Newsletter Datenschutz

Ausgabe 06 | 2022

Ziele der Cyberkriminellen: Ihre Daten!

Ihr Datenschutz-Info-Blatt

Liebe Leserin, lieber Leser,

wenn personenbezogene Daten übermittelt werden, müssen sie angemessen geschützt sein. Welche konkreten Folgen dieser einfache Grundsatz hat, zeigt diese neue Ausgabe Ihres Datenschutz-Info-Blatts.
So können personenbezogene Daten Teil einer Veröffentlichung im Internet sein. Hier müssen sie zum Beispiel gegen Verfälschung geschützt werden. Welche Auswirkungen eine Falschmeldung haben kann, zeigt Ihnen der erste Beitrag dieser Ausgabe. Personenbezogene Daten landen aber auch bei Cloud-Diensten, die sich oftmals in den USA befinden. Der zweite Beitrag erklärt, wie es dort um den angemessenen Datenschutz steht.
Aber auch das altbekannte Fax kann personenbezogene Daten enthalten. Erfahren Sie, was hier zu beachten ist. Den Abschluss dieser Ausgabe bildet ein Beitrag über die Gefahren für Daten im Internet durch Cyberkriminalität.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihr Frank Berns, Datenschutzbeauftragter

Darum sind Misinformation und Desinformation auch ein Datenrisiko

Das Netz ist voll von Falschinformationen. Manches ist schlecht recherchiert, anderes wird mit Absicht falsch dargestellt. Das ist nicht nur ärgerlich, sondern ein echtes Datenrisiko. Für die EU-Agentur für Cybersicherheit ENISA sogar eines der größten.

Das Ziel: Daten speichern, austauschen und sichern

Gerade im Internet gibt es viele „Sensationsmeldungen“. Sie sollen die Leserinnen und Leser dazu bewegen, die Nachricht und die eingebundene Werbung anzuklicken. Doch so manche Meldung ist nicht „nur“ übertrieben dargestellt, sie ist schlicht falsch.

Das kann bei den Medien passieren, wenn sie nicht sauber recherchieren. Das ist aber auch in den sozialen Netzwerken zu finden, wenn jemand etwas falsch verstanden hat und das dann als Wahrheit darstellt.

Doch nicht alles ist ein Versehen oder Schlamperei. Viele Falschdarstellungen im Netz werden mit voller Absicht veröffentlicht. Man unterscheidet hier zwischen:

- Desinformation als gezielter Verbreitung von falschen Informationen und
- Misinformation, die jemand ohne die Absicht, zu manipulieren, veröffentlicht.

KONTAKT zu uns MAIL@Konzept17.de

Desinformation erfolgt inzwischen über alle Kanäle

Wie der Digitalverband Bitkom berichtet, nehmen Verbraucher über alle Medien hinweg offensichtlich falsche Nachrichten oder Berichte wahr. Neun von zehn Social-Media-Nutzern (92 Prozent) ist dies in sozialen Netzwerken aufgefallen. Dabei war jeder Dritte (33 Prozent) häufig mit bewussten Falschinformationen konfrontiert. In klassischen Medien wurden Falschnachrichten etwas seltener beobachtet (79 Prozent aller Verbraucher insgesamt, 21 Prozent häufig). Über Messenger wie WhatsApp oder Tele-gram hat jeder zweite Messenger-Nutzer (53 Prozent) im Vorjahr Falschinformationen erhalten.

Verbreitet jemand über eine Person öffentlich falsche Informationen, ist die Privatsphäre der Person betroffen. Denn personenbezogene Daten müssen auch korrekt sein. Es gilt der Grundsatz der Richtigkeit nach der Datenschutz-Grundverordnung (DSGVO). Doch auch der Empfänger und die Empfängerin der Falschinformation kann Datenrisiken ausgesetzt sein.

Falschinformationen sind Angriffe oder bereiten Attacken vor

Tatsächlich erklärt die EU-Agentur für Cybersicherheit ENISA, dass Desinformation zu den größten Risiken gehört, und auch Misinformation kann Schaden anrichten.

Desinformations- und Fehlinformationskampagnen sind in der Cyberwelt von größter Bedeutung, so ENISA. Cyberkriminelle setzen Desinformation und Fehlinformation häufig bei hybriden Angriffen ein, um Zweifel zu schüren oder Verwirrung zu stiften.

Das führt bei den Empfängerinnen und Empfängern der falschen Nachrichten zu Fehlern und mangeln-der Vorsicht, also zum Beispiel dazu, eine schädliche Software zu installieren, die angeblich hilfreich sein soll.

Privacy Shield II – noch ist Geduld angesagt!

Das „Privacy Shield" war als Rechtsgrundlage für Datenübermittlungen in die USA sehr beliebt. Der Europäische Gerichtshof hat ihn im Juli 2020 für unwirksam erklärt. Eine verbesserte Neufassung soll möglichst bald kommen. Vor Ende des Jahres 2022 sollte man darauf aber lieber nicht hoffen.

Eine Grundsatzeinigung ist gelungen

Die EU und die USA haben eine grundsätzliche Einigung darüber erzielt, wie ein neues Privacy-Shield-Modell aussehen soll. Es soll die rechtlichen Schwächen beheben, an denen der ursprüngliche Privacy Shield beim Europäischen Gerichtshof gescheitert ist. Das haben US-Präsident Biden und die Präsidentin der EU-Kommission, Frau von der Leyen, am 25. März 2022 persönlich gemeinsam verkündet.

EU-Bürger erhalten Rechtsschutz gegen US-Geheimdienste

Wesentliches Kernstück des neuen Modells soll eine Verbesserung des Rechtsschutzes für EU-Bürger gegenüber US-Geheimdiensten sein. Präziser gesagt geht es darum, einen solchen Rechtsschutz erstmals einzuführen. Bisher können sich EU-Bürger gegen Zugriffe auf ihre persönlichen Daten durch US-Geheimdienste nämlich im Normalfall überhaupt nicht gerichtlich wehren.

Dafür ist sogar ein neues Gericht vorgesehen

Das soll sich künftig ändern. Dazu soll in den USA ein neues Gericht auf Bundesebene entstehen, bei dem EU-Bürger Rechtsschutz gegen die US-Geheimdienste beantragen können. Es soll „Data Protection Review Court" heißen. Zu den Einzelheiten halten sich die Beteiligten noch bedeckt. Sie sollen in den nächsten Monaten ausgearbeitet werden.

Was das genau heißt, bleibt abzuwarten

Wie so oft steckt auch hier der Teufel im Detail. Selbstverständlich werden die Geheimdienste dem Gericht ihre Tätigkeit nur begrenzt darlegen müssen. Und selbstverständlich werden Betroffene nicht alles erfahren können, was sie gern wüssten. Der Rechtsschutz, den dieses Gericht gewährt, wird den in Europa üblichen Rechtsschutz mit Sicherheit nicht eins zu eins kopieren. Aber es wird – anders als bisher – überhaupt Rechtsschutz für EU-Bürger geben.

Die nationale Sicherheit der USA wird wichtig bleiben

Gespannt darf man auf die Maßstäbe sein, nach denen das Gericht entscheiden soll. Bisher heißt es nur allgemein, es solle darüber entscheiden können, ob bestimmte Eingriffe „geeignet und verhältnismäßig" sind. Diese Formulierung knüpft an Begriffe an, die der Europäische Gerichtshof verwendet. Er hat sinngemäß kritisiert, dass nach dem Recht der USA persönliche Belange einzelner Betroffener zu pauschal gegenüber den Bedürfnissen der nationalen Sicherheit zurückstehen müssen.

Vorgesehen ist eine Adäquanzentscheidung der EU

Die Änderungen im US-Recht sollen den Weg dafür frei machen, dass die Europäische Kommission die Gleichwertigkeit des Datenschutzes in den USA und des Datenschutzes in der EU feststellen kann. Das soll in einer förmlichen „Adäquanzentscheidung" geschehen. Schon die dafür notwendigen Verfahrensabläufe in den EU-Institutionen werden mehrere Monate in Anspruch nehmen.

Es wird wieder ein Registrierungsverfahren geben

Allerdings können sich Unternehmen nicht „einfach so" auf die künftige Adäquanzentscheidung berufen. Wie schon beim ursprünglichen Privacy Shield müssen sie sich dazu förmlich registrieren lassen. Dabei müssen sie sich verpflichten, die Vorgaben des Privacy Shield zu beachten. Eine Registrierung ist nur für US-Unternehmen möglich. Registrieren lassen müssen sich also die Geschäftspartner von Unternehmen in der EU, nicht dagegen die Unternehmen in der EU selbst. Aber auch das war schon früher so.

Ist das Glas nun halb voll oder halb leer?

Ein Sprichwort sagt, dass Optimisten und Pessimisten ein- und dasselbe Glas als halb voll bzw. halb leer ansehen. Dies beschreibt die derzeitige Situation rund um den „Privacy Shield II", wie es manche inoffiziell schon nennen, wohl recht gut:

- Halb leer ist das Glas deshalb, weil die politische Grundsatzeinigung im Augenblick für Datenübermittlungen in die USA noch keine praktischen Auswirkungen hat. Dies wird erst der Fall sein, wenn die Grundsatzeinigung rechtlich umgesetzt ist.
- Andererseits kann man das Glas mit Fug und Recht als halb voll ansehen. Denn dass es überhaupt zu einer politischen Einigung gekommen ist, hat viele überrascht.

Der Weg zum Europäischen Gerichtshof wird sicher wieder beschritten

Wenn die neue Regelung irgendwann gilt, wird sie sehr schnell Gegenstand eines Verfahrens vor dem Europäischen Gerichtshof sein. Dies sehen alle Beobachter so. Man darf gespannt sein, wie der Gerichtshof dann entscheiden wird. Doch zunächst einmal gilt es, den detaillierten Inhalt des verbesserten Privacy Shield abzuwarten.

Datenschutz beim Telefax

Manche Unternehmen würden das Telefax am liebsten endlich abschaffen. Aber einige wichtige Kundinnen und Kunden scheinen es regelrecht zu lieben. Deshalb bleibt das Telefax einstweilen doch noch. Das bedeutet allerdings, dass man sich auch um den Datenschutz kümmern muss.

Das Telefax hat ein zähes Leben

In manchen Unternehmen ist das Telefax schon länger verschwunden, oft gehört es aber durchaus noch zum Alltag. Dann bildet es eine echte Gefahrenquelle für den Datenschutz. Aus diesem Grund hat der Bayerische Landesbeauftragte für den Datenschutz die Risiken aufgegriffen, die beim Telefax bestehen. Ein zwölfseitiges Papier listet alles auf, was zu beachten ist. Es steht zur Verfügung unter https://www.datenschutz-bayern.de/datenschutzreform2018/AP_Telefax.pdf .

Fehlversendungen sind ein Hauptproblem

Im Mittelpunkt steht das Problem, dass es immer wieder zu Fehlversendungen kommt. Dies zeigt die Auswertung der zahlreichen Meldungen von Datenpannen, die sich damit befassen. Die Ursachen von Fehlversendungen sind oft erschreckend banal. Als typische Beispiele nennt das Papier:

- Eingabe einer falschen Rufnummer, etwa durch Vertippen oder durch die Nutzung einer längst veralteten Rufnummer
- Fehler bei der notwendigen Eingabe einer zusätzlichen Vorwahl vor externen Rufnummern (etwa das Weglassen der „0“, die bei vielen Nebenstellenanlagen vor einer externen Rufnummer gewählt werden muss)
- irrtümliche Versendung eines Schreibens, das für einen ganz anderen Empfänger bestimmt ist

Faxgeräte sind „Praktikanten-Fallen“

Das Risiko von Fehlversendungen multipliziert sich, wenn eine Praktikantin oder ein Praktikant ein Fax verschicken soll. Häufig haben sie ein solches Gerät vorher noch nie gesehen, scheuen sich aber, dies zu sagen. Sogar die Kombination mehrerer Fehler ist dann schnell passiert. Ohne vorherige ausführliche Anleitung sollte man deshalb den Nachwuchs besser gar nicht an ein Faxgerät lassen.

Der Standort des Geräts muss passen

Oft steht das Faxgerät irgendwo, wo gerade noch Platz war. Das gilt vor allem dann, wenn es kaum noch verwendet wird und deshalb irgendwann buchstäblich „an den Rand gerückt" ist. Das kann erhebliche Probleme nach sich ziehen, wenn eine eingehende Sendung versehentlich oder absichtlich irgendwohin „verschwindet".

Dokumentation ist Pflicht

Spätestens dann wird klar, dass die Rechenschaftspflicht von Art. 5 Abs. 2 DSGVO auch für den Datenschutz beim Telefax gilt. Diese Rechenschaftspflicht zwingt dazu, die Einhaltung des Datenschutzes stets nachweisen zu können. Es ist deshalb notwendig, dass der Standort jedes einzelnen Faxgeräts nachvollziehbar dokumentiert ist. Diese Dokumentation muss auch Angaben dazu enthalten, wie unbefugte Zugriffe verhindert werden sollen. „Unbefugter Zugriff auf ein ausgedrucktes Fax" ist ein eigenes Risikoszenario. Mit ihm sollte man sich befassen, bevor es Realität geworden ist.

Klare Vorgaben vermeiden Pannen

Eine Dienstanweisung (so die Bezeichnung im Behördendeutsch) für die Aufstellung und Nutzung von Faxgeräten ist kein Luxus, sondern Notwendigkeit. Sie ist in der Praxis zwar oft vorhanden, nicht selten allerdings in einer Uralt-Version von vor 20 Jahren. Wenn dann ein Teil der Geräte gar nicht mehr existiert und die noch vorhandenen Geräte inzwischen an ganz anderen Stellen stehen, genügt die Anweisung den Anforderungen nicht mehr.

Kommunikationsjournale müssen sein

Kommunikationsjournale ermöglichen es, Fehlversendungen nachgehen zu können. Fehlen sie, ist es im Ernstfall kaum möglich, einen falschen Adressaten zu kontaktieren. Zu empfehlen ist die Aufbewahrung solcher Journale für etwa zwei Wochen. Ihre Vernichtung muss in der Dienstanweisung geregelt sein.

Sensible Daten erfordern eine Risikoanalyse

Sehr kritisch ist der Versand von Faxen mit sensiblen Inhalten zu sehen. Er findet erstaunlich oft statt, etwa im Zusammenhang mit Personaldaten. In Arztpraxen ist sogar die Übermittlung von Krankheitsdaten per Telefax nach wie vor häufig. Dies ist zwar nicht generell verboten. Notwendig ist allerdings eine Risikoanalyse dafür, ob die Übermittlung sensibler Inhalte vertretbar ist. Sollte die Risikoanalyse negativ ausgehen, müsste die Übermittlung sensibler Inhalte per Telefax untersagt werden.

Bessere Alternativen sind vorhanden

Wem der Aufwand rund um den Datenschutz beim Telefax zu groß ist, der sollte nach besser geeigneten Techniken Ausschau halten. Hierzu gehören etwa Mails, die Ende-zu-Ende-verschlüsselt sind, oder die Nutzung einer sicheren Cloud-Ablage.

Das sind die Ziele der Cyberkriminellen: Ihre Daten!

Cyberkriminalität nimmt immer bedrohlichere Ausmaße an. Acht von zehn Personen waren in den vergangenen zwölf Monaten von kriminellen Vorfällen im Netz betroffen, so der Digitalverband Bitkom. Wer sich besser schützen will, muss die Ziele der Internetkriminellen kennen.

Das Internet wird immer häufiger zu Tatmittel und Tatort

Die Polizeiliche Kriminalstatistik 2021, im April 2022 veröffentlicht, zeigt deutlich: Ein Bereich, bei dem seit Jahren kontinuierlich Anstiege zu verzeichnen sind, ist die Cyberkriminalität. Hier wurden im vergangenen Jahr 146.363 Fälle erfasst. Das ist eine Zunahme um 12,1 Prozent, wie das Bundeskriminalamt (BKA) mitteilte.

Die Cyberkriminalität betrifft Privatpersonen ebenso wie Unternehmen. In den letzten 12 Monaten hatten 32 Prozent der Unternehmen Schäden durch IT-Sicherheitsvorfälle, wie die eco IT-Sicherheitsumfrage 2022 ergab. Kommt es zu einem IT-Sicherheitsvorfall, dann ist wie in den Vorjahren das Unternehmen meist Opfer einer Ransomware-Attacke (21 Prozent). Erpressungstrojaner sind bei Cyberkriminellen hoch im Kurs. Auf Platz zwei liegt Website-Hacking mit 18 Prozent.

Cyberangriffe sind meistens finanziell motiviert

Während man früher davon ausging, dass viele Online-Attacken deshalb stattfinden, weil die Angreifenden ihr Hacking-Können ausprobieren und zeigen wollen, ist man sich seit einigen Jahren sicher, dass die Motive hinter den Attacken meistens finanzieller Natur sind: Man will Kontobestände räumen, Kryptowährungen stehlen oder führt gegen Bezahlung eine kriminelle Auftragsarbeit aus, einen Spionage-Auftrag oder einen Angriff auf den Wettbewerber des „Kunden“.

Auch wenn es letztlich meistens um Geld geht, sind die Ziele der Internetkriminellen zuerst und insbesondere Daten. Denn Daten sind wertvoll und können etwa Zugang zu Bankkonten verschaffen. Erfolgreiche Cyberangriffe bedeuten deshalb auch, dass der Datenschutz leider nicht ausgereicht hat.

Datenschützer warnen vor Internetkriminalität

„Mangelhafte Datensicherheit offenbart meist auch Schwächen beim Datenschutz“, so der damalige Sächsische Datenschutzbeauftragte Andreas Schurig. „Das ist nicht nur für die betroffenen Unternehmen existenzbedrohend, sondern auch für Menschen, deren Daten in den Besitz von Kriminellen gelangen. Identitätsdiebstahl gehört dabei zu den schlimmsten Folgen. Betroffenen droht ein finanzieller und sozialer Totalschaden“, warnt der Datenschützer.

In Zeiten der fortschreitenden Digitalisierung und der um sich greifenden Cyberkriminalität wird damit der Schutz personenbezogener Daten noch wichtiger. Das spüren auch die Internetnutzerinnen und -nutzer: In den vergangenen zwölf Monaten ist die Angst vor Cyberkriminalität deutlich gestiegen. Aktuell fürchten sich laut Digitalverband Bitkom

- 85 Prozent vor einer illegalen Nutzung persönlicher Daten durch Unternehmen (2020: 79 Prozent) und
- 83 Prozent vor Schadprogrammen (2020: 75 Prozent).
- Eine illegale Nutzung von Passwörtern und Konten befürchten 62 Prozent der Internet-Nutzerinnen und -Nutzer.

Furcht vor Cyberattacken allein schützt nicht

Zweifellos ist es gut, wenn man bei der Nutzung des Internets nicht sorglos ist und sich Gedanken macht, was passieren könnte. Allerdings sollte man sich ganz deutlich machen, auf was es die Internetkriminellen abgesehen haben: auf die personenbezogenen Daten.

Datenschutz ist deshalb auch ein zentraler Schutz vor Internetkriminalität und wird mit der digitalen Transformation nicht etwa zum Hindernis. Datenschutz ist im Gegenteil zwingend erforderlich, um den Cyberkriminellen so viel Gegenwehr wie nur möglich zu bieten.

Wissen Sie, was Cyberkriminelle wollen? Machen Sie den Test!

Frage: Internetkriminelle interessiert das Geld und nicht die Daten. Die Daten will nur die Werbewirt-schaft. Stimmt das?

1. Nein, die Cyberkriminellen haben finanzielle Motive, aber um an Geld zu kommen, missbrauchen und verkaufen sie Daten.
2. Ja, Datenschutz hat nichts mit dem Schutz vor Cyberkriminalität zu tun

Lösung: Die Antwort 1. ist richtig. Das Hauptziel jeder Cyberattacke sind Daten, und die meisten dieser Daten haben Personenbezug. In 63 Prozent der Unternehmen, in denen zuletzt sensible digitale Daten gestohlen wurden, handelte es sich laut Bitkom um Kommunikationsdaten. Diese Daten aber enthalten in aller Regel personenbezogene Informationen

Frage: Gegen Internetkriminelle sind wir machtlos. Das Internet ist eben gefährlich. Ist das so richtig?

1. Ja, gegen Cyberattacken kann man letztlich nichts machen.
2. Nein, wenn man die Daten schützt, kann es zwar zu Cyberangriffen kommen, aber die Angreifenden können keine Daten erbeuten.

Lösung: Die Antwort 2. ist richtig. Es gibt zwar keinen hundertprozentigen Schutz vor Internetkriminellen, man muss davon ausgehen, dass es zu erfolgreichen Cyberangriffen kommt. Doch das Ziel der Angriffe, die Daten, kann man weitaus besser schützen, als dies heute noch geschieht. Sind die Daten zum Beispiel stark verschlüsselt, kann ein Internetkrimineller sie zwar stehlen, aber nichts damit anfangen.

Impressum

Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de