Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bern, 13. November 2024

Massnahmen gegen Ransomware-Angriffe

Bericht des Bundesrats in Erfüllung des Postulates 21.4512 Graf-Litscher vom 16. Dezember 2021

Inhaltsverzeichnis

1 Einleitung ... 3

1.1 Allgemeines ... 3
1.2 Prüfauftrag ... 4

2 Schutzmassnahmen gegen Ransomware-Angriffe ... 5

2.1 Anleitungen und Richtlinien des Bundes ... 6
2.1.1 Informationen des BACS ... 6
2.1.2 IKT-Minimalstandard ... 9

2.2 Rechtliche Cybersicherheitsvorgaben ... 9
2.2.1 Energieversorgungsunternehmen ... 9
2.2.2 Rohrleitungsanlagen ... 9
2.2.3 Finanzmarkt ... 10
2.2.4 IKT-Grundschutz in der Bundesverwaltung ... 10
2.2.5 Datenschutzrechtliche Vorgaben an die Cybersicherheit ... 11
2.2.6 Informationssicherheitsrechtliche Vorgaben an die Cybersicherheit ... 12

2.3 Ergebnis der Prüfung ... 13

3 Einführung einer Meldepflicht bei Lösegeldzahlungen sowie Verpflichtung des Einbezugs von Behörden in die Verhandlungen mit den Kriminellen ... 13

3.1 Bestehende rechtliche Grundlagen ... 14
3.1.1 Mögliche strafrechtliche Konsequenzen bei der Zahlung von Lösegeld ... 14
3.1.2 Keine Meldepflicht bei Ransomware-Lösegeldzahlung und keine Pflicht zum Einbezug der Behörden für die Verhandlungen ... 15

3.2 Rechtsvergleich ... 17
3.2.1 Keine Meldepflicht bei Lösegeldzahlungen bei Ransomware-Angriffen ... 17
3.2.2 Verpflichtung des Einbezugs von Behörden in Verhandlungen mit Ransomware-Angreifern ... 18
3.2.3 Ergebnis des Rechtsvergleichs ... 19

3.3 Gesetzgeberische Möglichkeiten in der Schweiz ... 19
3.3.1 Beibehaltung der aktuellen Regelungen (keine spezifischen Massnahmen) ... 19
3.3.2 Einführung von Meldepflichten für Ransomware-Angriffe sowie für Lösegeldzahlungen und staatliche Unterstützung bei Verhandlungen ... 20
3.3.3 Verbot von Lösegeldzahlungen ... 21

3.4 Ergebnis der Prüfung ... 22

4 Stärkung des Informationsaustauschs ... 22

4.1 Informationsaustausch zur Verbesserung der Prävention und Reaktion ... 23
4.2 Informationsaustausch zur Verbesserung der Strafverfolgung ... 24
4.3 Ergebnis der Prüfung: Mögliche Umsetzung eines verstärkten Informationsaustauschs ... 24

5 Schlussbetrachtung ... 25

1 Einleitung

1.1 Allgemeines

Cyberangriffe auf Unternehmen und Behörden sind für diese ernstzunehmende Bedrohungen, da sie gravierende Auswirkungen auf den operativen Betrieb haben können und oft zu grossen finanziellen Einbussen und zu Reputationsschäden führen. Die Entwicklung der Cyberkriminalität über die letzten Jahre hat gezeigt, dass grundsätzlich alle Unternehmen und Organisationen potentielle Angriffsziele von Ransomware-Angriffen sind. In praktisch allen durch das Bundesamt für Cybersicherheit (BACS) begleiteten Ransomware-Vorfällen gingen die Cyberkriminellen opportunistisch vor und griffen dort an, wo sie mit möglichst wenig Aufwand einen möglichst hohen Ertrag in möglichst kurzer Zeit erzielen konnten. Entgegen der weit verbreiteten Annahme wählen Cyberkriminelle ihre Ziele für Ransomware-Angriffe meist nicht gezielt aus. Stattdessen nutzen sie häufig Schwachstellen, die daraus resultieren, dass Organisationen grundlegende und Sicherheitsmassnahmen im Bereich der Cybersicherheit nicht vollständig umgesetzt haben. Diese Lücken in der digitalen Verteidigung machen viele Unternehmen und Institutionen zu leichteren, wenn auch unbeabsichtigten Zielen für solche Angriffe.[1]

Als besonders lukratives Geschäftsmodel hat sich bei den Cyberkriminellen die Erpressungen durch die bereits erwähnten Ransomware-Angriffe[2] erwiesen. Die Angreifer dringen dabei in IT-Systeme ein, um Personen- sowie Geschäftsdaten zu entwenden oder sie zu verschlüsseln und fordern für die Rückgabe oder Entschlüsselung ein Lösegeld. Die Lösegeldzahlungen erfolgen fast immer über Kryptowährungen, so dass die Identifizierung der Cyberkriminellen erheblich erschwert oder in vielen Fällen gar unmöglich ist.[3]

Die Schweizer Unternehmen und Behörden gelten im internationalen Vergleich als zahlungskräftig und sind damit ein attraktives Ziel für Cyberkriminelle. Auch kleine und mittlere Unternehmen (KMU), welche oft über weniger Wissen und Ressourcen im Cybersicherheitsbereich verfügen, geraten deshalb zunehmend ins Visier der Angreifer. Dem BACS wurden im Jahr 2023 rund hundert Ransomware-Angriffe auf Unternehmen, Behörden sowie Privatpersonen gemeldet.[4] Da es keine Meldepflicht für solche Cyberangriffe gibt, ist davon auszugehen, dass diese Zahl längst nicht alle erfolgreichen Ransomware-Angriffe im letzten Jahr in der Schweiz beinhaltet. Die Cyberkriminellen haben sich stark professionalisiert und komplexe, arbeitsteilige Strukturen aufgebaut, so dass es wie in einem Unternehmen verschiedene Spezialisten innerhalb einer Gruppe gibt, welche für bestimmte Bereiche zuständig sind (z.B. Programmierer für die Erstellung von Schadsoftware, Hacker, Spezialisten für die Kommunikation mit Opfern oder die Geldwäsche). So können sie grosse und ausgefeilte Angriffe durchführen, was die Bekämpfung für Sicherheitsbehörden erheblich erschwert. Es entstehen zudem laufend neue Gruppen, welche typischerweise in Staaten tätig sind, in denen eine effektive Strafverfolgung nicht gewährleistet ist. Die geopolitischen Spannungen akzentuieren dieses Problem zusätzlich und erschweren die internationale Zusammenarbeit in der Strafverfolgung. Die Strafverfolgung der Angreifer entpuppt sich daher als eine komplexe Angelegenheit, welche viele

---

1 Vgl. hierzu: Bundesamt für Cybersicherheit (BACS; vormals NCSC), Erfolgreiche Ransomware-Angriffe auf Schweizer Unternehmen, vom 18. August 2024 (Webseite: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/ransomware-8.html; zuletzt besucht am 20. Oktober 2024).

2 Ransomware ist eine Art von Schadsoftware, die die Daten einer Organisation verschlüsselt und eine Zahlung als Bedingung für die Wiederherstellung des Zugriffs auf diese Daten fordert. Ransomware kann auch dazu verwendet werden, die Informationen einer Organisation zu stehlen und zusätzliche Zahlungen dafür zu verlangen, dass diese Informationen nicht an Behörden, Wettbewerber oder die Öffentlichkeit weitergegeben werden] (vgl. NISTIR 8374, Cybersecurity Framework Profile for Ransomware Risk Management; Webseite: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf; zuletzt besucht am 20. Oktober 2024).

3 Wenn bloss ein Lösegeld für die Entschlüsselung der Daten verlangt wird, dann spricht man von einer sog. «single extortion». Die doppelte Erpressung (sog. «double extortion») geht einen Schritt weiter: Hier drohen die Angreifer zusätzlich damit, sensible Daten zu veröffentlichen. Bei der dreifachen Erpressung (sog. «triple extortion») kommen noch Drohungen gegen Dritte hinzu, wie etwa Kunden oder Geschäftspartner des Opfers.

4 Vgl. hierzu: Bundesamt für Cybersicherheit (BACS), Informationssicherung, Lage in der Schweiz und International, Halbjahresbericht 2023/II (Juli – Dezember), vom 6. Mai 2024, S. 15 (Webseite: https://www.newsd.admin.ch/newsd/message/attachments/87433.pdf; zuletzt besucht am 20. Oktober 2024 und Bundesamt für Cybersicherheit (BACS), Informationssicherung, Lage in der Schweiz und International, Halbjahresbericht 2023/I (Januar – Juni), vom 2. November 2023, S. 4 und 20 f. (Webseite: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/lageberichte/NCSC_2023-1_HJB_DE.pdf.download.pdf/NCSC_2023-1_HJB_DE.pdf; zuletzt besucht am 20. Oktober 2024).

Ressourcen bindet und nur selten vom Erfolg gekrönt ist. Adäquate präventive Massnahmen für die Cybersicherheit sind daher unabdingbar.

Aufgrund des gut funktionierenden Geschäftsmodells der Cyberkriminellen, ist eine weitere Zunahme dieser Angriffe zu befürchten. Cybersicherheitsexperten gehen davon aus, dass die verschiedenen kriminellen Gruppen über Ransomware-Angriffe jährlich mehrere Milliarden US-Dollar einnehmen.[5] Cyberkriminelle setzen die Höhe ihrer Lösegeldforderungen so fest, dass sie unter den Kosten für die Behebung der Schäden durch die Angriffe, insbesondere für die Wiederherstellung der Daten, liegen. Dadurch ist es für viele Organisationen wirtschaftlich gesehen vorteilhafter, den Forderungen der Kriminellen nachzukommen. Die zahlenden Organisationen können damit zwar möglicherweise ihrem Datenverlust und der Betriebsunterbrechung abhelfen, unterstützen aber durch ihr Verhalten den Erfolg und den weiteren Ausbau des Geschäftsmodells der Cyberkriminellen. Als Folge steigen die wirtschaftlichen Kapazitäten der Cyberkriminellen und so im Endeffekt die Bedrohung durch Cybererpressungen.

In der Schweiz wirkt sich die Zunahme von Ransomware-Angriffen auf die öffentliche Sicherheit und die Wettbewerbsfähigkeit der Wirtschaft aus. Öffentliche Einrichtungen und Verwaltungen sind bei Ransomware-Angriffen besonders verwundbar. Datenverluste und Betriebsunterbrechungen können ihre Arbeit stark beeinträchtigen, was sowohl die Sicherheit als auch die Zuverlässigkeit öffentlicher Dienste gefährdet. Unternehmen stehen zudem vor erheblichen finanziellen Belastungen durch Lösegeldzahlungen, Wiederherstellungskosten und Reputationsschäden. Diese Angriffe destabilisieren nicht nur die betroffenen öffentlichen Einrichtungen, Behörden und Unternehmen, sondern schwächen auch das Vertrauen in die digitalen Infrastrukturen.

Der Schutz vor Ransomware ist nicht nur eine technische, sondern auch eine wirtschaftliche und gesellschaftliche Herausforderung:

- *Technische Herausforderung*: Die stete Weiterentwicklung von Ransomware stellt eine technische Herausforderung dar, da Behörden und Unternehmen kontinuierlich in aktuelle Sicherheitslösungen investieren und ihre IT-Infrastrukturen anpassen müssen, um neuen Bedrohungen zu begegnen.
- *Wirtschaftliche Herausforderung*: Die Implementierung umfassender Sicherheitsmassnahmen kann beachtliche Kosten verursachen, insbesondere für KMU.
- *Gesellschaftliche Herausforderung*: Es mangelt oft an Bewusstsein für die Bedeutung der Cybersicherheit. Initiativen zur Sensibilisierung und Aufklärung helfen mit, das Problembewusstsein zu stärken und eine Kultur der Sicherheit zu fördern. Kooperationen zwischen den Behörden und Unternehmen sind wichtig, um das Wissen und die Ressourcen zur Cybersicherheit breiter zu verankern und effizient zu nutzen.

1.2 Prüfauftrag

Der Bundesrat wurde mit dem am 16. Dezember 2021 überwiesenen Postulat 21.4512 Graf-Litscher «Massnahmen für einen besseren Schutz gegen Ransomware-Angriffe» mit der Prüfung folgender Fragestellungen beauftragt:

[5] Schwere Angriffe mit Datendiebstahl und -verschlüsselung können je nach Branche und Grösse CHF 50 bis 150 Mio. CHF kosten. Fällt bei einer solchen Attacke die IT komplett aus, so dauert es teils 5 bis 7 Tage, bis sich der Betrieb zumindest notdürftig wieder aufnehmen lässt. Die Dunkelziffer der Schäden ist aber gross, da viele Unternehmen und Behörden den Gang an die Öffentlichkeit aus Furcht vor Reputationsschäden scheuen (Vgl. KÜDERLI URS/DOHREN JOHANNES, PWC, «Im Fokus Cybersecurity: Wer zahlt, bleibt angreifbar», ohne Datumsangabe (https://www.pwc.ch/de/insights/disclose/33/cyberangriffe-wer-zahlt-bleibt-angreifbar.html; Webseite zuletzt besucht am 20. Oktober 2024; siehe hierzu bereits RASCH MICHAEL, Firmen scheuen die Anzeige von Cyberangriffen, in: NZZ Nr. 133, 12. Juni 2017, S. 20). Es wird vermutet, dass sich weltweit der wirtschaftliche Schaden, der jährlich durch Cyberkriminalität entsteht, auf über USD 900 Milliarden beläuft (GEIGER MICHAELA, «Hackerangriffe werden immer massiver, Cyberattacken: Banken und Versicherungen zahlen am häufigsten Lösegeld», vom 7. April 2023; Webseite: https://www.handelszeitung.ch/insurance/neue-studie-zu-cyberattacken-banken-und-versicherer-zahlen-am-haufigsten-losegeld-589550; Webseite zuletzt besucht am 20. Oktober 2024). Die Europäische Union geht gar von geschätzten jährlichen Kosten durch Cyberkriminalität in Höhe von 5,5 Billionen EUR aus (vgl. hierzu Webseite: https://digital-strategy.ec.europa.eu/de/library/cyber-resilience-act; Webseite zuletzt besucht am 20. Oktober 2024).

> «Cyberangriffe über Verschlüsselungstrojaner (sogenannte Ransomware) sind eine der grössten Cyberbedrohungen unserer Wirtschaft und Verwaltung geworden. Solche Angriffe sind für Cyberkriminelle attraktiv, weil es ihnen mit vergleichsweise wenig Aufwand gelingt, Systeme zu verschlüsseln und weil einzelne Unternehmen und Organisationen viel Lösegeld bezahlen, um die Verschlüsselung rückgängig zu machen.
>
> Für die Sicherheit der Bevölkerung und den Wirtschaftsstandort Schweiz ist es von grosser Bedeutung, dass der Schutz vor Ransomware gestärkt wird. Der Bundesrat wird deshalb gebeten, in einem Bericht darzulegen, über welche Massnahmen dies erreicht werden kann. Er soll dabei insbesondere folgende Massnahmen prüfen:
>
> 1. Einführung von verbindlichen Vorgaben für Organisationen mit öffentlichem Auftrag für den grundlegenden Schutz vor Ransomware-Angriffen.
> 2. Einführung einer Meldepflicht bei Lösegeldzahlungen sowie einer Verpflichtung, Behörden in die Verhandlungen mit den Kriminellen einzubeziehen.
> 3. Stärkung des Austausches von Informationen über versuchte und erfolgreiche Ransomware-Angriffe zwischen dem Bund, den Strafverfolgungsbehörden der Kantone, den privaten Security Incident Response Firmen und den Versicherungen.»

Der Bundesrat hat dem Nationalrat am 16. Februar 2022 die Annahme des Postulats beantragt. Das Postulat wurde am 8. Juni 2022 vom Nationalrat angenommen.

Der vorliegende Bericht zeigt auf, welche Schutzmassnahmen bestehen, in welchen Bereichen sie bereits vorgeschrieben sind und beurteilt dann, ob es nötig ist, zusätzliche verbindliche Vorgaben für Organisationen mit öffentlichem Auftrag zu erlassen. In einem nächsten Kapitel wird die Forderung nach einer Meldepflicht bei Lösegeldzahlungen geprüft. Dazu wird erläutert, welche rechtlichen Vorgaben in Bezug auf Meldepflichten im Zusammenhang mit Cyberangriffen es heute in der Schweiz gibt und in einem Rechtsvergleich aufgezeigt, wie andere Länder mit der Frage nach Meldepflichten umgehen. Daraus abgeleitet werden dann die Optionen der Schweiz für die Frage nach Meldepflichten bei Lösegeldzahlungen aufgezeigt. Im letzten Kapitel wird dann das Thema des Informationsaustausches besprochen. Es wird aufgezeigt, welcher Austausch heute stattfindet und wie er künftig gestärkt werden könnte. In den Schlussbetrachtungen werden die Prüfergebnisse bewertet und das weitere Vorgehen aufgezeigt.

2 Schutzmassnahmen gegen Ransomware-Angriffe

Cybersicherheit ist heute kein technisches Randthema mehr. Seit mehreren Jahren ist unbestritten, dass Cyberbedrohungen ein bedeutendes wirtschaftliches und gesellschaftliches Risiko darstellen. Entsprechend wurden verschiedene technische und organisatorische Massnahmen entwickelt, die den Schutz vor Cyberangriffen stärken sollen. Diese Massnahmen werden in Anleitungen und Richtlinien beschrieben. Es liegt grundsätzlich in der Eigenverantwortung der Unternehmen und Behörden, diese Schutzmassnahmen soweit umzusetzen, dass das Risiko von Cyberangriffen für sie tragbar ist.
Durch Cyberangriffe auf Organisationen entstehen aber häufig auch Schäden bei Dritten. Beispielsweise können Dienstleistungen zeitweise nicht mehr bezogen oder es besteht die Gefahr, dass gestohlene Personen- und/oder Geschäftsdaten veröffentlicht werden. Die Unternehmen und Behörden müssen sich deshalb nicht nur aus Eigeninteresse vor Cyberangriffen schützen, sondern tragen eine darüberhinausgehende Verantwortung für die Cybersicherheit ihrer Kunden, Mitarbeitenden und Partnerorganisationen. Dieser Verantwortungsaspekt stellt sich insbesondere dann, wenn es sich bei den Organisationen um solche mit einem öffentlichen Auftrag handelt. Darunter sollen in diesem Bericht Organisationen verstanden werden, die für Aufgaben im öffentlichen Interesse staatliche Finanzierung erhalten. Sie können sowohl in öffentlichem als auch in privatem Besitz sein. Darunter fallen insbesondere folgende Kategorien:

- *Öffentliche Verwaltungen*: Bundes-, Kantons- und Gemeindeverwaltungen, die öffentliche Aufgaben wahrnehmen und staatliche Dienstleistungen anbieten.
- *Öffentliche Institutionen*: Schulen, Universitäten, Krankenhäuser und andere Bildungseinrichtungen oder Gesundheitsdienstleister usw., die durch öffentliche Mittel finanziert werden oder öffentliche Aufgaben erfüllen.
- *Öffentliche Versorgungsunternehmen*: Unternehmen, die grundlegende Infrastrukturdienste für die Öffentlichkeit bereitstellen, wie Wasser-, Energie- und Abfallwirtschaft, Telekommunikationsdienste und öffentlicher Verkehr.

Diese Abgrenzung ist insbesondere für das Verständnis der rechtlichen Rahmenbedingungen wichtig, da sich die Anwendbarkeit der einschlägigen Gesetze, namentlich des Informationssicherheitsgesetzes[6] und des Datenschutzgesetzes[7], je nach Art des Auftrags sowie der Organisationsform unterscheidet.

Im vorliegenden Kapitel wird beschrieben, welche Cybersicherheitsschutzmassnahmen der Bund bereits heute mittels Anleitungen und Richtlinien vorsieht oder rechtlich vorgeschrieben werden. Weiter wird dargelegt, welche Vorschriften für die Umsetzung von Schutzmassnahmen für Organisationen mit öffentlichem Auftrag heute bereits gelten. Auf dieser Basis kann dann beurteilt werden, ob zusätzliche verbindliche Vorgaben für Organisationen mit öffentlichem Auftrag für den grundlegenden Schutz vor Ransomware-Angriffen gemacht werden sollen.

2.1 Anleitungen und Richtlinien des Bundes

Für Cyberangriffe nutzen die Täter Schwächen beim technischen Schutz von Systemen oder menschliche Fehler aus. Die meisten Cyberangriffe werden zu kriminellen Zwecken durchgeführt. Hierbei gehen die Angreifer meist opportunistisch vor, da sie mit möglichst geringem Aufwand möglichst viel Gewinn erzielen wollen. Das bedeutet, dass sie ihre Opfer nicht gezielt auswählen, oft vergleichsweise einfache Methoden anwenden und dort angreifen, wo sich eine günstige Gelegenheit bietet. Dies ist ein wichtiger Unterschied zu Akteuren, welche gezielt zu Zwecken der Spionage oder gar der Sabotage für sie interessante Organisationen angreifen und dabei sehr ausgeklügelte Methoden anwenden.

Für den Schutz vor finanziell motivierten Ransomware-Angriffen bedeutet dies, dass es um den Schutz vor opportunistischen Angriffen geht. Gegen solche sind vergleichsweise einfache Schutzmassnahmen bereits wirksam. Das effektivste Mittel, um Cybererpressungen infolge von Ransomware-Angriffen zu verhindern, ist, sich proaktiv vor diesen Angriffen durch organisatorische und technische Massnahmen zu schützen.

Das BACS sowie andere Stellen der Bundesverwaltung wie beispielsweise das Bundesamt für wirtschaftliche Landesversorgung (BWL) stellen auf ihren Webseiten Informationen, Anleitungen und Richtlinien zu IT-Grundschutzmassnahmen (z. B. Massnahmen gegen Ransomware) bereit, an welchen sich auch Organisationen mit öffentlichem Auftrag orientieren können.

2.1.1 Informationen des BACS

Der Bundesrat hat dem BACS gestützt auf Art. 15*a* Abs. 2 Bst. d und e Organisationsverordnung VBS (OV-VBS)[8] den Auftrag erteilt, Informationen zu Cybervorfällen, soweit dies dem Schutz vor Cyberbedrohungen dient, zu veröffentlichen und betroffene Unternehmen, Behörden sowie Privatpersonen vor unmittelbaren Cyberbedrohungen oder laufenden Cyberangriffen zu warnen. Ein wichtiger Teil dieses Auftrags besteht in der Veröffentlichung von Warnungen betreffend aktuelle Schwachstellen oder neuer Angriffsmethoden. Das BACS informiert dazu über seine Webseite und auf

6 Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG; SR **128**).
7 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG; SR **2351**).
8 Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (SR **172.214.1**).

der Informationsaustauschplattform für Betreiberinnen kritischer Infrastrukturen, dem Cyber Security Hub (CSH). Zudem informiert es Organisationen, bei denen kritische Schwachstellen entdeckt werden und welche eine unmittelbare Bedrohung für sie darstellen. So hat das BACS beispielsweise im Jahr 2022 über 2'000 Unternehmen in der Schweiz auf kritische Schwachstellen aufmerksam gemacht, welche nachweislich bereits von mehreren kriminellen Gruppen aktiv ausgenutzt wurden, um Unternehmen in der Schweiz mit Ransomware zu erpressen.[9]

Wichtig sind jedoch nicht nur aktuelle Warnungen zu aktuellen Schwachstellen und Angriffsmethoden, sondern auch Empfehlungen und Anleitungen zu Schutzmassnahmen. Das BACS listet auf seiner Webseite unter anderem die wichtigsten präventiven Schutzmassnahmen gegen Ransomware auf.[10] Es beschreibt sowohl organisatorische als auch technische Massnahmen und weist darauf hin, dass durch die Kombination dieser Massnahmen sämtliche Entitäten ihre Abwehr gegen Ransomware-Angriffe signifikant stärken können. Nachfolgend werden die wichtigsten Massnahmen aufgeführt, die auch von Organisationen mit öffentlichem Auftrag berücksichtigt werden sollten:[11]

Zu den minimalen organisatorischen Schutzmassnahmen gehören:

- *Sensibilisierung und Schulung der Mitarbeitenden*: Eine wichtige Massnahme zur Abwehr von Ransomware-Angriffen ist die kontinuierliche Sensibilisierung und Schulung von Mitarbeitenden. Schulungsprogramme sollten regelmässig durchgeführt werden, um das Bewusstsein und den sicheren Umgang mit digitalen Mitteln wie z. B. E-Mails zu fördern. Dies soll dabei helfen, dass beispielsweise Mitarbeitende vorsichtig mit Anhängen und Hyperlinks in verdächtigen E-Mails umgehen und diese weder öffnen noch anklicken, sowie Absender kritisch überprüfen, um sicherzustellen, dass diese bekannt und vertrauenswürdig sind.[12] Eine Sensibilisierung sowie Schulung kann unter anderem durch E-Learning-Plattformen, Workshops und simulierte Phishing-Angriffe erreicht werden.
- *Implementierung von Sicherheitsrichtlinien*: Organisationen sollten im Rahmen ihrer IT-Governance Richtlinien und Verfahren zur Cybersicherheit entwickeln und implementieren. Dazu gehören unter anderem Prozesse für die schnelle Reaktion auf Sicherheitsvorfälle sowie für die Durchführung von Sicherungskopien und deren regelmässige Überprüfung.

Zu den minimalen technischen Schutzmassnahmen gehören:

- *Regelmässige Sicherungskopien*: Regelmässige Sicherungskopien der Daten gehören zu den wirksamsten Massnahmen gegen Ransomware-Angriffe. Ein detailliertes «Backup & Restore-Konzept» hilft die Häufigkeit der Durchführung von Sicherungskopien, die Testmassnahmen für Wiederherstellungen sowie spezifische Verfahren für regelmässige Überprüfungen festzulegen und stellt sicher, dass im Falle eines Sicherheitsvorfalls oder Systemausfalls eine zuverlässige und zeitnahe Datenwiederherstellung möglich ist. Bei der Erstellung von Sicherungskopien sollte zudem das Generationenprinzip[13] genutzt werden. Des Weiteren sollte sichergestellt werden, dass das Medium, auf welchem die Sicherungskopie erstellt wird, nach dem Sicherungsvorgang vom Computer bzw. dem Netzwerk physisch getrennt und sicher aufbewahrt wird, um sie so vor Verschlüsselung durch Ransomware zu schützen.

---

9 Bundesamt für Cybersicherheit (vormals NCSC), Update: Noch immer über 2'000 ungesicherte Microsoft Exchange-Server in der Schweiz, vom 1. Dezember 2022 (Webseite: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/schwachstelle-proxynotshell-2.html; zuletzt besucht am 20. Oktober 2024).

10 Vgl. Webseite: https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/ransomware.html; zuletzt besucht am 20. Oktober 2024.

11 Vgl. hierzu die Inhalte der Webseite: https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen/ransomware.html; zuletzt besucht am 20. Oktober 2024.

12 Vgl. hierzu ausführlich die Webseite: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-private/aktuelle-themen/umgang-mit-e-mails.html; zuletzt besucht am 20. Oktober 2024.

13 Das Generationenprinzip bei Sicherungskopien, auch als Generationen-Backup bekannt, ist eine Strategie zur Datensicherung, die mehrere Versionen der gesicherten Daten über einen gewissen Zeitraum hinweg aufbewahrt. Dabei werden regelmässig Kopien erstellt und in verschiedenen «Generationen» gespeichert. Typischerweise gibt es tägliche, wöchentliche und monatliche Sicherungen. Die neueste Kopie ist die «jüngste Generation», während ältere Kopien als «ältere Generationen» bezeichnet werden. Dieses System ermöglicht es, nicht nur auf die aktuellsten Daten zuzugreifen, sondern auch auf frühere Versionen zurückzugreifen, falls Daten versehentlich gelöscht oder verändert wurden. So kann man beispielsweise eine Datei wiederherstellen, die vor einer Woche gelöscht wurde, oder auf den Zustand eines Systems vor einem Monat zurückgreifen. Das Generationenprinzip bietet somit einen umfassenden Schutz gegen Datenverluste und erhöht die Flexibilität bei der Datenwiederherstellung.

- *Aktualisierungen von Software und Betriebssystemen*: Software und Betriebssysteme sollten regelmässig aktualisiert werden, um bekannte Schwachstellen zu beheben. Sämtliche Systeme sollten konsequent und zeitnah mit Sicherheitsaktualisierungen (Updates) versorgt werden. Updates, welche kritische Sicherheitslücken in über das Internet erreichbare Systeme beheben, sollten innerhalb 24 Stunden vorgenommen werden. Software oder Systeme, welche vom Hersteller nicht mehr unterstützt werden, sollten abgeschaltet oder in eine separate, abgeschottete Netzzone verlegt werden.
- *Absicherung von Fernzugängen*: Virtuelles Privates Netzwerk (VPN), Remote Desktop Protokoll (RDP) und Citrix sind Technologien, die häufig für den Fernzugriff auf Computersysteme und Netzwerke genutzt werden. All diese Fernzugänge sowie sämtliche andere Zugänge auf interne Ressourcen (z. B. Webmail, Sharepoint, usw.) sollten mit Multi-Faktor-Authentifizierungen (MFA)[14] abgesichert werden. Dies gilt unter anderem auch für Zugänge von IT-Dienstleistern sowie Vertragspartner.
- *Verwendung von AppLockern*: Der Schutz einer IT-Infrastruktur vor Schadsoftware wie Ransomware kann durch die Verwendung von spezifischen Computerprogrammen, welche auch «AppLocker» genannt werden (z. B. Windows AppLocker, Gatekeeper, SELinux oder geeigneten Drittenanbieterlösungen etc.), zusätzlich gestärkt werden. Mit diesen lässt sich kontrollieren und definieren, welche Programme auf dem Computer in einer Organisationsumgebung ausgeführt werden dürfen.
- *Blockieren von gefährlichen E-Mail-Anhängen*: Organisationen sollen den Empfang von gefährlichen E-Mail Anhängen, also Datei-Typen, die oftmals für die Verbreitung von Malware verwendet werden, auf dem E-Mail-Gateway oder mittels dem Spam-Filter sperren oder zumindest in «Quarantäne» verschieben. Hierbei kann auf behördlich erstellte Listen zu blockierten Dateitypen zurückgegriffen werden. Gefährliche E-Mail-Anhänge sind auch dann zu blockieren, wenn diese Archiv-Dateien wie beispielsweise ZIP und RAR versenden. Zusätzlich sind sämtliche E-Mail-Anhänge zu sperren, welche Makros enthalten (z. B. Word, Excel oder PowerPoint-Anhänge).

Das BACS sensibilisiert zusammen mit Partnerorganisationen, Unternehmen, Organisationen und Privatpersonen über Ransomware-Angriffe und versucht so ein möglichst hohes Bewusstsein für die Cybersicherheit zu schaffen. Es führt dazu beispielsweise gemeinsam mit den Kantonspolizeikorps und weiteren Partnern regelmässig Sensibilisierungskampagnen durch.[15] Weitere vom BACS unterstützte Initiativen sind die Plattform für Internetsicherheit «iBarry.ch»[16] und die Labels «Cyber-safe.ch»[17], «Swiss Cyber Seal»[18] sowie der Cybersicherheits-Selbsttest «Cybero»[19]. Erwähnenswert in diesem Zusammenhang ist, dass es in der Schweiz auch regionale Initiativen zur Verbesserung der Cybersicherheit bei KMU gibt, wie z. B. «trust4sme»[20] im Kanton Waadt und «ITSec4KMU»[21] im Kanton Zug.

[14] Multi-Faktor-Authentifizierung ist ein Sicherheitsverfahren, bei dem Nutzer ihre Identität durch mindestens zwei verschiedene und voneinander unabhängige Komponenten nachweisen müssen, um Zugang zu einem Konto oder System zu erhalten. Typischerweise kombiniert es etwas, das der Nutzer weiss (wie ein Passwort), mit etwas, das er besitzt (wie ein Smartphone für einen Bestätigungscode) oder etwas, das er ist (wie ein Fingerabdruck). Diese Methode erhöht die Sicherheit erheblich, da ein potenzieller Angreifer mehrere Hürden überwinden müsste, um unbefugten Zugriff zu erlangen.

[15] Ein Beispiel dafür ist die Kampagne S-U-P-E-R, vgl. Website: https://www.s-u-p-e-r.ch/de/; zuletzt besucht am 20. Oktober 2024.

[16] Vgl. https://www.ibarry.ch/; zuletzt besucht am 20. Oktober 2024.

[17] Vgl. https://www.cyber-safe.ch/; zuletzt besucht am 20. Oktober 2024.

[18] Vgl. https://www.digitalsecurityswitzerland.ch/de/cyberseal; zuletzt besucht am 20. Oktober 2024.

[19] Vgl. Webseite: https://cybero.ch/; zuletzt besucht am 20. Oktober 2024.

[20] Vgl. Webseite: https://trustvalley.swiss/trust4smes/; zuletzt besucht am 20. Oktober 2024.

[21] Vgl. Webseite: https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/zuger-regierungsrat-lanciert-cybersecurity-offensive; zuletzt besucht am 20. Oktober 2024.

2.1.2 IKT-Minimalstandard

Die Nationale Cyberstrategie (NCS)[22] unterstützt die Umsetzung des vom BWL ausgearbeiteten Minimalstandards zur Verbesserung der Informations- und Kommunikationstechnik-Resilienz (IKT-Minimalstandard), um die allgemeine Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen.

Der IKT-Minimalstandard basiert auf dem US-amerikanischen National Institute of Standards and Technology (NIST) Cybersecurity Framework.[23] Er enthält 108 Massnahmen, die in 23 Kategorien unterteilt sind. Mit Hilfe dieser strukturierten Einteilung in Massnahmen und Kategorien kann eine Organisation einschätzen, wie weit fortgeschritten und effektiv ihre Cybersicherheit ist. Gleichzeitig bietet diese Struktur einen Rahmen, um die Cybersicherheit systematisch zu verbessern. Die grundlegenden Massnahmen des Standards sind im Wesentlichen unveränderlich, erfordern jedoch für ihre Umsetzung eine gewisse Flexibilität, Anpassung an unternehmensspezifische und neue Bedrohungen und Gefährdungen, technische Hilfsmittel und entsprechendes Fachwissen.[24] Es werden darin keine technischen Lösungen vorgeschrieben, da die Entitäten diese selbständig zu erarbeiten haben. Sie können sich hierzu auch im Rahmen der bestehenden Verbandsstrukturen zusammenschliessen und einen entsprechenden branchenspezifischen Standard erarbeiten.

2.2 Rechtliche Cybersicherheitsvorgaben

Es bestehen bereits heute rechtlich verbindliche Vorgaben an die Cybersicherheit. Diese finden sich in sektorspezifischen Vorgaben zur Sicherheit. Bundesrat und Verwaltungsbehörden haben insbesondere auf Verordnungsebene für Energieversorgungsunternehmen, Rohrleitungsanlagen, den Finanzsektor und auch für die Bundesverwaltung spezifische Vorgaben zur Cybersicherheit erlassen.

Zusätzlich zu diesen sektorspezifischen Verordnungen spielen das Datenschutzgesetz (DSG)[25] sowie das Informationssicherheitsgesetz (ISG)[26] eine wichtige Rolle für die Cybersicherheit.

2.2.1 Energieversorgungsunternehmen

Das revidierte Bundesgesetz über die Stromversorgung (StromVG)[27] sowie die Stromversorgungsverordnung (StromVV)[28] traten per 1. Juli 2024 in Kraft.[29] Damit wurden verbindliche Anforderungen an die Informationssicherheit der IT und OT (Operative Technologie) der Schweizer Stromerzeuger, Netzbetreiber, Speicherbetreiber und Dienstleister erlassen. Das zu erreichende Schutzniveau hängt von der Leistungsfähigkeit der Systeme ab. Die Massnahmen zur Erreichung des Schutzniveaus werden aus dem vorerwähnten IKT-Minimalstandard des BWL abgeleitet.

2.2.2 Rohrleitungsanlagen

Der Bundesrat hat am 29. November 2023 mit den Art. 39*a* der Verordnung über Sicherheitsvorschriften für Rohrleitungsanlagen[30] verabschiedet, die Betreiber von Rohrleitungsanlagen zur Verbesserung ihrer Cybersicherheit verpflichtet und vorsieht, dass gemeinsame Richtlinien über die Cybersicherheit erarbeiten werden müssen. In der Folge hat die Gasbranche ihren «G1008 d Minimalstandard für die

---

22 Vgl. Nationale Cyberstrategie (NCS), (Webseite: https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html; zuletzt besucht am 20. Oktober 2024).
23 Vgl. Webseite: https://www.nist.gov/cyberframework; zuletzt besucht am 20. Oktober 2024.
24 Jedes Unternehmen kann durch eine Risikoanalyse selbst feststellen, ob die verpflichteten Minimalmassnahmen ausreichend oder zusätzliche Massnahmen erforderlich sind. Der Leitfaden Schutz kritischer Infrastrukturen (SKI), herausgegeben vom Bundesamt für Bevölkerungsschutz (BABS), kann die Unternehmen bei dieser Aufgabe unterstützen (vgl. hierzu die Webseite: https://www.babs.admin.ch/de/leitfaden-schutz-kritischer-infrastrukturen; zuletzt besucht am 20. Oktober 2024).
25 SR **235.1**
26 SR **128**
27 SR **734.7**
28 SR **734.71**
29 Vgl. hierzu den Erläuternder Bericht zum Vorentwurf zur Revision vom Mai 2024 der Stromversorgungsverordnung (Schutz vor Cyberbedrohungen) (Webseite: https://pubdb.bfe.admin.ch/de/publication/download/11501; zuletzt besucht am 20. Oktober 2024).
30 Rohrleitungsverordnung (RLSV); SR **746.12**.

Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Gasversorgung»[31], welcher auf dem vorerwähnten «IKT-Minimalstandard» basiert, überarbeitet. Aufgrund der zunehmenden Bedrohungen und angesichts der grossen Unterschiede bei der Umsetzung der Cybersicherheit ist es nach Ansicht des Bundesrates zwingend notwendig, diesen neuen Branchenstandard verbindlich zu erklären (vgl. hierzu Art. 39*a* Abs. 2 und 4 E-RLSV).[32] Aus diesem Grund hat das Eidgenössische Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) am 18. September 2024 die Vernehmlassung zu dieser Verordnungsänderung eröffnet.

2.2.3 Finanzmarkt

Als unabhängige Aufsichtsbehörde über den schweizerischen Finanzmarkt hat die Eidgenössische Finanzmarktaufsicht (FINMA) hoheitliche Befugnisse über Banken, Versicherungen, Börsen, Finanzinstitute, kollektive Kapitalanlagen, deren Vermögensverwalter und Fondsleitungen sowie Versicherungsvermittler. Die FINMA setzt sich für den Schutz der Gläubiger, Anleger und Versicherten sowie für den Schutz der Funktionsfähigkeit der Finanzmärkte ein. Im Rahmen der Revision des Rundschreibens 2008/21 von 2019, bei welcher es sich um eine Verwaltungsverordnung handelt, hat die FINMA verschiedene Ergänzungen im Bereich der Cyberrisiken aufgenommen. Nach diesen Regeln ist das Vorgehen zum Schutz vor Cyberrisiken zu dokumentieren. Die Dokumentation soll mindestens folgende Aspekte abdecken:[33]

- Identifikation der spezifischen Bedrohungspotenziale durch Cyberangriffe;
- Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyberangriffen;
- Zeitnahe Erkennung und Aufzeichnung von Cyberangriffen;
- Reaktion auf Cyberangriffen mit zeitnahen und gezielten Massnahmen;
- Sicherstellung der zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyberangriffen.

Die Finanzdienstleister sind zudem verpflichtet, regelmässig Verwundbarkeitsanalysen und Penetrationstests durchzuführen.

2.2.4 IKT-Grundschutz in der Bundesverwaltung

Die Fachstelle des Bundes für Informationssicherheit im Staatssekretariat für Sicherheitspolitik[34] kann gestützt auf Art. 29 Abs. 1 ISV[35] Verwaltungsverordnungen für die gesamte Bundesverwaltung über den Grundschutz der Informatikmittel («IKT-Grundschutz») erlassen und Vorgaben zur Netzwerksicherheit in der Bundesverwaltung festlegen. Mit der Weisung «Si001 – IT-Grundschutz in der Bundesverwaltung» vom 5. Juli 2024 wurde dies gemacht.[36] Der IKT-Grundschutz legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Für jedes Informatikschutzobjekt ist der IKT-Grundschutz in der Bundesverwaltung

---

31 Minimalstandard für die IKT-Sicherheit in der Gasversorgung (Webseite: https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard/ikt_branchenstandards/gasversorgung.html; zuletzt besucht am 20. Oktober 2024).

32 Vgl. hierzu die Medienmitteilung «UVEK startet Vernehmlassung zur Revision von Verordnungen im Energiebereich» vom 20. Oktober 2024 (Webseite: https://www.uvek.admin.ch/uvek/de/home/uvek/medien/medienmitteilungen.msg-id-102488.html; zuletzt besucht am 20. Oktober 2024), der Verordnungsentwurf (Webseite: https://pubdb.bfe.admin.ch/de/publication/download/11856; zuletzt besucht am 20. Oktober 2024) sowie der erläuternde Bericht (Webseite: https://pubdb.bfe.admin.ch/de/publication/download/11857; zuletzt besucht am 20. Oktober 2024) dazu.

33 FINMA Rundschreiben 2008/21 (vgl. hierzu die Webseite: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=de; zuletzt besucht am 19. Juni 2024) sowie ROLF H. WEBER/OKAN YILDIZ, Cybersicherheit und Cyber-Resilienz in den Finanzmärkten, 9. Band der Schriften des Center for information technology, society and law (ITSL), S. 33 (vgl. hierzu die Webseite: https://eizpublishing.ch/wp-content/uploads/2022/04/Cybersicherheit-und-Cyber-Resilienz-in-den-Finanzmaerkten-Digital-V1_01-20220404.pdf; zuletzt besucht am 20. Oktober 2024).

34 Art. 51 Abs. 6 ISV sieht vor, dass bis zum 30. Juni 2025 das BACS die Aufgaben und Kompetenzen der Fachstelle des Bundes für Informationssicherheit wahrnehmen wird. Danach wird diese Aufgabe dem Staatsekretariat für Sicherheitspolitik (SEPOS) zukommen.

35 SR **128.1**

36 Die am 1. Januar 2024 in Kraft getretene ISV sieht in Art. 51 Abs. 1 vor, dass vor Inkrafttreten dieser Verordnung durch das Nationale Zentrum für Cybersicherheit (NCSC), aus welchem seit dem 1. Januar 2024 das BACS wurde, erlassene Vorgaben zur Informatiksicherheit und bewilligte Ausnahmen gelten bis höchstens drei Jahre nach Inkrafttreten dieser Verordnung.

umzusetzen. Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verantwortlichen Verwaltungseinheiten zu dokumentieren und zu überprüfen.[37]

2.2.5 Datenschutzrechtliche Vorgaben an die Cybersicherheit

Das Datenschutzgesetz (DSG)[38] und die Verordnung über den Datenschutz (DSV)[39] spielen eine wichtige Rolle bei der Cybersicherheit von Bundesbehörden und von Unternehmen. Art. 8 Abs. 1 und 2 DSG verlangt, dass Entitäten, welche Personendaten verarbeiten, dem Risiko angemessen bestimmte technische und organisatorische Massnahmen für die Sicherheit dieser Daten ergreifen müssen, um so Verletzungen der Datensicherheit zu vermeiden. Der Bundesrat hat gestützt auf Art. 8 Abs. 3 DSG Bestimmungen über die Mindestanforderungen an die Datensicherheit erlassen (Art. 3 ff. DSV):

- *Technische Massnahmen*: Der Schutz von Personendaten soll mitunter durch Datenverschlüsselung erreicht werden, um unbefugten Zugriff zu verhindern. Mittels Zugriffskontrollen sind Mechanismen zu implementieren, die sicherstellen, dass nur autorisierte Personen Zugang zu sensiblen Daten haben. Des Weiteren gilt es, auch Aspekte der Netzwerksicherheit zu beachten, damit unbefugte Personen nicht auf diese Daten zugreifen können (z. B. Schutz der IT-Infrastruktur durch Firewalls, Intrusion Detection Systeme (IDS), Durchführung von Updates zwecks Sicherstellung der Systemsicherheit etc.).
- *Organisatorische Massnahmen*: Es müssen Sicherheitsrichtlinien und -verfahren zur Datensicherheit entwickelt und implementiert sowie regelmässige Schulungen für Mitarbeitende zu den Themen Datenschutz und Cybersicherheit durchgeführt werden, um das Bewusstsein und die Kompetenz in diesen Themen zu erhöhen.
- *Risikoanalysen und Datenschutz-Folgenabschätzungen*: Falls Organisationen mit öffentlichem Auftrag Personendaten bearbeiten, sind diese verpflichtet, regelmässige Risikoanalysen durchzuführen, um potenzielle Schwachstellen in ihren Systemen zu identifizieren und entsprechende Massnahmen zu ergreifen. Bei der Einführung neuer Systeme oder Prozesse, die Personendaten betreffen, müssen Datenschutz-Folgenabschätzungen bei einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person durchgeführt werden, um die Auswirkungen auf den Schutz der Daten zu bewerten und Massnahmen zur Risikominderung zu ergreifen.

Es kann daher mit Blick auf die vorerwähnten Massnahmen festgehalten werden, dass das DSG und die DSV wesentlich zur Verbesserung der Cybersicherheit bei Organisationen mit öffentlichem Auftrag beigetragen haben, indem sie ein hohes Schutzniveau für Personendaten vorschreiben und damit sicherstellen, dass diese Daten vor unbefugtem Zugriff und Missbrauch geschützt werden sollen, und hiervon die IKT-Infrastruktur gesamthaft profitiert.

Wenn nun aber private Unternehmen einen öffentlichen Auftrag wahrnehmen (z.B. Privatschulen, Altersheime), so unterstehen diese nicht dem DSG und der DSV des Bundes sondern den jeweiligen kantonalen Datenschutzgesetzen. Diese orientieren sich inhaltlich stark am Datenschutzgesetz des Bundes orientieren, um den Umgang mit personenbezogenen Daten auf kantonaler Ebene, insbesondere im öffentlichen Sektor, zu regeln. Diese kantonalen Rechtserlasse enthalten weitgehend ähnliche Grundsätze und Anforderungen an den Datenschutz wie das DSG sowie die DSV und dementsprechend kann bezüglich der Cybersicherheit sinngemäss auf die vorstehenden Ausführungen verwiesen werden.

---

37 Vgl. hierzu: Weisung «Si001 – IT-Grundschutz in der Bundesverwaltung» vom 5. Juli 2024 (Webseite: https://www.ncsc.admin.ch/dam/ncsc/de/dokumente/dokumentation/vorgaben/sicherheit/si001/Si001-IT-Grundschutz_V5-1-d.pdf.download.pdf/Si001-IT-Grundschutz_V5-1-d.pdf; zusetzt besucht am 20. Oktober 2024).

38 SR **235.1**

39 SR **235.11**

2.2.6 Informationssicherheitsrechtliche Vorgaben an die Cybersicherheit

Das Informationssicherheitsgesetz (ISG) und seine Ausführungsverordnungen traten per 1. Januar 2024 in Kraft, um den Schutz der Informationen und die Cybersicherheit des Bundes zu verstärken. Die Cybersicherheit des Bundes hört nicht bei der eigenen Informatikinfrastruktur auf. Auch bei Dritten, Kantonen und internationalen Partnern muss der Schutz der Informationen und Daten des Bundes gewährleistet sein. So unterstehen beispielsweise auch private Unternehmen und öffentliche Organisationen, die einen öffentlichen Auftrag im Sinne von Art. 2 Abs. 3 und 5 ISG wahrnehmen, nicht nur dem DSG, sondern auch dem ISG. Auch kantonale öffentliche Organe unterstehen, obwohl jeweils die kantonalen Datenschutzgesetze anwendbar sind, dem ISG, sofern sie auf Informatikmittel des Bundes zugreifen und nicht über eine mindestens gleichwertige Informationssicherheit verfügen (Art. 3 ISG). Arbeiten die verpflichteten Behörden und Organisationen mit Dritten zusammen, so sorgen sie dafür, dass die Anforderungen und Massnahmen nach diesem Gesetz in den entsprechenden Vereinbarungen und Verträgen festgehalten werden (Art. 9 ISG).

Das ISG und die ISV bieten für die Cybersicherheit wirksame und zeitgemässe Vorgaben, weil in verschiedenen Bestimmungen (Art. 6-23 ISG) Vorgaben zum Aufbau eines Informationssicherheits-Managementsystems (ISMS) gemacht werden:

- Betroffene Behörden und Organisationen müssen Informationen, die sie verarbeiten, identifizieren, ihren Schutzbedarf beurteilen (Art. 6 ISG) und klassifizieren (Art. 11-15 ISG).
- Es muss sichergestellt sein, dass angemessene Schutzmassnahmen ergriffen werden, um diese Informationen vor unbefugtem Zugriff, Verlust, Störung oder Missbrauch zu schützen (Art. 6-10 ISG).
- Die verpflichteten Behörden und Organisationen müssen dafür sorgen, dass Risiken für die Informationssicherheit laufend beurteilt werden (Art. 8 ISG).
- Beim Einsatz von Informatikmitteln, zu welchem gemäss Art. 5 ISG Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen gehören, muss ein Sicherheitsverfahren zur Gewährleistung der Informationssicherheit vorhanden sein. Informatikmitteln ist eine Sicherheitsstufe (Grundschutz, hoher Schutz, sehr hoher Schutz) zuzuordnen. Diese Sicherheitsstufen definieren jeweils die Mindestanforderungen und Sicherheitsmassnahmen (Art. 16-19 ISG).
- Es muss sichergestellt werden, dass Personen, die Zugang zu Informationen, Informatikmitteln, Räumlichkeiten und anderen Infrastrukturen des Bundes haben, sorgfältig ausgewählt und risikogerecht identifiziert werden und (Art. 20 ISG). Personal muss stufengerecht aus- und weitergebildet werden und gegebenenfalls zur Geheimhaltung verpflichtet werden.
- Die verpflichteten Behörden und Organisationen müssen für einen angemessenen physischen Schutz der Informationen und Informatikmittel sorgen. Räumlichkeiten und Bereiche können Sicherheitszonen zugeordnet werden, welche mit Kontrollen (z.B. Taschenkontrollen usw.) verbunden sein können (Art. 22-23 ISG).

Das Parlament hat am 29. September 2023 eine Änderung des ISG verabschiedet, mit welcher eine Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen eingeführt wird. Diese Vorlage schafft die gesetzlichen Grundlagen zur Meldepflicht für Betreiberinnen und Betreiber kritischer Infrastrukturen und definiert die diesbezüglichen Aufgaben des BACS, welches als zentrale Meldestelle für Cyberangriffe vorgesehen ist. Diese Meldepflicht ist noch nicht in Kraft, da zur Umsetzung dieser Neuerung Ausführungsbestimmungen erlassen werden müssen. Das Inkrafttreten dieser Bestimmungen wurde vom Bundesrat noch nicht festgelegt.

2.3 Ergebnis der Prüfung

Es gibt heute in der Schweiz mit Blick auf die in diesem Bericht dargelegten behördlichen Informationen, Anleitungen und Richtlinien, verordnungsbasierten Cybersicherheitsvorschriften sowie den datenschutz- und informationsrechtlichen Vorgaben zahlreiche behördlich vorgeschlagene oder rechtlich verbindliche IT-Schutzmassnahmen, welche auch von Organisationen mit öffentlichem Auftrag zu berücksichtigen sind oder herangezogen werden können, um die Cybersicherheit zu verbessern und damit auch einen Schutz vor Ransomware-Angriffen zu gewährleisten.

Aufgrund der verfassungsrechtlichen Kompetenzordnung zwischen Bund und Kantonen hat der Bund, unter Beachtung der Kantons- und Gemeindeautonomie, grundsätzlich keine Möglichkeit, Organisationen mit öffentlichem Auftrag, welche diesen kraft kantonalen oder kommunalen Rechts haben und auf welche nicht das DSG oder das ISG anwendbar sind, rechtlich verbindliche Cyberschutzmassnahmen vorzuschreiben. Diese Autonomie der Kantone und Gemeinden bedeutet mit anderen Worten, dass der Bund mangels einer verfassungsrechtlichen Grundlage für den Cyberbereich weder gesetzliche Vorgaben erlassen, noch eine Aufsicht über die Umsetzung von Schutzmassnahmen ausüben kann und die Verantwortung für die Implementierung entsprechender Schutzmassnahmen bei den jeweiligen kantonalen oder kommunalen Behörden liegt. Entsprechend müssen die Kantone und Gemeinden grundsätzlich eigenständig Regelungen und Massnahmen zum Schutz ihrer IT-Infrastrukturen festlegen und umsetzen. Aus diesem Grund verfügen die meisten Kantone auch über kantonale Cybersicherheitsstrategien oder -konzepte, welche die sich mitunter an der Nationalen Cyberstrategie (NCS) orientieren und Vorgaben für die Umsetzung von Cyberschutzmassnahmen machen. Des Weiteren können sich die kantonalen und kommunalen Gesetzgeber oder Behörden auch an den Inhalten der vorerwähnten Informationen, Anleitungen und Richtlinien des Bundes orientieren.

Der Bundesrat ist der Ansicht, dass die Einführung von flächendeckenden rechtlich verbindlichen Vorgaben für Organisationen mit öffentlichem Auftrag für den grundlegenden Schutz vor Ransomware-Angriffen nicht sinnvoll ist, weil der Bund bereits heute viel für eine Resilienz gegenüber Cyberangriffen und damit auch Ransomware-Angriffen tut. Er wirkt in diesem Bereich unterstützend, informiert transparent, setzt Anreize oder greift im Rahmen der in der Bundesverfassung festgehaltenen Kompetenzordnung sowie der bundesrechtlichen Rechtsgrundlagen regulativ ein, wie er dies jüngst bei den Stromversorgungs- und Rohrleitungsinfrastrukturen aufgrund ihrer volkswirtschaftlichen Bedeutung gemacht hat. Hierbei wird stets ein intensiver Austausch mit den betroffenen Akteuren geführt und eine enge Zusammenarbeit mit diesen angestrebt.

3 Einführung einer Meldepflicht bei Lösegeldzahlungen sowie Verpflichtung des Einbezugs von Behörden in die Verhandlungen mit den Kriminellen

Die Stärkung des Schutzes vor Cyberangriffen ist das wichtigste Mittel ist, um Ransomware-Angriffe zu verhindern. Trotz Schutzmassnahmen kann es aber zu erfolgreichen Angriffen kommen. Entsprechend muss die Reaktion auf Ransomware-Angriffe so ausgestaltet werden, dass Schäden so weit wie möglich verhindert und die Aktivitäten der Angreifer erschwert werden. Im Vordergrund steht die Frage, wie sichergestellt wird, dass in möglichst wenigen Fällen von Ransomware-Angriffen Lösegeld bezahlt wird.[40] Die vom Angriff betroffenen Organisationen können allenfalls durch die Lösegeldzahlung zwar

[40] Vgl. Webseite: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ransomware.html; zuletzt besucht am 20. Oktober 2024. Die Erfolgsquote bei der Datenwiederherstellung nach Lösegeldzahlung ist offenbar nicht so hoch, wie es sich die betroffenen Unternehmen wünschen. Statistiken zeigen, dass dies keine Garantie für die Datenwiederherstellung bietet. Laut dem «State of Ransomware Report 2023» von Sophos konnten nur 58 % der Organisationen nach der Lösegeldzahlung wieder auf ihre Daten zugreifen.

ihr eigenes Problem lösen, unterstützen aber durch ihr Verhalten den Erfolg und den weiteren Ausbau des Geschäftsmodells der Cyberkriminellen. Als Folge dieses Effekts steigen nicht nur die Kapazitäten der Cyberkriminellen, sondern auch die Attraktivität der Schweiz als Angriffsziel und dadurch im Endeffekt die Bedrohung durch Cybererpressungen.

Das Postulat 21.4512 Graf-Litscher fordert den Bundesrat diesbezüglich auf, zu prüfen, ob solchen Fehlanreizen mit der Einführung einer Meldepflicht bei Lösegeldzahlungen und einer Verpflichtung, Behörden in Verhandlungen mit Kriminellen einzubeziehen, entgegengewirkt werden kann.

In diesem Kapitel werden zunächst die bestehenden rechtlichen Grundlagen in Bezug auf Lösegeldzahlungen bei Ransomware-Angriffen erörtert, dann in einem kurzen Rechtsvergleich die Situation in anderen Staaten dargelegt und schliesslich die Handlungsoptionen der Schweiz beschrieben und bewertet.

3.1 Bestehende rechtliche Grundlagen

Um zu beurteilen, ob die zu prüfenden Massnahmen eingeführt werden sollten, muss geklärt werden, welche rechtlichen Grundlagen aktuell bei der Zahlung von Lösegeldern nach Ransomware-Angriffen zu beachten sind. Der Fokus liegt dabei auf den möglichen strafrechtlichen Konsequenzen einer Lösegeldzahlung und auf allfälligen Meldepflichten.

3.1.1 Mögliche strafrechtliche Konsequenzen bei der Zahlung von Lösegeld

In der Schweiz besteht kein allgemeines Verbot von Lösegeldzahlungen bei einem Ransomware-Angriff; solche Leistungen stehen daher grundsätzlich nicht unter Strafe.[41] Es gilt jedoch zu beachten, dass Ransomware-Lösegeldzahlungen mit Blick auf das zahlende Opfer[42] folgende strafrechtliche Konsequenzen nach sich ziehen können:

- *(Gehilfenschaft zur) Geldwäscherei (Art. 305bis StGB[43])*: Ransomware-Angreifer fordern häufig Zahlungen in Kryptowährungen, die normalerweise pseudonym erfolgen. Dies wirft die Frage auf, ob eine solche Lösegeldzahlung nicht als eine (Gehilfenschaft zur) Geldwäscherei (Art. 305bis StGB) betrachtet werden kann, insbesondere da das Unternehmen[44] und allenfalls gar die mandatierten Banken wissen oder davon ausgehen können, dass die Zahlung für illegale Aktivitäten erfolgt und es damit wahrscheinlich ist, dass auch Geldwäscherei involviert ist. Diese Fragestellung wurde bislang noch nicht höchstrichterlich geklärt. Überdies wäre im

Von denjenigen, die das Lösegeld zahlten, konnten nur 21 % ihre Daten vollständig wiederherstellen, während 37 % nur einen Teil der Daten zurückerhielten. Dies zeigt, dass selbst wenn Organisationen den Lösegeldforderungen nachkommen, die vollständige Datenwiederherstellung keineswegs garantiert ist. Die Zahlung des Lösegelds garantiert nicht nur keine vollständige Wiederherstellung, sondern kann auch die Wahrscheinlichkeit erhöhen, erneut Ziel eines Angriffs zu werden. Laut demselben Sophos-Bericht erlebten 80 % der Organisationen, die ein Lösegeld zahlten, einen weiteren Ransomware-Angriff, oft von derselben Gruppe (Webseite: https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/; zuletzt besucht am 20. Oktober 2024).

41 Vgl. FABIAN TEICHMANN/LÉONARD GERBER, Les cyberattaques per spyware – Poursuite et qualification en droit pénal suisse, in: Sicherheit & Recht 3/2021, OLIVER M. BRUPBACHER/CLAUDIA GÖRTZ STAEHELIN, Herausforderungen durch Cybersecurity in der modernen Unternehmensrealität, in: SJZ 118/2022, S. 518; YANIV BENHAMOU/LOUISE WANG, Cyberattaque et ransomware : risques juridiques à payer et assurabilité des rançons, in: SZW 2023, S. 83: «En droit suisse, aucun texte ne sanctionne expressément le paiement de la rançon par la victime» sowie DELPHINE SARASIN/SARA PANGRAZZI/PAULINE MEYER, The Legal Risks of Ransomware Payments, in: AJP 2023, S. 1080.

42 Die Frage der Strafbarkeit von Ransomware-Angreifern ist nicht Gegenstand der vorliegenden rechtlichen Abklärungen, daher wird nachfolgend lediglich der mögliche Deliktskatalog aufgelistet, welchen Angreifer allenfalls durch Ihrer Lösegeldforderung infolge eines Ransomware-Angriffs verwirklicht haben könnten: Art. 143 (Unbefugte Datenbeschaffung), Art. 143bis (Unbefugtes Eindringen in ein Datenverarbeitungssystem), Art. 144bis Ziff. 1 (Datenbeschädigung), Art. 144bis Ziff. 2 (Herstellen von datenschädigenden Programmen), Art. 147 (Computerbetrug), Art. 156 (Erpressung), Art. 179novies (Unbefugtes Beschaffen von Personendaten), Art. 260ter StGB (Kriminelle Organisationen; vgl. hierzu gesamthaft SANDRO GERMANN/DAVID WICKI-BIRCHLER, Hacking und Hacker im Schweizer Recht, in: AJP 2020, S. 87 ff.; TEICHMANN/GERBER, a.a.O., S. 124 ff. und BENHAMOU/WANG, a.a.O., S. 81 ff.).

43 SR **311.0**

44 Gemäss Art. 102 Abs.1 StGB kann sich auch ein Unternehmen (vgl. Legaldefinition in Art. 102 Abs. 4 Bst. a–d StGB) strafbar machen, wenn in einem Unternehmen in Ausübung geschäftlicher Verrichtung im Rahmen des Unternehmenszwecks ein Verbrechen oder Vergehen begangen wurde und diese Tat wegen mangelhafter Organisation des Unternehmens keiner bestimmten natürlichen Person zugerechnet werden kann, so wird das Verbrechen oder Vergehen dem Unternehmen zugerechnet. In Art. 102 Abs. 2 StGB wird präzisiert, dass, wenn es sich dabei um eine Straftat namentlich nach den Artikeln 260ter, 260quinquies, 305bis StGB handelt, das Unternehmen unabhängig von der Strafbarkeit natürlicher Personen bestraft wird, wenn dem Unternehmen vorzuwerfen ist, dass es nicht alle erforderlichen und zumutbaren organisatorischen Vorkehren getroffen hat, um eine solche Straftat zu verhindern (vgl. hierzu auch SARASIN/PANGRAZZI/MEYER, a.a.O., S. 1084).

Einzelfall jeweils zu prüfen, inwiefern sich die lösegeldzahlende Partei als Rechtfertigungsgrund auf einen Notstand (Art. 17 StGB) bzw. entschuldbaren Notstand (Art. 18 StGB) berufen kann.[45]

- *Unterstützung einer kriminellen Organisation (Art. 260ter StGB) und die Finanzierung des Terrorismus (Art. 260quinquies StGB)*: Falls kriminelle Organisationen oder Terrorgruppen durch Cyber-Lösegelderpressung Geld generieren, sind auch die Tatbestände der Unterstützung einer kriminellen Organisation (Art. 260ter StGB) und Finanzierung des Terrorismus (Art. 260quinquies StGB) zu prüfen. Anders als bei der Terrorismusfinanzierung reicht es bei der Unterstützung einer kriminellen Organisation aus, dass das Unternehmen zumindest eventualvorsätzlich damit rechnen muss, dass die Lösegeldzahlung der kriminellen Zwecksetzung der Organisation dient. Für Personen, die zu Unterstützungshandlungen wie z. B. Lösegeldzahlungen gezwungen werden, kommen als Rechtfertigungsgründe der Notstand (Art. 17 StGB) bzw. entschuldbare Notstand (Art. 18 StGB) in Frage.[46] Auch diese Fragestellung wurde bislang noch nicht höchstrichterlich geklärt. Erwähnenswert ist in diesem Zusammenhang, dass eine Lösegeldzahlung internationale Sanktionen und Massnahmen im Kampf gegen Terrorismusfinanzierung oder verhängte Embargos verletzen könnte.[47]

3.1.2 Keine Meldepflicht bei Ransomware-Lösegeldzahlung und keine Pflicht zum Einbezug der Behörden für die Verhandlungen

In der Schweiz muss die Leistung einer Ransomware-Lösegeldzahlung den Behörden nicht gemeldet werden, und es gibt auch keine gesetzliche Regelung, die Unternehmen oder Einzelpersonen dazu verpflichtet, Behörden in die Verhandlungen mit Ransomware-Angreifern einzubeziehen. Dies bedeutet, dass die Entscheidung, ob und in welcher Form staatliche Stellen konsultiert oder informiert werden, im Ermessen des betroffenen Unternehmens oder der betroffenen Person liegt.

Es gibt Meldepflichten gegenüber Behörden bei Cyberangriffen, welche nachfolgend erörtert werden:

- *Meldungen von Verletzungen der Datensicherheit gemäss der Datenschutzgesetzgebung*: Das revidierte Datenschutzgesetz (DSG) und die Verordnung über den Datenschutz (DSV) beinhalten die oben dargelegten Anforderungen an technische und organisatorische Massnahmen zur Cybersicherheit.[48] Verletzungen der Datensicherheit («Databreach» genannt), welche typischerweise auch durch einen Ransomware-Angriff passieren, müssen gemäss Art. 24 Abs. 1 DSG dem Eidgenössischen Datenschutzbeauftragten (EDÖB) gemeldet werden, falls diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen. Das bedeutet, dass namentlich Verletzungen der Datensicherheit an den EDÖB meldepflichtig sind, welche dazu führen, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert, Unbefugten offengelegt oder zugänglich gemacht werden und dies voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte von betroffenen Personen führt. Für die Meldung hat der EDÖB ein elektronisches Meldeformular[49] geschaffen, mit welchem der in Art. 24 Abs. 2 DSG sowie Art. 15 Abs. 1 Bst. a–g DSV aufgeführte Inhalt gemeldet werden muss. Hierbei müssen insbesondere gemäss Art. 15 Abs. 1 Bst. a DSV die Art der Verletzung und gemäss Art. 15 Abs. 1 Bst. f DSV die Massnahmen, welche getroffen wurden oder vorgesehen sind, um den Mangel zu beheben und die Folgen zu mindern, einschliesslich der

---

45 BRUPBACHER/GÖRTZ STAEHELIN, a.a.O., S. 518 f.; BENHAMOU/WANG, a.a.O., S. 83; SARASIN/PANGRAZZI/MEYER, a.a.O., S. 1082 ff.

46 Vgl. hierzu ebenfalls: BRUPBACHER/GÖRTZ STAEHELIN, a.a.O., S. 519 f.; BENHAMOU/WANG, a.a.O., S. 83 f. sowie SARASIN/PANGRAZZI/MEYER, a.a.O., S. 1080 ff.

47 So könnte beispielsweise eine ausländische Behörde eine Lösegeldzahlung durch eine Person, die der ausländischen Gerichtsbarkeit unterliegt, als Sanktionsverstoss betrachten und zivilrechtliche Strafen aufgrund verschuldensunabhängiger Haftung verhängen. Unternehmen könnten so behördliche Kontrollen oder Gerichtsverfahren riskieren, was ihre zukünftigen Geschäfte in Ländern mit solchen Vorschriften beeinträchtigen könnte.

48 Vgl. vorstehend Ziff. 2.2.5, S. 12.

49 Vgl. hierzu die Webseite: https://databreach.edoeb.admin.ch/report; zuletzt besucht am 20. Oktober 2024.

allfälligen Risiken, gemeldet werden. Gemäss Art. 24 Abs. 4 DSG informiert sodann der Verantwortliche die betroffenen Personen, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

- *Meldepflicht von Cyberangriffen für von der FINMA beaufsichtigte Unternehmen*: Unternehmen, die unter die Aufsicht der FINMA fallen, sind gesetzlich dazu verpflichtet, Cyberangriffe der FINMA zu melden. Diese Regelung zielt darauf ab, die Integrität und Stabilität des Schweizer Finanzmarkts zu gewährleisten. Die Meldepflicht schliesst verschiedene Arten von Cyberangriffen ein, einschliesslich solcher, die durch Ransomware verursacht werden. Bei der Meldung eines Cyberangriffs müssen betroffene Unternehmen detaillierte Informationen bereitstellen, um der FINMA eine umfassende Bewertung der Situation zu ermöglichen. Dazu gehören die Art des Angriffs, der Zeitpunkt des Vorfalls, die betroffenen Systeme und Daten sowie die voraussichtlichen Auswirkungen auf die Geschäftstätigkeit. Ebenso wichtig ist die Beschreibung der ergriffenen Massnahmen zur Eindämmung und zur Behebung des Angriffs. Diese Informationen helfen der FINMA, das Risiko für das Finanzsystem als Ganzes zu beurteilen und gegebenenfalls weitere Schritte zur Unterstützung oder Regulierung vorzuschlagen. Zusätzlich müssen die Unternehmen erläutern, welche vorbeugenden Massnahmen sie implementiert haben, um ähnliche Vorfälle in Zukunft zu verhindern. Diese Transparenz ist entscheidend, um das Vertrauen in die Finanzmärkte zu stärken und die Resilienz gegenüber Cyberbedrohungen zu fördern. Die FINMA überwacht die Einhaltung dieser Vorschriften streng und kann bei Nichteinhaltung Sanktionen verhängen, was die Bedeutung der Meldepflicht unterstreicht.[50]
- *Meldepflicht von Cyberangriffen auf kritische Infrastrukturen*: Die voraussichtlich im Jahr 2025 in Kraft tretenden Bestimmungen von Art. 74*a* ff. ISG[51] sehen im Fall eines Cyberangriffs eine Meldepflicht für Betreiberinnen von kritischen Infrastrukturen vor. Art. 74*e* Abs. 2 ISG nennt den Inhalt der Meldung, d. h. die wesentlichen Informationen, die zur Erfüllung der Meldepflicht notwendig sind. Der konkrete Umfang und Inhalt der zu meldenden Informationen werden in der künftigen Cybersicherheitsverordnung präzisiert und vom BACS in einem Formular in die Informationsaustauschplattform des BACS (Cyber Security Hub) übernommen. In diesem Formular wird zudem detailliert umschreiben, was unter den jeweils zu meldenden Informationen zu verstehen ist. In Art. 19 Abs. 1 Bst. c, d und e des Entwurfs der Cybersicherheitsverordnung wird verlangt, dass die Art, die Angriffsmethode sowie die Angaben zum Verursacher des Cyberangriffs gemeldet werden müssen. Als Beispiel wird in den Erläuterungen der unautorisierte Zugriff bzw. der Einsatz von Schadsoftware aufgeführt. Des Weiteren sieht Art. 19 Abs. 2 des Entwurfs der Cybersicherheitsverordnung[52] vor, dass Angaben darüber gemacht werden müssen, ob im Zusammenhang mit dem Cyberangriff eine Erpressung erfolgt ist. Die Offenlegung von Erpressungsversuchen oder Drohungen im Zusammenhang mit einem Cyberangriff kann dazu beitragen, andere potenzielle Opfer zu warnen und Massnahmen zur Prävention ähnlicher Vorfälle zu ergreifen. Die Angabe, ob eine Lösegeldzahlung geleistet wurde oder ob beabsichtigt ist, eine zu leisten, wird nicht gefordert.[53]

Selbst wenn den vorgenannten Behörden ein Ransomware-Angriff gemeldet wird und diese seitens von Unternehmen und Privatpersonen um Unterstützung bei den Verhandlungen mit den Angreifern

---

50 Vgl. FINMA-Aufsichtsmitteilung 05/2020 vom 7. Mai 2020 – Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG (vgl. Webseite: https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf; zuletzt besucht am 20. Oktober 2024), welche sich auf Art. 29 Abs. 2 des Bundesgesetzes über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz, FINMAG; SR **956.1**) stützt und durch die FINMA im FINMA-Rundschreiben 2023/1 – Operationelle Risiken und Resilienz – Banken (vgl. Webseite: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf?sc_lang=de&hash=3DA82629BEBD5388845AB8FD93121801; zuletzt besucht am 20. Oktober 2024) und in der FINMA-Aufsichtsmitteilung 3/2024 – Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen präzisiert wurde (vgl. Webseite: https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=de&hash=666EEE255C04FB42F01BFD0BC6C80191; zuletzt besucht am 20. Oktober 2024).

51 Das Datum des Inkrafttretens wurde seitens des Bundesrates im Zeitpunkt des Verfassens dieses Berichts noch nicht bestimmt.

52 Vgl. hierzu die Webseite: https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2024/35/cons_1/doc_1/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2024-35-cons_1-doc_1-de-pdf-a.pdf; zuletzt besucht am 20. Oktober 2024.

53 Erläuterungsbericht zum Entwurf der Cybersicherheitsverordnung, S. 29 ff. (Webseite: https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/2024/35/cons_1/doc_2/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-2024-35-cons_1-doc_2-de-pdf-a.pdf; zuletzt besucht am 20. Oktober 2024).

gebeten werden, gilt es, das Legalitätsprinzip zu beachten. Das heisst, es erwachsen dem EDÖB, der FINMA oder dem BACS daraus keine diesbezüglichen Unterstützungspflichten.

3.2 Rechtsvergleich

Die rechtlichen Rahmenbedingungen für den Umgang mit Lösegeldzahlungen bei Ransomware-Angriffen und die Verpflichtung des Einbezugs von Behörden in Verhandlungen mit Ransomware-Angreifern variieren zwischen den Ländern kaum. Es gibt zahlreiche Gemeinsamkeiten bei den jeweiligen Regelungen über die Meldepflicht bei Lösegeldzahlungen und die Verpflichtung, Behörden in Verhandlungen mit den Angreifern einzubeziehen. Im Folgenden werden für einen internationalen Vergleich die Meldepflichten für Lösegeldzahlungen oder Pflichten für den Einbezug von Behörden der USA, welche eine Vorreiterrolle im Kampf gegen Ransomware-Angriffe einnehmen, und unseren beiden Nachbarstaaten Deutschland und Frankreich kurz erläutert. Diese Analyse der rechtlichen Rahmenbedingungen in den USA, Deutschland und Frankreich bietet einen repräsentativen Überblick über die Herangehensweisen in führenden Industrienationen und ermöglicht es, bewährte Praktiken zu identifizieren und potenzielle Verbesserungen für die eigene Gesetzgebung abzuleiten.

3.2.1 Keine Meldepflicht bei Lösegeldzahlungen bei Ransomware-Angriffen

Ähnlich wie in der Schweiz sind in vielen Ländern Meldepflichten für Cyberangriffe bereits umgesetzt oder zumindest geplant. Meldepflichten zu Lösegeldzahlungen gibt es hingegen nicht. Die Regelungen zur Meldepflicht sehen in den nachfolgend aufgeführten Ländern wie folgt aus:

- *USA*: Wie in der Schweiz ist die Zahlung von Lösegeld nach einem Ransomware-Angriff nicht verboten und ist auch nicht meldepflichtig, aber in bestimmten Situationen strafbar, wenn sie an Personen erfolgt, die nach US-Recht Blockaden oder Sanktionen unterliegen oder wenn gegen das Geldwäschereiverbot verstossen wird. Die Nichteinhaltung dieser Regeln kann zivilrechtliche Sanktionen nach sich ziehen, die auf einer strengen Haftung beruhen, unabhängig vom Bewusstsein, sich auf ein Geschäft mit einer Person einzulassen, die Gegenstand von US-Sanktionen ist. Aus diesem Grund ermutigt das US Office of Foreign Assets Control (OFAC) Opfer und Personen, die mit der Bewältigung von Ransomware-Angriffen befasst sind, umgehend Kontakt mit OFAC aufzunehmen, wenn sie vermuten, dass eine Forderung nach einer Ransomware-Zahlung möglicherweise einen Bezug zu Sanktionen haben könnte. Opfer sollten sich auch an das Büro für US Cybersecurity and Infrastructure Security Agency (CISA) wenden, wenn ein Angriff ein US-Finanzinstitut betrifft oder die Fähigkeit eines Unternehmens, kritische Finanzdienstleistungen zu erbringen, erheblich beeinträchtigen könnte.[54]
- *Deutschland*: Gemäss dem Bundeskriminalamt (BKA) besteht in Deutschland kein Verbot von Lösegeldzahlungen bei Ransomware-Angriffen; seitens der Behörden wird aber dazu geraten, nicht auf Lösegeldforderungen einzugehen.[55] Die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) lässt es seit dem 15. September 2017 ausdrücklich zu, dass Versicherungen die Zahlung von Ransomware-Lösegeld unter bestimmten Bedingungen decken dürfen.[56] Im Übrigen gibt es keine spezifische gesetzliche Verpflichtung zur Meldung

[54] Vgl. BENHAMOU/WANG, a.a.O., S. 86; U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 1. Oktober 2020 (Webseite: https://ofac.treasury.gov/media/48301/download?inline; zuletzt besucht am 20. Oktober 2024) und OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, September 21, 2021 (Webseite: https://ofac.treasury.gov/media/912981/download?inline; zuletzt besucht am 20. Oktober 2024) sowie SARASIN/PANGRAZZI/MEYER, a.a.O., S. 1089.

[55] Vgl. Webseite: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/DigitaleErpressung/digitaleErpressung_node.html; zuletzt besucht am 20. Oktober 2024.

[56] Vgl. Webseite: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_170915_loesegeldversicherung.html; zuletzt besucht am 20. Oktober 2024, unter Verweis auf das vorbestehende Rundschreiben 3/1998 (VA) – Hinweise des BAV zum Betrieb

von Lösegeldzahlungen nach einem Ransomware-Angriff; Unternehmen werden aber dazu angehalten, IT-Sicherheitsvorfälle zu melden.[57]

- *Frankreich*: In Frankreich ist die Situation ähnlich wie in der Schweiz. Die Zahlung eines Lösegelds nach einem Ransomware-Angriff ist nicht per se verboten. Die Behörden raten aber davon ab, da dies die kriminellen Aktivitäten weiter fördern kann. In bestimmten Situationen kann die Zahlung eines Ransomware-Lösegelds den Straftatbestand der Terrorismusfinanzierung erfüllen, wenn das Opfer Kenntnis davon hat, dass die Gelder für einen terroristischen Akt verwendet werden sollen. Das Haut Comité Juridique de la Place Financière de Paris (HCJP) hielt namentlich in diesem Zusammenhang in einem Bericht vom 28. Januar 2022 fest, dass Unternehmen des Finanzsektors bei ihrer Tätigkeit besonderen Regeln unterliegen und Transaktionen mit Geldern melden bzw. unterlassen müssen, bei denen sie vermuten oder einen begründeten Verdacht haben, dass diese aus einer Straftat stammen, die mit einer Freiheitsstrafe von mehr als einem Jahr bedroht ist, oder mit der Finanzierung von Terrorismus in Verbindung stehen.[58]

3.2.2 Verpflichtung des Einbezugs von Behörden in Verhandlungen mit Ransomware-Angreifern

Ein Rechtsvergleich bezüglich einer Verpflichtung des Einbezugs von staatlichen Behörden in die Verhandlungen mit Ransomware-Angreifern zeigt was folgt:

- *USA*: Es gibt in den USA keine Verpflichtung des Einbezugs von Behörden in Verhandlungen mit Ransomware-Angreifern. Das OFAC, das Federal Bureau of Investigation (FBI), die CISA, der US Secret Service und andere (Strafverfolgungs-)Behörden empfehlen aber, bei Ransomware-Fällen mit ihnen zusammenzuarbeiten, da sich dies strafmildernd auswirken kann, falls die Lösegeldzahlung als ein Akt der Geldwäscherei eingestuft wird.[59] Die Opfer eines Ransomware-Angriffs werden seitens der Behörden ermutigt, den Vorfall zu melden. Ein Opfer muss den Vorfall nur einmal melden, die vorgenannten Behörden werden in der Folge jeweils via Schnittstellen benachrichtigt.[60]
- *Deutschland*: Die deutschen Strafverfolgungsbehörden, insbesondere die Landeskriminalämter (LKA) und das BKA, raten Opfern zur Zusammenarbeit mit den Behörden bei Ransomware-Angriffen. Eine gesetzliche Verpflichtung besteht nicht, aber es wird darauf hingewiesen, dass die Zusammenarbeit die Erfolgschancen bei der Strafverfolgung erhöhen kann.[61]
- *Frankreich*: In Frankreich gibt es keine Verpflichtung, Behörden in Verhandlungen mit Ransomware-Angreifern einzubeziehen. Die französischen Strafverfolgungsbehörden, einschliesslich die Police Nationale und die Gendarmerie Nationale, empfehlen dringend, bei Ransomware-Angriffen mit ihnen zusammenzuarbeiten. Diese Zusammenarbeit ermöglicht eine effektivere Strafverfolgung und Prävention.[62]

---

von Lösegeldversicherungen (Webseite: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_9803_va_loesegeldversicherung.html;jsessionid=0AA1AC030FE93BF2BB27BE3F90E9BCA8.internet972?nn=19659504; zuletzt besucht am 20. Oktober 2024).

57 Vgl. hierzu die allgemeine Webseite des Bundesamtes für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?nn=133680&cms_pos=4; zuletzt besucht am: 20. Oktober 2024.

58 Vgl. Haut Comité Juridique de la Place Financière de Paris (HCJP), Rapport sur l'assurabilité des risques cyber, 28 janvier 2022 (Webseite: https://www.banque-france.fr/system/files/2023-10/rapport_45_f.pdf; zuletzt besucht am 20. Oktober 2024).

59 Vgl. OFAC, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, 1. Oktober 2020 (Webseite: https://ofac.treasury.gov/media/48301/download?inline; zuletzt besucht am 20. Oktober 2024) und OFAC, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Webseite: https://ofac.treasury.gov/media/912981/download?inline; zuletzt besucht am 20. Oktober 2024).

60 So bietet beispielsweise das sog. «Internet Crime Complaint Center (IC3)» der Öffentlichkeit einen zuverlässigen und bequemen Meldemechanismus, um Informationen über mutmassliche kriminelle Aktivitäten im Internet zu übermitteln. Dem FBI kann auch direkt eine Meldung über folgende Webseite erstattet werden: https://ransomware.ic3.gov/default; zuletzt besucht am 3. Juli 2024. Es ist auch möglich, einen Ransomware-Angriff direkt bei der US Cybersecurity & Infrastructure Security Agency (CISA) mittels folgender Webseite zu melden: https://www.cisa.gov/forms/report; zuletzt besucht am 20. Oktober 2024.

61 Vgl. Webseite: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/DigitaleErpressung/digitaleErpressung_node.html; zuletzt besucht am 20. Oktober 2024.

62 Vgl. hierzu die Webseite: https://www.internet-signalement.gouv.fr/PharosS1/; zuletzt besucht am 20. Oktober 2024 und die Webseite: https://www.service-public.fr/particuliers/vosdroits/N31138; zuletzt besucht am 20. Oktober 2024.

3.2.3 Ergebnis des Rechtsvergleichs

Der vorstehende Rechtsvergleich zeigt, dass von den ausgewählten Ländern weder Verbote von Ransomware-Lösegeldzahlung noch spezifische Meldepflichten gegenüber von Behörden vorgesehen werden und die Behörden nicht verpflichtet sind, sich an Verhandlungen mit Ransomware-Angriffen zu beteiligen, dass aber eine Meldung und Zusammenarbeit mit den Behörden empfohlen wird. Zwar wird in vielen Staaten über eine stärkere Regulierung von Ransomware-Lösegeldzahlungen diskutiert,[63] effektiv eingeführt haben mit der Schweiz vergleichbare Länder solche Massnahmen jedoch nicht.

3.3 Gesetzgeberische Möglichkeiten in der Schweiz

Es gibt in der Schweiz derzeit kein Verbot von Ransomware-Lösegeldzahlungen, keine spezifische gesetzliche Meldepflicht bei Lösegeldzahlungen in Folge von Ransomware-Angriffen oder anderen Cyber-Erpressungsfällen. Ebenso besteht keine gesetzliche Verpflichtung, Behörden in die Verhandlungen mit Kriminellen einzubeziehen und dementsprechend auch kein diesbezüglicher Anspruch auf behördliche Unterstützung. Im Folgenden wird erörtert, welche Vor- und Nachteile entstehen, wenn einerseits der Status quo beibehalten würde, oder andererseits, wenn neue rechtliche Grundlagen für die Einführung der Meldepflicht und der Pflicht zum Einbezug von Behörden bei Lösegeldverhandlungen geschaffen würden. Abschliessend wird in diesem Sinne auch die Möglichkeit der Schaffung eines staatlichen Verbots von Lösegeldzahlungen bei Ransomware-Angriffen erläutert.

3.3.1 Beibehaltung der aktuellen Regelungen (keine spezifischen Massnahmen)

Die Beibehaltung der aktuellen Regelungen basiert auf einer sorgfältigen Abwägung von Nutzen und Aufwand. Ein zentraler Aspekt ist die Effektivität zusätzlicher Meldepflichten im Vergleich zum damit verbundenen administrativen Aufwand für Unternehmen und Behörden. Ein erfolgreicher Cyberangriff stellt für die Betroffenen eine äusserst belastende Situation dar, in der schnelles und flexibles Handeln oft entscheidend ist. Zusätzliche Auflagen könnten die Bewältigung dieser kritischen Phase erschweren, ohne zwangsläufig bessere Ergebnisse zu erzielen. Behördenseitig wären erhebliche Ressourcen erforderlich, um Meldungen effektiv zu verarbeiten und darauf zeitnah zu reagieren. Es ist fraglich, ob dieser Aufwand in einem angemessenen Verhältnis zum potenziellen Nutzen steht, insbesondere angesichts der bereits bestehenden Meldepflichten bei Cybervorfällen. Der aktuelle rechtliche Rahmen ermöglicht es zudem, marktbasierte Lösungen zu entwickeln, beispielsweise in Zusammenarbeit mit Versicherungen, ohne diese durch zusätzliche Regulierungen einzuschränken. Sollte sich in Zukunft zeigen, dass eine Meldepflicht für Lösegeldzahlungen notwendig wird, müsste dafür zunächst eine entsprechende rechtliche Grundlage geschaffen werden. Die Entscheidung gegen eine solche Pflicht zum jetzigen Zeitpunkt beruht auf der Einschätzung, dass die bestehenden Massnahmen derzeit am effektivsten sind, um die Herausforderungen von Ransomware-Angriffen zu bewältigen.

Das Grundproblem des falschen Anreizes für die Bezahlung von Lösegeld bleibt beim Status Quo jedoch bestehen. Das Bezahlen von Lösegeld bleibt in vielen Fällen eine billige und schnelle Lösung für die Betroffenen, verschärft aber gleichzeitig das Problem für alle anderen, weil die Cyberkriminellen so bestärkt werden, weitere Ransomware-Angriffe durchzuführen. Diese Dynamik belastet die gesamte Gesellschaft, da die erhöhte Anzahl an Angriffen die allgemeine Sicherheit und Widerstandsfähigkeit gegen Cyberkriminalität schwächt. Zudem bleiben die Lösegeldzahlungen unbekannt. Diese fehlende Transparenz über das Ausmass von Ransomware-Angriffen erschwert es Strafverfolgungs- und Cybersicherheitsbehörden, umfassende Strategien zur Bekämpfung dieser Bedrohungen zu entwickeln. Auch bei einer Beibehaltung des Status quo müssen deshalb Massnahmen umgesetzt

[63] Vgl. die Diskussionen in Grossbritannien (U.K. Government To Consider Licensing Ransomware Payments | Lawfare (lawfaremedia.org)), Australien (Australia: New Law in Australia will require mandatory reporting of ransomware payments (therecord.media) oder in den USA (Proposed Legislation Would Add Ransomware Reporting and Compliance Obligations for Covered U.S. Financial Institutions, Brock Dahl, David Sewell, Nathaniel Balk, David Benger (freshfields.us)).

werden, welche bessere Einschätzungen zu den Auswirkungen von Ransomware-Angriffen ermöglichen.

3.3.2 Einführung von Meldepflichten für Ransomware-Angriffe sowie für Lösegeldzahlungen und staatliche Unterstützung bei Verhandlungen

Angesichts der Häufigkeit von Ransomware-Angriffen kann argumentiert werden, dass gesetzgeberische Massnahmen nötig sind, um zu verhindern, dass Lösegelder bezahlt werden. Die Einführung von Meldepflichten und die Pflicht zum Einbezug von Behörden bei Verhandlungen sind solche Massnahmen. Die Vorteile einer solchen Lösung liegen in erster Linie beim erhofften abschreckenden Effekt. Würden Unternehmen verpflichtet, Lösegeldzahlungen zu melden, müssten sie Transparenz schaffen. Es ist wäre nicht mehr möglich, den Sicherheitsvorfall durch eine Zahlung an Kriminelle ohne Offenlegung zu bewältigen. Damit würde die Lösegeldzahlung für Opfer an Attraktivität verlieren. Zudem wirkt die verpflichtende Einschaltung der Behörden abschreckend auf die Angreifer, da diese in der Regel vermeiden möchten, direkt mit der Polizei zu verhandeln. Wenn Kriminelle wissen, dass bei jedem Angriff automatisch die Strafverfolgungsbehörden involviert werden, so könnte dies dazu führen, dass Schweizer Unternehmen als weniger attraktive Zielobjekte wahrgenommen würden, da das Risiko für die Angreifer steigt, identifiziert zu werden.

Neben diesen abschreckenden Effekten schafft eine Meldepflicht mehr Transparenz über Cyberangriffe, indem Behörden detaillierte Einblicke in das Ausmass, die finanziellen Dimensionen und die angewandten Taktiken der Bedrohungen erhalten. Dadurch könnten präventive Massnahmen gezielter entwickelt und Schwachstellen in der digitalen Infrastruktur identifiziert werden, um zukünftige Angriffe zu verhindern.

Die Einführung zusätzlicher Verwaltungsaufwände könnte jedoch besonders kleinere Unternehmen überfordern und die Effizienz der Vorfallbewältigung beeinträchtigen. Insgesamt führen die Massnahmen auch zu einer Belastung der Opfer. Neben den direkten Angriffsschäden müssten diese auch noch gesetzliche Anforderungen erfüllen, was zusätzliche Ressourcen erfordert. Zudem würde die Rolle des Staates durch eine solche Regelung schwieriger. Einerseits würden Behörden empfehlen, kein Lösegeld zu zahlen, um Kriminelle nicht zusätzlich zu motivieren. Andererseits würden die gleichen Behörden als Kompetenzzentrum für Verhandlungen mit Kriminellen wirken, was gewissermassen einen Interessenskonflikt darstellt. Diese duale Rolle könnte nicht nur Verwirrung und Unsicherheit bei den betroffenen Unternehmen hervorrufen, sondern auch die Effektivität staatlicher Empfehlungen untergraben.

Eine mögliche Alternative zur Einführung von Meldepflichten für Lösegeldzahlungen wäre eine vereinfachte Meldepflicht für diejenigen Entitäten, die Ransomware-Lösegelder im Auftrag Dritter bezahlen oder das Lösegeld über eine Versicherung decken lassen. Diese Variante hätte folgende Vorteile: Erstens würde diese vereinfachte Meldepflicht vermeiden, dass Opfer von Ransomware-Angriffen kriminalisiert oder zusätzlich belastet werden, da die Verantwortung für die Meldung auf die zahlenden Dienstleister oder Versicherungsanbieter übertragen würde. Dadurch würde sichergestellt, dass Unternehmen und Einzelpersonen, die bereits unter dem Angriff leiden, nicht noch weiter bürokratisch belastet würden. Zweitens würde eine solche Meldepflicht einen besseren Überblick über gezahlte Lösegelder ermöglichen. Behörden könnten detaillierte Statistiken über die Häufigkeit und Höhe der Zahlungen führen, was wertvolle Daten für die Bekämpfung von Cyberkriminalität erheben würde. Diese Transparenz könnte dazu beitragen, präventive Massnahmen datenbasiert zu verbessern und gezielte Strategien zur Reduzierung von Ransomware-Angriffen zu entwickeln.

Allerdings gibt es auch bei dieser Variante der vereinfachten Meldepflicht Nachteile: Die Einführung einer solchen Meldepflicht würde zusätzlichen bürokratischen Aufwand sowohl für die

Versicherungsunternehmen als auch für die zahlenden Dienstleister wie Finanzintermediäre bedeuten. Diese müssten neue Prozesse und Systeme einführen, um sicherzustellen, dass alle Lösegeldzahlungen korrekt gemeldet würden. Ein weiterer Nachteil wäre die Möglichkeit der Umgehung dieser Regelung durch die Nutzung ausländischer Versicherungen und Dienstleister, die nicht der Meldepflicht in der Schweiz unterliegen. Dies könnte dazu führen, dass ein Teil der Lösegeldzahlungen weiterhin im Verborgenen bleibt und die erhoffte Transparenz nicht vollständig erreicht werden würde. Zudem würde eine solche Regelung Wettbewerbsnachteile für Schweizer Versicherer schaffen, da andere Länder keine solche Meldepflicht kennen.

3.3.3 Verbot von Lösegeldzahlungen

Ein Verbot von Lösegeldzahlungen bei Ransomware-Angriffen stellt eine sehr weitgehende Massnahme dar, die darauf abzielt, die Finanzierung krimineller Aktivitäten zu unterbinden und die Anreize für Kriminelle zu verringern. Um ein Verbot von Lösegeldzahlungen in der Schweiz zu implementieren, wäre es notwendig, eine gesetzliche Grundlage zu schaffen. Hierzu wird entweder im Strafgesetzbuch (StGB) eine entsprechende Strafnorm mit Sanktionen wie einer Busse vorgesehen oder man müsste die Einführung eines speziellen Gesetzes zur Bekämpfung von Cyberkriminalität diskutieren, in welchem der rechtliche Rahmen für ein Verbot vorgegeben wird. Es wird in diesem Zusammenhang notwendig sein, den Begriff der Lösegeldzahlungen einschliesslich der Unterscheidung zwischen direkten und indirekten Zahlungen präzise zu definieren. Zudem müsste auch festgelegt werden, ob das Verbot nur für Ransomware-Angriffe oder auch generell für Entführungen und andere Formen der Erpressung gilt. Des Weiteren müssen die behördlichen Zuständigkeiten und Befugnisse zur Durchsetzung des Verbots diskutiert werden. Es wären insbesondere Systeme und Technologien zur Überwachung verdächtiger Transaktionen und zur Identifizierung von Lösegeldzahlungen anzudenken sowie zu entwickeln. Zu diesem Zweck könnten beispielsweise Banken und Finanzinstitute dazu verpflichtet werden, verdächtige Aktivitäten zu melden. Einhergehend mit dem Verbot müsste man auch die Kapazitäten der Strafverfolgungsbehörden zur Ermittlung und Verfolgung von Verstössen gegen das Verbot stärken, Schulungen durchführen und allenfalls gar spezialisierte Einheiten schaffen, um diese Aufgabe übernehmen zu können.

Die Einführung eines Verbots von Ransomware-Lösegeldzahlungen bringt potenzielle Vorteile mit sich, die darauf abzielen, die Effektivität und Rentabilität solcher kriminellen Aktivitäten zu verringern. Ein solches Verbot würde eine Abschreckungswirkung haben, da es den finanziellen Anreiz für Ransomware-Angriffe mindert. Diese klare gesetzliche Position sendet ein Signal aus, das die Null-Toleranz gegenüber Erpressung und Cyberkriminalität unterstreicht. Langfristig könnte dies dazu beitragen, die Häufigkeit und Schwere von Ransomware-Angriffen zu reduzieren und die Cyberkriminalität einzudämmen.

Jedoch gibt es erhebliche Nachteile zu bedenken: Die praktische Durchsetzbarkeit eines solchen Verbots bringt einen beträchtlichen Verwaltungsaufwand mit sich, sowohl für Unternehmen bei der Implementierung von Compliance-Massnahmen als auch für staatliche Behörden bei der Überwachung und Durchsetzung. Dies könnte die Effizienz und Flexibilität sowohl der Wirtschaft als auch der öffentlichen Verwaltung beeinträchtigen. Zudem besteht die Gefahr der Kriminalisierung von Ransomware-Opfern, die unter Druck gesetzt werden könnten, das Verbot zu umgehen, um ihre Daten zu retten. Ein weiterer Nachteil ist die potenzielle Verlagerung der Bedrohung auf andere, weniger regulierte kriminelle Aktivitäten, was die Gesamtsicherheit weiter gefährden könnte. Nicht zuletzt erhöht ein solches Verbot das Risiko für Opfer, die ohne die Option der Lösegeldzahlung gezwungen sein könnten, schwerwiegende betriebliche und finanzielle Verluste zu erleiden oder sogar ihre Existenz zu gefährden.

3.4 Ergebnis der Prüfung

In der Schweiz gibt es zwar keine generelle Meldepflicht für Lösegeldzahlungen, aber es bestehen datenschutz- und finanzmarktrechtliche Meldepflichten bei Cyberangriffen, die künftig mit der Meldepflicht gemäss ISG für Betreiberinnen kritischer Infrastrukturen ergänzt werden. Diese Meldepflichten dienen der Einschätzung der Bedrohungslage sowie der Stärkung der Frühwarnung und haben gegenüber Ransomware-Angreifern aber keine abschreckende Wirkung gezeigt. Eine zusätzliche Meldepflicht oder ein Verbot von Lösegeldzahlungen einzuführen, um das Verhalten von betroffenen Unternehmen zu ändern, wurde vorstehend geprüft. Dabei wurden verschiedene Aspekte berücksichtigt, wie die fragliche Effektivität solcher Massnahmen zur nachhaltigen Abschreckung von Angreifern, mögliche unbeabsichtigte Folgen wie das Verschweigen von Vorfällen, die Notwendigkeit von Flexibilität in der Krisenbewältigung und der Fokus auf präventive Massnahmen statt zusätzlicher Pflichten nach einem Angriff. Eine Verpflichtung zur Meldung von Lösegeldzahlungen durch Dritte wie Versicherungen, Finanzintermediäre oder Sicherheitsdienstleister wurde ebenfalls erwogen. Stattdessen wird jedoch ein verstärkter freiwilliger Informationsaustausch zwischen Behörden und diesen Akteuren angestrebt, um mehr Transparenz zu erreichen, ohne zusätzliche regulatorische Hürden zu schaffen.[64]

Nach sorgfältiger Abwägung wird die Beibehaltung und Optimierung der aktuellen Regelungen als zielführendster Ansatz erachtet. Dies ermöglicht eine Balance zwischen effektiver Bedrohungsabwehr, Flexibilität in der Reaktion auf Angriffe und der Förderung proaktiver Sicherheitsmassnahmen. Gleichzeitig bleibt die Schweiz im Einklang mit den Ansätzen anderer führender Nationen wie den USA, Deutschland und Frankreich.

Diese Strategie wird kontinuierlich evaluiert und bei Bedarf angepasst, um auf die sich ständig weiterentwickelnde Bedrohungslage reagieren zu können. Ziel ist es, einen ganzheitlichen Ansatz zu verfolgen, der Prävention, schnelle Reaktionsfähigkeit und internationale Zusammenarbeit in den Vordergrund stellt, ohne die Handlungsfähigkeit der betroffenen Unternehmen in Krisensituationen unnötig einzuschränken.

4 Stärkung des Informationsaustauschs

Der Informationsaustausch zu Bedrohungen, Schwachstellen und Angriffsmustern gilt in der Cybersicherheit als entscheidendes präventives Mittel, um die Verteidigung gegen Angriffe zu stärken. Weil Angreifer im Cyberraum mit der gleichen Methode eine sehr hohe Zahl von Opfern angreifen können, lässt sich der Schutz der Betroffenen am effizientesten durch eine Stärkung des Informationsaustausches verbessern. Der Austausch von Informationen hilft dabei, Muster und Trends bei Ransomware-Angriffen schneller zu erkennen. Wenn Unternehmen und Institutionen Informationen über erfolgte Angriffe, verwendete Methoden und identifizierte Schwachstellen teilen, können andere potenzielle Opfer proaktiv Massnahmen ergreifen, um sich gegen ähnliche Angriffe zu schützen. Früherkennung und Prävention sind entscheidend, um die Auswirkungen von Ransomware-Angriffen zu minimieren.

Neben der Stärkung der Frühwarnung fördert der Informationsaustausch auch die Transparenz. Nehmen genügend Organisationen am Informationsaustausch teil, ist es auch ohne die Einführung von Meldepflichten möglich, detailliertere Erkenntnisse über die Bedrohungslage zu gewinnen.

Nachfolgend wird dargelegt, welche Formen des Informationsaustausches bereits heute gepflegt werden und wo diese spezifisch für Ransomware-Angriffe noch ausgebaut werden könnte.

[64] Siehe hierzu nachfolgend Ziff. 4, S. 21.

4.1 Informationsaustausch zur Verbesserung der Prävention und Reaktion

In der Schweiz koordiniert das BACS den Informationsaustausch von Behörden und Betroffenen bei Cyberbedrohungen. Es stellt Unternehmen und Behörden eine Meldestelle für freiwillige Meldungen zu Cyberangriffen und -bedrohungen sowie eine Plattform zur Verfügung, über welche Informationen zu Bedrohungen, Schwachstellen und Angriffsmuster ausgetauscht werden können. Dies trägt dazu bei, Bedrohungen schneller zu erkennen und angemessen darauf zu reagieren und ermöglicht es, bestehende Sicherheitsmassnahmen kontinuierlich zu verbessern und neue Technologien und Verfahren zu entwickeln, die den Schutz vor Ransomware-Angriffen erhöhen. Dies trägt zur gesamthaften Resilienz der digitalen Infrastruktur der Schweiz bei und hilft, das Vertrauen in digitale Dienste und Produkte zu stärken.

Die Zusammenarbeit des BACS mit internationalen Stellen ist ein weiterer wichtiger Aspekt. Das Bundesamt arbeitet eng mit internationalen Partnern und Netzwerken zusammen, um Informationen über globale Cyberbedrohungen und Angriffe auszutauschen. Das BACS beteiligt sich seit 2021 gemeinsam mit weiteren Stellen des Bundes an der «Counter Ransomware Initiative».[65] Diese internationale Initiative, an der sich die EU und mehr als 30 weitere Staaten beteiligen, koordiniert die Bemühungen bei der Bekämpfung der Cyberkriminalität auf politischer und strategischer Ebene. Dies ist besonders wichtig, da Cyberkriminalität meist grenzüberschreitend stattfindet und einer effektiven Bekämpfung durch internationale Zusammenarbeit bedarf. Durch den Austausch von Informationen und Best Practices mit internationalen Partnern kann die Schweiz von globalen Erkenntnissen profitieren und ihre eigenen Strategien entsprechend anpassen. Zudem spielen völkerrechtliche Instrumente wie die Budapest-Konvention[66] und die seitens der UNO ausgehandelte UN Cybercrime Convention[67] eine wichtige Rolle bei der Förderung des grenzüberschreitenden Informationsaustauschs. Diese internationalen Formate ermöglichen einen breiteren Überblick über globale Trends und Taktiken von Cyberkriminellen und stärken die koordinierte Reaktion auf Ransomware-Angriffe.

Auf nationaler Ebene wird die bereits beschlossene Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen und der weitere Ausbau der Plattform für den Informationsaustausch beim BACS die Fähigkeit zur Bedrohungserkennung und -abwehr zusätzlich verbessern. Diese Kombination aus nationalen Initiativen und internationaler Zusammenarbeit schafft ein umfassendes Netzwerk für den Informationsaustausch, das entscheidend zur Bekämpfung von Ransomware-Angriffen beiträgt.

Des Weiteren sind regelmässige Treffen und Workshops zwischen dem Bund, den kantonalen Strafverfolgungsbehörden, privaten Sicherheitsunternehmen und Versicherungen von zentraler Bedeutung. Solche Zusammenkünfte bieten eine Basis für den Austausch von Erfahrungen, die Diskussion aktueller Bedrohungen und die gemeinsame Erarbeitung von Best Practices. Durch regelmässige Workshops können die Beteiligten ihre Kenntnisse und Fähigkeiten kontinuierlich erweitern und anpassen. Diese Veranstaltungen fördern das Verständnis für die Herausforderungen, mit denen die verschiedenen Akteure konfrontiert sind, und helfen dabei, gemeinsame Lösungen zu entwickeln. Darüber hinaus stärken sie das Netzwerk und das Vertrauen zwischen den Beteiligten, was die Zusammenarbeit im Ernstfall erleichtert. Das BACS fördert diese Form der Zusammenarbeit durch

---

65 Vgl. Webseite: https://counter-ransomware.org/; zuletzt besucht am 20. Oktober 2024.

66 Die Budapest-Konvention, offiziell bekannt als «Übereinkommen über Computerkriminalität» (SR **0.311.43**) ist ein am 23. November 2001 vom Europarat verabschiedetes internationales Abkommen. Es ist das erste völkerrechtlich bindende Instrument, das sich speziell mit Cyberkriminalität befasst. Die Konvention zielt darauf ab, nationale Gesetze zu harmonisieren, Ermittlungstechniken zu verbessern und die internationale Zusammenarbeit bei der Bekämpfung von Computerdelikten zu fördern. Sie deckt Bereiche wie unerlaubtes Eindringen in Computersysteme, Computerbetrug und die Verbreitung von Kinderpornografie im Internet ab. Die Schweiz ist seit 1. Januar 2012 Vertragspartei der Budapest-Konvention und hat damit ihre Verpflichtung zur internationalen Kooperation im Kampf gegen Cyberkriminalität bekräftigt. Durch die Ratifizierung hat sich die Schweiz verpflichtet, ihre nationale Gesetzgebung an die Vorgaben der Konvention anzupassen und im Rahmen des Strafrechts an grenzüberschreitenden Ermittlungen und dem Informationsaustausch teilzunehmen.

67 Die UN Cybercrime Convention beabsichtigt, einen rechtlichen Rahmen zur Kriminalisierung von Cyberdelikten, einschliesslich von Ransomware-Angriffen, zu schaffen und die internationale Zusammenarbeit bei der Strafverfolgung zu fördern. Die Konvention zielt darauf ab, eine koordinierte Antwort auf die transnationale Bedrohung durch Ransomware zu ermöglichen. Das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) und das Bundesamt für Justiz (BJ) koordinieren die Schweizer Position zur Konvention. Die Wirksamkeit der Konvention hängt von ihrer breiten Ratifizierung und konsequenten Umsetzung durch die Mitgliedstaaten ab. Es ist üblich, dass dieser Prozess einige Zeit in Anspruch nimmt, oft mehrere Jahre. Die Schweiz wird die Konvention im Hinblick auf eine mögliche Unterzeichnung und spätere Ratifizierung gemäss ihrem innerstaatlichen Verfahren prüfen.

sektorspezifische Veranstaltungen und den Aufbau von sektoriellen Organisationen für den Informationsaustausch. So hat es beispielsweise dazu beigetragen, das Swiss Financial Sector Cyber Security Centre (FS-CSC)[68] zu etablieren. Der Informationsaustausch innerhalb eines Industriesektors ermöglicht es den Teilnehmenden, sich auf für ihren Sektor relevante Bedrohungen und Angriffsmuster zu fokussieren. Projekte für den Aufbau ähnlicher Organisationen in anderen Sektoren laufen.

4.2 Informationsaustausch zur Verbesserung der Strafverfolgung

Der am 19. Juni 2024 veröffentlichte Bericht des Bundesrats «Wie fit sind die Kantone in der Cyber-Strafverfolgung» in Erfüllung der Postulate 22.3145 von Andri Silberschmidt vom 16. März 2022 und 22.3017 der Sicherheitspolitischen Kommission des Nationalrats vom 15. Februar 2022, betont die Notwendigkeit einer stärkeren Koordination und Zusammenarbeit im Bereich der Cyber-Strafverfolgung auf nationaler und internationaler Ebene. In diesem Bericht wird aufgezeigt, dass die Anzahl der Straftaten sowie deren Schweregrad und das Schadensausmass stetig zunehmen und unterstreicht die Bedeutung spezialisierter Netzwerke und Arbeitsgruppen sowie die Notwendigkeit organisatorischer und personeller Anpassungen in den Kantonen, um die Cyberkriminalität effektiver zu bekämpfen. Trotz der Fortschritte bestehen weiterhin Herausforderungen, darunter der Mangel an Ressourcen und gesetzliche Hindernisse für den Informationsaustausch. Der Bericht fordert daher eine Intensivierung der Präventions- und Repressionsmassnahmen und eine stärkere Zusammenarbeit zwischen Bund, Kantonen und internationalen Partnern.[69]

Dieser Bericht bestätigt, dass die hier diskutierte Verstärkung des Informationsaustauschs die Zusammenarbeit und das Vertrauen zwischen dem Bund, den kantonalen Strafverfolgungsbehörden, privaten Sicherheitsunternehmen und Versicherungen fördern kann. Wenn alle Beteiligten regelmässig und systematisch Informationen teilen, wird Transparenz geschaffen, was dem gegenseitigen Vertrauen dient. Dies ist entscheidend, um gemeinsam effektive Lösungen zur Bekämpfung von Ransomware-Angriffen zu entwickeln und umzusetzen. Die Bevölkerung, Unternehmen und Institutionen fühlen sich sicherer, wenn sie wissen, dass sie auf die Unterstützung und das Wissen einer breiten Gemeinschaft zählen können. Ein koordinierter Ansatz zwischen Bund, den kantonalen Strafverfolgungsbehörden, privaten Sicherheitsfirmen und Versicherungen stärkt die Gesamtabwehr gegen Ransomware-Angriffe. Gemeinsam können effektivere und umfassendere Abwehrstrategien entwickelt werden, was auch eine bessere Ressourcenallokation zur Bekämpfung von Cyberkriminalität ermöglicht.

Der Informationsaustausch unterstützt die Strafverfolgung bei der Identifikation und Verfolgung von Cyberkriminellen. Durch die gemeinsame Nutzung von Daten über Angriffe, Techniken und Täterprofile können Strafverfolgungsbehörden Muster erkennen und gezielte Ermittlungen durchführen. Dies erhöht die Chancen, die Verantwortlichen hinter den Angriffen zu identifizieren und zur Rechenschaft zu ziehen. Eine effektive Strafverfolgung hat eine abschreckende Wirkung auf potenzielle Täter.

4.3 Ergebnis der Prüfung: Mögliche Umsetzung eines verstärkten Informationsaustauschs

Der aktuelle Informationsaustausch fokussiert sich stark auf die Früherkennung und Frühwarnung vor Bedrohungen. Es ist entscheidend, über die technischen Details der Angriffe hinaus ein umfassendes Verständnis der weitreichenden Auswirkungen zu erlangen. Dazu gehört die Erfassung der Anzahl betroffener Systeme, der Dauer der Betriebsunterbrechungen, der finanziellen Verluste und des

[68] Vgl. Website: www.fscsc.ch; zuletzt besucht am 20. Oktober 2024.
[69] Medienmitteilung «Bundesrat veröffentlicht Bericht zur Bekämpfung der Cyberkriminalität in der Schweiz» (Webseite: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-101469.html; zuletzt besucht am 20. Oktober 2024).

Umfangs der kompromittierten Daten. Gerade in Bezug auf Ransomware-Angriffe würden es solche Informationen erlauben, Aussagen zur Problematik der Lösegeldzahlungen zu machen.

Um solche Informationen systematischer zu erfassen, muss der bestehende Informationsaustausch auf weitere Akteure ausgeweitet werden. Insbesondere Versicherungen, andere Finanzintermediäre und Sicherheitsdienstleister verfügen über wertvolle Informationen zu den Auswirkungen von Cyberangriffen. Wenn es gelingt, diese Informationen verstärkt auszutauschen, kann die Transparenz bezüglich Schäden durch Ransomware-Angriffe erhöht werden. In einem ersten Schritt könnte dabei auf einen freiwilligen Informationsaustausch gesetzt werden, statt eine gesetzliche Meldepflicht für Versicherungen, andere Finanzintermediäre und Sicherheitsdienstleister einzuführen. Diese Entscheidung basiert auf mehreren Überlegungen: Eine Meldepflicht würde erhebliche administrative und finanzielle Belastungen für Versicherungen und Behörden mit sich bringen, die möglicherweise nicht im Verhältnis zum erwarteten Nutzen stehen. Ein freiwilliger Austausch ermöglicht es, das System kontinuierlich an neue Erkenntnisse und Bedürfnisse anzupassen, ohne langwierige Gesetzesänderungen durchführen zu müssen. Zudem sind freiwillig geteilte Informationen oft detaillierter und kontextreicher als solche, die aufgrund einer gesetzlichen Verpflichtung gemeldet werden. Ein kooperativer Ansatz fördert das Vertrauen zwischen den Beteiligten und kann zu einer offeneren Kommunikationskultur führen. Um diesen Informationsaustausch zu fördern, könnte der Bund eine Plattform zur Verfügung stellen, auf welcher Informationen geteilt werden können, die über den Zweck der Früherkennung und Frühwarnung hinausgehen und vertiefte Analysen zu den Ursachen und Wirkungen von Cyberangriffen erlauben. In diesen Informationsaustausch sollen insbesondere Versicherungen und Sicherheitsdienstleister integriert werden. Die Wirksamkeit dieses freiwilligen Ansatzes könnte sodann periodisch evaluiert werden. Sollte sich aber zeigen, dass der freiwillige Informationsaustausch nicht die gewünschten Ergebnisse liefert, könnten verbindlichere Massnahmen in Betracht gezogen. Dies könnte beispielsweise eine anonyme Meldepflicht für Versicherer, andere Finanzintermediäre sowie Sicherheitsdienstleister beinhalten. Durch diesen gestuften Ansatz und die regelmässige Überprüfung kann ein umfassenderes und nuancierteres Bild der Cybersicherheitslage gewonnen werden, als es durch eine sofortige Meldepflicht möglich wäre. Dies ermöglicht es, effektivere Strategien zur Prävention und Bekämpfung von Cyberangriffen zu entwickeln und umzusetzen. Es wird geprüft, ob für diesen Informationsaustausch die bestehenden Plattformen des BACS genutzt werden können, um Synergien zu nutzen und den Aufwand für alle Beteiligten zu minimieren. Diese Vorgehensweise stellt ein konkretes Instrument dar, um die Entwicklung und Wirksamkeit des Informationsaustauschs zu verfolgen und bei Bedarf zeitnah reagieren zu können.

5 Schlussbetrachtung

Für den Schutz vor Ransomware-Angriffen bestehen in der Schweiz bereits heute zahlreiche behördliche Informationen, Anleitungen sowie Richtlinien zu IT-Grundschutzmassnahmen und rechtliche Vorgaben zur Cybersicherheit. Der Bundesrat ist der Ansicht, dass man im Bedarfsfall vielmehr die bestehenden allgemeinen Cybersicherheitsvorgaben weiterentwickeln sollte, um eine breitere und flexiblere Abwehrstrategie zu ermöglichen, als spezifische neue Vorgaben zu Ransomware zu erlassen.

Die Kompetenzordnung zwischen Bund und Kantonen sowie das in der Bundesverfassung enthaltene Subsidiaritätsprinzip bedeuten, dass der Bund keine flächendeckenden verbindlichen Cyberschutzmassnahmen für kantonale oder kommunale Organisationen mit öffentlichem Auftrag vorschreiben kann. Die Kantone sowie Gemeinden müssen daher eigenständig Vorgaben zum Schutz ihrer IT-Infrastrukturen entwickeln, wobei sie sich an der nationalen Cybersicherheitsstrategie sowie den Informationen, Anleitungen und Richtlinien, Rechts- und Verwaltungsverordnungen des Bundes zur Cybersicherheit orientieren können.

Massnahmen **gegen Ransomware-Angriffe**

Die Prüfung einer möglichen Meldepflicht von Lösegeldzahlungen bei Ransomware-Angriffen hat ergeben, dass die Ziele einer erhöhten Transparenz und einer besseren Übersicht über die Schäden durch Ransomware-Angriffe eher durch eine Förderung des Informationsaustauschs als durch die Einführung einer weiteren Meldepflicht erreicht werden können.

Durch die Verbesserung des bestehenden Informationsaustauschs auf freiwilliger Basis könnten technische und organisatorische Massnahmen getroffen werden, welche die Resilienz gegenüber Ransomware-Angriffen erhöhen und die digitale Infrastruktur langfristig stärken würden. Mehr Kooperation und ein vertiefter Informationsaustausch zwischen Bund, kantonalen Strafverfolgungsbehörden, privaten Sicherheitsdienstleister, Versicherungen und anderen Finanzintermediären sind entscheidend, um die Bedrohung durch Cyberkriminalität effektiv zu bekämpfen und die Sicherheit der digitalen Infrastruktur langfristig zu gewährleisten.

Der Bund unterstützt den Informationsaustausch und kann eine koordinierende Rolle übernehmen, umso die gemeinsame Abwehr von Ransomware-Angriffen zu stärken. Falls die Wirksamkeit des freiwilligen Informationsaustausches nicht die gewünschten Ergebnisse liefert, könnten verbindlichere Massnahmen wie eine anonyme Meldepflicht für Versicherer, andere Finanzintermediäre sowie Sicherheitsdienstleister in Betracht gezogen werden. Diese Vorgehensweise ist nach Ansicht des Bundesrats zielführender als neue Vorgaben spezifisch für Ransomware-Angriffe.

Glossar

AppLocker	Eine Software zur Kontrolle, welche Anwendungen Benutzer ausführen dürfen.
Backup	Eine Kopie von Daten, die zur Wiederherstellung verwendet werden kann, falls die Originaldaten verloren gehen oder beschädigt werden.
Best Practices	Bewährte, als optimal anerkannte Methoden oder Verfahrensweisen.
Citrix	Eine Virtualisierungsplattform, die Fern-Zugriffe auf Anwendungen und Desktops ermöglicht.
E-Learning	Elektronisch unterstütztes Lernen, oft über das Internet.
E-Mail	Elektronische Post; ein digitales Nachrichtensystem zum Austausch von Nachrichten und Dateien über Computernetzwerke.
Excel	Ein Tabellenkalkulationsprogramm von Microsoft, das zur Erstellung und Bearbeitung von Tabellen, Diagrammen und Berechnungen verwendet wird.
Gatekeeper	Ein Sicherheitsmechanismus in macOS, der die Installation und Ausführung von Software kontrolliert.
Governance	Grundsätze, Verfahren und Massnahmen, mit denen ein Unternehmen geführt und kontrolliert wird.
Informationssicherheits-Managementsystem (ISMS)	Ein Informationssicherheits-Managementsystem (ISMS) ist ein strukturiertes System von Richtlinien, Prozessen und Massnahmen, das Unternehmen dabei unterstützt, die Sicherheit ihrer Informationen zu gewährleisten. Es basiert häufig auf internationalen Standards wie ISO/IEC 27001 und umfasst die Festlegung von Sicherheitsrichtlinien, ein Risikomanagement sowie die Implementierung technischer und organisatorischer Massnahmen. Ziel ist es, Informationen vor Bedrohungen zu schützen und gesetzliche Anforderungen zu erfüllen, während gleichzeitig eine kontinuierliche Überprüfung und Verbesserung des Systems erfolgt.
IKT	Informations- und Kommunikationstechnologie; umfasst alle technischen Mittel zur Verarbeitung und Übertragung von Informationen.

IT	Informationstechnologie; umfasst alle technischen Mittel zur Verarbeitung von Informationen.
IT-Infrastruktur	Die Gesamtheit der Hardware, Software, Netzwerke und Einrichtungen, die für den Betrieb und die Verwaltung der IT-Umgebung einer Organisation erforderlich sind.
IT-System	Eine Kombination von Hardware, Software und Netzwerkressourcen, die zusammenarbeiten, um Informationen zu verarbeiten und zu speichern.
Makro	Eine Folge von Befehlen oder Anweisungen, die automatisiert in einem Programm ausgeführt werden können, um wiederholende Aufgaben zu vereinfachen.
Multi-Faktor-Identifikation (MFA)	Ein Sicherheitssystem, das zur Authentifizierung mehr als einen Nachweis (Faktor) der Identität erfordert.
Nationale Cyberstrategie (NCS)	Ein umfassender Plan auf nationaler Ebene zur Verbesserung der Cybersicherheit und zum Schutz kritischer Infrastrukturen vor Cyberbedrohungen.
Netzzone	Ein abgegrenzter Bereich innerhalb eines Netzwerks mit spezifischen Sicherheitsrichtlinien.
Operative Technologie (OT)	Hardware und Software, die physische Geräte, Prozesse und Ereignisse in Unternehmen überwacht und steuert.
PowerPoint	Ein Präsentationsprogramm von Microsoft, das zur Erstellung und Vorführung von visuellen Präsentationen verwendet wird.
RAR	Ein Dateiformat für komprimierte Archive.
Ransomware	Eine Art von Malware, die Daten verschlüsselt und Lösegeld für deren Freigabe verlangt.
Remote Desktop Prozedur (RDP)	Ein Protokoll, das Benutzern erlaubt, sich mit einem anderen Computer über ein Netzwerk zu verbinden.
SELinux	Security-Enhanced Linux; ein Sicherheitsmodul für den Linux-Kernel, das zusätzliche Zugriffskontrollmechanismen bietet.
SPAM-Filter	Ein Programm oder Gerät, das unerwünschte E-Mails (Spam) erkennt und blockiert.
Sharepoint	Eine webbasierte Plattform von Microsoft für Zusammenarbeit und Dokumentenverwaltung.
Virtuelles Privates Netzwerk (VPN)	Eine verschlüsselte Netzwerkverbindung, die es ermöglicht, sicher über öffentliche Netzwerke zu kommunizieren.
Webmail	Ein E-Mail-Dienst, der über einen Webbrowser zugänglich ist. I

Glossar

Word	Ein Textverarbeitungsprogramm von Microsoft, das zur Erstellung und Bearbeitung von Dokumenten verwendet wird.
Workshops	Interaktive Veranstaltungen, bei denen Teilnehmer praktische Erfahrungen sammeln und Wissen austauschen.
ZIP	Ein weit verbreitetes Dateiformat für komprimierte Archive.