28. März 2025 | Bundesamt für Cybersicherheit BACS

Jahresbericht 2024

Bundesamt für Cybersicherheit BACS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Inhalt

Vorwort

Das Bundesamt für Cybersicherheit (BACS) blickt auf sein erstes Jahr zurück. Dabei konnten die als Nationales Zentrum für Cybersicherheit (NCSC) im Eidgenössischen Finanzdepartement (EFD) aufgebauten Leistungen dank der neuen Struktur als Bundesamt optimiert und stabilisiert werden. Nach wie vor sind wir ein kleines Bundesamt und stehen oft vor der Herausforderung, mit wenig Mitteln viele Aufgaben gleichzeitig bewältigen zu müssen. Mit innovativen Ansätzen, viel Einsatz aller Mitarbeitenden und Investitionen in die Digitalisierung ist es uns aber gelungen, unseren Output weiter zu steigern und unser Angebot einem breiteren Publikum zur Verfügung zu stellen.

Wir haben somit nun eine Basis dafür gelegt, unseren gesetzlichen Auftrag zu erfüllen und können unsere Dienstleistungen zu skalieren. Dies ist wichtig, da die Anforderungen aus Gesellschaft, Wirtschaft und Politik an das Bundesamt weiter steigen. Die Bedrohungslage im Cyberbereich nimmt weiter zu. Der Wandel von Globalisierung hin zu Regionalisierung, die Fragmentierung von Regulation zwischen Wirtschaftsräumen und die zunehmende Nutzung von Cyber als Hilfsmittel zur Durchsetzung von Interessen haben direkten Einfluss auf die Cybersicherheit von Wirtschaft und Gesellschaft.

Im Dialog mit dem Ausland zeigt sich, dass die Schweiz in diesem Bereich eine wichtige Rolle spielen kann. Die Strategie des BACS wird gerne als gutes Beispiel aufgeführt, die Arbeiten des BACS und seiner Mitarbeitenden wird geschätzt und die Art und Weise wie wir mit unseren nationalen und internationalen Angelegenheiten herausfordernde Operationen durchführen, stösst über die Landesgrenzen hinweg auf Interesse.

Es bleibt aber anspruchsvoll, die Vielzahl von Herausforderungen zu bewältigen und den Wünschen und Ideen, welche von Wirtschaft, Hochschulen, Kantonen und Politik an uns herangetragen werden, gebührend Rechnung zu tragen. Wir müssen darauf achten, dass wir uns nicht verzetteln und sicherstellen, dass wir unser operatives Tagesgeschäft stets in der gewohnt hohen Qualität erledigen. Ausserdem müssen wir bereit sein, unsere Leistung auszubauen, wenn dies gewünscht und finanziert wird.

Ich bin stolz darauf, dass wir es geschafft haben, eine breite Palette von Dienstleistungen anzubieten und gleichzeitig einen hohen Qualitätsstandard zu halten. Dies zeigen die positiven Rückmeldungen, die wir von unseren Partnern als auch aus der Bevölkerung erhalten.

Die nächsten zwei bis drei Jahre werden für unsere Weiterentwicklung entscheidend sein. Ich freue mich darauf mit den Mitarbeitenden des BACS und all unseren Partnerorganisationen die Cybersicherheit der Schweiz zu gestalten. Ich erhoffe mir zudem, dass die Politik möglichst klare Vorgaben darüber macht, welche Leistungen von uns in welchem Umfang erwartet werden und auf welche Ressourcen wir dabei zurückgreifen dürfen.

Das BACS ist motiviert, die Chancen zu nutzen, damit die Schweiz weiterhin ein verlässlicher Akteur im Cyberbereich zum Nutzen der Wirtschaft, der Gesellschaft und der Behörden sein kann.

Florian Schütz, Direktor Bundesamt für Cybersicherheit

Wichtigste Kennzahlen 2024

13.3 Mio. CHF
Ausgaben

63
Mitarbeitende

62’954
Freiwillige Meldungen zu Cybervorfällen

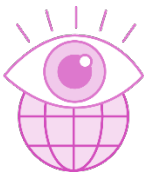
616
Medienkontakte

1’100
Unternehmen auf dem Cyber Security Hub

991’309
Meldungen zu mit Schadsoftware infizierten Geräten analysiert

371
Meldungen von Schwachstellen durch ethische Hacker

38
Weekly Cyber Situation Briefings



7
Sensibilisierungskampagnen

8’116
Command and Control Systeme von Angreifern identifizert und gesperrt

Stand Dezember 2024

Ziele des BACS

Vision

Cybersicherheit ist eine Gemeinschaftsaufgabe von Politik, Wirtschaft, Hochschulen und Gesellschaft. Viele Organisationen und Einzelpersonen haben Schwierigkeiten, Cyberrisiken einzuschätzen und mit ihnen umzugehen. Intransparenz über die Sicherheit digitaler Produkte führt zu Unsicherheit bei den Konsumentinnen und Konsumenten und zu Verwundbarkeiten. Durch die zunehmende Vernetzung können durch unzureichend geschützte Systeme grossflächige Schäden verursacht werden.

Die Vision des BACS ist es, die Cybersicherheit in der Schweiz in enger Zusammenarbeit mit allen relevanten Akteuren zu verbessern:

Das BACS legt das Fundament für eine sichere Nutzung digitaler Dienstleistungen und Infrastrukturen in der Schweiz und befähigt die Schweiz, zu einem der führenden Länder bezüglich sicherer Digitalisierung zu werden.

Mission

Der Kernauftrag des BACS ist es, die Cybersicherheit von kritischen Infrastrukturen, Wirtschaft, Bildungswesen, Bevölkerung und Behörden zu stärken, indem es die Umsetzung der Nationalen Cyberstrategie (NCS) koordiniert.

Um seine Kernaufgabe zu erfüllen, richtet das BACS seine Leistung entlang vier strategischer Säulen aus:

Die vier strategischen Säulen

1 Cyberbedrohungen verständlich machen

Das BACS macht die komplexen Zusammenhänge, die zu Cyberbedrohungen führen, zielgruppengerecht verständlich. Damit ermöglicht es einen fundierten Dialog zwischen Politik, Wirtschaft und Gesellschaft über Cybersicherheit und befähigt alle, ihre individuelle Verantwortung so wahrzunehmen, dass die systemischen Risiken sinken.

2 Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen

Das BACS reduziert die Angriffsfläche von Schweizer Personen und Organisationen im Cyberraum. Es warnt vor Angriffen und stellt Informationen sowie gegebenenfalls technische Instrumente zur Verfügung, die deren Verhinderung erleichtern.

3 Schäden aus Cybervorfällen reduzieren

Das BACS hilft Betroffenen von Cybervorfällen, Schäden zu reduzieren und das Risiko einzugrenzen, dass Vorfälle sich auf weitere Opfer ausweiten.

4 Sicherheit von digitalen Produkten und Dienstleistungen erhöhen

Das BACS fördert ökonomische Modelle und schafft Anreize für Hersteller, sichere und erschwingliche Produkte und Dienstleistungen anzubieten. Es fördert die Tranparenz für Nutzer, sodass sie informierte Entscheide über die Cybersicherheit von Produkten und Dienstleistungen treffen können.

Finanzielle Mittel

Das Jahr 2024 war für das BACS finanziell geprägt von der Transformation in ein Bundesamt sowie der bevorstehenden Einführung der Meldepflicht. Die gestaffelte Rekrutierung und die Verschiebung geplanter IT-Projekte sorgten für eine Budgetunterschreitung. Aus diesen werden für die kommenden Jahre zweckgebundene Reserven geschaffen, welche helfen werden, die wichtigsten Projekte auch bei knappem Budget voranzutreiben.

Ausgaben im Jahr 2024

Im Jahr 2024 belief sich die definitive Rechnung des BACS auf 13.3 Millionen CHF. Die Sach- und Betriebsausgaben beliefen sich auf 2,6 Millionen CHF. Von den 1,9 Millionen CHF, die für Informatik ausgegeben wurden, entfielen 0,4 Millionen auf den Betrieb und 1,5 Millionen auf Weiterentwicklungen. Ein wesentlicher Teil der IT-Ausgaben wurde für die Etablierung der neuen Meldestelle für Cyberangriffe auf kritische Infrastrukturen bereitgestellt. 1 Million CHF floss in den Ausbau des «Cyber Security Hub (CSH)». Nicht aufgeführt sind Kosten der Bundesleistungserbringer, welche durch das Generalsekretariat des Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (GS-VBS) getragen wurden. Rund 0,35 Millionen CHF wurden für die Durchführung von Bug-Bounty-Programmen genutzt, um Schwachstellen in IT-Systemen der Bundesverwaltung zu identifizieren und zu beheben. Für Projekte im Rahmen der NCS wurden insgesamt 0.33 Millionen CHF eingesetzt, darunter der Aufbau einer Analyseplattform für Cybervorfälle und Sensibilisierungsmassnahmen.

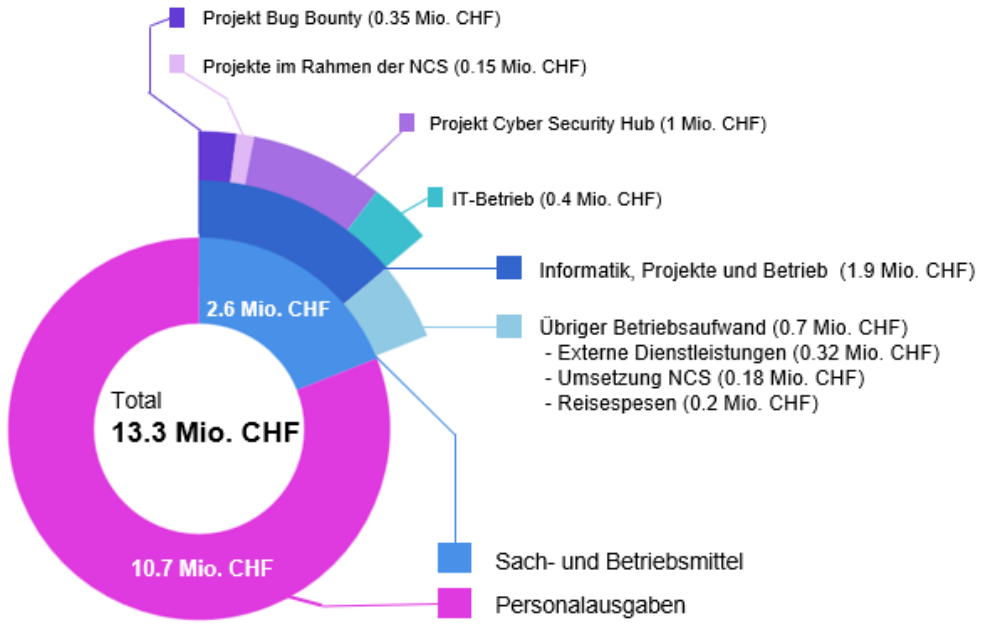


Abbildung 1: Finanzielle Mittel BACS - Rechnung 2024

Einsatz der finanziellen Mittel

Der grösste Teil der Sach- und Betriebsmittel fliesst in die Prävention und in die Behandlung und Nachbearbeitung von Cybervorfällen (88%). Sie werden somit für den Kernauftrag des BACS verwendet. Der administrative Aufwand wird möglichst klein gehalten, er betrug im Jahr 2024 8 Prozent.

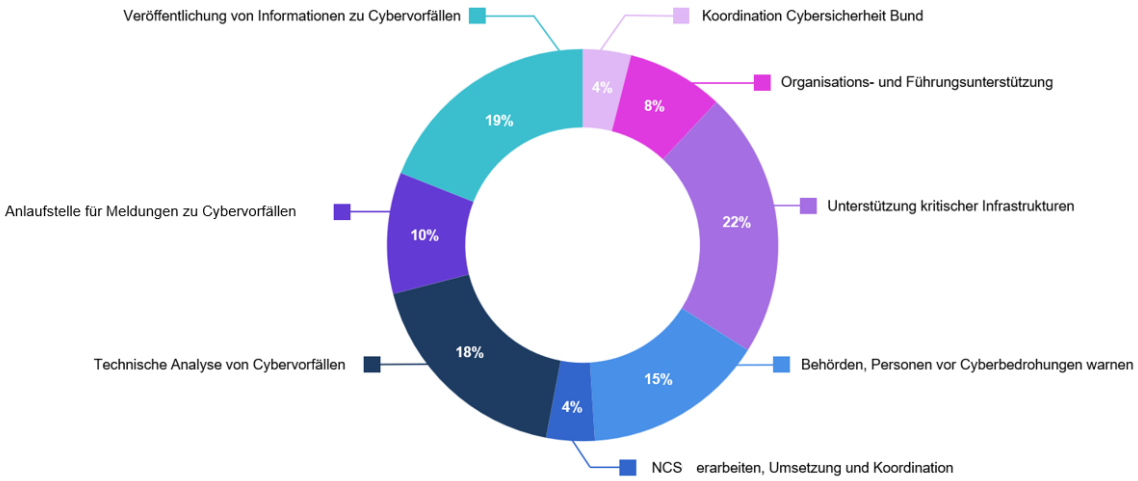


Abbildung 2: Verteilung der finanziellen Mittel nach Aufgaben

Personalstruktur

Die Personalausgaben betrugen 10,7 Millionen CHF. Im Laufe des Jahres konnte das BACS 24 neue Mitarbeitende einstellen. Vor allem das Incident Response Team wurde erheblich gestärkt. Der personelle Ausbau war bereits bei der Überführung in ein Bundesamt geplant und fand auch im Hinblick auf die Einführung der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen statt. Um junge Talente zu fördern und ihnen einen wertvollen Einblick in die Cybersicherheit zu ermöglichen, hat das BACS gezielt Hochschulpraktikantinnen und Hochschulpraktikanten eingestellt, die uns bei unseren Projekten unterstützen.

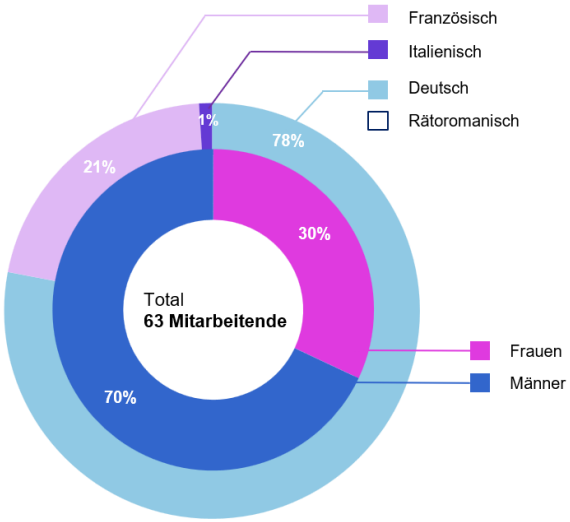


Abbildung 3: Mitarbeitende BACS Stand Dezember 2024

Managementmethode

Objectives and Key Results

Das BACS arbeitet seit dem 4. Quartal 2024 nach der OKR-Methodik (Objectives & Key Results). Die Einführung bzw. Umstellung auf das BACS ausgerichtete OKR-Framework erfolgte schrittweise, bedarfsorientiert und abgestimmt auf die Verwaltungsstruktur sowie die Organisationsgrundlagen des BACS.

Das Planungs- und Steuerungsinstrument stellt sicher, dass im BACS alle Organisationsbereiche quartalsweise koordiniert und zielgerichtet an der Umsetzung strategischer Themen sowie im Rahmen des gesetzlichen Auftrags arbeiten. Die Anwendung der Methodik stärkt die Teamautonomie, involviert die Mitarbeitenden über alle Hierarchiestufen hinweg sowohl in der Planungs- als auch in der Umsetzungsphase und bietet klare Rahmenbedingungen. Durch die Schaffung von Transparenz und Nachvollziehbarkeit sowie einen reibungslosen Informationsfluss innerhalb der gesamten Organisation trägt die Methodik auch zur Weiterentwicklung der Betriebskultur des BACS bei.

Nach der Pilotphase konnte bereits ein erster positiver Effekt festgestellt werden. Die Einführungsphase wurde abgeschlossen, und die Methodik ist seit 2025 fester Bestandteil der Führungsinstrumente im BACS. Das Planungs- und Steuerungsinstrument erfordert weiterhin besondere Aufmerksamkeit, um die Strukturen und Prozesse des Bundesamtes in den Gesamtkontext der Bundesverwaltung optimal einzubetten.

Objectives Q4 2024

- O1 - Interessierte Personen und Organisationen informieren sich über die zur Verfügung stehenden Leistungen des BACS.
- O2 - Das BACS schafft die Ausgangslage, sich international zu positionieren.
- O3 - Das BACS weist den Nutzen seiner Arbeit aus.
- O4 - Die systemrelevanten Bereiche der Schweiz sehen sich in ihrer Cybersicherheit durch das BACS begleitet.

Abbildung 4: Visualisierte Objectives Q4 2024

Tätigkeiten des BACS anhand der vier Strategischen Säulen

1 Cyberbedrohungen verständlich machen

Im Jahr 2024 hat das BACS kontinuierlich und zielgerichtet Informationen über Cyberbedrohungen der Wirtschaft, den Behörden und der Bevölkerung weitergegeben. Solche Informationen helfen den Schutz vor Cyberbedrohungen gezielt zu stärken. Als Kommunikationskanäle für die Öffentlichkeit nutzt das BACS die Website auf welcher sie aktuelle Warnungen, Wochenrückblicke und technische Kurzanalysen publiziert. Darüber hinaus trugen die Halbjahresberichte dazu bei, einen umfassenden Überblick über die wichtigsten Cybersicherheitsereignisse und -entwicklungen zu bieten und strategische Handlungsempfehlungen abzuleiten.

Mit Sensibilisierungskampagnen trägt das BACS zu einem besseren Verständnis der Cybersicherheit bei. Mit der SUPER Kampagne 2024 und dem European Cyber Security Month hat das BACS gemeinsam mit Partnerorganisationen die breite Öffentlichkeit angesprochen. Für einzelne Zielgruppen – etwa für Gemeindebehörden – wurden auch spezifische Kampagnen durchgeführt.

Präventive Cybersicherheit

Neben den Informationen zu Cyberbedrohungen stärkt das BACS die Prävention auch durch die Entwicklung von Methoden und Schulungen sowie Publikationen und Referaten, die gezielt Entscheidungsträger aus der Wirtschaft, Verwaltung und Politik unterstützten. Kernelement dieser Arbeiten sind die Minimalstandards für die IKT-Sicherheit und die Empfehlungen und Best Practices. Diese Grundlagen erarbeitet das BACS in enger Abstimmung mit international anerkannten Normungsorganisationen. Im Jahr 2024 fokussierte sich das BACS auf die Erarbeitung von Grundlagen über die Integration von Post-Quanten-Kryptographie und zur Verbesserung der Sicherheitsverfahren in Unternehmen. Das BACS publizierte Ergebnisse seiner Studien unter anderem auch in international renommierten Fachzeitschriften. Die Publikationen des BACS, insbesondere zur kritischen Hinterfragung von Wahrscheinlichkeitsschätzungen im Risikomanagement und Sicherheitsstandards, stiessen international auf Interesse und trugen zu einem transparenten und kritischen Austausch im Bereich Cybersicherheit bei.

Pilotprojekt «Cybersicherheit in der Lieferkette»

2024 führte das BACS gemeinsam mit Planzer Transport AG ein Pilotprojekt zur Cybersicherheit in der Lieferkette durch. Ziel war es, Fachwissen und Ressourcen aus der Branche und der Cybersicherheit zu bündeln und ein strukturiertes Vorgehen sowie praxisorientierte Hilfsmittel zur Verbesserung der Cybersicherheit von Unternehmen entlang der Lieferketten zu entwickeln. Die Hilfsmittel sollen Unternehmen dabei unterstützen, Cybersicherheitsrisiken in der Lieferkette systematisch zu identifizieren, zu bewerten und gezielt zu managen.

Das erfolgreiche Pilotprojekt unterstreicht, dass Cybersicherheit kein einmaliges Vorhaben, sondern ein fortlaufender Prozess ist. Durch die enge Zusammenarbeit aller Beteiligten konnte eine Lösung entwickelt werden, die langfristig zur Erhöhung der Sicherheit in der Lieferkette beiträgt.

Meilensteine und Erfolge

Entwicklung eines strukturierten Ansatzes: Der entwickelte Kreislauf ermöglicht eine kontinuierliche Verbesserung der Cybersicherheitslage.

Pragmatische Umsetzung: Dank eines praxisnahen und skalierbaren Ansatzes konnte das Konzept schnell implementiert und das Engagement der Verbände gewonnen werden.

Herausforderungen gemeistert: Zu den grössten Herausforderungen zählten die Festlegung eines gemeinsamen Ansatzes, die Schaffung einer einheitlichen Sprache sowie die Ressourcenplanung für parallele und überschneidende Aktivitäten.

Wissenstransfer für KMU: Die Erkenntnisse des Projekts kommen nicht nur der Logistik- und Transportbranche zugute, sondern sollen ab 2025 auch weiteren KMU in der Schweiz zur Verfügung gestellt werden.

Weiterentwicklung des Produkts: Eine Fachgruppe wird sich kontinuierlich mit der Optimierung und Ergänzung der Hilfsmittel befassen, um neue Anforderungen an die Cybersicherheit zu integrieren.

Abbildung 5: Massnahmen zum Schutz vor Cyberangriffen in der Lieferkette

Umsetzung der Nationalen Cyberstrategie (NCS)

Die aktuelle Nationale Cyberstrategie (NCS) wurde im April 2023 durch den Bundesrat und die Kantone gutgeheissen. Die Umsetzung der NCS wurde durch das BACS auch 2024 weiter vorangetrieben und koordiniert, mit dem Ziel, die nationale Widerstandsfähigkeit gegenüber wachsenden Cyberbedrohungen zu stärken. Die Umsetzung wird von einem Steuerungsausschuss begleitet (StA NCS). Die Rolle und die Zusammensetzung des StA NCS wurden erweitert, um ihm mehr Unabhängigkeit zu verleihen und eine bessere strategische Ausrichtung und breitere Abstützung zu ermöglichen. Der StA NCS tagte erstmals im Juni 2024. Nach seiner Einsetzung hat er im Jahr 2024 fünf Arbeitsgruppen entlang der fünf strategischen Ziele der NCS gebildet, um sich vertieft mit der Strategie auseinanderzusetzen und die anstehenden Prioritäten zu bewerten und zu gewichten.

Im September 2024 organisierte das BACS in Zusammenarbeit mit dem Sicherheitsverbund Schweiz (SVS) die Nationale Cybersicherheitskonferenz. Der Schwerpunkt der Konferenz lag auf der Thematik «Geopolitik und operative Sicherheit». Die Konferenz trug zur Vertiefung des Wissensaustauschs und der nationalen Zusammenarbeit bei und unterstrich das gemeinsame Engagement aller Akteure, die Ziele und Massnahmen der NCS umzusetzen. Über 280 Personen aus Wirtschaft, Wissenschaft sowie Kantonen und der Bundesverwaltung nahmen teil. 93 Prozent der Teilnehmer bewerteten die Veranstaltung als gut oder ausgezeichnet (Weiterempfehlungswert (NPS): 59). Das BACS spielt eine zentrale Rolle bei der Umsetzung der NCS und leistet mit den in diesem Bericht dargestellten Arbeiten einen wesentlichen Beitrag zur Implementierung aller fünf strategischen Ziele, konkret zu 15 der 17 Massnahmen. Detaillierte Informationen zur Umsetzung der NCS, werden im ersten Umsetzungsbericht des NCS im Frühjahr 2025 publiziert.

Abbildung 6: Ziele und Massnahmen NCS

2 Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen

Der Austausch von Informationen zu aktuellen Bedrohungen, Angriffsmustern und möglichen Gegenmassnahmen ist ein Schlüsselelement bei der Verhinderung von Cyberangriffen. Das BACS versteht sich als Plattform für diesen Informationsaustausch und arbeitet darauf hin, dass relevante Informationen zu Cyberangriffen zentral zusammenfliessen, analysiert werden und die Ergebnisse der Analysen dann als Handlungsempfehlung wiederum allen interessierten Organisationen zur Verfügung gestellt werden können.

Informationsaustausch über den CSH

Für den Informationsaustausch über Cyberbedrohungen und Massnahmen zwischen Behörden und Unternehmen betreibt das BACS seit Herbst 2022 den Cyber Security Hub (CSH). Diese online Plattform dient als Instrument für den Austausch und das Management von Informationen über Cyberbedrohungen, Cybervorfälle, Schwachstellen und Cybersicherheitspraktiken.

Der CSH hat sich im Jahr 2024 zu einer leistungsfähigeren, benutzerfreundlicheren und effizienteren Plattform entwickelt. Die Verbesserungen tragen dazu bei, dass Organisationen in der Schweiz besser vor Cyberbedrohungen geschützt sind. Dies zeigt sich auch darin, dass die Nutzerzahlen des CSH von 1’000 Nutzenden im Jahr 2023 auf 3’300 Nutzende im Jahr 2024 gesteigert werden konnten.

Die auf dem CSH registrierten Unternehmen werden wöchentlich mittels einem Online-Austausch über die aktuelle Cyberbedrohungslage informiert. Wöchentlich nehmen rund 350 Cybersicherheitsspezialistinnen und -spezialisten an diesen Veranstaltungen teil (Weiterempfehlungswert (NPS): 60).

Sektorspezifische Initiativen

Der Informationsaustausch wird auch durch die sektorspezifische Cyberdienstleistung erarbeitet. Dazu unterstützt das BACS in verschiedenen Sektoren und Communities den Aufbau von «Cyber Security Centres» (CSC). CSCs sind sektorspezifische Kompetenzzentren für präventive Cybersicherheitsmassnahmen, Informationsaustausch, Bedrohungsanalysen und Sensibilisierungsmassnahmen sowie die Bewältigung von Vorfällen, die mit dem BACS eng zusammenarbeiten, aber auch die Bedürfnisse der sektoriellen Akteure im Cyberbereich berücksichtigen. Das BACS agiert dabei insbesondere als zentraler Koordinator und Betreiber des nationalen CSH. Die Vision des BACS ist es, alle kritischen Sektoren in sektoriellen CSCs zu organisieren. Bereits etablierte CSCs sind das FS-CSC mit dem Finanzsektor oder das Swiss Industry Cybersecurity Association (SWICYBA - CSC). Im Aufbau befindet sich das Healthcare-CSC, wo die Pilotphase im Februar 2025 abgeschlossen wurde und der Rail-Information Sharing and Analysis Center (Rail-ISAC) mit dem Bahnsektor. Das Konzept des IG-CSC mit NGOs des internationalen Genfs ist bereit und wird nach verfügbaren Ressourcen umgesetzt.

Weitere Initiativen betreffen die Organisation von sektorspezifischen Roundtables mit kritischen Infrastrukturen.

Cyber Threat Intelligence

Für die Betreiberinnen von kritischen Infrastrukturen stellt das BACS technische Informationen zu aktuellen Cyberbedrohungen (sogenannte «Cyber Threat Intelligence») bereit und tauscht sich mit den Betreiberinnen von kritischen Infrastrukturen aus.

Über die Plattform antiphising.ch wurden dem BACS 975'309 Meldungen zu verdächtigen Webseiten mitgeteilt, aus welchen über 20'000 Phishing Webseiten erhoben werden konnten. Zudem hat das BACS fast 1'000'000 Hinweise zu infizierten Geräten wie Smartphones, Computer oder «Internet of Things» (IoT) Geräten in der Schweiz erhalten und an die jeweilige Betreiberin oder den zuständigen Internetanbieter versendet. Schliesslich konnte das BACS 8'116 Server identifizieren, welche von Cyberkriminellen für die Steuerung von mit Schadsoftware (sogenannter «Malware») infizierten Geräten verwendet wird.

Der Austausch von technischen Informationen zu Cyberbedrohungen findet jedoch auch über die Grenzen hinweg statt. Dies ermöglicht eine zeitnahe Verfolgung der Cyberbedrohungslage. Zudem können technische Informationen schnell und adäquat geteilt werden, was eine rasche Reaktion auf neue Cyberbedrohungen ermöglicht. So konnte das BACS 2024 beispielsweise durch technische Analysen wichtige Erkenntnisse zu einem ausgeklügelten «Spear-Phishing-Angriff» gegen Europäische Staaten identifizieren und die betroffenen Staaten durch die etablierten Kanäle zeitnah warnen.

Zudem hat das BACS im Rahmen eines «Proof of Concepts» und einer «Public-Private-Partnerschaft» eine Analyseplattform entwickelt, welche es erlaubt, Informationen zu systemischen Cyberrisiken auszutauschen und zu analysieren. Dabei stellen vier verschiedene Informationslieferanten aus der Wirtschaft, unterschiedliche Informationen über Cybervorfälle auf organisatorischer, personeller und technischer Ebene zur Verfügung, die durch das BACS analysiert werden. Künftig erstellt das BACS anhand dieser Informationen Produkte, die zur Verbesserung der Cyberresilienz in der Schweiz beitragen werden.

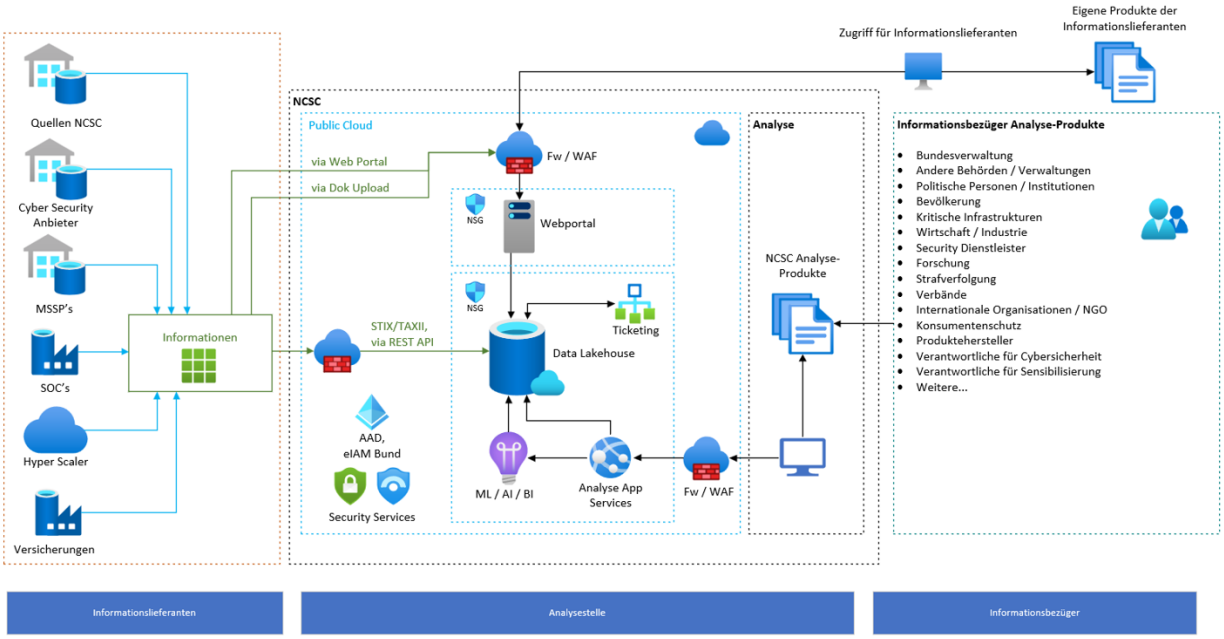
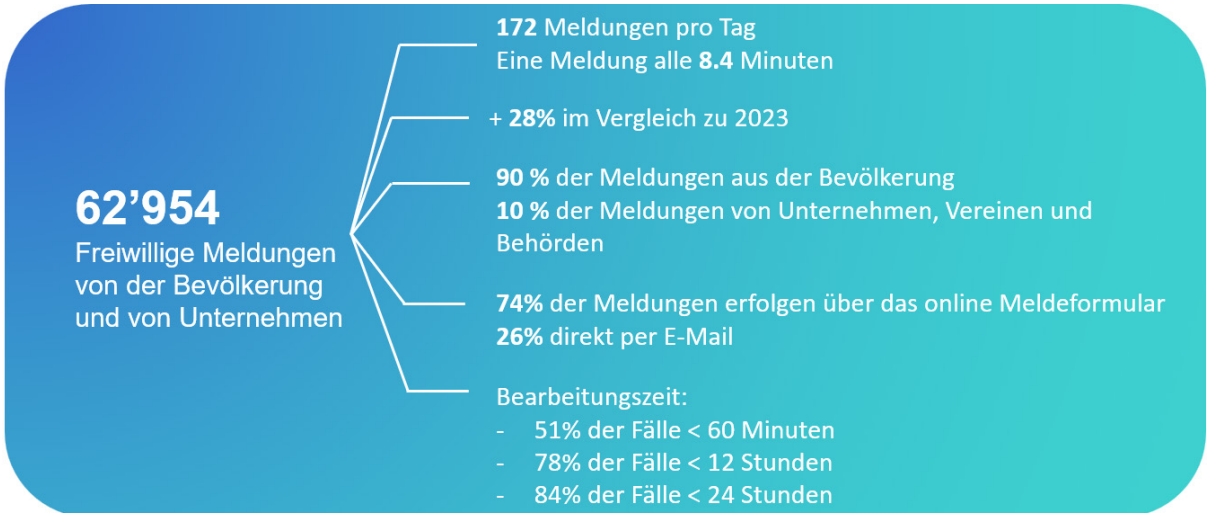


Abbildung 7: Logische Architektur Cyber Analysis, Research & Collaboration (CyARC)

Anlaufstelle für Cybervorfälle

Zusätzlich zum Austausch über Cyberbedrohungen mit kritischen Infrastrukturen betreibt das BACS eine Anlaufstelle für Cybervorfälle, die sich an die Bevölkerung und an Kleine und Mittlere Unternehmen richtet. Dank dieser freiwilligen Meldungen erkennt das BACS mögliche Trends zu Gefahren im Internet und kann entsprechende Warnungen veröffentlichen. Auf seiner Website stellt das BACS eine Statistik der gemeldeten Cybervorfälle zur Verfügung und fasst in seinem Wochenrückblick jeweils die interessantesten Fälle zusammen.



Bei den am häufigsten von Unternehmen gemeldeten Betrugsdelikten ist ein starker Anstieg beim Phänomen CEO-Betrug zu verzeichnen, mit einem gesamten Eingang von 719 Meldungen. Leicht rückläufig waren im Jahr 2024 die Meldungen zu Ransomware-Vorfällen. Wurden im Vorjahr noch 109 Vorfälle gemeldet, waren es im aktuellen Berichtsjahr 92 Meldungen.

Das Meldeformular wurde im April 2024 überarbeitet, um einerseits den stetig steigenden Meldeeingang mit gleichbleibenden Ressourcen bewältigen zu können, anderseits um den Meldenden einen besseren Service bieten zu können.

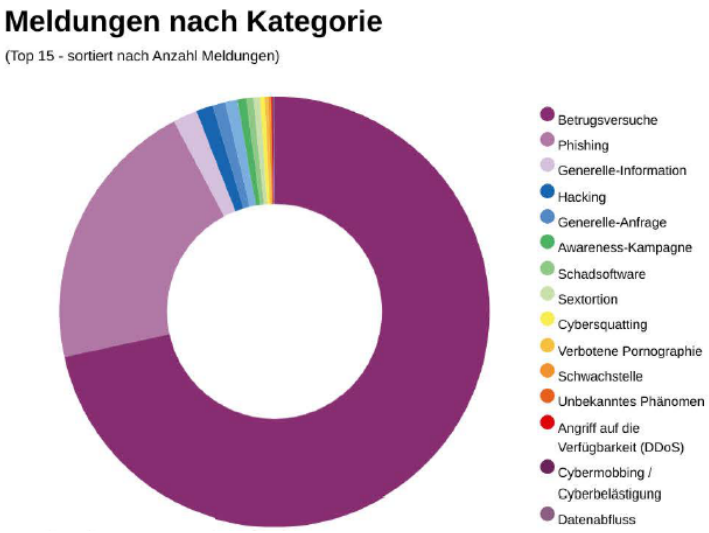


Abbildung 8: Freiwillige Meldungen nach Kategorie

3 Schäden aus Cybervorfällen reduzieren

Das BACS analysierte nicht nur Bedrohungen, sondern unterstützte auch Betreiberinnen kritischer Infrastrukturen, den Behörden und den Wirtschaftsstandort Schweiz bei der Bewältigung von Cybervorfällen. Bei Cybervorfällen im Bund übernahm das BACS die operative Führung. Um bei Cybervorfällen bestmöglich zu unterstützen betrieb das BACS eine Pikettorganisation, sodass die technischen Fachleute rund um die Uhr (24/7) telefonisch erreichbar waren. Die Unterstützung des BACS half dabei, die Schäden einzudämmen und die mögliche Weiterentwicklung der Vorfälle zu verhindern. Weitere Arbeiten, die nach dem Angriff anfielen, wie etwa die Neuinstallation von Computersystemen, mussten die betroffenen Organisationen ohne Hilfe des Bundes bewältigen. Auf diese Weise wurde die Subsidiarität gewahrt.

2024 standen in Bezug auf die Vorfallbewältigung die Einsätze gegenüber Cyberbedrohungen bei speziell exponierten Anlässen im Fokus. Es fanden gleich mehrere solche Anlässe statt. So zum Beispiel das Jahrestreffen des World Economic Forums (WEF) im Januar 2024 oder die hochrangige Konferenz zum Frieden in der Ukraine vom 15. und 16. Juni 2024. Bei der Durchführung dieser Veranstaltungen kam es zu mehreren Cyberangriffen, die jedoch dank der guten Vorbereitung rasch bewältigt werden konnten. Neben der Gesamtkoordination der Gegenmassnahmen war das BACS auch für die Erstellung der Risikoanalyse, das Prüfen der wichtigsten Infrastrukturen auf Schwachstellen (sog. «Attack Surface Management»), die Sensibilisierung aller Involvierten, dem Erstellen von Threat Intelligence und der Abwehr – in enger Zusammenarbeit mit allen Partnern - zuständig. An dieser Stelle sei hervorgehoben, wie gut die Zusammenarbeit funktionierte und dies solche Anlässe zeigen. Aus dem Ausland gab es mehrere Anfragen an die Schweiz mit dem Wunsch aufzuzeigen, wie man in kurzer Zeit solche Anlässe adäquat schützt.

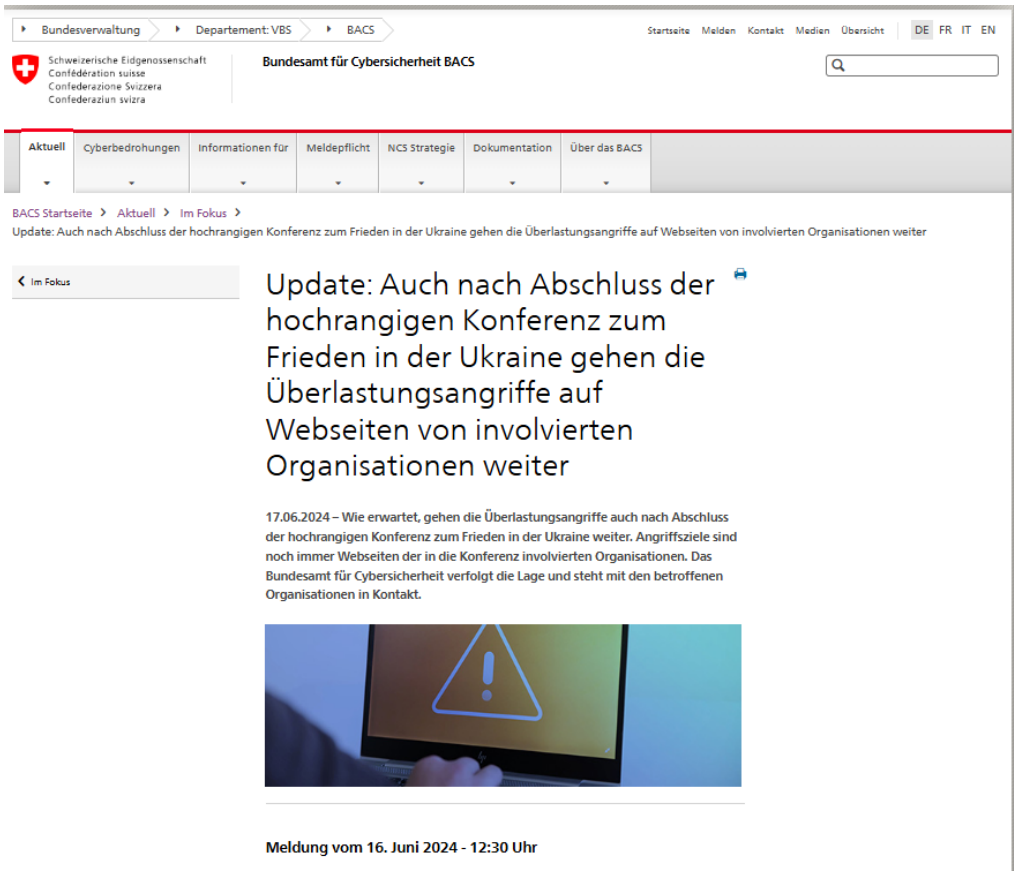


Abbildung 9: Lageupdate während der Konferenz zum Frieden in der Ukraine

4 Sicherheit von digitalen Produkten und Dienstleistungen erhöhen

Schwachstellen in technischen Geräten sowie Hard- und Software gehören noch immer zu den häufigsten Einfallstoren bei Cybervorfällen. Um hier die Wirtschaft und die Bevölkerung zu unterstützen hat das BACS zwei Schwerpunkte gelegt. Zum einen ist das BACS als «CVE Numbering Authority» die offizielle Stelle in der Schweiz, wo Forschende entdeckte Schwachstellen in Produkten melden können. Hier nimmt das BACS eine vermittelnde Rolle zwischen den Meldenden und den Produktherstellern ein, damit die Schwachstellen möglichst rasch behoben werden können und vergibt eine eindeutige Nummer, welche die Schwachstelle weltweit eindeutig identifizierbar macht. Zum andern führt das BACS das Bug-Bounty-Programm der Bundesverwaltung, um die Cybersicherheit der IT-Infrastruktur zu stärken. Ausserdem stärkte das BACS die Zusammenarbeit mit dem Nationalen Testinstitut für Cybersicherheit (NTC), einer Initiative des Kantons Zug. Das NTC überprüft IT-Produkte auf Sicherheitslücken, sofern dies nicht durch eine andere Organisation vorgenommen wird.

Bug Bounty

Durch die Durchführung von Bug-Bounty-Programmen in der Bundesverwaltung, wird die Cybersicherheit der IT-Infrastruktur erhöht und Cyberrisiken effektiv und kosteneffizient gesenkt. 2024 hat das BACS von ethischen Hackern insgesamt 371 Meldungen zu Schwachstellen erhalten. Davon wurden 239 nach erfolgter technischer Analyse als gültig eingestuft und in Summe CHF 250’900 an Prämien (Bounties) ausbezahlt. Betroffen von den Sicherheitslücken waren sämtliche Departemente sowie die Bundeskanzlei. 12 Prozent der validen Sicherheitslücken, total 45 Meldungen, wurden als «critical», also als hochgradig kritische Schwachstellen, klassifiziert und innerhalb der Bundesverwaltung folglich mit höchster Priorität behandelt und ohne unnötige Verzögerung behoben werden. 51 weitere Schwachstellenmeldungen reihten sich in die Kategorie «high» ein. Sicherheitslücken, welche in diese Bewertungskategorie fallen, stellen für die Bundesverwaltung ein erhebliches Risiko dar und bedürfen analog den kritischen Fällen ebenfalls grosser Aufmerksamkeit, da das Schadenspotenzial im Falle einer Ausnutzung gleichermassen erheblich ist. Der Behebungsprozess muss daher auch für diese Fälle so rasch als möglich initiiert werden, um die Angriffsfläche für Cyberkriminelle zu reduzieren. Weitere 102 Sicherheitslücken wurden als «medium» eingestuft. Die restlichen 41 Meldungseingänge verteilten sich schliesslich auf die wenig kritische Kategorie «low». Das Bug-Bounty-Programm musste im September 2024 pausiert werden, da das zur Verfügung stehende Budget aufgebraucht war. Die Finanzierung der Prämien erfolgte mehrheitlich durch den Rückfluss zentraler Digitalisierungsmittel innerhalb der Bundesverwaltung.

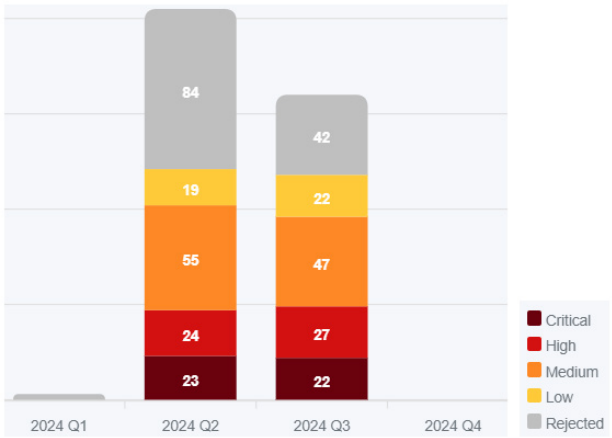


Abbildung 10: Anzahl Meldungen zu Schwachstellen

Ausblick und Ziele für das kommende Jahr

Für das Jahr 2025 stehen dem BACS sowohl bedeutende Chancen als auch Herausforderungen im Bereich der Cybersicherheit gegenüber. Die Anforderungen in diesem dynamisch wachsenden Sektor nehmen kontinuierlich zu, weshalb es entscheidend ist, die verfügbaren Ressourcen gezielt einzusetzen und klare Prioritäten zu setzen. Mit dem geplanten Budget von 16.1 Millionen CHF und den zweckgebundenen Reserven, die eine Übertragung finanzieller Mittel ins nächste Jahr ermöglichen, können die laufenden Projekte im Jahr 2025 fortgeführt werden. In der vorliegenden Finanzplanung sind keine signifikanten Investitionen ins BACS geplant. Es ist jedoch davon auszugehen, dass Cyberbedrohungen weiter zunehmen, insbesondere auch mit Blick auf das geopolitisch herausfordernde Umfeld. Das BACS diese Herausforderung mit einer dualen Taktik angehen:

1. Fokus: Das BACS priorisiert Aufgaben nach Kosten / Nutzen hinsichtlich der kurz- und mittelfristigen Cybersicherheit der Schweiz.

2. Plattform: Das BACS fungiert primär als Drehscheibe und Multiplikator für Beiträge von Partnern. Wo immer möglich agiert das BACS als befähigende und koordinierende Stelle und schliesst Fähigkeitslücken wo vorhanden.

Klare Prioritäten in einem wachsenden Umfeld

Aufgrund der dualen Taktik liegt der Fokus des BACS im Jahr 2025 auf drei zentralen Handlungsfeldern:

1. Weiterentwicklung der digitalen Plattform: Die digitale Plattform bildet das Rückgrat der Cybersicherheitsstrategie des Bundesamtes. Ihre kontinuierliche Verbesserung ist entscheidend, um den sich verändernden Bedrohungen effektiv begegnen zu können.

2. Umsetzung der NCS: Die konsequente Verwirklichung der festgelegten Strategie bleibt eine Kernaufgabe, um die langfristige Sicherheit der Schweiz im Cyberraum zu gewährleisten. Der erste Umsetzungsbericht der NCS wird veröffentlicht. Dieser wird die bisherigen Fortschritte evaluieren.

3. Zuverlässige Ausführung der operativen Geschäfte: Die Qualität und Verlässlichkeit der operativen Tätigkeiten sind für das BACS von zentraler Bedeutung. Der Fokus wird auf operative und taktische Tätigkeiten mit kurz und mittelfristigen Auswirkungen gelegt, während strategische, langfristige Vorhaben vorerst lediglich punktuell bewirtschaftet werden.

Effizienzsteigerung durch interne Optimierung

Neben der Fokussierung auf die genannten Kernbereiche wird das BACS auch die internen Strukturen weiter optimieren. Ziel ist es durch Automatisierung Prozesse effizienter zu gestalten, die Zusammenarbeit mit Partnern weiter zu vereinfachen und den Fokus noch mehr auf Koordination legen. Dies wird es erlauben, die Gesamtleistung des BACS so zu steigern, dass zumindest mittelfristig die steigenden Cyberrisiken in gleichbleibende Qualität adressiert werden können.

Langfristige Perspektive und Partnerschaften

Das BACS wird weiterhin alles daransetzen, mit den vorhandenen Ressourcen bestmögliche Ergebnisse zu erzielen und die Schweiz auch im Jahr 2025 sicherer zu machen. Es kann dabei auf eine breite Unterstützung von Partnerbehörden und aus der Privatwirtschaft zählen. Dabei bleibt der Grundauftrag unverändert: Die Rolle als Koordinator auszufüllen und qualitativ hochwertige Leistungen für Wirtschaft, Gesellschaft, Behörden und Wissenschaft zu erbringen.

Das BACS dankt allen, die sich für die Cybersicherheit einsetzen und uns helfen, unseren Auftrag zu erfüllen.

Publikationen und Referenzen

BACS-Publikationen im 2024:

- Halbjahresbericht 2023/2
- Halbjahresbericht 2024/1
- Bericht: Telefonbetrug im Cyberbereich
- Technische Kurzanalyse zum Botnetz «Gorilla»
- Technische Kurzanalyse zur Schadsoftware «Poseidon Stealer»
- Bericht zu den Datenanalysen nach dem Cyberangriff auf die Firma Xplain
- Anti-Phishing Bericht 2023
- Technologiebetrachtung: Quantencomputer und Post-Quantum-Kryptographie,
- Einschätzung zum Handlungsbedarf im Zusammenhang mit Post-Quanten-Kryptografie (PQK)
- Bericht Informatiksicherheit Bund 2023
- Empfehlungen für die Sicherheitsüberprüfung von Personen in Unternehmen
- Massnahmen zur Cyberresilienz im Kontext von Grossveranstaltungen und internationalen Konferenzen
- Erste Bilanz des BACS zu den Arbeiten des Cyberlageverbunds in Zusammenhang mit der hochrangigen Konferenz zum Frieden in der Ukraine

Wissenschaftliche Artikel

- A. Grünert, J. B. Michael, R. Oppliger and R. Rytz, "Why Probabilities Cannot Be Used in Cyber Risk Management," in *Computer*, vol. 57, no. 10, pp. 86-89, Oct. 2024
- R. Oppliger and A. Grünert, "How to Measure Cybersecurity and Why Heuristics Matter," in Computer, vol. 57, no. 2, pp. 111-115, Feb. 2024