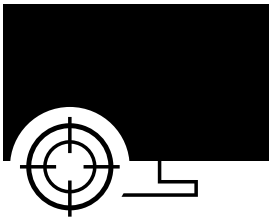
Cyberangriff



Dieses Gefährdungsdossier ist Teil der nationalen Risikoanalyse «Katastrophen und Notlagen Schweiz»

Definition

Cyberangriffe sind gemäss der Nationalen Cyberstrategie (NCS) beabsichtigte, unerlaubte Handlungen privater oder staatlicher Akteure bei der Nutzung von Informatik- und Kommunikationsmitteln (IKT), um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen; dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen.

Je nach Motivation und Mittel des/der Angreifenden lassen sich Cyberangriffe gliedern in:

- Cyberkriminalität: Kriminelle Handlung im Cyberraum resp. mit Cybermitteln mit Bereicherungsabsicht
- Cyberspionage: Unerlaubtes Erlangen von (vertraulichen) wirtschaftlichen, politischen oder militärischen Informationen
- Cybersabotage: Gezieltes Verursachen an Schäden an Informatik- und Kommunikationsmitteln (IKT) und physischen Gütern zur Machtdemonstration und Einschüchterung
- Cybersubversion: Unterminierung des politischen Systems eines anderen Staates durch staatliche, staatsnahe oder politische Akteure
- Cyberoperationen in bewaffneten Konflikten: Hybride, asymmetrische Konfliktführung bis hin zum reinen Cyberwar

Die Angriffsformen treten häufig in Kombination auf und ihre Übergänge sind fliessend. Das vorliegende Dossier behandelt insbesondere Cyberkriminalität, Cybersabotage und Cybersubversion.

Februar 2026

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Bevölkerungsschutz BABS

Inhalt

Ereignisbeispiele

Vergangene Ereignisse tragen dazu bei, eine Gefährdung besser zu verstehen. Sie veranschaulichen die Entstehung, den Ablauf und die Auswirkungen der untersuchten Gefährdung.

Januar 2025 **Schweiz** **DDoS-Angriffe**	Im Januar 2025 erlebte die Schweiz mehrere Distributed-Denial-of-Service (DDoS)-Angriffe, zu denen sich zwei verschiedene Hacktivistengruppen bekannten. Am 6. Januar 2025 waren die Geldautomaten, die Webseite und die E-Banking-App einer Schweizer Bank von einem DDoS-Angriff beeinträchtigt, jedoch waren die meisten Dienste am Ende des Tages wieder verfügbar. Die pro-muslimische Hacktivistengruppe RooT-DoS bekannte sich zu den Angriffen und begründete diese damit, dass die Schweiz mit dem Inkrafttreten des Verhüllungsgesetzes ein anti-muslimisches Gesetz eingeführt habe. Am 10. Januar wurden weitere Angriffe auf die Webdienste der Schweizer Bundesverwaltung verübt, durch dieselbe Hacktivistengruppe. Während rund 45 Minuten waren Dienste wie Telefonie, Outlook sowie verschiedene Webseiten und Fachapplikationen des Bundes beeinträchtigt, doch dank Gegenmassnahmen konnte die Situation stabilisiert werden. Vom 20. bis 26. Januar 2025 führte die pro-russische Hacktivistengruppe NoName057(16) täglich DDoS-Angriffe gegen verschiedene Schweizer Webseiten durch, wobei unter anderem die Webseiten der Region Davos, des Mediensektors, von Schweizer Banken, Gemeinden und Kantonen sowie von Portalen für den Zugang zu staatlichen Dienstleistungen betroffen waren. Diese Angriffe fielen mit dem Weltwirtschaftsforum (WEF) in Davos zusammen, bei dem der ukrainische Präsident Wolodymyr Selenskyj anwesend war. NoName057(16) bekannte sich zu den Angriffen. Das Bundesamt für Cybersicherheit (BACS) hatte während des WEF mit solchen Angriffen gerechnet und Betreiber kritischer Infrastrukturen im Vorfeld gewarnt.
Februar 2022 **Ukraine** **Cybersabotage**	Am 24. Februar 2022 fielen in Europa verschiedentlich die Verbindungen mit dem Satelliten KA-SAT des US-Unternehmens ViaSat aus. Zahlreiche europäische Firmen, Behörden und private Nutzerinnen und Nutzer verwenden diesen Telekommunikationssatelliten für den Internetzugang, insbesondere in entlegenen Regionen. So führte der Vorfall zu Störungen in der Ukraine, aber auch über deren Grenzen hinaus. Beispielsweise waren in Deutschland Zugriffe auf Überwachungs- und Fernsteuerungssysteme von Windkraftanlagen nicht mehr möglich. ViaSat veröffentlichte eine Analyse des Vorfalls. Aus dieser geht hervor, dass es sich um einen gezielten Cyberangriff handelte, der lediglich auf den für die Abdeckung der Ukraine zuständigen Teil des Satellitennetzes ausgerichtet war, dessen Auswirkungen jedoch nicht darauf beschränkt blieben. Weiterhin sind seit Beginn des Kriegs in der Ukraine zahlreiche verschiedene Wiper aufgetaucht. Ziel derartiger Schadsoftware ist es, Daten zu zerstören, respektive sie durch Verschlüsselung oder Überschreiben unlesbar zu machen und damit unwiderruflich zu löschen. Es wurden Organisationen unterschiedlicher Bereiche der öffentlichen Verwaltung sowie des Energie- und Finanzsektors ins Visier genommen.
März bis Dezember 2020 **Vereinigte Staaten** **Cyberspionage**	Am 13. Dezember 2020 meldeten amerikanische Behörden, dass eine Angreifergruppe über ein kompromittiertes Update der Software Orion IT in ihr Netzwerk eingedrungen war. In das offizielle Programm-Update war effektiv im März 2020 eine Hintertür eingebaut worden. Rund 18 000 Anwender dieser Software hatten das Update heruntergeladen. Die Angreifer suchten darunter interessante Ziele aus, um dort den Angriff weiterzuführen und schlossen bei den kollateral betroffenen Opfern die Hintertür wieder. Amerikanischen Quellen zufolge war diese Operation Teil einer grösseren Spionagekampagne, die weitere Unternehmen traf.

Einflussfaktoren

Diese Faktoren können Einfluss auf die Entstehung, Entwicklung und Auswirkungen der Gefährdung haben.

Gefahrenquelle	– Merkmale der Täterschaft (Ideologie und Motivation, Gewaltbereitschaft, Fähigkeit und Knowhow, Organisationsgrad und Professionalisierung sowie Zugang zu finanziellen Mitteln, IT-Ressourcen und Infrastrukturen) – Verhalten des angreifenden (staatlichen oder nicht staatlichen) Akteurs – Verletzlichkeit der Zielsysteme (mangelndes Risikobewusstsein gegenüber Cybergefährdungen, mangelnde Governance und Prozesse mit Bezug zur Informationssicherheit, fehlerhafte Soft- und Hardware, keine oder mangelnde Wartung, mangelnde Compliance, fahrlässiges Handeln, nicht vorhandene organisatorische/technische/bauliche Schutzmassnahmen) – Abhängigkeiten und Komplexität der Systeme (z. B. Cloud Services, Lieferkettenrisiken), Durchdringungsgrad in Staat, Wirtschaft und Gesellschaft – Neue technische Angriffs-Möglichkeiten, gegen die eventuell noch kein ausreichendes Abwehrdispositiv besteht (z. B. Künstliche Intelligenz, Quantum Computing)
Zeitpunkt	– In der Regel abhängig von betrieblichen, politischen oder gesellschaftlichen Entscheiden und Entwicklungen – Tageszeit und Wochentag: Der Zeitpunkt des Cyberangriffs bei einem gezielten Angriff wird oftmals so gewählt, dass das Opfer wenige Ressourcen zur Detektion und Reaktion eingeteilt hat (Wochenende/Ferienzeit). – Die vorbereitenden Aktivitäten für einen Cyberangriff können zeitlich deutlich früher erfolgen als der eigentliche Angriff selbst. Der Aufbau der notwendigen Mittel und Infrastrukturen kann auch in einem anderen Zusammenhang erfolgt sein.
Ort / Ausdehnung	– Grösse und relevante Merkmale des angegriffenen Objektes oder Zielsystems (Einzelperson oder Einzelobjekt, Organisation oder Unternehmen, Branche, Sektor bzw. Vernetzung der Sektoren, spezifische Technologie, staatliche Institutionen usw.) – Identifikation der Urheberschaft (Attribution) und Lokalisierung (Ort, wo sich die Urheber und die Mitwirkenden des Angriffs befinden) – Verwendete Ressourcen (Hard-/Software, Netzwerke, Schnittstellen, Technologien, Protokolle, Manpower usw.)

Ereignisablauf	– Vorhersagbarkeit des zeitlichen und örtlichen Auftretens und der Art und Intensität (Vorwarnzeiten, Zeitpunkt Verhaltensempfehlungen) – Angriffsform und -merkmale (bekannt/unbekannt) – Wirkung der präventiven Schutzmassnahmen – Ablauf des eigentlichen Angriffs (einmalig; in Wellen; sich langsam entwickelnd bzw. sofort eskalierend; hybrid in Kombination mit physischen Aktionen) – Wirkung der spezifisch ergriffenen Gegenmassnahmen – Verhalten/Reaktion von betroffenen Personen, Organisationen und Staaten – Verhalten/Reaktion von Einsatzkräften, verantwortlichen Behörden, beigezogenen Experten und Security Dienstleistern (z. B. Computer Security Incident Response Team (CSIRT), Computer Emergency Response Team (CERT), Security Operation Center (SOC)) – Reaktion der Bevölkerung und der Politik

Intensitäten von Szenarien

Abhängig von den Einflussfaktoren können sich verschiedene Ereignisse mit verschiedenen Intensitäten entwickeln. Die unten aufgeführten Szenarien stellen eine Auswahl von vielen möglichen Abläufen dar und sind keine Vorhersage. Mit diesen Szenarien werden mögliche Auswirkungen antizipiert, um sich auf die Gefährdung vorzubereiten.

1 – erheblich	– Bekannte Angriffsform – Gegenmassnahmen sind vorhanden oder können schnell entwickelt werden – Tritt nur einmal auf – Angriffe auf kritische Infrastrukturen in den Sektoren Industrie und Behörden – Diebstahl von behördlich und wirtschaftlich relevanten Daten – Die Öffentlichkeit ist vom Angriff nicht betroffen – Angriff wird erst nach dessen Ende in der Öffentlichkeit bekannt
2 – gross	– Kombination bekannter Angriffsformen bzw. relativ unbekannte Angriffsform – Gegenmassnahmen sind nicht vorhanden, können aber innert Tagen entwickelt werden – Tritt in Wellen auf – Diebstahl von behördlich und wirtschaftlich relevanten Daten – Angriffe auf kritische Infrastrukturen in den Sektoren Finanzen und Behörden, gezielte Informationsmanipulationen bei staatlichen und privaten Webseiten und Informationskanälen, Einstellung elektronischer Dienstleistungen bei Finanzinstituten (z. B. E-Banking) – Die Öffentlichkeit wird informiert, dass Angriffe stattfinden – Die Öffentlichkeit ist von den Angriffen betroffen, Auswirkungen sind im Alltag spürbar – (z. B. Bargeldbezug nicht mehr möglich; Transaktionen können nicht getätigt werden)
3 – extrem	– Neue oder weiterentwickelte Angriffsform – Gegenmassnahmen sind nicht vorhanden, die Entwicklung dauert Wochen oder ist innert nützlicher Frist nicht möglich – Form des Angriffs ändert sich, Angriff eskaliert – Angriffe auf kritische Infrastrukturen in den Sektoren Energie, Telekommunikation und Verkehr – Manipulation und physische Schäden bei Verkehrs- und Energiesteuerungssystemen, massive Störung bei Telekommunikations-Dienstleistungen – Die Öffentlichkeit realisiert unmittelbar, dass Angriffe stattfinden – Die Öffentlichkeit ist von Angriffen direkt betroffen, die Auswirkungen sind im Alltag stark spürbar

Szenario

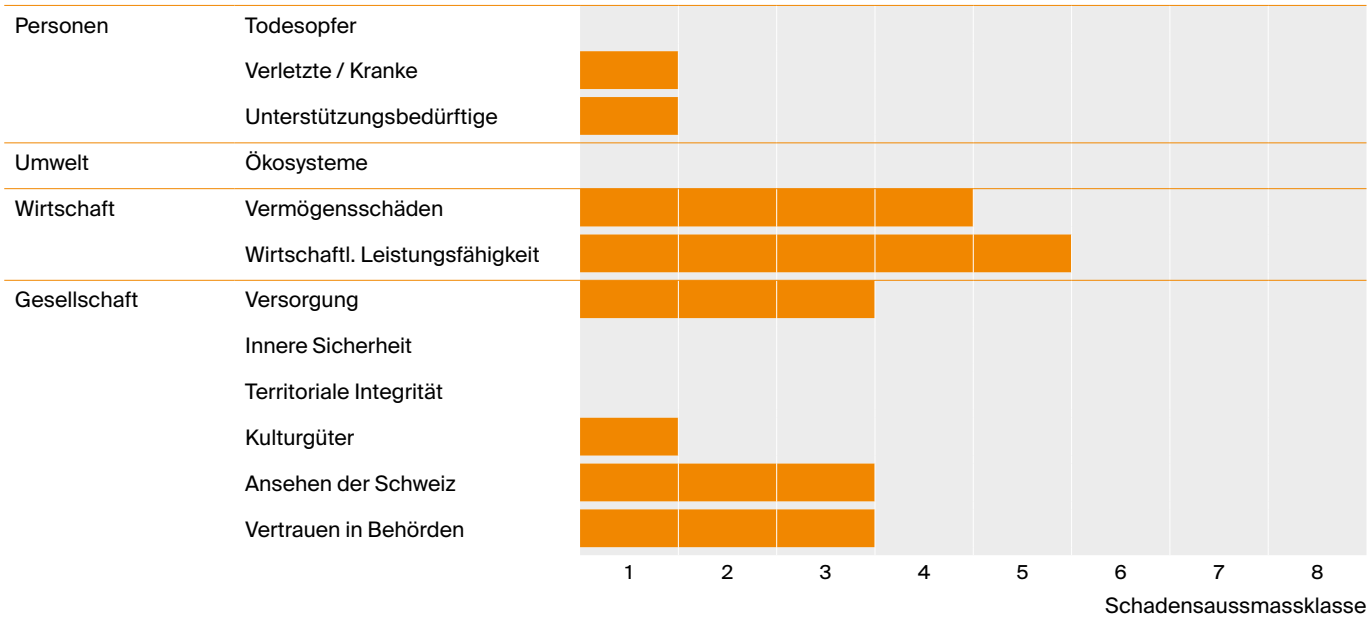
Das nachfolgende Szenario basiert auf der Intensitätsstufe «gross».

Ausgangslage / Vorphase	Ein politisches Ereignis (z. B. sensibler Volksentscheid) oder eine in der Schweiz geduldete Tätigkeit einer Organisation, eines Unternehmens oder einer Branche werden von einer ausländischen Organisation oder einem Staat als inakzeptabel verurteilt. Es wird mit einem Cyberangriff darauf reagiert.
Ereignisphase	Verschiedene Webauftritte von Organisationen und Informationsportalen werden kompromittiert. Über die manipulierten Webseiten sowie über Soziale Medien werden gezielt Falschinformationen verbreitet. Betroffen von diesen Angriffen sind in erster Linie Medienunternehmen. Die Angriffe finden in einem Zeitraum von zwei bis drei Monaten statt und treten zuerst nur vereinzelt auf, häufen sich dann aber. Einige betroffene Organisationen melden die Attacken der nationalen Anlaufstelle des Bundesamts für Cybersicherheit (BACS) oder den lokalen Strafverfolgungsbehörden. Das BACS bewertet diese Informationen gesamtheitlich und stellt die Erkenntnisse den zuständigen Behörden und betroffenen Unternehmen zur Verfügung. In einer offiziellen Stellungnahme verurteilt der Bundesrat die Angriffe auf die Webauftritte und verteidigt die als Provokation empfundene Haltung der Schweiz. Ein bis drei Tage nach der Stellungnahme des Bundes finden konzentrierte DDoS-Angriffe auf Webauftritte der öffentlichen Hand statt. Von den Angriffen sind vor allem Departemente und Bundesämter betroffen, die inhaltlich mit dem Thema verbunden sind. Als Einfallstor für die Angriffe werden zunächst städtische und kantonale Webserver vermutet. Neben der Manipulation der Webauftritte werden jetzt auch die Online-Dienstleistungen der betroffenen Bundesämter (E-Government) stark gestört. Zudem erhält eine grosse Zahl zufällig ausgewählter Mitarbeitenden E-Mails mit manipulierten Anhängen, die Ransomware enthalten. Die Bereinigung beziehungsweise das Neuaufsetzen der befallenen Rechner nimmt viel Zeit in Anspruch. Vereinzelt werden Einbruchsversuche in IKT-Systeme des Bundes registriert. Ein Abfluss von Daten kann aber nicht festgestellt werden. Die betroffenen Stellen des Bundes melden dem BACS die Ereignisse. Drei Wochen später verlagern sich die Angriffe auf den Finanzsektor. Zuerst werden die Webauftritte verschiedener Finanzdienstleister angegriffen. Während zwei bis drei Wochen sind wichtige Funktionen massiv gestört. Dabei ist insbesondere die Kommunikation der Schweizer Börse über deren Webseite während mehrerer Tage nur eingeschränkt möglich. Der Interbankenhandel ist partiell beeinträchtigt, er fällt jedoch nicht aus. Neben den Online-Dienstleistungen der Finanzinstitute sind auch die Zahlungsterminals mehrerer Detailhändler in der ganzen Schweiz betroffen, da die korrespondierenden Server zwei Tage lang nicht mehr erreicht werden können. Auch ein Grossteil der Geldautomaten in der ganzen Schweiz steht nicht oder nur eingeschränkt zur Verfügung.

	Der E-Mail-Verkehr wird durch ein hohes Aufkommen von Spam (u. a. Propaganda) und Phishing-Mails stark beeinträchtigt. Organisationen, die Dienstleistungen für Finanzinstitute erbringen, sind von den Attacken ebenfalls tangiert. Dies betrifft etwa die Informationsanbieter von Finanzdaten. Des Weiteren ist die Abwicklung von Transaktionen beeinträchtigt. Um in die IT-Systeme der Finanzinstitute einzudringen, werden zuerst die Managed IT-Serviceprovider dieser Institute angegriffen und über deren direkte Zugriffsrechte wird versucht, auf die Systeme und Daten zuzugreifen. Die Börse in Zürich wird kurz nach der Handelseröffnung scheinbar aus der Schweiz heraus mittels Malware attackiert. Die Angreifer können Malware in ein System einschleusen, das mit den Systemen der Schweizer Börse verbunden ist. Die Börse muss in der Folge den Handel einstellen und kann erst nach der Implementierung zusätzlicher Schutzmechanismen zwei Handelstage später wieder öffnen. Im Hintergrund arbeiten die zuständigen Schweizer Bundesstellen seit längerer Zeit eng mit den entsprechenden Stellen anderer Staaten zusammen. Es gelingt, die Organisation zu identifizieren, die für die Angriffe verantwortlich ist. Einem Drittland gelingt es, zuerst die für die Angriffe genutzte Infrastruktur und dann die Organisation selbst unschädlich zu machen. In der Folge flauen die Angriffe schnell ab.
Regenerationsphase	Die Webauftritte von Behörden, Finanzinstituten und Medienunternehmen können nach und nach wieder aufgeschaltet bzw. stabilisiert werden. Eine Woche nach dem Ende der Angriffe stehen die wesentlichen Webauftritte wieder zur Verfügung. Bei schlecht geschützten Providern dauert die Wiederherstellung länger. Etwa einen Monat nach Ende der Angriffe sind alle Webauftritte wiederhergestellt. Ein Datenabfluss aus den Systemen, die von den Angreifern attackiert worden sind, kann nicht ausgeschlossen werden. Die betroffenen Stellen sind nach Abflauen der Angriffe noch über Wochen damit beschäftigt, das Ausmass des Datenabflusses einzuschätzen. Für die Bevölkerung hat sich die Lage einen Monat nach Ende der Angriffe normalisiert.
Zeitlicher Verlauf	Die Ereignisphase dauert gut fünf Monate und läuft in drei Wellen ab: 1: Kompromittierung der Webauftritte von Medienunternehmen. 2: Angriffe auf IT-Infrastruktur des Bundes. 3: Angriffe auf IT-Infrastrukturen des Finanzsektors. Die Auswirkungen erstrecken sich insgesamt über ungefähr sechs Monate.
Räumliche Ausdehnung	Die Angriffe richten sich gegen Online-Medien, die öffentliche Hand und den Finanzsektor in der Schweiz. Die Angriffe sind grundsätzlich für alle Personen bemerkbar, die in einer Kundenbeziehung mit den betroffenen Organisationen stehen.

Auswirkungen

Um die Auswirkungen eines Szenarios abzuschätzen, werden zwölf Schadensindikatoren aus vier Schadensbereichen untersucht. Das erwartete Schadensausmass des beschriebenen Szenarios ist im Diagramm zusammengefasst und im nachfolgenden Text erläutert. Pro Ausmassklasse nimmt der Schaden um den Faktor drei zu.



Personen

Das Ereignis hat keine Todesopfer zur Folge.

Durch Streitereien vor Geldautomaten kann es zu einzelnen körperlich Verletzten kommen. Auch müssen einige Personen wegen psychischer Belastung behandelt werden. Die Abwehr und die unmittelbare Bewältigung des Angriffs verursacht beim Fachpersonal der betroffenen Organisationen eine hohe Arbeitsbelastung. Das führt bei einigen IT-Angestellten zu Erschöpfungszuständen. Die Angriffe auf den Staat und das Finanzwesen sowie die Desinformation lösen zudem bei zahlreichen Personen Zukunftsängste aus. Insgesamt wird von knapp 100 Verletzen ausgegangen, die meisten davon leicht.

Vom Ausfall der Finanzdienstleistungen sind auch rund 20 000 Sozialhilfeempfänger/Sozialhilfeempfängerinnen betroffen, die kaum finanzielle Reserven haben und deshalb während 10 Tagen zusätzlich unterstützt werden müssen.

Umwelt

Das Ereignis hat keine geschädigten Ökosysteme zur Folge.

Wirtschaft

Die Börse fällt zwei Tage aus.

Der Interbankenhandel gerät ins Stocken, funktioniert international aber weiter.

Der Zahlungsverkehr mehrerer Detailhändler ist temporär in der ganzen Schweiz gestört. Es werden auch Ausfälle an einem Grossteil der Geldautomaten in der ganzen Schweiz verzeichnet, so dass bei den noch funktionsfähigen Automaten Engpässe auftreten. Zudem finden sich immer weniger Schalter, an denen Bargeld bezogen werden kann, weshalb der Bargeldbezug nur noch begrenzt sichergestellt werden kann.

Nach der Behebung der Störungen kommt es zu einer stark erhöhten Nachfrage nach Lebensmitteln, Gütern des täglichen Bedarfs und Bargeld, was wiederum zu einem kurzfristigen Engpässen führt.

Die Online-Dienstleistungen der betroffenen Finanzinstitute sind stark eingeschränkt und allenfalls korrumpiert oder stehen gar nicht zur Verfügung. Da die entsprechenden Transaktionen wie beispielsweise Zahlungs- oder Börsenaufträge auch nicht über die Schalter abgewickelt werden können, kommt es zu Zahlungsverzögerungen. Dies führt bei den betroffenen Kunden zu einem Vertrauensverlust, weshalb einige Kunden ihre Geschäftsbeziehungen auflösen, darunter auch einzelne internationale Grosskunden. Ebenfalls kommt es zu vereinzelten Klagen und Schadenersatzforderungen.

Die betroffenen Organisationen erleiden weitere finanzielle Schäden aufgrund des personellen und technischen Mehraufwands, der zur Eindämmung beziehungsweise Abwehr der Angriffe, zur Abschätzung des Datenabflusses und zur Identifikation der Täterschaft betrieben wird. Zudem kommt es zu Investitionen in zusätzliche Sicherheitsmassnahmen.

Des Weiteren ist aufgrund der Ausfälle auch der Schweizer Zoll eingeschränkt.

Die direkten Schäden und Bewältigungskosten werden auf rund 870 Mio. CHF geschätzt.

Die Einschränkung der wirtschaftlichen Leistungsfähigkeit infolge dieses Ereignisses beträgt rund 1.7 Mrd. CHF.

Gesellschaft

Es kommt zu folgenden Versorgungsengpässen bzw. -unterbrüchen:

- Finanzdienstleitungen: Infolge des Ereignisses kommt es zu Unterbrüchen bei Finanzdienstleistungen (Bargeld und Online-Transaktionen); sie betreffen während 3 Tagen rund 4 Mio. Personen. Der Ausfall führt bei den betroffenen Finanzinstituten selbst nicht zu grösseren Versorgungsengpässen.
- Lebensmittel: Durch die Einschränkungen beim Bargeldbezug und bei den Finanztransaktionen können nicht alle Personen wie gewohnt Lebensmitteleinkäufe tätigen. Betroffen sind ca. 400 000 Personen.
- Erdölversorgung: Das Treibstoff-Tanken ist wegen des Ausfalls von Zahlterminals an den meisten Orten nur noch mit Bargeld möglich. Davon betroffen sind rund 100 000 Personen.
- Medien: Durch den Angriff auf die Medienunternehmen kommt es zu einem reduzierten Angebot an Medien-Dienstleistungen. Davon betroffen sind ca. 500 000 Personen während 10 Tagen.

In der Bevölkerung kommt es zu Verunsicherungen, allerdings entstehen keine Panikreaktionen. Das Vertrauen der Schweizer Bevölkerung in staatliche Organisationen und Finanzinstitutionen ist hingegen beeinträchtigt. In betroffenen Finanzinstituten, die einen grossen Ansturm auf die Schalter verzeichnen, wird vermehrt privates Sicherheitspersonal eingesetzt. Die Ordnung und die innere Sicherheit bleiben ohne Einschränkungen erhalten.

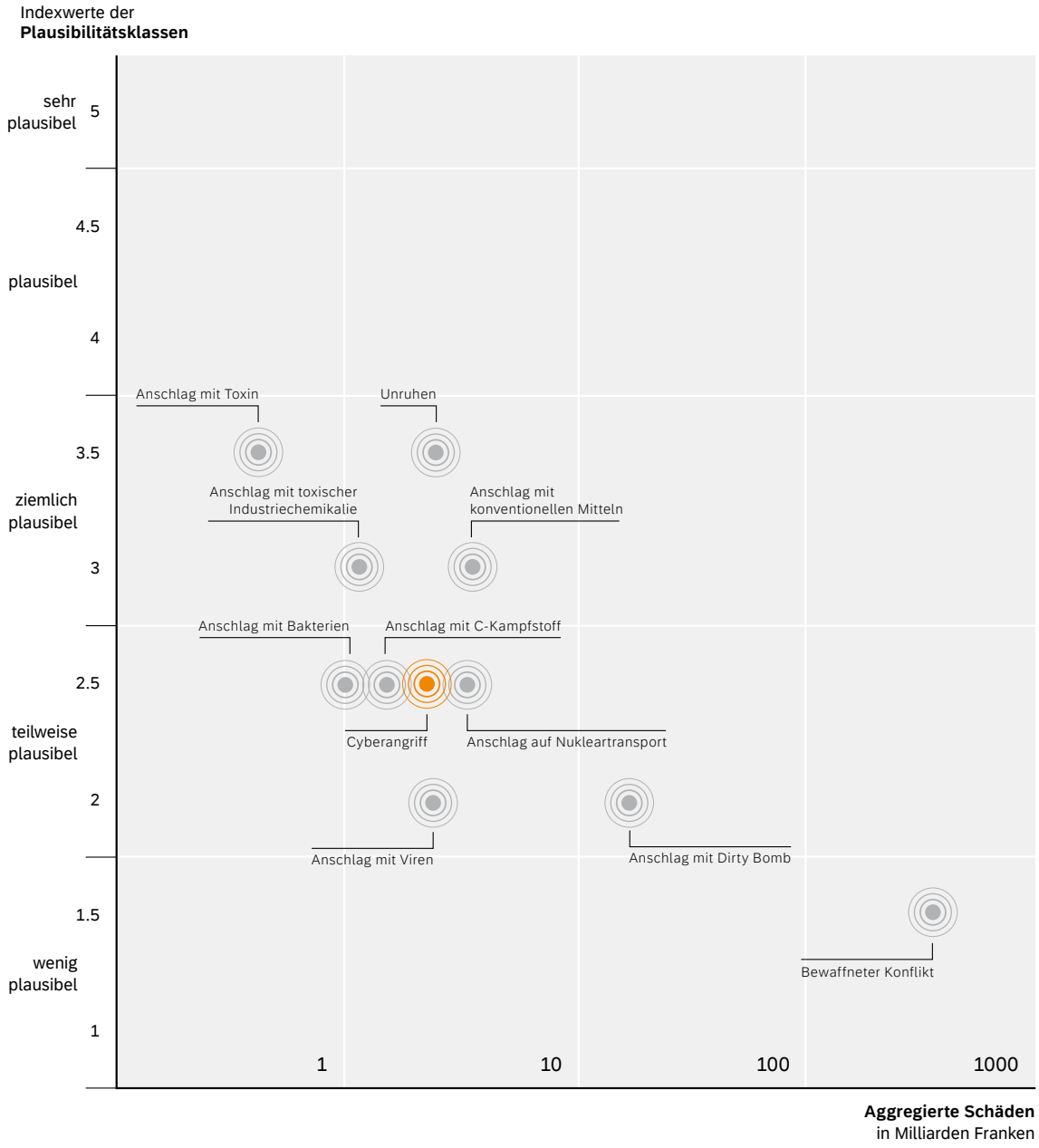
(Digitale) Kulturgüter sind kaum gefährdet. Insbesondere (grosse) Archive sind jedoch an die kantonalen IKT-Systeme angebunden, weshalb es durch Cyberangriffe auf kantonale Systeme zu einer Beeinträchtigung und reduzierten Verfügbarkeit der Archivbestände kommen kann. Ebenso kann es zur irreversiblen Zerstörung, Entwendung oder Publikation sensibler Informationen aus Archiven kommen.

Internationale Medien berichten wiederholt über die verschiedenen Wellen der Cyberangriffe. Insbesondere der Angriff auf Finanzinstitutionen und die zweitägige Einstellung der Börse erregt international grosse Aufmerksamkeit.

Im Nachgang der Angriffe kommt es während einiger Wochen auch zu einer kritischen Berichterstattung in den Schweizer Medien («So verletzlich ist die Schweiz!»), die sich auch auf die Diskussionen und die Wahrnehmung in der Öffentlichkeit auswirkt. Der Zusammenhang zwischen «Cyberspace», der möglichen Verletzung territorialer Integrität sowie den Massnahmen, die die Schweiz gegen weitere, ähnlich gelagerte Attacken ergreifen kann, wird intensiv diskutiert.

Risiko

Die Plausibilität und das Schadensausmass des beschriebenen Szenarios sind zusammen mit den anderen analysierten Szenarien in einer Plausibilitätsmatrix dargestellt. In der Matrix ist die Plausibilität für die mutwillig herbeigeführten Szenarien auf der y-Achse (Skala mit 5 Plausibilitätsklassen) und das Schadensausmass aggregiert und monetarisiert in CHF auf der x-Achse (logarithmische Skala) eingetragen. Das Produkt aus Plausibilität und Schadensausmass stellt das Risiko eines Szenarios dar. Je weiter rechts und oben in der Matrix ein Szenario liegt, desto grösser ist dessen Risiko.



Rechtliche Grundlagen

Gesetz	– Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997; SR 120. – Bundesgesetz über die Informationssicherheit beim Bund (ISG) vom 18. Dezember 2020; SR 128. – Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht vom 30. März 1911); SR 220. – Bundesgesetz über den Datenschutz (DSG) vom 25. September 2020; SR 235.1. – Schweizerisches Strafgesetzbuch vom 21. Dezember 1937; SR 311.0. – Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG) vom 17. Juni 2016; SR 531. – Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 18. März 2016; SR 780.1.
Verordnung	– Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) vom 8. November 2023; SR 128.1. – Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV) vom 7. März 2025, SR 128.51 – Verordnung über die Krisenorganisation der Bundesverwaltung (KOBV) vom 20. Dezember 2024; SR 172.010.8. – Verordnung zum Bundesgesetz über den Datenschutz vom 31. August 2022; SR 235.11.
Weitere rechtliche Grundlagen	– Council of Europe (2001): European Convention on Cybercrime.

Weiterführende Informationen

Zur Gefährdung

- Denning, D. E. (2007): A View of Cyberterrorism Five Years Later. In: Himma, K. (Hrsg.): Internet Security. Hacking, Counterhacking and Society. Jones and Bartlett, Boston.
- Der Bundesrat (2023): Nationale Cyberstrategie (NCS). Nationales Zentrum für Cybersicherheit (NCSC), Bern.
- Der Bundesrat (2023): Nationale Strategie zum Schutz kritischer Infrastrukturen. BABS, Bern.
- European Union Agency for Network and Information Security (ENISA) (2019): ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. EU, Heraklion.
- Ministry of Economic Affairs and Communications: Department of State Information Systems (2008): Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn.
- National Cyber Security Centre (NCSC) (diverse Jahrgänge): Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht. EFD und VBS, Bern.

Zur nationalen Risikoanalyse

- Bundesamt für Bevölkerungsschutz (BABS) (2026): Sammlung der Gefährdungsdossiers. Katastrophen und Notlagen Schweiz 2025. BABS, Bern.
- Bundesamt für Bevölkerungsschutz (BABS) (2026): Welche Risiken gefährden die Schweiz? Katastrophen und Notlagen Schweiz 2025. BABS, Bern.
- Bundesamt für Bevölkerungsschutz (BABS) (2026): Methode zur nationalen Risikoanalyse. Katastrophen und Notlagen Schweiz 2025. Version 3.0. BABS, Bern.
- Bundesamt für Bevölkerungsschutz (BABS) (2026): Bericht zur nationalen Risikoanalyse. Katastrophen und Notlagen Schweiz 2025. BABS, Bern.
- Bundesamt für Bevölkerungsschutz (BABS) (2023): Katalog der Gefährdungen. Katastrophen und Notlagen Schweiz 2025. 3. Auflage. BABS, Bern.

Impressum

Herausgeber
Guisanplatz 1B
CH-3003 Bern
risk-ch@babs.admin.ch
www.bevölkerungsschutz.ch
www.risk-ch.ch

88.123.14