Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

26. Juni 2024

Bericht Informatiksicherheit Bund 2023

Inhalt

1 Einleitung

Gestützt auf die während der Berichtsperiode massgebende Cyberrisikenverordnung (CyRV, Art. 11 Abs. 2) [1] erstattet das Bundesamt für Cybersicherheit (BACS) dem Bundesrat Bericht über den Stand der Informationssicherheit beim Bund per Ende 2023. Ab Berichtsperiode 2024 wird diese Aufgabe aufgrund des Inkrafttretens des neuen Informationssicherheitsgesetzes an das Staatssekretariat für Sicherheitspolitik (SEPOS) übergehen (vgl. unten Ziff. 5.2.2). [2]

Als Basis des Berichtes dient eine strukturierte Umfrage bei allen Informatiksicherheits-beauftragten der Departemente und der Bundeskanzlei zum Stand ihrer Informatiksicherheit, welche - zusammen mit den Sicherheitsmeldungen und -berichten der bundesinternen Leistungserbringer (LE) - berücksichtigt wurden. Das BACS schätzt aufgrund dieser Datenlage die Informationssicherheit im Bund ein.

Das Jahr 2023 war geprägt von Cybervorfällen, welche die Bundesverwaltung stark betroffen haben. Im Zentrum stehen dabei die Angriffe der pro-russischen Hacktivistengruppe «NoName057(16)» auf die Verfügbarkeit von Informatikmitteln der Bundesverwaltung, der Datenabfluss bei Dienstleistern des Bundes (insbesondere bei der Firma Xplain AG) sowie Sicherheitsvorfälle bei Cloud-Anbietern des Bundes. Für die Aufarbeitung des Datenabflusses im Fall Xplain AG hat der Bundesrat eine Administrativuntersuchung beschlossen. Diese beinhaltet Empfehlungen, wie künftig solche Vorfälle vermieden werden können. Der vorliegende Bericht enthält keine Analyse zu möglichen Massnahmen in diesem Bereich, weil die erwähnte Administrativuntersuchung vor diesem Bericht veröffentlicht wurde.

Das zweite Kapitel beschreibt den aktuellen Stand der Informatiksicherheit in der Bundesverwaltung im Berichtsjahr 2023, die Organisation der Informatiksicherheit in der Bundesverwaltung sowie die Ergebnisse aus der Umfrage zu den Compliance-Anforderungen betreffend Sicherheitsdokumentationen.

Die gravierendsten Sicherheitsvorfälle in der Bundesverwaltung des vergangenen Jahres werden im dritten Kapitel erläutert.

Im vierten Kapitel werden die wichtigsten Aktivitäten und Massnahmen, sowohl innerhalb als auch ausserhalb der Bundesverwaltung, dargestellt.

Zum Schluss werden im fünften Kapitel die wichtigsten Erkenntnisse aus dem Bericht zusammengefasst und es erfolgt ein kurzer Ausblick.

2 Stand der Informatiksicherheit in der Bundesverwaltung

Die Risiken und damit die Angriffsversuche auf die Informatik der Bundesverwaltung, wie auch auf die der externen Zulieferer, nehmen nicht zuletzt wegen der aktuellen geopolitischen Lage stetig zu.

Die Vorfälle im Berichtsjahr 2023 haben unter anderem aufgezeigt, wie wichtig das Lieferantenmanagement für die Cybersicherheit ist. Es bestehen Defizite bei der bundesweiten Daten-Governance und Mängel bei der Übersicht über die Geschäftsbeziehungen mit externen Partnern. In der Vergangenheit gab es nur beschränkte Möglichkeiten, die

[1] Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisiken-verordnung; CyRV, AS 2023 735). Diese wurde am 01.1.2024 durch die Informationssicherheitsverordnung (ISV; SR 128.1) abgelöst.

[2] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-98807.html

Cybersicherheit bei den Lieferanten und bei gelieferter Software zu überprüfen. In beiden Fällen liegt die Verantwortung der Vertragsgestaltung und Abnahme dezentral bei der beschaffenden Verwaltungseinheit. Dies führt dazu, dass kein einheitlicher Sicherheitsstandard erreicht wird.

Bei einer Vorfallbewältigung auf mehreren Staatsebenen, wie im Fall Xplain AG, zeigte es sich ausserdem, dass die notwendigen Prozesse in der Bundesverwaltung zwar mehr oder weniger eingespielt waren, sich diese Prozesse mit den Kantonen, aber erst etablieren mussten.

Die Vorfälle im Berichtsjahr 2023 haben aufgezeigt, dass die Compliance allein keine Cybersicherheit garantieren kann. Zudem müssen bei den Schutzobjektverantwortlichen noch Kompetenzen bezüglich Cybersicherheit aufgebaut werden, damit diese die zur Compliance geforderten Massnahmen auch beurteilen und richtig umsetzen können (siehe Kapitel 4.3.2).

2.1 Organisation der Informatiksicherheit in der Bundesverwaltung

Die Informatiksicherheit in der Bundesverwaltung umfasst alle Massnahmen, um Cybervorfälle zu verhindern bzw. auftretende Cybervorfälle möglichst rasch zu erkennen und zu bewältigen. Ein Cybervorfall ist nach Artikel 5 Buchstabe d der Revision des Informationssicherheitsgesetzes (ISG) vom 29. September 2023[3] definiert als «Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist».

Damit die notwendigen Massnahmen zur Sicherstellung der Informatiksicherheit in der gesamten Bundesverwaltung umgesetzt werden, erlässt der Bundesrat entsprechende Verordnungen und Weisungen. Die Erarbeitung der Informatiksicherheitsvorgaben erfolgte bis anhin durch das Nationale Zentrum für Cybersicherheit (NCSC), welches per 1. Januar 2024 in das Bundesamt für Cybersicherheit (BACS) im VBS überführt wurde. Die Erarbeitung der Informationsschutzvorgaben für die Bundesverwaltung erfolgte bis anhin im Generalsekretariat VBS (GS-VBS). Künftig werden die Vorgaben zusammengeführt und durch die Fachstelle Informationssicherheit im Staatssekretariat für Sicherheitspolitik (SEPOS) erlassen.[4]

Die Verwaltungseinheiten sind für die Einhaltung bzw. Umsetzung der Informatiksicherheitsvorgaben in ihrem jeweiligen Zuständigkeitsbereich verantwortlich. Dazu prüfen sie ihre Informatikschutzobjekte[5] regelmässig, bestimmen die notwendigen Sicherheitsmassnahmen und setzen diese um.

[3] BBl 2023 2296 (Referendumsvorlage)

[4] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-98807.html

[5] Anwendungen, Services, Systeme, Netzwerke, Datensammlungen, Infrastrukturen und Produkte der Informatik; mehrere gleiche oder zusammenhängende Objekte können zu einem Informatikschutzobjekt zusammengefasst werden, Art. 3 Bst. h CyRV

2.2 Ergebnisse Compliance-Anforderungen von Sicherheitsdokumentationen

Für 81.8% der gesamthaft erhobenen 2176 Schutzobjekte sind gültige Sicherheitsdokumentationen vorhanden. Die sich daraus ergebenden Sicherheitsmassnahmen sowie deren Kontrolle wurden 2023 bei 74.4% aller Schutzobjekte ausgewiesen (Vorjahr 72.5%).

Damit Sicherheitsmassnahmen erfolgreich umgesetzt werden können, müssen die dazu erforderlichen Sicherheitsdokumentationen in aktueller Form (nicht älter als 5 Jahre) vorliegen. Dies trifft für 92% der eingangs erwähnten 81.8% gültigen Sicherheitsdokumentationen zu. Im Vergleich zum Vorjahr mit 92.6% ist dieser Wert nur marginal gesunken. Dies lässt sich dadurch erklären, dass gegenüber 2022 viele Unterlagen im 2023 aus der 5-Jahres-Gültigkeitsperiode gefallen sind. Sie traten 2018 in Kraft und die Departemente haben Schwierigkeiten, diese jetzt gleichzeitig zu aktualisieren. Nichtsdestotrotz zeigen die Zahlen dem BACS auf, dass die Erhebung der Schutzobjekte und die Umsetzung der Sicherheitsmassnahmen von den Verwaltungseinheiten auf vergleichbarem Niveau gegenüber dem Vorjahr geblieben sind.

Die gemeldeten Zahlen waren und sind generell zu tief und weisen auf ein Problem bei der Compliance hin. Auch lässt sich aus den Zahlen keine allgemeine Aussage ableiten, ob die Qualität der IT-Sicherheitsdokumente ausreichend geprüft und ob diese auch wirklich kritisch hinterfragt wurden. Selbst eine aktuelle Dokumentation garantiert nicht, dass die Sicherheitsmassnahmen entsprechend implementiert und überprüft worden sind. Das BACS hat keine Auditmöglichkeiten dazu. Neue Möglichkeiten im Rahmen des Informationsschutzgesetzes müssen geprüft werden.

3 Sicherheitsvorfälle

Sicherheitsvorfälle können schwerwiegende Folgen haben, wie die Offenlegung vertraulicher Informationen, Sabotage, Erpressung oder den Ausfall kritischer Systeme. Nachfolgend werden diejenigen Sicherheitsvorfälle aufgelistet, welche im Berichtsjahr 2023 für die Bundesverwaltung eine grosse Relevanz hatten.

3.1 DDoS-Angriffe

DDoS (Distributed Denial of Service) -Angriffe sind Angriffe auf Netzwerkressourcen bis hin zum Zielserver, bei denen Kriminelle oder staatliche Akteure die Kapazitätsbeschränkungen ausnutzen, die für jede Netzwerkressource besteht. Ziel ist es, die Verfügbarkeit der angegriffenen Ressource zu stören, indem sehr viele Anfragen an diese gesendet werden, um ihre Kapazität zur Verarbeitung von Anfragen zu überlasten. Die Anzahl von Anfragen überschreitet die Kapazitätsgrenze des Angriffsziels, was dazu führt, dass Antworten viel langsamer als gewöhnlich erfolgen oder manche Benutzeranfragen unbeantwortet bleiben.

3.1.1 DDoS-Angriff der Gruppe «NoName057(16)» auf die Bundesverwaltung

Ab dem 7. Juni 2023 startete eine pro-russische Hacktivisten-Gruppe mit dem Namen «NoName057(16)» DDoS-Attacken auf ausgewählte Ziele in der Schweiz. Erstes Ziel war die Parlaments-Webseite (www.parlament.ch). Die Gruppierung gab die bevorstehende Ansprache des ukrainischen Präsidenten Wolodymyr Selenskyj sowie die Diskussion zu den Waffenexporten im Schweizer Parlament als Grund der Angriffe an.

Die Angriffe erfolgten in einem Zeitraum von rund zwei Wochen auf wechselnde Angriffsziele. Am 19. Juni wechselte die Gruppe auf neue Ziele im Ausland.

Ziele	Datum						
	12.06.2023	13.06.2023	14.06.2023	15.06.2023	16.06.2023	17.06.2023	18.06.2023
Bundesverwaltung	4	1		1		2	
Kantone			2		3		
Städte			6				6
Public Service	2		1	1			1
Flughafen		8				6	
Finanzsektor				5		2	1
Andere				1	3		
Rüstung				1			
Total 57	**6**	**9**	**9**	**9**	**6**	**10**	**8**

Tabelle: Darstellung der erfolgreichen DDoS-Angriffe pro Tag

Die Angriffe waren so dimensioniert, dass sie alle angegriffenen Organisationen in Bedrängnis brachten. Die Bekämpfung der Angriffe war in der Bundesverwaltung mit erheblichem Aufwand verbunden.

Die Bundesverwaltung ist bestrebt, dass im Falle eines DDoS-Angriffs interne Anwendungen weiterlaufen, auch wenn extern erreichbare Systeme überlastet sind und diese nicht mehr korrekt auf Anfragen antworten können. Bei diesem Angriff war das nicht der Fall. Wichtige interne Systeme waren auf Dienste von externen Systemen angewiesen, was schliesslich zu Arbeitseinschränkungen über wenige Stunden führte. Das NCSC hat im November 2023 einen detaillierten Analysebericht zu den DDoS-Angriffen publiziert (siehe Beilage).[6]

In den Auswirkungen wesentlich schwerwiegender als die DDoS-Angriffe, sind jedoch Ransomware-Angriffe auf Firmen und Behörden, auf welche im nachfolgenden Kapitel 3.2 vertiefter eingegangen wird.

3.2 Ransomware Angriffe

Ein Ransomware-Angriff ist ein Cybervorfall, bei dem die Daten und Dateien des Opfers gestohlen und verschlüsselt werden. Die Angreifer fordern im Anschluss ein Lösegeld, um einerseits die Daten wieder frei zu geben und andererseits auf eine Veröffentlichung zu verzichten («double extortion», zu Deutsch doppelte Erpressung). Wird das Lösegeld nicht bezahlt, riskiert das Opfer die Veröffentlichung der gestohlenen Daten im Darknet. Ransomware-Angriffe können Unternehmen oder Behörden betreffen, aber auch Privatpersonen, deren Daten häufig zum Kollateralschaden dieser Angriffe gehören.

3.2.1 Vorfall bei der Firma Xplain AG

Der Ransomware-Angriff auf die Firma Xplain AG, ein wichtiger Dienstleister verschiedener Verwaltungseinheiten und Kantone, hat zum Abfluss von grossen Mengen an Informationen von insgesamt 431GB geführt. Darin enthalten sind 146’623 Dateien und 19’863 Ordner.

[6] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/ddos-bericht-6-2023.html

Betroffen waren auch sicherheitsrelevante und personenbezogene Daten, insbesondere aus dem Bereich der inneren Sicherheit. Die Angreifer haben die Daten im Darknet publiziert, womit sie öffentlich einsehbar wurden. Die Veröffentlichung vertraulicher und sicherheitsrelevanter Daten hat gravierende Auswirkungen und führt zu grossen Aufwänden. Es mussten Sofortmassnahmen identifiziert und umgesetzt werden, um die unmittelbaren Risiken einzudämmen und Betroffene zu informieren. Es musste zudem beurteilt werden, ob Systeme und Datenbanken der Bundesverwaltung kompromittiert wurden.

Der Vorfall führte dazu, dass wichtige Systeme vorübergehend nicht mehr genutzt werden konnten. Zudem war ein hoher personeller Aufwand nötig, um abschliessend zu eruieren, welche Ämter Kunden der Xplain AG sind, welcher Art die Vertragsbeziehungen sind, welche Auditrechte festgelegt wurden und über welchen Zeitraum die Verträge laufen.

Ein erster Schritt ist eine umfassende Aufarbeitung des Vorfalls. Der Bundesrat hat am 1. Mai 2024 die Ergebnisse der Administrativuntersuchung veröffentlicht. Am gleichen Tag hat der Eidgenössische Datenschutzbeauftragte seinen Bericht publiziert.
Im Bericht der Administrativuntersuchung wird festgestellt, dass in den letzten Jahren in wenigen Fällen aktiv produktive Daten des Bundes an die IT-Umgebung der Xplain AG übermittelt wurden. Dies geschah in Test- und Integrationsphasen einer Software oder im Rahmen von Wartungs- oder Supportdienstleistungen sowohl durch Mitarbeitende der Xplain AG, welche über ein E-Mail-Konto des Bundes verfügten, als auch durch Mitarbeitende des Bundes. Zudem führte eine in einigen Xplain-Anwendungen enthaltene und inzwischen deaktivierte Support-Funktion zu grossen Mengen von Datentransfers von der IT-Umgebung des Bundes in die IT-Umgebung der Xplain AG. Auf der Basis des Berichts hat der Bundesrat Massnahmen zur Vermeidung künftiger Datenabflüsse beschlossen und diese in einem Massnahmenpaket (siehe Kapitel 5.2.1) festgehalten.

Das Nationale Zentrum für Cybersicherheit (NCSC) hat die Vorfallbewältigung geleitet, hat Massnahmen zur Wiederherstellung der Sicherheit der Systeme definiert und eine vollständige Analyse, welche durch BV-interne und externe Ressourcen mit unterstützt wurde, aller veröffentlichten Daten durchgeführt. Als Beitrag zur Aufarbeitung des Vorfalls und zur Schaffung einer grösstmöglichen Transparenz publizierte es einen Bericht über das Vorgehen und die Resultate der Datenanalyse.[7]

Dieser Ransomware-Angriff bei der Firma Xplain AG zeigt exemplarisch auf, dass die Ermittlung des Schadensausmasses bei einem Datenabfluss sehr schnell sehr aufwändig werden kann. Der grosse Aufwand wäre jedoch verhinderbar gewesen, wenn man von Anfang an gewusst hätte, welche Daten beim Lieferanten waren und wer Kunde der Xplain AG war. Weiter wurde festgestellt, dass das Vorfallmanagement über mehrere Staatsebenen hinweg nicht standardisiert ist. Die Prozesse in der Bundesverwaltung waren mehr oder weniger eingespielt, jedoch mussten sich die Prozesse mit den Kantonen erst etablieren. Basierend auf dieser Erfahrung wird nun ein Standardvorgehen und eine einheitliche Einstufung der Schwere eines Vorfalls definiert. Ausserdem wurde die gelieferte Software bei der Abnahme einer ungenügenden Überprüfung unterzogen. So ist z. B. niemandem aufgefallen, dass die Fehler-Reportfunktion sensible Daten an Xplain AG versendet hat.

[7] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/bericht-datenanalyse-xplain.html

3.2.2 Weitere Vorfälle analog Xplain AG

3.2.2.1 Ransomware-Angriff auf arb Architekten AG

Das Bundesamt für Bauten und Logistik (BBL) wurde am 21. Juli 2023 über einen Angriff bei der Zulieferfirma arb Architekten AG informiert. Die Ransomware-Gruppierung «Abyss» hatte ca. 220GB an unkomprimierten Daten, darunter Baupläne von Schweizer Botschaften und Residenzen im Ausland, entwendet und diese in verschlüsselter Form im Darknet publiziert. Die Firma konnte die verschlüsselten Daten wiederherstellen und reichte Strafanzeige ein. Nach Ablauf der Zahlungsfrist für das Lösegeld am 1. September 2023 wurde der Schlüssel zum Entschlüsseln der gestohlenen Dokumente publiziert.

3.2.2.2 Vorfall bei der Firma Concevis AG

Am 14. November 2023 wurde eine weitere Schweizer Softwarefirma, Concevis AG, das Opfer eines Ransomware-Angriffs. Die Angreifer verschlüsselten sämtliche Server der Firma und entwendeten Daten, darunter mutmasslich auch operative Daten der Bundesverwaltung. Die betroffenen Stellen wurden rasch informiert und erste Massnahmen wurden getroffen, um das Sicherheitsrisiko für die Bundesverwaltung zu minimieren. Die von Concevis entwickelten Anwendungen werden durch Leistungserbringer der Bundesverwaltung betrieben. Eine Kompromittierung von Systemen des Bundes ist aktuell unwahrscheinlich. Die Folgen des Angriffs sind zum aktuellen Zeitpunkt noch nicht vollständig bekannt.

3.3 Sicherheitsprobleme bei Cloud-Anbietern

Fehlkonfigurationen und Sicherheitslücken bei Cloud-Anbietern können zu Datenlecks und Angriffen führen. Nicht geschlossene Sicherheitslücken und Fehlkonfigurationen in Cloud-Umgebungen können von Angreifern ausgenutzt werden, um in die Systeme einzudringen. Die zwei in diesem Kapitel aufgeführten Cloud-Sicherheitsprobleme, hatten zwar noch keine direkten Auswirkungen auf die Bundesverwaltung. Sie haben aber das Potential das Vertrauen der Bevölkerung in die vom Bund genutzten Cloud-Lösungen zu beinträchtigen. Die Erkenntnisse aus diesen Sicherheitsvorfällen müssen bei der Konzeption von Sicherheitsmassnahmen zu Cloud-Lösungen mit einbezogen werden.

3.3.1 Malware-Verteilung mittels Microsoft Teams

Die Bundesverwaltung hat festgestellt, dass externe Benutzer über Chat-Nachrichten in Microsoft Teams Anhänge an Bundesmitarbeitende versenden können. Diese werden innerhalb Microsoft Teams nicht automatisiert auf Schadcode überprüft. Bei einem Test stellte das Computer Security Incident Response Team (CSIRT) des Bundesamts für Informatik (BIT) fest, dass die Datei erst beim Speichern durch den Virenschutz auf den Bundesgeräten erkannt und gelöscht wird. Das bedeutet, dass wir Bundesmitarbeitenden im Gegensatz zur heutigen Praxis keine zweite Verteidigungslinie gegen Malware beim Einsatz von Teams haben und der Schutz der Bundesgeräte nur noch vom lokalen Malware-Schutz abhängig sein wird.

3.3.2 Storm-0558 Vorfall in der Microsoft Cloud

Am 11. Juli 2023 veröffentlichte Microsoft in zwei Blogbeiträgen, dass erfolgreiche Angriffe auf E-Mails in Exchange Online und Outlook.com von einer US-Bundesbehörde bemerkt wurden. Diese konnten aber in der Zwischenzeit unterbunden werden. Diese Angriffe wurden einer mutmasslich staatlichen chinesischen Hackergruppe namens «Storm-0558» zugeschrieben. Die Angreifer hatten ab dem 11. Mai 2023 Zugriff auf E-Mails von ca. 25, mehrheitlich

europäischen Behörden erhalten. Zusätzlich konnten sie auf mehrere private E-Mail-Konten von Mitarbeitenden dieser Behörden zugreifen.
Die Angreifer konnten mittels eines entwendeten Signier-Schlüssels die für die Zugriffe genutzten Authentifizierungstoken[8] fälschen. Mit diesem Vorgehen hätten auch weitere Services der M365 Cloud[9] kompromittiert werden können. Diese Angriffe wurden am 16. Juni 2023 entdeckt und die ausgenutzten Schwachstellen anschliessend von Microsoft geschlossen. Die Bundesverwaltung war von diesem Angriff nicht betroffen.
Der Vorfall zeigt aber auf, dass ein sicheres Schlüsselmanagement auch für einen Grosskonzern eine grosse Herausforderung darstellt. Er hat den Entscheid der Bundesverwaltung, die Verschlüsselungsmöglichkeiten der Microsoft Cloud nicht zu nutzen, bestätigt.

4 Aktivitäten und Massnahmen

4.1 Bug-Bounty-Programme

In der Berichtsperiode 2023 hat das NCSC für mehrere Verwaltungseinheiten Bug-Bounty-Programme für einzelne Services und Applikationen durchgeführt. Zusätzlich wurde im Sommer 2023 das NCSC-eigene Bug-Bounty-Programm lanciert und schrittweise weiterentwickelt, so dass ethische Hacker ab September 2023 Schwachstellen in allen öffentlich exponierten Systemen (*.admin.ch) der Bundesverwaltung suchen und melden konnten.

Im September und Oktober 2023 erreichten das NCSC innerhalb von 10 Tagen insgesamt 134 Meldungen zu Schwachstellen, welche in den öffentlich exponierten Systemen der Bundesverwaltung identifiziert wurden. 98 dieser Meldungen wurden nach einer technischen Analyse als gültige Schwachstellen eingestuft. Betroffen von den Sicherheitslücken waren alle Departemente und die Bundeskanzlei.

Die bisherigen Erkenntnisse aus dem Bug-Bounty-Programm des NCSC demonstrieren, dass nicht alle vorhandenen Sicherheitslücken in Systemen und Anwendungen mit Hilfe bestehender Sicherheitsmassnahmen identifiziert werden konnten. Die weit mehr als 100 gemeldeten Schwachstellen innerhalb von 10 Tagen belegen, dass die Bundesverwaltung auch in Zukunft dringend weiter in das Bug-Bounty-Programm des NCSC (heute BACS) investieren und weiter ausbauen sollte. Auf diese Weise erhält der Bund die Möglichkeit, proaktiv zu handeln, um potenzielle Sicherheitsrisiken in seinen IT-Systemen zu beseitigen, bevor diese von Angreifern ausgenutzt werden. Ausserdem leistet das Bug-Bounty-Programm des BACS einen massgeblichen Beitrag zur Steigerung der Cyberresilienz der Bundesverwaltung. Die Folgen von falsch oder unzureichend konfigurierten IT-Komponenten in der Bundesverwaltung können erhebliche Auswirkungen auf die Sicherheit und Integrität von Systemen, Applikationen oder Netzwerken haben.

[8] Die tokenbasierte Authentifizierung ist eine Möglichkeit, die Identität eines Nutzers oder Geräts zu bestätigen.

[9] Microsoft 365 (M365) ist ein Cloud-basierter Dienst von Microsoft, der eine Reihe von Produktivitäts-anwendungen und Kollaborationstools für Unternehmen umfasst.

4.2 Ausbildungsmassnahmen

4.2.1 Nationale Sensibilisierungskampagne Cybersicherheit S-U-P-E-R

Im Berichtsjahr 2023 organisierten die Schweizerische Kriminalprävention (SKP) und das NCSC, gemeinsam mit kantonalen und städtischen Polizeikorps, die dritte nationale Sensibilisierungskampagne S-U-P-E-R (www.s-u-p-e-r.ch) zum Thema Cybersicherheit. Zusätzlich zu den kantonalen und städtischen Polizeikorps beteiligte sich die Bundesverwaltung mit den Departementen EDI, EFD, EDA und WBF am Vertrieb der Kampagneninhalte. Die Kampagnen wurden departementsintern via Intranet, E-Mail und Plakate beworben.

Die Auswertung der Kampagne im November 2023 zeigte auf, dass das Konzept mit der Kampagnen-Startseite zum jeweils neuen Thema, den interaktiven Seiten[10] sowie mit dem gezeigten Quiz erfolgreich war. Erfreulich zu erwähnen ist die breite Unterstützung der Kampagne durch die Polizeikorps, die einzelnen Departemente der Bundesverwaltung und die Gemeinden. Die positiven Erkenntnisse aus dem Jahr 2023 fliessen in die Konzeption der S-U-P-E-R Abschlusskampagne 2024 mit ein.

4.2.2 Expertenkurse

Das NCSC hat 2023 drei Online-Expertenkurse zu den Themen «Sicherheitstechnologien für Cloud Computing», «End-to-End Encrypted (E2EE) Messaging» und «DNS-Sicherheit» für Mitarbeitende der Bundesverwaltung durchgeführt. Am ersten Kurs nahmen ca. 140 Mitarbeitende teil, am zweiten und dritten Kurs jeweils ca. 110 Mitarbeitende. Die Expertenkurse sind freiwillig und bieten den Teilnehmenden die Möglichkeit, spezifische, sicherheitsrelevante Problemstellungen besser zu beurteilen und/oder das neu erworbene Fachwissen in der Bundesverwaltung zu verteilen. Sie bilden ein zentrales Ausbildungselement, um das notwendige Sicherheitswissen bei IT-Fachkräften kosteneffizient zu steigern.

4.2.3 Mitarbeiterschulung Informatiksicherheit (Compliance)

Um Fragen der Mitarbeitenden zur Informatiksicherheit in den jeweiligen Verwaltungseinheiten direkt behandeln zu können, verfügt die Bundesverwaltung auf Stufe Departement und Bundeskanzlei über Informatiksicherheitsbeauftragte der Departemente (ISBD) und auf Stufe Amt über Informatiksicherheitsbeauftragte der Organisation (ISBO). Unter deren Leitung wurden 2023 rund 94% (Vorjahr ebenfalls 94%) der neu eintretenden Mitarbeitenden in die Belange der Informatiksicherheit eingeführt. Dieser Wert liegt nie bei 100%, weil es immer Mitarbeitende gibt, welche erst gegen Ende Jahr eingestellt werden und noch keine Zeit hatten das Modul «Informationssicherheit in der Bundesverwaltung» zu absolvieren. Andere Gründe sind krankheitsbedingte Abwesenheiten oder Benutzerkontos für Externe, welche nicht auf das Modul zugreifen können.

[10] Interaktiven Webseiten sind besonders beliebt um die User-Experience zu erhöhen.

4.3 Herausforderungen bei der Ausbildung

4.3.1 Schulung externer Dienstleister

Mehrere Departemente melden, dass sie ein grundsätzliches Problem haben, externe Mitarbeitende oder Dienstleister hinsichtlich der IT-Sicherheit adäquat zu sensibilisieren. Bundesinterne Mitarbeitende müssen obligatorisch bei Neueintritt und innerhalb der Probezeit spezifische E-Learnings zur Informatiksicherheit absolvieren. Für externe Mitarbeiter gilt diese Regel nicht und kann teilweise wegen technischen Gegebenheiten nicht generell umgesetzt werden, weil die externen Mitarbeitenden z. B. über kein Bundesgerät und/oder über keinen Zugriff auf das Web Based Training (WBT) verfügen. Einzelne Ämter haben gemeldet, dass sie Prozesse einführen, um externe Mitarbeiter gezielt aus- bzw. weiterbilden zu können.

Zusätzlich wurde erkannt, dass Ausschreibungsunterlagen und Vertragsbedingungen bei externen Dienstleistern um Schulungs- oder Weiterbildungsaspekte erweitert werden müssen, damit die Bundesverwaltung bei externen Mitarbeitern, die Kenntnisse in der Informatiksicherheit voraussetzen kann oder diese funktions- und stufengerecht schulen darf.

4.3.2 Schulung der Schutzobjektverantwortlichen

Aus den Meldungen geht hervor, dass die Rolle des Schutzobjektverantwortlichen[11] punktuell grössere fachliche Kompetenzen in Bezug auf die Bewertung und Umsetzung der IT-Sicherheitsdokumentation erfordert als die bezeichneten Schutzobjektverantwortlichen in der Realität aufbringen. Um diesem Umstand gerecht zu werden, müssen sie von den Informatiksicherheitsbeauftragten der Organisation (ISBO) enger begleitet oder wo möglich, entsprechend geschult oder ersetzt werden.

5 Schlussfolgerungen und Ausblick

5.1 Erkenntnisse

Neben Massnahmen für ein sicheres Datenmanagement und einer guten Cyberhygiene empfiehlt das BACS, Daten generell nur nach dem Prinzip «so viel wie nötig, so wenig wie möglich» und wenn möglich anonymisiert mit Dritten zu teilen. Sämtliche Geschäftsbereiche müssen ihre Lieferanten- und Dienstleistungsabhängigkeiten gemäss ihrer Kritikalität überprüfen. Basierend auf dieser Überprüfung sollte, besonders bei hoher Kritikalität, ein Auditrecht bei Lieferanten oder Dienstleistern sowie eine Meldepflicht von Vorfällen vertraglich festgehalten werden. Im Vertrag müssen auch Regelungen enthalten sein, wie mit Daten zu verfahren ist, welche nicht bis zum Dienstleister hätten gelangen sollen.
Ferner sind weitere technische Massnahmen für den proaktiven Schutz und zur Überwachung der eigenen Systeme sehr wichtig, um bei Unregelmässigkeiten entsprechende Gegenmassnahmen einleiten zu können. Dies beinhaltet, dass Verbindungs- und Kommunikationskanäle zwischen Zulieferern und den eigenen Organisationen bestmöglich geschützt werden. Die Notfallplanung muss stetig aktualisiert und getestet werden. Die Übungsszenarien sollten auch Lieferantenbeziehungen und indirekte Effekte von Datenabflüssen mit einbeziehen.

[11] Für das Schutzobjekt muss eine verantwortliche Person (innerhalb der verantwortlichen VE) als Schutzobjekt-verantwortliche/r definiert sein. Diese Person ist für die Umsetzung dieser Vorgabe zuständig. Sie muss sich ihrer Verantwortung bewusst und fachtechnisch in der Lage sein, die Verantwortung auch wahrzunehmen.

5.2 Ausblick

5.2.1 Angekündigte Massnahmen 2024

Der Bundesrat hat für das Jahr 2024 Massnahmen in einem Massnahmenpaket zur Stärkung der Informationssicherheit beschlossen und wird die Aktivitäten diesbezüglich noch weiter verstärken.

Das Massnahmenpaket fokussiert sich auf drei Bereiche:

- Erstens wird das Sicherheitsmanagement gestärkt, indem unter anderem bis Ende 2024 zusätzliche Sicherheitsvorgaben zur Zusammenarbeit mit Lieferanten erstellt werden. Die Kontroll- und Auditfähigkeit soll gestärkt werden.
- Zweitens wird bis Ende 2024 ein funktionsbezogenes Ausbildungskonzept für die Schulung und Sensibilisierung von Mitarbeitenden in Bezug auf bestehende Sicherheitsvorgaben erarbeitet.
- Drittens wird bis Ende 2024 eine Übersicht über die vorhandenen Kommunikationsmittel der Bundesbehörden erstellt.

Die Bundesverwaltung reagiert damit auf die Sicherheitsvorfälle im 2023.

Zur kurz- und mittelfristigen Stärkung der Informatiksicherheit werden die Departemente und die Bundeskanzlei weiterhin daran arbeiten, die Sicherheitsdokumentation aktuell zu halten und die darin geforderten Massnahmen zeitgerecht umzusetzen. Das BACS empfiehlt speziell bei der Implementation der Massnahmen einen Fokus zu setzen, da Dokumentation und effektive Implementierung zum Teil voneinander abweichen.

5.2.2 Änderung zukünftige Berichterstattung

Ab dem Berichtsjahr 2024 erstattet die Fachstelle des Bundes für Informationssicherheit im SEPOS dem Bundesrat gemäss Art. 83 Abs. 1 Bst. h ISG[12] jährlich Bericht über den Stand der Informationssicherheit des Bundes.

[12] SR 128 - Bundesgesetz vom 18. Dezember 2020 über... | Fedlex (admin.ch)