Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

20. Juni 2024

Erste Bilanz des BACS zu den Arbeiten des Cyberlageverbunds in Zusammenhang mit der hochrangigen Konferenz zum Frieden in der Ukraine

Vom 15. bis am 16. Juni 2024 fand auf dem Bürgenstock die hochrangige Konferenz zum Frieden in der Ukraine unter Beteiligung von Delegationen aus fast hundert Staaten statt. Im Vorfeld wurde mit Cyberangriffen auf die Konferenz und auf Infrastrukturen in der Schweiz gerechnet. Tatsächlich kam es dann auch zu verschiedenen Cyberangriffen, die jedoch alle frühzeitig erkannt und rasch abgewehrt werden konnten. Im vorliegenden Bericht zieht das Bundesamt für Cybersicherheit (BACS) eine erste Bilanz über den Einsatz des Cyberlageverbundes.

1. Ziele und Auftrag

Die prioritären Ziele in der Cyberabwehr waren:

1. **Bewegungsfreiheit** und allzeitig **verfügbare Kommunikationsmittel** der Sicherheits- und Einsatzkräfte gewährleisten;

2. **Vertraulichkeit, Integrität und Verfügbarkeit von IT-Mitteln** aller Konferenz-Teilnehmenden und Cyberlageverbund-Partner gewährleisten;

3. **Informationen fliessen** effizient dorthin, wo sie den maximalen operativen Nutzen erbringen;

4. Klares **Rollenverständnis** und einheitliche **Massnahmen** zwischen Partnern.

Das BACS übernahm zusätzlich zu seinem Schutzauftrag die Gesamtkoordination der Vorbereitung, Durchführung und Nachbereitung. Der Cyberlageverbund umfasste knapp hundert Spezialistinnen und Spezialisten von nationalen und kantonalen Behörden sowie Organisationen aus der Privatwirtschaft. Jede Organisation erfüllte ihre Aufgabe und teilte die notwendigen Informationen mit den Partnern. Der Auftrag wurde erfüllt, die Ziele erreicht.

2. Cyberlageverbund und Cyberlagezentrum

Zusammen mit der Luzerner Polizei hat das BACS am Donnerstag, 12. Juni 2024 das Cyberlagezentrum für den Einsatz zur hochrangigen Konferenz zum Frieden in der Ukraine in den Büroräumlichkeiten der Luzerner Polizei in Betrieb genommen. Zuvor fanden über

Wochen hinweg Planungsarbeiten und die Durchführung präventiver Arbeiten statt. Diese umfassten unter anderem Sensibilisierungsmassnahmen für potentielle Ziele und das Reduzieren der Angriffsfläche («Attack Surface Management») von kritischen Infrastrukturen und involvierter Organisationen.
Dank dem hohen Engagement aller Beteiligten und der guten Vorbereitung hat die Zusammenarbeit zu jedem Zeitpunkt reibungslos funktioniert. Die breite Abstützung des Cyberlageverbunds hat wesentlich dazu beigetragen, dass bereits im Vorfeld der Konferenz die Cyberresilienz erhöht sowie während der Durchführung der Konferenz auf Cyberbedrohungen rasch und effektiv reagiert werden konnte.

Parallel dazu wurde unter Leitung des BACS die Kommunikation an die Öffentlichkeit sichergestellt. Ziel war es, dass alle Partner möglichst transparent, korrekt und rasch über für sie relevante Vorfälle informiert wurden. Dies erforderte es, laufend aktuelle Informationen aus dem Lageverbund aufzubereiten und sich mit den Partnerorganisationen abzugleichen.

3. Ereignisse im Cyberraum aufgrund der Konferenz

Kurz vor, während und für kurze Zeit nach der Konferenz kam es in der Schweiz zu verschiedenen Ereignissen im Cyberraum. Hierbei sind insbesondere die folgenden Ereignisse erwähnenswert.

- **Überlastungsangriffe gegen Webseiten von Behörden und Organisationen:**
  Am Donnerstag, 13. Juni 2024, detektierte das BACS zusammen mit dessen Partnern Überlastungsangriffe (sogenannte «DDoS-Angriffe»), welche nachweislich von einer pro-russischen Hacktivisten-Gruppe namens «NoName057(16)» ausgeführt wurden. Diese Cyberangriffe waren gegen öffentliche Webauftritte von total 22 Schweizer Behörden und Organisationen gerichtet. Insgesamt lagen die Überlastungsangriffe im Bereich des Erwarteten und führten lediglich zu kleineren Störungen von IT-Infrastrukturen. Zu keiner Zeit bestand jedoch eine Gefährdung von IT-Systemen oder Daten der Konferenz oder in die Durchführung der Konferenz involvierten Organisationen.

- **Digitale Einbruchsversuche in IT-Systeme der Kantone NW/OW:**
  Die Informatik der Kantone Nidwalden (NW) und Obwalden (OW) meldeten digitale Einbruchsversuche auf deren E-Mail-Systeme. Eine Analyse des BACS hat ergeben, dass es sich dabei um opportunistische Einbruchsversuche handelt, welche nicht im Zusammenhang mit der Konferenz stehen. Die Einbruchsversuche blieben erfolglos. Die Kantonsinformatik identifizierte zusammen mit dem BACS Massnahmen zur Härtung und setzte diese umgehend um.

- **Phishing-Angriff gegen Mitarbeitende der Sanitätsnotrufzentrale Luzern (LU):**
  Kurz vor der Konferenz fand ein mutmasslicher Cyberangriff gegen Mitarbeitende der Sanitätsnotrufzentrale des Kantons Luzern statt. Dabei haben unbekannte Täter mutmasslich versucht, mittels gefälschter E-Mails (sogenannte «Phishing E-Mails») an Zugangsdaten von Mitarbeitenden zu gelangen. Der Cyberangriff wurde durch Mitarbeitende als solcher erkannt und dem Cyberlageverbund gemeldet. Dank der raschen Reaktion der Mitarbeitenden konnte der Cyberangriff frühzeitig abgewehrt werden.

- **Fauxpas während Live-Stream des EDA führt zu Gerüchten um Cyberangriffe:**
  Nach einer Liveübertragung einer Rede von Bundespräsidentin Viola Amherd und des ukrainischen Präsidenten Selenskyj haben Mitarbeitende des Dolmetscherdienstes vergessen ihr Mikrofon abzuschalten. In der darauffolgenden Diskussion berichteten diese im Live-Stream des EDA von «technischen Problemen» während der

Übersetzung, wobei der eine anmerkte, er habe im Vorfeld der Konferenz ja vor Cyberangriffen gewarnt. Dieses Missgeschick führte zu verschiedenen Medienanfragen beim BACS und dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) sowie zu Berichterstattungen über mögliche (russische) Cyberangriffe in einigen Schweizer Medien. Den genannten technischen Problemen lag jedoch kein Cyberangriff zu Grunde.

- **Stromausfall in der Stadt Bern:**
  Ein Stromausfall in der Stadt Bern am Sonntagmorgen schürte Gerüchte über einen möglichen Cyberangriff. Der Stromausfall führte dazu, dass bei einigen Bundesbehörden sowie weiteren in Bern beheimateten Organisationen auf Notstrom umgeschaltet wurde. Nach Abklärung mit den Netzbetreibern und Elektrizitätswerken konnte ein Cyberangriff als Ursache des Stromausfalls ausgeschlossen werden.

- **Digitaler Vandalismus:**
  Eine unbekannte Täterschaft hat durch digitalen Vandalismus auf einem öffentlich zugänglichen Portal zu einer kurzzeitigen Beeinträchtigung eines Einsatzsystems geführt. Das Portal wird durch einen Schweizer Verein getragen und betrieben. Der Vorfall wurde rasch erkannt und die «verunstalteten» Daten konnten zeitnah aus dem Einsatzsystem entfernt werden. Zu keiner Zeit bestand eine Gefährdung der Sicherheit von einsatzrelevanten Systemen oder deren Daten.

Es gab weitere mutmassliche Cyberangriffe gegen das Sicherheitsdispositiv der Konferenz. Massnahmen wurden schnell getroffen. Über diese Angriffe wird zum aktuellen Zeitpunkt keine weitere Auskunft erteilt. Die Angriffe konnten jedoch aufgrund der Massnahmen die Sicherheit oder Durchführung der Konferenz zu keiner Zeit gefährden.

4. Generelles

Das BACS beendete den Einsatz des Cyberlageverbunds am Sonntag, 16. Juni.
Am 20. Juni 2024 stellte das BACS noch immer einzelne DDoS-Angriffe auf Ziele in der Schweiz fest. Es ist davon auszugehen, dass sich die Lage in den kommenden Tagen wieder normalisiert.