Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat
Le Conseil fédéral
Il Consiglio federale
Il Cussegl federal

Comunicato stampa

Data: 28.06.2023

Attacco hacker contro Xplain: il Consiglio federale istituisce uno stato maggiore di crisi politico-strategico per la fuga di dati

Nella seduta del 28 giugno 2023, il Consiglio federale ha istituito uno stato maggiore di crisi politico-strategico per la fuga di dati. L'organo interdipartimentale sarà responsabile del coordinamento dei lavori in corso per la gestione dell'attacco ransomware contro Xplain, che ha coinvolto anche dati dell'Amministrazione federale, nonché dell'individuazione delle relative misure. In tale contesto, il Consiglio federale ha conferito un mandato per un'inchiesta amministrativa. Inoltre, ha deciso di far verificare i contratti esistenti con i fornitori di servizi informatici della Confederazione e, all'occorrenza, di adeguarli, in modo tale da migliorare la loro cibersicurezza e permettere all'Amministrazione federale di agire prontamente in caso di riuscita di un attacco. Infine, l'Esecutivo intende far esaminare le misure volte ad assicurare che le prestazioni essenziali attualmente erogate da Xplain per la polizia e per le autorità di sicurezza e migrazione possano essere garantite in ogni caso.

In un attacco ransomware contro Xplain, il gruppo di hacker Play ha rubato un'ingente quantità di dati, tra cui dati operativi dell'Amministrazione federale. Poiché la ditta Xplain, d'intesa con le autorità di perseguimento penale e la Confederazione, non si è prestata al ricatto rifiutando di pagare la somma richiesta, il 14 giugno 2023 gli aggressori hanno pubblicato sul dark web quello che è probabilmente l'intero pacchetto di dati sottratti. Da quando è stata resa nota la fuga di dati, il Centro nazionale per la cibersicurezza (NCSC) ha istituito un'organizzazione incaricata della gestione dell'incidente in stretta collaborazione con le autorità coinvolte. Sono tuttora in corso gli intensi lavori di valutazione e analisi dei dati. Inoltre, la Confederazione ha introdotto le misure necessarie volte a ridurre al minimo i rischi di sicurezza per l'Amministrazione federale.

Coordinamento dei lavori interni e coinvolgimento dei Cantoni

A partire dal 9 giugno 2023 il Consiglio federale è stato informato a più riprese in merito all'incidente. Il 16 giugno 2023 ha deciso di istituire uno stato maggiore di crisi politico-strategico per la fuga di dati (SMCPS-D), incaricato di organizzare i lavori di notevole portata a livello operativo. L'SMCPS-D si è già riunito due volte, rispettivamente il 21 e il 26 giugno 2023. Ciò ha permesso di ottenere una panoramica sui compiti da svolgere nonché di elaborare proposte all'attenzione dell'Esecutivo sugli ulteriori provvedimenti. Nella seduta del 28 giugno 2023, il Consiglio federale ha approvato il mandato dell'SMCPS-D. Sotto la guida della segretaria generale del Dipartimento federale delle finanze (DFF), all'interno dello stato

di crisi collaborano tutti i dipartimenti, la Cancelleria federale e una rappresentanza della Conferenza dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP). Lo stato maggiore di crisi avrà il compito di analizzare e valutare costantemente la situazione strategica, coordinare i lavori interni della Confederazione, garantire lo scambio interno ed esterno di informazioni nonché di elaborare le basi per le ulteriori decisioni del Consiglio federale.

Verifica dei contratti con i fornitori di servizi informatici

Il Consiglio federale ha incaricato il DFF, in collaborazione con l'SMCPS-D, di elaborare un mandato per un'inchiesta amministrativa. Quest'ultima, svolta da un organismo indipendente, consentirebbe di determinare se, dove e perché le direttive in materia di sicurezza della Confederazione presentano delle lacune nell'attuazione, potendo così identificare le misure volte a impedire in futuro un incidente analogo.

Inoltre, nella sua seduta il Consiglio federale ha disposto di verificare i contratti esistenti tra la Confederazione e i fornitori di servizi informatici e, all'occorrenza, di farli adeguare in modo tale da migliorare la cibersicurezza dei fornitori e permettere all'Amministrazione federale di agire prontamente in caso di riuscita di un attacco. Così facendo, unitamente a una definizione dei requisiti nel processo di acquisto, sarebbe possibile garantire che i fornitori della Confederazione rispettino gli standard di protezione definiti in riferimento ai ciberattacchi.

La ditta Xplain vittima dell'incidente è un importante fornitore di servizi informatici per le autorità nazionali e cantonali. Pertanto, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia di esaminare in collaborazione con il CDDGP e il DFF le misure volte ad assicurare la manutenzione e l'ulteriore sviluppo dei software di Xplain, che rivestono un ruolo essenziale.

La Confederazione continuerà a comunicare in modo trasparente gli aggiornamenti sugli ulteriori provvedimenti per la gestione del ciberincidente.

Misure adottate finora

Dopo essere stata informata da Xplain a inizio giugno in merito all'attacco ransomware, l'Amministrazione federale ha adottato misure immediate volte a minimizzare i rischi per la propria sicurezza. Proseguono intanto i lavori di valutazione e le analisi approfondite dei dati, i quali, in ragione delle dimensioni del pacchetto (contenente diversi milioni di dati), richiederanno alcune settimane o persino mesi.

Cronologia degli avvenimenti più importanti

Fine maggio / inizio giugno	La ditta Xplain subisce un ricatto a seguito di un attacco ransomware. D'intesa con le autorità di perseguimento penale e la Confederazione, Xplain rifiuta di pagare la somma richiesta per il riscatto e sporge denuncia contro ignoti. La Confederazione adotta misure immediate volte a minimizzare i rischi per l'Amministrazione federale e i terzi coinvolti. Subito dopo la pubblicazione dei primi dati sul dark web, viene avviata l'analisi del primo pacchetto di dati. I servizi colpiti dall'attacco vengono informati. L'NCSC si occupa del coordinamento dei vari lavori a livello operativo.
8 giugno 2023	Pubblicazione delle prime informazioni concernenti l'attacco ransomware sferrato contro Xplain e l'eventuale furto di dati operativi. (cfr. comunicato stampa dell'8 giugno 2023)
9 giugno 2023	Nel corso della seduta del 9 giugno, il Consiglio federale viene informato

	dal DFF in merito allo stato della situazione e alle misure adottate.
14 giugno 2023	Pubblicazione sul dark web verosimilmente dell'intero pacchetto di dati sottratti da parte del gruppo di hacker Play. La Confederazione avvia il recupero dei dati pubblicati sul dark web, esegue analisi approfondite e fornisce periodicamente informazioni ai servizi colpiti dall'attacco. Poiché sono stati colpiti dati operativi, l'Ufficio federale di polizia (fedpol) e l'Ufficio federale della dogana e della sicurezza dei confini (UDSC) sporgono denuncia contro ignoti per chiarire in quale modo i dati dell'Amministrazione federale sono finiti nel sistema della ditta Xplain. (cfr. comunicato stampa del 14 giugno 2023)
16 giugno 2023	Il DFF informa nuovamente il Consiglio federale in merito ai dati pubblicati sul dark web e ai lavori in corso. L'Esecutivo decide di istituire uno stato maggiore di crisi politico-strategico per la fuga di dati (SMCPS-D) e incarica il DFF di eseguire i relativi lavori.
21 giugno 2023	L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) avvia un'inchiesta su fedpol e l'UDSC poiché sussistono indizi di violazioni potenzialmente gravi delle norme sulla protezione dei dati. Ancor prima entrambi gli Uffici avevano già segnalato attivamente la fuga di dati. Successivamente ulteriori uffici colpiti hanno effettuato simili segnalazioni (cfr. comunicato stampa del 21 giugno 2023).
28 giugno 2023	Il Consiglio federale approva il mandato relativo allo stato maggiore di crisi politico-strategico per la fuga di dati (SMCPS-D) e adotta ulteriori misure.

Per ulteriori informazioni: Comunicazione DFF
Tel. +41 58 462 60 33, kommunikation@gs-efd.admin.ch

Dipartimento responsabile: Dipartimento federale delle finanze DFF

Con il presente comunicato stampa, su www.efd.admin.ch è disponibile quanto segue:

- Comunicato stampa dell'8 giugno 2023: Attacco hacker alla ditta Xplain: colpita anche l'Amministrazione federale (admin.ch)
- Comunicato stampa del 14 giugno 2023: Attacco hacker contro Xplain: le prime analisi dei dati indicano che occorre intervenire (admin.ch)
- Comunicato stampa del 21 giugno 2023: Inchiesta contro fedpol e UDSC (admin.ch)