

30. März 2026 | Bundesamt für Cybersicherheit BACS



Halbjahresbericht 2025/II (Juli – Dezember)

# Cybersicherheit

Lage in der Schweiz und international



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

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

## Management Summary

Das Bundesamt für Cybersicherheit (BACS) beschreibt in seinem Halbjahresbericht die relevanten Vorfälle und Entwicklungen im Kontext der Cyberbedrohungen gegen die Schweiz und international. Im zweiten Halbjahr 2025 erhielt das BACS 29'006 freiwillige Meldungen sowie 145 meldepflichtige Cybervorfälle, womit der gesamte Meldeeingang weiterhin auf hohem Niveau stabil bleibt. 52 Prozent der Meldungen sind dem Phänomen «Betrug» zugeordnet, wobei jedoch die seit Mitte 2023 dominierenden betrügerischen Drohanrufe im Namen von Behörden<sup>1</sup> signifikant abnahmen. Die zentralen Bedrohungsphänomene blieben in der Schweiz auch dieses Halbjahr dieselben, relevante Entwicklungen gab es jedoch bezüglich der jeweiligen Ausprägungen der beschriebenen Bedrohungsformen.

### **Auf die Schweiz zugeschnittene Phishing-Varianten**

Cyberkriminelle führten weiter «Voice-Phishing»- und «Real-Time-Phishing»-Kampagnen<sup>2</sup> mit betrügerischen Werbeanzeigen in Suchmaschinen durch. Zusätzlich zeigten sich aber auch mehr aufwändigere, zielgerichtetere Varianten, die u. a. auch Schweizer Besonderheiten mit z. B. Treuepunkteprogrammen beinhalteten. Zudem nutzten Angreifer beim doppelten Phishing («Double Phishing»<sup>3</sup>) einen gerade erst stattgefundenen, erfolgreichen Phishing-Vorfall, um die Opfer am Telefon ein weiteres Mal zu schädigen. Ab Sommer 2025 setzten Kriminelle SMS-Blaster erstmals auch in der Schweiz ein. Damit umgehen sie Filtermethoden der Kommunikationsanbieter für die Verteilung von SMS-Phishing.

### **Ransomware als konstante und ernstzunehmende Bedrohung**

«Ransomware»<sup>4</sup> und die damit verbundene Datenerpressung bedrohen nach wie vor opportunistisch Schweizer Organisationen aller Art. Insgesamt 57 Ransomware-Vorfälle wurden dem BACS freiwillig oder auf Basis der Meldepflicht direkt mitgeteilt. Die Ransomware-Variante «Akira» war bereits im ersten Halbjahr 2025 in der Schweiz führend, ihre Aktivitäten intensivierten sich zusätzlich in der Berichtsperiode. Besonders die Ausnützung von SonicWall-Geräten trug zu diesen Auswirkungen bei, da Korrekturanweisungen des Herstellers nach einer Schwachstelle aus dem Jahr 2024 nicht von allen Betroffenen konsequent umgesetzt wurden.

### **Angriffe auf internationale Software-Lieferketten**

Zahlreiche Schweizer Organisationen waren im zweiten Halbjahr 2025 nebst Schwachstellen in gängigen Software-Produkten auch von Kompromittierungen etablierter und viel genutzter Komponenten in «Open-Source»-Software (OSS) betroffen. Im Kontext der beiden «Shai-Hulud»-Kampagnen im September und November 2025 wurden beispielsweise über tausend npm-Pakete («Node Package Manager») mit monatlichen Downloads im dreistelligen Millio-

---

<sup>1</sup> [Anrufe im Namen von Fake-Behörden \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/news/2025/07/01/anrufe-im-namen-von-fake-behoerden)

<sup>2</sup> [Vishing, Smishing \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/news/2025/07/01/vishing-smishing)

<sup>3</sup> [Woche 39: Wenn ein Phishing-Versuch auf den nächsten folgt \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/news/2025/07/01/woche-39-wenn-ein-phishing-versuch-auf-den-naechsten-folgt)

<sup>4</sup> [Ransomware \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/news/2025/07/01/ransomware)

nenbereich infiziert. Diese komplexen, technischen Abhängigkeiten fordern IT-Verantwortliche, da beim Vorliegen einer Sicherheitslücke in diesen Software-Bibliotheken alle Anwendungen potenziell verwundbar sind, die diese Komponente im Code enthalten.

### **ORB-Netzwerke in der Schweiz**

Die Anzahl kompromittierter Geräte, die zu verdeckten ORB-Netzwerken gehören, wächst kontinuierlich. Solche Netzwerke bestehen in der Regel aus mit «Schadsoftware»<sup>5</sup> infizierten, mit dem Internet vernetzten Geräten (IoT) und Routern, die für verschiedene Angriffe genutzt werden und die Privatsphäre der Eigentümer beeinträchtigen. Eine Vielzahl von Geräten der Schweizer Privatpersonen und Organisationen wurden somit für Angriffe gegen Ziele der Nutzer dieser Angriffsinfrastruktur missbraucht. Deshalb ist ein regelmässiges Aktualisieren von Geräten, die gegenüber dem Internet exponiert sind, für die Bekämpfung solcher Netzwerke zentral. Bereits im Jahr 2024 zeigte sich international, dass staatliche Akteure Infrastrukturen wie ORB-Netzwerke ebenfalls für Spionage- und Sabotageaktivitäten nutzen.

Der Halbjahresbericht beleuchtet in weiteren Kapiteln Beobachtungen und Entwicklungen aus den Bereichen Malware, Angriffe auf die Verfügbarkeit von Websites und Webdiensten, Datenmanagement sowie Cyberspionage und -sabotage. Trotz eines zunehmend angespannten geopolitischen Umfelds zeigen sich die Auswirkungen der Cyberbedrohungslage auf die Schweiz als relativ stabil und die Cyberresilienz als grösstenteils robust.

---

<sup>5</sup> [Schadsoftware \(ncsc.admin.ch\)](https://www.ncsc.admin.ch)

## Inhalt

|          |   |           |
|----------|---|-----------|
|          | <b>Editorial .....</b>  | <b>4</b>  |
| <b>1</b> | <b>Cyberbedrohungen in der Schweiz – ein Überblick .....</b>                | <b>6</b>  |
| <b>2</b> | <b>Phishing .....</b>   | <b>10</b> |
| <b>3</b> | <b>Schadsoftware .....</b>  | <b>15</b> |
|          | 3.1 Initialer Zugang mit Schadsoftware .....                                | 15        |
|          | 3.2 Ransomware .....  | 17        |
|          | 3.3 Verdeckte ORB-Netzwerke in der Schweiz .....                            | 20        |
| <b>4</b> | <b>Schwachstellen.....</b>  | <b>21</b> |
| <b>5</b> | <b>Betrug und Social Engineering .....</b>                                  | <b>23</b> |
| <b>6</b> | <b>Angriffe auf die Verfügbarkeit von Websites und Webdiensten .....</b>    | <b>27</b> |
| <b>7</b> | <b>Datenmanagement, -abflüsse und -erpressung.....</b>                      | <b>28</b> |
| <b>8</b> | <b>Cyberspionage und -sabotage .....</b>                                    | <b>30</b> |
|          | 8.1 Cyberspionage .....   | 30        |
|          | 8.2 Bedrohung industrieller Kontrollsysteme und operativer Technologie..... | 32        |

## Editorial

Die Cyberbedrohungslage in der Schweiz bewegt sich weiterhin auf einem hohen Niveau. Weiterhin ist der überwiegende Teil der festgestellten Cybervorfälle auf kriminelle Aktivitäten zurückzuführen. Gleichzeitig führen wirtschaftliche Unsicherheiten und ein zunehmend angespanntes geopolitisches Umfeld dazu, dass Cyberangriffe gezielter, koordinierter und wirkungsvoller eingesetzt werden. Neben der anhaltenden Bedrohung durch Cyberkriminalität ist vermehrt auch mit ausgeklügelten und professionell vorbereiteten Angriffen staatlich unterstützter Akteure zu rechnen, die strategische Interessen verfolgen.

Unverändert stellen Ransomware-Angriffe eine der grössten Herausforderungen für Organisationen in der Schweiz dar. Die Kombination aus Systemverschlüsselung und Datenerpresung bleibt ein ernst zu nehmendes Risiko für Wirtschaft und Verwaltung. So hat etwa die Hackergruppe Akira ihre Aktivitäten in der Schweiz in den vergangenen Monaten deutlich ausgedehnt. Parallel dazu nehmen Angriffe entlang von Lieferketten zu, Online-Werbung wird vermehrt für Täuschungs- und Betrugszwecke missbraucht, und die fortschreitende Digitalisierung führt zu einer stetig wachsenden Zahl potenziell ausnutzbarer Schwachstellen. Diese Entwicklungen vergrössern die Angriffsfläche und erhöhen die Komplexität der Bedrohungslage insgesamt.

Eine realistische und belastbare Einschätzung dieser Lage ist nur möglich, wenn Cybervorfälle konsequent gemeldet und systematisch ausgewertet werden. Der vorliegende Bericht stützt sich auf die zahlreichen freiwilligen Meldungen aus Bevölkerung und Wirtschaft, die eine unverzichtbare Grundlage für das nationale Lagebild darstellen. Im vergangenen Jahr gingen rund 65'000 solcher Meldungen beim BACS ein. Mit der Einführung der Meldepflicht für Betreiberinnen kritischer Infrastrukturen am 1. April 2025 wurde ein wichtiger Schritt zur Stärkung der nationalen Cyberresilienz vollzogen. Erstmals können meldepflichtige Vorfälle strukturiert in die Analyse einbezogen werden.

Die bisherigen Meldungen liefern wertvolle Erkenntnisse über Angriffsarten, betroffene Sektoren und mögliche systemische Risiken. Die Auswertung der gemeldeten Vorfälle zeigt deutlich, dass Cybersicherheit keine isolierte Aufgabe einzelner Akteure ist. Staat, Wirtschaft und Gesellschaft sind gleichermaßen betroffen und gefordert. Cyberangriffe machen nicht an Organisations-, Branchen- oder Landesgrenzen halt, sondern entfalten ihre Wirkung entlang digitaler Abhängigkeiten.

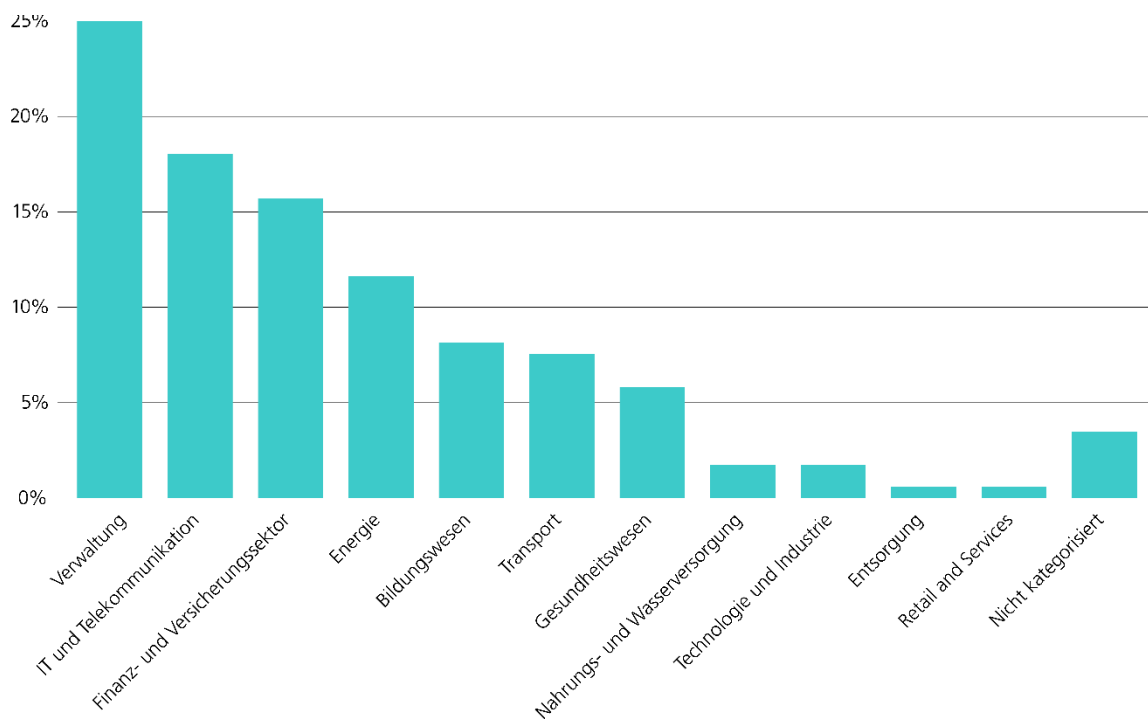
Vor diesem Hintergrund wurden auf nationaler und internationaler Ebene verstärkt geopolitische Fragestellungen diskutiert. Im Zentrum dieser Diskussionen standen dabei insbesondere die zunehmende Systemrelevanz digitaler Abhängigkeiten, der Einfluss neuer Technologien wie künstliche Intelligenz sowie die Notwendigkeit eines koordinierten Vorgehens zwischen Staaten, Aufsichtsbehörden und privaten Akteuren.

Ein wiederkehrendes Fazit dieser Diskussionen ist, dass Cyberresilienz über reine Prävention hinausgehen muss. Neben technischer Sicherheit braucht es klare Governance-Strukturen, funktionierende Reaktions- und Wiederherstellungsfähigkeiten sowie eine enge nationale und internationale Zusammenarbeit. Genau in diesem Bereich, die Zusammenarbeit weiter zu vereinfachen und vereint aktiver gegen Cyberbedrohungen vorzugehen, wollen wir weiter investieren.

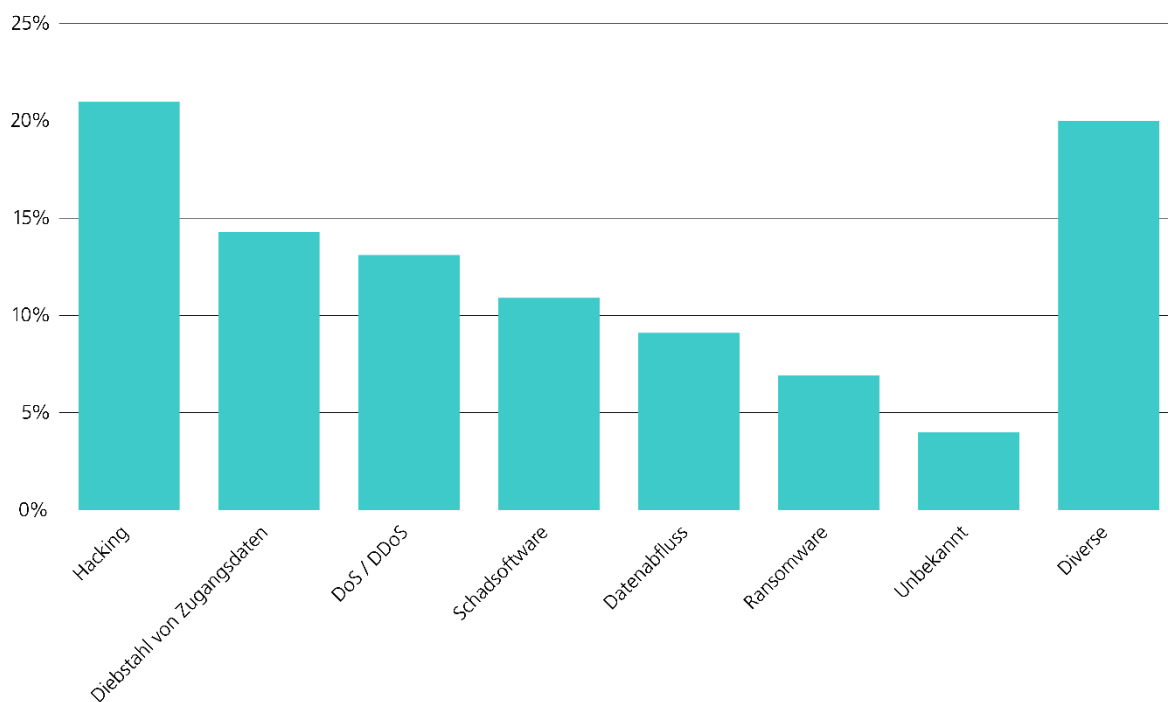
Das BACS dankt allen Organisationen und Personen, die durch ihre Beiträge zur Nationalen Cyberstrategie (NCS), Meldungen über Vorfälle oder Gefahren, und ihr Engagement und Interesse am Thema einen wesentlichen Beitrag zur Stärkung der nationalen Cyberresilienz leisten. Dieser gemeinsame Einsatz ist entscheidend, um den Herausforderungen im Cyberraum auch künftig wirksam begegnen zu können.

**Florian Schütz, Direktor Bundesamt für Cybersicherheit**





**Abb. 1:** Prozentuale Verteilung meldepflichtiger Cybervorfälle gemeldet an das BACS nach Sektoren im zweiten Halbjahr 2025



**Abb. 2:** Prozentuale Verteilung meldepflichtiger Cybervorfälle gemeldet an das BACS nach Angriffsart im zweiten Halbjahr 2025

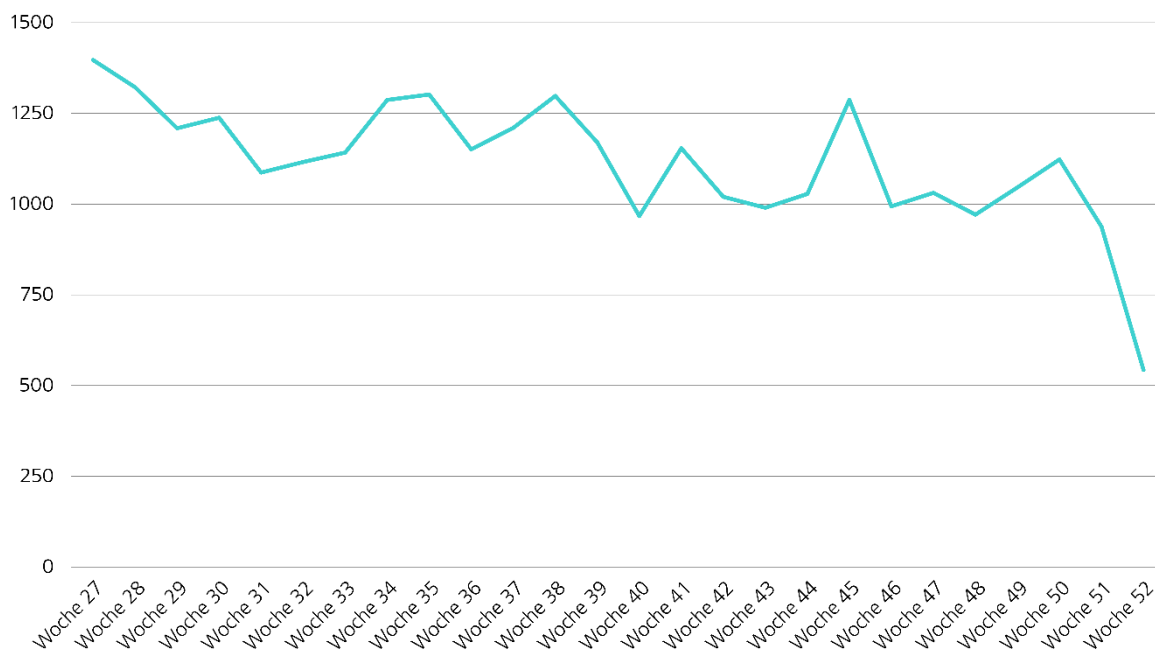


Abb. 3: Anzahl freiwillige Meldungen pro Woche an das BACS im zweiten Halbjahr 2025, vgl. [Aktuelle Zahlen \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/aktuelle-zahlen)

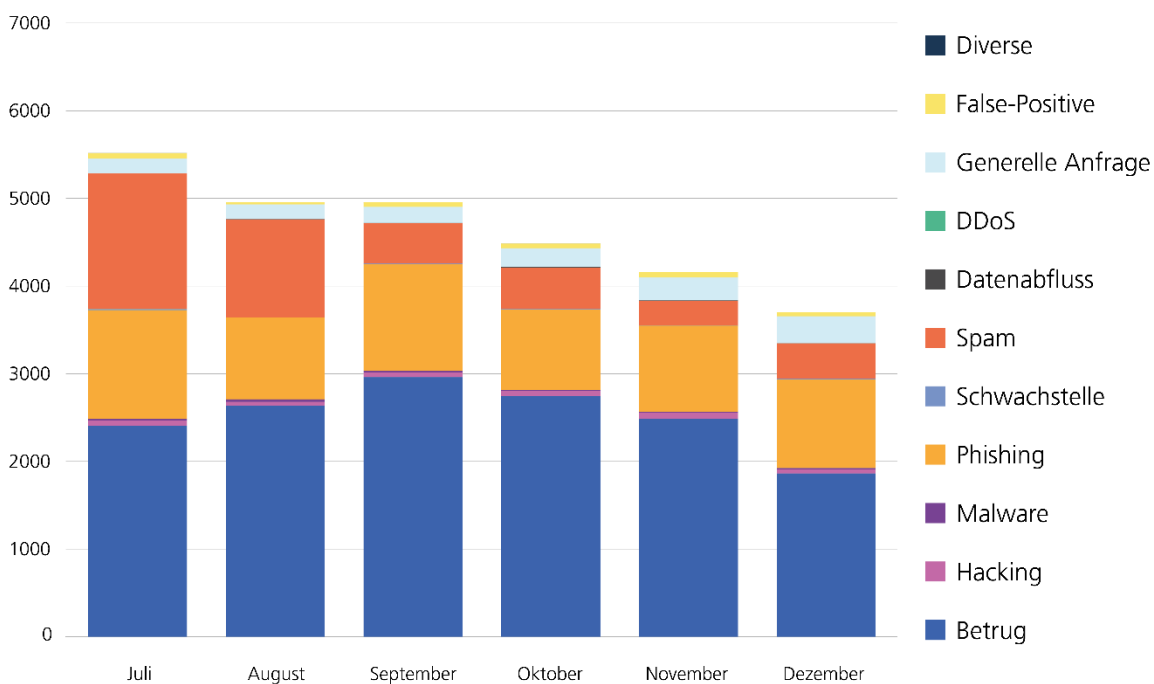


Abb. 4: Freiwillige Meldungen an das BACS im zweiten Halbjahr 2025 nach Kategorien, vgl. [Aktuelle Zahlen \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/aktuelle-zahlen)

Demgegenüber gingen Meldungen zu «betrügerischen Drohanrufen im Namen von Behörden»<sup>9</sup> im Vergleich zum zweiten Halbjahr 2024 von 8'173 auf 5'941 zurück. Erstmals seit ihrem Auftreten im zweiten Halbjahr 2023 sind die Meldungen dieses Phänomens klar gesunken. Notifikationen zu «Online-Anlagebetrug»<sup>10</sup> blieben mit 430 Fällen gegenüber dem ersten Halbjahr weitgehend konstant. Es häuften sich jedoch Meldungen, in denen Opfer nach einem Online-Anlagebetrug erneut unter dem Vorwand kontaktiert wurden, dass das gestohlene Geld angeblich zurückgeholt werden könne.

Das Verhältnis der freiwilligen Meldungen aus der Bevölkerung zu jenen von Unternehmen, Vereinen und Behörden bleibt mit 90 zu 10 Prozent unverändert. Während Unternehmen wie Privatpersonen von betrügerischen Drohanrufen und Phishing-Versuchen betroffen sind, sahen sich 57 Unternehmen gemäss ihrer Meldung mit Ransomware im zweiten Halbjahr 2025 konfrontiert. Typische Betrugsvarianten gegen Organisationen sind weiterhin der «Rechnungsmanipulationsbetrug»<sup>11</sup> (BEC) und der «CEO-Betrug»<sup>12</sup>. Während die Meldungen zu CEO-Betrug nach einer Zunahme im ersten Halbjahr 2025 wieder zurückgegangen sind, zeigt sich beim Rechnungsmanipulationsbetrug ein anhaltender Aufwärtstrend: Nach 59 Meldungen im ersten Halbjahr 2025 wurden im zweiten Halbjahr bereits 73 Fälle registriert. Dieser Betrugstyp verursacht hohe finanzielle Schäden, so erbeuteten in einem Fall Kriminelle CHF 1,5 Millionen. Ausserdem ermöglicht diese Vorgehensweise den Angreifern auch Zugriff auf vertrauliche Firmenkommunikation, was schwerwiegende Konsequenzen für Dritte haben kann.

Die Statistik verdeutlicht, dass die Cybersicherheit und der Schutz der Schweiz vor Cyberrisiken eine kontinuierliche Herausforderung für Wirtschaft, Staat und Gesellschaft darstellt. Entsprechend präsentiert der Halbjahresbericht die Kernphänomene, welche die Bedrohungslandschaft im Cyberraum für die Schweiz charakterisieren. Diese beinhaltet Phishing, Schadsoftware, Schwachstellen, Betrugsfälle und «Social Engineering»<sup>13</sup>, Angriffe auf die Verfügbarkeit von Websites und anderen Internetdiensten (DDoS), Datenabflüsse sowie Cyberspionage und -sabotage. Der Fokus des Berichts liegt dabei auf den Ereignissen und Entwicklungen in der Schweiz. Internationale Entwicklungen werden im Bericht erwähnt, wenn sie die Bedrohungslandschaft in der Schweiz illustrieren (vgl. Kap. 8). Mithilfe der Themenkapitel können sich Leserinnen und Leser einen Überblick über die aktuellen Ausprägungen, die interessanten Vorfälle sowie die Entwicklungen der Kernphänomene verschaffen. Im Sinne der Eigenverantwortung für eine sicherere, digitale Schweiz leitet der Bericht Empfehlungen für die Öffentlichkeit ab, wie diesen Herausforderungen begegnet werden kann.

---

<sup>9</sup> Um auf das Phänomen «betrügerische Anrufe im Namen von Behörden» tiefer einzugehen, hat das BACS einen [Bericht](#) verfasst, der gleichzeitig mit dem [Halbjahresbericht 2024/1](#) veröffentlicht wurde.

<sup>10</sup> [Online-Anlagebetrug \(ncsc.admin.ch\)](#)

<sup>11</sup> [Rechnungsmanipulationsbetrug \(ncsc.admin.ch\)](#)

<sup>12</sup> [CEO-Betrug \(ncsc.admin.ch\)](#)

<sup>13</sup> [Social Engineering \(ncsc.admin.ch\)](#)

## 2 Phishing

Phishing ermöglicht Cyberakteuren, ohne das Wissen der Nutzerinnen und Nutzer Zugangsdaten, Finanzinformationen und andere vertrauliche Daten zu sammeln. Typisch dabei ist, dass die zwischenmenschliche Beeinflussung (Social Engineering) der Empfängerinnen und Empfänger eine zentrale Rolle spielt und keine Schadsoftware verteilt wird.<sup>14</sup> Das klassische Vorgehen beinhaltet das Versenden einer Nachricht mit einem Link an einen grossen Empfängerkreis. Dieser Link führt zu einer Phishing-Webseite, die einer legitimen Seite nachgeahmt wurde. Wenn die Empfängerinnen und Empfänger die Phishing-Webseite für glaubwürdig halten, geben die Opfer sensible Daten – wie z. B. Zugangs- und Kreditkartendaten – ein und die Daten gelangen so zu den Betrügern. Während Phishing via E-Mail noch immer zu den gängigsten Methoden gehört, nutzen andere Ansätze die Stimme (Voice-Phishing oder «Vishing») oder SMS («Smishing») und andere Arten mobiler Nachrichten, um an Informationen zu gelangen. Wenn hingegen das Phishing zielgerichtet gegen eine bestimmte Person oder eine ausgewählte Personengruppe erfolgt, handelt es sich um ein sogenanntes «Spear-Phishing». Im Gegensatz zu der breit gestreuten Variante können Opfer diese Angriffsart deutlich schwieriger erkennen, da sie spezifisch auf die Angriffsziele zugeschnitten ist.

Im Jahr 2025 erhielt das BACS über das öffentliche Meldeformular 12'280 Meldungen zu Phishing-Versuchen, womit dieser Wert im Vorjahresvergleich fast unverändert blieb. Davon fielen 6'299 Meldungen im zweiten Halbjahr an, was eine leichte Erhöhung um 903 Meldungen im Vergleich zur Vorjahresperiode darstellt.

Anders verhielt sich die Phishing-Statistik der über die vom BACS betriebenen Plattform [antiphishing.ch](https://antiphishing.ch)<sup>15</sup> eingegangenen Meldungen. Hier lässt sich nach mehreren Perioden des steten Zuwachses bis Ende 2024 eine Reduktion im Jahr 2025 beobachten. Während im zweiten Halbjahr 2024 noch 9'355 einzigartige Phishing-URLs rapportiert wurden, verringerte sich die Zahl auf 7'969 im gleichen Zeitraum des Jahres 2025. Um die Phishing-Seiten so vertrauenswürdig wie möglich zu gestalten, locken Kriminelle die Opfer immer wieder unerlaubt im Namen bekannter Marken und Unternehmen auf ihre Phishing-Seiten. Am häufigsten wurden in dieser Berichtsperiode Postdienste (24 %), der öffentliche Verkehr (20 %), der Finanzsektor (19 %), der IT-Sektor (7 %) und der Versicherungssektor (7 %) für Phishing missbraucht (vgl. Abb. 5). Nebst dem kontinuierlichen Anstieg von Phishing-Versuchen im Kontext von Krankenkassen<sup>16</sup> erhöhte sich auch im Einzelhandel die Anzahl gemeldeter Phishing-URLs (5 %).

---

<sup>14</sup> International wird das Phänomen Phishing nicht einheitlich verwendet, weshalb in anderen Definitionen auch häufig die Verteilung von Schadsoftware inkludiert wird (vgl. [Phishing \(attack.mitre.org\)](https://attack.mitre.org)). Das BACS schliesst diese Dimension aber explizit in der angewendeten Definition aus.

<sup>15</sup> Das BACS erhält Meldungen zu Phishing nicht nur in Form von Vorfallmeldungen, sondern auch über die Plattform [antiphishing.ch](https://antiphishing.ch), welche zusätzliche Quellen miteinspeist. Aufgrund dessen können die hier genannten Zahlen von der Zahl der Direktmeldungen für Phishing abweichen.

<sup>16</sup> Siehe z. B. [Phishing-Mail richtet sich an Helsana-Kunden \(cybercrimepolice.ch\)](https://www.cybercrimepolice.ch), [Phishing-Mail – Rückerstattung CSS-Krankenkassengelder \(cybercrimepolice.ch\)](https://www.cybercrimepolice.ch)

Generell demonstriert das zweite Halbjahr 2025 eine Weiterführung schon beobachteter Entwicklungen des ersten Halbjahres. Die gängigen, unpersönlichen und in grosser Anzahl versendeten Phishing-Nachrichten halten weiterhin an. So macht Phishing im Namen von SwissPass und Paketdienstleistern immer noch rund 40 Prozent aller Phishing-URLs aus. Daneben werden aber auch immer aufwändigere, zielgerichtete Varianten beobachtet, was für die Täter einen Mehraufwand bedeutet. Einerseits hielten die Meldungen zu Real-Time-Phishing gegen Bankkunden mithilfe bössartiger Werbung via Suchmaschinen an.<sup>17</sup> Aufgrund steigenden Bewusstseins veränderten die Phisher aber ihren Verteilmechanismus dahingehend, dass sie nicht mehr nur Werbeanzeigen zu ihren Phishing-Seiten schalteten, sondern ebenfalls «SEO-Poisoning»<sup>18</sup> einsetzten. Auch Voice-Phishing wird weitergeführt, wobei den Opfern unter anderem per E-Mail oder Textnachricht angebliche E-Banking-Transaktionen vorgetäuscht werden, mit der Aufforderung bei einem Fehler zurückzurufen.<sup>19</sup> Andererseits nutzten Phisher aber auch das gestiegene Sicherheitsbewusstsein in der Schweizer Bevölkerung aus, indem sie vermehrt Phishing als Verifizierungs-E-Mails tarnten.<sup>20</sup> Demnach sollen die Opfer ihre Identität bestätigen, indem sie ihre Zugangsdaten auf einer Phishing-Seite eingeben. Abgesehen von diesen Entwicklungen wurden in der Schweiz mehrere Vorkommnisse mit SMS-Blastern<sup>21</sup> und doppeltem Phishing<sup>22</sup>, einer neuen Art der Phishing-Methodik, beobachtet.



## Empfehlungen

Melden Sie dem BACS verdächtige Phishing-Versuche via [reports@antiphishing.ch](mailto:reports@antiphishing.ch) oder direkt über die Website [antiphishing.ch](https://antiphishing.ch). Falls Sie gerne eine Rückmeldung erhalten möchten, können Sie den Phishing-Vorfall auch via [Meldeformular](#) oder [incidents@ncsc.ch](mailto:incidents@ncsc.ch) an die Spezialistinnen und Spezialisten des BACS melden. Mit Ihrer Hilfe kann das BACS gezielt warnen und Massnahmen einleiten, damit die betrügerischen Webseiten blockiert werden.

## Auf die Schweiz zugeschnittene Phishing-Kampagnen

Im zweiten Halbjahr 2025 führten Betrüger vermehrt gezielte Phishing-Angriffe mit typisch schweizerischen Inhalten oder für ausgewählte Personengruppen durch. Mit dieser Vorgehensweise erhöhen sie ihre Erfolgchancen im Gegensatz zu unpersönlichen Massen-Phishings. Dieses Muster zeigte sich beispielsweise in einem E-Mail-Phishing, welches Seniorinnen und Senioren über ein angeblich offenes Pensionskassen-Guthaben informierte. Auch gab es Phishing-Varianten, bei denen alte Datenlecks genutzt worden sind (vgl. Kap. 7), um

---

<sup>17</sup> Siehe [Halbjahresbericht 2025/1](#); Kap. 2.

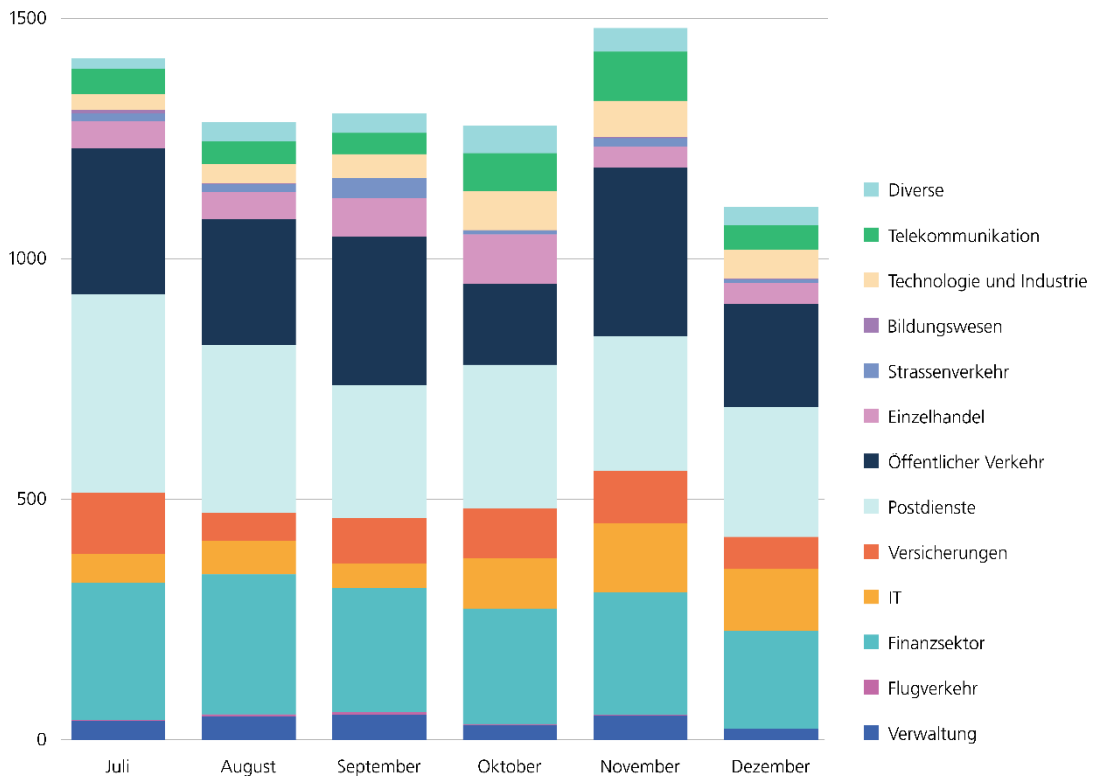
<sup>18</sup> Bei SEO Poisoning versuchen Angreifer, Suchmaschinen so zu manipulieren, dass ihre bössartigen Websites bei den relevantesten Ergebnissen, zuerst angezeigt werden (vgl. [Search engine optimization poisoning \(cyber.gc.ca\)](#)).

<sup>19</sup> [Woche 50: Rückruf mit finanziellen Folgen \(ncsc.admin.ch\)](#)

<sup>20</sup> Siehe z. B. [Woche 48: Phishing im Namen der SERAFE - Vorwand «Wohnsitz-Verifizierung» \(ncsc.admin.ch\)](#)

<sup>21</sup> [Woche 46: Wie Betrüger die SMS-Filter der Provider umgehen \(ncsc.admin.ch\)](#)

<sup>22</sup> [Woche 39: Wenn ein Phishing-Versuch auf den nächsten folgt \(ncsc.admin.ch\)](#)



**Abb. 5:** Anzahl der durch das BACS überprüften und bestätigten Phishing-URLs nach Sektorenzugehörigkeit missbrauchter Marken im zweiten Halbjahr 2025

die betrügerische Kommunikation mit sensiblen Informationen des Empfängers glaubwürdig erscheinen zu lassen. In einem anderen Versuch richteten sich die Angreifer direkt an Swisscom-Kunden. Anstelle der üblichen Rückerstattungs-E-Mails wurde in diesem Fall der Verfall angeblicher Treuepunkte vorgegaukelt. Eine aufwändig gestaltete, voll funktionsfähige Website gab vor, dass dem Empfänger oder der Empfängerin 8'517 Treuepunkte zur Verfügung stünden. Damit konnten sich die Opfer Gegenstände wie Fahrräder oder Smartphones in einen Warenkorb legen, bis die Treuepunkte aufgebraucht waren. Um die Waren einzulösen, mussten dann aber Gebühren bezahlt und sensible Daten der Opfer für die angeblichen Produkte eingegeben werden.<sup>23</sup> Diese Strategie funktioniert, denn sie nutzt die Angst der Empfängerinnen und Empfänger, eine Gelegenheit zu verpassen. Ähnliche Kampagnen wurden auch in anderen Sektoren mit ähnlichen Kundenbindungsprogrammen beobachtet. Dies beinhaltete beispielsweise Schweizer Supermärkte, Banken und auch Kreditkartenunternehmen.

### Mit Phishing zum umfassenden Datenprofil

Nebst den klassischen Phishing-Kampagnen, die auf Login-Daten oder Kreditkartendaten zielen, beobachtete das BACS zahlreiche Angriffe, bei denen die abgefragten Daten weit über Zugangsdaten hinausgingen. Die Täter erstellten in diesen Fällen Webseiten im Design vertrauenswürdiger Institutionen wie Banken, Versicherungen, Krankenkassen oder anderen Zahlungsdienstleistern. Unter dem Vorwand Daten zu verifizieren oder zu aktualisieren, wur-

<sup>23</sup> [Phishing-SMS lockt mit angeblichen Cumulus-Punkten \(cybercrimepolice.ch\)](https://www.cybercrimepolice.ch)

den die Nutzerinnen und Nutzer aufgefordert, umfangreiche persönliche Informationen preiszugeben. In einem Fall verlangten die Angreifer im Zusammenhang mit einer angeblichen Rückerstattung neben persönlichen Angaben sogar eine digitale Unterschrift.

Die Betrüger verfolgen mit diesen Angriffen das Ziel, ein möglichst vollständiges Datenprofil ihrer Opfer zu erstellen. Solche Profile sind für kriminelle Aktivitäten besonders wertvoll, da sie Identitätsdiebstahl, Social-Engineering-Angriffe oder den Weiterverkauf der Daten auf dem Schwarzmarkt ermöglichen. Je umfangreicher die Profile sind, desto höher ist deren Wert. Diese Angriffe decken sich mit der generellen Erkenntnis, dass sich Phishing-Angriffe von generischen Massennachrichten zu gezielten Angriffen verschieben: Schon eine korrekte Anrede oder Anschrift erhöht das Vertrauen des Opfers. Kennt die Täterschaft zusätzlich die Bankverbindung oder andere persönliche Lebensumstände, steigt die Wahrscheinlichkeit zusätzlich, dass die Opfer ihre Daten eingeben.

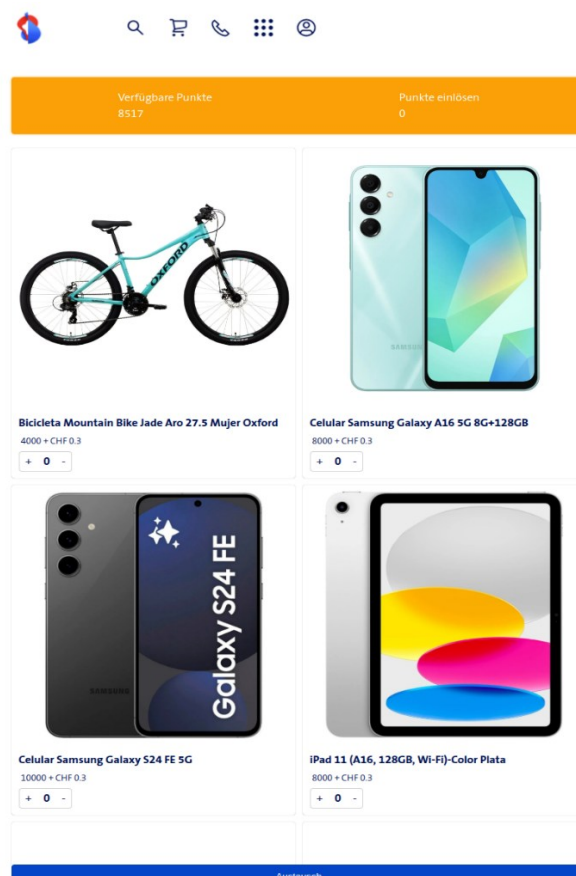


Abb. 6: Betrügerische Treuepunkte-Website im Namen der Swisscom

### Das doppelte Phishing

In der Berichtsperiode erhielt das BACS auch Meldungen neuer Varianten von aufwändigen Phishing-Angriffen, was den Trend zu mehr zielgerichteteren und raffinierteren Methoden stützt. Die Täter setzen beim doppelten Phishing (Double Phishing) auf eine mehrstufige Methode, bei der sie die erschwindelten Daten nach einem ersten erfolgreichen Phishing für ein zweites Voice-Phishing sogleich wiederverwenden: Zunächst erhielten die Opfer eine klassische Phishing-Nachricht mit einem Link zur Phishing-Seite, z. B. wegen einer angeblichen Steuerrückerstattung oder einer Parkbusse. Neben Kreditkartendaten mussten in diesen Fällen auch der Bankname und die eigene Telefonnummer angegeben werden. Nach ein paar

Minuten riefen die Täter auf die zuvor angegebene Telefonnummer des Opfers an und gaben sich als vermeintliche Sicherheitsabteilung des Finanzinstituts aus. Sie behaupteten, dass das Konto soeben gehackt worden oder Geld abgeflossen sei. Um das Konto zu schützen, müsse ihnen nun das Opfer sofort Zugriff auf den Computer via Fernzugriffs-Tool gewähren. In Wirklichkeit nutzten die Angreifer den Zugriff aber, um Transaktionen auf dem E-Banking-Konto des Opfers auszuführen.

Dank verstärkter Sicherheitsmassnahmen seitens der Banken sind direkte Angriffe auf E-Banking-Konten selten geworden. Daher bringen die Täter die Opfer dazu, ihnen selbst die Kontrolle über das E-Banking zu übergeben, wodurch gängige Sicherheitsmassnahmen ausgehebelt werden. Für die Opfer erscheint der Anruf plausibel, da der Sicherheitsvorfall durch das erste Phishing tatsächlich stattgefunden hat. Diese Variante zeigt zudem, dass Betrüger schriftliche und telefonische Angriffe kombinieren, um glaubwürdiger zu erscheinen und ihren Gewinn zu maximieren. Ähnliche Vorgehensweisen wurden auch bei Parkbussen-Phishings und Kleinanzeigen-Verkäufen beobachtet. Jedoch ist die Sprache bei solchen telefonischen Angriffsversuchen immer noch ein Hindernis. In einem Fall konnten die Angreifer ausschliesslich in Französisch kommunizieren. Gerade durch den Einsatz von künstlicher Intelligenz (KI) ist jedoch zu erwarten, dass Sprachkenntnisse bei Telefonanrufen künftig irrelevanter werden, da solche Anrufe mithilfe von Simultanübersetzungs-Tools getätigt werden können.

### **SMS-Blaster**

Ende Sommer 2025 wurde in der Schweiz erstmals eine neue Verbreitungsform für Phishing und Betrug beobachtet: der SMS-Blaster.<sup>24</sup> Obwohl diese Methode in Teilen Europas und Asiens bereits bekannt ist, stellt sie in der Schweiz eine neue Art der Verbreitung dar und erfordert für die Mitigation eine enge Zusammenarbeit zwischen Behörden und Telekomanbieter. Technisch handelt es sich beim SMS-Blaster um ein portables, taschengrosses Gerät, das sich als Mobilfunkantenne ausgibt und Mobiltelefone in der Nähe dazu bringt, sich mit ihm zu verbinden. Nach Verbindungsaufbau wird das Zielgerät auf das veraltete 2G-Protokoll herabgestuft. Im 2G-Modus nutzen die Angreifer dann eine bekannte Schwachstelle – eine sogenannte «Null-Cipher» – aus, damit SMS-Nachrichten ohne die üblichen Prüfungen und ohne Beteiligung des legitimen Mobilfunkanbieters zugestellt werden können. Dadurch können die Angreifer Smishing-Nachrichten an Mobilgeräte in einem Umkreis von bis zu einem Kilometer zustellen und umgehen so die standardmässigen, vom Netzbetreiber gepflegten Blockfilter und -mechanismen zur Erkennung und Abwehr von Phishing. Die Inhalte der übermittelten SMS und die verlinkten Websites entsprechen den beim BACS bereits bekannten Phishing-Mustern wie beispielsweise die Nachahmung von Lieferdiensten, Androhung von Geldstrafen oder Lockangeboten mit Prämienpunkten, um Zugangsdaten oder Kreditkarteninformationen abzugreifen.

### **Empfehlungen**

Aktivieren Sie wo immer möglich die Multi-Faktor-Authentisierung (MFA) als zusätzliche Sicherheit Ihrer Konten. Obwohl MFA das Risiko für eine Kompromittierung reduziert, kann auch

<sup>24</sup> [Woche 46: Wie Betrüger die SMS-Filter der Provider umgehen \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/woche-46)





immer gewinnbringend für sie ist. Die Angreifer gehen immer noch hauptsächlich opportunistisch vor. Sie versuchen, die Geräte einer möglichst grossen Anzahl von Nutzenden zu infizieren, ohne dabei eine Bevölkerungsgruppe oder Branche spezifisch ins Visier zu nehmen. In bestimmten Fällen lassen sich jedoch punktuelle Anpassungen erkennen, die die Glaubwürdigkeit bei Schweizer Opfern erhöhen sollen.

So wurden in mehreren Fällen falsche Rechnungen per E-Mail verschickt, die angeblich von einem in der Schweiz aktiven Inkassounternehmen stammten. Die E-Mails verwiesen zur Zahlung auf eine angehängte QR-Rechnung. Der Anhang – eine HTML-Datei – zeigt beim Öffnen eine Fehlermeldung, dass aufgrund eines deaktivierten JavaScripts das PDF nicht angezeigt werden könne. Daher müsse nun die Nutzerin oder der Nutzer die Tastenkombination «Windows+R» gefolgt von «Ctrl+V» drücken. Entsprechend der ClickFix-Methode startet dies ein zuvor in die Zwischenablage kopiertes böses Skript und führt zur Installation der Schadsoftware.<sup>28</sup> Das BACS erhielt ebenfalls mehrere Meldungen im Zusammenhang mit Kleinanzeigen-Portalen. Die Kriminellen gaben sich als Käuferinnen oder Käufer in Eile aus. Sie behaupteten, bereits eine Zahlung geleistet zu haben und fügten der E-Mail eine Datei mit dem Namen «twint-rechnung.zip» an. Diese Datei enthielt eine auf den Diebstahl von Personen- oder Finanzdaten spezialisierte Schadsoftware («Infostealer»), die hauptsächlich im Browser gespeicherte Zugangsdaten ausliest.<sup>29</sup> Weiter fanden mehrere Angriffe über gefälschte Rekrutierungsprozesse statt, hauptsächlich über LinkedIn.<sup>30</sup> In einem Fall wurde beim Hochladen eines Bewerbungsvideos ein technisches Problem vorgetäuscht. Der Bewerber wurde daraufhin aufgefordert, einen in seine Zwischenablage kopierten Befehl auszuführen. Auch dabei handelte es sich um eine Variante von ClickFix. In einem anderen Fall musste ein Bewerber im Rahmen eines vermeintlichen Bewerbungsprozesses Dateien für eine Programmieraufgabe herunterladen. Diese enthielten jedoch einen Schadcode, der vertrauliche Daten vom Computer des Opfers stahl. Diese beiden zuletzt beschriebenen Vorgehensweisen werden auch international regelmässig beobachtet und gelten als typische Methoden staatlich gesteuerter nordkoreanischer Gruppen (vgl. Kap. 8). Sie zielen besonders auf Mitarbeitende von Unternehmen, die im Bereich Kryptowährungen oder Blockchain tätig sind – auch in der Schweiz.<sup>31</sup>

Parallel zu diesen gezielten Angriffen wurden zahlreiche Vorfälle im Zusammenhang mit internationalen Kampagnen beobachtet, deren Ziel nicht spezifisch die Schweiz war. Schädliche Werbung in Suchmaschinenergebnissen («Malvertising»)<sup>32</sup> wird vom BACS weiterhin festgestellt. Bei einem Vorfall kam es über diesen Angriffsvektor zu einer Infektion, die schliesslich in einen Ransomware-Angriff mündete.<sup>33</sup> Weitere Kampagnen machten sich scheinbar nützlich

---

<sup>28</sup> [Woche 33: Angreifer setzen bei der Verteilung von Schadsoftware auf Social Engineering \(ncsc.admin.ch\)](#)

<sup>29</sup> [Woche 40: Kleinanzeigen-Phishing – Angreifer verteilen neu Schadsoftware statt nur Phishing-Links \(ncsc.admin.ch\)](#)

<sup>30</sup> [Woche 49: Verlockende Jobs, versteckte Risiken – So tappen Stellensuchende in die Malware-Falle \(ncsc.admin.ch\)](#)

<sup>31</sup> [Analysis of Contagious Interview Campaigns by North Korean Threat Actors \(sentinelone.com\)](#)

<sup>32</sup> Siehe [Halbjahresbericht 2025/1, Kap. 3.3.](#)

<sup>33</sup> [From Bing Search to Ransomware: Bumblebee and AdaptixC2 Deliver Akira \(thedfirreport.com\)](#)

che Software wie z. B. einen PDF-Editor als Tarnung zunutze, um Malware zu verteilen. Tatsächlich aber aktivierte sich der Schadcode erst nach mehreren Monaten der Installation und der einwandfreien Funktionalität, weshalb die Applikation als legitim wahrgenommen wurde.<sup>34</sup>

Ausserdem gab es mehrere Angriffe auf die Software-Lieferkette. In diesen Fällen wurden Konten von Packet-Verwaltern auf Open-Source-Entwicklungsplattformen (z. B. GitHub und npm) kompromittiert, wodurch die Angreifer bösartigen Code in weitverbreiteten Komponenten einschleusen konnten. Zu diesen Vorfällen zählen einerseits die Kompromittierung des Kontos des Entwicklers «Qix», wodurch manipulierte Versionen von Dutzenden gängigen Bibliotheken veröffentlicht werden konnten.<sup>35</sup> Andererseits veränderten Angreifer bei der grossangelegten Kampagne «Shai-Hulud 2.0» Hunderte von Komponenten aus Open-Source-Projekten derart, dass sie bei ihrer Installation automatisch bösartigen Code ausführten.<sup>36</sup> Letztere Kampagne ermöglichte es den Angreifern, sensible Daten zu stehlen und sich mithilfe kompromittierter Anmeldedaten von einem Entwicklerkonto zum nächsten zu bewegen.



### Empfehlungen

Klicken Sie in verdächtigen Nachrichten keine Links an, öffnen Sie keine angefügten Dateien und scannen Sie keine QR-Codes. Fragen Sie im Zweifelsfall über andere etablierte Kanäle beim vermeintlichen Absender nach, ob die Nachricht tatsächlich von ihm stammt. Seien Sie immer vorsichtig, wenn sich ein Download-Fenster öffnet.

Verifizieren Sie bei der Suche nach Software im Internet vor dem Download, dass Sie sich auf den Websites der Hersteller oder einer anderen vertrauenswürdigen Website befinden. Beachten Sie besonders beim Nutzen von Suchmaschinen, ob die angezeigte Website als bezahlte Werbung deklariert ist oder nicht. Wenn es sich um bezahlte Werbung handelt, ist Vorsicht geboten. Angreifer setzen oft auf diese Methode, um bei Suchergebnissen zuoberst platziert zu sein.

Patchen Sie regelmässig Ihre Systeme und schränken Sie Zugänge so weit als möglich ein. Besteht der Verdacht einer Infektion, lassen Sie den Computer unverzüglich von einer Fachperson untersuchen und gegebenenfalls säubern. Die sicherste Variante ist, den Computer vollständig neu aufzusetzen. Vergessen Sie dabei aber nicht, alle persönlichen Daten vorher zu sichern.

## 3.2 Ransomware

Ransomware umschreibt eine Angriffsart, bei welcher Angreifer mithilfe einer Schadsoftware Daten auf den IT-Systemen des Opfers verschlüsseln und diese somit für das Opfer unbrauchbar machen.<sup>37</sup> In der Regel entnehmen die Angreifer vor der Verschlüsselung eine Kopie der

<sup>34</sup> [TamperedChef: Malvertising to Credential Theft \(labs.withsecure.com\)](https://labs.withsecure.com)

<sup>35</sup> [Dev snared in crypto phishing net, 18 npm packages compromised \(theregister.com\)](https://theregister.com)

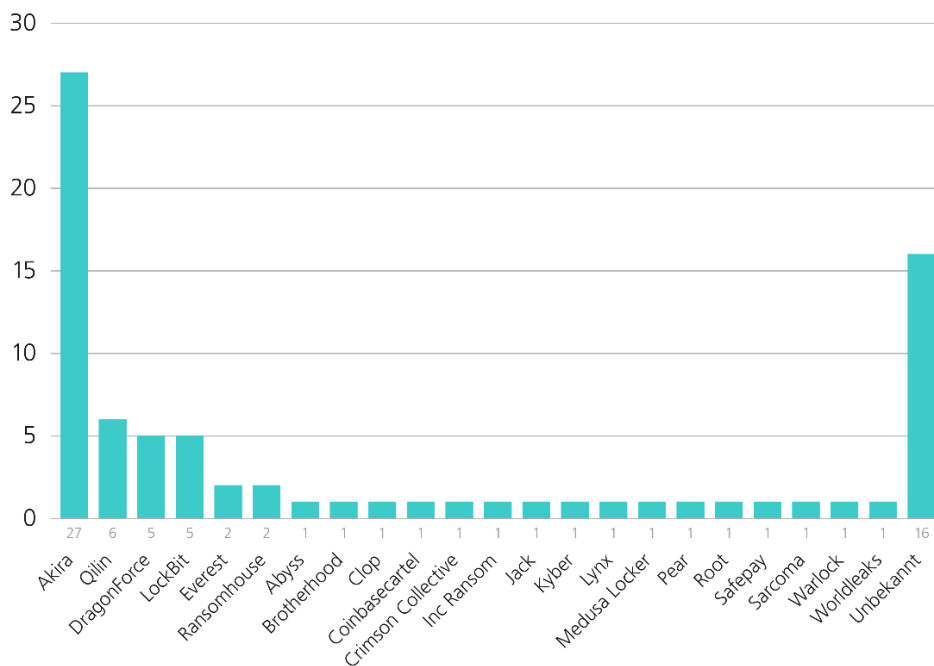
<sup>36</sup> [Shai-Hulud 2.0 Supply Chain Attack \(wiz.io\)](https://wiz.io)

<sup>37</sup> [Ransomware \(ncsc.admin.ch\)](https://ncsc.admin.ch)

Daten und fordern nach der Verschlüsselung vom Opfer ein Lösegeld. Wenn das Opfer zahlt, stellen die Kriminellen ein Entschlüsselungs-Tool (Dekryptor) in Aussicht. Wenn das Opfer nicht auf die Forderungen reagiert, drohen die Angreifer mit der Veröffentlichung der gestohlenen Daten. Zudem versuchen die Ransomware-Gruppen häufig, den Druck zusätzlich zu erhöhen, um das Opfer doch noch zu einer Zahlung zu bewegen. Dies kann z. B. die Kontaktaufnahme mit Kunden und Lieferanten des Opfers beinhalten, um diese ebenfalls mit der Veröffentlichung der gestohlenen Daten zu erpressen.

Im zweiten Halbjahr 2025 verzeichnete das BACS 79 Ransomware-Vorfälle bei Schweizer Organisationen (vgl. Abb. 7). Die statistische Zunahme verglichen zu 57 Meldungen im ersten Halbjahr 2025 oder den 47 Fällen des zweiten Halbjahres 2024 begründet sich auf einer Anpassung der BACS-internen Erfassungsmethode. Der vorliegende Bericht berücksichtigt nun nicht mehr nur die bei der Nationalen Anlaufstelle Cyberrisiken des BACS freiwillig gemeldeten Vorfälle (47), sondern auch die aufgrund der Meldepflicht für Cyberangriffe auf kritische Infrastrukturen gemeldeten Fälle (10) sowie Ransomware-Vorfälle, von denen das BACS über nationale Partner Kenntnis (22) erhalten hat. Daher blieb die Anzahl der bei der Nationalen Anlaufstelle Cyberrisiken des BACS freiwillig gemeldeten Vorfälle konstant. Die tatsächliche Anzahl Ransomware-Vorfälle in der Schweiz ist wahrscheinlich trotzdem noch höher als die gesamthaft vom BACS beobachteten 79 Vorfälle, da nicht alle betroffenen Organisationen einen Vorfall melden oder dieser nicht öffentlich bekannt wird.

Die aktivste Ransomware-Gruppe in der Schweiz war auch im zweiten Halbjahr 2025 «Akira». Sie war bereits im ersten Halbjahr 2025 führend und intensivierte ihre Aktivitäten von 7 auf 26



**Abb. 7:** Anzahl der dem BACS gemeldeten und beobachteten Erpressungsvorfälle im Kontext operierender Ransomware-Gruppen im zweiten Halbjahr 2025

dem BACS bekannte Angriffe.<sup>38</sup> Akira gehört international zu den aktivsten Ransomware-Gruppen, wobei sie Organisationen aller Grössen und Sektoren angreift. Im Berichtszeitraum betrafen Angriffe dieser Gruppe insbesondere Organisationen, die SonicWall-Geräte einsetzen, weshalb anfänglich von der Ausnutzung einer «Zero-Day»-Schwachstelle ausgegangen wurde (vgl. Kap. 4). Die Angreifer nutzten jedoch eine ältere Schwachstelle, die bereits im August 2024 aufgedeckt worden ist und für die ein Sicherheits-Update zur Verfügung steht. Zahlreiche Organisationen befolgten aber die entsprechenden Korrekturanweisungen nicht vollständig. Akira konnte sich deshalb – dank noch immer gültiger Verbindungsdaten – mit weitgehenden Rechten einen Erstzugang verschaffen, was die Verbreitung ihrer Ransomware vereinfachte.<sup>39</sup>

«Qilin», «DragonForce» und «LockBit» zählen mit jeweils fünf bis sechs erfolgreichen Angriffen ebenfalls zu den aktivsten Gruppen in der Schweiz. Im September 2025 verkündete DragonForce, dass diese drei Gruppen eine Allianz schliessen würden. Drei Monate später schien dies jedoch eher eine Strategie zur Gewinnung neuer Beteiligter («Affiliates») zu sein, als eine tatsächliche operative Zusammenarbeit.<sup>40</sup> Qilin beansprucht global mehr als 700 Angriffe im Berichtszeitraum für sich, womit Qilin weltweit die aktivste Gruppe darstellt. Das hohe Aktivitätsniveau hängt mit dem «Ransomware-as-a-Service»-Modell (RaaS) zusammen. Die Entwicklerinnen und Entwickler der Ransomware stellen dabei eine gebrauchsfertige Plattform bereit. Mithilfe dieser können Beteiligte gegen Abgabe eines Teils des Lösegelds Ransomware-Angriffe durchführen, Daten abgreifen und veröffentlichen sowie Verhandlungen führen. Die besonders hohe Zahl von Opfern der Gruppe Qilin lässt darauf schliessen, dass ihr RaaS-Modell von den Beteiligten als attraktiv angesehen wird.<sup>41</sup> Die Gruppe hat beispielsweise einen Rechtsdienst eingerichtet, der gestohlene Daten im Kontext gesetzlicher Richtlinien analysiert. So können Qilins Partner den Druck bei Verhandlungen erhöhen, indem sie auf die Risiken bei Nichteinhaltung des geltenden Rechts und möglicher Strafverfolgungen hinweisen. Die Aktivität der Gruppe LockBit nahm im Jahr 2025 aufgrund mehrerer internationaler Strafverfolgungsoperationen und interner Datenlecks stark ab.<sup>42</sup> Im September 2025 kündigten die Verantwortlichen eine neue Version ihrer Ransomware «LockBit 5.0» an. Über 100 angekündigte Opfer, darunter eines in der Schweiz, wurden allein im Dezember 2025 dieser Version zugeschrieben. Dies kann bedeuten, dass die Gruppe neue Beteiligte rekrutieren und ihre Operationen erneut aufnehmen konnte.

Im Berichtszeitraum zeigten mehrere grössere Vorfälle auf internationaler Ebene das mögliche Ausmass von Ransomware-Angriffen auf. Im Vereinigten Königreich beispielsweise verursachte ein Vorfall bei Jaguar Land Rover einen Produktionsstopp von mehreren Wochen, was sich auf über 5'000 Unternehmen der Lieferkette auswirkte. Eine direkte Intervention der britischen Regierung in Form einer Kreditgarantie von GBP 1,5 Milliarden war erforderlich und der gesamte wirtschaftliche Schaden beläuft sich schätzungsweise auf knapp GBP 1,9 Milliarden.<sup>43</sup> Auch weitere Organisationen wie beispielsweise Collins Aerospace waren von Ransom-

---

<sup>38</sup> [Cyberkriminalität: Hackergruppe AKIRA intensiviert ihre Aktivitäten \(admin.ch\)](#)

<sup>39</sup> [Akira Ransomware Group Utilizing SonicWall Devices for Initial Access \(rapid7.com\)](#)

<sup>40</sup> [In depth analysis of the alleged Qilin, DragonForce and LockBit alliance \(yarix.com\)](#)

<sup>41</sup> [The Evolution of Qilin RaaS \(sans.org\)](#)

<sup>42</sup> Siehe [Halbjahresbericht 2025/1](#), Kap. 3.2.

<sup>43</sup> [Jaguar Land Rover cyberattack cost \\$2.5 billion, says monitoring group \(therecord.media\)](#)

ware betroffen, wobei die Kompromittierung in mehreren europäischen Flughäfen den Flugverkehr störte. Unter anderem betraf dies ein von zahlreichen Fluggesellschaften verwendetes Check-in-System, welches wegen des Cyberangriffs während mehrerer Tage nicht verfügbar war.<sup>44</sup>

In der Schweiz wurde im Berichtszeitraum kein Vorfall solchen Ausmasses beobachtet. Die Bedrohung durch Ransomware bleibt jedoch hoch und wird durch Gruppen verstärkt, die Schwachstellen oder kompromittierte Zugänge rasch ausnutzen können. Auch wenn keine der bekannten Gruppen spezifisch auf die Schweiz zielt, sind opportunistische Angriffe die Norm und treffen deshalb auch Schweizer Organisationen.



### Empfehlungen

Auf der Website des BACS finden Sie eine [Auflistung von präventiven Massnahmen](#) zum Schutz vor Ransomware sowie [Handlungsanweisungen für den Ereignisfall](#). Die Schulung und das Training der Mitarbeitenden in Bezug auf IT-Ausfälle sind essenziell, um im Ernstfall eine schnelle und effektive Reaktion zu gewährleisten. Insbesondere sollte die Erreichbarkeit der Mitarbeitenden und der Kunden auf einem alternativen Kanal (z. B. telefonisch oder mittels Messenger-Dienst) sichergestellt werden. Generell raten das BACS und seine internationalen Partner<sup>45</sup> den Opfern von Ransomware ab, Lösegeld zu zahlen. Es besteht keine Garantie, dass Cyberkriminelle ihr Wort halten. Mit einer Lösegeldzahlung werden die Cyberkriminellen finanziell unterstützt, um ihre Strukturen weiter auszubauen und weitere Angriffe auszuführen.

### 3.3 Verdeckte ORB-Netzwerke in der Schweiz

Die zunehmende Bedrohung durch verdeckte Proxy-Netzwerke, sogenannte ORB-Netzwerke («Operational Relay Boxes»)<sup>46</sup>, wird auch in der Schweiz beobachtet. Die Anzahl kompromittierter Geräte, die Teil solcher Netzwerke sind, wächst kontinuierlich. Es wurden mehrere bösartige Aktivitäten festgestellt, die von diesen Infrastrukturen ausgehen und sich gegen Schweizer Systeme oder Organisationen richten. Abgesehen davon können Angreifer unentdeckt in das Privatleben der Besitzer der infizierten Geräte eindringen.

Ein ORB-Netzwerk besteht aus kompromittierten Routern und anderen vernetzten Objekten. Häufig handelt es sich z. B. um kompromittierte Server und Router von Privatpersonen und Kleinunternehmen sowie um infizierte Geräte aus dem Bereich des Internets der Dinge (IoT). In den vergangenen Jahren sind Netzwerke, die früher überwiegend aus gemieteter Server-Infrastruktur bestanden, zunehmend zur Ausnahme geworden. Stattdessen basieren die heute am weitesten verbreiteten und exponierten ORB-Netzwerke auf einem grossen Bestand kompromittierter Endgeräte, die über eine kleinere Anzahl gemieteter Server erreichbar gemacht werden und so verwaltet werden können.

---

<sup>44</sup> [Ransomware behind global airport outage, says ENISA \(theregister.com\)](#)

<sup>45</sup> [Guidance for organisations considering payment in ransomware incidents \(ncsc.gov.uk\)](#)

<sup>46</sup> Siehe [Halbjahresbericht 2025/1](#), Kap. 8.1 und [Halbjahresbericht 2024/2](#), Kap. 8.1. sowie [IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders \(cloud.google.com\)](#)

Diese Netzwerke werden häufig von spezialisierten Organisationen im Auftrag aufgebaut und betrieben. Sie bieten Dritten die entsprechenden Infrastrukturen für ein Entgelt zur Nutzung an («Proxy-Network-as-a-Service»). Dadurch können Bedrohungsakteure die Herkunft ihrer Aktivitäten effektiv verschleiern, Erkennungsmechanismen umgehen und ihre Operationen mit geringem operativem Risiko skalieren. ORB-Netzwerke unterscheiden sich von klassischen kriminellen Botnetzen insbesondere durch ihren starken Fokus auf Tarnung, Widerstandsfähigkeit und Skalierbarkeit, die gezielt auf die Anforderungen fortgeschrittener – auch staatlicher – Bedrohungsakteure<sup>47</sup> zugeschnitten sind.



### Empfehlungen

ORB-Netzwerke sind in hohem Masse auf infizierte Geräte angewiesen. Deshalb ist es entscheidend, dass Sie Massnahmen ergreifen, um das Risiko einer Kompromittierung zu reduzieren und zu verhindern, dass Ihre Systeme ungewollt Teil krimineller Infrastrukturen werden. Die folgenden Sicherheitsmassnahmen sind daher dringend empfohlen:

- Zeitnahes Einspielen von Sicherheits-Updates für internetverbundene Geräte;
- Aktivieren automatischer Updates;
- Starke Passwörter und Multi-Faktor-Authentisierung (MFA) – wo immer möglich – verwenden;
- Dienste und offene Ports sollten nur dann aus dem Internet erreichbar sein, wenn dies zwingend erforderlich ist;
- Sofern nicht benötigt: «Universal-Plug-and-Play» (UPnP) deaktivieren.

Die konsequente Umsetzung dieser Massnahmen reduziert die Angriffsfläche erheblich und trägt dazu bei, das Wachstum und die Effektivität verdeckter Proxy-Netzwerke einzudämmen.

## 4 Schwachstellen

Eine Schwachstelle bezeichnet eine Sicherheitslücke in einem IT-System. Dabei kann es sich um Software- oder Design-Schwachstellen, aber auch um einen schlecht konfigurierten Schutz wie z. B. bei Standardpasswörtern handeln.<sup>48</sup> Besonders herausfordernd sind dabei «Zero-Day»-Schwachstellen. Dabei handelt es sich um bereits entdeckte Schwachstellen, für die aber noch kein offizieller Sicherheits-Patch des Herstellers zur Verfügung steht und die somit von den Angreifern ausgenutzt werden können. Besonders durch die zunehmende Digitalisierung und die Vernetzung von Geräten kann die Ausnützung einzelner Schwachstellen oder deren Verkettung zu Schäden durch die anschliessende Kompromittierung von Daten und Systemen führen.

---

<sup>47</sup> Siehe z. B. [Halbjahresbericht 2024/2](#), Kap. 8.1.

<sup>48</sup> [Schwachstelle \(ncsc.admin.ch\)](https://www.ncsc.admin.ch)

Im Bereich der Schwachstellen zeigte sich im zweiten Halbjahr 2025 eine hohe Dynamik. Diese manifestierte sich in Vorfällen, die im Zusammenhang mit Cyberangriffen über die Software-Lieferkette («Supply Chain») standen. Moderne Software-Produkte basieren zu einem grossen Teil auf externen Programm-Bibliotheken und vorgefertigten Komponenten. Diese Vorgehensweise erlaubt eine effiziente Entwicklung, da nicht jede Funktion von Grund auf neu programmiert werden muss. Daraus ergeben sich jedoch komplexe technische Abhängigkeiten. Wenn eine dieser im Code verankerten Bibliotheken eine Sicherheitslücke aufweist, sind potenziell alle Anwendungen verwundbar, die diese Komponente nutzen.

Ein konkretes Beispiel hierfür lieferten die Vorfälle im Umfeld der Entwicklerplattform Node Package Manager (npm), bei denen Angreifer diesen Hebel in den beiden «Shai-Hulud»-Kampagnen im September und November 2025 gezielt missbrauchten (vgl. Kap. 3.1). In der zweiten Welle wurden dabei mehrere hundert npm-Pakete infiziert, die wiederum in monatlichen Downloads im dreistelligen Millionenbereich weiterverbreitet wurden. Die Schadsoftware durchsucht unter anderem die übernommenen Code-Repositories nach Zugangsdaten und publiziert diese mit dem Konto des Opfers.<sup>49</sup> Für IT-Verantwortliche in Unternehmen stellt dies eine besondere Herausforderung dar: Herkömmliche Inventarisierungssysteme oder Asset-Management-Lösungen erfassen meist nur die installierte Endanwendung und listen die darin enthaltenen Fremdkomponenten nicht einzeln auf. Dadurch bleibt das tatsächliche Risiko oft unsichtbar und kann durch den Anwender kaum direkt gemanagt werden.

In der Folge besteht eine starke Abhängigkeit von der Sorgfalt der Software-Hersteller. Diese stehen in der Pflicht, ihre verwendeten Komponenten transparent zu dokumentieren und kontinuierlich auf Schwachstellen zu prüfen. Nur wenn Entwickler ihre Abhängigkeiten kennen und bei Bekanntwerden einer Lücke unverzüglich bereinigte Updates bereitstellen, lässt sich die Sicherheit für die Endkunden gewährleisten. Ohne diese proaktive Pflege der Lieferkette bleibt das Risiko für die Anwender kaum kontrollierbar. Denn schon reguläre Schwachstellen stellen sie bereits vor Probleme. So wurde das BACS in der zweiten Julihälfte auf die massenhafte Ausnutzung einer Schwachstelle in der Datenmanagement-Plattform SharePoint aufmerksam, die auch viele Schweizer Organisationen betraf. Wie eine spätere Analyse des Herstellers<sup>50</sup> aufzeigte, nutzen sowohl staatliche wie kriminelle Akteure diese Schwachstelle, um sich Zugang zu Organisationen mit verwundbaren Systemen zu verschaffen (vgl. Kap. 8.1).

## Empfehlungen

Lassen Sie Programme, wenn immer möglich, automatisch aktualisieren. Ansonsten verwenden Sie die integrierte Update-Funktion oder laden Sie die neueste Version direkt beim Hersteller herunter.

Besonders für Unternehmen ist es wichtig, ein etabliertes Patch-Management einzurichten, um Schwachstellen zeitgerecht zu beheben. Eine Grundvoraussetzung hierfür ist ein aktuelles Inventar der Infrastruktur und der eingesetzten Produkte (SBOM-Liste<sup>51</sup>). Priorisieren Sie besonders jene Sicherheitslücken in Internet-exponierten Teilen Ihrer Infrastruktur. Führen Sie

<sup>49</sup> [Shai-Hulud 2.0 Aftermath: Trends, Victimology and Impact \(wiz.io\)](https://wiz.io)

<sup>50</sup> [Disrupting active exploitation of on-premises SharePoint vulnerabilities \(microsoft.com\)](https://microsoft.com)

<sup>51</sup> [Software-Lieferkette \(wikipedia.org\)](https://wikipedia.org)



regelmässig Penetrationstests und Schwachstellen-Scans durch, um potenzielle Sicherheitslücken proaktiv zu identifizieren. Software oder Systeme, welche vom Hersteller nicht mehr unterstützt werden («End of Life», EOL) sollten abgeschaltet oder – wenn möglich – in eine separate, abgeschottete Netzwerkzone verlegt werden. Nutzen Sie zudem ein Monitoring und verfügbare Bedrohungsinformationen («Threat Intelligence»), um auf relevante Entwicklungen zeitnah reagieren zu können. Die Echtzeitüberwachung Ihrer Infrastruktur gepaart mit den Möglichkeiten der Automatisierung helfen Ihnen bei der zeitnahen Erkennung von Angriffsversuchen und Anomalien. Auch flankierende Massnahmen wie der Einsatz von «Red Teaming»<sup>52</sup>, regelmässige Sicherheitsprüfungen oder der Betrieb eines Bug-Bounty-Programms können helfen, die Wirksamkeit der eigenen Sicherheitsprozesse kontinuierlich zu bewerten und zu verbessern.

## 5 Betrug und Social Engineering

Betrug ist die vorsätzliche Täuschung einer Person mit dem Ziel, sich selbst oder jemand anderes unrechtmässig zu bereichern, wodurch das Opfer materiellen Schaden erleidet.<sup>53</sup> Im digitalen Raum besteht die Herausforderung besonders darin, dass Kriminelle aus der Ferne operieren können. Häufig agieren Cyberkriminelle aus Ländern heraus, in denen sich die Strafverfolgung schwierig gestaltet. In der Regel verwenden Cyberbetrüger keine ausgeklügelten Cyberangriffstechniken, sondern sie versuchen, potenzielle Opfer zu manipulieren (Social Engineering<sup>54</sup>). Sie bringen das Opfer auf zwischenmenschlicher Ebene dazu, selbst einige der notwendigen Schritte des Betrugsablaufs auszuführen.

Betrug bleibt auch im zweiten Halbjahr 2025 das dominierende Phänomen der beim BACS freiwillig getätigten Meldungen – trotz eines Rückgangs von 18'269 im zweiten Halbjahr 2024 auf 15'090 Meldungen. Dies hängt vor allem mit einer signifikanten Abnahme von betrügerischen Drohanrufen im Namen von Behörden zusammen, die seit Mitte 2023 einen wesentlichen Bestandteil aller Betrugsmeldungen darstellen. Diese Meldungen reduzierten sich von 8'173 in der Vorhalbjahresperiode auf 5'941 Meldungen im Berichtszeitraum. Dies impliziert einen stabilen, abnehmenden Trend<sup>55</sup>, wobei betrügerische Anrufe noch immer mit 39.4 Prozent den grössten Anteil in der Kategorie aufweisen.

Mit 11 Prozent bleiben «betrügerische Gewinnspiele» im Namen bekannter Firmen das am zweithäufigsten gemeldete Betrugsphänomen (1'698). Dabei handelt es sich um Nachrichten, die falsche Gewinnversprechen beispielsweise für technische Geräte, Werkzeuge oder Gut-

---

<sup>52</sup> Das «Red Team» ist eine unabhängige Gruppe, die bei einer Organisation in der Rolle eines potenziellen Angreifers die Infrastruktur und ihre Prozesse unter realen Bedingungen überprüft. Ziel ist es, die bestehende Sicherheitslücke vor einem richtigen Cyberangriff aufzudecken und sie so zeitnah schliessen zu können (vgl. [Red Team \(wikipedia.org\)](https://de.wikipedia.org/wiki/Red_Team)).

<sup>53</sup> Siehe für eine rechtliche Definition Art. [146 StGB \(Strafgesetzbuch\)](#)

<sup>54</sup> [Social Engineering \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/social-engineering)

<sup>55</sup> Siehe [Halbjahresbericht 2025/1](#); Kap. 5.

scheine enthalten. Häufig werden diese im Namen von bekannten Lebensmittel- oder Detailhändlern versendet. Die vermeintlichen Gewinner landen anschliessend auf einer Webseite, auf der sie ihre Kreditkartendaten eingeben müssen und unbewusst ein Abonnement abschliessen. Am dritthäufigsten wurden gefälschte E-Mails im Namen von Behörden (1'436) gemeldet, gefolgt von Vorschussbetrug (1'243). Bezüglich «Fake-Sextortion»-E-Mails ist der Meldeeingang rückläufig – von 1'209 Meldungen im zweiten Halbjahr 2024 auf 837 in der Berichtsperiode. Trotzdem kann keine nachhaltige Reduktion bei diesem Phänomen erwartet werden, da Fake-Sextortion-E-Mails in Wellen versandt werden. Eine zunehmende Entwicklung ist bei den betrügerischen Webshops zu beobachten. Im zweiten Halbjahr wurden 824 Meldungen verzeichnet, das sind 266 mehr als noch im ersten Halbjahr. Auffallend bei diesem Phänomen ist die Häufung der Meldungen jeweils zwischen November und Januar, denn die Betrüger wollen vom Weihnachtsgeschäft profitieren. Im Gegensatz dazu hat der Meldeeingang von Kleinanzeigenbetrug von 553 im zweiten Halbjahr 2024 auf 462 in der aktuellen Berichtsperiode leicht abgenommen und bleibt auch im Jahresvergleich relativ stabil. Die Meldungen mit den höchsten Schadenssummen betreffen weiterhin das Phänomen Online-Anlagebetrug. Verglichen mit der zweiten Jahreshälfte 2024 haben sich die Zahlen um rund 100 Meldungen erhöht. Mit 418 Meldungen im ersten und 430 Meldungen im zweiten Halbjahr bleibt der Meldeeingang über das Jahr 2025 relativ konstant. Gestiegen sind hingegen die nachgelagerten Betrugsversuche, die den Opfern eine Rückerstattung des gestohlenen Geldes versprechen. Während in der ersten Jahreshälfte 2025 145 Meldungen zu dieser Betrugsform des «Rückforderungsbetrugs» eingingen<sup>56</sup>, waren es in der aktuellen Berichtsperiode mit 325 Meldungen mehr als doppelt so viele.

### **Betrugsdelikte mit Fokus auf Unternehmen**

Unternehmen meldeten im zweiten Halbjahr deutlich weniger Fälle im Kontext von CEO-Betrug als im ersten Halbjahr. Nach einem Rekordwert von 605 Meldungen in den ersten sechs Monaten von 2025 wurden nur noch 366 Fälle registriert. Auch verglichen mit dem zweiten Halbjahr 2024 ist der Meldeeingang um 68 Fälle gesunken. Verantwortlich für den markanten Rückgang ist das Ausbleiben von Betrugswellen gegen Schulen, Gemeinden und Kirchen, welche in der ersten Jahreshälfte noch typisch waren. Meldungen zu Rechnungsmanipulation («Business-E-Mail-Compromise», BEC)<sup>57</sup> stiegen hingegen wiederum an, gegenüber 49 im zweiten Halbjahr 2024 auf 73 Fälle im zweiten Halbjahr 2025. Konträr zum CEO-Betrug stammen die Daten, die für den Betrugsversuch verwendet werden, nicht aus öffentlichen Quellen, sondern aus gehackten E-Mail-Konten. Diese stehen meist im Zusammenhang mit vorgängigen Phishing-Versuchen gegen Angestellte des Unternehmens, wie z. B. «Chain-Phishing»<sup>58</sup> (vgl. Kap. 2). Wenn ein neues E-Mail-Konto gehackt werden konnte, durchsuchen die Angreifer dieses nach verwertbaren Inhalten. Beim Auffinden von z. B. Kundenbestellungen oder -

---

<sup>56</sup> Siehe [Halbjahresbericht 2025/1](#); Kap. 5, Abs. zu Rückforderungsbetrug.

<sup>57</sup> International wird das Phänomen «Business-E-Mail-Compromise» (BEC) nicht einheitlich verwendet, weshalb in anderen Definitionen z. B. der CEO-Betrug als Unterform des BECs verstanden wird (vgl. [Business Email Compromise \(fbi.gov\)](#)). Das BACS unterscheidet die beiden Phänomene aber explizit und folgt der Definition des Bundesamts für Polizei (fedpol).

<sup>58</sup> Chain-Phishing ist eine schneeballartige Verteilung von Spam oder Phishing-Nachrichten, bei der nach der Kompromittierung des E-Mail-Postfachs sofort Phishing-Nachrichten an alle Kontakte im gesamten Adressbuch versendet werden.

rechnungen manipulieren sie die Kommunikation mit dem Geschäftskunden, so dass dieser den offenen Betrag an eine IBAN-Kontonummer unter der Kontrolle der Angreifer überweist.

### **Identitätsdiebstahl bei Firmen**

Nicht nur Privatpersonen sind von Identitätsdiebstahl betroffen, sondern zunehmend auch Unternehmen. Der Grund hierfür liegt in der hohen Glaubwürdigkeit eines etablierten Firmennamens, den Betrüger für ihre Zwecke missbrauchen. Besonders gefährdet sind dabei Unternehmen ohne eigenen Webauftritt. Cyberkriminelle gehen dabei systematisch vor: Sie durchsuchen Handelsregister nach geeigneten Unternehmen, registrieren passende Domains und erstellen anschliessend eine Website in deren Namen. Um seriös zu wirken, übernehmen sie offizielle Angaben wie Adresse und Handelsregisternummer der echten Firma. Auf dieser Basis setzen sie danach verschiedene Betrugsmaschen um – von gefälschten Webshops bis hin zu Plattformen für Online-Anlagebetrug. Ein konkretes Beispiel betraf eine etablierte Treuhandfirma mit über zehn Jahren Marktpräsenz. Die Täter nutzten öffentlich zugängliche Handelsregisterdaten, erstellten eine passende Website und traten gegenüber Kunden als das echte Unternehmen auf. Sie forderten Vorauszahlungen für vermeintliche Treuhanddienstleistungen, ohne aber jemals Leistungen zu erbringen. Während die Opfer Geld verloren, erlitt die echte Firma einen erheblichen Reputationsschaden, da Aussenstehende die betrügerischen Aktivitäten fälschlicherweise mit dieser Firma in Verbindung brachten.

### **Betrügerische Stellenangebote**

Auch bei gefälschten Stellenangeboten erstellen Betrüger Websites im Namen bestehender Firmen, um vermeintlich attraktive Stellenangebote zu bewerben. Das BACS erhält schon seit Bestehen regelmässig Meldungen über solche gefälschten Stellenanzeigen, die auf diversen Portalen verbreitet werden. Besonders betroffen sind Arbeitssuchende in der Gastronomie, die oft aus dem Ausland stammen. Nach Einsendung von Dokumenten wie Ausweisen oder dem Lebenslauf folgt meist eine sofortige Zusage. Kurz darauf fordern die Betrüger Geld – etwa für Krankenkassen- oder Registrierungsgebühren – häufig unter Verwendung gefälschter E-Mail-Adressen des Staatssekretariats für Migration (SEM). Viele Stellensuchende sind mit den administrativen Abläufen in der Schweiz nicht vertraut und zahlen daher bereitwillig die betrügerischen Gebühren.

Die Masche betrifft aber nicht nur ausländische Stellensuchende, auch Personen in der Schweiz sind im Visier. Dem BACS werden regelmässig Websites gemeldet, die bekannte Unternehmen imitieren und dabei den Namen seriöser Unternehmen wie Manor oder Zalando missbrauchen. Interessenten erhalten dann Zugang zu Plattformen dieser fingierten Firmen, auf denen sie scheinbar einfache Aufgaben zur Entlohnung erledigen sollen. Solche Aufgaben beinhalten beispielsweise die Produktbewertungen oder das Testen von Applikationen und Spielen. Der angebliche Verdienst wird dann auf den Plattformen ebenfalls angezeigt. Um Vertrauen aufzubauen, wird den Stellensuchenden vielfach zu Beginn tatsächlich ein kleiner Betrag ausbezahlt. Später werden die Opfer dann gedrängt, Gebühren für höhere Verdienste zu zahlen, die sich aber nicht realisieren. Auch eigene Bankkonten und Krypto-Wallets sollen sie für Transaktionen zur Verfügung stellen, womit diese z. B. für Geldwäscherei verwendet werden können. In einem gemeldeten Fall verlor ein Opfer fast CHF 80'000.



## Empfehlungen

Das BACS versucht, betrügerische Seiten möglichst zeitnah vom Netz nehmen zu lassen. Da diese aber meist auf ausländischen Servern gespeichert sind, ist das BACS auf die Kooperation ausländischer Anbieter angewiesen. Firmen wird daher empfohlen, auf ihren Webseiten transparent über solche Betrugsversuche zu informieren. Stellensuchende prüfen meist vorab die Firmenwebsite – finden sie auf der legitimen Website eine Warnung, können sie den Betrug eher erkennen.

## Rückerstattungsbruch weiterhin steigend

Online-Anlagebruch verursacht aktuell in der Schweiz die grössten, gemeldeten Schadenssummen. Nach dem Bemerkten eines Anlagebruchs endet der Bruch aber in vielen Fällen nicht, sondern führt in einen Rückerstattungsbruch («Recovery Scam»). Nicht selten werden die Opfer im Nachgang gleich mehrfach von den Kriminellen kontaktiert, welche behaupten, dass das gestohlene Geld vom initialen Anlagebruch im Rahmen einer Strafuntersuchung aufgetaucht sei. Daher könne nun das Geld zurückgegeben werden. Die Meldungen diesbezüglich haben sich wiederum mehr als verdoppelt, von 145 Meldungen im ersten Halbjahr 2025 auf 325 im zweiten.

Wie bereits im ersten Halbjahr 2025<sup>59</sup> festgestellt, geben sich die Betrüger in der Regel als Anwaltsbüro oder Behörde wie z. B. Europol, Interpol oder der zypriotischen Wertpapierbehörde aus. Auch ein fiktiver Mitarbeiter des BACS trat bereits als angebliche Kontaktperson auf.<sup>60</sup> Die Betrüger registrieren offiziell wirkende E-Mail-Adressen, die real existierenden Personen dieser Organisationen nachgeahmt sind. Zusätzlich nutzen sie gefälschte, offiziell wirkende Dokumente, um die Glaubwürdigkeit bei den Opfern zu erhöhen oder gefälschte Forderungen geltend zu machen. Neben dem Versand von E-Mails kontaktieren die Betrüger die Opfer auch per Telefon, weil im direkten Gespräch gezielter auf das Opfer eingegangen werden kann. Die Anrufe erfolgen meist in Englisch.

Das Perfide an dieser Vorgehensweise ist, dass der Folgeschaden oft den ursprünglichen Schaden des eigentlichen Online-Anlagebruchs übersteigt. Ein Opfer verlor beispielsweise CHF 10'000 im Jahr 2023. Zwei Jahre später behaupteten die Betrüger, das Geld für eine Gebühr von CHF 22'000 zurückzuholen. Opfer willigen zu solch höheren Gebühren ein, weil ihnen die Täter einen vermeintlichen Gewinn der Investition in Aussicht stellen. In diesem Fall betrug dieser angeblich CHF 600'000 CHF.



## Empfehlungen

Seien Sie skeptisch bei E-Mails, Textnachrichten und Anrufen, in denen Ihnen mit Konsequenzen gedroht wird und zeitlicher Druck erzeugt wird (z. B. Geldverlust, Strafanzeige, Konto-

<sup>59</sup> Siehe [Halbjahresbericht 2025/1](#); Kap. 5, Abs. Rückforderungsbruch.

<sup>60</sup> [Woche 38: «Gestatten, Daniel Bruno, NCSC» - Falscher NCSC-Mitarbeiter verspricht Hilfe \(ncsc.admin.ch\)](#)

oder Kartensperrung). Bedenken Sie, dass Betrüger ihre eigene Identität mithilfe von «Spoofing»<sup>61</sup> leicht fälschen können. Seien Sie deshalb generell vorsichtig bei ungewöhnlichen Zahlungsaufforderungen und Gewinnversprechungen. In Unternehmen sollten sämtliche Prozesse, welche den Zahlungsverkehr betreffen, firmenintern klar geregelt sein. Ferner wird Sie keine Schweizer Bank und kein Kreditkarteninstitut jemals per E-Mail auffordern, Passwörter zu ändern oder Kreditkartendaten zu verifizieren. Auch verwenden Bankangestellte nie Sicherheits-Token und andere persönliche Zugangsdaten für Ihr E-Banking oder Twint als Grundlage zur Verifizierung Ihrer Identität bei Anrufen.

## 6 Angriffe auf die Verfügbarkeit von Websites und Webdiensten

Bei Angriffen auf die Verfügbarkeit von Websites und Webdiensten – meistens in Form von «Distributed Denial of Service» (DDoS) – versuchen Angreifer, die Nutzung eines aus dem Internet zugänglichen Dienstes mithilfe einer grossen Anzahl von Anfragen temporär zu stören. Solche Angriffe führen direkt weder zu einem unberechtigten Zugriff auf Daten, zu einem Datenabfluss noch zur nachhaltigen Beschädigung von Systemen. Diese Angriffsart wird besonders für Aktivismus im Cyberraum (Hacktivismus), zur Verschleierung einer anderen Aktivität oder von Kriminellen für die Erpressung der Opfer genutzt.

Im zweiten Halbjahr 2025 blieben öffentlichkeitswirksame DDoS-Angriffe betreffend Hacktivismus in der Schweiz aus. Auch erhielt das BACS keine Meldungen zu DDoS-Erpressungsversuchen seitens des kriminellen Milieus. Dies steht im Gegensatz zum vorangegangenen Halbjahr<sup>62</sup>, hier wurden mehrere Organisationen in der Schweiz rund um Grossveranstaltungen wie dem «World Economic Forum» (WEF) oder des «Eurovision Song Contests» (ESC) zum Ziel solcher Angriffe. Im zweiten Halbjahr 2025 gab es zwar vereinzelte Meldungen zu Angriffsversuchen ohne bekannte Täterschaft, vorwiegend aus den Sektoren Finanz, IT und der öffentlichen Verwaltung. Die Auswirkungen beschränkten sich jedoch auf kurzzeitige Ausfälle, die sich mit etablierten Massnahmen beheben liessen.

Eine temporär dämpfende Wirkung auf die Aktivitäten von pro-russischen Hacktivist\*innen hatte die Operation «Eastwood»<sup>63</sup> der Strafverfolgungsbehörden von Mitte Juli 2025. An den Verhaftungen, Beschlagnahmungen und Störung der Infrastruktur waren auch Schweizer Ermittler beteiligt. Das Kollektiv «NoName057(16)» erneuerte danach seine Werkzeuge und kehrten nach einigen Wochen zu seinen Störaktionen zurück. So bekannte sich dieselbe Gruppierung zu Angriffen auf die französische Post, welche deren Dienstleistung kurz vor Weihnachten zu verzögern vermochte. Die behauptete Urheberschaft wurde vom Opfer jedoch nicht bestätigt.<sup>64</sup>

---

<sup>61</sup> [Spoofing \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/news/2025/01/spoofing)

<sup>62</sup> [Halbjahresbericht 2025/1 \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/en/news/2025/01/halbjahresbericht-2025-1)

<sup>63</sup> [Global operation targets NoName057\(16\) pro-Russian cybercrime network – The offenders targeted Ukraine and supporting countries, including many EU Member States \(europol.europa.eu\)](https://www.europol.europa.eu/news-room/2025/07/global-operation-targets-no-name-057-16-pro-russian-cybercrime-network-the-offenders-targeted-ukraine-and-supporting-countries-including-many-eu-member-states)

<sup>64</sup> [Pro-Russian hacking group claims cyberattack on France's postal service \(apnews.com\)](https://www.apnews.com/story/pro-russian-hacking-group-claims-cyberattack-on-france-s-postal-service/2025/12/15)

Bereits Anfang Dezember 2025 hatte die amerikanische Justiz zudem Anklage gegen die Gruppe erhoben und sie mit staatlichen russischen Institutionen in Verbindung gebracht.<sup>65</sup> Ein angemessenes Abwehrdispositiv muss somit auch hinsichtlich anstehender Grossanlässe<sup>66</sup> in und um die Schweiz gewährleistet werden, um die Verfügbarkeit von Onlinediensten auch in Zeiten mit erhöhter internationaler Aufmerksamkeit aufrecht zu erhalten.

In Bezug auf eingesetzte Angriffsinfrastruktur gilt es auf das Botnetz «Aisuru» hinzuweisen, das mit DDoS-Angriffen mit immensem Netzwerkverkehr von bis zu 30 Tb/s global auf sich aufmerksam gemacht hat. Solche Bandbreiten bringen nicht nur die eigentlichen Ziele an ihre technischen Grenzen. Auch angrenzende Teile des Internets können durch diese Angriffe in Mitleidenschaft gezogen werden.<sup>67</sup>



### Empfehlungen

Die Website des BACS bietet unter der Rubrik [Angriff auf die Verfügbarkeit \(DDoS-Angriff\)](#) verschiedene Informationen und Massnahmen zur Prävention und Abwehr solcher Angriffe an. Bereiten Sie sich in Kooperation mit Ihrem Dienstleister oder Hosters auf einen potenziellen Angriff vor, um die Auswirkungen abzumildern. Für kritische Systeme kann es sinnvoll sein, einen kommerziellen DDoS-Schutz zur Unterstützung hinzuzuziehen.

Bei DDoS-Angriffen im Zusammenhang mit Erpressung empfiehlt das BACS, nicht auf die Forderungen einzugehen. Die Kriminellen können nach einer ersten Zahlung mehr Geld verlangen und die Angriffe danach trotzdem fortführen. Stattdessen können Sie den Fall dem BACS melden und mit der Polizei in Kontakt treten, um eine Strafanzeige zu erstatten. Im Falle eines DDoS-Angriffs finden Sie Empfehlungen auf der Website des BACS [DDoS-Angriff – Was nun?](#)

## 7 Datenmanagement, -abflüsse und -erpressung

Datenlecks und ungewollte Datenexpositionen stehen sowohl in der Schweiz als auch international immer wieder im Fokus. Besonders in Fällen, bei denen ein nachgelagertes Risiko für weitere Organisationen und Privatpersonen besteht, können Datenabflüsse nebst der Verletzung der Datenvertraulichkeit zu zusätzlichem Schaden führen. Während Unternehmen nach einem Datenabfluss bei einem Zulieferer gegebenenfalls ihre Zugänge zur eigenen IT-Infrastruktur überwachen müssen, steigt auch das Risiko, Opfer eines Betrugsversuchs zu werden (vgl. Kap. 5). Ähnlich können bei Privatpersonen sensible Informationen für Kontoübernahmen, Phishing (vgl. Kap. 2), Identitätsdiebstahl oder Finanzbetrug missbraucht werden. Bei Datenabflüssen spielen besonders bei Angriffen im Erpressungs- und Ransomware-Umfeld die Täter eine bedeutende Rolle, da sie die Daten beim Ausbleiben der Lösegeldzahlung in

<sup>65</sup> [Office of Public Affairs | Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups \(justice.gov\)](#)

<sup>66</sup> Siehe [Cyberresilienz im Kontext von Grossveranstaltungen und internationalen Konferenzen \(ncsc.admin.ch\)](#)

<sup>67</sup> [Cloudflare's 2025 Q3 DDoS threat report -- including Aisuru, the apex of botnets \(cloudflare.com\)](#)

der Regel veröffentlichen und/oder z. B. durch deren Verkauf monetarisieren (vgl. Kap. 3.2). Auch andere Ursachen wie ein unzureichendes Datenmanagement in der eigenen Infrastruktur, vorhandene Schwachstellen (vgl. Kap. 4) oder technische Fehlkonfigurationen können eine Datenexposition begründen.

Die Schweizer Bevölkerung und Organisationen waren auch im zweiten Halbjahr des Jahres 2025 von Datenabflüssen und ihren teilweise langanhaltenden Konsequenzen betroffen. Dabei fielen besonders ältere Datenabflüsse auf, da sie Angreifern je nach Gültigkeitsdauer der Information selbst Jahre nach der Publikation immer noch als wertvolles Hilfsmittel dienen können. So gab es beispielsweise Beobachtungen, dass abgeflossene, sensible Daten auch in der Schweiz von Angreifern systematisch wiederverwendet werden. Indem sie Informationen wie Name, Geburtsdatum oder Telefonnummern in E-Mails aufführen, lassen sie Phishing- oder Fake-Sextortion-Kampagnen bei potenziellen Opfern glaubwürdiger erscheinen.

Schweizer Organisationen waren auch von internationalen, grossangelegten Datenexfiltrations- und Erpressungskampagnen durch Kriminelle betroffen. Exemplarisch kann hier der Vorfall bei Logitech genannt werden.<sup>68</sup> Logitech wurde – wie zahlreiche andere international tätige Unternehmen – Opfer einer Erpressungskampagne der Gruppe «Clop», die mithilfe einer Zero-Day-Software-Schwachstelle in der Oracle E-Business Suite (EBS) Unternehmensdaten stahlen.<sup>69</sup> Bei Logitech führte der unautorisierte Zugriff zu keinen Konsequenzen in Bezug auf ihre Produkte und Geschäftsoperationen, jedoch zu einem Abfluss von Kunden- und Mitarbeitendaten ohne sensiblen Charakter. Clop verfolgte noch zu Beginn ihrer Aktivität ab 2019 das klassische Ransomware-Vorgehen mit Verschlüsselung (vgl. Kap. 3.2), jedoch spezialisierte sich die Gruppe zunehmend auf die massenhafte Kompromittierung von Datentransfer-Produkten und die anschliessende Erpressung betroffener Geschäftskunden durch Androhung der Publikation der abgegriffenen Daten.<sup>70</sup> Auch beim Vorfall mit Oracle EBS ging Clop nach demselben Muster vor: Während Angriffshandlungen bis zum 10. Juli 2025 zurückverfolgt werden konnten, informierten die Angreifer die Führungskräfte der ersten Opferorganisationen jedoch erst am 29. September 2025 per E-Mail über den Datenabfluss und die Möglichkeit, mit einem Lösegeld eine bevorstehende Veröffentlichung der Daten zu verhindern. Im Gegensatz zu einem Erpressungsangriff mit Verschlüsselung können die Angreifer so länger im Verborgenen operieren, weil sie die Angriffsserie mit dem Stichtag der ersten Bekanntmachungen ihrer Kampagne publik machen. Sobald dann auch nur wenige Opfer das geforderte Geld zahlen, lohnt sich das Vorgehen für die Angreifer bereits, da sie von Skaleneffekten bei ihren Angriffen profitieren. Dadurch, dass sie immer wieder dieselbe – noch unbekannte – Schwachstelle unbemerkt ausnützen, können sie die Zahl der Opfer maximieren und ihren Aufwand pro Opfer minimieren.

---

<sup>68</sup> [Logitech Cybersecurity Disclosure \(ir.logitech.com\)](https://ir.logitech.com)

<sup>69</sup> [Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign \(cloud.google.com\)](https://cloud.google.com)

<sup>70</sup> Der [Halbjahresbericht 2023/1](#) beleuchtet im Kap. 4.4.1 eine solche Kampagne («MOVEit») sowie den Akteur im Kap. 4.5.1 im Detail. Weitere solche Kampagnen bestanden bspw. im Kontext von [Accellion FTA](#), [Go-Anywhere MFT](#) und [Cleo](#).



## Empfehlungen

Wenn Inhalte einmal im Internet sind, ist eine endgültige Löschung kaum mehr durchführbar. Daher gilt im Allgemeinen: Legen Sie gemäss dem Grundprinzip der Datenhaltung fest, wer welche Daten, in welcher Form, wo abspeichert und bearbeitet und mit wem diese geteilt werden. Nebst einer konservativen Speicherung sollten Sie Daten in regelmässigen Abständen überprüfen und nicht mehr benötigte Daten löschen. Verschlüsseln Sie besonders sensible Daten. Archivieren Sie aufbewahrungswürdige, aber nicht mehr aktiv genutzte Daten offline. Etablieren Sie klare, umsetzbare Prozesse für Datenbearbeitung und Datenschutz und kontrollieren Sie die Implementation.

Daten aus älteren Datenabflüssen können für spätere Angriffe wiederverwendet werden. Überprüfen Sie periodisch, ob Ihre Zugangsdaten in einem Datenleck enthalten sind, etwa auf der Website [Have I Been Pwned](#)<sup>71</sup> oder dem [Identity Leak Checker des Hasso Plattner Instituts](#)<sup>72</sup>.

## 8 Cyberspionage und -sabotage

Staatliche oder staatlich gesteuerte Akteure stellen eine besondere Art der Bedrohung im Cyberraum dar. Die oft auch als «Advanced Persistent Threat» (APT)<sup>73</sup> bezeichneten Gruppen führen Spionage- oder seltener Sabotageoperationen durch, wenn dies den Interessen des jeweiligen Staates dient. Während Cyberspionage eine kontinuierliche Herausforderung für die Schweizer Spionageabwehr bedeutet, wird gezielte Cybersabotage in der Regel nur im Umfeld von Konflikten und Situationen mit hohen geopolitischen Spannungen beobachtet.<sup>74</sup> Im Gegensatz zu finanziell motivierten Cyberkriminellen wählen APTs ihre Ziele spezifisch aus und betreiben einen immensen Aufwand, um an die gewünschten Informationen zu kommen oder die beabsichtigte Wirkung zu erzielen. Dementsprechend müssen potenziell betroffene Organisationen ihr Abwehrdispositiv umfassend gegen diese Bedrohungsart gestalten. Denn bereits Vorbereitungsmaßnahmen können durch die personellen, technischen und finanziellen Ressourcen von APTs Jahre vor einer aktiven Ausnützung durchgeführt werden.

### 8.1 Cyberspionage

Wie in den vergangenen Jahren zeigte sich auch im zweiten Halbjahr 2025, dass Schwachstellen von in Unternehmen verbreitet genutzten Produkten für APTs attraktive Gelegenheiten darstellen, ob in Form von Zero-Day-Schwachstellen oder solche, die trotz vorliegendem Patch noch nicht behoben wurden. Im Juli 2025 veröffentlichte Microsoft nacheinander Patches für vier Schwachstellen, die verschiedene Versionen ihrer SharePoint-Software für lokale Server betrafen. Ferner informierten sie, dass verschiedene, aus China operierende Akteure diese

---

<sup>71</sup> Siehe [Have I Been Pwned \(haveibeenpwned.com\)](#)

<sup>72</sup> Siehe [Identity Leak Checker \(sec.hpi.de\)](#)

<sup>73</sup> [APT – Glossary \(csrc.nist.gov\)](#)

<sup>74</sup> Siehe auch Pressemitteilung zum Lagebericht «Sicherheit Schweiz 2025»: [Globale Konfrontation hat direkte Auswirkungen auf die Schweiz \(vbs.admin.ch\)](#)

Schwachstellen für Spionage, aber auch zur Verbreitung von Ransomware missbraucht hatten.<sup>75</sup> Ausserdem detektierte Microsoft verschiedene Aktivitäten, die sich durch die Installation von zusätzlichem Schadcode einen dauerhaften und mutmasslich exklusiven Serverzugriff verschafften. Dieser Fall fand weltweit grosse Beachtung, denn verschiedene kritische Infrastrukturen gehörten zu den Zielen des Angriffs.<sup>76</sup> In vielen anderen Fällen mit Schwachstellen haben APTs mit deren Bekanntgabe die Möglichkeit einer exklusiven Ausnutzung verloren. Besonders Kriminelle monitorieren solche Entwicklungen, um selbst neuartige Schwachstellen auszunützen, was z. B. bei einer Schwachstelle der JavaScript-Bibliothek «React» zu beobachten war.<sup>77</sup>

Peripheriegeräte («Edge»-Geräte) sind nach wie vor ein effizientes Mittel für Angreifer, um in ein System über eine Schwachstelle oder eine ungenügend geschützte Zugangskontrolle einzudringen. Daher sind Geräte am Ende des Produktzyklus (EOL), die keine Updates mehr erhalten, einem erhöhten Risiko für Angriffe ausgesetzt. So nutzte der APT «Static Tundra» – mutmasslich für den russischen Militärgeschwehndienst agierend – insbesondere veraltete, nicht mehr unterstützte Cisco-Geräte aus, um Organisationen aus den Bereichen Telekommunikation, Hochschulbildung und verarbeitendes Gewerbe zu kompromittieren.<sup>78</sup>

Die im Bereich der Cyberkriminalität breit genutzte Arbeitsteilung und Spezialisierung beeinflusste auch die Aktivitäten staatlicher Akteure. Insbesondere das Bereitstellen des zuvor erwähnten initialen Zugriffs lässt sich effizient an Externe auslagern. Zu dieser Hypothese gelangte die französische Behörde für die Sicherheit von Informationssystemen (ANSSI), als sie Angriffe über Netzwerkgeräte der Firma Ivanti untersuchte, von denen Organisationen der Sektoren Verwaltung, Telekommunikation, Medien, Finanzen und Transport betroffen waren. Die Behörde stellt Verbindungen zwischen den Aktivitäten des Bedrohungsakteurs «Houken» und China her und vermutet, dass dieser Zugriffe an staatliche Stellen verkauft hat.<sup>79</sup>

Während das Ausnützen von Schwachstellen oder unsicherer Konfigurationen von Netzwerkgeräten eine bevorzugte Methode darstellt, versenden Angreifer auch Spear-Phishing-E-Mails (vgl. Kap. 2) oder greifen auf «Watering-Hole»-Angriffe zurück. Letzteres nutzte die mutmasslich für die russischen Nachrichtendienste operierende Hackergruppe «APT29», um rund 10 Prozent der Besucher legitimer, aber infizierter Websites auf eine von ihr kontrollierte Website umzuleiten.<sup>80</sup>

Um nach dem Erstzugang langfristig auf das System zuzugreifen und das Kernziel der heimlichen Datenexfiltration zu ermöglichen, implementieren Angreifer technische Hintertüren («Backdoors»). In diesem Zusammenhang erregte der Fall «Brickstorm» in der Berichtsperiode Aufmerksamkeit. Gemäss US-amerikanischen und kanadischen Behörden nutzen staatliche, chinesische Akteure diese Backdoors, besonders bei Angriffen auf virtuelle Netzwerkumgebungen. Ziele seien hauptsächlich behördliche Infrastrukturen und Dienstleistungen sowie Organisationen des IT-Sektors gewesen.<sup>81</sup> In einem ersten, im September erschienen Bericht,

---

<sup>75</sup> [Disrupting active exploitation of on-premises SharePoint vulnerabilities \(microsoft.com\)](#)

<sup>76</sup> [ToolShell Attacks Hit 400+ SharePoint Servers, US Government Victims Named \(securityweek.com\)](#)

<sup>77</sup> [Multiple Threat Actors Exploit React2Shell \(CVE-2025-55182\) \(cloud.google.com\)](#)

<sup>78</sup> [Russian state-sponsored espionage group Static Tundra compromises unpatched end-of-life network devices \(blog.talosintelligence.com\)](#)

<sup>79</sup> Siehe [Rapport menaces et incidents du CERT-FR \(cert.ssi.gouv.fr\)](#)

<sup>80</sup> [Amazon disrupts watering hole campaign by Russia's APT29 \(aws.amazon.com\)](#)

<sup>81</sup> [BRICKSTORM Backdoor \(cisa.gov\)](#)

nannte Google auch den juristischen Sektor als Angriffsziel und unterstrich, dass Kompromittierungen auch als Ausgangspunkt zu anderen Organisationen dienen können.<sup>82</sup>



## Empfehlungen

Die Abwehr von Cyberspionage muss auf mehreren Ebenen durch eine «Defence-in-Depth»-Strategie<sup>83</sup> erfolgen. Die hohe Bereitschaft staatlicher Angreifer, Zeit und Ressourcen in Hilfsmittel zu investieren, ermöglicht ihnen, in den meisten Fällen neue Schwachstellen zu identifizieren und auszunützen. Daher ist eine erfolgreiche Verteidigungsstrategie davon abhängig, verschiedene Teile der IT-Infrastruktur zu beachten, zu schützen und zu sensibilisieren. Dies beinhaltet beispielsweise den Perimeter, das Netzwerk, die Endpunkte aber auch den Faktor Mensch und die Organisation selbst. Dabei ist es wichtig zu wissen, dass ein Eindringen durch einen APT aufgrund seiner immensen Ressourcen und Fähigkeiten nie komplett ausgeschlossen werden kann, selbst wenn ein Sicherheitskonzept mehrschichtig aufgebaut ist und eine Organisation dieses aktiv umsetzt. Eine Segmentierung des Netzwerks, bei der z. B. kritische Systeme oder sensible Daten isoliert werden, kann bei einer Kompromittierung eine komplette Infektion der Systeme erschweren. Weitere Empfehlungen finden sich im [IKT-Minimalstandard](#).

## 8.2 Bedrohung industrieller Kontrollsysteme und operativer Technologie

Die Digitalisierung führt nicht nur zum zunehmenden Einsatz von Informationstechnologie im Daten- und Informationsraum, sondern erfasst – respektive steuert – immer mehr auch physische Prozesse. Die dafür eingesetzte, früher meistens isolierte operative Technologie (OT), wie z. B. industrielle Steuerungen (ICS), vernetzt sich zunehmend mit der restlichen Systemlandschaft und setzt sich so auch Risiken aus deren Umfeld aus. Personen, die sich nicht im industriellen Umfeld bewegen, kommen mit dieser Entwicklung wohl am ehesten durch die Fortschritte in der Gebäudeautomatisierung im Rahmen von «Smart Home»-Projekten in Kontakt.

Die Schweiz blieb nach Kenntnis des BACS auch im zweiten Halbjahr 2025 von Cybersabotageangriffen gegen industrielle Systeme verschont. Die internationale Bedrohungslage zeichnet sich weiterhin durch destruktive Aktivitäten<sup>84</sup> im Umfeld von Kriegen und Konflikten, wie dem Krieg in der Ukraine oder dem Nahen Osten, aus. Ausserhalb der Konfliktzonen machen Hacktivist\*innen auf sich aufmerksam, die im Internet exponierte und ungenügend geschützte OT-

---

<sup>82</sup> [Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors \(cloud.google.com\)](#)

<sup>83</sup> Siehe [Empfehlungen IKT-Minimalstandards \(ncsc.admin.ch\)](#), Abs. 1.6 «Defence-in-Depth»-Strategie.

<sup>84</sup> [Sandworm hackers use data wipers to disrupt Ukraine's grain sector \(bleepingcomputer.com\)](#), [Iran-linked cyberattack reportedly disrupts public services in Albania's capital \(therecord.media\)](#)

Systeme zu manipulieren versuchen. Sowohl amerikanische<sup>85</sup>, norwegische<sup>86</sup>, dänische<sup>87</sup> als auch kanadische<sup>88</sup> Behörden sehen bei diesen Hacktivisten jedoch Verbindungen zum russischen Staat. Die Fähigkeiten dieser Angreifer bleiben jedoch bisher auf simple Manipulationsversuche beschränkt und lassen sich mit herkömmlichen Sicherheitsvorkehrungen<sup>89</sup> eindämmen.

Sabotageversuche gibt es aber nicht nur gegen industrielle Systeme, sondern auch gegen Informations- und Kommunikationssysteme. Gemäss der luxemburgischen Regierung war dies der Fall, als am 23. Juli 2025 für drei Stunden das Mobilfunknetz ausfiel und weitreichende Auswirkungen auf die luxemburgische Gesellschaft entfaltete. Der Ausfall hatte Einschränkungen bei der Erreichbarkeit der Notfallnummern zur Folge, auch Internetverbindung und Online-Bankdienstleistungen standen nicht zur Verfügung.<sup>90</sup> Dabei soll es sich um eine beabsichtigte Störung gehandelt haben und war somit ein erfolgreicher Versuch, z. B. das Mobilfunknetz gezielt zu infiltrieren. Als Angriffsziel wurden Schwachstellen in Routern des Herstellers Huawei vermutet, deren Ausnutzung zum grossflächigen Ausfall des Netzwerkes führte.<sup>91</sup>

Eine Rolle bei der Bedrohung von OT-Systemen spielen auch Schwachstellen in industriellen Geräten, da diese in integrierten Systemen teilweise nur mit grossem Aufwand behoben werden können. So beobachteten Sicherheitsforscher in digitalen Fallen, sogenannten «Honey-pots», wie Angreifer neben disruptiven Schaltheandlungen auch alte Schwachstellen zu ihren Zwecken nutzten.<sup>92</sup> Die US-amerikanische Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) bestätigte zudem, dass mehrere Schwachstellen auch in Systemen zur Steuerung von Fabrikationsprozessen ausgenutzt wurden.<sup>93</sup> Neben der zunehmenden Vernetzung dieser Systeme, stellt auch die Einbindung von KI in industrielle Prozesse eine zusätzliche Herausforderung dar. Diese neue Technologie bringt viele Vorteile und Effizienzgewinne, vergrössert aber auch die Angriffsfläche. Deshalb muss die Integration dieser Technologie geeignet abgesichert werden.<sup>94</sup>

---

<sup>85</sup> [Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups \(justice.gov\)](#)

<sup>86</sup> [Norwegian Police Say Pro-Russian Hackers Were Likely Behind Suspected Sabotage at a Dam \(securityweek.com\)](#)

<sup>87</sup> [Denmark summons Russian ambassador over alleged cyberattacks on water utility \(therecord.media\)](#)

<sup>88</sup> [AL25-016 Internet-accessible industrial control systems \(ICS\) abused by hackers \(cyber.gc.ca\)](#)

<sup>89</sup> [Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure \(cisa.gov\)](#)

<sup>90</sup> [Luxembourg probes reported attack on Huawei tech that caused telecoms outage \(therecord.media\)](#)

<sup>91</sup> [Huawei, at the heart of the Post outage \(paperjam.lu\)](#)

<sup>92</sup> [Anatomy of a Hactivist Attack: Russia-Aligned Group Targets OT/ICS \(forescout.com\)](#)

<sup>93</sup> [CISA CVE-2025-5086 to Catalog \(cisa.gov\)](#), [CISA Adds two Vulnerabilities to Catalog \(cisa.gov\)](#)

<sup>94</sup> [Principles for the secure integration of Artificial Intelligence in Operational Technology \(cyber.gov.au\)](#)



## Empfehlungen

Sichern Sie Ihre industriellen Systeme, um wie in diesem Kapitel beschriebene Angriffe zu verhindern. Das BACS schlägt hierzu [Massnahmen zum Schutz von ICS](#) vor. Etwas umfassender sind die [Branchenstandards](#), welche das Bundesamt für wirtschaftliche Landesversorgung (BWL) in Zusammenarbeit mit den jeweiligen Branchenorganisationen erarbeitet hat. Eine weitere Hilfestellung bieten die [Empfehlungen zu OT](#)<sup>95</sup> der Information Security Society Switzerland (ISSS). Die CISA hat eine [Grundlage](#)<sup>96</sup> für die sichere Nutzung von künstlicher Intelligenz im OT-Umfeld bereitgestellt.

---

<sup>95</sup> [ISSS Operational Technology \(OT\) Empfehlungen \(cybernavi.ch\)](#)

<sup>96</sup> [Joint Guidance on Deploying AI Systems Securely \(cisa.gov\)](#)