Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

14. Mai 2020 [redacted]

Prüfbericht «Backup und Recovery-Konzepte»

IKT Prüfung I 2020-02

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 14. Mai 2020

Prüfbericht IKT-Prüfung «Backup und Recovery-Konzepte»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Backup und Recovery-Konzepte» zukommen. Unsere Prüfarbeiten fanden zwischen Januar und Februar 2020 statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern besprochen. Die Stellungnahme der Gruppe Verteidigung zu unserem Bericht ist in Kapitel 8 ersichtlich.

Diese Prüfung wurde in Übereinstimmung mit den internationalen Standards für die berufliche Praxis der internen Revision durchgeführt. Die Interne Revision VBS ist Mitglied des Schweizerischen Verbands für Interne Revision (SVIR).

Sollten Sie Fragen zu unserem Bericht haben, stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted] [redacted]

Verteiler
- GS VBS
- CdA
- Chef FUB

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Backup und Recovery – Grundlagen

IKT-Systemausfälle und Datenverluste gehören heutzutage zu den grössten Risiken innerhalb einer Unternehmung oder Verwaltung. Um diesen Risiken Rechnung zu tragen, sind funktionierende Backup und Recovery-Prozesse elementar. Die Datensicherung (Backup) bezeichnet dabei das Sichern von Daten mit der Absicht, diese im Fall eines Datenverlustes wiederherstellen zu können. Diese Wiederherstellung der Originaldaten aus einer Sicherungskopie wird als Datenwiederherstellung (Recovery) bezeichnet.

Eine systematische Datensicherung basiert auf einer angemessenen Backup und Recovery-Strategie (Konzept) und sollte möglichst angemessen dokumentiert sein. Wichtig dabei ist eine klare Zuteilung der Verantwortungen und Aufgaben. Die Dokumentation sollte gemäss den Grundsätzen der Datensicherung[1] mindestens folgende Themenbereiche abdecken:

– Ablauf der Datensicherung
– Aufbau der Daten-Archivierung
– zu treffende (Sofort-)Massnahmen
– Regelung der Kompetenzen
– Prioritäten für besonders zeitkritische Daten und Systeme

Für ein fundiertes Backup und Recovery-Konzept ist es zentral, die Datensicherung als Ganzes zu verstehen und konzeptionell mit anderen IT-Prozessen zu verbinden. Die sich stetig verändernde IT-Landschaft und -Nutzung stellen zusätzliche Anforderungen hinsichtlich deren Funktionalität, Leistung und Umsetzung dar.

In der konkreten Planung für Datensicherungsmassnahmen sollte einerseits der Umfang der zu sichernden Informationen angemessen und andererseits die Häufigkeit der Datensicherung an die geschäftlichen Anforderungen der Organisation angepasst sein. Das Sichern der Daten alleine reicht jedoch nicht aus. Es sollte zusätzlich getestet und verifiziert werden, ob die Daten erfolgreich und zeitnah aus dem Backup wiederhergestellt werden können. Der ISO Standard fordert deshalb explizit auch zum Testen der gewählten Backup-Methode auf.

2 Organisation innerhalb des VBS

Grundsätzlich obliegt die Verantwortung für das Backup und Recovery bei den Systembetreibern. Beim VBS nimmt meist die FUB als zentraler Leistungserbringer für IKT-Leistungen diese Aufgabe wahr und trägt somit die Hauptverantwortung für das Backup und Recovery. Heute werden diverse Systeme jedoch nicht mehr über die FUB, sondern durch das BIT oder Drittdienstleister betrieben. Diese Systeme sind daher nicht Bestandteil der zentralen Datensicherung in der FUB.

[1] ISO/IEC 27001; Standard für die Information Security Management Systeme

3 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS am 6. Dezember 2019 den Auftrag, die bestehenden Abläufe und Verfahren bezüglich Datensicherung (Backup und Recovery) zu prüfen. Zudem beurteilte die IR VBS, ob die bestehenden Konzepte den heutigen Standards genügen und ob die festgelegten Verfahren auch angewendet und getestet werden.

Im Rahmen unserer Prüfhandlungen führten wir strukturierte Befragungen durch und analysierten Dokumente. Um die Angemessenheit der Unterlagen beurteilen zu können, haben wir zu unseren Abklärungen Fachliteratur und Referenzdaten herangezogen.

Anwendungen, die nicht von der FUB als Dienstleister betrieben werden, sind nicht Gegenstand dieser Prüfung.

4 Würdigung

Während unserer Prüfung trafen wir ausnahmslos auf engagierte Interviewpartner[2], die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen die Betriebsabläufe hinsichtlich Datensicherheit ein wichtiges Anliegen sind. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit.

5 Datensicherung und Wiederherstellung

5.1 Allgemeiner Beschrieb – Prozess

Feststellung: Innerhalb der FUB ist das Storage-Team für die Datensicherung zuständig. Der Bereich Storage verantwortet die gesamte Backupinfrastruktur. Die Prüfung der korrekten Wiederherstellung liegt in der Verantwortung der Datenbezüger. Die Datensicherung der Anwendungen[3] erfolgt innerhalb eines definierten Zeitfensters auf speziell dafür geeigneten Speicherungssystemen. Die Speicherungsinfrastruktur ist für alle Anwendungen georedundant (doppelt und örtlich getrennt) aufgebaut und garantiert, dass bei einem teilweisen oder totalen Ausfall eines Rechenzentrums alle Daten dennoch wiederhergestellt werden könnten.

Der Zeitaufwand der Datenwiederherstellung ist abhängig vom Datenvolumen und der Netzwerkleistung. Bei sehr umfangreichen Datenwiederherstellungen kann dies mehrere Stunden oder sogar Tage dauern. Der Recovery-Service kommt dann zum Einsatz, wenn sämtliche

[2] Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt; es ist jedoch immer auch die weibliche Form mitgemeint.

[3] Unter Anwendungen verstehen wir die verschiedenen Applikationen sowie deren zugehörige Daten, Datenbanken und Filesysteme.

sonstigen Sicherheitsvorkehrungen seitens Applikation, Datenbank oder Filesystem beeinträchtigt wurden und ein grosser oder gar vollständiger Datenverlust droht; beziehungsweise bereits erfolgte. Mittels eines Pikettdiensts wird auch ausserhalb der Betriebszeiten ein reibungsloser Backup-Service gewährleistet.

Beurteilung: Den Backup und Recovery-Prozess innerhalb der FUB erachten wir als angemessen und wirksam. Die wesentlichen Schlüsselelemente der Datensicherung werden regelmässig überwacht. Bei Abweichungen und Störungen stellt der Prozess geeignete Massnahmen zeitnah sicher.

5.2 Konzepte

Feststellung: Sämtliche vom Storage-Team der FUB betreuten Systeme (Anwendungen) basieren auf einem durch die Anwendungsverantwortlichen abgenommenen Datensicherungskonzept. Nicht jede einzelne Anwendung benötigt ein eigenes Datensicherungskonzept. Die Anwendungen werden in Gruppen zusammengefasst und jede Anwendungsgruppe hat ein eigenes Konzept, welches die Prozesse und Zuständigkeiten regelt. Dabei werden nebst den Schlüsselanforderungen auch die Einhaltung von gesetzlichen Vorgaben für den Umgang mit Daten festgelegt. Ebenfalls Bestandteil der Datensicherungskonzepte ist die Handhabung von nicht mehr benötigten Sicherungsmitteln (Vernichtung, Löschung). Die Konzepte werden nach Bedarf überarbeitet.

Beurteilung: Die Datensicherungskonzepte sind gemäss den Vorgaben von ITIL[4] aufgebaut. Die Zuteilung der Verantwortungen und Aufgaben sind klar geregelt. Die geforderten Mindestgrundsätze der Datensicherung sind abgedeckt und entsprechen ebenfalls den Vorgaben. Die Konzepte werden mittels geeigneten Prozessen den laufenden Neuerungen angepasst.

5.3 Testing

Feststellung: Das Storage-Team stellt sicher, dass sämtliche Datensicherungen erfolgreich durchgeführt werden. Die FUB führt jedoch keine regelmässigen und systematischen Tests der Datenwiederherstellung durch. Der Prozess sieht vor, dass ein Backup und Recovery bei der erstmaligen Einführung eines Systems oder bei wesentlichen Veränderungen innerhalb der Applikation geprüft wird. Aufgrund fehlender Ressourcen (Infrastruktur, Manpower) wurde in der Vergangenheit auf periodische Tests der Wiederherstellung verzichtet. Gemäss Aussage unserer Interviewpartner würden insbesondere grössere Systeme für ein solches Testing eine eigene Testumgebung benötigen, da der laufende Betrieb nicht unterbrochen bzw. gestört werden darf. Weiter würde eine solche Überprüfung eine Beteiligung der Anwender bedeuten, damit die Abnahme der Tests zeitnah erfolgen kann. In den vergangenen

[4] ITIL: IT Infrastructure Library ist eine Sammlung von Best Practices in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements (ITSM). Sie gilt international als De-facto-Standard.

zwei Jahren gab es keine grösseren Betriebsstörungen, welche einen Recovery-Service benötigten.

Beurteilung: Die aktuellen Betriebsprozesse sind in der Praxis eingespielt und es treten kaum Störungen auf. Dennoch erachten wir ein regelmässiges Testen der Datensicherung und Wiederherstellung als zwingenden Bestandteil eines angemessenen Backup und Recovery-Prozesses.

6 Fazit

Die Backup und Recovery-Abläufe innerhalb der FUB sind eingerichtet und entsprechend dokumentiert. Unsere Erhebung hat ergeben, dass in den vergangenen zwei Jahren keine Datenverluste in den von uns geprüften Anwendungen vorgekommen sind. Die geprüften Konzepte sind gemäss den Vorgaben von ITIL aufgebaut und angemessen dokumentiert. Sie erfüllen die Mindestanforderungen der Grundsätze zur Datensicherung.

Wir haben jedoch auch festgestellt, dass keine regelmässigen und systematischen Tests der Datensicherungen und Wiederherstellungen erfolgten. Dementsprechend können wir die Wirksamkeit der Backups und Recoverys nur eingeschränkt bestätigen. Eine systematische und risikobasierte Überprüfung der relevanten Betriebs-Risiken (Backup und Recovery-Tests) auf den Anwendungen ist nur bedingt möglich.

7 Empfehlung

Wir empfehlen der FUB, ein systematisches und periodisches Testen der Datensicherung und Wiederherstellung zu etablieren. Die Ausprägung dieser Tests sollte risikobasiert auf der Grundlage eines Business Continuity Management Planes festgelegt werden und damit auf die Bedürfnisse der Anwender abgestimmt sein. Eine Dokumentation der Ergebnisse dieser Tests erachten wir als zweckmässig.

8 Stellungnahme

Gruppe Verteidigung
Wir stimmen der Empfehlung zu. Das periodische und systematische Testen der Datensicherung und Wiederherstellung wird im Rahmen des Service Continuity Management umgesetzt. Die Ausprägung dieser Tests wird risikobasiert auf der Grundlage eines IT Services Continuity Managements bzw. im Rahmen des Wiederanlaufplans des Betriebes festgelegt. Ein entsprechender Plan mit den festgelegten Systemen und der benötigten Infrastruktur und Ressourcen wird bis am 31.12.2020 vorgelegt.