Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Der Bundesrat
Le Conseil fédéral
Il Consiglio federale
The Federal Council

Press release

Date: 28.06.2023

Xplain hack: Federal Council commissions a policy strategy crisis team on data leaks

During its meeting on 28 June 2023, the Federal Council commissioned a policy strategy crisis team on data leaks. The aim of the cross-departmental crisis team is to coordinate the ongoing efforts to deal with the ransomware attack on Xplain, which has also affected Federal Administration data, and to propose related measures. In addition, the Federal Council ordered that a mandate be drawn up for an administrative investigation. Moreover, it decided to review existing contracts with federal IT service providers and to amend them where necessary in order to improve service providers' cybersecurity and allow the federal government to react swiftly in the event of a successful attack. Finally, it ordered an examination of measures to ensure that the essential services currently provided by Xplain for the police and the security and migration authorities can be guaranteed in any case.

During a ransomware attack on Xplain, the hacker group known as "Play" stole large amounts of data, including operational data, from the Federal Administration. On 14 June 2023, after Xplain, in consultation with the prosecution authorities and the federal government, did not give in to the blackmail attempt or pay any ransom to the hackers, they published what is presumed to be the entire stolen data package on the darknet. Since this data leak became public, the National Cybersecurity Centre (NCSC) has been working closely with the affected authorities to set up an organisation to deal with the incident. Intensive efforts to evaluate and analyse the data are ongoing. Moreover, the federal government has taken measures to minimise the security risk to the Federal Administration.

Coordinating internal federal activities, involving the cantons

Since 9 June 2023, the Federal Council has received regular information updates on this incident. On 16 June 2023, it decided to set up a policy strategy crisis team on data leaks (PSC-D) to supplement the wide-ranging activities at operational level. Since then, the PSC-D has met twice – on 21 and 26 June 2023. It used these meetings to obtain an overview of the tasks at hand and set out proposals on how to proceed, which were submitted to the Federal Council. At its meeting on 28 June 2023, the Federal Council approved the PSC-D's mandate. The crisis team is headed by the General Secretary of the Federal Department of Finance (FDF), and brings together all departments, the Federal Chancellery and a representative of the Conference of Cantonal Justice and Police Directors (CCJPD). The crisis team should continuously analyse and evaluate the strategic situation, coordinate internal federal activities, ensure the flow of information both internally and externally, and lay the groundwork for further Federal Council decisions.

Contracts with IT service providers will be reviewed

Furthermore, the Federal Council has instructed the FDF, together with the PSC-D, to draw up a mandate for an administrative investigation. The aim of the administrative investigation is to provide an independent assessment of whether, where and why the implementation of federal security requirements might have been lacking. This should allow measures to be identified to prevent similar incidents in the future.

Moreover, at its meeting the Federal Council ordered that existing contracts with federal IT service providers be reviewed and amended where necessary in order to improve service providers' cybersecurity and allow the federal government to react swiftly in the event of a successful attack. This, together with the definition of requirements in the procurement process, should ensure that federal suppliers must comply with specific security standards with regard to cyberattacks.

The company affected by the hack, Xplain, is a major provider of IT services to national and cantonal authorities. The Federal Council has therefore instructed the Federal Department of Justice and Police, together with the CCJPD and the FDF, to examine measures to ensure the maintenance and further development of these essential software components.

The federal government will continue to be fully informed about the next steps in dealing with the incident.

Measures taken to date

After the Federal Administration was notified of the ransomware attack on Xplain at the beginning of June, measures were immediately taken to minimise the security risk for the Federal Administration. The evaluation and in-depth analyses of the data package are still ongoing. This work will take several weeks or even months because of the size of the data package (several million files).

Key events timeline

Late May/ early June	The IT company Xplain is blackmailed following a ransomware attack. After consulting the prosecution authorities and the federal government, Xplain refuses to pay the ransom demand. Xplain files criminal charges against persons unknown. The federal government immediately takes measures to minimise the risk for the Federal Administration and affected third parties. As soon as the first set of data is published on the darknet, analysis of the first data package commences. The units concerned are informed. The NCSC coordinates the various operational activities.
8 June 2023	The public is informed for the first time about the ransomware attack on Xplain and the fact that operational data could be affected. (See press release of 8 June 2023)
9 June 2023	During the Federal Council's meeting, the FDF briefs it on the current state of affairs and the measures taken.
14 June 2023	"Play" publishes what is presumed to be the entire data package on the darknet. The federal government starts to secure the data published on the darknet, conducts thorough analyses and updates the units concerned on an

	ongoing basis. Following further indications that operational data could be affected by the attack, the Federal Office of Police (fedpol) and the Federal Office for Customs and Border Security (FOCBS) file criminal charges. The aim of this is to clarify the circumstances that led to Federal Administration data ending up on the Xplain system. (See press release of 14 June 2023)
16 June 2023	The FDF again informs the Federal Council about the data published on the darknet and the work being carried out. The Federal Council decides to commission a policy strategy crisis team on data leaks (PSC-D) and instructs the FDF to perform the corresponding work.
21 June 2023	The Federal Data Protection and Information Commissioner (FDPIC) launches an investigation into fedpol and the FOCBS due to indications of potentially serious breaches of data protection provisions. This was after the two offices had proactively reported the data leak. Other affected offices have since submitted similar reports. (See press release of 21 June 2023)
28 June 2023	The Federal Council adopts the mandate for the policy strategy crisis team on data leaks (PSC-D) and decides on further measures.

Further details: FDF Communications
Tel. +41 58 462 60 33,
kommunikation@gs-efd.admin.ch

Relevant department: Federal Department of Finance FDF

The following can be found as an enclosure to this press release at www.finance.admin.ch:

- Press release of 8 June 2023: Federal Administration also impacted by Xplain hack (admin.ch)
- Press release of 14 June 2023: Xplain hack: initial findings from data analyses indicate need for action (admin.ch)
- Press release of 21 June 2023: Fedpol and the FOCBS under investigation (admin.ch)