RISIKO

GRUNDLAGEN

Die Schweizerische Eidgenossenschaft, die internationale Rolle als Vermittlerin und der Gedanke der Helvetia Mediatrix (Gastbeitrag)
[Andrey Burnashev]

Zeugnisverweigerungsrecht für Sozialarbeitende im Kontext von Fanarbeit im Fussball
[Tim Willmann / Elena Urech / Alain Brechbühl / Jonas Weber]

POLIZEI & MILITÄR

Polizeiliche Vorermittlungen als Mittel zur Verdachtsbegründung?
[Lucien Müller]

TECHNIK & INFRASTRUKTUR

Cyberangriffe auf Schweizer Unternehmen und Behörden 2023–2025
[Fabian Teichmann]

RISIKO & RECHT AUSGABE 03 / 2025

RECHT

Risiko & Recht macht es sich zur Aufgabe, Rechtsfragen der modernen Risikogesellschaft zu analysieren. Berücksichtigung finden Entwicklungen in verschiedensten Gebieten, von denen Sicherheitsrisiken für Private, die öffentliche Ordnung, staatliche Einrichtungen und kritische Infrastrukturen ausgehen. Zu neuartigen Risiken führt zuvorderst der digitale Transformationsprozess und der damit verbundene Einsatz künstlicher Intelligenz; des Weiteren hat die Covid-Pandemie Risikopotentiale im Gesundheitssektor verdeutlicht und auch der Klimawandel zwingt zu umfassenderen Risikoüberlegungen; schliesslich geben gesellschaftliche Entwicklungen, u.a. Subkulturenbildung mit Gewaltpotential, Anlass zu rechtlichen Überlegungen. Risiko und Recht greift das breite und stets im Wandel befindliche Spektrum neuartiger Risikosituationen auf und beleuchtet mit Expertenbeiträgen die rechtlichen Herausforderungen unserer Zeit.

Editorial

Sehr geehrte Damen und Herren

Die vorliegende Ausgabe 3/2025 der Risiko & Recht deckt ein breites Themenspektrum aktueller Sicherheitsfragen ab. Eingangs setzt sich der Historiker und Informations- und Dokumentationsspezialist Andrey Burnashev mit der Tradition von Neutralität und «guten Diensten» auseinander. Hierbei nimmt die Schweiz eine internationale Rolle als Vermittlerin ein. Der Autor analysiert dies anhand der beiden Missionen NNSC-Korea und UNTAG-Namibia.

Die Autorinnen und Autoren Tim Willmann, Elena Urech, Alain Brechbühl und Jonas Weber befassen sich mit dem Zeugnisverweigerungsrecht für Sozialarbeitende im Kontext von Fanarbeit im Fussball. Anhand eines Urteils des Amtsgerichts Karlsruhe werden die Problematik nachgezeichnet, eine Kontextualisierung des Berufsfelds erstellt, die rechtlichen Grundlagen dargelegt und schliesslich für eine Erweiterung des Zeugnisverweigerungsrechts im Strafprozess argumentiert.

Lucien Müller befasst sich in seinem Beitrag mit der umstrittenen Frage, ob polizeiliche Vorermittlungen als Mittel zur Verdachtsbegründung eingesetzt werden dürfen.

Weiter analysiert Fabian Teichmann die Zunahme und Eskalation von Cyberangriffen auf Schweizer Unternehmen und Behörden in den Jahren 2023 bis 2025 und ordnet hierbei exemplarische Fälle sowohl technisch als auch juristisch ein.

Schliesslich setzt sich Patrice Martin Zumsteg im Rahmen einer Buchrezension mit der Dissertation von Roman Schuppli auseinander. Die besprochene Dissertation untersucht die bevölkerungsnahe Polizei(-arbeit) im Gesamtkontext des Polizeirechts und zeigt auf, welche Aspekte davon in der Schweiz umsetzbar sind und welche Hindernisse ihrer Realisierung entgegenstehen.

Wir wünschen Ihnen, geschätzte Leserinnen und Leser, eine anregende Lektüre und erlauben uns noch auf die Möglichkeit eines Print-Abonnements hinzuweisen.

Tilmann Altwicker
Dirk Baier
Goran Seferovic
Franziska Sprecher
Stefan Vogel
Sven Zimmerlin

Cyberangriffe auf Schweizer Unternehmen und Behörden 2023–2025

Fabian Teichmann*

Der Beitrag analysiert die Zunahme und Eskalation von Cyberangriffen auf Schweizer Unternehmen und Behörden in den Jahren 2023 bis 2025 und ordnet exemplarische Fälle technisch sowie juristisch ein. Im Zentrum stehen Angriffe mit erheblichen Auswirkungen auf öffentliche Verwaltungen, Medienhäuser und privatwirtschaftliche Akteure, darunter Xplain, das Erziehungsdepartement Basel-Stadt, die NZZ, BERNINA sowie die Gemeinde Saxon. Erörtert werden insbesondere Ransomware-Angriffe, Datenexfiltration, DDoS-Attacken durch Hacktivisten und Lieferkettenrisiken. Die Einführung der Meldepflicht für kritische Infrastrukturen per 1. April 2025 sowie die Errichtung des Bundesamtes für Cybersicherheit (BACS) markieren regulatorische Meilensteine zur Stärkung der nationalen Cybersicherheit. Eine systematische Auswertung der Vorfälle zeigt wiederkehrende Schwachstellen in den Bereichen IT-Security, Auftragskontrolle, organisatorische Resilienz und rechtliche Verantwortlichkeit. Abschliessend formuliert der Beitrag praxisnahe Empfehlungen für Behörden und Unternehmen zur Prävention, Reaktion und langfristigen Compliance im Umgang mit Cyberbedrohungen. Der Beitrag plädiert für einen koordinierten, ganzheitlichen Ansatz, der technische, rechtliche und strategische Massnahmen miteinander verzahnt und die internationale Zusammenarbeit in den Fokus rückt.

Inhalt

* RA Dr. iur. Dr. rer. pol. Fabian Teichmann, LL.M. (London), MBA (Oxford) ist Managing Partner der Teichmann International (Schweiz) AG sowie Präsident des Verwaltungsrats der Teichmann International (IT Solutions) AG. Er hat u.a. einen Master in Information Management Systems an der Harvard University und beschäftigt sich vorwiegend mit Cyberkriminalität. Fabian Teichmann hat Lehraufträge an den Universitäten Kassel, Trier und zu Köln sowie an der International Anti-Corruption Academy in Wien.

I. Einleitung

Cyberangriffe auf Schweizer Firmen und Behörden haben in den letzten Jahren deutlich zugenommen. Allein im Jahr 2022 wurden dem Nationalen Zentrum für Cybersicherheit (NCSC) über 34'000 Vorfälle gemeldet – 58 % mehr als im Vorjahr.[1] Dieser Trend setzte sich 2023 fort (im ersten Halbjahr rund 19'000 Meldungen, ca. 2'000 mehr als im ersten Halbjahr 2022)[2], was die Dringlichkeit effektiver Schutzmassnahmen unterstreicht. Die Bedrohungslage reicht von Ransomware-Angriffen mit Datendiebstahl bis zu politisch motivierten DDoS-Attacken, die kritische Dienste lahmlegen. Angesichts dieser Entwicklung hat die Schweiz die Meldepflicht für Cyberangriffe auf kritische Infrastrukturen eingeführt. Seit dem 1. April 2025 sind gemäss des revidierten ISG (Informationssicherheitsgesetz) Betreiber kritischer Infrastrukturen verpflichtet, erhebliche Cyberangriffe innerhalb von 24 Stunden an das neu geschaffene Bundesamt für Cybersicherheit (BACS) zu melden.[3]

II. Zentrale Fallbeispiele 2023–2025

Fall Xplain (Mai 2023): Ein besonders gravierender Vorfall ereignete sich beim Bundes-Auftragsnehmer *Xplain* AG. Am 23. Mai 2023 wurde bekannt, dass Hacker mittels Ransomware eine Schwachstelle bei Xplain ausgenutzt und rund 900 GB an Daten der Bundesverwaltung entwendet hatten. Darunter befanden sich hochsensible Informationen, u. a. Namen von Mitgliedern einer Armeespezialeinheit, Einträge aus der polizeilichen Hooligan-Datenbank sowie Privatadressen von Bundesratsmitgliedern. Die Täter, die der Ransomware-Gruppe «Play» zugeordnet werden, forderten Lösegeld – andernfalls würden

1 Computerworld.
2 Swiss IT Magazine.
3 Vasella; Art. 74e Abs. 1 des Schweizerischen Informationssicherheitsgesetzes vom 29. September 2023 (Informationssicherheitsgesetz, ISG, SR 128); BACS.

sie die Daten veröffentlichen. Xplain ging nicht darauf ein, woraufhin die Angreifer ihre Drohung wahrmachten und das Material im Darknet publizierten. Technisch handelte es sich um einen Double-Extortion-Angriff (Datenverschlüsselung plus Exfiltration). Xplain informierte die Behörden (u. a. BACS) und erstattete Anzeige.[4] Das unbefugte Eindringen in Xplains Systeme und der Datendiebstahl erfüllten Straftatbestände wie *unbefugtes Eindringen in ein Datenverarbeitungssystem* (Art. 143bis StGB)[5] und *Datenbeschädigung* durch Malware (Art. 144bis StGB).[6] Die anschliessende Erpressung fällt unter *Art. 156 StGB*[7] *(Erpressung)*.[8] Zudem waren hier datenschutzrechtliche Pflichten tangiert. Bundesstellen hatten teils personenbezogene Daten an Xplain weitergegeben, ohne klare Vereinbarung über deren Speicherung. Der Eidg. Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) stellte in seinem Untersuchungsbericht Fehler bei Bund und Xplain fest, etwa fehlende vertragliche Limitierungen und unzureichende Sicherheitsvorkehrungen. Als Konsequenz beschloss der Bundesrat diverse Massnahmen, z. B. striktere Sicherheitsvorgaben für externe IT-Auftragnehmer und ein verstärktes Sicherheitsmanagement in der Bundesverwaltung.[9] Dieser Fall zeigte deutlich die Risiken von Lieferketten-Angriffen und löste umfangreiche Diskussionen über die Verantwortlichkeit externer IT-Dienstleister aus.

Ransomware im Erziehungsdepartement Basel-Stadt (Januar/Mai 2023): Im Januar 2023 wurde das Erziehungsdepartement des Kantons Basel-Stadt Opfer eines Ransomware-Angriffs. Die Bande «BianLian» drang ins Netzwerk ein und entwendete etwa 1,2 Terabyte an Daten, darunter vermutlich auch Personendaten von Schülern und Angestellten. Nachdem das Departement die Lösegeldforderung ignorierte, stellten die Täter im Mai 2023 mehrere Datenpakete mit dem gesamten erbeuteten Datensatz ins Darknet. Die Behörden reagierten umgehend, indem Strafanzeige gegen Unbekannt eingereicht und sowohl der kantonale Datenschutzbeauftragte als auch das NCSC informiert wurden.[10] Die technischen Auswirkungen vor Ort waren erheblich – Teile der IT-Infrastruktur mussten vorsorglich vom Netz genommen und bereinigt werden. Juristisch erfüllen solche Angriffe den Tatbestand der *Datenbeschädi-*

4 Kanton Basel-Stadt.
5 BSK StGB-Weissenberger, Art. 143bis, Rz. 8-17.
6 BSK StGB-Weissenberger, Art. 144, Rz. 3, 20.
7 BSK StGB-Weissenberger, Art. 156, Rz. 4.
8 Art. 143bis, 144bis und 156 des Schweizerischen Strafgesetzbuches vom 21. Dezember 1937 (Strafgesetzbuch, StGB, SR 311).
9 SRF, Datenschützer sieht nach Hackerangriff Fehler bei Bund und Xplain.
10 Kanton Basel-Stadt.

gung (durch Verschlüsselung) sowie *Art. 143bis StGB* (*Unbefugtes Eindringen in ein Datenverarbeitungssystem*).[11] Das abgeflossene personenbezogene Datenmaterial unterliegt dem Datenschutzrecht; trotz damals noch fehlender Meldepflicht im alten DSG war das Departement aufgrund des Öffentlichkeitsprinzips und kantonaler Vorgaben gehalten, die Betroffenen und Behörden zu informieren. Die verweigerte Zahlung entsprach zudem der Empfehlung der Strafverfolgungsbehörden, da Lösegeldzahlungen das *Erpressungsdelikt* (*Art. 156 StGB*) nicht beenden, sondern oft Folgeforderungen nach sich ziehen. Der Fall Basel zeigte die Verwundbarkeit auch kantonaler Verwaltungen und die Wichtigkeit von Notfallplänen, um Bildungsbetrieb und Services trotz Ausfalls der IT fortführen zu können.

Gemeinde Saxon VS (April 2023): Ende April 2023 drang die Ransomware-Gruppe «Play» in das System der Vormundschaftsbehörde der Walliser Gemeinde *Saxon* ein. Dabei wurden Datenbestände gestohlen und verschlüsselt. Die unbekannten Täter drohten, vertrauliche Informationen – darunter persönliche Daten, Finanzdaten, Personalakten, Verträge – offenzulegen, sollte kein Lösegeld gezahlt werden. Die Erpresser setzten der Gemeinde eine Frist bis zum 11. Mai und verlängerten sie um einen Tag, bevor sie mit der Veröffentlichung beginnen würden.[12] Saxon ging nicht öffentlich auf die Forderungen ein; in der Folge tauchten erste Datenauszüge im Leak-Forum der Gruppe auf. Der Angriff wurde polizeilich untersucht, die Staatsanwaltschaft leitete ein Verfahren ein.[13] Juristisch sind hier, ähnlich wie bei Basel-Stadt, *Unbefugtes Eindringen in ein Datenverarbeitungssystem* und *Erpressung* einschlägig (Art. 143bis, Art. 144bis, Art. 156 StGB).[14] Für eine kleine Gemeindebehörde stellen solche Angriffe eine besondere Herausforderung dar, da oft Ressourcen und spezialisierte Kenntnisse zur Abwehr fehlen. Im Fall Saxon wurde technische Unterstützung vom Kanton und NCSC beigezogen, was die Bedeutung kantonaler Zusammenarbeit bei Cybervorfällen unterstreicht. Auch dieser Fall demonstriert, dass *Lösegeldverzicht* zwar zum Leak der Daten führte, aber aus Sicht der öffentlichen Hand die rechtlich und ethisch richtige Entscheidung war – ein Präzedenzfall, der anderen Gemeinden als Orientierung dient.

Cyberangriff auf NZZ und CH Media (März/April 2023): Im März 2023 wurden die Verlagshäuser Neue Zürcher Zeitung (NZZ) und CH Media nahezu gleichzeitig Opfer eines koordinierten Ransomware-Angriffs. Die Hackergruppe

---

11 BSK StGB-Weissenberger, Art. 143bis, Rz. 17 ff.; Art. 143bis StGB.

12 Jaun/Züllig.

13 SRF, Hacker stehlen Daten der Vormundschaftsbehörde der Gemeinde Saxon.

14 BSK StGB-Weissenberger, Art. 156, Rz. 10-12; Art. 143bis, 144bis und 156 StGB.

«Play» bekannte sich zu den Angriffen und erlangte Zugriff auf interne Systeme. Sie entwendete vertrauliche Unternehmensdaten, insbesondere Mitarbeitendendaten (z. B. Lohnlisten), Projektunterlagen und weitere Geschäftsinfos. Die Angreifer sperrten teils IT-Systeme und forderten von der NZZ Lösegeld, andernfalls würden die Daten ab dem 24. April veröffentlicht.[15] Die Verlage verzichteten auf Zahlungen. Daraufhin veröffentlichten die Kriminellen Anfang Mai ein erstes Datenpaket von ca. 5 GB auf ihrem Leak-Portal.[16] Technisch war der Geschäftsbetrieb der Medien zunächst kaum beeinträchtigt – Redaktionssysteme liefen weiter –, aber der Datenschutz-Vorfall war beträchtlich. Personalakten und vertrauliche E-Mails gelangten in fremde Hände. Beide Verlage arbeiteten eng mit Spezialisten und der Polizei zusammen, um den Vorfall zu untersuchen. Juristisch liegen auch hier *Computerdelikte und Erpressung*[17] vor; besonders heikel war, dass potentiell Quellen- und Redaktionsgeheimnisse gefährdet sein konnten, falls journalistisch vertrauliche Informationen kompromittiert wurden. Zwar gibt es in solchen Fällen (anders als etwa im Gesundheitswesen) keine spezifische Branchenaufsicht, doch können sich Pressunternehmen im Ernstfall auf das Redaktionsgeheimnis berufen, um bestimmte Daten gegenüber Ermittlern zu schützen. Gleichwohl mussten sie im Rahmen der Sorgfaltspflichten nach revidiertem DSG prüfen, ob eine Meldung an den EDÖB und eine Information betroffener Mitarbeiter erforderlich ist (bei potenziellem *hohem Risiko für die Persönlichkeitsrechte* gemäss Art. 24 DSG).[18] Der Vorfall NZZ/CH Media unterstrich, dass auch vermeintlich gut geschützte Medienhäuser ins Visier professioneller Erpresserbanden geraten können.

Angriff auf BERNINA International (April 2023): Ein Beispiel aus der Privatwirtschaft ist der Cyberangriff auf die *BERNINA International* AG, einen Schweizer Hersteller von Näh- und Textilmaschinen mit Sitz in Steckborn. Ende April 2023 tauchte auf der Leak-Seite der Ransomware-Gruppe ALPHV/BlackCat die Meldung «BERNINA International gehackt» auf. Die Täter behaupteten, über 200 GB an Daten (rund 415'000 Dateien) entwendet zu haben, und verschlüsselten gleichzeitig grosse Teile der IT-Infrastruktur (sieben Hyper-V-Server). Backups auf Bändern und Netzwerkspeichern wurden offenbar gelöscht, um die Wiederherstellung zu erschweren. Zu den gestohlenen Informationen zählten umfangreiche Kundendaten, Mitarbeiterdaten, Versi-

15 SRF, Hacker erbeuten bei der NZZ offenbar vertrauliche Personaldaten.

16 Jaun/Züllig.

17 BSK StGB-Weissenberger, Art. 143bis, Rz. 146-156.

18 Art. 24 des Bundesgesetzes über den Datenschutz vom 25. September 2020 (Datenschutzgesetz, DSG, SR 235.1); Keller/Tschudin/Roos/Boller.

cherungsdetails, vertrauliche Verträge (NDAs) sowie technische *Zeichnungen und Entwicklungsdokumente*. Die Angreifer brüsteten sich sogar, den kompletten E-Mail-Verlauf und die Kontaktlisten erbeutet zu haben.[19] BERNINA schaltete umgehend externe Cyber-Forensiker ein und erstattete Anzeige; eine öffentliche Stellungnahme erfolgte erst nach und nach, während der Betrieb, soweit möglich, manuell weiterlief. Juristisch bewegt sich der Fall im Bereich der *Wirtschaftskriminalität*. Neben den üblichen Strafnormen (Unbefugtes Eindringen in ein Datenverarbeitungssystem, Datenbeschädigung, Erpressung) steht hier die Verletzung von Geschäftsgeheimnissen im Raum – wären die Täter interne Personen, käme Art. 162 StGB (Verletzung des Fabrikations- und Geschäftsgeheimnisses)[20] ins Spiel, doch bei externen Hackern greifen primär die allgemeinen Cyberstrafnormen. Aus zivilrechtlicher Sicht könnten Kunden oder Partner Ansprüche stellen, falls BERNINA vertragswidrig deren vertrauliche Informationen nicht ausreichend geschützt hat. Der Vorfall machte deutlich, dass international tätige KMU ebenso im Fadenkreuz stehen und dass *Industriegeheimnisse* durch Cyberangriffe akut gefährdet sind.

Hackerangriff auf Concevis AG (Nov 2023): Im Herbst 2023 wurde bekannt, dass ein Bundes-Auftragnehmer attackiert wurde – die in Basel ansässige Concevis AG, ein Softwareunternehmen, fiel einem Ransomware-Angriff zum Opfer. Alle Server der Firma wurden verschlüsselt, und gleichzeitig erbeuteten die Täter umfangreiche Daten. Laut Eidg. Finanzdepartement handelte es sich dabei um ältere Betriebsdaten der Bundesverwaltung, die bei Concevis gespeichert waren. Nach der Datenentwendung weigerten sich die Verantwortlichen von Concevis, das geforderte Lösegeld zu zahlen. Daraufhin drohten die Cyberkriminellen, auch diese Bundesdaten im Darknet zu veröffentlichen. Concevis erstattete umgehend Strafanzeige. Es war das zweite Mal im Jahr 2023, dass Bundesdaten über einen externen IT-Dienstleister abflossen – eine Parallele zum Xplain-Vorfall vom Mai, auf den der Bundesrat bereits reagiert hatte. Juristisch ist der Fall Concevis praktisch ein Spiegelbild von Xplain. Wieder liegen *Unbefugtes Eindringen in ein Datenverarbeitungssystem* und *Erpressung* gemäss Art. 143bis und Art. 156 StGB vor, und wiederum stellt sich die Frage der Verantwortlichkeiten.[21] Obwohl der Bund selbst nicht direkt gehackt wurde, war er «indirekt betroffen»[22] – dies offenbart Lücken in der Auftragskontrolle. Nach neuem Recht (DSG) bleibt die Bundesbehörde als Verantwortlicher[23] für

19 Khaitan.
20 BSK StGB-Niggli/Hagenstein, Art. 162, Rz. 6-25; Art. 162 StGB.
21 Art. 143bis und 156 StGB.
22 SWI, Swiss government data affected by cyberattack on Basel firm.
23 Art. 33 DSG.

Personendaten verpflichtet, für angemessene Sicherheit auch beim Auftragsbearbeiter zu sorgen und Verletzungen der Datensicherheit gegebenenfalls dem EDÖB zu melden.[24] Der Concevis-Hack verdeutlichte, dass Vorgaben zur Datenlöschung und -minimierung strikt eingehalten werden müssen. Offensichtlich waren noch Bundesdaten vorhanden, die nicht mehr gebraucht wurden. Regulatorisch wird künftig das ISG hier greifen, das für Bundesstellen und ihre Auftragnehmer verbindliche Sicherheitsstandards etabliert.[25]

«Ultra»-Leak (Dez 2023) – Schweizer Militärdaten über US-Firma entwendet: Ein Fall mit internationaler Dimension betraf die Schweizer Armee. Im Dezember 2023 tauchten geheime Dokumente der Schweizer Luftwaffe im Darknet auf. Die Unterlagen – rund 30 GB teils als *klassifiziert* eingestufte Daten – stammten nicht direkt von der Armee, sondern von einem US-Rüstungsunternehmen, der Ultra Intelligence&Communications (Ultra I&C). Dieses Unternehmen liefert verschlüsselte Kommunikationssysteme an verschiedene Staaten, u. a. an das VBS und den Rüstungsbetrieb RUAG. Ultra I&C war zuvor von der Ransomware-Gruppe ALPHV (BlackCat) gehackt worden. Die Angreifer stahlen zehntausende Dokumente, darunter offenbar auch vertrauliche Informationen über den Einsatz von Ultra-Technologie in der Schweiz, und forderten Lösegeld. Nachdem Ultra die Zahlung verweigert hatte, veröffentlichte ALPHV die Daten am 27. Dezember 2023 vollständig im Darknet. Dies bedeutete einen Leak von militärisch sensiblen Informationen, der auch als *Lieferkettenrisiko* für die nationale Sicherheit zu bewerten ist. Das VBS bestätigte den Vorfall und leitete Untersuchungen ein. Experten warnten, dass durch die Veröffentlichung z. B. Schwachstellen von Geräten bekannt werden könnten, was weitere Angriffe erleichtert. In jedem Fall wirft der Ultra-Leak Fragen nach der Vertragssicherheit und Kontrolle auf, ob die Schweiz von ihren ausländischen Lieferanten mehr Sicherheitsnachweise verlangen sollte. Der EDÖB-Experte meinte dazu, die Verantwortung liege bei den Partnerfirmen und die Schweiz müsse allenfalls *höhere Sicherheitsstandards einfordern und überwachen*.[26] Dieser Vorfall machte deutlich, dass Cyberangriffe keine Landesgrenzen kennen und die internationale Zusammenarbeit essenziell ist, um solche Leaks einzudämmen und zukünftige zu verhindern.

---

24 Keller/Tschudin/Roos/Boller.

25 ISG; BACS, Informationen zur Meldepflicht; Eckert/Glaus.

26 SWI, Cyberattack exposes Swiss Air Force documents on the darknet.

III. Übergreifende Schwachstellen und Herausforderungen

Die geschilderten Fälle erlauben es, gemeinsame Schwachstellen und Herausforderungen im Umgang mit Cyberangriffen zu identifizieren. Viele Angriffe erfolgten über bekannte Schwachstellen oder fehlende Sicherheitsupdates. So nutzen Ransomware-Gruppen häufig bereits lange bekannte Lücken oder *Phishing*-E-Mails, um sich Zugang zu verschaffen.[27] In einigen Fällen (z. B. Xplain) wurde eine unzureichend gepatchte Server-Komponente ausgenutzt. Weiter begünstigt mangelnde Netzwerk-Segmentierung den Schadensumfang. Wenn sich ein Angreifer einmal Zugang verschafft, kann er sich in einem flach aufgebauten Netzwerk ungehindert ausbreiten und grosse Datenmengen abziehen oder verschlüsseln. Fehlen *Multifaktor-Authentifizierung* und strikte Zugriffskontrollen, haben es Angreifer zudem leichter, Administratorrechte zu erlangen. Patchmanagement und eine durchdachte Netzwerk-Architektur sind daher essenzielle technische Massnahmen, um das Risiko zu reduzieren.

Mehrere Vorfälle (Xplain, Concevis, Ultra) zeigen, dass Zulieferer und Drittparteien ein erhebliches Risiko darstellen. Häufig lagerten kritische Daten bei externen IT-Firmen, ohne dass Auftraggeber und Auftragnehmer klare Abmachungen zur Datensicherheit und -haltung getroffen hatten. Es entstand teils eine unstrukturierte Ansammlung sensibler Daten auf den Servern der Dienstleister.[28] Die *Verantwortlichkeiten* waren unklar, wer welche Daten zu Supportzwecken kopieren darf. Wer muss sie löschen? Wer informiert im Ernstfall die Betroffenen? Diese Lücken nutzten Kriminelle aus. Das Staatssekretariat für Sicherheitspolitik (Sepos) kam in einem Bericht zum Schluss, dass bei künftigen Beschaffungen die Sicherheitsanforderungen frühzeitig definiert und in Ausschreibungen verbindlich verankert werden müssen. Zudem dürfe sich die Sicherheitsprüfung nicht nur auf den direkten Lieferanten beschränken, da hinter einem Produkt oft weitverzweigte Unterlieferketten stehen.[29] Der Fall Ultra illustriert dies international, da hier ein Schweizer Geheimhaltungsschutz indirekt über einen ausländischen Subkontraktor unterlaufen wurde. Unternehmen und Behörden stehen vor der Herausforderung, *Due Diligence* in der gesamten Lieferkette auszuüben und vertraglich Audit-Rechte, Sicherheitsstandards und Meldewege bei Incidents klar festzulegen. Diese aufsichts-

27 Meier.
28 SRF, Datenschützer sieht nach Hackerangriff Fehler bei Bund und Xplain.
29 SRF, Der Bund gibt Empfehlungen zu Informationssicherheit ab.

rechtliche Kontrolle muss auch tatsächlich wahrgenommen werden, z.B. durch regelmässige Sicherheits-Audits bei IT-Zulieferern. An welche Rechte sich diese Unternehmen halten müssen, ist einzelfallabhängig und hängt u.a. davon ab, wo sie ihren Sitz haben und wo ihre Kunden ansässig sind.

Viele Täter operieren aus dem Ausland (oft Osteuropa/Russland) und agieren anonym im Darknet. Die Fälle *Play*, *BianLian*, *ALPHV* etc. zeigen, dass international tätige Cyberkriminelle selten dingfest gemacht werden. Selbst wenn die Schweiz Strafverfahren einleitet (Xplain, Saxon u. a.), ist sie auf internationale Rechtshilfe angewiesen. Doch die Zusammenarbeit mit Staaten, in denen sich diese Gruppierungen mutmasslich aufhalten, ist politisch heikel oder faktisch nicht vorhanden. So gelten Russland und einige andere Länder als *Safe Havens* für Ransomware-Gangs, da Auslieferungsbegehren oder Ermittlungsersuchen dort oft unbeantwortet bleiben. Diese Strafverfolgungsproblematik untergräbt die abschreckende Wirkung des Strafrechts. Zwar bestehen auf internationaler Ebene Übereinkommen (z. B. die *Budapester Konvention* über Cybercrime oder die neue Cybercrime Konvention der UN)[30] und Zusammenarbeit via Interpol/Europol, doch benötigen diese Prozesse viel Zeit. In der Schweiz selbst wurden die gesetzlichen Grundlagen für Cyberstrafverfolgung in den letzten Jahrzehnten zwar ausgebaut (Art. 143bis, 144bis StGB seit 1995; *Cybermobbing*, *Doxing* und ähnliche Phänomene werden diskutiert)[31]; ohne grenzüberschreitende Zusammenarbeit und diplomatischen Druck bleiben viele Hacker jedoch straflos. Ein weiteres Hindernis ist die Attribuierung. Bei DDoS-Angriffen ist es schwierig, individuelle Täter zu identifizieren, da es sich oft um lose Hacktivisten-Kollektive handelt. Hier stellt sich die Frage, ob in Zukunft staatliche Gegenmassnahmen (z. B. *Hack-Back* oder finanzielle Sanktionen gegen Schutzgeber-Staaten) Teil der Strategie werden sollten, was allerdings juristisch und ethisch umstritten ist.

Abseits rein technischer Lücken treten auch organisatorische Schwächen zutage. In einigen Fällen fehlte es an einer ganzheitlichen IT-Governance, die Cyberrisiken angemessen berücksichtigt. Beispielhaft hatten betroffene Organisationen keine aktuellen Notfallpläne oder klar definierte Prozesse zur Incident Response.

---

30 European Council; UN.

31 Bericht des Bundesrats vom 19. Oktober 2022 über Ergänzungen betreffend Cybermobbing im Strafgesetzbuch; Interpellation des Nationalrats vom 13. Dezember 2022 über Schutz vor Doxing; Art. 143bis und 144bis StGB.

IV. Empfehlungen für Behörden und Unternehmen

Vor dem Hintergrund der analysierten Angriffe sollten Behörden und Firmen, insbesondere Betreiber kritischer Infrastrukturen, umfassende Massnahmen ergreifen. Die Empfehlungen lassen sich in präventive Vorkehrungen, reaktive Schritte und dauerhafte Compliance-Massnahmen gliedern.

1. Prävention stärken

Jede Organisation sollte verbindliche IT-Sicherheitsgrundsätze etablieren (z. B. orientiert am ISMS [Informationssicherheits-Managementsystem] nach ISO 27001[32], das für Bundesstellen bis 2026 vorgeschrieben ist). Dazu gehören Netzsegmentierung, regelmässige Software-Updates, Backup-Konzepte mit Offline-Kopien, verpflichtende Multifaktor-Authentifizierung und ein strenges Rechte-Management. Für kritische Infrastrukturen sollten branchenspezifische Mindeststandards (wie NIST-Framework oder BSI-Grundschutz) als Basis dienen.

Es empfiehlt sich, Cyber-Risikoanalysen durchzuführen, um Schwachstellen proaktiv zu erkennen (inkl. Penetrationstests). Anschliessend sind die identifizierten Risiken mit Priorität zu behandeln. Unabhängige Security Audits – bei grossen Organisationen jährlich – können die Einhaltung der Policies prüfen. Gerade bei Zulieferern sollte der Auftraggeber regelmässige Audits einfordern. Im Fall Xplain wurde dies schmerzlich vermisst; künftig soll die Auditfähigkeit gegenüber Lieferanten deutlich gestärkt werden.[33]

Bei der Beschaffung von IT-Leistungen müssen Sicherheitsanforderungen bereits in der Ausschreibung und im Vertrag festgeschrieben werden. Verträge mit Cloud- oder Softwarelieferanten sollten *Datenschutz* und *Datensicherheit* ausführlich regeln, mit den Fragen «Wo werden welche Daten gespeichert? Wie werden sie geschützt (Verschlüsselung, Zugriffsprotokollierung)? Welche Meldepflichten hat der Auftragnehmer im Falle eines Incidents?» Empfehlenswert sind Klauseln zu regelmässigen Updates, *Vulnerability-Management* und sofortiger Benachrichtigung bei Sicherheitsvorfällen. Zudem sollte der Auftraggeber ein Recht auf Sicherheitsprüfungen (Pen-Tests) erhalten. Nach den Vorfällen 2023 fordert der Bund explizit genauere Abklärungen und Vorgaben

32 Fleischauer/Stiemerling, 147 Rz. 73.

33 SRF, Datenschützer sieht nach Hackerangriff Fehler bei Bund und Xplain.

bei der Auftragsvergabe, um Datenabflüsse bei externen IT-Dienstleistern zu verhindern.[34]

Unternehmen und Behörden sollten ihre Daten nach Sensitivität klassifizieren (z. B. öffentlich, intern, vertraulich, geheim) und entsprechend unterschiedlich schützen. *Kritische Datenbestände*, wie Personendaten, Forschungs- und Entwicklungsdaten und Behördengeheimnisse gehören besonders gesichert (starke Verschlüsselung, begrenzter Zugriff, idealerweise kein Internetzugang von Systemen mit Staatsgeheimnissen). Im Fall Ultra wäre z. B. zu prüfen gewesen, ob hochsensible militärische Infos überhaupt extern gespeichert werden durften. Eine strenge Datenklassifikation hilft auch im Krisenfall, da man sofort weiss, welche Systeme höchste Priorität bei Schutz und Wiederherstellung geniessen.

2. Reaktion optimieren

Jede Organisation benötigt einen Incident Response Plan für Cyberangriffe. Dieser sollte definieren, wer im Ereignisfall welche Rolle übernimmt (IT-Forensik, Kommunikation, Recht, Management) und welche externen Partner zu informieren bzw. hinzuzuziehen sind (z. B. NCSC/BACS, spezialisierte Cyber-Security-Firmen, Strafverfolgung). Regelmässige Notfallübungen (inkl. Simulation von Ransomware-Befall oder DDoS) schulen das Team und decken Lücken auf. So kann z. B. geübt werden, wie man ein vom Netz getrenntes Backup einspielt oder welche Entscheidungen das Krisenteam bei einer Lösegeldforderung trifft. Im Ernstfall sorgt ein erprobter Plan für schnellere und koordiniertere Reaktionen, da jede Stunde Verzögerung sonst Schaden in Millionenhöhe bedeuten kann.

Nach einem Angriff müssen umgehend juristische Abklärungen erfolgen. Zum einen sind Meldepflichten zu beachten[35] – seit 2025 gilt für viele Betreiber kritischer Infrastrukturen die Pflicht zur Meldung an das BACS innert 24 Stunden.[36] Daneben verlangt das revidierte DSG, dass *Datenpannen mit hohem Risiko* unverzüglich dem EDÖB gemeldet werden.[37] Es ist ratsam, dies in Abstimmung mit internen oder externen Datenschützern zu tun, um die Schwelle des «hohen Risikos» korrekt einzuschätzen. Gegebenenfalls müssen auch die betroffenen Personen informiert werden (z. B. Kunden, deren Daten geleakt

34 SRF, Der Bund gibt Empfehlungen zu Informationssicherheit ab.
35 Art. 74b ISG.
36 VASELLA.
37 Art. 24 DSG.

wurden). Juristisch sollte weiter geprüft werden, ob *Haftungsansprüche* Dritter zu erwarten sind oder ob man selbst Regress bei einem Lieferanten nehmen kann. Beispielsweise könnte eine Behörde nach einem Lieferketten-Leak Schadenersatz vom unsorgfältigen IT-Dienstleister fordern. In Strafsachen ist zudem die Erstattung einer Strafanzeige unerlässlich (wie in allen genannten Fällen erfolgt). Auch wenn die Täter unbekannt bleiben, zeigt man so Kooperationsbereitschaft mit den Behörden und wahrt allfällige Versicherungsansprüche (Cyber-Versicherungen verlangen meist eine Anzeige). Zudem können Ermittlungen später doch zur Identifizierung führen oder mindestens zur Informationsgewinnung (Indicators of Compromise), die anderen hilft.

V. Fazit und Ausblick

Die Jahre 2023–2025 haben gezeigt, dass Cyberangriffe in der Schweiz zur realen Gefahr für Wirtschaft und Staat geworden sind. Kein Sektor ist ausgenommen – von der kleinen Gemeindebehörde bis zum international tätigen Industriekonzern wurden Schwachstellen ausgenutzt. Die Einführung der *Meldepflicht ab 2025* markiert einen wichtigen Schritt. Nun erhält das Bundesamt für Cybersicherheit (BACS) einen umfassenderen Überblick über die Angriffslage. Dies wird es erlauben, Trends frühzeitig zu erkennen und Warnungen gezielter auszusprechen.

Trotzdem bleibt viel zu tun, um resiliente Infrastrukturen zu schaffen. Resilienz bedeutet, Angriffe abwehren zu können oder bei Erfolg der Angreifer den Schaden einzugrenzen und schnell wieder handlungsfähig zu sein. Dazu müssen technische, organisatorische und personelle Massnahmen verzahnt werden. Die in diesem Artikel diskutierten Fälle liefern wertvolle Lehren. *Backups offline aufbewahren*, *kritische Systeme isolieren*, *Notfallprozesse üben*, *Verträge nachschärfen*, *Mitarbeiter schulen* und vor allem Cybersecurity als Chefsache behandeln. Geschäftsleitungen und Behördenleitungen tragen die Verantwortung, hierfür ausreichend Ressourcen bereitzustellen. Die Bedrohungsakteure entwickeln sich ständig weiter. Beispielsweise setzen Ransomware-Gruppen vermehrt auf Zero-Day-Exploits und Hacktivisten koordinieren sich global über Messaging-Plattformen. Dem müssen die Abwehrstrategien immer einen Schritt voraus sein.

Abschliessend lässt sich feststellen, dass die Welle von Cyberangriffen 2023–2025 ein Weckruf war. Schweizweit wurden Defizite offenbart, aber zugleich entstanden durch den Erfahrungsaustausch neue Best Practices. Behörden, IT-Verantwortliche und Unternehmensjuristen sind gefordert, gemeinsam eine robuste Cyber-Resilienz aufzubauen. Cyberangriffe werden nicht

verschwinden; aber die Schadwirkung kann durch vorausschauendes Handeln und abgestimmte rechtliche sowie technische Mittel deutlich begrenzt werden. Die Devise lautet, dass *Prävention der beste Schutz ist, und im Ernstfall zählt jede Minute – vorbereitet sein zahlt sich aus.*

Literaturverzeichnis

BACS, Informationen zur Meldepflicht, Admin.ch vom 5. August 2025, abrufbar unter <https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/meldepflicht-info.html>.

Computerworld, Mehr gemeldete Cybervorfälle 2022, Computerworld vom 3. Januar 2023, abrufbar unter <https://www.computerworld.ch/security/hacking/gemeldete-cybervorfaelle-2022-2827203.html>.

Eckert Martin/Noëlle Glaus, Update zum neuen Informationssicherheitsgesetz, MME vom 5. April 2024, abrufbar unter <https://www.mme.ch/de-ch/magazin/artikel/update-zum-neuen-informationssicherheitsgesetz>.

European Council, Übereinkommen über Computerkriminalität vom 23. November 2001, SEV NR. 185, abrufbar unter <https://rm.coe.int/168008157a>.

Interpellation des Nationalrats vom 13. Dezember 2022 über Schutz vor Doxing, eingereicht von Bellaiche Judith, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20224361>.

Jaun René/Züllig Yannick, Update: Ransomware-Bande Play gewährt Walliser Gemeinde mehr Zeit, Swisscybersecurity vom 11. Mai 2023, abrufbar unter <https://www.swisscybersecurity.net/cybersecurity/2023-05-02/walliser-vormundschaftsbehoerde-wird-opfer-eines-cyberangriffs>.

Kanton Basel-Stadt, Cyberkriminelle veröffentlichen Daten des Erziehungsdepartements im Darknet, Medienmitteilung vom 10. Mai 2023, <https://www.bs.ch/medienmitteilungen/ed/2023-cyberkriminelle-veroeffentlichen-daten-des-erziehungsdepartements-im-darknet>.

Keller Claudia/Tschudin Michael/Roos Dominique/Boller Marcel, Handlungsbedarf aufgrund des revidierten Schweizer Datenschutzgesetzes, LEXOLOGY vom 28. Januar 2021, abrufbar unter <https://www.lexology.com/library/detail.aspx?g=8114b455-09eb-4d9a-9c9e-301d66340a7c>.

Khaitan Ashish, BERNINA International hacked: ALPHV Ransomware group strikes the sewing machine manufacturer, The Cyber Express vom 26. April 2023, abrufbar unter <https://thecyberexpress.com/bernina-international-hacked/>.

Meier Sara, Diese Cybercrime-Trend haben das Jahr 2023 geprägt, Swisscybersecurity vom 17. Januar 2024, abrufbar unter <https://www.swisscybersecurity.net/news/2024-01-17/diese-cybercrime-trends-haben-das-jahr-2023-gepraegt>.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Schweizerisches Strafrecht, Basler Kommentar, Basel 2019 (zit.: BSK StGB-Bearbeiter/in, Art. XX Rz. YY).

FLEISCHAUER HARALD/STIEMERLING OLIVER, Technisches Risikomanagement, in: Remmertz Frank/Kast Christian (Hrsg.), Digital Escrow, München 2022, 127 ff.

SRF, Hacker erbeuten bei der NZZ offenbar vertrauliche Personaldaten, SRF vom 22. April 2023a, abrufbar unter <https://www.srf.ch/news/schweiz/cyberangriff-hacker-erbeuten-bei-der-nzz-offenbar-vertrauliche-personaldaten>.

SRF, Hacker stehlen Daten der Vormundschaftsbehörde der Gemeinde Saxon, SRF vom 28. April 2023b, abrufbar unter <https://www.srf.ch/news/schweiz/cyberangriff-im-wallis-hacker-stehlen-daten-der-vormundschaftsbehoerde-der-gemeinde-saxon>.

SRF, Datenschützer sieht nach Hackerangriff Fehler bei Bund und Xplain, SRF vom 1. Mai 2024, abrufbar unter <https://www.srf.ch/news/schweiz/nach-datenklau-bei-xplain-datenschuetzer-sieht-nach-hackerangriff-fehler-bei-bund-und-xplain>.

SRF, Der Bund gibt Empfehlungen zu Informationssicherheit ab, SRF vom 1. Mai 2025, abrufbar unter <https://www.srf.ch/news/schweiz/nach-hackerangriff-auf-xplain-der-bund-gibt-empfehlungen-zu-informationssicherheit-ab>.

Swiss IT Magazine, Zahl der gemeldeten Cybervorfälle beim NCSC deutlich gestiegen, Swiss IT-Magazine vom 3. November 2023, abrufbar unter <https://www.itmagazine.ch/artikel/80871/Zahl_der_gemeldeten_Cybervorfaelle_beim_NCSC_deutlich_gestiegen.html>.

SWI swissinfo, Swiss government data affected by cyberattack on Basel firm, SWI vom 14. November 2023, abrufbar unter <https://www.swissinfo.ch/eng/business/swiss-government-data-affected-by-cyber-attack-on-basel-firm/48977580>.

SWI swissinfo, Cyberattack exposes Swiss Air Force documents on the darknet, SWI vom 6. Januar 2024, abrufbar unter <https://www.swissinfo.ch/eng/business/cyberattack-exposes-swiss-air-force-documents-on-the-darknet/49100914>.

UN, Convention against Cybercrime of 24 December 2024, Resolution 79/247, Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes <https://docs.un.org/en/A/RES/79/243>.

VASELLA DAVID, Meldepflicht für Cyberangriffe auf kritische Infrastrukturen gilt ab 1. April 2025, Datenrecht vom 12 März 2025, <https://datenrecht.ch/meldepflicht-fuer-cyberangriffe-auf-kritische-infrastrukturen-gilt-ab-1-april/?hilite>.

RISIKO RECHT

3. Jahrgang

HERAUSGEBER

WISSENSCHAFTLICHER BEIRAT

REDAKTION

Dr. Tobias Baumgartner, LL.M., Rechtsanwalt /
MLaw Sophie Tschalèr
Europa Institut an der Universität Zürich
Bellerivestrasse 49
8008 Zürich
Schweiz

ERSCHEINUNGSWEISE

R&R – Risiko & Recht erscheint dreimal jährlich online. Die Ausgaben werden zeitgleich im Wege des print on demand veröffentlicht; sie können auf der Verlagswebseite (www.eizpublishing.ch) sowie im Buchhandel bestellt werden.

ZITIERWEISE

R&R, Ausgabe 3/2025, …

KONTAKT

EIZ Publishing
c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Bellerivestrasse 49
8008 Zürich
Schweiz
eiz@eiz.uzh.ch

ISSN

2813-7841 (Print)
2813-785X (Online)

ISBN:

978-3-03994-045-5 (Print – Softcover)
978-3-03994-046-2 (ePub)

VERSION

1.01-20251120

DOI

Zeitschrift: https://doi.org/10.36862/eiz-rrz01;
Ausgabe: https://doi.org/10.36862/70SK-JD1N;
Andrey Burnashev, Die Schweizerische Eidgenossenschaft, die internationale Rolle als Vermittlerin und der Gedanke der Helvetia Mediatrix, https://doi.org/10.36862/60V3-GD1S;
Tim Willmann et al., Zeugnisverweigerungsrecht für Sozialarbeitende im Kontext von Fanarbeit im Fussball, https://doi.org/10.36862/6RRK-6DHJ;
Lucien Müller, Polizeiliche Vorermittlungen als Mittel zur Verdachtsbegründung?, https://doi.org/10.36862/64W3-8C9H;
Fabian Teichmann, Cyberangriffe auf Schweizer Unternehmen und Behörden 2023–2025, https://doi.org/10.36862/64SK-EE1J

RISIKO

EIZ Publishing

Herausgeber:
Prof. Dr. Tilmann Altwicker
Prof. Dr. Dirk Baier
Prof. Dr. Goran Seferovic
Prof. Dr. Franziska Sprecher
Prof. Dr. Stefan Vogel
Dr. Sven Zimmerlin

RISIKO & RECHT AUSGABE 03 / 2025

RECHT