Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat
Le Conseil fédéral
Il Consiglio federale
Il Cussegl federal

Communiqué

Date: 28.06.2023

Cyberattaque contre l'entreprise Xplain: le Conseil fédéral mandate un état-major de crise politico-stratégique «Fuite de données»

Lors de sa séance du 28 juin 2023, le Conseil fédéral a mandaté un état-major de crise politico-stratégique «Fuite de données». Cette entité interdépartementale est chargée, d'une part, de coordonner les travaux en cours visant à gérer l'attaque par rançongiciel menée contre l'entreprise Xplain, qui a aussi touché des données de l'administration fédérale, et, d'autre part, de formuler des propositions quant aux mesures à prendre. Par ailleurs, le Conseil fédéral fait actuellement élaborer un mandat d'enquête administrative. Il a également décidé de faire vérifier et, le cas échéant, modifier les contrats en cours avec les fournisseurs de prestations informatiques de l'administration fédérale, afin que ces derniers offrent une cybersécurité accrue et que la Confédération puisse réagir rapidement en cas d'attaque fructueuse. Pour terminer, le Conseil fédéral fait examiner les mesures qui permettraient de garantir que les prestations essentielles fournies actuellement par l'entreprise Xplain à la police ainsi qu'aux autorités de sécurité et de migration puissent être assurées dans tous les cas.

Dans le cadre d'une attaque par rançongiciel lancée contre l'entreprise Xplain, le groupe de pirates informatiques connu sous le nom de «Play» a dérobé de grandes quantités de données, parmi lesquelles des données opérationnelles de l'administration fédérale. En accord avec les autorités de poursuite pénale et la Confédération, l'entreprise Xplain n'a pas cédé au chantage et n'a pas versé de rançon aux pirates, si bien que le 14 juin 2023 ceux-ci ont vraisemblablement publié sur le darknet l'ensemble du lot de données dérobées. Depuis que cette fuite de données a été révélée, le Centre national pour la cybersécurité a mis en place, en collaboration étroite avec les autorités concernées, une organisation pour gérer l'incident. Le travail intensif d'évaluation et d'analyse des données se poursuit. La Confédération a également pris des mesures pour réduire au minimum les risques encourus par l'administration fédérale sur le plan de la sécurité.

Coordonner les travaux entrepris au sein de l'administration fédérale, collaborer avec les cantons

Depuis le 9 juin 2023, le Conseil fédéral a été informé à plusieurs reprises au sujet de l'incident survenu. Le 16 juin 2023, il a décidé de mettre sur pied un état-major de crise politico-stratégique «Fuite de données» (EMPS-F), destiné à compléter les vastes démarches engagées sur le plan opérationnel. L'EMPS-F a déjà tenu deux réunions (les 21 et 26 juin 2023), à l'occasion desquelles il a établi une synthèse des tâches à accomplir et a

élaboré des propositions à l'intention du Conseil fédéral quant à la suite à donner. Lors de sa séance du 28 juin 2023, le Conseil fédéral a adopté le mandat de l'EMPS-F. Collaborent au sein de ce dernier des représentants de l'ensemble des départements, de la Chancellerie fédérale et de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), sous la direction de la secrétaire générale du Département fédéral des finances (DFF). L'EMPS-F est chargé d'analyser et d'évaluer la situation stratégique en continu, de coordonner les travaux entrepris au sein de l'administration fédérale, d'assurer la diffusion de l'information à l'intérieur et à l'extérieur de l'administration fédérale et d'élaborer les bases sur lesquelles se fonderont les décisions ultérieures du Conseil fédéral.

Vérification des contrats portant sur des prestations informatiques

Par ailleurs, le Conseil fédéral a chargé le DFF d'élaborer un mandat d'enquête administrative en collaboration avec l'EMPS-F. Cette enquête vise à examiner de manière indépendante si, où et pourquoi les directives de sécurité de la Confédération ont éventuellement été mal appliquées. Elle devra permettre d'identifier les mesures à prendre pour éviter tout nouvel incident similaire.

Lors de sa séance, le Conseil fédéral a en outre ordonné que les contrats qui lient actuellement la Confédération à des fournisseurs de prestations informatiques soient vérifiés et, le cas échéant, modifiés, afin que ces derniers offrent une cybersécurité accrue et que la Confédération puisse réagir plus rapidement en cas d'attaque fructueuse. Cette mesure ainsi que la définition d'exigences applicables dans le cadre du processus d'acquisition visent à garantir le respect par les prestataires de la Confédération des normes de protection concernant les cyberattaques.

L'entreprise visée par la cyberattaque est l'un des principaux fournisseurs de prestations informatiques des autorités fédérales et cantonales. C'est pourquoi le Conseil fédéral a chargé le Département fédéral de justice et police d'examiner, avec l'aide de la CCDJP et du DFF, quelles mesures permettraient d'assurer la maintenance et le développement des composants logiciels essentiels qui sont concernés.

La Confédération entend continuer de fournir une information transparente sur le processus de gestion de l'incident survenu.

Mesures déjà prises

Après avoir pris connaissance de l'attaque lancée par rançongiciel contre Xplain, l'administration fédérale a immédiatement mis en place des mesures afin de réduire le risque qu'elle encourait sur le plan de la sécurité. L'évaluation et l'analyse approfondie du lot de données volées se poursuivent. Étant donné qu'il comprend plusieurs millions de données, les travaux pourraient durer des semaines, voire des mois.

Chronologie des événements principaux

Fin mai / début juin	À la suite d'une attaque par rançongiciel, l'entreprise Xplain fait l'objet d'une tentative de chantage. En accord avec les autorités de poursuite pénale et la Confédération, elle refuse de payer la rançon qu'exigent les cybercriminels. Xplain porte plainte contre inconnu. La Confédération met immédiatement des mesures en place afin de réduire les risques encourus par l'administration fédérale et d'autres entités. Dès que les premières données sont publiées sur le darknet, elle lance l'analyse du lot de données et en informe les services concernés. Le NCSC coordonne les divers travaux opérationnels.

8 juin 2023	Le public est informé de l'attaque par rançongiciel contre Xplain et du fait que des données opérationnelles pourraient être touchées (cf. le communiqué de presse du 8 juin 2023).
9 juin 2023	Lors de la séance du Conseil fédéral, le DFF informe celui-ci de l'état de la situation et des mesures qui ont été prises.
14 juin 2023	«Play» publie vraisemblablement l'ensemble des données sur le darknet. La Confédération commence à sécuriser les données publiées sur le darknet, procède à des analyses approfondies et informe les services concernés en continu. De nouvelles preuves semblant indiquer que des données opérationnelles auraient été dérobées, l'Office fédéral de la police (fedpol) et l'Office fédéral de la douane et de la sécurité des frontières (OFDF) ont déposé une plainte pénale. Ils entendent ainsi déterminer les circonstances dans lesquelles les données de l'administration fédérale se sont retrouvées sur l'infrastructure de l'entreprise Xplain (cf. le communiqué de presse du 14 juin 2023).
16 juin 2023	Le DFF informe à nouveau le Conseil fédéral des données publiées sur le darknet et des travaux en cours. Le Conseil fédéral décide de mettre sur pied un état-major politico-stratégique «Fuite des données» (EMPS-F) et charge le DFF des travaux en la matière.
21 juin 2023	Le Préposé fédéral à la protection des données et à la transparence ouvre une enquête contre fedpol et l'OFDF sur la base d'indices de violations potentiellement graves des dispositions sur la protection des données. Il l'a lancée après que les deux offices ont signalé la fuite de données de leur propre initiative. Depuis, d'autres offices concernés ont effectué des signalements similaires (cf. le communiqué de presse du 21 juin 2023).
28 juin 2023	Le Conseil fédéral adopte le mandat confié à l'EMPS-F et définit de nouvelles mesures.

Renseignements: Communication DFF
n° tél. +41 58 462 60 33, kommunikation@gs-efd.admin.ch

Département responsable: Département fédéral des finances DFF

Sous www.dff.admin.ch, le présent communiqué est complété par les documents suivants:

- Communiqué du 8 juin 2023: Cyberattaque contre l'entreprise Xplain: l'administration fédérale est également touchée (admin.ch)
- Communiqué du 14 juin 2023: Cyberattaque contre l'entreprise Xplain: les premiers résultats des analyses indiquent que des mesures sont nécessaires (admin.ch)
- Communiqué du 21 juin 2023: Enquête contre fedpol et l'OFDF (admin.ch)