Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS

20 giugno 2024

Primo bilancio dell'UFCS sui lavori della Rete integrata della situazione ciber in relazione con la conferenza di pace di alto livello sull'Ucraina

Il 15 e 16 giugno 2024 sul Bürgenstock ha avuto luogo la conferenza di alto livello sulla pace in Ucraina che ha visto la partecipazione di delegazioni provenienti da quasi cento Paesi. Già alla vigilia dell'evento erano prevedibili ciberattacchi contro la conferenza e le infrastrutture in Svizzera. In effetti hanno avuto luogo diversi ciberattacchi, tutti tempestivamente individuati e rapidamente respinti. Nel presente rapporto l'Ufficio federale della cibersicurezza (UFCS) traccia un primo bilancio sull'impiego della Rete integrata della situazione ciber.

1. Obiettivi e incarico

Gli obiettivi prioritari in materia di ciberdifesa erano:

1. garantire la **libertà di movimento** e la **disponibilità costante dei mezzi di comunicazione** delle forze di sicurezza e d'impiego;

2. garantire la **confidenzialità**, la **disponibilità** e l'**integrità dei mezzi informatici** di tutti i partecipanti alla conferenza e dei partner della Rete integrata della situazione ciber;

3. far **confluire le informazioni** in modo efficiente laddove apportano il massimo vantaggio operativo;

4. garantire una comprensione **chiara dei ruoli** e **misure unitarie** tra i partner.

Parallelamente al compito di protezione, l'UFCS ha assunto anche il coordinamento globale della preparazione, dello svolgimento e dei lavori successivi della conferenza dando vita alla Rete integrata della situazione ciber, che comprende un centinaio di specialisti di autorità nazionali e cantonali nonché di organizzazioni dell'economia privata. Ogni organizzazione ha assolto i propri compiti e ha condiviso con i partner le informazioni necessarie, contribuendo così all'adempimento del mandato e al raggiungimento degli obiettivi.

2. Rete integrata della situazione ciber e centro di situazione ciber

Giovedì 12 giugno 2024, negli uffici della Polizia cantonale di Lucerna e in collaborazione con essa, l'UFCS ha avviato il centro di situazione ciber per l'impiego nell'ambito della conferenza di pace di alto livello sull'Ucraina. La messa in funzione del centro è stata preceduta da

settimane di pianificazione e di lavori preventivi, tra cui misure di sensibilizzazione per potenziali obiettivi e la riduzione della superficie d'attacco («Attack Surface Management») delle infrastrutture critiche e delle organizzazioni coinvolte.

Grazie al grande impegno di tutte le parti coinvolte e alla buona preparazione, la collaborazione si è svolta in ogni momento senza attriti. La vasta cerchia di partner della Rete integrata della situazione ciber ha contribuito in maniera essenziale all'aumento della ciberresilienza già prima della conferenza e a un disbrigo rapido ed efficiente dei ciberattacchi perpetrati per perturbare la conferenza.

Allo stesso tempo, sotto la direzione dell'UFCS è stato possibile garantire la comunicazione all'opinione pubblica, con l'obiettivo di informare tutti i partner nel modo più trasparente, corretto e rapido possibile sugli incidenti rilevanti per loro. Ciò ha richiesto l'elaborazione costante di informazioni aggiornate dalla Rete integrata della situazione ciber e il confronto con le organizzazioni partner.

3. Eventi nel ciberspazio verificatisi a causa della conferenza

Poco prima, durante e per un breve periodo dopo la conferenza, si sono registrati diversi incidenti nel ciberspazio svizzero, tra cui vale la pena ricordare:

- **Attacchi di sovraccarico contro i siti web di autorità e organizzazioni**
  Giovedì 13 giugno 2024 l'UFCS e i suoi partner hanno rilevato attacchi di sovraccarico (cosiddetti attacchi DDoS), chiaramente riconducibili a un gruppo di hacktivisti filorussi denominato «NoName057(16)», diretti contro i siti web pubblici di 22 autorità e organizzazioni svizzere. Nel complesso gli attacchi sferrati si sono mantenuti entro i limiti del previsto e hanno comportato soltanto brevi perturbazioni delle infrastrutture informatiche. In nessun momento vi è stata una minaccia concreta per i sistemi informatici e i dati della conferenza o delle organizzazioni coinvolte nel suo svolgimento.

- **Tentativi di effrazione digitale nei sistemi informatici dei Cantoni di NW/OW**
  Il centro informatico dei Cantoni di Nidvaldo (NW) e Obvaldo (OW) ha segnalato tentativi di effrazione digitale indirizzati contro i suoi sistemi di posta elettronica. Da un'analisi svolta dall'UFCS è emerso che si è trattato di tentativi di carattere opportunistico privi di un nesso con la conferenza. Tali tentativi non sono andati a buon fine. Insieme all'UFCS il centro informatico dei due Cantoni ha individuato misure di rafforzamento e le ha messe in atto immediatamente.

- **Attacco di phishing rivolto contro i collaboratori della centrale per chiamate d'emergenza sanitaria del Cantone di Lucerna (LU)**
  Poco prima della conferenza è stato posto in essere un presunto ciberattacco diretto contro i collaboratori della centrale per chiamate d'emergenza sanitaria del Cantone di Lucerna. Inviando e-mail fasulle (cosiddette e-mail di phishing), gli autori ignoti avevano tentato verosimilmente di ottenere i dati di accesso dei collaboratori. Questi ultimi hanno riconosciuto il ciberattacco come tale e lo hanno segnalato alla Rete integrata della situazione ciber. Il fatto che i collaboratori abbiano reagito in modo rapido ha consentito di respingere il ciberattacco con tempestività.

- **Da una gaffe durante la diretta streaming del DFAE sono nate voci riguardo a ciberattacchi**
  Dopo la trasmissione in diretta di un intervento della presidente della Confederazione Viola Amherd e del presidente ucraino Zelensky, i collaboratori dei servizi di interpretazione hanno dimenticato di spegnere i loro microfoni. Durante la diretta

streaming del DFAE, questi ultimi discutendo hanno parlato di «problemi tecnici» durante l'interpretazione e un collaboratore ha aggiunto di aver messo in guardia da ciberattacchi prima della conferenza. In seguito a questo inconveniente vi sono state diverse richieste dei media rivolte all'UFCS e al Dipartimento federale degli affari esteri (DFAE) e sono apparsi diversi contributi in alcuni media svizzeri in merito a possibili ciberattacchi (russi). I problemi tecnici riscontrati però non erano riconducibili a un ciberattacco.

- **Blackout nella città di Berna**
  Un blackout verificatosi domenica mattina nella città di Berna ha dato adito a voci riguardo a un possibile ciberattacco. In seguito al blackout, alcune autorità federali e altre organizzazioni insediate a Berna hanno attivato l'alimentazione elettrica di emergenza. Gli accertamenti svolti insieme ai gestori di rete e alle centrali elettriche hanno consentito di escludere un ciberattacco all'origine del blackout.

- **Vandalismo digitale**
  Perpetrando atti di vandalismo digitale su un portale pubblicamente accessibile, autori ignoti hanno compromesso per breve tempo la fruibilità di un sistema d'impiego. Il portale viene gestito da un'associazione svizzera. L'incidente è stato individuato in tempi brevi e i dati «corrotti» sono stati immediatamente rimossi dal sistema d'impiego. La sicurezza di sistemi rilevanti per gli impieghi e dei relativi dati non è stata messa in pericolo in nessun momento.

Si sono verificati altri presunti ciberattacchi contro il dispositivo di sicurezza della conferenza e relative misure sono state adottate in tempi rapidi. In questo momento non vengono fornite ulteriori informazioni in merito a tali attacchi. Grazie alle misure adottate, tali attacchi non hanno messo in pericolo in nessun momento la sicurezza o lo svolgimento della conferenza.

4. In generale

L'UFCS ha concluso l'impiego della Rete integrata della situazione ciber domenica 16 giugno. Il 20 giugno 2024, l'UFCS ha rilevato ancora alcuni attacchi DDoS contro obiettivi in Svizzera. La situazione dovrebbe normalizzarsi nei prossimi giorni.