Q&A: Xplain ransomware incident

Based on the information currently available, it appears that operational data of the Federal Administration could also be affected by the ransomware attack on the IT company Xplain, which resulted in some of the stolen data being published on the darknet. In-depth analyses are still ongoing.

Date: 09.06.2023

Contents

1. Which administrative units of the Federal Administration are affected?

Determining which federal offices are affected is part of the ongoing analyses.

2. Is the attack on Xplain connected to the Parliamentary Services attack?

No, they are two separate incidents that are unrelated. Moreover, different groups are behind the attacks. For example, the group Play is behind the attack on Xplain, and the group NoName claimed responsibility for the DDoS attack on the Parliamentary Services website on Telegram.

3. Was a ransom paid?

The NCSC was told that no ransom was paid.

4. What data is affected?

Contrary to the initial findings and following recent in-depth clarifications, it has to be assumed that operational data could also be affected.
Operational data is data that is used for work purposes. The analysis of the data is ongoing, so we cannot provide more specific information.

5. Did the attackers manage to access the federal systems?

No attempt to access federal systems has been observed so far.

6. Why did the NCSC wait until now to take on the role of coordinator?

The NCSC offered its support to Xplain immediately after the incident was reported. Once the extent of the incident became clear, the NCSC took over the lead and the role of coordinator in accordance with its mandate.
The responsibilities are governed by Article 12 paragraphs 5 and 6 of the Cyber-Risks Ordinance (CyRO).

7. What do you know about the Play hacker group?

The NCSC cannot add anything to the information that is publicly available.

8. What are the next steps?

The published data is currently being analysed. The findings will be discussed with the administrative units concerned and further measures will be defined.

9. Who is involved in the analyses?

Various Federal Administration units and the prosecution authorities are involved in analysing the incident. We cannot provide more specific information in this regard due to the ongoing criminal proceedings.

10. To what extent is it problematic that various federal offices use the same IT service provider?

It is not problematic as such that various federal offices use the same IT service provider. A certain risk concentration is offset by improved cost-effectiveness.

Furthermore, it is important to bear in mind that we do not have countless companies that can provide the required goods/services.
Finally, it should be noted that the use of several suppliers also leads to additional interfaces and exchanges of data, which in turn can increase the risk of a security incident.

11. What course does a ransomware attack follow?

After the attackers gain unauthorised access to a company's systems, the data is first stolen, then encrypted and the company is blackmailed. If the company in question does not pay, they threaten to publish the stolen data. If the company still does not respond to the blackmail, the data is usually published gradually in order to put it under additional pressure.

12. Have you noticed a rise in cybercrime?

In recent years, the topic of cybersecurity has increasingly come under the spotlight in all sectors. Because of this, as well as greater media coverage, many companies that are now victims of a cyberattack are more likely to go public. However, the NCSC is also noticing a slight rise in cyberincidents.

13. Are there more ransomware attacks?

Reports regarding ransomware attacks surged in the period from 2020 to 2021, and have now stabilised at that level. Nevertheless, in percentage terms, more companies and fewer private individuals have been affected this year than in the previous two years. While ransomware attacks reported to the NCSC by individuals accounted for about 35% of the total in 2021 and 2022, the figure is only around 10% in 2023. The attackers seem to be focusing more on companies. Unpatched systems and credential misuse are the most common gateways for ransomware attacks.

Number of reports concerning ransomware attacks:

2020: 66 reports
2021: 161 reports
2022: 159 reports
2023: 56 reports (as at 05.06.2023)

Total number of cyberincident reports:

2020: 10,833 reports
2021: 21,714 reports
2022: 34,527 reports
2023: 15,977 reports (as at 05.06.2023)

It is important to note that there is no cyberincident reporting duty in Switzerland. Consequently, it can be assumed that the number of unreported cases is much higher.

14. How can a company protect itself against ransomware?

With the right protective measures, the risk of a successful cyberattack can be greatly minimised. For this reason, the NCSC regularly warns of the increased security risks posed by ransomware. Nevertheless, many Swiss companies do not implement them or only partially implement them. This leads not only to a very high level of risk exposure for companies, but also to the fact that Swiss companies repeatedly fall victim to ransomware and that their data, as well as that of employees and customers, is published on the internet.

Remote access protection:
All remote access connections such as VPN, RDP, Citrix, etc., as well as all other ways of accessing internal resources (e.g. webmail, SharePoint), must be consistently secured with two-factor

authentication (2FA). This also applies to access connections for suppliers, contracting parties and students, for example.

Patch and lifecycle management:
All systems must promptly and consistently receive security updates. Updates that fix critical security vulnerabilities in systems accessible via the internet must be applied within 24 hours. Software or systems that are no longer supported by the manufacturer (end of life, EOL) must be switched off or moved to a separate, isolated network zone.

Offline backups:
Make regular backups of your data. Use the generation principle (daily, weekly, monthly – at least 2 generations). Ensure that the medium on which you create the backup copy is physically separated from the computer or network after the backup process and stored securely. Alternatively, use WORM storage media.

Further information:

Ransomware gangs are still very active in Switzerland (admin.ch)