Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung Bevölkerungsschutz und Sport VBS

Staatssekretariat für Sicherheitspolitik SEPOS
Fachstelle des Bundes für Informationssicherheit

Massnahmenpaket zur Vermeidung künftiger Datenabflüsse
Zusätzlich identifizierter Handlungsbedarf

Ergebnisse aus dem Workshop «Empfehlungen Informationssicherheit» vom 20. März 2024

Basierend auf den Empfehlungen aus dem Untersuchungsbericht vom 28.03.2024 der Administrativuntersuchung Datenabfluss haben die Informationssicherheitsbeauftragten (ISD) der BK und der Departemente, die internen Leistungserbringer der Bundesverwaltung und Vertreterinnen und Vertreter des BACS, des BBL und der armasuisse den Handlungsbedarf zur Vermeidung künftiger Datenabflüsse, insbesondere bei Lieferanten, beurteilt und gemeinsam Massnahmen erarbeitet. Der Workshop wurde moderiert von der Fachstelle des Bundes für Informationssicherheit im Staatssekretariat für Sicherheitspolitik (SEPOS).

Unmittelbar nach dem Vorfall bei der Xplain AG haben die Departemente und Verwaltungseinheiten Sofortmassnahmen ergriffen und umgesetzt. Weiter hat der Bundesrat auf den 1. Januar 2024 das neue Informationssicherheitsgesetz (ISG) in Kraft gesetzt, wodurch bereits viele Massnahmen eingeleitet wurden, welche die Sicherheit systemisch und nachhaltig verbessern werden. Die nachfolgend beschriebenen Massnahmen stellen den zusätzlich identifizierten Handlungsbedarf dar, ergänzend zu den bereits getroffenen oder im neuen Gesetz vorgesehenen Vorkehrungen.

Die zivile Bundesverwaltung und die Armee arbeiten zurzeit an der Umsetzung des neuen Rechts. Da damit grundlegende und systemische Änderungen im bisherigen Sicherheitsmanagement des Bundes vorgenommen werden, ist der Aufwand in der Anfangsphase gross. Handlungsspielraum für zusätzliche Massnahmen ohne zusätzliche Ressourcen ist bei den Departementen und Ämtern kaum vorhanden. Die ISD der Departemente und der BK sind sich einig, dass die Umsetzung des ISG hohe Priorität haben muss.

Die Massnahmen werden in drei Kategorien eingeteilt: Sicherheitsmanagement, Ausbildung und Sensibilisierung sowie die sichere Kommunikation mit Dritten.

1.1 Standardisierte Vertragsklauseln in Lieferantenverträgen

Die AGB des Bundes und die Standardklauseln zu Cybersicherheitsbedrohungen sind in der Praxis oft zu unspezifisch, um mit den Lieferanten die konkreten, auftragsbezogenen Sicherheitsbedürfnisse zu stipulieren. Aus diesem Grund hat das VBS (GS) bereits im Jahr 2022 die Gestaltung von detaillierten Informationssicherheitsklauseln in Auftrag gegeben, bestehend aus zwingend für sämtliche Beschaffungen des VBS geltenden Vertragsklauseln (Muss-Vorschriften) und aus massgeschneiderten, die je nach Auftrag und Datenschutzbedürfnissen zur Anwendung kommen (Kann-Vorschriften). Das SEPOS (Fachstelle des Bundes für Informationssicherheit) wird gemäss Artikel 10 Absatz 3 ISV entsprechende Klauseln empfehlen.

Die Gestaltung dieser standardisierten Vertragsklauseln hat sich als schwierig erwiesen, weil gewisse dafür nötige technische Sicherheitsvorgaben heute entweder fehlen oder für Externe teilweise schwierig umzusetzen sind (z.B. IKT-Grundschutz des Bundes). Die neuen Vorgaben des Bundes müssen so gestaltet werden, dass sie grundsätzlich sowohl für die internen Leistungserbringer des Bundes als auch für externe Dienstleister praktisch umsetzbar und in den Verträgen vereinbar sind. Dieser Bedarf betrifft im Übrigen auch die Kantone, die den IT-Grundschutz des Bundes umsetzen müssen, wenn sie auf Systeme des Bundes zugreifen.

Massnahme 1:

Das VBS (SEPOS) wird beauftragt, standardisierte Vertragsklauseln zur Informationssicherheit nach Artikel 10 Absatz 3 ISV bis Ende 2024 zu erarbeiten.

Massnahme 2:

Das VBS (SEPOS) wird beauftragt, bis Ende 2024 Sicherheitsvorgaben zur Zusammenarbeit mit Lieferanten zu erarbeiten. Zu regeln sind beispielsweise die Quittierung der Herausgabe von Daten an bundesexterne Stellen sowie das regelmässige und dokumentierte Löschen von operativen Bundesdaten bei Lieferanten.

1.2 Inventarisierung von Lieferantenbeziehungen

Eine wichtige Erkenntnis aus der Administrativuntersuchung «Datenabfluss Xplain» ist die Notwendigkeit, ein aktives und effektives Lieferantenmanagement zu führen. Mittelfristig werden die Departemente und die Ämter in der ISMS-Anwendung ihre Schutzobjekte mit ihren Lieferanten verbinden können und somit die entsprechenden Risiken und Abhängigkeiten beurteilen können. Die Bundesverwaltung kann aber nicht zwei Jahren warten, um eine bessere Übersicht über ihre Lieferantenbeziehungen zu verfügen. Das BBL ist heute bereits in der Lage, auf Anfrage Listen der Beziehungen von vertraglichen wie finanziellen Natur mit Lieferanten der Verwaltungseinheiten zu erstellen.

Massnahme 3:

Die Verwaltungseinheiten werden beauftragt, bis Ende 2024 ihr Inventar der Schutzobjekte mit den beteiligten Lieferanten zu ergänzen. Die Listen von Lieferanten werden durch das EFD (BBL) zur Verfügung gestellt.

Massnahme 4:

Die BK und die Departemente werden beauftragt, dem VBS (SEPOS) im Rahmen der ordentlichen Berichterstattung 2024 über die Umsetzung der Massnahme zur Inventarisierung der Lieferantenbeziehungen zu rapportieren.

1.3 Kontrollen und Audits

Die Informationssicherheitsbeauftragten der Departemente sind sich einig, dass im Bereich Audits dringender Handlungsbedarf besteht. Der Bedarf betrifft nicht nur die Überwachung der Umsetzung der Informationssicherheit bei Lieferanten, sondern auch die internen Sicherheitsaudits. Artikel 13 ISV verlangt von allen Verwaltungseinheiten, dass sie in einem jährlichen Kontroll- und Auditplan festhalten, wie sie die Umsetzung der Informationssicherheit in ihrem Bereich sowie bei Dritten überprüfen wollen. Die Sicherheitsverantwortlichen der Ämter entscheiden über die Durchführung von Audits. Eine zentrale Beschaffung wäre effizienter als wenn jede einzelne Verwaltungseinheit selber externe Unterstützung für die Durchführung von Audits beschaffen würde. Das BBL soll beauftragt werden, Auditdienstleistungen auf Abruf für alle Verwaltungseinheiten zu beschaffen. Die ISV sieht zudem vor, dass die Fachstelle des Bundes für Informationssicherheit (SEPOS) den Auditbedarf der gesamten Bundesverwaltung erhebt und selber Audits durchführen kann. Es geht darum, dass die Audits bei den internen und externen Leistungserbringer bundesweit konsolidiert und priorisiert erfolgen. Dies ist insbesondere der Fall für sicherheitsempfindliche Firmen, bei denen das Betriebssicherheitsverfahren durchgeführt wird. Als zentrale Anlaufstelle sieht das ISG die Fachstelle Betriebssicherheit im SEPOS vor.

Massnahme 5:

Das VBS (SEPOS) erarbeitet zusammen mit den Beschaffungsstellen des Bundes und den Informationssicherheitsbeauftragen ein Konzept zur Kontroll- und Auditfähigkeit bei Lieferanten aufgrund der gesetzlichen Verpflichtung aus dem ISG und setzt dieses Konzept auf einem risikobasierten Ansatz um.

Massnahme 6:

Das EFD (BBL) wird beauftragt, Auditdienstleistungen auf Abruf für alle Verwaltungseinheiten zu beschaffen.

1.4 ISMS-Anwendung

Für eine möglichst wirksame und effiziente Umsetzung durch die Departemente und die Ämter der neuen Vorgaben, insbesondere der ISMS-Vorgaben der Informationssicherheitsverordnung (ISV), arbeiten das EFD (BIT) und das VBS (GS) gemeinsam an der Beschaffung und Einführung einer standardisierten ISMS-Anwendung, mit welcher die Aufgaben und Prozesse der ISV digitalisiert werden. Die ISMS-Anwendung soll im

Jahre 2025 zur Einführung und Nutzung durch die Ämter bereitstehen. Der Zuschlag wurde am 20.03.2024 auf SIMAP publiziert.

Mit der ISMS-Anwendung wird die Inventarisierung von Informationen und Informationssysteme (sogenannte «Schutzobjekte») systematisiert und standardisiert. Mit der ISMS-Anwendung wird inskünftig die Beteiligung von Dritten (Lieferanten oder Kantone) systematisch erfasst, die Risiken beurteilt und allfällige Sicherheitsmassnahmen dokumentiert. Das VBS und das EFD werden mittelfristig dafür sorgen, dass die Daten über die Lieferanten aus bereits bestehenden Datensammlungen bezogen werden («once-only» Prinzip). Bis dahin stellt die BBL bei Bedarf Listen zur Verfügung.

Wenn alle Verwaltungseinheiten die standardisierte ISMS-Anwendung für ihr Sicherheitsmanagement benutzen, können sowohl die Departemente als auch das SEPOS per Mausklick unter anderem die Übersicht über die Schutzobjekte, die informationssicherheitsrelevanten Lieferanten und den Stand der Umsetzung von Vorgaben und Massnahmen haben. Die ISD befürworten deshalb eine Bezugspflicht der ISMS-Anwendung für alle Verwaltungseinheiten des Bundes. Das Informationssicherheitsrecht des Bundes soll an geeigneter Stelle mit einer entsprechenden Vorgabe ergänzt werden.

Massnahme 7:

Das VBS (SEPOS) wird beauftragt, bis Mitte 2025 zu prüfen, ob die Verwaltungseinheiten (BK, Departemente und Ämter) verpflichtet werden sollen, für ihr Sicherheitsmanagement die standardisierte ISMS-Anwendung des Bundes zu benutzen, sobald diese bereitsteht.

2.1 Ausbildungskonzept für die funktionsbezogenen Ausbildungsbedürfnisse

Bei der Analyse von Sicherheitsvorfällen wird immer wieder festgestellt, dass die Mitarbeiterinnen und Mitarbeiter aller Stufen die bestehenden Vorgaben entweder nicht kennen oder nicht systematisch anwenden. Ein Beispiel dafür ist Artikel 11 der Verordnung über die digitale Transformation und die Informatik, welcher das Zugänglichmachen von Daten für externe Leistungserbringer regelt. Einmalige Ausbildungs- und Sensibilisierungsmassnahmen nach einem Vorfall sind oft kostspielig und ziehen meistens keine nachhaltige Verbesserung der Sicherheit nach sich. Deshalb müssen Ausbildungsmassnahmen Teil eines übergeordneten und nachhaltigen Konzepts sein und deren Umsetzung und Wirksamkeit gemessen werden.

Das VBS soll beauftragt werden, in Zusammenarbeit mit der BK und den Departementen, bis Ende 2024 in einem Ausbildungskonzept die Ausbildungsbedürfnisse für die jeweiligen Personenkategorien (z.B. Anwendungsverantwortliche, Projektleitende, Projektrollen wie ISDSV, Führungskräfte, allgemeine Mitarbeitende, Informationssicherheitsverantwortliche und -beauftragte usw.) zu definieren und den Zeitplan für die

Durchführung der Ausbildungsmassnahmen zu erarbeiten. Es stellt dabei sicher, dass die Wirksamkeit der Ausbildungsmassnahmen überprüft wird.

Massnahme 8:

Das VBS (SEPOS) wird beauftragt, in Zusammenarbeit mit der BK und den Departementen, bis Ende 2024 in einem Ausbildungskonzept die funktionsbezogenen Ausbildungsbedürfnisse zu definieren und einen Zeitplan für die Durchführung der Ausbildungsmassnahmen zu erarbeiten. Die Fachstelle stellt dabei sicher, dass die Wirksamkeit der Ausbildungsmassnahmen überprüft wird.

Für die sichere Kommunikation auf Stufe «vertraulich» steht der Bundesverwaltung der Standarddienst-Service VSK bzw. «Threema» zur Verfügung. Die Bundesverwaltung ist jedoch mit dem Umstand konfrontiert, dass ihr geeignete Mittel fehlen, um departementsübergreifend oder mit externen Partnern in Gruppen sicher auf Stufe «vertraulich» oder sogar «geheim» per Video zu kommunizieren. Während der Pandemie wurde beispielsweise der Bedarf an ein sicheres Videokonferenzsystem klar. Die Bundesbehörden müssen in der Lage sein, untereinander und mit Partnern aus den Kantonen und der Industrie sowie mit den internationalen Partnern sicher zu kommunizieren (Daten, Sprache, Bilder und Video). Die BK führt deshalb im Rahmen der Standarddienste Mitte 2024 mit dem Projekt Secure Video Conferencing Service eine auf Webex basierende Lösung zur sicheren (bis Stufe besonders schützenswerte Personendaten) Videokommunikation zur Verfügung.

Massnahme 9:

Die BK wird beauftragt, nach Konsultation der Konferenz der Informationssicherheitsbeauftragten, der Generalsekretärenkonferenz (GSK) bis Ende 2024 eine Übersicht der vorhandenen Kommunikationsmittel und deren Einsatz für die jeweiligen Klassifizierungsstufen, insbesondere mit Dritten, vorzulegen.

Bern, 24.04.2024