Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

Cybervorfall bei der Firma Xplain

Einschätzung des NCSC zum Audit-Bericht von Compass-Security aus technischer und organisatorischer Sicht der Cybersicherheit im Hinblick auf eine allfällige Weiterführung der Zusammenarbeit der Bundesverwaltung mit Xplain

Datum:	16. November 2023
Absender:	Nationales Zentrum für Cybersicherheit NCSC
Für:	PSK-D, sowie die Verwaltungseinheiten des Bundes mit Geschäftsbeziehungen mit Xplain
Kopien an:	Xplain

1 Ausgangslage

Die Firma Xplain wurde im Mai 2023 Opfer eines Ransomware-Angriffs der Gruppe «PLAY». Diese ist in der Schweiz seit längerem aktiv und hat auch bei diesem Vorfall viele, zum Teil klassifizierte Daten und Informationen gestohlen und im Darknet publiziert.

Xplain hat daraufhin ihre gesamte IT-Infrastruktur neu aufgebaut und ihre Prozesse angepasst. Um die Voraussetzungen für eine allfällige Weiterführung der Zusammenarbeit zwischen den betroffenen Organisationseinheiten der Bundesverwaltung und Xplain zu prüfen, ist ein externes Audit der neu aufgebauten IT-Infrastruktur und der Prozesse bei Xplain notwendig. Dieses wurde in den vergangenen Wochen durch Compass-Security durchgeführt und bildet die Grundlage für die vorliegende Einschätzung des NCSC.

2 Durchgeführtes Audit

Xplain hat am 21. August 2023 die Firma Compass-Security mit dem externen Audit beauftragt. Das NCSC hat an den jeweiligen Abgleichmeetings eine detaillierte Einsicht in das Audit und die durchgeführten Arbeiten, erhalten.
Die Basis für dieses Audit bildet der Massnahmenkatalog des NCSC vom 07. Juli 2023, welcher mit den betroffenen Bundesstellen erarbeitet worden ist (s. Massnahmenkatalog im Anhang). Die Kosten für das Audit und die Umsetzung der Massnahmen trägt Xplain.

2.1 Geforderte Massnahmen des NCSC

Das NCSC hat in Zusammenarbeit mit den betroffenen Bundesstellen die folgenden Massnahmenbereiche definiert, welche auditiert wurden:

- Authentifikation

- Data Management
- Netzwerk Sicherheit
- Active Directory
- Antivirus / EDR
- Zentrales Logging
- Build Environment
- Patch / Vulnerability Management
- Organisation (Verantwortlichkeiten und Prozesse)

2.2 Zusätzliche Massnahmen

Compass-Security hat aufgrund ihrer Erfahrungen und den neuesten Erkenntnissen mit Cyber-Vorfällen zusätzliche Massnahmen zum Massnahmenkatalog des NCSC vorgeschlagen, welche in ihrem Audit ebenfalls überprüft wurden.

Dies sind:
Vulnerabilities and Remediation

- General Infrastructure
- Automated Vulnerability Scanning
- Manual Hacking Network Services
- Network Discovery

External Penetration Test

- General Infrastructure
- Automated Vulnerability Scanning
- Manual Hacking Network Services
- Network Discovery

Detection Capabilities

- SIEM & Centralized Logging
- Endpoint Protection

Das NCSC war in die durchgeführten Arbeiten eingebunden und es fanden regelmässige Meetings mit Xplain und Compass-Security statt, dies mindestens einmal wöchentlich. Die Zusammenarbeit verlief offen und zielführend und das NCSC war über den Umsetzungsstand der geforderten Massnahmen jederzeit informiert.

Die Umsetzung der geforderten Massnahmen musste innert kürzester Zeit von Xplain in die Wege geleitet werden. Massnahmen wurden entsprechend ihrer Kritikalität priorisiert, abgearbeitet und umgesetzt. Dem NCSC ist bewusst, dass es nicht möglich war, alle Massnahmen in kürzester Zeit umzusetzen. Für Massnahmen, die noch nicht vollständig erfüllt sind, muss jedoch ein Umsetzungsplan vorgelegt werden. Die Umsetzungspläne liegen für alle noch nicht erfüllten Massnahmen vor. Die wichtigsten noch nicht erfüllten Massnahmen werden im folgenden Kapitel beschrieben.

2.3 Noch nicht vollumfänglich umgesetzte Massnahmen

Mit dem Umsetzungstand vom 16. Oktober 2023, wurden wichtige, jedoch noch nicht vollumfänglich umgesetzte Massnahmen erkannt.

Die eine Massnahme betrifft den **Aufbau eines Security Operation Centers (SOC).**
Die primäre Aufgabe eines SOC ist, sämtliche Aktivitäten auf Servern, Websites, in Datenbanken, Netzwerken, Anwendungen, Endgeräten und anderen Systemen zu überwachen mit dem Fokus, mögliche Sicherheitsbedrohungen aufzuspüren und so schnell wie möglich abzuwenden und entsprechend zu reagieren.
Aktuell werden durch Xplain zwar bereits sehr viele Logs gesammelt und an einem zentralen Ort gespeichert. Der Aufbau eines SOC ist dennoch zwingend, ist aber aufwändig und braucht Zeit. Xplain prüft aktuell verschiedene Lösungen und die Inbetriebnahme eines SOC ist zeitlich schwierig zu beziffern.

Eine weitere, noch nicht vollumfänglich umgesetzte Massnahme betrifft die **Zugriffskontrolle auf die Quellcodes**. Seitens Xplain besteht ein Konzept, welches von Compass-Security bereits geprüft wurde. Das Konzept sieht vor, dass Xplain mit einem Development-Branch arbeitet. Auf diesen Development-Branch können alle Xplain-Entwickler schreiben. Die Freigabe in den Master-Quellcode erfolgt nach Prüfung durch einen Xplain-Lead-Developer im 4-Augen-Prinzip.
Der Rollout ist umfangreich und erfolgt bis Ende Oktober 2023 durch Xplain (keine Segmentierung nach Kunden). Als Sofortmassnahme werden alle Auslieferungen durch einen Lead-Entwickler vor der Freigabe geprüft.

Eine zentrale Anforderung des NCSC ist die strikte **Segmentierung des Netzwerks** und Isolation der unterschiedlichen Systeme. Das Netzwerk nach aktuellem Umsetzungsstand, ist segmentiert und einige wichtige Einschränkungen sind konfiguriert. Zum Beispiel ist sichergestellt, dass nur Administratoren über einen gesicherten Jump-Host Systeme administrieren können. Allerdings gibt es noch Verbesserungsmöglichkeiten, beispielsweise sind die Testsysteme nicht ausreichend von anderen Systemen abgeschottet. Diese Verbesserungen konnten zum Zeitpunkt der Erstellung dieses Dokuments aus zeitlichen Gründen noch nicht umgesetzt werden. Es ist geplant, dass diese raschmöglichst umgesetzt werden.

3 Einschätzung von Compass-Security

Im Rahmen der Beurteilung durch Compass-Security hat sich gezeigt, dass die gesamte IT-Infrastruktur von Xplain von Grund auf neu aufgebaut wurde. Die neue Infrastruktur basiert auf modernen Komponenten und Security Best Practices. Dies ermöglicht es Xplain, ihre Dienstleistung und Services auf einer möglichst sicheren Infrastruktur anzubieten.

Viele der vom NCSC vorgeschlagenen Massnahmen konnten in kurzer Zeit umgesetzt werden. Einige der wichtigsten Punkte sind im Folgenden aufgeführt.

Multifaktor-Authentifizierung:
Alle externen Zugänge (z.B. VPN, Office 365) für Mitarbeitende erfordern eine starke Multifaktor-Authentifizierung. Diese wird durch entsprechende Policies sichergestellt und kann durch die Mitarbeitenden nicht umgangen werden.

Quellcode-Sicherheit:
Im Rahmen einer internen Untersuchung hat Xplain geprüft, dass die Gruppe «PLAY» keine Backdoors in den Quellcode der Kundenapplikationen eingebaut hat. Aufgrund der bekannten Verhaltensmuster der Gruppe «PLAY» und der Erkenntnisse aus der durchgeführten Untersuchung bewertet Compass das Risiko von eingeschleustem Schadcode als gering.

Daten-Management:
Im überarbeiteten Datenmanagement-Konzept werden striktere Regeln für die Handhabung

von Daten definiert. Insbesondere wird festgelegt, dass Xplain ab sofort keine Produktionsdaten speichert und auch keinen Zugriff auf produktive Systeme hat. Dies wird durch entsprechende Prozesse sichergestellt.

Externe Angriffsoberfläche:
Der externe Penetrations-Test und das Konfigurations-Review der Infrastruktur haben gezeigt, dass nur die notwendigen Komponenten ins Internet exponiert werden. Dadurch wird die potenzielle Angriffsoberfläche für einen Angreifer aus dem Internet minimiert.

Netzwerkverkehr:
Die Mitarbeitenden dürfen keine direkten Verbindungen ins Internet aufbauen, sondern werden über ein Zwischensystem (Proxy) umgeleitet. Der Proxy blockiert bösartige Webseiten basierend auf einer anerkannten Blockliste. Die Verbindung über den Proxy wird durch entsprechende Firewall-Regeln auf dem Client forciert und kann somit nicht umgangen werden.

4 Einschätzung des NCSC

Xplain hat nach dem Ransomware-Vorfall die nötigen technischen Massnahmen ergriffen und ihre gesamte IT-Infrastruktur von Grund auf neu aufgebaut. Dies ist nach jedem Cyberangriff dieses Ausmasses eine grundlegende Voraussetzung für die Wiederaufnahme eines sicheren Betriebs.

Sowohl die vom NCSC und den betroffenen Organisationseinheiten wie auch die zusätzlichen von Compass-Security geforderten Massnahmen wurden, wo dies möglich war, alle umgesetzt und durch das externe Audit bestätigt.
Für die noch nicht vollständig umgesetzten Massnahmen (Aufbau SOC, Zugriffskontrolle Sourcecode und Segmentierung Netzwerk) wurden Umsetzungspläne vorgelegt.

Diese sehen wie folgt aus:

Segmentierung Netzwerk:	15. Oktober 2023
Zugriffskontrolle Sourcecode:	31. Oktober 2023
Aufbau SOC:	31. Dezember 2023

Das NCSC schätzt die geplante Umsetzung als plausibel und vertretbar ein. Xplain hat die Umsetzung der Massnahmen im Bereich der Netzwerk Segmentierung, sowie der Sourcecode Zugriffskontrolle unterdessen umgesetzt und dies dem NCSC schriftlich bestätigt. Compass-Security wird diese Umsetzung nachprüfen und Xplain, sowie dem NCSC schriftlich bestätigen.

Auf Basis der dem NCSC zur Verfügung gestellten Informationen und der Einschätzungen der mit dem Audit beauftragten Firma Compass-Security kommt das NCSC zum Schluss, dass die technischen und organisatorischen Anforderungen an die Cybersicherheit, welche als eine der Bedingungen für eine mögliche weitere Zusammenarbeit zwischen Bundesstellen und der Firma Xplain definiert wurden, erfüllt sind.

Eine mögliche weitere Zusammenarbeit der Bundesstellen mit Xplain hängt noch von weiteren Faktoren ab; die Einschätzung des NCSC beschränkt sich auf die technischen und organisatorischen Aspekte der Cybersicherheit.

5 Weitere Schritte

Der vorliegende Bericht ist die Einschätzung des NCSC. Daraus kann keine Verbindlichkeit für eine zwingende Weiterführung der Zusammenarbeit zwischen den Bundesämtern und Xplain abgeleitet werden.

Ob nach diesem Cybervorfall die Zusammenarbeit weitergeführt werden kann oder nicht, muss von jedem betroffenen Bundesamt individuell beurteilt werden.
Einige der betroffenen Anwendungen sind end of Life und die Bundesämter müssen eine Gesamtbeurteilung machen und schlussendlich entscheiden, wie die zukünftige Planung aussieht.

Die Resultate des Audits und die vorliegende Einschätzung basieren auf einer Momentaufnahme. Die Gewährleistung der Cybersicherheit ist jedoch ein kontinuierlicher Prozess. Dieser muss von der Geschäftsleitung von Xplain verantwortet und regelmässig überprüft werden. Falls nötig, müssen Massnahmen definiert und umgehend umgesetzt werden. Eine wichtige Voraussetzung dafür ist, dass die Geschäftsleitung von Xplain ein entsprechendes Risikobewusstsein für Cybersicherheit zeigt. Auftraggeber sollten von der Firma Xplain – wie auch von allen anderen sicherheitsrelevanten Dienstleistern und Lieferanten – regelmässige Nachweise für die Umsetzung zentraler Massnahmen der Cybersicherheit verlangen und sicherstellen, dass umfassende Notfallpläne vorliegen für den Fall, dass die Cybersicherheit wichtiger Dienstleister und Lieferanten kompromittiert wurde.

Cybervorfall Xplain - Massnahmen

Datum:	07. Juli 2023
Absender:	Nationales Zentrum für Cybersicherheit NCSC
Für:	Xplain
Kopien an:	Betroffene Verwaltungseinheiten und deren Informatiksicherheitsbeauftragte des Departements

6 Inhaltsverzeichnis

7 Einleitung

Die beschriebenen Massnahmen gelten im vorliegenden Fall ausschliesslich für die Firma Xplain, welche Opfer eines Ransomwarevorfalls der Gruppe PLAY wurde, wobei insbesondere auch Daten und Informationen der Bundesverwaltung und Strafverfolgungsbehörden abgeflossen und veröffentlicht wurden.
Wir befürchten, dass ein versierter Angreifer unentdeckt geblieben ist und Xplain als Ausgangspunkt für einen Angriff auf die Lieferkette der Bundesverwaltung oder andere kritische Infrastrukturen in der Schweiz nutzen könnte. Scheinbar gab es nur sehr wenige Sicherheitsvorkehrungen, die es erlauben würden, einen solchen Angriff zu entdecken, da der Angreifer Daten exfiltrieren konnte und die Entdeckung erst durch die Verschlüsselung erfolgt ist.

Das bedeutet, dass eigentlich vier Themengebiete erfüllt sein müssen:

- Sicherheit des Zugangs zu BV- Infrastrukturen / Daten
- Sicherheit der verteilten Software
- Sicherheit der Software Entwicklung
- Sicherheit der Testplattform (nach erfolgtem Testen sind die Daten zu löschen)

Die folgende Liste sind vorgeschlagene Massnahmen, welche Xplain umsetzen muss.
Sie hat nicht den Anspruch auf Vollständigkeit, soll aber als Ausgangspunkt für die Reduktion solcher Cyberrisiken dienen. Der letztliche Entscheid, ob die Restrisiken für den Bund tragbar sind, muss auf der Basis eines externen Auditberichts der neu aufzubauenden Systeme von Xplain und eigener Prüfungen und Abwägungen getroffen werden. Wir empfehlen Xplain ebenfalls ein ISMS einzuführen, in welchem klar definiert ist, wie mit Informationen und Daten ihrer Kunden umgegangen wird. Zudem müsste eine Zertifizierung nach ISO 27000 erfolgen.

8 Massnahmen

8.1 Authentisierung

Auf Seiten der Accounts von Xplain:

- Eine Multifaktor Authentisierung auf sämtlichen Systemen und Anwendungen ist unverzichtbar.
- Passwörter dürfen in keinem Fall unverschlüsselt aufbewahrt werden.
- Für lokale Admin Accounts muss ein System wie LAPS[1] eingesetzt werden. Diese sind jährlich auf dessen Gültigkeit und Verwendbarkeit sowohl von Xplain wie auch kundenseitig zu überprüfen, dies zu dokumentieren und gegebenfalls zu löschen.
- Für Service Accounts müssen gemanagte Service Accounts verwendet werden.

Auf Seiten der Accounts des Bundes:

- Sämtliche Credentials müssen revoziert worden sein.
- Zugriffe sind nur von Systemen in der komplett neu aufgebauten Infrastruktur erlaubt.
- Wird mit diesen Geräten Wartung gemacht oder Software verteilt, müssen diese besonders geschützt sein (z.B. kein Surfen, kein E-Mail über diese Geräte).

[1] Local Administrator Password Solution

- Die Mitarbeitenden, welche einen Zugang benötigen, müssen neu identifiziert werden. Die Identifikation muss von einem Mitarbeitenden des Bundes ausgelöst und auf einem vertrauenswürdigen und nachprüfbaren Kanal durchgeführt werden.

8.2 Datenmanagement

Es ist untersagt, dass Xplain produktive Daten von Verwaltungseinheiten des Bundes oder Kantone auf ihren Systemen hat.

Auf Seiten der Daten des Bundes ist sicherzustellen, dass:

- das Zugänglichmachen von Daten eines Bundesorgans an Xplain darf nur unter Einhaltung von Art. 11 VDTI[2] erfolgen.
- das verantwortliche Bundesorgan sicher stellt, dass seine Daten Xplain nur in anonymisierter Form zur Verfügung gestellt werden.
- die Firma xPlain nicht mehr verwendete Daten (insbesondere Log- und Debug Daten) sofort löscht, wenn diese nicht mehr für die Bearbeitung von Supportfällen verwendet werden.

8.3 Netzwerksicherheit

- Das Netzwerk von Xplain muss segmentiert sein – es darf einem Angreifer nicht möglich sein, so rasch zu einem so zentralen Element wie dem Build Server vordringen zu können.
- Ein- und ausgehender Netzwerkverkehr muss überwacht, die Logs zentral gespeichert und permanent ausgewertet werden, dies sowohl auf bekannte IOCs wie auch auf Anomalien hin (z.B. von einem bestimmten Gerät aus oder in Richtung einer bisher unbekannten IP zusammen mit dem Überschreiten eines bestimmten Schwellwertes.
- Server und Clients dürfen nicht direkt mit dem Internet kommunizieren, es braucht einen Web-Proxy dazwischen, welcher für Server und für heikle Entwickler-Administratorgeräte mit hohen Rechten einen Whitelisting-Approach verfolgt.
- Netzwerkverkehr von Benutzern muss überwacht und gefiltert werden. Wir empfehlen auch den Einsatz von frei verfügbaren Daten (OSINT) wie z.B. von abuse.ch.
- Zwangstunneling für Remote Worker, so dass die Netzwerksicherheit auch hier greift.
- VPN-Zugänge müssen eingeschränkt und überwacht sein.

8.4 Active Directory

- Wenn es ein Active Directory (AD) gibt, würden wir von einer Kompromittierung ausgehen und einen kompletten Neuaufbau machen, inklusive doppeltem TGT[3] Wechsel, Passwort
  Reset (auch von den Service Accounts!)
- Das AD muss mit dem zentralen Logging überwacht werden.

[2] https://www.fedlex.admin.ch/eli/cc/2020/988/de#art_11

[3] Ticket Granting Ticket

- Eine Sicherheitsprüfung mit der AD Audit Software «PingCastle» muss einen tiefen «Domain Risk Score» ausweisen (Status: grün).
- Wir empfehlen die Durchführung eines AD RAP[4].

8.5 Antivirenschutz / EDR

- Der Einsatz eines EDR[5] ist sehr zu empfehlen, um die Sichtbarkeit auf den Endgeräten zu erhöhen.
- AV Logs müssen überwacht und bei einer Infektion auf internen Systemen ein Alert ausgelöst werden.
- Zusätzlich macht der Einsatz von Sysmon mit einer branchenüblichen Konfiguration Sinn.

8.6 Zentrales Logging

- Logs müssen zentral gesammelt und permanent ausgewertet werden
- Diese müssen hinreichend lange (>6 Monate) aufbewahrt und regelmässig ausgewertet werden (täglich).

8.7 Build Umgebung / Source Code Security

- Die Buildumgebung muss gehärtet werden
- Zwingend 2FA für alle Zugriffe
- Veränderungen an der Konfiguration dürfen nur von einem kleinen Kreis gemacht werden. Es muss dokumentiert sein, wer welche Berechtigung besitzt und was machen darf
- Code Signing Keys müssen auf einer Smartcard oder einem HSM[6] gespeichert sein.
- Es sollte regelmässige Snapshots vom Source Code Repository auf einem WORM geben.
- Das Dazufügen von neuen Libraries benötigt einen Freigabeprozess mit klaren Verantwortlichkeiten.
- Kunden sollten soweit als möglich voneinander, in einer separaten Kundenumgebung, getrennt werden.
- Testdaten müssen regelmässig daraufhin geprüft werden, dass sie nicht versehentlich produktive oder vertrauliche/geheime Elemente enthalten.
- Wir schlagen vor, den Source Code soweit als möglich auf Manipulationen hin zu überprüfen. Wenn die Menge an Code überschaubar ist, kann dies vermutlich manuell gemacht werden, ansonsten kann evtl. mit statischen Code Analysatoren etwas erreicht werden. Dazu ist auch eine Sicherheitsmarge zu verwenden, die über den vermuteten Zeitpunkt des initialen Access hinausgeht.

[4] Risk Assessment Program

[5] Extended Detection and Response

[6] Hardeware Security Module

- Ein Angreifer muss nicht zwingend ein Backdoor hinterlassen, er kann auch eine Verwundbarkeit einbauen oder einen Check ausschalten, dessen Kenntnis es ihm später erlaubt, Zugang zu erlangen.
- Wir empfehlen ebenfalls alle Softwarepakete, die seit dem Incident entstanden sind, neu zu kompilieren und mit dem neuen Zertifikat zu signieren. Wenn das Zertifikat nicht auf einem HSM gespeichert war, muss dieses revoziert werden und es müssen alle Software Pakete neu erstellt und signiert werden.
- Geprüfter Source Code muss komplett neu kompiliert werden. Dazu ist eine neu aufgebaute und geprüfte Buildumgebung mit neuen und geprüften Bibliotheken, neu ausgestellten Zertifikaten zu verwenden.
- Die Auslieferung erfolgt auf einem sicheren Kanal, der Bund prüft danach die Echtheit und Integrität der Pakete.

8.8 Patch / Vulnerability Management

- Systeme müssen sehr zeitnah gepatched werden, kritische Lücken innerhalb weniger Stunden, falls das System gegen das Internet hin exponiert ist. Auch interne Systeme müssen bei kritischen Lücken innerhalb ein bis zwei Tagen patchbar sein.
- Der Patchlevel sollte überwacht werden und es braucht klare Verantwortlichkeiten wer für das Einspielen eines Securitypatches zuständig ist.
- Vulnerability Scans müssen regelmässig durchgeführt werden.

8.9 Organisation

- Es braucht einen klaren Incident Response Plan mit zugewiesenen Verantwortlichkeiten.
- Ebenso sollte sichergestellt sein, dass das nötige Wissen für Detektion und Reaktion entweder innerhalb der Firma vorhanden ist oder bei einem externen Dienstleister eingekauft werden kann.
- Es braucht ein Inventar und ein Life Cycle Management der Daten, die der Kunde der Firma anvertraut.
- Es ist ein Löschverfahren für Testdaten nach dessen Gebrauch zu implementieren.
- Wir empfehlen Xplain die Verwendung eines Frameworks zur kontinuierlichen Verbesserung der IT-Sicherheit, wie z.B. OpenSAMM[7] und die Einhaltung von entsprechenden Security Guidelines wie sie. z.B von OWASP[8] herausgegeben werden.

9 Audit

- Die Firma Xplain muss nach Umsetzung der obigen Empfehlungen ein komplettes Audit durchführen lassen und darauf basierend gefundene Mängel beheben.
- Die für das Audit gewählte Firma soll möglichst neutral und unabhängig sein. Sie darf keine bisherigen Geschäftsbeziehungen zu Xplain gehabt haben.

[7] https://www.opensamm.org/

[8] https://owasp.org/

- Der Auditscope muss zusammen mit dem Bund definiert werden, sollte aber mind. folgende Punkte umfassen:
- Das Audit muss sowohl technische, physische wie auch organisatorische Massnahmen umfassen (kein reines Konzept Review).
    - Wurden die in diesem Dokument gelisteten Massnahmen vollständig umgesetzt?
    - Existieren technische und organisatorische Massnahmen, um einen Angriff zu detektieren?
    - Entspricht der Aufbau der Systeme und Anwendungen einem Vorgehen nach Best Practice für eine Firma, die sicherheitssensitive Anwendungen entwickelt?
    - Idealerweise wird dies zusätzlich mit einem Red Teaming kombiniert, bei dem eine Verbindung nach aussen aufgebaut wird und geprüft wird, ob diese detektiert wurde.
    - Die Auditfirma sollte zusätzlich den gesamten Buildprozess, sowie die Auslieferung und Installation der Software Pakete prüfen und auch prüfen, ob allfällige Supportzugänge sicher und nachvollziehbar genutzt werden.
    - Der Scope des Audits darf keine Ausschlüsse beinhalten.
    - Diese Resultate müssen den Kunden transparent und vollständig offengelegt werden. Die Bundesverwaltung entscheidet basierend auf dem Auditbericht über die weiteren Schritte. Wir empfehlen, das Audit in regelmässigen Abständen zu wiederholen.
- Der Bund definiert ein Control Set wie zukünftige und regelmässig Prüfungen gemacht werden. Das Control Set orientiert sich am IKT Minimalstandard und ergänzt diesen wo nötig mit zusätzlichen Massnahmen, um den erhöhten Schutzbedarf zu abzudecken.