16. Februar 2026 | Bundesamt für Cybersicherheit BACS

Jahresbericht 2025

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

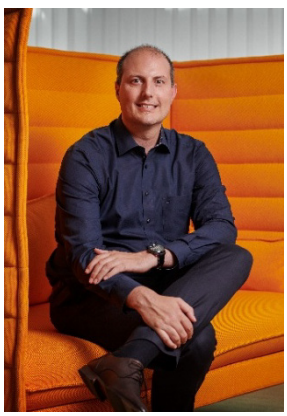
Geschätzte Leserinnen und Leser

Das Jahr 2025 stand für das Bundesamt für Cybersicherheit (BACS) im Zeichen der Konsolidierung und der Vertiefung unseres Auftrags. Nach der Aufbauphase konnten wir zentrale Prozesse weiter festigen und die Zusammenarbeit innerhalb des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) sowie mit unseren Partnerorganisationen gezielt ausbauen. Die geschaffenen Strukturen haben sich bewährt und ermöglichen eine zuverlässige und kohärente Aufgabenerfüllung.

Ein wesentlicher Meilenstein war die Einführung der Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen. Neun Monate nach deren Inkrafttreten zeigt sich, dass die Umsetzung funktioniert: Cyberangriffe werden fristgerecht gemeldet, die vorgesehenen Instrumente werden genutzt, und die Zusammenarbeit mit den Betreiberinnen kritischer Infrastrukturen ist etabliert. Besonders entscheidend für eine reibungslose Einführung waren die proaktive Kommunikation über Branchenverbände sowie ergänzende Erklärvideos. Auf dieser Grundlage verfügt die Schweiz nun über stabile Melde- und Unterstützungsprozesse in diesem sicherheitsrelevanten Bereich.

Die rund 65'000 freiwilligen Meldungen belegen, dass Cyberrisiken im Bewusstsein angekommen sind und Menschen sich aktiv schützen, informieren und Vorfälle melden. Der Meldeeingang trägt wesentlich dazu bei, ein aktuelles Lagebild zu erstellen und die Bedrohungslage besser einzuschätzen. Auf dieser Grundlage kann das BACS seinen Auftrag zur Sensibilisierung der Bevölkerung gezielter wahrnehmen und Informations- und Präventionsmassnahmen besser auf aktuelle Bedürfnisse und Gefahren ausrichten. Ein weiterer Schwerpunkt lag auf dem Ausbau der nationalen digitalen Plattform den Cyber Security Hub. Neben dem Meldeformular für kritische Infrastrukturen wurden verbesserte Funktionen und neue Austauschformate eingeführt. Diese stärken die sektorübergreifende Zusammenarbeit und erleichtern den Zugang zu relevanten Fachinformationen. Auch die Controlling-Instrumente der Nationalen Cyberstrategie (NCS) wurden weiter ausgebaut: Sie umfassen über 90 Projekte mit Partnern aus Behörden, Wirtschaft und Gesellschaft. Zusätzlich wurde durch die Etablierung weiterer sektorspezifischer Cyber Security Centers (CSC), wie beispielsweise das «Healthcare-CSC», die gemeinsame Umsetzung der NCS gestärkt.

Diese Leistungen wurden in einem Jahr erbracht, das von finanziellen Unsicherheiten geprägt war. Umso bedeutender ist der parlamentarische Entscheid, das Budget des BACS für 2026 um 10 und ab 2027 um weitere 5 Mio. Franken zu erhöhen. Den Beschluss des Parlaments verstehen wir als ein starkes Zeichen des Vertrauens in unsere Arbeit. Er ermöglicht es uns, bestehende Unterfinanzierungen auszugleichen, notwendige Investitionen zu tätigen und neue gesetzliche Aufgaben - insbesondere im Zusammenhang mit der Meldepflicht - nachhaltig umzusetzen. Gleichzeitig ist dieser Entscheid mit klaren Erwartungen verbunden: an Wirkung, Verlässlichkeit und einen verantwortungsvollen Umgang mit den anvertrauten Mitteln. Wir werden unseren strategischen Kurs konsequent weiterverfolgen. Die langfristigen Ziele bleiben unverändert, können nun jedoch mit höherer Verlässlichkeit und in angemessenem Tempo erreicht werden.



Ich danke allen Mitarbeitenden sowie unseren Partnerorganisationen für ihr Engagement und die konstruktive Zusammenarbeit. Gemeinsam leisten wir einen wichtigen Beitrag zur Cybersicherheit der Schweiz.

Florian Schütz
Direktor des Bundesamtes für Cybersicherheit

Wichtigste Kennzahlen 2025

18.4 Mio. CHF
Ausgaben

+ 38%

71
Mitarbeitende
(davon 4 Hochschulpraktikantinnen und praktikanten)

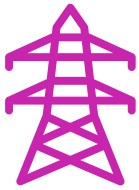
+ 5%

64’733
Freiwillige Meldungen zu Cybervorfällen

+ 3%

501
Medienkontakte

- 19%



222
Meldungen zu Cyberangriffen im Rahmen der Meldepflicht

Neu eingeführt

2’347’618
Meldungen zu mit Schadsoftware infizierten Geräten analysiert

+ 141%

1’600
Unternehmen auf dem Cyber Security Hub

+ 45%

400
Durchschnittliche Teilnehmende an den Online Bi-Weekly Situation Exchanges

Neu erfasst

525
Meldungen von Schwachstellen durch ethische Hacker

+ 41%

17’468
Command and Control Systeme von Angreifern identifiziert und gesperrt

+ 115%

Im Vergleich zu 2024

Stand Dezember 2025

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

Ausgaben im Jahr 2025

Im Jahr 2025 belief sich die definitive Rechnung des BACS auf 18.4 Millionen Franken. Davon entfielen 13.0 Millionen Franken auf Personalaufwand und 5.4 Millionen Franken auf Sach- und Betriebsausgaben. Von den Sach- und Betriebsausgaben wurden 3.8 Millionen Franken für Informatik aufgewendet. 1.2 Millionen Franken davon wurden für den Betrieb und 2.6 Millionen Franken für Weiterentwicklungen genutzt. Das Budget für Weiterentwicklungen wurde durch den Einsatz zweckgebundener Reserven in der Höhe von 2.5 Millionen Franken erhöht. Dadurch standen dem BACS ausreichende Mittel zur Verfügung, um die bestehenden IT-Systeme im Hinblick auf die per 1. April 2025 eingeführte Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen auszubauen.

Für Weiterentwicklungen am Cyber Security Hub (CSH) wurden 1.8 Millionen Franken eingesetzt. Weitere 0.1 Millionen Franken entfielen auf die Analyseplattform für Cybervorfälle (CyARC). Für die Durchführung von Bug-Bounty-Programmen wurden 0.5 Millionen Franken verwendet, um Schwachstellen in IT-Systemen der Bundesverwaltung zu identifizieren und zu beheben. Die übrigen Mittel im Informatikbereich wurden für Dienstleistungen für kritische Infrastrukturen sowie für Cybersicherheitsprüfungen in den Bereichen Peripheriegeräte, Photovoltaik und Open Source eingesetzt.

Von den übrigen Sach- und Betriebsausgaben in der Höhe von 1.6 Millionen Franken entfielen 0.4 Millionen Franken auf externe Dienstleistungen. Davon wurden 0.2 Millionen Franken für die Weiterentwicklung der GEVER-Geschäftsprozesse und 0.2 Millionen Franken für die Entwicklung eines Open-Source-Zielbilds eingesetzt. Die Ausgaben für Reisen und Teilnahmen an Tagungen beliefen sich auf 0.3 Millionen Franken. Die restlichen Mittel wurden für Mietkosten, Büromaterial, Büromatik und Drucksachen verwendet.

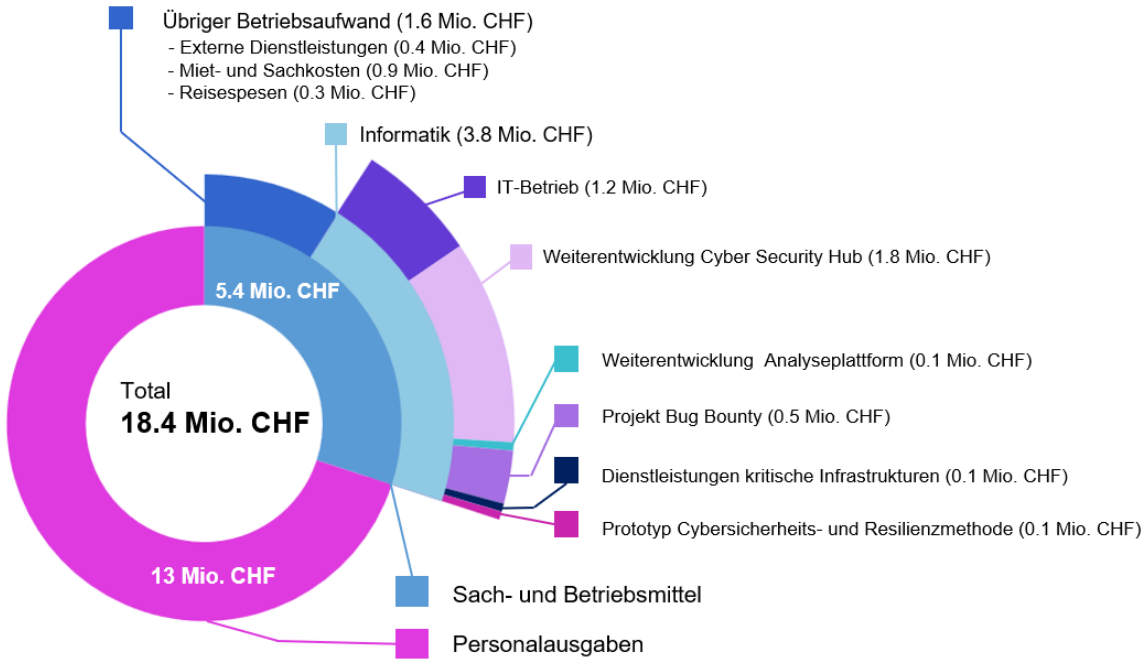


Abbildung 1: Finanzielle Mittel BACS - Rechnung 2025

Einsatz der finanziellen Mittel nach Aufgaben

Der grösste Teil der Sach- und Betriebsmittel wurde für den Kernauftrag des BACS eingesetzt. Die Mittel flossen in die Prävention und in die Behandlung und Nachbearbeitung von Cybervorfällen. Der administrative Aufwand wurde möglichst klein gehalten, er betrug im Jahr 2025 9 Prozent.

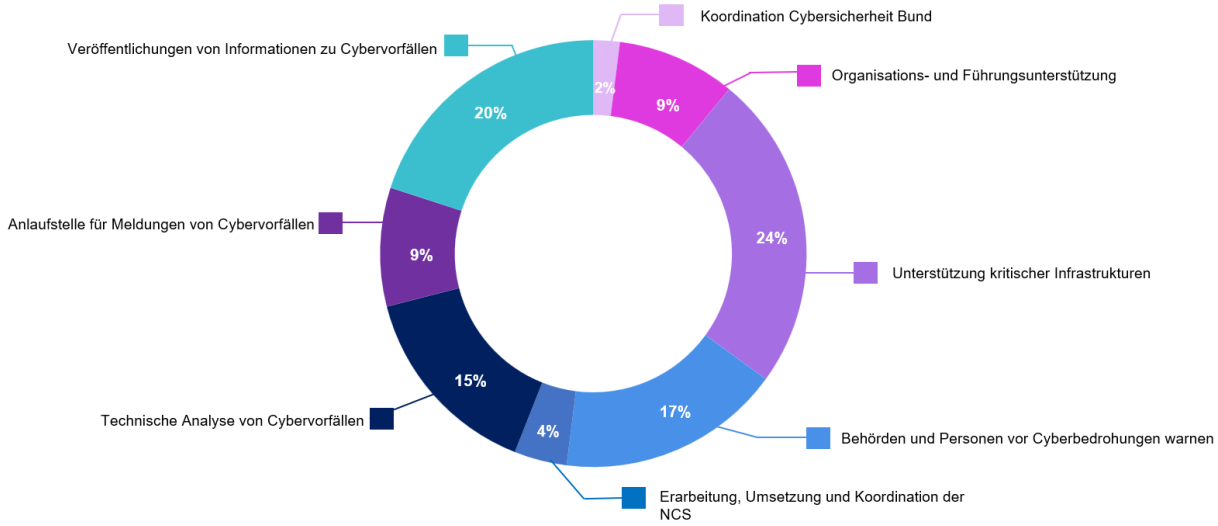


Abbildung 2: Verteilung der finanziellen Mittel nach Aufgaben

Personalstruktur

Die Personalausgaben beliefen sich auf insgesamt 13 Mio. CHF. Diese entfielen auf 71 Stellen, darunter vier Hochschulpraktikantinnen und -praktikanten.

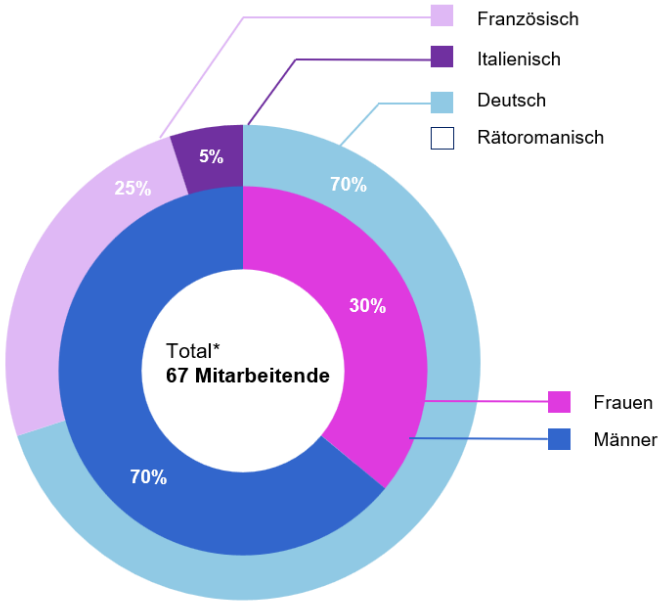


Abbildung 3: Mitarbeitende BACS Stand Dezember 2025
*ohne Hochschulpraktikantinnen und Praktikanten

Tätigkeiten des BACS anhand der vier strategischen Säulen

1 Cyberbedrohungen verständlich machen

Ein zentrales Ziel des BACS ist es, seine Zielgruppen zu befähigen, sich effektiv vor Cyberbedrohungen zu schützen. Auch 2025 hat das BACS deshalb einen starken Fokus darauf gelegt, Informationen zu Cyberbedrohungen und möglichen Schutzmassnahmen zielgruppengerecht aufzubereiten und zu verbreiten.

Für die öffentliche Kommunikation nutzt das BACS insbesondere seine Website, auf der laufend aktuelle Warnmeldungen, Wochenrückblicke, Medieninformationen sowie technische Kurzanalysen veröffentlicht werden. Für die Öffentlichkeit wurden 2025 verschiedene Sensibilisierungskampagnen durchgeführt. Die etablierte Kampagne «S-U-P-E-R» wurde fortgeführt. Durch die erstmalige Präsenz an der Publikumsmesse BEA 2025 konnte das Thema Cybersicherheit zudem einem noch grösseren Publikum nähergebracht werden. Im Rahmen des Cyber Security Month (CSM) legte die diesjährige Schweizer Kampagne ihren Schwerpunkt auf die Themen «Online-Daten» und «Phishing». In Zusammenarbeit mit der Partnerorganisation Netpathie sowie dem Kampagnenbotschafter Ivano Somaini entstanden vielfältige Inhalte wie Videos, Quizformate, Sticker sowie ein Online-«Brown Bag Lunch» zu den Risiken von «Oversharing» und dem bewussten Umgang mit digitalen Daten.

Zur Unterstützung von Unternehmen und Gemeinden engagierte sich das BACS zudem in zahlreichen Informations- und Weiterbildungsveranstaltungen. Gemeinsam mit Partnern wie ITSec4KMU, dem Schweizerischen Versicherungsverband (SVV) und branchenrelevanten Verbänden wurden praxisnahe Fachreferate, Hacking-Demos und Workshops durchgeführt, welche die eigenständige Stärkung der Cybersicherheit sowie die Bedeutung sicherer Lieferketten betonten.

Stärkung der präventiven Cybersicherheit

Mit der Entwicklung der Cybersicherheits- und Resilienzmethode (CSRM) hat das BACS im Jahr 2025 einen wichtigen Schritt zur Stärkung der präventiven Cybersicherheit umgesetzt. Die Methode bietet einen praxisnahen Ansatz zur Behandlung von Cyberrisiken, ausgerichtet auf zentrale Geschäfts- und Produktionsprozesse. Sie basiert auf einem erweiterten Grundschutz, orientiert sich an internationalen Standards und verzichtet auf eine Risikoquantifizierung. Das vom BACS entwickelte Cyberresilienz-Assessment umfasst einen strukturierten Prüfkatalog, der Organisationen eine systematische Selbstbeurteilung ermöglicht und als Grundlage für einen Vergleich mit anderen Organisationen dienen wird.

Das Cyberresilienz-Assessment wird im Rahmen eines Pilotversuchs im Kanton Aargau mit Gemeinden und Unternehmen unter Realbedingungen getestet, um Methode und Tool gemeinsam weiterzuentwickeln.

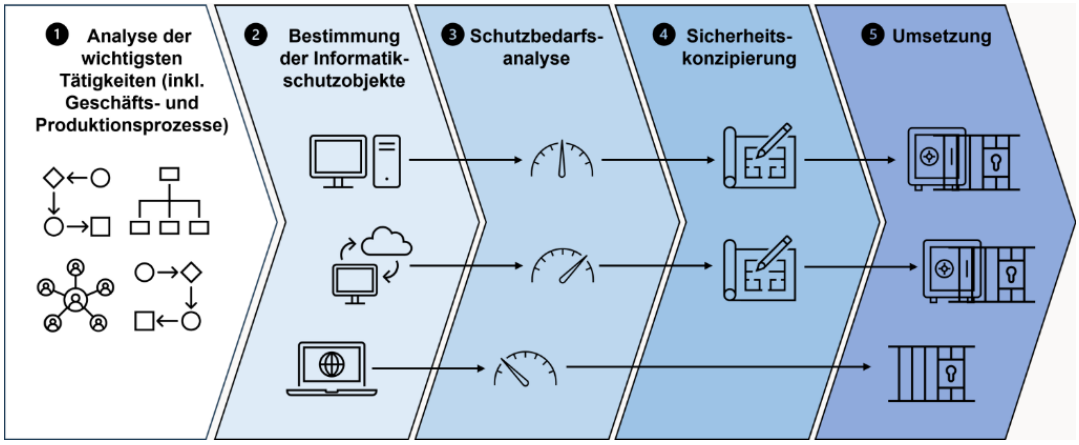


Abbildung 4: Cybersicherheits – und Resilienzmethode Methode BACS

Projekt Cyber-Notfallkonzept für die Gemeinden

Cyber-Vorfälle in der Vergangenheit sowie die Gemeindeumfrage 2025 von «Myni Gmeind» haben gezeigt, dass sich viele Gemeinden noch besser auf Cybervorfälle vorbereiten können. Damit Gemeinden und Organisationen in der Schweiz ihre Cyberresilienz verbessern können, hat das BACS zusammen mit seinem Partnernetzwerk ein Notfallkonzept-Modell, praxisnahe Hilfsmittel sowie ein Erklärvideo erstellt und auf der Webseite des BACS publiziert. Die Inhalte wurden in zwei Online Brown Bag Lunches vertieft.
Notfallkonzepte sind ein wesentlicher Bestandteil eines wirksamen Risikomanagements. Sie dienen dazu potenzielle Probleme und ihre Auswirkungen nicht erst im Nachhinein zu analysieren, sondern ihnen proaktiv zu begegnen. Durch die frühzeitige Auseinandersetzung mit potenziellen Risiken ermöglichen Notfallkonzepte, präventive Massnahmen zu identifizieren und umzusetzen. Sie beinhalten die Krisenorganisation, ein Konzept für die Krisenkommunikation sowie zentrale Notfallkontakte und konkrete Massnahmen. Diese Elemente bilden die Grundlage für eine koordinierte und angemessene Reaktion in zeitkritischen Situationen.

Meilensteine und Erfolge:
Entwicklung eines strukturierten Prozesses:
Der entwickelte Prozess (siehe Infografik unten) ermöglicht einen pragmatischen Ansatz zur Vorbereitung, Bewältigung und Nachbearbeitung möglicher Cybervorfälle.

Pragmatische Umsetzung:
Dank des praxisnahen und pragmatischen Ansatzes konnten das Konzept und die dazugehörigen Hilfsmittel schnell verbreitet werden.

Wissenstransfer für KMU:
Die Erkenntnisse des Projekts kommen nicht nur den Gemeinden zugute. Ab 2026 werden sie auch für KMU angepasst und zur Verfügung gestellt.

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

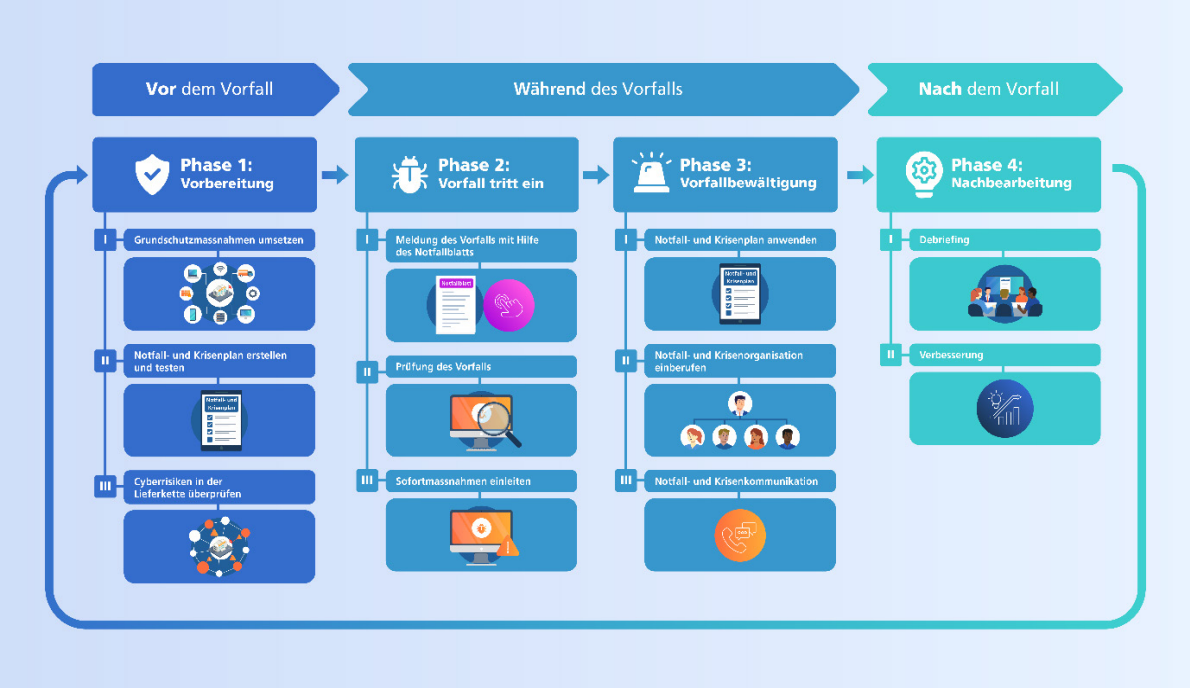


Abbildung 5: Übersicht Notfallkonzept BACS

Umsetzung der Nationalen Cyberstrategie (NCS)

Im Jahr 2025 stand die operative Umsetzung der Nationalen Cyberstrategie (NCS) im Vordergrund. Aufbauend auf der im Vorjahr erfolgten Einrichtung des Steuerungsausschusses wurden die Governance-Strukturen weiter konsolidiert und gezielt für die Umsetzung der NCS ausgebaut, um die Koordination zwischen den zahlreichen Beteiligten zu stärken. Dafür wurden regelmässige Austauschformate geschaffen, die den Dialog und die Zusammenarbeit fördern. Ein zentrales Resultat dieser Arbeiten ist die Konzeption eines NCS-Umsetzungsforums, das ab 2026 eingeführt wird. Dieses Forum soll als Plattform dienen, um Fortschritte in der Umsetzung der NCS zu überprüfen, Impulse für neue Massnahmen zu setzen und die strategische Weiterentwicklung der NCS zu unterstützen. Ein wichtiger Schritt auf diesem Weg war der Kick-off-Workshop im Dezember 2025, an dem rund 60 Umsetzungspartner teilgenommen haben. Ziel war die Ausgestaltung der zukünftigen Forenformate. Die Diskussionen unterstrichen die hohe Relevanz solcher Plattformen für eine erfolgreiche Umsetzung der NCS. Die gewonnenen Erkenntnisse fliessen nun in die Vorbereitung der ab 2026 geplanten regelmässigen Umsetzungsforen ein.

Durch die Weiterentwicklung des NCS-Portfoliomanagements umfasst das Umsetzungsportfolio mittlerweile über 90 Vorhaben, die von über 70 Umsetzungspartnern getragen werden und sich über alle fünf strategischen Ziele verteilen. Eine Übersicht der aktiven Vorhaben ist auf der BACS Webseite verfügbar.[1] Zudem wurde ein klar strukturierter Prozess zur Aufnahme neuer Vorhaben[2] erarbeitet und veröffentlicht, sodass interessierte Akteure die Kriterien für eine Portfolioaufnahme transparent nachvollziehen können.

NCSK 2025

Am 25. September 2025 organisierten der Sicherheitsverbund Schweiz und das BACS die Nationale Cybersicherheitskonferenz (NCSK) in Bern unter dem Leitthema «Cyberresilienz: Regulierung oder Selbstverantwortung?». Rund 250 Teilnehmende aus Politik, Verwaltung, Wirtschaft und Wissenschaft diskutierten die Balance zwischen gesetzlichen Vorgaben und eigenverantwortlichen Massnahmen zur Stärkung der digitalen Widerstandskraft. Die Veranstaltung bot eine Plattform für den Austausch von Best Practices und Impulsen zur Weiterentwicklung der NCS. Beiträge aus Politik, Forschung und Praxis sowie Breakout-Sessions zu Regulierung und Eigenverantwortung unterstrichen die gemeinsame Verantwortung aller Akteure

[1] Umsetzung NCS
[2] Neue NCS-Vorhaben

2 Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen

Informationsaustausch über den Cyber Security Hub (CSH)

Der Cyber Security Hub (CSH) ist die zentrale Plattform für den operativen Informationsaustausch zwischen dem BACS und den Betreiberinnen kritischer Infrastrukturen. Im Jahr 2025 wurde der technische Ausbau des CSH weitergeführt und konsequent auf die Meldepflicht gemäss Informationssicherheitsgesetz (ISG) ausgerichtet. Seit April 2025 steht im CSH ein mehrsprachiges Meldeverfahren für Cybervorfälle zur Verfügung, einschliesslich der Erstmeldung sowie der Abschlussmeldung. Dieses wurde in die bestehenden Prozesse des BACS integriert. Im August wurde zudem die Funktion «Share with NCSC» aufgeschaltet. Sie ermöglicht es, dem BACS zusätzliche Informationen, die für die Beurteilung der Cyberbedrohungslage oder für Massnahmen zum Schutz kritischer Infrastrukturen relevant sind, über einen sicheren Kanal zu übermitteln. Bis Ende November 2025 gingen über diesen Kanal rund 40 Meldungen ein.

Das BACS setzte auch 2025 die etablierten Formate fort. Dazu gehörte insbesondere der wöchentliche Cybersicherheitsbericht, der auf zwei Seiten die wichtigsten Ereignisse und Entwicklungen zusammenfasst und über den CSH mehr als 6’000 Nutzerinnen und Nutzer in rund 1’600 Organisationen informiert. Ergänzend dazu führte das BACS die regelmässigen Online-Austausche zur Cybersicherheit weiter. Es fanden 39 Austausche auf Deutsch und Französisch statt, mit durchschnittlich knapp 400 Teilnehmenden. Diese bieten der CSH-Community eine zentrale Plattform für den kontinuierlichen Dialog, den Austausch zu aktuellen Entwicklungen und Vorfällen sowie die Vernetzung der beteiligten Organisationen.

Cyber Threat Intelligence

Im Bereich der Cyber Threat Intelligence konnte das BACS wichtige Fortschritte bei der Aufdeckung und Eindämmung komplexer Cyberbedrohungen erzielen. Hervorzuheben ist insbesondere die Identifikation und Analyse eines gross angelegten sogenannten ORB-Netzwerks («Operational Relay Box»). Dabei handelt es sich um verdeckte Infrastrukturen, die von staatlich unterstützten Akteuren genutzt werden, um Cyberangriffe zu verschleiern. Das BACS konnte ein Netzwerk mit über 2’000 kompromittierten Systemen identifizieren und die gewonnenen Erkenntnisse im Rahmen der internationalen Zusammenarbeit weitergeben. Dadurch wurde der missbräuchliche Einsatz dieser Systeme wirksam eingeschränkt.

Parallel dazu beobachtete das BACS eine zunehmende Bedrohung für die Schweiz durch die als «Trader Traitor» bekannte Gruppe, hinter der mutmasslich nordkoreanische Gruppierungen stecken. Ihre Aktivitäten richten sich insbesondere gegen Unternehmen aus dem Finanz- und Kryptobereich. Die Angreifer nutzen dabei insbesondere Methoden des «Social Engineerings», indem sie gezielt Fachpersonen über vermeintliche Stellenangebote kontaktieren und diese zur Ausführung schädlicher Software verleiten.

Das BACS verfolgt diese Bedrohungen kontinuierlich und hat im Berichtsjahr mehrere technische Sensibilisierungsmassnahmen für Partnerorganisationen durchgeführt. Durch die gezielte Weitergabe von Warnhinweisen und technischen Indikatoren leistete das BACS einen wichtigen Beitrag zur Prävention von Infektionen und zur Stärkung der Abwehrfähigkeit betroffener Organisationen.

Sektorspezifische Initiativen

Auch im Jahr 2025 wurde das Programm der Cyber Security Centres (CSC) weiterentwickelt. Das Konzept dient dazu, branchen- oder sektorspezifisches Wissen zu bündeln und mit dem BACS zu verknüpfen. Ein Fokus lag auf der vertieften Zusammenarbeit zwischen dem BACS und dem Swiss Financial Sector CSC (FS-CSC). Mit einer neuen Kooperationsvereinbarung bündeln beide Organisationen ihre Kräfte, um den wachsenden Cyberrisiken im Finanzsektor gezielt zu begegnen. Kern der Partnerschaft ist ein strukturierter Informationsaustausch: Analystinnen und Analysten des FS-CSC erhalten Zugang zu relevanten Daten des BACS und erstellen darauf basierende Lagebilder und Analysen für den Finanzplatz. Diese Erkenntnisse fliessen in die Arbeit der Mitglieder sowie in den CSH ein und stärken die gesamtheitliche Lagebeurteilung. Neben dem Finanzsektor wurden mit dem Healthcare-CSC und dem Rail ISAC zwei weitere sektorspezifische Zentren etabliert. Nach Abschluss der Pilotphase wurde das Healthcare-CSC im August 2025 als Verein mit 18 Spitälern gegründet. Dies fördert den Austausch von Bedrohungsinformationen, gemeinsamen Schutzmassnahmen und Best Practices im Gesundheitswesen.

Abbildung 6: Unterschrift der neuen Kooperationsvereinbarung mit dem FS-CSC

Parallel dazu wurde mit dem Rail ISAC eine Plattform aufgebaut, welche die Schweizer Bahnbranche bei der Abwehr von Cyberangriffen unterstützt.

Ergänzend zu den CSCs förderte das BACS den sektoriellen Austausch mit Organisationen der Stromversorgung durch die Durchführung von zwei Roundtables. Diese dienten der Vermittlung der aktuellen Bedrohungslage sowie dem moderierten Austausch zwischen den Teilnehmenden zu sektorspezifischen Fragestellungen.

Anlaufstelle für Cybervorfälle

Über die Anlaufstelle erhält das BACS freiwillige Meldungen aus der Bevölkerung sowie von Unternehmen in der Schweiz. Im Jahr 2025 erhielt das BACS 64'733 Meldungen, welche es ermöglichen, Entwicklungen und neue Gefahren im Internet frühzeitig zu erkennen und entsprechende Warnungen zu veröffentlichen. Zudem wurde wöchentlich auf der Webseite des BACS über die aktuellen Gefahren dank der Informationen der freiwilligen Meldungen berichtet.

Am häufigsten wurden Betrugsversuche gemeldet. Ein weiterer klarer Trend war die Veränderung im Bereich der Phishing-Angriffe. Während weiterhin generische Phishing-E-Mails festgestellt wurden, ist ein klarer Trend hin zu zunehmend personalisierten Angriffsmethoden erkennbar. Insbesondere nahmen Betrugsversuche im Zusammenhang mit Online-Kleinanzeigen deutlich zu. Darüber hinaus haben sich auch telefonische Betrugs- und Phishing-Versuche weiter etabliert. Die Sprachbarriere, die bislang als Hürde galt, spielt dabei immer weniger eine Rolle. Eine ebenfalls interessante Erkenntnis ist der verstärkte Einsatz künstlicher Intelligenz (KI) durch kriminelle Akteure, um Betrugsmaschen realistischer und überzeugender zu gestalten. Besonders im Bereich des Online-Anlagebetrugs kommt KI zum Einsatz, beispielsweise zur Erstellung gefälschter Interviews oder professionell wirkender Werbeinhalte.

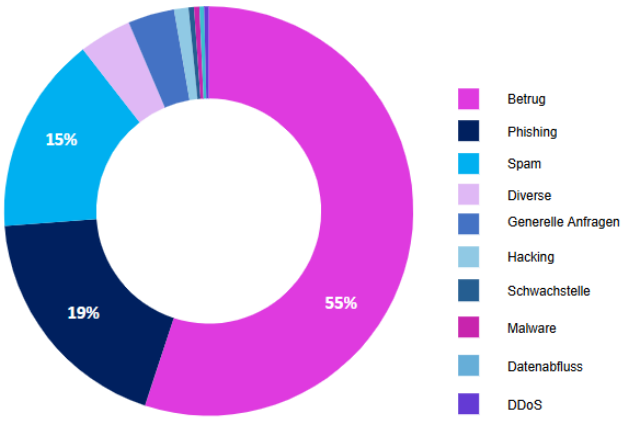
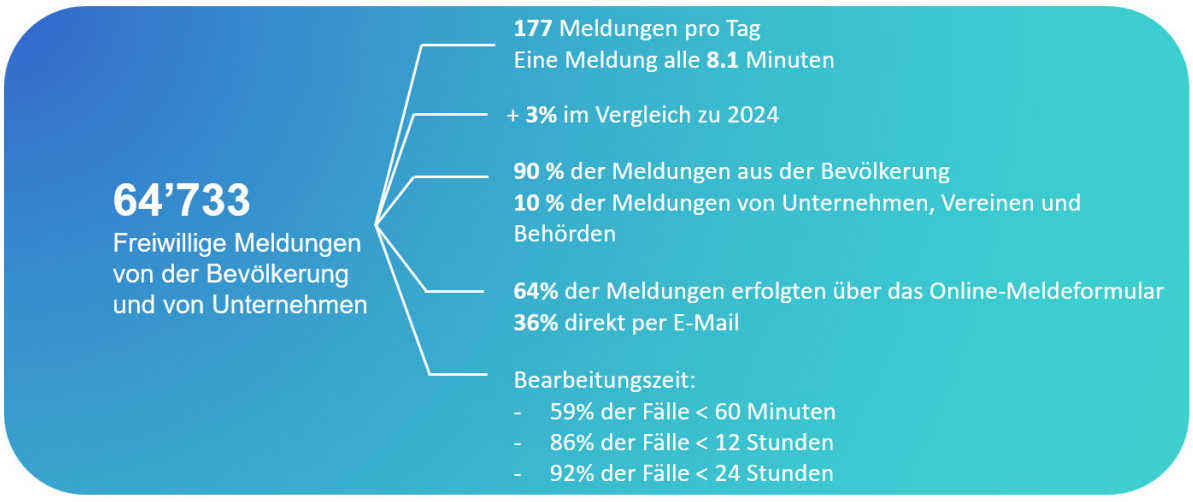


Abbildung 7: Freiwillige Meldungen nach Hauptkategorien

Im Verlauf des Jahres wurde das öffentliche Meldeformular an die veränderten Anforderungen angepasst. Die gesetzliche Meldepflicht ist nun auch im öffentlichen Meldeformular vollständig integriert. Darüber hinaus wurde die Möglichkeit verbessert, Meldende bei Bedarf auf die Webseite von Suisse ePolice zu leiten, auf der bei bestimmten Delikten Online-Strafanzeige erstattet werden kann. Auch die Kommunikation mit den meldenden Personen wurde optimiert: Die Standardantworten wurden vollständig überarbeitet und stärker an den Informationsbedürfnissen der Nutzerinnen und Nutzer ausgerichtet. Auf Ebene der internen Bearbeitung wurden die Prozesse weiter optimiert, wodurch die durchschnittliche Bearbeitungszeit pro Fall reduziert werden konnte.



Einführung der Meldepflicht

Seit dem 1. April 2025 gilt in der Schweiz die gesetzliche Meldepflicht für Cyberangriffe auf kritische Infrastrukturen. Betreiberinnen von meldepflichtigen Organisationen - beispielsweise aus der Energie- oder Trinkwasserversorgung, Transportunternehmen oder kantonale und kommunale Verwaltungen - müssen seither Cyberangriffe innerhalb von 24 Stunden nach deren Entdeckung an das BACS melden. Diese neue Verpflichtung wurde durch eine Revision des Informationssicherheitsgesetzes (ISG) eingeführt und ist in den Artikeln 73 ff. ISG verankert. Konkretisiert wird die Meldepflicht durch die neue Cybersicherheitsverordnung (CSV), die ebenfalls am 1. April 2025 in Kraft getreten ist. Die meldepflichtigen Organisationen werden in Artikel 74b ISG festgelegt, während die Ausnahmen in Artikel 16 CSV geregelt sind.

Um den Meldeprozess möglichst einfach zu gestalten, stellt das BACS den meldepflichtigen Organisationen den Cyber Security Hub (CSH) (vgl. Informationsaustausch auf S.11) als zentrale Meldeplattform sowie begleitende Erklärvideos und Merkblätter zur Verfügung. Bis Ende 2025 gingen 222 Meldungen ein. Die eingegangenen Meldungen ermöglichen dem BACS eine verbesserte Analyse der Cyberbedrohungslage in der Schweiz. Dadurch können Angriffsmuster auf kritische Infrastrukturen frühzeitig erkannt und analysiert werden, wodurch potenziell betroffene Organisationen rechtzeitig gewarnt werden können, um geeignete Präventions- und Abwehrmassnahmen einzuleiten. Weil das Meldeformular auf dem CSH bereitgestellt wird, besteht ein Anreiz für Betreiberinnen kritischer Infrastrukturen, sich auf der Plattform zu registrieren. Dadurch fördert die Einführung der Meldepflicht den generellen Informationsaustausch und erzielt eine Wirkung, welche über die Erfüllung der rechtlichen Pflicht hinausgeht.

Am häufigsten meldeten Organisationen der öffentlichen Verwaltung, des Informations- und Kommunikationssektor sowie Finanz- und Versicherungsunternehmen. Die Analyse der gemeldeten Fälle zeigt, dass die am häufigsten gemeldeten Angriffsarten Hacking (19,5%), gefolgt von DDoS-Angriffen (17,6 %) und Diebstahl von Zugangsdaten (11,8%) sind. Auch Malware (9,5%), Ransomware-Angriffe (9,2 %) und Data-Leaks (8,8 %) wurden vermehrt gemeldet.

Am 1. Oktober 2025 traten zudem die Sanktionsbestimmungen in Kraft, wonach bei Nichterfüllung der Meldepflicht nach entsprechenden Mahnverfahren Bussen von bis zu 100'000 Franken verhängt werden können. Die ersten Monate zeigen jedoch, dass die meldepflichtigen Organisationen die neue Regelung ernst nehmen und ihre Verantwortung für die nationale Cybersicherheit wahrnehmen.

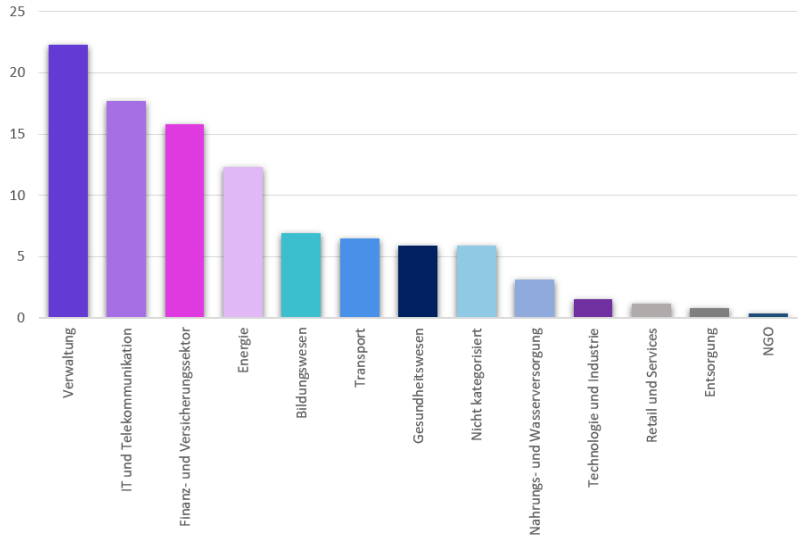


Abbildung 8: Bearbeitete Angriffsmeldungen pro Hauptsektor in Prozent

3 Schäden aus Cybervorfällen reduzieren

Warnungen vor schwerwiegenden Cyberbedrohungen über Alertswiss

Um Bevölkerung und Unternehmen noch gezielter vor schwerwiegenden Cyberbedrohungen zu warnen, hat das BACS die Zusammenarbeit mit dem Bundesamt für Bevölkerungsschutz (BABS) verstärkt und kann seit Mitte September Warnungen auch über die App und die Web-Plattform von Alertswiss publizieren. Damit steht ein zusätzlicher Kanal zur Verfügung, um die Bevölkerung im Fall von grossflächigen oder neuartigen Cyberangriffen möglichst rasch zu informieren, zu warnen und mit konkreten Handlungshinweisen zu schützen.

Einsätze des BACS bei Grossanlässen

Auch im Jahr 2025 übernahm das BACS bei drei Grossanlässen die zentrale Steuerung der Cybersicherheit im Cyberlageverbund: Beim World Economic Forum (WEF) im Januar, beim Eurovision Song Contest (ESC) im Mai und bei der UEFA Women's Euro im Juli. Ein Kernbestandteil der Einsätze war die Frühwarnung und Bedrohungsanalyse: Das BACS wertete Indikatoren und Meldungen aus, erstellte Bedrohungsszenarien und gab rechtzeitig Warnungen an Betreiberinnen kritischer Infrastrukturen heraus, damit diese präventiven Schutzmassnahmen ergreifen konnten. Parallel dazu wurde operative Unterstützung bereitgestellt, von technischen Empfehlungen über die Incident-Response-Koordination bis hin zur direkten Hilfe bei der Bewältigung laufender Angriffe.

Die Einsätze erfolgten im engen Rahmen des Cyberlageverbundes und in intensiver Zusammenarbeit mit Veranstaltern, Polizei und weiteren Bundesbehörden. Durch gemeinsame Lagekonferenzen, abgestimmte Kommunikationskanäle und standardisierte Meldeprozesse konnten Reaktionszeiten verkürzt und Informationsflüsse gesichert werden.

Austausch von Informationen

Die vom BACS betriebene MISP-Plattform («Malware Information Sharing Plattform») wurde auch 2025 als zentrales Instrument für den automatisierten Austausch technischer Informationen zu Cybervorfällen genutzt. Sie unterstützt den proaktiven Schutz der Schweizerischen kritischen Infrastrukturen, indem sie den zeitnahen Informationsfluss zwischen nationalen und internationalen Partnern sowie den beteiligten Organisationen ermöglicht. Es wurden über die Plattform technische Informationen zu 4'615 Cybersicherheitsvorfällen (MISP Events) ausgetauscht. Dabei handelt es sich sowohl um Informationen aus der Schweiz wie auch aus dem Ausland. Zudem hat das BACS 30 Betreiberinnen kritischer Infrastrukturen der Schweiz neu auf die MISP-Plattform integriert. Neben der MISP-Plattform, die dediziert für die Betreiberinnen von kritischen Infrastrukturen reserviert ist, betreibt das BACS noch drei weitere solche Plattformen für andere Interessensgruppen, wie zum Beispiel für die kantonalen und nationalen Polizeikorps.

4 Sicherheit von digitalen Produkten und Dienstleistungen erhöhen

Schwachstellen in Hard- und Software bleiben zentrale Einfallstore für Cyberangriffe. Das BACS fokussiert deshalb auf die gezielte Überprüfung kritischer Komponenten, auf denen Verwaltung und Wirtschaft aufbauen. Im Berichtsjahr standen zwei Schwerpunkte im Vordergrund: das etablierte Bug-Bounty-Programm der Bundesverwaltung und ein Pilotprojekt zur Sicherheit von Open Source Software.

Open Source

Open Source Software (OSS) hat bereits heute eine grosse Bedeutung für den sicheren Betrieb von kritischen Infrastrukturen, da heute verwendete Software oftmals auf OSS zurückgreift. Um die Sicherheit von OSS aktiv zu stärken, führte das BACS 2025 gemeinsam mit dem Nationalen Testinstitut für Cybersicherheit (NTC) ein Pilotprojekt durch, bei dem die Anwendungen «TYPO3» und «QGIS» exemplarisch geprüft wurden. Die Untersuchung bestätigte, dass auch in etablierten Projekten relevante Schwachstellen existieren. Diese wurden im Rahmen des Projekts in direkter Zusammenarbeit mit den Entwickler-Communities behoben. Das BACS nutzt diese Erkenntnisse nun, um Grundlagen für eine dauerhafte Unterstützung der OSS-Sicherheit durch den Bund zu erarbeiten.

Ebenfalls hat das BACS eine verbindliche Open-Source-Strategie eingeführt und «Open Source by default» als Arbeitsprinzip etabliert. Damit stärkt das BACS die Interoperabilität und Innovationsfähigkeit seiner Produkte und schafft offene Grundlagen für Projekte, Architekturen und Beschaffungen.

Bug Bounty

Das Bug-Bounty-Programm der Bundesverwaltung hat sich als effizientes Instrument und unverzichtbare Ergänzung zu klassischen Sicherheitstests etabliert. Ethische Hacker prüfen dabei die Systeme des Bundes nach klar definierten Regeln. Da Prämien («Bounties») ausschliesslich für technisch validierte Schwachstellen mit nachweisbarem Impact ausbezahlt werden, ist das Modell äusserst kosteneffizient. Finanzielle Mittel werden somit gezielt dort eingesetzt, wo reale Risiken bestehen.

Über das Bug-Bounty-Programm werden regelmässig relevante und kritische Schwachstellen identifiziert, die in herkömmlichen Tests nicht immer erkannt werden. Im Jahr 2025 gingen beim BACS insgesamt 525 Meldungen zu möglichen Schwachstellen ein. Nach Analyse und Prüfung wurden 328 Meldungen als gültig anerkannt und führten zu Massnahmen zur Behebung oder zur Verbesserung der Sicherheit in der Bundesverwaltung. Für diese Meldungen wurden Prämien in der Höhe von insgesamt rund 260’000 Franken ausbezahlt.

Das BACS führt das Bug-Bounty-Programm weiter und setzt sich dafür ein, entsprechende Programme als etabliertes Instrument der Informationssicherheit in der Schweiz zu verankern.

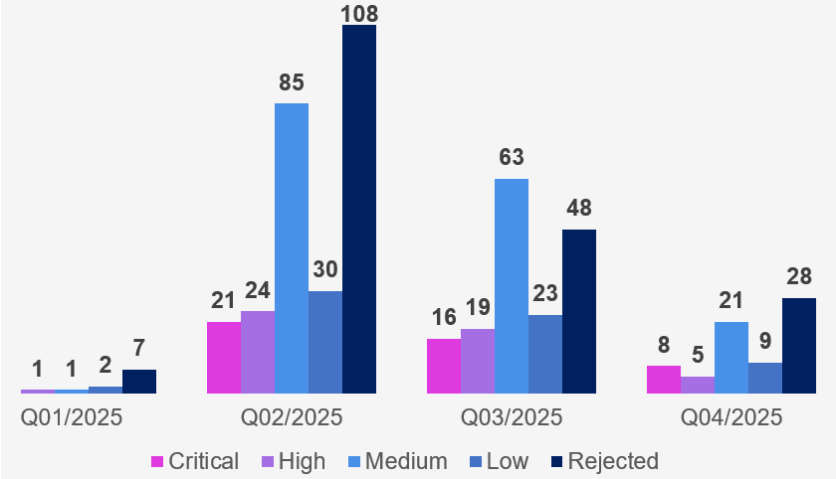


Abbildung 9: Gemeldete Schwachstellen und deren Einstufung

Wirkungsmanagement BACS

Im Rahmen seines Betriebskonzepts entwickelt und optimiert das BACS seine Planungs- und Steuerungsinstrumente stetig weiter. Dies insbesondere mit Blick auf die Schaffung von Transparenz und Nachvollziehbarkeit und im Gesamtkontext der Bundesverwaltung.

Das Wirkungsmanagement BACS bringt den Grundauftrag bzw. alle damit verbundenen Kerntätigkeiten des Bundesamtes in einen strukturierten und alignierten Ablauf und gibt Einsicht in die diversen Wirkungsebenen. Der Output gibt Aufschluss über die erbrachten Services und Produkte des Bundesamtes, während Outcome und Impact auf die mittel- bzw. langfristig zu erzielende Wirkung bei den jeweiligen Zielgruppen und Teilen der Gesellschaft fokussieren. Entlang der Kerntätigkeiten des Bundesamtes werden alle Wirkungsketten durchgängig im Organisationsportfolio geführt und mit Programmen, Projekten und anderen Vorhaben verknüpft.

Die koordinierte und zielgerichtete Umsetzung strategischer Themen im Rahmen des gesetzlichen Auftrags erfolgt im Bundesamt weiterhin gemäss OKR-Methodik («Objectives & Key Results»). Die mit OKR einhergehende konsequente quartalsweise Priorisierung, Planung und Steuerung der benötigten finanziellen, personellen und zeitlichen Ressourcen sowie das dazugehörige Controlling, in Form der Überprüfung der Erreichung der Resultate, stellen eine erfolgreiche Strategieumsetzung sicher. Nach der Einführung im Vorjahr konnte die Managementmethode 2025 weiter etabliert werden. Ein besonderer Fokus wird dabei unter anderem auf die koordinierte Zusammenarbeit bei gleichzeitiger Förderung der Teamautonomie innerhalb des BACS gelegt.

In seiner Gesamtheit ermöglicht das Wirkungsmanagement einen ganzheitlichen Blick auf die Tätigkeiten des Bundesamtes. Es schafft Orientierung, macht Zusammenhänge sichtbar und erlaubt es, Veränderungen frühzeitig zu erkennen und gezielt darauf zu reagieren. Damit bildet es die Grundlage für ein lernendes, wirkungsorientiertes Handeln und unterstützt das BACS dabei, seinen Auftrag auch künftig verlässlich, transparent und zielgerichtet zu erfüllen.

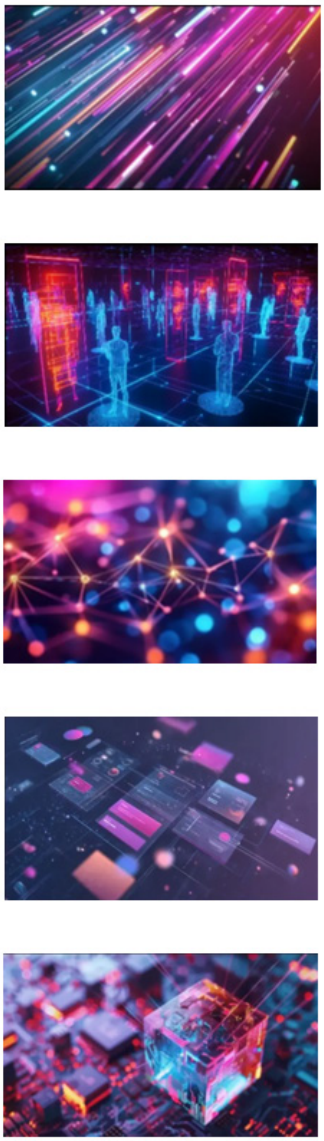


Abbildung 10 – 14: OKR BACS

Publikationen

BACS-Publikationen im 2025:

- Das Notfallkonzept als Schlüssel zur Cyberresilienz
- Erster Umsetzungsbericht zur Nationalen Cyberstrategie (NCS)
- Technologiebetrachtung: Quantencomputer und Post-Quanten-Kryptografie
- Technologiebetrachtung: Cybersicherheit und -resilienz
- Technologiebetrachtung: Passkeys
- Medienmitteilungen
- Mess- und Prüfbarkeit der IT-Sicherheit
- Technologiebetrachtung: Confidential Computing
- Technologiebetrachtung: Cloud Computing
- Technologiebetrachtung: SCION
- Wochenrückblicke
- Halbjahresbericht 2024/2
- Halbjahresbericht 2025/1
- Open-Source-Strategie BACS

Wissenschaftliche Artikel

A. Grünert, J. B. Michael, R. Oppliger, and R. Rytz, “On the measurability and testability of IT security,” *Computer*, vol. 57, no. 3, pp. 120–126, Mar. 2025, https://ieeexplore.ieee.org/document/10896924