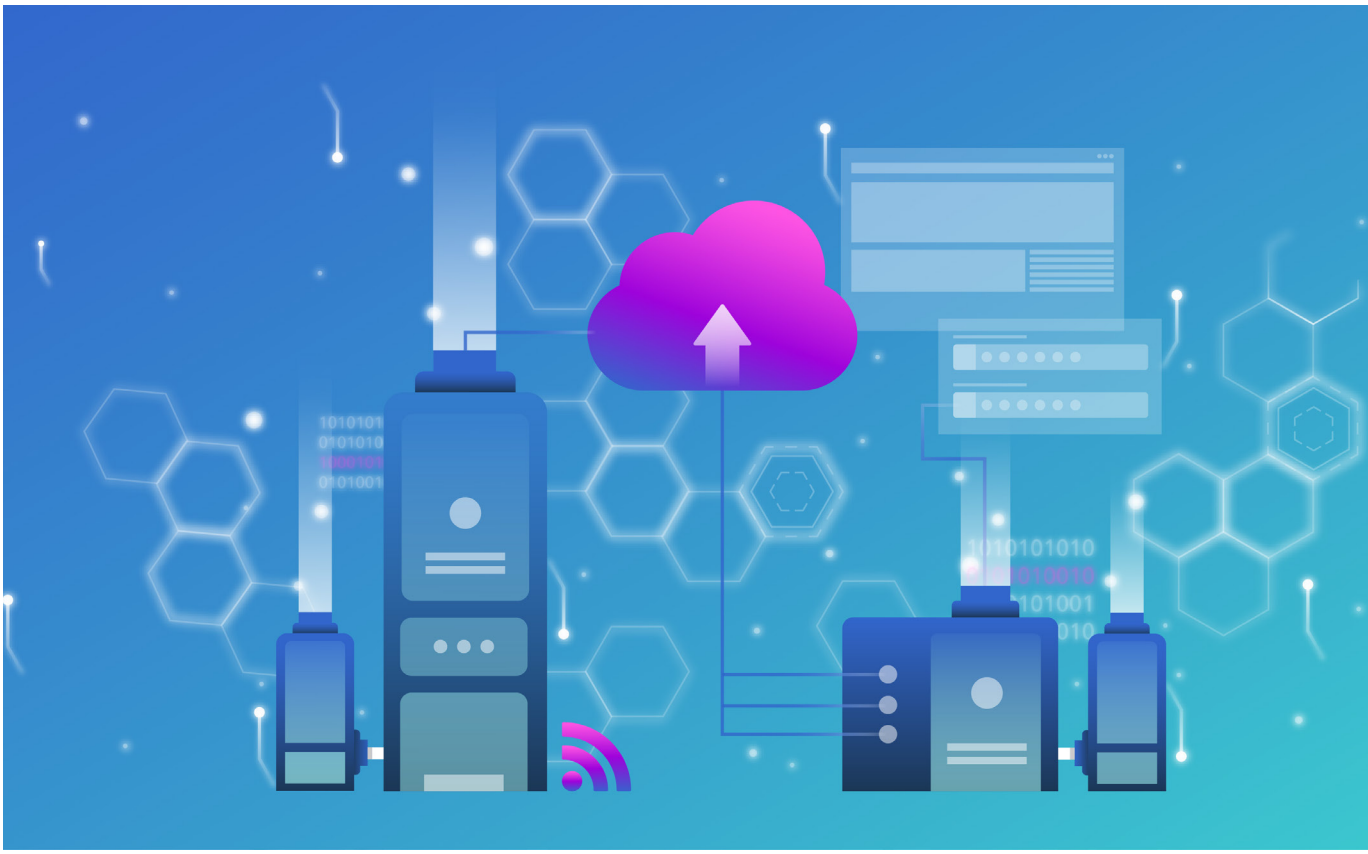
6. Mai 2024 | Bundesamt für Cybersicherheit BACS



Strategie des Bundesamtes für Cybersicherheit BACS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Übersicht / Inhalt

1 Ausgangslage: Herausforderungen in der Cybersicherheit in der Schweiz

Im Bereich der Cybersicherheit bestehen in der Schweiz derzeit folgende wichtigste Herausforderungen[1]:

- Hohe Verwundbarkeit von Wirtschaft, Behörden, Bildungsinstitutionen und der Bevölkerung im Cyberraum;
- Unzureichende Reaktionsfähigkeit auf systemrelevante Cybervorfälle und -krisen;
- Geringe Maturität von digitalen Produkten und Dienstleistungen bezüglich Cybersicherheit sowie fehlende Mechanismen zur Qualitätskontrolle;
- Nur punktuell ausgereiftes Verständnis von Cybersicherheit in Wirtschaft, Gesellschaft und Politik;
- Mangelnde Transparenz und fehlende Daten, um Aussagen zur Cybersicherheit einzuordnen und entsprechende politische und ökonomische Massnahmen abzuleiten;
- Begrenzter Schutz von Akteuren, welche nicht als kritische Infrastruktur gelten;
- Lückenhafte Koordination und rechtliche Graubereiche zwischen behördlichen und privaten Instrumenten der Cybersicherheit.

Diese Herausforderungen führen dazu, dass Cyberangriffe oft erfolgreich sind und hohe wirtschaftliche Schäden sowie ein hohes Risiko von Ausfällen bei nationalen kritischen Infrastrukturen verursachen.

Die Meldungen von Cybervorfällen mit Schadensfolge sind in den letzten Jahren jährlich um ca. 30% gestiegen. Die Anzahl der Meldungen nicht-kritischer Infrastrukturen hat sich in den letzten 12 Monaten ungefähr verdreifacht. Im Jahr 2023 hat das BACS 187'000 Meldungen zu Phishing bearbeitet und 8’223 Webseiten in der Schweiz, die für Phishing verwendet wurden, identifiziert und ausser Betrieb genommen. Bei mehreren hundert Meldungen hat das BACS Schadsoftware bei kritischen Infrastrukturen festgestellt und in Zusammenarbeit mit den betroffenen Unternehmen beseitigt. Im Durchschnitt wird dem BACS alle 40 Stunden eine Malware-Infektion gemeldet, bei deren Bewältigung Unterstützung gewünscht wird.

Insbesondere KMU geraten immer mehr ins Visier von Cyberkriminellen. Mittels Ransomware-Angriffen verschlüsseln die Angreifer Daten und stehlen diese. Sie verlangen anschliessend Lösegeld für die Entschlüsselung und die Verhinderung der Publikation der gestohlenen Daten. Die Angriffe sind stark automatisiert, weshalb es für die Kriminellen wenig Aufwand bedeutet, auch kleine Unternehmen anzugreifen. In der Schweiz erwirtschaften rund 75% aller Unternehmen weniger als 500'000 CHF Umsatz pro Jahr. Gerade für diese Unternehmen ist es schwierig, in die Cybersicherheit zu investieren. Sie sind darauf angewiesen, dass digitale Produkte und Dienstleistungen sicher entwickelt und gewartet werden oder dass Sicherheitsdienstleistungen kostengünstig verfügbar sind.

[1] Basierend auf der Wirksamkeitsüberprüfung «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018 bis 2022», der Nationalen Cyberstrategie (NCS) und den Weekly Reports und Fallstatistiken von Anlaufstelle, GovCERT und OIC.

Aber auch die Bevölkerung ist vor Cyberangriffen nicht gefeit. Hier dominiert vor allem das Phänomen des Cyberbetrugs. Eine zunehmende Verunsicherung und das Bedürfnis nach Informationen und Unterstützung sind deutlich spürbar.

Gleichzeitig produzieren Schweizer Hochschulen und innovative Unternehmen attraktive Lösungen für die Cybersicherheit. Diese auf den Markt zu bringen oder gar globale Standards zu schaffen, erweist sich jedoch als Herausforderung.

2 Vision des BACS

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 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.

3 Mission: Die vier strategischen Säulen des BACS

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. Es richtet dazu seine Leistung entlang vier strategischer Säulen aus:

1. **Cyberbedrohungen verständlich machen**
2. **Mittel zur Verhinderung von Cyberangriffen zur Verfügung stellen**
3. **Schäden aus Cybervorfällen reduzieren**
4. **Sicherheit von digitalen Produkten und Dienstleistungen erhöhen**

3.1 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.

Eine der meistgestellten Fragen von Verwaltungsräten, Geschäftsleitungen und Privatpersonen ist: «Was können wir tun, um uns vor Cybervorfällen zu schützen?» Auch in der Politik ist Cybersicherheit häufig ein Thema. Entscheidungsträger stehen immer vor der Herausforderung, Cyberbedrohungen einzuschätzen und Gegenmassnahmen zu identifizieren.

Das BACS sammelt Informationen über die verschiedenen Aspekte von Cybervorfällen, zeigt Zusammenhänge auf und leitet daraus Handlungsfelder, Diskussionsthemen und Empfehlungen ab. Damit ermöglicht das BACS einen informierten Dialog über Cyberbedrohungen und befähigt alle Akteure ihre Verantwortung so wahrzunehmen, dass die systemischen Risiken sinken. Die Analysen des BACS bieten eine Grundlage für Anbieter von Cybersicherheitslösungen, ihre Dienstleistungen und Produkte bedürfnisgerecht weiterzuentwickeln.

3.2 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.

Cyberangriffe erfordern Vorbereitung. Das bedeutet, dass die Angreifer Ziele auf Schwachstellen untersuchen, entsprechende Schadsoftware entweder selbst entwickeln oder einkaufen und initiale Zugangsversuche machen. Viele Angreifer verwenden dabei ähnliche Methoden und Vorgehensweisen. Das BACS erkennt solche Muster der Angreifer und teilt entsprechende Informationen und Warnungen mit Partnern und potentiell Betroffenen. Die Informationen reichen von technischen Angaben über die Angriffsvektoren bis hin zu Erkenntnissen darüber, wie ein bestimmter Angreifer Ziele auswählt. Mit diesen Informationen können betroffene Organisationen gewarnt werden, damit sie ihren Schutz erhöhen.

Noch wichtiger als die Früherkennung ist das Reduzieren der Angriffsfläche. Drei Faktoren schwächen die Cybersicherheit massgeblich: 1) Schwachstellen in Systemen, 2) Fehlkonfigurationen von Systemen und 3) Fehlmanipulationen durch Benutzer.

Das BACS reduziert die Angriffsfläche der von Schweizer Personen und Organisationen genutzten Systeme, indem es die frühzeitige Erkennung und Behebung von Schwachstellen fördert. Es warnt vor Angriffen und stellt Informationen für deren Abwehr zur Verfügung. Um grossangelegten Angriffen mit potentiell systemischen Auswirkungen vorzubeugen, setzt das BACS gezielt technologische Instrumente ein und arbeitet mit den zuständigen Behörden zusammen, um Schutzmassnahmen regulatorisch vorzuschreiben.

Das BACS entwickelt Technologien zur Erkennung und Abwehr von Gefährdungen. Das BACS erbringt diese Dienstleistung dann, wenn keine entsprechenden Produkte am Markt verfügbar sind oder die Gefährdungslage einen Markteingriff rechtfertigt. Eigenentwicklungen zur Erkennung und Abwehr werden wenn immer möglich als Open Source Software / Methodik zur Verfügung gestellt.

3.3 Schäden aus Cybervorfällen reduzieren

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

Cybervorfälle verursachen unterschiedliche Arten von Schäden. Der Schaden hängt vom Geschäftsmodell oder der persönlichen Situation der Betroffenen ab. Darüber hinaus besteht bei einem Cybervorfall häufig die Gefahr, dass sich der Schaden ausweitet. Einerseits dadurch, dass Angreifer die Vernetzung des Opfers nutzen, um weitere Ziele anzugreifen. Andererseits können durch Cybervorfälle ausgelöste Funktionsstörungen oder -ausfälle bei Dritten erhebliche Schäden verursachen.

Schäden können dann reduziert werden, wenn die Auswirkungen von Cybervorfällen zeitlich und organisatorisch eingegrenzt werden. In erster Priorität widmet sich das BACS der Aufgabe, systemische Gefahren zu verhindern, die das Funktionieren des Staates gefährden. Dabei geht es nicht nur um Systemausfälle, sondern auch um grosse wirtschaftliche Schäden, die die Entwicklung des Brutto Inland Produktes (BIP) erheblich beeinflussen können. Das BACS unterstützt die Betroffenen bei der Bewältigung von Vorfällen mit fachlicher Beratung und organisatorischer Unterstützung. Die Unterstützungsleistungen reichen je nach potentiellem Ausmass von der Beratung bis hin zum vollumfänglichen Cyberkrisenmanagement einschliesslich technischer Abwehr und Wiederherstellung. Dabei gilt das Prinzip, dass die Leistungen des BACS für Private subsidiär erbracht werden. Dies bedeutet, dass die Betroffenen den Vorfall möglichst selbstständig und unter Einbezug von Leistungen aus der Wirtschaft bewältigen müssen.

Das BACS schafft nationale und internationale Strukturen, welche eine vereinfachte Koordination bei der Bewältigung von Cybervorfällen ermöglicht. Bei Vorfällen, die mehrere Behörden in der Schweiz betreffen, übernimmt das BACS die Führung. Zudem ermöglicht das BACS Organisationen und Privatpersonen, sich optimal auf die Bewältigung eines Cybervorfalls vorzubereiten, indem es Unterlagen und Empfehlungen zu «Best Practices» zur Verfügung stellt.

3.4 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 Transparenz für Nutzer, sodass sie informierte Entscheide über die Cybersicherheit von Produkten und Dienstleistungen treffen können.

Sicherheitsforschende haben festgestellt, dass fast jede Applikation mindestens eine sicherheitsrelevante Schwachstelle aufweist. Auch Hardware ist nicht immun gegen Fehler, die die Cybersicherheit beinträchtigen. Solche Fehler lassen sich aufgrund der Komplexität heutiger IKT-Systeme nicht vollständig vermeiden. Ein Grossteil der Fehler kann jedoch durch einen gut struktu-

rierten Entwicklungsprozess und Testing über den gesamten Produktlebenszyklus hinaus vermieden oder schnell erkannt und beseitigt werden. Höhere Investitionen in Cybersicherheit führen zwangsläufig zu teureren Produkten. Sichere Produkte stehen aber immer im Wettbewerb mit günstiger hergestellten Produkten. Dabei ist für den Konsumenten kaum ersichtlich, wie sicher ein Produkt ist und ob der höhere Preis auch wirklich mehr Sicherheit bedeutet.

Das BACS unterstützt und erarbeitet Initiativen und Modelle, die Transparenz über die Cybersicherheit von Produkten schaffen und den Markt für sichere Produkte begünstigen. Beispiele für solche Modelle reichen von «Labeling»-Schemas bis hin zu Regulationsvorschlägen, Anreizschaffung und Finanzierungsmodellen.

4 Betriebsmodell des BACS

Um dieses Leistungsversprechen möglichst effizient umzusetzen, konsolidiert und aggregiert das BACS bestehende Inhalte, stellt deren Qualität sicher und vermittelt sie bedarfsgerecht zwischen den Leistungserbringern und den Leistungsbezügern.

Das BACS ist dem in der NCS verankerten Kooperationsmodell verpflichtet und arbeitet eng mit den Kantonen, der Wirtschaft und den Hochschulen zusammen. Ziel dieser Zusammenarbeit ist es, Fachwissen zu bündeln und sich gegenseitig so zu unterstützen, dass der Schutz vor Cyberbedrohungen optimiert werden kann.

Das BACS erstellt originäre Inhalte und erbringt originäre Leistungen nur dann, wenn keine adäquaten Inhalte Dritter zur Verfügung stehen, diese nicht zum Wohle aller nutzbar sind, oder diese aufgrund gesetzlicher Bedingungen oder Vertrauensgründen direkt durch den Bund erbracht werden müssen. Das BACS versteht sich insbesondere auch als «Inkubator», der neue Leistungen – für die ein Bedarf besteht – initiiert. Es gibt diese Leistungen an andere Organisationen ab, sobald sie eine gewisse Maturität erreicht haben und von einer anderen Stelle besser erbracht werden können.

Die Leistungen des BACS werden nach Möglichkeit im Plattformmodell als digitale Dienstleistung erbracht. Eine direkte Leistungserbringung erfolgt nur wo unbedingt notwendig, insbesondere im Bereich der Unterstützung der Vorfallbewältigung und Teilen der Sensibilisierung. Die Fokussierung auf das Plattformmodell ermöglicht die Skalierung der Leistungen des BACS mit überschaubarem Mitteleinsatz.

Zu diesem Zweck erstellt und betreibt das BACS eine Self-Service-Plattform, die Zugang zu Informationen über Cyberbedrohungen, spezifische und allgemeine Empfehlungen und Mittel zur Prävention und zum «Information Sharing» bietet.