Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Autorité de surveillance indépendante des activités de renseignement AS-Rens

AS-Rens Inspection 23-4

IT Service continuity management (ITSCM) et Disaster Recovery-IT au SRC

Résumé

Lors de la présente inspection, l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) a examiné si le Service de renseignement de la Confédération (SRC) disposait de processus efficaces et appropriés pour pouvoir garantir le maintien de l'exploitation informatique et donc de son activité principale, en cas de scénario de crise ou de catastrophe, et pour pouvoir restaurer ses données.

Les événements majeurs imprévus tels que les incendies, les inondations ou les activités criminelles constituent une menace pour toute organisation. De tels événements sont de nature à potentiellement causer des dommages, notamment à l'infrastructure des technologies de l'information, qui peuvent être bien plus graves qu'une simple panne. Il appartient dès lors aux organisations d'assurer une continuité de leur activité (Business continuity management [BCM]). Le BCM se concentre ainsi sur un événement et s'emploie à réduire l'impact d'un risque sur les prestations et processus opérationnels essentiels.

Une informatique fiable et hautement disponible est essentielle à la survie d'une entreprise, étant donné la grande dépendance de son activité principale envers les technologies de l'information. L'IT Service continuity management (ITSCM), qui découle du BCM, a pour objectif de pouvoir fournir les prestations informatiques critiques identifiées par l'entreprise conformément aux exigences, même en cas d'événement majeur. Pour ce faire, des mesures préventives (renforcement de la résilience) et des mesures préparées en cas de survenue d'un événement (renforcement de la réaction) sont évaluées et mises en œuvre. L'ITSCM doit garantir que les services et l'infrastructure des technologies de l'information et de la communication (TIC) sont disponibles suite à une défaillance ou qu'ils puissent être rétablis dans un délai convenu. Le Disaster Recovery-IT vise quant à lui à remettre les services et l'infrastructure TIC en état suite à une défaillance.

Le thème de l'ITSCM répond ainsi à des risques très actuels et concrets. La numérisation continuant ses progrès et le traitement des données étant au cœur de l'activité du SRC, celui-ci est d'autant plus dépendant d'une exploitation continue et fiable de ses infrastructures informatiques, et ce dans un monde où la pénurie d'électricité menace, où les cyber-attaques se multiplient et où la guerre n'est plus étrangère au continent européen. De même, des pertes de données seraient de nature à menacer sa capacité à exécuter sa mission.

La partie BCM avait déjà fait l'objet d'un rapport de l'organe de révision interne du DDPS (rapport I 2022-01 du 15 août 2022). Une des recommandations de ce rapport invitait les unités administratives du DDPS à mettre à jour leur documentation relative au BCM. Le SRC travaille pour appliquer cette recommandation. De plus, la direction du SRC a décidé de n'approuver et de mettre en œuvre un nouveau BCM qu'au terme de sa transformation actuellement en cours. L'AS-Rens a donc fait preuve de retenue quant à ce qui avait trait au BCM.

S'agissant de l'ITSCM, l'AS-Rens a constaté l'absence de documentation. Cette absence de documentation relève d'un défaut de gouvernance TIC au sein du SRC. En effet, les mesures existent, mais ont été prises au niveau technique uniquement. L'unité TIC a ainsi adopté de nombreuses mesures pour garantir une continuité de l'activé en cas d'évènement majeur. Ces mesures sont efficaces et adéquates. Elles permettent de limiter les risques de manière conséquente. En particulier, la redondance de l'infrastructure TIC de même que la stratégie de sauvegarde des données sont adéquates et efficaces. Cela étant, il n'existe aucune stratégie de test, de sorte que si les services TIC bénéficient d'une grande stabilité, il n'est pas certain qu'il en soit de même en cas d'événement majeur. De même, l'absence de tests variés et réguliers ne permet pas de mettre à jour l'ITSCM. Des recommandations ont été prononcées en lien avec la documentation de l'ITSCM et l'organisation de tests.

AB-ND Prüfung 23-4

IT Service continuity management (ITSCM) und Disaster Recovery-IT beim NDB

Zusammenfassung

In dieser Prüfung untersuchte die AB-ND, ob der NDB über effiziente und geeignete Prozesse verfügt, mit denen im Krisen- oder Katastrophenfall der IT-Betrieb und dadurch auch der Betrieb des Kerngeschäfts des NDB sichergestellt und seine Daten wiederhergestellt werden können.

Unvorhergesehene Grossereignisse wie Brände, Überschwemmungen oder kriminelle Aktivitäten stellen eine Bedrohung für jede Organisation dar. Solche Ereignisse können insbesondere an der informationstechnologischen Infrastruktur Schäden verursachen, die möglicherweise viel schlimmer als eine einfache Panne sind. Daher müssen Organisationen das Business Continuity Management (BCM) sicherstellen. Das BCM konzentriert sich somit auf ein Ereignis und soll seine Auswirkungen auf Risiken für kritische Leistungen und Geschäftsprozesse minimieren.

Eine zuverlässige und hochverfügbare IT ist für das Überleben eines Unternehmens essenziell, da sein Kerngeschäft stark von Informationstechnologien abhängt. Das mit dem BCM einhergehende ITSCM hat zum Ziel, auch bei Grossereignissen gemäss den Anforderungen vom Unternehmen identifizierte kritische IT-Leistungen liefern zu können. Dafür werden vorsorgliche Massnahmen (Stärkung der Resilienz) und für den Ereignisfall vorbereitete Massnahmen (Stärkung der Reaktion) beurteilt und umgesetzt. Mit dem ITSCM soll sichergestellt werden, dass die Leistungen und die Infrastruktur der Informations- und Kommunikationstechnologien (IKT) nach einem Ausfall verfügbar sind oder innert einer vereinbarten Frist wiederhergestellt werden können. Die Disaster-Recovery-IT hingegen soll die IKT-Leistungen und -Infrastruktur nach einem Ausfall wieder instand setzen.

Ein solches ITSCM muss den aktuellen und konkreten Risiken gerecht werden. Vor dem Hintergrund einer drohenden Strommangellage, zunehmender Cyberangriffe und einem Krieg in Europa ist der NDB durch die fortschreitende Digitalisierung und die

Datenbearbeitung als seine zentrale Tätigkeit mehr denn je von einem kontinuierlichen und zuverlässigen Betrieb der IT-Infrastrukturen abhängig. Zudem gefährden Datenverluste die Fähigkeit des NDB, seinen Auftrag zu erfüllen.

Das BCM war bereits Gegenstand eines Berichts der Internen Revision des VBS (Bericht I 2022-01 vom 15. August 2022). Eine der Empfehlungen dieses Berichts forderte die Verwaltungseinheiten des VBS auf, ihre Dokumentation über das BCM zu aktualisieren. Der NDB arbeitet daran, diese Empfehlung umzusetzen. Zudem hat die Leitung des NDB beschlossen, erst nach Abschluss der laufenden Transformation ein neues BCM zu genehmigen und umzusetzen. Die AB-ND zeigt sich deshalb in Bezug auf das BCM zurückhaltend.

Beim ITSCM hat die AB-ND fehlende Dokumentation festgestellt. Die fehlende Dokumentation ist auf einen Mangel bei der IT-Governance innerhalb des NDB zurückzuführen. Es wurden zwar Massnahmen getroffen, aber nur auf technischer Ebene. Die IKT-Einheit des NDB hat zahlreiche Massnahmen ergriffen, um im Falle eines Grossereignisses die Betriebskontinuität sicherzustellen. Diese effizienten und angemessenen Massnahmen, zu denen insbesondere die Sicherstellung der Redundanz der IKT-Infrastruktur sowie die Datensicherungsstrategie zählen, ermöglichen, die Risiken konsequent zu minimieren. Allerdings gibt es keine Teststrategie, sodass nicht sicher ist, ob die hohe Stabilität der IKT-Leistungen auch bei einem Grossereignis wirklich gegeben ist. Ohne verschiedenartige und regelmässige Tests kann zudem das ITSCM nicht aktualisiert werden. Im Zusammenhang mit der Dokumentation des ITSCM und der Organisation von Tests wurden Empfehlungen ausgesprochen.