Ausgabe 1 / 2025

tribune

Das Magazin für Wirtschaft und Recht

Unsere Daten, das neue Gold

Von Kurt Tschan

Das weltweite Datenvolumen wird nach Angaben der globalen Datenbank Statista in zwei Jahren über 284 Zettabyte erreichen. Dies entspricht 284 Billionen Gigabyte. Daten gibt es inzwischen wie Sand am Meer. Allerdings sind sie deutlich teurer, was sie zum Goldschatz des 21. Jahrhunderts macht.

Deshalb gehören Daten wie Gold in gut geschützte Tresore. Nach Schätzungen des Prüfungs- und Beratungsunternehmens PwC erreichen die Schäden durch Cyberkriminalität weltweit inzwischen 9,5 Billionen Franken.

Gerade jetzt, wo die ganze Welt nach Basel schaut, geniesst das Thema Cybersicherheit einen hohen Wert. Wenn vom 10. bis 17. Mai in der St. Jakobshalle der Eurovision Song Contest (ESC) über die Bühne geht, werden Millionen Zuschauer an den Bildschirmen sitzen. Auch die Fussball-EM der Frauen im Juli wird zu einem Grossanlass. In beiden Fällen geht es auch um Fragen des Datenschutzes.

Ohne freiwillige Helfer wären beide Anlässe nicht zu stemmen. «Um akkreditiert zu werden, muss ein Sicherheitscheck durchlaufen werden, bei welchem auch zahlreiche sensible Daten erhoben werden», bestätigt die Basler Datenschutzbeauftragte Danielle Kaufmann. Die datenschutzrechtliche Verantwortung liegt beim Kanton Basel-Stadt. Gefordert ist nach Angaben von Kaufmann in erster Linie das Präsidialdepartement. Für die Sicherheitsprüfungen ist die Kantonspolizei Basel-Stadt zuständig. Deshalb fungiert der Basler Datenschutz bei beiden Grossanlässen als Berater.

Im Fall des ESC ist auch das Televoting eine datenschutzrechtliche Herausforderung. 13 Seiten dick ist ein Dossier, das die Details regelt. Wem das zu aufwendig und zu kompliziert ist, könnte gut und gerne zum Schluss kommen, auf die Abgabe seiner Stimme zu verzichten. Datenschutz hin oder her.

beider basel handelskammer

Advokatenkammer Basel
Basellandschaftlicher Anwaltsverband

Ohne Transformation geht es nicht

Viele Schweizer Unternehmen haben in den letzten drei Jahren ihr Cyberbudget deutlich erhöht. Aus gutem Grund: Cyberkriminelle nutzen die Künstliche Intelligenz (KI) immer häufiger, um Angriffe noch effektiver durchführen zu können.

Von Chris Girling

Nie waren Regulatoren und Gesetzgeber im europäischen Raum aktiver, neue Vorschriften zur Steigerung der Cyberresilienz in Kraft zu setzen oder zu erarbeiten. Dadurch rückt das Thema Cybersicherheit noch stärker in den Fokus von Schweizer Unternehmen. Während einige Firmen proaktiv handeln, werden andere erst durch die neuen Regelungen damit konfrontiert. Insbesondere ein Thema, die persönliche Haftung der Geschäftsleitung bei Cyberangriffen, lässt breitere Wirtschaftssegmente nun stärker aktiv werden.

Vertrauen und Resilienz

Eine aktuelle Umfrage[1] von PwC unter Schweizer CEOs zeigt, dass rund 40 Prozent davon ausgehen, ihr Unternehmen werde ohne substanzielle Transformation die nächsten zehn Jahre nicht überleben. Neben der Notwendigkeit, das eigene Geschäftsmodell weiterzuentwickeln und neue Technologien wie generative KI zu nutzen, stellen Cybersicherheit, geopolitische Konflikte und makroökonomische Unsicherheiten die grössten Risiken für ihre Unternehmen dar.

Die neuen Vorschriften haben zwei zentrale Aspekte hervorgebracht: Vertrauen und Resilienz. Denn sowohl Behörden als auch Kunden erwarten, dass Unternehmen anerkannte IT-Sicherheitsstandards einhalten, ihre Systeme regelmässig verbessern und testen, Notfallpläne bereithalten und sich umfassend gegen Cyberangriffe absichern – was die gesamte Lieferkette einschliesst. Klare Verantwortlichkeiten sind dabei entscheidend.

Allerdings gibt es grosse Unterschiede zwischen verschiedenen Branchen: Während stark regulierte Unternehmen, vor allem im Finanzsektor, seit Jahren in Cybersicherheit investieren, stehen andere eher am Anfang. Das muss sich nun rasant ändern.

Zusätzliche Bedrohungen durch KI

Auch die Schweiz verfolgt auf nationaler Ebene eine Strategie zum Schutz des digitalen Ökosystems. Mit dem Nationalen Zentrum für Cybersicherheit (NCSC) und der aktualisierten Nationalen Cyberstrategie (NCS) von 2023 setzt sie klare Prioritäten.

Neue Technologien lösen «Goldrausch»-Phasen aus.

So bauen Schweizer Unternehmen ihre Sicherheitsmassnahmen kontinuierlich aus: Laut der PwC-Studie «Digital Trust Insights 2025»[2] haben rund 70 Prozent ihr Cyberbudget in den letzten drei Jahren deutlich erhöht.

Dennoch gibt es grosse Herausforderungen: Qualifizierte Sicherheitsexperten zu finden, ist aufgrund des Fachkräftemangels schwierig. Gleichzeitig entstehen durch neue Technologien wie KI und Quantencomputer nicht nur neue Möglichkeiten, sondern zusätzliche Bedrohungen, die Unternehmen dazu zwingen, ihre Ressourcen auf verschiedene Sicherheitsbereiche zu verteilen.

In bisher wenig regulierten Branchen wie der Industrie oder der Schweizer Startup-Szene wächst der Handlungsdruck – sowohl durch die neuen Vorschriften als auch durch die zunehmende Anzahl an Cyberangriffen. Laut unserer Studie fühlen sich Schweizer Führungskräfte im internationalen Vergleich weniger sicher in der Einhaltung von Cybervorschriften – schätzen aber die regulatorische Klarheit mehr als ihre globalen Kollegen.

Schnellere und effizientere Angriffe

Neue Technologien entwickeln sich rasant und lösen regelmässig regelrechte «Goldrausch»-Phasen aus. Unternehmen setzen dann überstürzt auf neue Lösungen – oft ohne deren Risiken genau zu kennen. Gleichzeitig haben Cloud-Technologien, Application Programming Interfaces (APIs), Automatisierung (zum Beispiel in Operational Technology), Roboter, Big Data und maschinelles Lernen in den letzten Jahren neue Sicherheitslücken geschaffen.

Besonders der Einsatz von KI bringt neue Herausforderungen mit sich. Unternehmen müssen verhindern, dass die von ihnen genutzten Daten manipuliert, ihre Modelle gestohlen oder verfälscht werden und die erzeugten Inhalte unzuverlässig sind.

Gleichzeitig nutzen Cyberkriminelle KI, um Angriffe effizienter und schneller durchzuführen. Die Abwehrstrategien der Unternehmen und die Schulung der Mitarbeitenden müssen sich entsprechend weiterentwickeln, um mit dieser Dynamik Schritt zu halten.

Quanten resistente Kryptographie

Fortschritte bei Quantencomputern verändern ebenfalls das Bedrohungsszenario. Bis 2029 könnten sie gängige Datenverschlüsselungsverfahren unterlaufen und Internetnachrichten entschlüsseln und damit die digitale Wirtschaft gefährden. Um diesem noch immer unterschätzten Risiko zu begegnen, arbeiten Experten an Quanten resistenter Kryptografie.

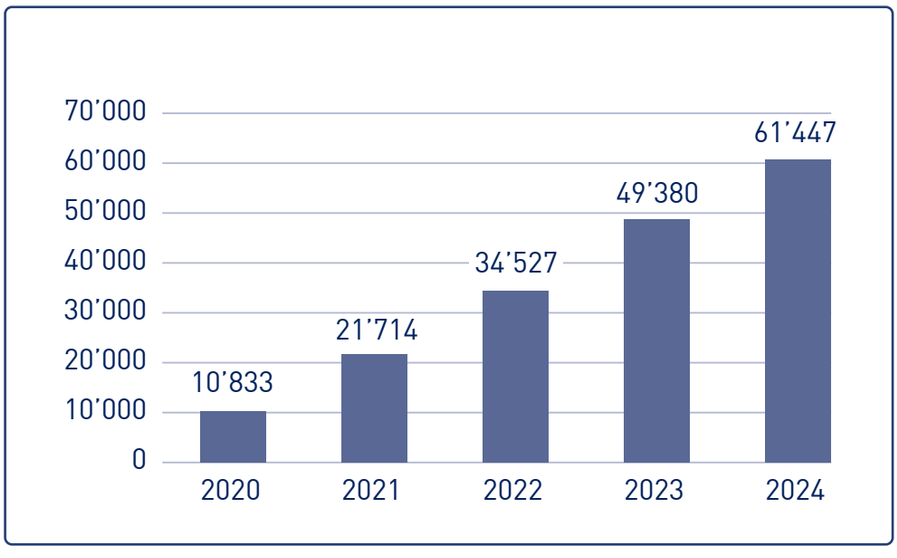
Unternehmen unterschätzen auch, dass der Austausch veralteter Systeme komplex ist und oft Jahre dauert. Die bestehenden Vorschriften verlangen bereits, dass anfällige Verschlüsselungstechnologien nachverfolgt und schnell ersetzt werden können, aber praktische Lösungen wurden gerade erst eingeführt und die meisten Unternehmen haben die Umsetzung noch nicht einmal geplant.

Etwa die neue Meldepflicht von Cyberangriffen ermöglicht eine schnellere Reaktion und eine gezieltere Datenerfassung. Doch müssen die Mitarbeitenden den Meldeprozess verstehen und aktiv nutzen. Dieser soll die Transparenz fördern, die Zusammenarbeit zwischen Unternehmen und Behörden stärken und bessere und schnellere Abwehrmechanismen schaffen und umsetzen.

Chris Girling,
Partner Cybersecurity and Privacy
bei PwC Schweiz

Girling unterstützt Unternehmen in allen Sektoren dabei, sicherer zu werden. Als ehemaliger Chief Information Security Officer (CISO) im Finanzdienstleistungssektor stand er im direkten Austausch mit Regulierungsbehörden zur Formulierung von Vorschriften im Bereich Cybersicherheit.

Starker Anstieg bei gemeldeten Vorgängen



Die Vorfälle, die dem Bundesamt für Cybersicherheit gemeldet werden, steigen. Nicht immer handelt es sich jedoch um erfolgreiche Cyberangriffe. Es befinden sich auch Meldungen zu Phishing-Versuchen darunter. Ausserdem besteht in der Schweiz keine generelle Meldepflicht. Daher kann die Dunkelziffer entsprechend höher sein.

[1] https://www.pwc.ch/de/insights/ceo-survey/2025.html
[2] https://www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2025.html

Die Risikoanalyse ist ein erster guter Schritt

Unternehmen behandeln datenschutzrechtliche Vorgaben oft stiefmütterlich. Datensicherheit ist aber unerlässlich, um Sicherheitsrisiken und mit ihnen Reputationsschäden und strafrechtliche Folgen zu vermeiden.

Von Tobias Schwaller

Unternehmen verfügen über eine Vielzahl von Informationen und Systemen, welche sie aus Eigeninteresse gerne schützen möchten. Zu denken ist dabei beispielsweise an internes Know-how und Geschäftsgeheimnisse. Darüber hinaus ist für Unternehmen der Zugang zu ihren Betriebssystemen und den darin enthaltenen Informationen an sich essenziell, um den Geschäftsbetrieb überhaupt aufrechterhalten zu können.

Datensicherheit aus datenschutzrechtlicher Sicht behandelt gemäss Datenschutzgesetz (DSG) hingegen ausschliesslich den Schutz von Personendaten (Art. 2 Abs. 1 DSG). Ziel des Datenschutzrechtes ist primär der Schutz der Persönlichkeit Dritter, auch wenn dieser Schutz durchaus im Interesse des Unternehmens selbst liegen kann. Der (datenschutzrechtliche) Begriff der Datensicherheit ist somit enger als der Begriff der Cybersecurity im Allgemeinen.

Risikobasierter Ansatz

Wer Personendaten bearbeitet, muss gemäss Art. 8 DSG durch geeignete «technische und organisatorische Massnahmen» (TOM) ein dem Risiko angemessenes Datensicherheits-Niveau sicherstellen. Je höher der Schutzbedarf der bearbeiteten Daten und je höher die mit der Bearbeitung verbundenen Risiken, desto strengere Anforderungen gelten bezüglich der Massnahmen, welche deren Sicherheit garantieren sollen.

So sind zum Beispiel an den Schutz von Gesundheitsdaten oder der in nahezu jedem Unternehmen vorhandenen Personaldossiers höhere Anforderungen zu stellen als an einen Newsletter-Verteiler. In der Praxis ist deshalb in einem ersten Schritt eine Risikoanalyse empfehlenswert, in deren Rahmen die unternehmensinternen Daten nach Sensibilität klassifiziert sowie die mit der Datenbearbeitung verbundenen Risiken eruiert werden.

Absolute Datensicherheit ist nicht zu erreichen.

Ein solches Inventar über die unternehmensintern bearbeiteten Personendaten zu erstellen, ist zwar mit einem gewissen Aufwand verbunden, hilft aber über die Thematik der Datensicherheit hinaus ungemein bei der Erfüllung verschiedenster datenschutzrechtlicher Pflichten wie der Informationspflicht oder der Gewährung von Betroffenenrechten.

Implementierung geeigneter Massnahmen

Abhängig vom Ergebnis der Risikoanalyse sind im Anschluss geeignete TOM zu implementieren. Diese haben vor unbefugtem Zugriff (Vertraulichkeit), vor Verlust (Verfügbarkeit) und unbefugter Veränderung (Integrität) zu schützen. Zudem soll eruiert werden können, wer die Daten bearbeitet (Nachvollziehbarkeit).

Zu berücksichtigen ist dabei stets der aktuelle Stand der Technik. Das bedeutet, dass eine fortlaufende Anpassung an die technische Entwicklung erforderlich ist. Gerade heute führt der rasante technische Fortschritt mit neuen

Technologien und immer stärkerer Rechenleistung zu neuen Bedrohungen (und Schutzmöglichkeiten), welche laufend miteinzubeziehen sind.

Der Gesetzgeber hat darauf verzichtet, konkrete Mindestanforderungen zu definieren, welche zwingend erfüllt sein müssen. Vielmehr ergibt sich aus dem risikobasierten Ansatz, dass im Einzelfall abzuwägen ist, welche konkreten Massnahmen ergriffen werden sollen. Grundlegende technische Massnahmen sind beispielsweise Firewalls, regelmässige Backups und Softwareaktualisierungen sowie die Zwei-Faktor-Authentifizierung. In organisatorischer Hinsicht unverzichtbar ist insbesondere die Sensibilisierung der Mitarbeitenden, welche mittels Schulungen und Richtlinien für den Umgang mit Daten erreicht werden kann.

Was ist im Ernstfall zu tun?

Absolute Datensicherheit ist nicht zu erreichen und wird vom Gesetzgeber auch nicht erwartet. Trotz angemessener TOM kann es zu Datensicherheitsverletzungen kommen. Ist dies der Fall, sieht Art. 24 DSG in gewissen Fällen Melde- und Informationspflichten vor. Unternehmen müssen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) Datensicherheitsverletzungen melden, wenn diese zu einem hohen Risiko für die Persönlichkeit der betroffenen Personen führen könnten. Der EDÖB stellt hierzu auf seiner Webseite ein Formular zur Verfügung.

Weiter müssen die betroffenen Personen selbst informiert werden, wenn es zu ihrem Schutz erforderlich ist. Dies ist primär dann der Fall, wenn sie selbst Massnahmen ergreifen können, um Schaden abzuwenden (etwa bei Passwortänderungen). Um im Ernstfall schnell und rechtskonform reagieren zu können, lohnt es sich, Prozesse und Zuständigkeiten für den Notfall im Vorfeld zu definieren.

Fehlende Datensicherheit kann teuer werden

Gemäss Art. 61 lit. c DSG werden private Personen mit Bussen bis zu 250'000 Franken bestraft, wenn sie vorsätzlich die Mindestanforderungen an die Datensicherheit nicht einhalten. Konkrete Mindestanforderungen werden aber weder im Gesetz noch in der Ausführungsverordnung definiert. Die Justiziabilität dieser Bestimmung wird deshalb mangels Bestimmtheit zurecht kritisch hinterfragt.[1] Seit der Einführung des neuen DSG vor knapp anderthalb Jahren sind – soweit ersichtlich – auch noch keine entsprechenden Verurteilungen erfolgt. Neben rechtlichen Konsequenzen drohen jedoch auch erhebliche Reputationsschäden und Vertrauensverluste, die oft genauso schwer wiegen wie ein allfälliges Strafbarkeitsrisiko.

Tobias Schwaller,
LEXTERNA AG in Basel

Schwaller arbeitet als Rechtsanwalt in Basel. Er berät vorwiegend KMU sowie Behörden und Institutionen in den Bereichen des Datenschutzrechts und des Immaterialgüterrechts.

[1] Vgl. GASSMANN, Kommentierung zu Art. 61 DSG, in: STEINER/MORAND/HÜRLIMANN (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 12.08.2023: https://onlinekommentar.ch/de/kommentare/dsg61 (besucht am 7. Februar 2025), N 17 m.w.H.

«Ein konstruktives Miteinander steht im Vordergrund»

Danielle Kaufmann ist seit letzten August die Datenschutzbeauftragte des Kantons Basel-Stadt. Sie besitzt zwar ein Weisungsrecht. Weder sie noch ihr Vorgänger mussten aber davon je Gebrauch machen. Ihre Empfehlungen stossen stets auf offene Ohren.

Interview: Kurt Tschan

Frau Kaufmann, als frühere Präsidentin der Justiz-, Sicherheits- und Sportkommission des Grossen Rats waren Sie in die Revision des Informations- und Datenschutzgesetzes auf kantonaler Ebene involviert. Hätten Sie ein anderes Gesetz vorgelegt, wenn Sie gewusst hätten, dass Sie eines Tages selbst Datenschutzbeauftragte werden?

Danielle Kaufmann: Nein. Bereits das alte Gesetz hatte sich bewährt und war mir als Datenschutzbeauftragte der Universität Basel bestens bekannt. Im neuen Gesetz brauchte es allerdings Ergänzungen, damit die Schweiz und auch der Kanton Basel-Stadt datenschutzkonform mit der Europäischen Union bleiben. Andere Paragrafen bedurften einer Präzisierung oder zum Teil auch der Anpassung an die gelebte Praxis.

War die anfängliche Aufregung überzogen? In der Schweiz reagieren bestimmte Kreise sensibel auf fremde Richter und Gesetze?

Es ging um neue Formulierungen, also auch um notwendige Anpassungen – zum Beispiel im Bereich der Datenschutzverletzungen. Das bisherige Recht wurde nicht neu nach europäischem Recht erschaffen, sondern es musste in gewissen Punkten angepasst werden. Jetzt ist es aus europäischer Sicht wieder auf gleichem Niveau.

Geben Sie uns ein Beispiel?

Im Vorfeld des Inkrafttretens des revidierten Informations- und Datenschutzgesetzes hat die Verschärfung der Informationspflicht zu Unsicherheit geführt. Betroffene Personen müssen neu immer transparent informiert werden, wenn von ihnen Daten erhoben und bearbeitet werden. Das Transparenz-Gebot ist wichtig, weil Betroffene sonst gar nicht wissen können, dass Daten von ihnen gesammelt werden. Die Verschärfung sorgte für Verunsicherung, da nicht klar war, wie im konkreten Fall, zum Beispiel an einem Schalter eines Amtes vorzugehen ist. Wir bieten hier gerne Unterstützung, um praktikable Lösungen zu finden und wir werden auch einen entsprechenden Leitfaden ausarbeiten.

> «Der Umgang mit Daten vollzieht sich in den meisten Fällen verantwortungsvoll.»

Gab es auch andere Aufreger?

Eine wichtige Neuerung ist die Verpflichtung zu einer Datenschutz-Folgeabschätzung. Diese greift dann, wenn für betroffene Personen bei der Datenbearbeitung ein besonders hohes Risiko für ihre Grundrechte besteht. Auch dafür haben wir Anleitungen und Merkblätter erstellt. Sie sehen also, dass wir die öffentlichen Organe, unsere Ansprechpartnerinnen und -partner bestmöglich begleiten und unterstützen. Ich bin zuversichtlich, dass sich die Neuerungen in den nächsten Monaten einpendeln werden.

Sind die Personendaten jetzt besser geschützt?

Eine gute Frage! Erst kürzlich wurden mehrere «Klinik-Informationssysteme» in Schweizer Spitälern auf ihre Sicherheit überprüft. Und es hat sich gezeigt, dass die darauf gespeicherten Daten von Patientinnen und Patienten nicht ausreichend sicher waren. Grundsätzlich gehe ich davon aus, dass sich alle Mühe geben, den Datenschutz und die

Informationssicherheit bestmöglich zu gewährleisten. Allerdings verläuft die technologische Entwicklung derart rasant, dass wir grosse Schwierigkeiten haben ihr zu folgen. Und ich erlebe auch oft eine – aus meiner Sicht zu unkritische Haltung gegenüber den Anbietern von Informationstechnologie. Zudem werden zunehmend unsere Daten in Clouds verschoben, die sich meistens im Ausland befinden. Hier frage ich mich tatsächlich, ob die Datenbearbeitenden die Kontrolle ausreichend wahrnehmen können und sich dieser Schwierigkeit auch bewusst sind.

Welche personellen und technischen Ressourcen stehen Ihnen zur Verfügung?
Mein Team besteht aus vier Juristinnen und Juristen, sowie aus drei Mitarbeitenden in der Informatik. Um datenschutzrechtliche Abklärungen und Kontrollen zu machen, bedarf es sowohl der juristischen wie auch der technischen Expertise.

Was passiert, wenn eine Datenbearbeitung nicht gesetzeskonform erfolgt? Fahren Sie dann mit der Polizei auf?
Nein, so ist es nicht. Allerdings kann ich den öffentlichen Organen für das Bearbeiten von Personendaten Empfehlungen aussprechen und sollte dies nicht ausreichen, kann ich auch Weisungen erlassen. Meines Wissens haben bisher die Empfehlungen ausgereicht, weder mein Vorgänger noch ich mussten je eine Weisung aussprechen. Auf unsere Empfehlungen wird eingegangen, sodass wir jeweils eine Lösung für das Problem finden. Ein konstruktives Miteinander steht im Vordergrund.

Wie gut steht es um den Datenschutz im Kanton Basel-Stadt?
Noch gibt es sicherlich einige Baustellen, da jedes einzelne Tool, jede Datenbearbeitung richtig gemanagt werden muss. Nach neuem Gesetz müssen die öffentlichen Organe nachweisen können, dass sie jedes Tool mit welchem Personendaten bearbeitet werden, datenschutzkonform betreiben. Konkret heisst das, dass zum Beispiel die Risiken für die Grundrechte der betroffenen Personen und die entsprechenden Schutzvorkehrungen beschrieben werden müssen. Oder auch müssen Rollen- und Berechtigungssysteme korrekt eingeführt sein, es braucht Löschkonzepte und so weiter. Verlässt jemand zum Beispiel seine Arbeitsstelle, muss diese Person etwa aus dem System gelöscht werden. Hinter der datenschutzrechtlich korrekten Verwendung von Tools steckt also viel Arbeit.

Ohne Daten könnte die kantonale Verwaltung gar nicht arbeiten. Wie verantwortungsvoll gehen die Behörden mit ihnen um?
Der Umgang mit Daten vollzieht sich in den meisten Fällen verantwortungsvoll. Hätte ich dieses Gefühl nicht, könnte ich meinen Job nicht machen. Aber klar, es gibt auch bewusstes oder wohl vor allem unbewusstes risikobehaftetes Bearbeiten von Personendaten, da schauen wir dann auch genau hin. Welches die heiklen Daten sind, wissen die Mitarbeitenden der Verwaltung aber in der Regel.

Von welchen Daten sprechen Sie konkret
Diese sensitiven Daten oder besonderen Personendaten sind vom Gesetzgeber beispielhaft genannt. Es geht etwa um Informationen, die die gewerkschaftliche Tätigkeit einer Person, ihre politische Haltung, aber auch ihre Gesundheit, eine allfällige Abhängigkeit von der Sozialhilfe, oder auch ihre Ethnie betreffen. Auch die Kombination von Daten kann heikel sein. Daten lassen sich nicht gegeneinander ausspielen. Deshalb können Daten aus der Schule ebenso heikel sein wie jene in der Steuerverwaltung.

Was ist Ihnen im gesellschaftlichen Diskurs um Daten besonders wichtig?
Heikle unverschlüsselte Personendaten gehören nicht in öffentliche Clouds, die sich im Ausland befinden. So verliert man die Kontrolle. Diese Auffassung vertreten auch die anderen Datenschutzbehörden der Schweiz. Was ich auch einen sehr interessanten Ansatz finde, ist das Konzept der digitalen Souveränität. Der Kanton Genf hat diese als Grundrecht bereits in seiner Verfassung aufgenommen. Gerade in der jetzigen geopolitischen Lage sollten wir überlegt mit unseren Daten umgehen, die Kontrolle darüber behalten und uns nicht in eine völlige Abhängigkeit von den grossen Techfirmen begeben.

Würden Sie auch ein Basler Gesetz zur digitalen Souveränität befürworten?
Ja, ich finde das ist ein sehr interessanter Ansatz. Aber zuvor braucht es eine vertiefte Daten-Diskussion.

Danielle Kaufmann,
Datenschutzbeauftrage Kanton Basel-Stadt

Kaufmann ist seit August 2024 Datenschutzbeauftragte des Kantons Basel-Stadt. Zuvor arbeitete sie als Datenschutzbeauftragte der Universität Basel, wo sie auch Mitglied der Ethikkommission war. Von 2013 bis 2022 war sie Mitglied des Grossen Rates Basel-Stadt. Von 2020 bis 2022 leitete sie die Justiz-, Sicherheits- und Sportkommission.

Nur jedes vierte Delikt wird aufgeklärt

Die Opfer von Cyberkriminalität bekommen ihr Geld oder ihre gestohlen Daten in den meisten Fällen nicht zurück.

Von Alexander Schwab

Cyberkriminalität umfasst eine Vielzahl von Straftaten, die unter Ausnutzung von Informations- und Kommunikationstechnologien begangen werden oder sich gegen solche richten. In der Regel wollen Täter entweder an Geld kommen oder Opfer einschüchtern.

Die wichtigsten Straftatbestände im Schweizer Strafgesetzbuch zur Cyberkriminalität sind etwa die unbefugte Datenbeschaffung, das unbefugte Eindringen in ein Datenverarbeitungssystem (Hacking), der betrügerische Missbrauch einer Datenverarbeitungsanlage sowie der Check- und Kreditkartenmissbrauch.

Neben diesen spezifischen Delikten können aber regelmässig auch weitere Straftatbestände wie Betrug (zum Beispiel Phishing), Erpressung, Identitätsmissbrauch, Drohung etc., erfüllt sein.

Cyberkriminalität stellt die Strafverfolgungsbehörden vor grosse Herausforderungen. Im Jahr 2023 lag die Aufklärungsrate für Cyberkriminalität in der Schweiz bei nur 23,3 Prozent. Diese niedrige Aufklärungsrate ist insbesondere auf die Anonymität im Internet sowie die Tatsache zurückzuführen, dass sich die Täterschaft oftmals im Ausland aufhält.

Präventive Massnahmen erforderlich

Da die Wahrscheinlichkeit, die Täterschaft zu fassen, relativ klein ist, sind auch die Chancen der Geschädigten gering, dass sie wie bei Betrugs- oder Kreditkartenmissbrauchs ihr Geld zurückerhalten.

Vor diesem Hintergrund ist es umso wichtiger, durch präventive Massnahmen und Sensibilisierung der Bevölkerung potenzielle Opfer zu schützen und die Gesellschaft widerstandsfähiger gegenüber digitalen Bedrohungen zu machen.

FOTOS/GRAFIKEN Seite 3: Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS Bundesamt für Cybersicherheit BACS; Seite 7: Dominik Plüss; Seite 8: Handelskammer beider Basel.

IMPRESSUM
TRIBUNE erscheint viermal jährlich **HERAUSGEBER** Handelskammer beider Basel (info@hkbb.ch), Advokatenkammer Basel, Basellandschaftlicher Anwaltsverband (maier@svwam.ch), grosszügig unterstützt von der Jubiläumsstiftung La Roche & Co; St. Jakobs-Strasse 25, Postfach, 4010 Basel, Telefon: +41 61 270 60 55, E-mail: info@hkbb.ch **REDAKTION**: Roman Felix, Jasmin Fürstenberger, Alexander Schwab, Kurt Tschan **LAYOUT** Elmar Wozilka, Handelskammer beider Basel, **DRUCK** Druckerei Dietrich, Basel gedruckt in der Schweiz.
«tribune» ist eine offizielle Publikation der herausgebenden Organisationen für deren Mitglieder. Der Abonnementspreis ist im Mitgliederbeitrag inbegriffen. Für Nichtmitglieder kostet das Jahresabonnement CHF 20.–.