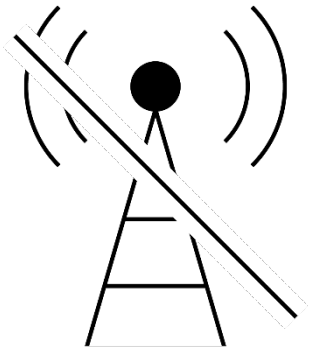
Ausfall Rechenzentrum



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

Definition

Von einem Ausfall eines Rechenzentrums wird dann gesprochen, wenn ein Rechenzentrum Dienstleistungen nicht mehr oder nur noch teilweise erbringen kann. Dies ist der Fall, wenn eine Störung, eine Fehlfunktion oder ein Ausfall bei der Infrastruktur oder in der Software vorgefallen, oder eine unabsichtliche oder vorsätzliche Manipulation von Personen erfolgt ist. Wegen der hohen Abhängigkeit in allen Bereichen der Gesellschaft kann ein solcher Ausfall gravierende Konsequenzen haben. Das Schadensausmass ist abhängig von der Dauer, von der Art der betroffenen Technologien, der Anzahl und der Bedeutung der betroffenen Dienste und Nutzer sowie der Beschädigung von Daten. Ausfälle spezifischer Systeme oder Dienstleistungen können zu grossen Schäden führen, wenn Kontrollsysteme kritischer Infrastrukturen (Kraftwerke, Transportsysteme etc.) davon betroffen sind. Ein Ausfall eines Rechenzentrums kann deshalb zu verschiedenen Folgeschäden führen.

Der Ausfall eines Rechenzentrums kann durch verschiedene Ereignisse ausgelöst werden. Beispiele dafür sind technische Störungen wie Stromausfall oder Komponentenfehler, menschliche Fehlhandlungen und Manipulationen oder Naturereignisse (z. B. Erdbeben).

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.

---

28. Mai 2019
Deutschland

Verschiedene Finanzämter

Eine Störung beim Provider «Dataport» wirkt sich auf alle 141 Finanzämter der deutschen Bundesländer Bremen, Hamburg, Schleswig-Holstein, Sachsen-Anhalt, Mecklenburg-Vorpommern und Niedersachsen aus. Knapp 30 000 Mitarbeitende sind betroffen. Die Störung tritt in Zusammenhang mit einem geplanten Lasttest auf, der die Abschaltung des Kühlsystems auslöst. In der Folge schalten sich alle Systeme des Rechenzentrums ab. Die Störung hält während fünf Arbeitstagen an.

---

27. Mai 2017
England

British Airways

Beim Provider «CBRE Managed Services» überbrückt ein Mitarbeiter die Stromversorgung des Rechenzentrums versehentlich so, dass sowohl Hauptsystem (power supply) als auch Hilfssysteme (uninterruptable power supply) sofort vollständig ausfallen. Der Schaden wird grösser, weil auch die Backup- und Disaster-Recovery-Systeme nicht starten. Nach einigen Minuten kann die Stromversorgung wiederhergestellt werden. Der unkontrollierte Restart beschädigt allerdings Hard- und Software. Hauptkundin British Airways erleidet einen grossen Schaden, da in der Folge 75 000 Passagiere für ein ganzes Wochenende gegroundet werden.

---

20. März 2017
Zürich (Schweiz)

Informatik-Kompetenz-zentrum der Stadt Zürich

Bei «Organisation und Informatik» (OIZ) der Stadt Zürich tritt an einer zentralen Hardwarekomponente im Rechenzentrum Hagenholz ein Defekt auf. In der Folge treten in der Stadtzürcher Verwaltung starke Probleme bei der IT am Arbeitsplatz und bei der IT in den Spitälern auf. Alle Websiten der Stadt Zürich sind nicht erreichbar. In der Nacht auf den 21. März kann der Schaden behoben werden.

Einflussfaktoren

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

Gefahrenquelle	– Ausfall der Stromversorgung oder der Datenleitungen (z. B. durch Naturgefahren, Sabotage) – Technische Defekte (Materialversagen, schadhafte Software usw.) – Bedienungsfehler im Betrieb oder Unterhalt – Andere Fehlfunktionen – Aktive Gefährdungen (Vandalismus, Sabotage, Cyberangriff)
Zeitpunkt	– Geschäftszeiten oder nachts – Arbeitstage oder Wochenende, Feiertage, Ferienzeit, Jahreszeit
Ort / Ausdehnung	– Grad der Verbreitung betroffener Systeme – Grad der Vernetzung betroffener Systeme (Kaskadeneffekte) – Anzahl und Bedeutung der betroffenen Dienste/Services – Anzahl und Bedeutung der betroffenen Sektoren / Nutzer / Kunden – Grad des Datenverlustes – Ausweichmöglichkeiten; proprietäre Systeme
Ereignisablauf	– Vorwarnzeit – Dauer des Ausfalls – Verhalten der betroffenen Organisationen (Ereignisbewältigung) – Reaktion der Kundschaft und der Nutzer

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

- Auswirkungen beschränken sich auf IKT-Sektor
- Keine kritischen Dienste betroffen
- Bekanntes Ereignis, Massnahmen ebenfalls bekannt
- Es kommt zu keinen oder geringen Datenverlusten
- Kurze Dauer (weniger als 1 Tag)

---

2 – gross

- Auswirkungen auf einige kritische Sektoren
- Kritische Dienste betroffen
- Unbekanntes Ereignis, Massnahmen aber aus Erfahrungen anwendbar
- Es kommt teilweise zu korrumpierten Daten oder Datenverlusten
- Mittlere Dauer (zwei bis drei Tage)

---

3 – extrem

- Auswirkungen auf eine grosse Zahl kritische Infrastrukturen, u. a. in den Sektoren Energie, Telekommunikation, Finanzen, medizinische Versorgung und Verkehr
- Grosse Anzahl kritischer Dienste betroffen (z. B. korrumpierte Authentifizierung)
- Es kommt zu massiven korrumpierten Daten oder Datenverlusten
- Schäden bei Verkehrs- und Energiesteuerungssystemen, massive Störung bei Telekom-Dienstleistungen
- Gegenmassnahmen sind nicht vorhanden, deren Entwicklung dauert Wochen
- Die Öffentlichkeit ist von den Angriffen indirekt, aber im Alltag spürbar betroffen
- Lange Dauer (mehr als 1 Woche)

Szenario

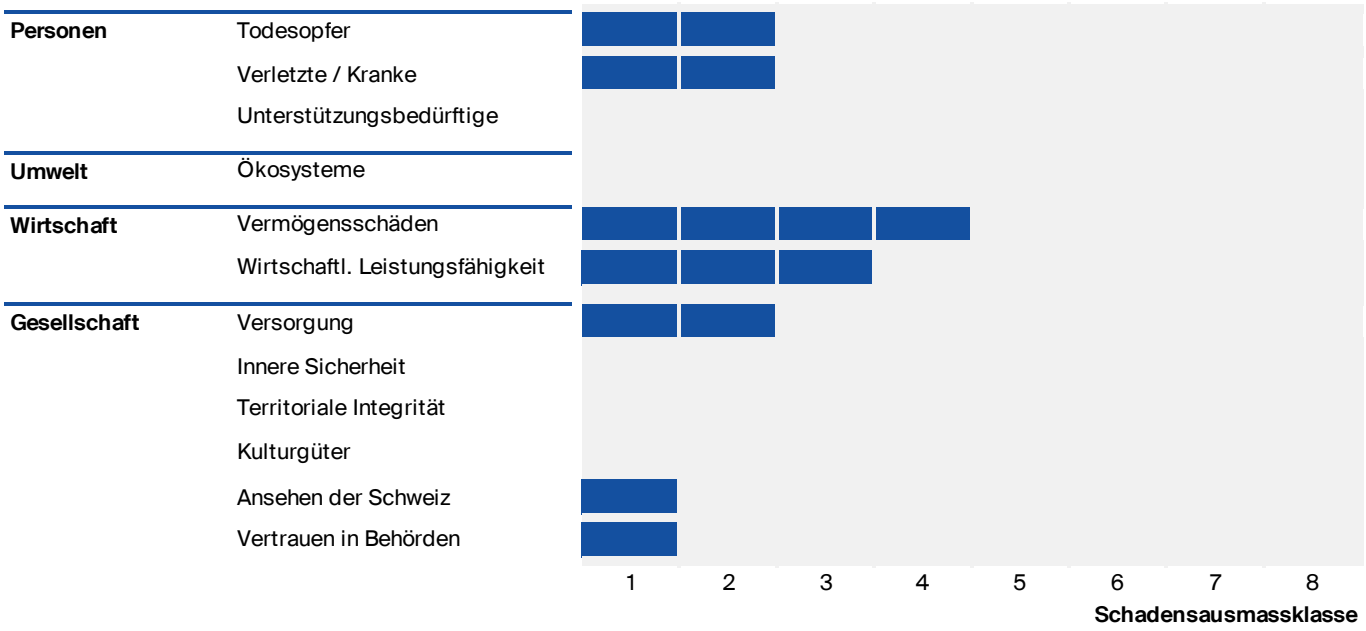
Das nachfolgende Szenario basiert auf der Intensitätsstufe «gross».

Ausgangslage / Vorphase	Ein Betreiber von Rechenzentren verfügt über verschiedene geografisch getrennte Cloud-Standorte, die redundant betrieben werden. Um die Last des Datenverkehrs unter den Rechenzentren besser zu regeln, will der Betreiber den Betrieb auf eine neue Steuerungssoftware (Load Balancing Software) migrieren.
Ereignisphase	Wegen eines Konfigurationsfehlers kommt es bei der Migration zur neuen Software zum kompletten Ausfall eines der Rechenzentren, da der Datenverkehr nicht regelmässig verteilt wird, sondern das betroffene Rechenzentrum überlastet. Der Betreiber versucht erfolglos, den Fehler durch eine veränderte Konfiguration zu beheben. In der Folge trennt der Betreiber das betroffene Rechenzentrum vom Netz und macht die Migration rückgängig. Da die Daten des ausgefallenen Rechenzentrums als Redundanz auch an den anderen Standorten gespeichert sind, übernehmen diese vorübergehend den Datenaustausch mit der Kundschaft. Bei der Wiederinbetriebnahme des betroffenen Rechenzentrums beginnt das automatische Rückspielen der Daten aus den anderen Rechenzentren auf das ausgefallene Rechenzentrum. Ein solcher Fall tritt zum ersten Mal auf und es stellt sich heraus, dass der generierte Datentransfer enorm viel Bandbreite beansprucht, dass das Rechenzentrum extrem viele Daten verarbeiten muss und dass der Restore-Prozess deshalb deutlich länger dauert als erwartet. Zum einen entstehen beim Restore korrupte Dateien, die später eigens wiederhergestellt werden müssen, zum anderen kann der Betreiber der Rechenzentren keinen Einfluss auf den Restore des ausgefallenen Rechenzentrums nehmen, da die Steuerungssoftware keinen Abbruch des Prozesses zulässt. Während Stunden entsteht ein intensiver Netzwerkverkehr, der sich direkt auf die mit dem Betreiber arbeitenden Diensten auswirkt: Deren internetbasierten Dienstleistungen unterliegen praktisch alle massiven Einschränkungen oder fallen vollständig aus. Als Erste spürbar betroffen und eingeschränkt sind Dienste, die auf eine tiefe Latenz angewiesen sind wie etwa solche, die abhängig sind von der Synchronisation grosser Datenbanken, sowie Streamingdienste wie z. B. Multimedia-Anbieter. Aber auch Webzugriffe, E-Mail, Remote Access und Zugriffe von mobilen Geräten sowie Teile der Telefonie sind betroffen. Die Notfalldienste funktionieren. 20 000 KMU, zwei der zehn grössten Online-Shops der Schweiz, ein grosses Logistik-Unternehmen, Teile einer städtischen Verwaltung sowie zahlreiche kleine Hostinganbieter haben als Kunden des Betreibers während zweier Tage nur erschwert Zugriff auf ihre virtualisierte Umgebung und sind von korrupten Datenbeständen betroffen. Durch den fehlerhaften Restore-Prozess und fehlende Backups erleiden ein Spital mit 500 Betten, 2000 KMU sowie die Steuerverwaltung einer mittelgrossen Stadt einen partiellen Datenverlust, 500 KMU gar einen kompletten. Nicht oder nur wenig betroffen sind Nutzer mit dedizierten Verbindungen, eigenen Netzwerken oder Ausweichsystemen wie z. B. Funk, Satellitenkommunikation sowie Provider mit eigenen Verbindungen.

Regenerationsphase	Nach gut zwei Tagen stellt sich wieder eine normale Netzwerkbelastung ein. Bei Kunden, die nicht ausreichend auf ein solches Ereignis vorbereitet waren, weil etwa Backups der Daten und Konfigurationen fehlen, dauern die Massnahmen zur Behebung der Schäden deutlich länger. Dazu gehören das Wiederherstellen konsistenter Datenbestände, das Nacherfassen von Transaktionen und Ähnliches.
Zeitlicher Verlauf	Spontaner Beginn des Ereignisses; innert Minuten spürbar, Einschränkungen treten sofort auf. Normale Netzwerkbelastung nach zwei Tagen wieder vorhanden, die Behebung der Schäden dauert aber nochmals einige Tage.
Räumliche Ausdehnung	Eine klare Abgrenzung ist nicht möglich. Die Engpässe sind in der ganzen Schweiz und ggf. in Europa spürbar.

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

Durch den Verlust von Patientendaten im betroffenen Spital und in einzelnen Arztpraxen kommt es zu Nicht- oder Falschbehandlungen, die bei mehreren Patienten zu gesundheitlichen Schäden oder gar zum Tod führen.

Wegen der eingeschränkten Kommunikationsmöglichkeiten kommt es bei einigen pflegebedürftigen Personen zu Verzögerungen bei Unterstützungsleistungen.

Insgesamt erleiden je nach Ausfall eines kritischen Service bis zu 100 Personen gesundheitliche Schäden oder werden verletzt. Vereinzelte Todesopfer sind nicht auszuschliessen, Es kommen in der Folge des Ausfalls des Rechenzentrums aber voraussichtlich höchstens 10 oder weniger Personen ums Leben.

Umwelt

Das Ereignis hat grundsätzlich keine geschädigten Ökosysteme zur Folge.

Falls das Ereignis auch Auswirkungen auf Steuerungen von Anlagen und Systemen aufweist, die potenzielle Umweltrisiken bergen, können Umweltschäden auftreten; z. B. durch unkontrollierte Freisetzung gefährlicher Stoffe in Boden, Wasser, Luft.

Wirtschaft

Die direkt betroffene Kundschaft des Rechenzentrum-Betreibers sowie jene der Reseller betreiben einen personellen und technischen Mehraufwand zur Aufrechterhaltung ihrer

Dienstleistungen oder stellen die Arbeit in betroffenen Bereichen ein. Dies betrifft rund 20 000 KMU.

Die beiden direkt betroffenen Online-Shops erleiden in den zwei Tagen eine markante Umsatzeinbusse. Das betroffene Logistik-Unternehmen muss zur Disposition seiner Dienstleistungen einen grossen Mehraufwand betreiben. Die ausgelagerten Bereiche der städtischen Verwaltung sind zwei Tage lang nur schlecht online oder telefonisch erreichbar.

Wo Kunden von Resellern direkt betroffen oder Online-Dienstleistungen durch den hohen Netzverkehr stark eingeschränkt sind, kommt es während der zwei Tage ebenfalls zu Ausfällen in der Geschäftstätigkeit.

2000 KMU, die Steuerbehörde und das Personenmeldeamt der betroffenen Stadt erleiden einen partiellen Datenverlust; unter anderem gehen wichtige Steuer- und Einwohnerdaten verloren.

500 KMU erleiden sogar einen vollständigen Verlust der beim Betreiber gespeicherten Daten mit entsprechenden Folgen.

Die Vermögensschäden und Bewältigungskosten belaufen sich auf rund 1 Mrd. CHF. Das Ereignis verringert in der Folge die wirtschaftliche Leistungsfähigkeit um ca. 350 Mio. CHF.

Gesellschaft

Infolge des Ausfalls des Rechenzentrums kommt es zu Versorgungsengpässen und -unterbrüchen wegen Ausfällen in der Logistik verschiedener Unternehmen, z. B. bei den Grossverteilern.

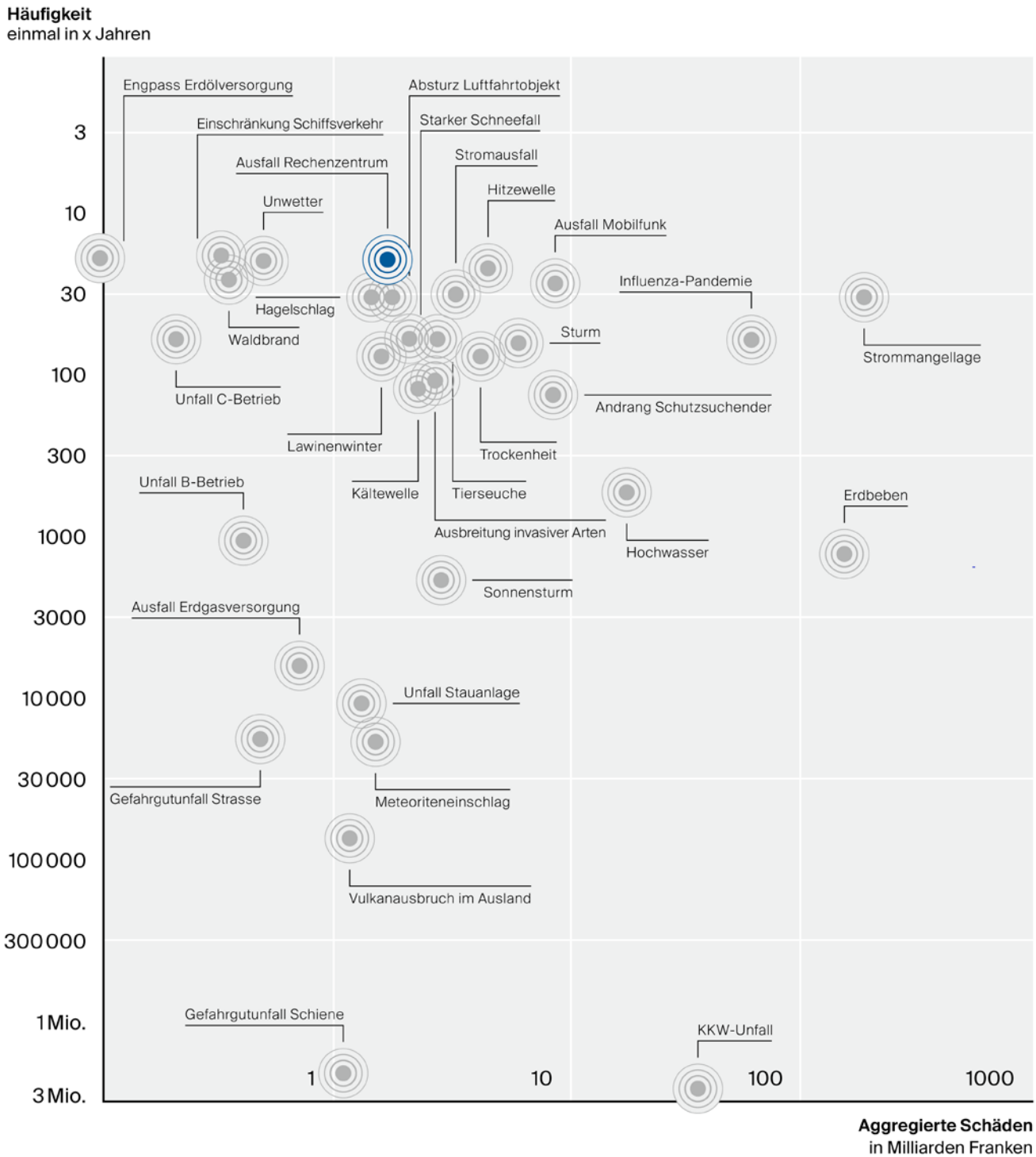
Betroffene Nutzer haben keinen Webzugriff (Wegfall internetbasierter Dienstleistungen wie E-Mail, Social Media, online einkaufen, Streamingdienste etc.).

Der Datenaustausch zwischen z. B. Spitex, Spitälern, Personenmeldeämtern etc. ist eingeschränkt.

Im Nachgang des Ausfalls kommt es während einiger Tage zu einer äusserst kritischen Berichterstattung über den Betreiber des Rechenzentrums, der nicht in der Lage sei, einen zuverlässigen Service zu bieten und dessen Probleme die halbe Schweiz lahmlege». Auch Kunden des Providers geraten wegen der starken Abhängigkeit von wenigen Rechenzentren / Betreiberfirmen oder mangelnder eigener Vorsorge in die Schlagzeilen.

Risiko

Das Risiko des beschriebenen Szenarios ist zusammen mit den anderen analysierten Szenarien in einer Risikomatrix dargestellt. In der Risikomatrix ist die Eintrittswahrscheinlichkeit als Häufigkeit (1-mal in x Jahren) auf der y-Achse (logarithmische Skala) und das Schadensausmass aggregiert und monetarisiert in CHF auf der x-Achse (ebenfalls logarithmische Skala) eingetragen. Das Produkt aus Eintrittswahrscheinlichkeit 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

Verfassung	— Art. 13 (Schutz der Privatsphäre), Art. 92 (Post- und Fernmeldewesen), Art. 173 (Weitere Aufgaben und Befugnisse) der Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999; SR 101.
Gesetz	— Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) vom 21. März 1997; SR 120. — Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992; SR 235.1. — 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. — Entwurf Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG); noch in der parlamentarischen Beratung.
Verordnung	— Organisationsverordnung für das Eidgenössische Finanzdepartement (OV-EFD) vom 17. Februar 2010; SR 172.215.1. — Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993; SR 235.11. — Verordnung über den Bundesstab Bevölkerungsschutz (VBSTB) vom 2. März 2018; SR 520.17. — Verordnung zum Bundesgesetz über die Schweizerische Nationalbank (Nationalbankverordnung, NBV) vom 18. März 2004; SR 951.131.

Weiterführende Informationen

Zur Gefährdung

— Bundesamt für Bevölkerungsschutz (BABS) (2015): Leitfaden Schutz kritischer Infrastrukturen. BABS, Bern.

— 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.

— Eidgenössische Finanzmarktaufsicht (FINMA) (2018): Rundschreiben 2018/3. Outsourcing – Banken und Versicherer. Auslagerungen bei Banken und Versicherungsunternehmen. FINMA, Bern.

— ISO/IEC 27018 (2019): Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO.

— ISO/IEC 27001 (2013): Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen. ISO.

— ISO 50001 (2011): Energiemanagement – Energiemanagementsysteme – Anforderungen mit Anleitung zur Anwendung. ISO.

— Melde- und Analysestelle Informationssicherung (MELANI) (diverse Jahrgänge): Informationssicherung. Lage in der Schweiz und international. Halbjahresbericht. EFD und VBS, Bern.

— National Institute of Standards and Technology (NIST) (2018): Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. NIST.

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