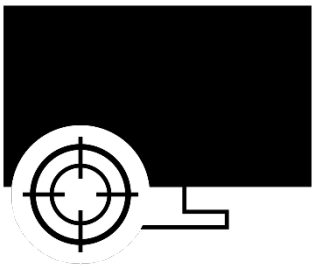
Cyber-Angriff



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

Definition

Cyber-Angriffe sind gemäss der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) beabsichtigte unerlaubte Handlungen privater oder staatlicher Akteure im Cyber-Raum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beinträchtigen; dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen.

Je nach Motivation und Mittel des Angreifers lassen sich Cyber-Angriffe gliedern in:

- Cyber-Kriminalität: Kriminelle Handlung im Cyber-Raum resp. mit Cyber-Mitteln mit Bereicherungsabsicht
- Cyber-Extortion: Erpressung mittels Ransomware
- Cyber-Sabotage und Terrorismus: Schäden an IKT und physischen Gütern sowie zur Machtdemonstration und Einschüchterung
- Cyber-Spionage: Unerlaubtes Erlangen von (vertraulichen) wirtschaftlichen, politischen, militärischen Informationen
- Desinformation/Propaganda: Verunsicherung durch gezielte Falschinformation
- Cyber-Angriff in Konflikten: Hybride, asymmetrische Konfliktführung bis hin zum reinen Cyber-War

Die Übergänge unter den Cyber-Angriffsformen sind fliessend.

November 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Bevölkerungsschutz BABS

Ereignisbeispiele

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

---

27. Juni 2017
Ukraine

Angriff mit Crypto-Locker

Im Juni 2017 befällt der Crypto-Locker «NotPetya» Rechner weltweit, v. a. aber in der Ukraine. Dabei werden Daten auf der Harddisk verschlüsselt und das Opfer wird aufgefordert, Lösegeld zu bezahlen, damit die Daten wieder entschlüsselt werden. Betroffen sind nebst Organisationen in der Ukraine auch Grossunternehmen wie z. B. die dänische Reederei Maersk, der russische Ölproduzent Rosneft, der amerikanische Pharmakonzern Merck Sharp & Dohme oder der Lebensmittelproduzent Mondelez. Maersk schätzt ihren Schaden durch die Cyber-Attacke auf 300 Millionen US-Dollar. Andere Unternehmen weisen ähnlich grosse Schäden aus.

Dezember 2010
Schweiz

DDoS-Angriff «Operation Payback»

Nach der Sistierung der Kundenbeziehungen bzw. Schliessung der Konten des WikiLeaks-Gründers Julian Assange durch die schweizerische PostFinance, MasterCard und Visa werden die Webseiten der Finanzdienstleister zum Ziel von massiven Denial-of-Service-Angriffen. Als Urheber dieser «Operation Payback» gilt das Umfeld der Gruppe Anonymous. Die Webseiten sind während Stunden nicht erreichbar; es können keine Online-Transaktionen abgewickelt werden. Die genauen Schäden lassen sich nicht beziffern.

April / Mai 2007
Estland

Breit angelegter DDoS-Angriff

Nachdem Estland ein sowjetisches Kriegerdenkmal aus dem Zentrum der Hauptstadt Tallinn auf einen weiter entfernten Militärfriedhof verlegt hatte, legen Unbekannte Ende April und im Mai 2007 über einen Distributed Denial-of-Service-Angriff (DDoS) verschiedene estnische Organisationen, darunter das estnische Parlament (inkl. E-Mail-Server), Banken, Ministerien und Newsportale lahm. Teilweise werden Webseiten verunstaltet. Zusätzlich werden Backbone-Router und DNS-Server angegriffen, was zu kurzen Unterbrüchen im Backbone-Datenverkehr führt (kürzer als fünf Minuten). Die Angriffe auf die zwei grössten Banken Estlands führen bei einer der beiden zum Ausfall des Internetbankings (kürzer als zwei Stunden). Eine betroffene Bank schätzt die finanziellen Schäden durch den Cyber-Angriff auf rund 1 Mio. USD. Angaben zu Schäden an staatlichen IT-Infrastrukturen und -Systemen liegen keine vor. Die Integrität der wichtigsten Systeme ist nicht beeinträchtigt, allerdings sind die Systeme stark überlastet und für die Bevölkerung nicht oder nur schwer erreichbar.

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, Zugang zu finanziellen Mitteln und zu IT-Ressourcen, kontrollierte / bereits verfügbare Infrastruktur) – Verhalten eines Staates oder im Land ansässiger Organisationen (krimineller oder parastaatlicher Natur) – Verletzlichkeit der Zielsysteme (mangelnde Wartung oder Unmöglichkeit der Wartung der Zielsysteme, mangelndes Risikobewusstsein insb. bei Führungskräften, mangelnde Governance und Prozesse mit Bezug zur Informationssicherheit, Vernetzung der Systeme sowie Abhängigkeiten und Komplexität, Durchdringungsgrad in Staat, Wirtschaft und Gesellschaft, Monokultur der IKT, fehlerhafte Soft- und Hardware, mangelnde Compliance, fahrlässiges Handeln, vorhandene organisatorische, technische, bauliche Schutzmassnahmen)
Zeitpunkt	– In der Regel abhängig von betrieblichen, politischen oder gesellschaftlichen Entscheiden und Entwicklungen – Arbeitstag oder Feiertag/Wochenende. In der Regel unerwartet für das Opfer – Die vorbereitenden Aktivitäten, die für den Angriff verwendet werden, können zeitlich deutlich früher erfolgen als der eigentlich Cyber-Angriff selbst. Aufbau der notwendigen Mittel und Infrastrukturen kann auch in einem anderen Zusammenhang erfolgt sein
Ort / Ausdehnung	– Grösse und relevante Merkmale des angegriffenen Objektes (Einzelperson oder Einzelobjekt, Organisation oder Unternehmen, Branche, Sektor bzw. Vernetzung der Sektoren, spezifische Technologie, staatliche Institutionen etc.) – Quelle des Angriffs (Ort, wo sich die Urheber und die Mitwirkenden des Angriffs befinden) – Verwendete Infrastrukturen (Hard-/Software, Netzwerke, Schnittstellen, Technologien, Protokolle etc.)
Ereignisablauf	– Wirkung der präventiven Schutzmassnahmen, inkl. Rechtspraxis – Vorbereitung des Angriffs – Ablauf des eigentlichen Angriffs (einmalig; in Wellen; langsam entwickelnd bzw. eskalierend; hybrid in Kombination mit physischen Aktionen) – Wirkung der spezifisch ergriffenen Gegenmassnahmen – Verhalten/Reaktion von betroffenen Personen, Organisationen, Staaten – Verhalten/Reaktion von Einsatzkräften, verantwortlichen Behörden und beigezogenen Experten – 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
- Angriff kommt nicht überraschend; 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

- Relativ unbekannte Angriffsform resp. Kombination bekannter Formen
- Gegenmassnahmen sind nicht vorhanden, können aber innert Tagen entwickelt werden
- Angriff kommt nicht völlig überraschend; 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 (e-banking)
- Die Öffentlichkeit wird informiert, dass Angriffe stattfinden
- Die Öffentlichkeit ist von den Angriffen indirekt betroffen, Auswirkungen sind im Alltag spürbar

---

3 – extrem

- Neue oder weiterentwickelte Angriffsform (z. B. Ransomware-Attacken mit verschlüsselten Back-Ups)
- Gegenmassnahmen sind nicht vorhanden, die Entwicklung dauert Wochen oder ist innert nützlicher Frist gar nicht möglich
- Angriff kommt völlig überraschend; Form ändert sich, Angriff eskaliert
- Angriffe auf kritische Infrastrukturen in den Sektoren Verkehr, Energie und Telekommunikation
- Manipulation und physische Schäden bei Verkehrs- und Energiesteuerungssystemen, massive Störung bei Telekom-Dienstleistungen
- Die Öffentlichkeit realisiert unmittelbar, dass Angriffe stattfinden
- Die Öffentlichkeit ist von Angriffen direkt betroffen, Auswirkungen 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 Cyber-Angriff darauf reagiert.
Ereignisphase	Verschiedene Webauftritte von Organisationen und Informationsportalen werden gehackt und es werden gezielt Falschinformationen gestreut. Betroffen von diesen Angriffen sind in erster Linie Medienhäuser. 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 (Melde- und Analysestelle Informationssicherung MELANI / National Cyber Security Centre NCSC) oder den lokalen Strafverfolgungsbehörden. MELANI/NCSC 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 Angriffe auf Webauftritte der öffentlichen Hand statt. Betroffen sind vor allem Departemente und Bundesämter, die inhaltlich mit dem Thema verbunden sind. Als Einfallstor für die Angriffe werden zunächst kantonale Webserver vermutet. Neben der Verunstaltung 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 einen Crypto-Locker enthalten. Die Bereinigung bzw. das Neuaufsetzen der befallenen Rechner nimmt viel Zeit in Anspruch. Vereinzelt werden Einbruchsversuche in Datensysteme des Bundes registriert. Ein Abfluss von Daten kann aber nicht festgestellt werden. Die betroffenen Stellen des Bundes melden MELANI 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 das Internet 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 im Detailhandel lokal und temporär betroffen, da die korrespondierenden Server zwei Tage lang nicht mehr erreicht werden können. Punktuell werden auch Geldautomaten blockiert. Zudem wird der E-Mail-Verkehr durch ein hohes Aufkommen von SPAM (u. a. Propaganda und Phishing-Mails) stark beeinträchtigt. Auch Organisationen, die für die Finanzinstitute Dienstleistungen erbringen, sind von den Attacken tangiert. Dies betrifft etwa die Informationsanbieter von Finanzdaten oder die Abwicklung von Transaktionen. Es wird versucht, in die IT-Systeme der Institute einzudringen. Dazu werden zuerst die Managed IT-

Serviceprovider dieser Finanzinstitute angegriffen und über deren direkte Zugriffsrechte wird versucht, auf die Systeme und Daten zuzugreifen.

Als an einem Morgen die asiatischen Börsen deutlich schwächer eröffnen, wird die Börse in Zürich pünktlich zur Handelseröffnung scheinbar aus der Schweiz heraus mittels DDoS attackiert. Den Angreifern gelingt dies, indem zuvor in eine weit verbreitete Smartphone-App eingeschleuste schädliche Funktionen aktiviert werden. Die Börse muss 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 kriminelle Organisation zu identifizieren, die für die Angriffe verantwortlich ist. Ein Drittland kann diese Organisation und deren Infrastruktur unschädlich machen. In der Folge flauen die Angriffe schnell ab.

Regenerationsphase

Die Webauftritte von Behörden, Finanzinstituten und Medienhäusern können nach und nach wieder aufgeschaltet bzw. stabilisiert werden. Bei schlecht gesicherten Providern dauert die Wiederherstellung länger oder gelingt gar nicht mehr. Etwa einen Monat nach Ende der Angriffe sind alle Webauftritte wiederhergestellt.

Eine Woche nach dem Ende der Angriffe stehen alle betroffenen Webauftritte des Bundes und der Finanzinstitute wieder zur Verfügung. 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

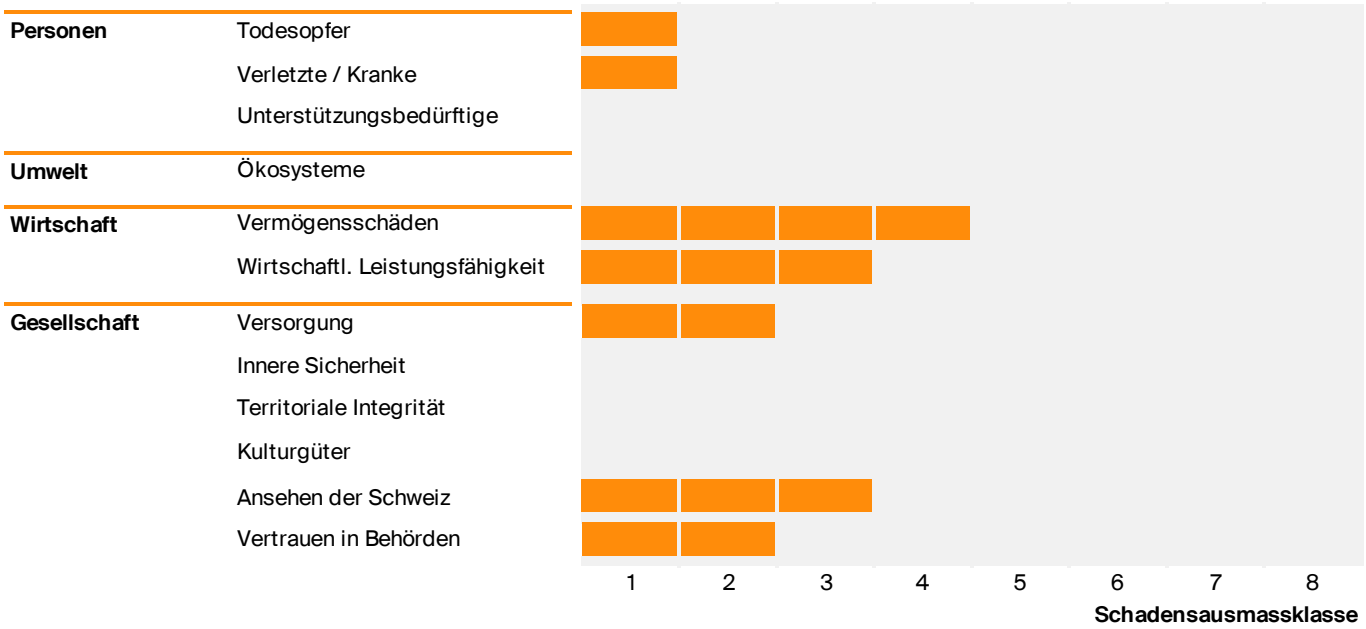
Die Ereignisphase dauert gut fünf Monate und läuft in drei Wellen ab (1: gehackte Webauftritte von Medien, 2: Angriffe auf IT-Infrastruktur des Bundes, 3: Angriffe auf IT-Infrastrukturen des Finanzsektors). Die Auswirkungen sind insgesamt über ungefähr sechs Monate festzustellen.

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 kann wenige Todesopfer (z. B. infolge Suizid) und/oder Verletzte oder unterstützungsbedürftige Personen zur Folge haben.
Umwelt	Das Ereignis hat keine geschädigten Ökosysteme zur Folge.
Wirtschaft	Die Börse fällt zwei Tage aus. Der Interbankenhandel gerät ins Stocken, funktioniert aber international weiter. Die direkt Betroffenen betreiben einen personellen und technischen Mehraufwand zur Eindämmung bzw. Abwehr der Angriffe und zur Identifikation der Täterschaft und müssen Investitionen in zusätzliche Sicherheitsmassnahmen tätigen. Der Zahlungsverkehr im Detailhandel ist lokal und temporär gestört. Teilweise werden Ausfälle an Geldautomaten verzeichnet, der Bezug von Bargeld kann jedoch durch andere Automaten bzw. durch den Bezug am Schalter abgedeckt werden. Da Online-Dienstleistungen stark eingeschränkt und allenfalls korrumpiert sind oder gar nicht zur Verfügung stehen, werden diese Geschäfte teilweise am Schalter abgewickelt. Der Ausfall bei den betroffenen Finanzinstituten führt zu Zahlungsverzögerungen. Ein Teil der Kunden wickelt die Zahlungen am Schalter ab, was für die Finanzinstitute zu einem hohen personellen und für die Kunden zu einem zeitlichen Mehraufwand führt. Teilweise

lösen Kunden ihre Geschäftsbeziehungen auf, weil sie das Vertrauen verloren haben. Wo Kunden keine Zahlungen abwickeln können, kommt es in der Folge zu vereinzelten Klagen und Schadenersatzforderungen.

Betroffene Finanzinstitute erleiden zudem einen finanziellen Schaden. Er umfasst einerseits den personellen und technischen Aufwand, der zur Eindämmung bzw. Abwehr der Angriffe und zur Abschätzung des Datenabflusses betrieben wird. Andererseits enthält er Ausfälle entgangener Geschäfte, weil die Finanzdienstleistungen beeinträchtigt waren.

Die direkten Schäden und Bewältigungskosten werden auf rund 870 Mio. CHF geschätzt. Die Einschränkung der wirtschaftlichen Leistungsfähigkeit infolge dieses Ereignisses beträgt rund 150 Mio. CHF.

Gesellschaft

Infolge des Ereignisses kommt es zu Versorgungsunterbrüchen bei Finanzdienstleistungen, von denen an einzelnen Tagen mehrere Tausend Personen betroffen sind. Der Ausfall führt bei den betroffenen Finanzinstituten jedoch insgesamt nicht zu grösseren Versorgungsengpässen.

Es sind keine lebensnotwendigen oder sehr wichtigen Prozesse betroffen. Vereinzelt werden Provider aufgefordert, Server vom Netz zu nehmen, die als Zwischenstationen für Angriffe missbraucht werden.

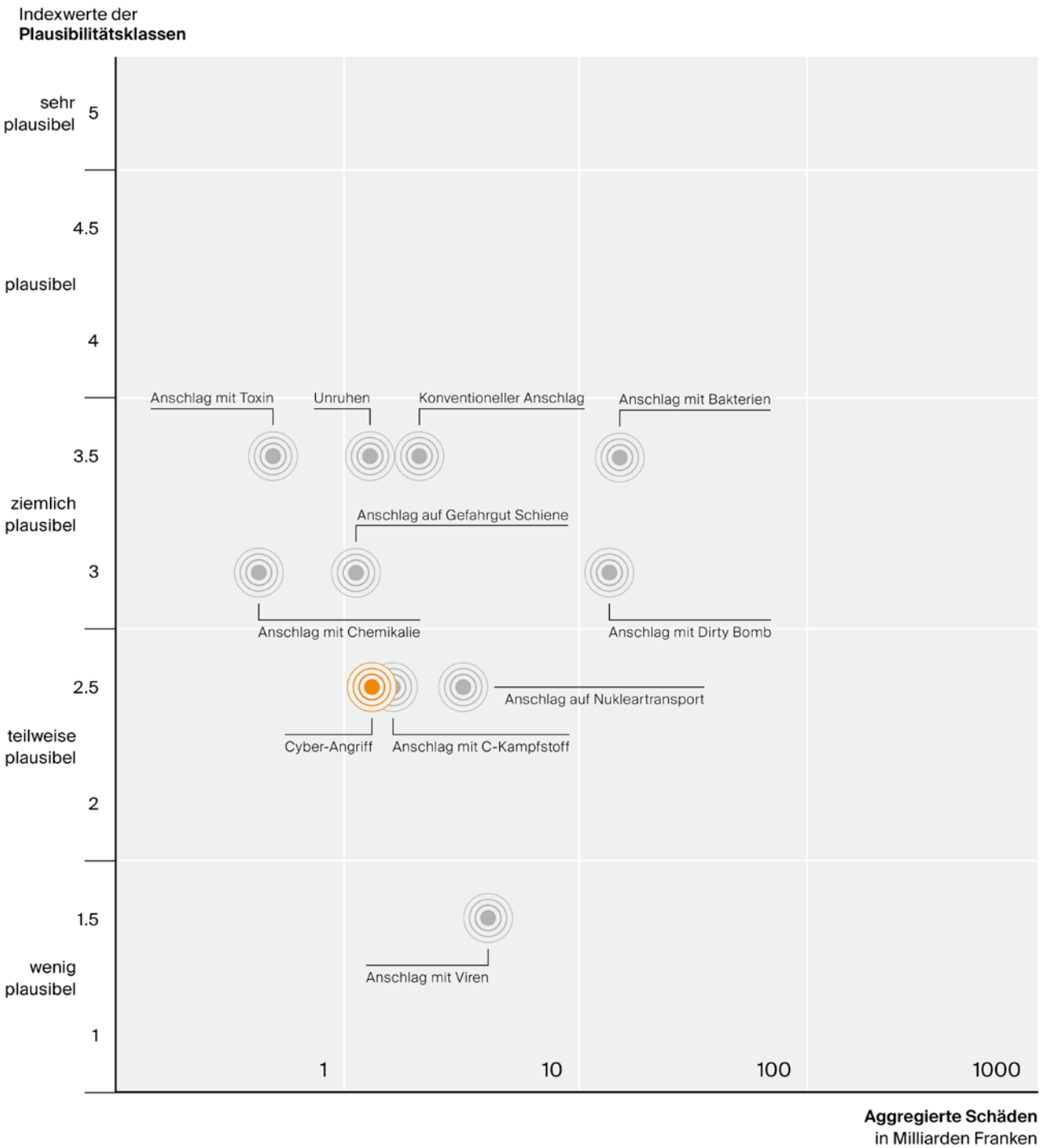
In der Bevölkerung kommt es zu Verunsicherungen, allerdings entstehen keine Panikreaktionen. Das Vertrauen der Schweizer Bevölkerung in staatliche und Finanzinstitutionen ist hingegen beeinträchtigt. In betroffenen Finanzinstituten, die einen grossen Ansturm an die Schalter verzeichnen, wird vermehrt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

Die Berichterstattung der ausländischen Medien über die Bewältigung des Cyberangriffs ist sachlich und dauert einige Tage.

Im Nachgang der Angriffe kommt es während einiger Wochen zu einer sehr 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 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht vom 30. März 1911; SR 220. – Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992; 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 den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020; SR 120.73. – Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993; SR 235.11.
Weitere rechtliche Grundlagen	– Council of Europe (2001): European Convention on Cybercrime.

Weiterführende Informationen

Zur Gefährdung

- Der Bundesrat (2018): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022. ISB, Bern.
- Der Bundesrat (2017): Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022. Bern.
- Der Bundesrat (2012): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken. VBS, Bern.
- Der Bundesrat (2012): Nationale Strategie zum Schutz kritischer Infrastrukturen. Bern.
- Check Point (2019): Cyber Attack Trends: 2019 Mid-Year Report.
- 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.
- European Union Agency for Network and Information Security (ENISA) (2019): ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. EU, Heraklion.
- Melde- und Analysestelle Informationssicherung (MELANI) (diverse Jahrgänge): Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht. EFD und VBS, Bern.
- Ministry of Economic Affairs and Communications: Department of State Information Systems (2008): Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn.

Zur nationalen Risikoanalyse

- Bundesamt für Bevölkerungsschutz (BABS) (2020): Bericht zur nationalen Risikoanalyse. Katastrophen und Notlagen Schweiz 2020. BABS, Bern
- Bundesamt für Bevölkerungsschutz (BABS) (2020): Methode zur nationalen Risikoanalyse. Katastrophen und Notlagen Schweiz 2020. Version 2.0. BABS, Bern.
- Bundesamt für Bevölkerungsschutz (BABS) (2020): Welche Risiken gefährden die Schweiz? Katastrophen und Notlagen Schweiz 2020. BABS, Bern.
- Bundesamt für Bevölkerungsschutz (BABS) (2019): Katalog der Gefährdungen. Katastrophen und Notlagen Schweiz. 2. Auflage. BABS, Bern.

Bundesamt für Bevölkerungsschutz BABS

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