Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat
Le Conseil fédéral
Il Consiglio federale
Il Cussegl federal

Medienmitteilung

Datum: 28.06.2023

Hackerangriff auf Firma Xplain: Bundesrat mandatiert politisch-strategischen Krisenstab «Datenabfluss»

Der Bundesrat hat an seiner Sitzung vom 28. Juni 2023 einen politisch-strategischen Krisenstab «Datenabfluss» mandatiert. Der departementsübergreifende Krisenstab soll die laufenden Arbeiten zur Bewältigung des Ransomware-Angriffes auf die Firma Xplain, von dem auch Daten aus der Bundesverwaltung betroffen sind, koordinieren und Massnahmen vorschlagen. Zudem lässt der Bundesrat ein Mandat für eine Administrativuntersuchung erarbeiten. Auch hat er entschieden, bestehende Verträge mit Informatikdienstleistern des Bundes überprüfen und nötigenfalls so anpassen zu lassen, dass die Cybersicherheit der Dienstleister verbessert wird und der Bund im Fall eines erfolgreichen Angriffs rasch reagieren kann. Schliesslich lässt er Massnahmen prüfen, mit denen sichergestellt werden kann, dass die heute von Xplain für die Polizei sowie für Sicherheits- und Migrationsbehörden erbrachten essenziellen Leistungen in jedem Fall gewährleistet werden können.

Die unter dem Namen «Play» auftretende Hackergruppierung hatte bei einem Ransomware-Angriff auf die Firma Xplain grosse Datenmengen gestohlen. Darunter befinden sich auch operative Daten aus der Bundesverwaltung. Da Xplain sich in Absprache mit den Strafverfolgungsbehörden und dem Bund nicht erpressen liess und keine Lösegeldzahlung an die Hacker leistete, veröffentlichten diese am 14. Juni 2023 mutmasslich das gesamte entwendete Datenpaket im Darknet. Seit Bekanntwerden dieses Datenabflusses hat das Nationale Zentrum für Cybersicherheit (NCSC) in enger Zusammenarbeit mit den betroffenen Behörden eine Organisation zur Bewältigung des Vorfalls etabliert. Es laufen weiterhin intensive Arbeiten zur Auswertung und Analyse der Daten. Der Bund hat zudem Massnahmen eingeleitet, um ein Sicherheitsrisiko für die Bundesverwaltung zu minimieren.

Bundesinterne Arbeiten koordinieren, Kantone einbeziehen

Seit dem 9. Juni 2023 hat sich der Bundesrat mehrmals über diesen Vorfall informieren lassen. Am 16. Juni 2023 hat er entschieden, einen politisch-strategischen Krisenstab «Datenabfluss» (PSK-D) einzusetzen, der die umfangreichen Arbeiten auf operativer Stufe ergänzen soll. Der PSK-D hat seither bereits zwei Mal – am 21. Juni und am 26. Juni 2023 – getagt. Dabei verschaffte er sich einen Überblick über die zu bewältigenden Aufgaben und erarbeitete zuhanden des Bundesrats Vorschläge zum weiteren Vorgehen. An seiner Sitzung vom 28. Juni 2023 hat der Bundesrat nun das Mandat des PSK-D verabschiedet. Unter der Leitung der Generalsekretärin des Eidgenössischen Finanzdepartements (EFD) arbeiten in diesem

Krisenstab alle Departemente, die Bundeskanzlei sowie eine Vertretung der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) zusammen. Der Krisenstab soll die strategische Lage fortlaufend analysieren und beurteilen, die bundesinternen Arbeiten koordinieren, die Information nach innen und aussen sicherstellen und Grundlagen für weitere Entscheide des Bundesrats erarbeiten.

Verträge mit Informatik-Dienstleistern werden überprüft

Weiter hat der Bundesrat das EFD beauftragt, in Zusammenarbeit mit dem PSK-D ein Mandat für eine Administrativuntersuchung zu erarbeiten. Mit einer Administrativuntersuchung soll von unabhängiger Seite untersucht werden, ob, wo und weshalb die Sicherheitsvorgaben des Bundes allenfalls mangelhaft umgesetzt worden sind. Damit sollen Massnahmen identifiziert werden, um einen ähnlichen Vorfall künftig zu verhindern.

Der Bundesrat hat an seiner Sitzung zudem angeordnet, bestehende Verträge des Bundes mit Informatikdienstleistern zu überprüfen und nötigenfalls so anpassen zu lassen, dass die Cybersicherheit der Dienstleister verbessert wird und der Bund im Fall eines erfolgreichen Angriffs rascher reagieren kann. Damit und mit der Definition von Anforderungen im Beschaffungsprozess soll sichergestellt werden, dass Lieferanten des Bundes definierte Schutzstandards in Bezug auf Cyberangriffe einhalten müssen.

Die vom Hackerangriff betroffene Firma Xplain ist für nationale und kantonale Behörden ein zentraler IT-Dienstleister. Der Bundesrat hat deshalb das Eidgenössische Justiz- und Polizeidepartement beauftragt, unter Beizug der KKJPD und des EFD Massnahmen zu prüfen, um die Wartung und Weiterentwicklung dieser essentiellen Softwarekomponenten sicherzustellen.

Der Bund wird über die weiteren Schritte bei der Bewältigung dieses Vorfalls weiterhin transparent informieren.

Bisher getroffene Massnahmen

Nachdem die Bundesverwaltung Anfang Juni von Xplain über den Ransomware-Angriff informiert worden war, wurden umgehend Massnahmen getroffen, um das Sicherheitsrisiko für die Bundesverwaltung zu minimieren. Die Auswertung und vertieften Analysen des Datenpakets laufen weiter. Aufgrund der Grösse des Datenpaketes (mehrere Millionen Dateien) werden diese Arbeiten einige Wochen oder gar Monate in Anspruch nehmen.

Chronologie der wichtigsten Ereignisse

Ende Mai / Anfang Juni	Nach einem Ransomware-Angriff auf die Firma Xplain wird diese erpresst. In Absprache mit den Strafverfolgungsbehörden und dem Bund verweigert Xplain die Zahlung des geforderten Lösegeldes. Xplain reicht Strafanzeige gegen Unbekannt ein. Der Bund setzt Sofortmassnahmen um, um das Risiko für die Bundesverwaltung und betroffene Dritte zu minimieren. Unmittelbar nach der Veröffentlichung der ersten Daten im Darknet startet die Analyse des ersten Datenpaketes. Die betroffenen Stellen werden informiert. Das NCSC koordiniert die verschiedenen operativen Arbeiten.
8. Juni 2023	Eine erste Information der Öffentlichkeit über den Ransomware-Angriff auf Xplain und den Umstand, dass operative Daten betroffen sein könnten, erfolgt. (vgl. Medienmitteilung vom 8. Juni 2023)
9. Juni 2023	Das EFD informiert den Bundesrat an seiner Sitzung zum aktuellen Stand

	und zu den getroffenen Massnahmen.
14. Juni 2023	«Play» veröffentlicht das mutmasslich gesamte Datenpaket im Darknet. Der Bund beginnt mit der Sicherung der veröffentlichten Daten aus dem Darknet, führt vertiefte Analysen durch und informiert die betroffenen Stellen fortlaufend. Nach weiteren Hinweisen, dass operative Daten vom Angriff betroffen sein könnten, haben von den betroffenen Behörden das Bundesamt für Polizei (fedpol) und das Bundesamt für Zoll und Grenzsicherheit (BAZG) Strafanzeige erstattet. Mit diesem Vorgehen soll geklärt werden, unter welchen Umständen die Daten aus der Bundesverwaltung auf das System der Firma Xplain gelangt sind. (vgl. Medienmitteilung vom 14. Juni 2023)
16. Juni 2023	Das EFD informiert den Bundesrat erneut über die im Darknet veröffentlichten Daten und die laufenden Arbeiten. Der Bundesrat entscheidet, einen politisch-strategischen Krisenstab «Datenabfluss» (PSK-D) einzusetzen und beauftragt das EFD mit den entsprechenden Arbeiten.
21. Juni 2023	Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) eröffnet eine Untersuchung gegen das fedpol und das BAZG wegen Anzeichen auf potenziell schwerwiegende Verstösse gegen die Datenschutzvorschriften. Dies, nachdem die beiden Ämter den Datenabfluss proaktiv gemeldet hatten. Seither haben weitere betroffene Ämter ähnliche Meldungen erstattet. (vgl. Medienmitteilung vom 21. Juni 2023)
28. Juni 2023	Der Bundesrat verabschiedet das Mandat für den politisch-strategischen Krisenstab «Datenabfluss» (PSK-D) und beschliesst weitere Massnahmen.

Für Rückfragen: Kommunikation EFD
Tel.-Nr. +41 58 462 60 33,
kommunikation@gs-efd.admin.ch

Verantwortliches Departement: Eidgenössisches Finanzdepartement EFD

Folgende Beilagen finden Sie als Dateianhang dieser Mitteilung auf www.efd.admin.ch:

- Medienmitteilung vom 8. Juni 2023: Hackerangriff auf die Firma Xplain: Auch die Bundesverwaltung ist betroffen (admin.ch)
- Medienmitteilung vom 14. Juni 2023: Hackerangriff auf die Firma Xplain: Erste Erkenntnisse aus Datenanalysen zeigen Handlungsbedarf (admin.ch)
- Medienmitteilung vom 21. Juni 2023: Untersuchung gegen fedpol und BAZG (admin.ch)