex espace zu überarbeiten und allfällig notwendige Massnahmen umzusetzen.

Die Empfehlung ist akzeptiert.

Stellungnahme des BFS

Die im BFS geführten Sicherheitsdokumente 2023 sind bereits heute vollständig. Im Rahmen der Umsetzung der unter 2.2 erwähnten Massnahmen werden die Dokumente aktualisiert und konkretisiert.

2.6 Fehlendes Code-Signing des sedex-Clients für Unix-basierte Systeme

Innerhalb der Bundesverwaltung kann auf Windows-Rechnern von Benutzern nur noch mittels Code Signing signierte Software installiert werden. Die Software-Bausteine des sedex-Clients wurden entsprechend signiert, so dass alle Verwender (bundesintern als auch -extern) bzw. deren Windows Betriebssysteme die Authentizität des Herausgebers und die Integrität der Software überprüfen können. sedex Kunden (Teilnehmer) laden den sedex-Client auf der sedex-Webseite herunter[7]. Dort ist auch der Hash-Wert verfügbar, mit welchem die Authentizität der Software vor der Installation überprüft werden kann.

Anders verhält es sich bei der Software für Unix-basierte Systeme, welche noch nicht signiert ist. Die Authentizität und Integrität des sedex-Clients kann dabei nicht durch die Teilnehmer überprüft werden. Die Teilnehmer müssen darauf vertrauen, dass die Software wirklich vom BFS stammt und nicht von einem unbekannten Dritten manipuliert wurde.

Beurteilung

Teilnehmer vertrauen auf die Authentizität und Integrität des sedex-Clients. Eine kompromittierte Version des sedex-Clients, welche auf einer gefälschten Website zum Download angeboten wird, könnte dazu führen, dass Malware im Namen des BFS verbreitet wird. Ein solches Szenario gefährdet die Informationssicherheit bei den Teilnehmern und die Reputation des BFS.

[7] https://www.bfs.admin.ch/bfs/de/home/register/personenregister/sedex/downloads.html

Empfehlung 5 (Priorität 2)

Die EFK empfiehlt dem BFS, die Software des sedex-Clients für Unix-basierte Systeme so bald wie möglich zu signieren.

Die Empfehlung ist akzeptiert.

Stellungnahme des BFS

Die Umsetzung wird im Rahmen der Wartung und Weiterentwicklung geplant.

2.7 Keine Ankündigung von neuen Client-Versionen

Pro Jahr werden ein bis zwei neue Releases des sedex-Clients veröffentlicht und auf der Website des BFS zum Download zur Verfügung gestellt. Zudem werden bei Bedarf kleine Änderungen mittels Minor Releases eingeführt.

Auf der Webseite[8] Betrieb von sedex steht: «Der Betreiber eines sedex-Client verpflichtet sich, mindestens einmal pro Jahr, die neuste Version des sedex-Client zu installieren.».

Seitens der Teilnehmer wurde moniert, dass neue Releases nicht angekündigt würden. Dies bedeutet, dass Domänenvertreter und Teilnehmer eigenständig aktiv werden und regelmässig prüfen müssen, ob eine neue Version des Clients verfügbar ist.

Laut BFS werden grosse Releases mittels Newsletter angekündigt. Zudem erhalten die Domänenvertreter vom BFS in regelmässigen Abständen eine Übersicht zu den in ihrer Domäne eingesetzten Client-Versionen der Teilnehmer. Minor-Releases werden jedoch nicht angekündigt und die Teilnehmer werden nicht direkt informiert.

Beurteilung

Ohne Information der Teilnehmer des sedex-Clients ist es wahrscheinlich, dass neue Releases nicht oder verzögert installiert werden. Damit besteht die Gefahr, dass Nutzer veraltete Versionen des Clients einsetzen. Veraltete Softwareversionen bergen die Gefahr von bekannten Schwachstellen, welche durch einen Angreifer ausgenutzt werden können. Auch wenn die Software-Komponenten nicht direkt von extern erreichbar sind, birgt dies die Gefahr, dass ein Angreifer Malware einschleusen kann, welche anschliessend Schaden auf den Systemen anrichtet oder für weiterführende Angriffe innerhalb des jeweiligen Netzwerks verwendet werden kann.

Es ist legitim, die Benutzer in die Pflicht zu nehmen einmal jährlich die neuste Version zu installieren. Erfahrungsgemäss dürfte das aber bei der grossen Anzahl an Benutzern nicht flächendeckend funktionieren.

Empfehlung 6 (Priorität 2)

Die EFK empfiehlt dem BFS, den Benutzern von sedex Client-Updates automatisiert anzukündigen.

Die Empfehlung ist akzeptiert.

Stellungnahme des BFS

Das BFS hat in der Regel keine direkte Beziehung zu den Inhabern der sedex Teilnehmer, sondern mit dem Domäneninhaber. Im Rahmen der Kundenplattform wird geprüft, ob die

[8] https://www.bfs.admin.ch/bfs/de/home/register/personenregister/sedex/betrieb.html

Teilnehmer besser eingebunden werden können und die Domäneninhaber Mittel zur Überprüfung ihrer Teilnehmer erhalten. Zudem werden die Teilnehmer verstärkt in die Pflicht genommen, indem die Nutzrichtlinien (Pflicht zum mindestens jährlichen Update, Recht des BFS einzelne Teilnehmer zu deaktivieren) konsequenter angewendet werden.

2.8 Unklarer Auftrag an die sedex-Abteilung als BFS-interner Leistungserbringer

Für die Datenübertragung an sedex espace (siehe Einleitung Kapitel 2) verfügt die sedex-Plattform über einen eigenen sedex-Client. Dieser Client wird auf dem «Letzte Meile»-Server betrieben. Auf diesem Server werden noch weitere sedex-Clients für andere Abteilungen des BFS betrieben. Diese nutzen die Clients für den Versand ihrer eigenen sedex Meldungen.

Beurteilung

Mit dem Betrieb von sedex-Clients für weitere BFS Abteilungen übernimmt die sedex-Abteilung die Rolle eines internen Dienstleisters, welche über den Betrieb des sedex Services hinausgeht. Aus Sicht der EFK sind die Rollen und Verantwortlichkeiten unklar. Es sollte klar definiert werden, wer für den Betrieb und allfällige Updates der installierten sedex-Clients auf dem «letzte Meile»-Server verantwortlich ist. Weiter besteht die Gefahr, dass die Betriebsorganisation der sedex-Abteilung nicht auf den Betrieb dieses Service ausgelegt ist.

Anhang 1: Abkürzungen

BFS	Bundesamt für Statistik
BIT	Bundesamt für Informatik und Telekommunikation
CyRV	Cyberrisikenverordnung
EFK	Eidgenössische Finanzkontrolle
GEVER	Elektronische Geschäftsverwaltung
ISDS-Konzept	Informationssicherheits- und Datenschutzkonzept
ISMS	Informationssicherheits-Management-System
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
RPO	Recovery Point Objective
RTO	Recovery Time Objective
sedex	secure data exchange

Anhang 2: Glossar

Domäne	Die Koordination der sedex-Teilnehmer basiert auf dem sogenannten Domänenkonzept. Eine Domäne ist ein Verbund von sedex-Teilnehmern, die in einem spezifischen Kontext Geschäftsfälle abwickeln und dazu sedex-Meldungen austauschen oder Web-Services konsumieren.
Domänenvertreter	Jede sedex-Domäne definiert einen Domänenvertreter, der die Schnittstelle zwischen dem Serviceerbringer und den Anspruchsträgern seiner Domäne bildet. Er koordiniert auch die fachlichen Belange in der Domäne.
Hashwert	Hashing bezeichnet die Umwandlung einer Zeichenfolge in einen eindeutigen und normalerweise kürzeren numerischen Wert mit fester Länge. Dieser numerische Wert ist der Hashwert und ein Fingerabdruck der ursprünglichen Zeichenfolge. Vom Hashwert sollen keine Rückschlüsse auf den Eingabewert gemacht werden können.
ISMS	Ein Information Security Management System (ISMS) ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
RPO	Recovery Point Objective (RPO) bezieht sich auf die Datenmenge, die innerhalb eines für ein Unternehmen relevanten Zeitraums verloren gehen kann, bevor ein signifikanter Schaden entsteht, und zwar vom Zeitpunkt eines kritischen Ereignisses bis zum vorhergehenden Backup.
RTO	Recovery Time Objective (RTO) legt die maximal tolerierbare Zeitspanne fest, die eine Anwendung, ein System und/oder ein Prozess ausfallen kann, ohne dass ein signifikanter Schaden für das Unternehmen entsteht. Daran müssen sich die Massnahmen für die Wiederherstellung der Anwendung und ihrer Daten ausrichten.

Swiss Government PKI[9]	Die Swiss Government PKI ist das Kernstück der Bundes-Trust-Services und kommt immer dann zum Einsatz, wenn die Vertraulichkeit speziell sichergestellt sein muss. Das BIT stellt den Schweizer Behörden und bundesnahen Organisationen Schlüssel zur Verfügung mit denen Daten signiert (beglaubigt) oder verschlüsselt (Inhalt für Unberechtigte unlesbar) werden können. Die Schlüssel können auch verwendet werden, um sich bei einer Anwendung anzumelden (Authentifizierung).
Teilnehmer	Ein sedex-Teilnehmer steht für eine Organisationseinheit, die Meldungen mit anderen Organisationseinheiten innerhalb einer Domäne austauscht, und der vom sedex-Support eine eindeutige, adressierbare sedex-ID zugewiesen wurde. Der sedex-Teilnehmer beauftragt in der Regel einen IT-Partner mit dem Betrieb seiner Fachanwendung.

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrundeliegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

[9] https://www.bit.admin.ch/bit/de/home/subsites/allgemeines-zur-swiss-government-pki.html