Mangelnder Datenschutz bei Kundenportalen

Unbefugte Zugriffe

Andreas Wiegenstein

Nahezu jeder Dienstleister stellt heutzutage ein Onlineportal bereit, über das Kunden Informationen abrufen und Dinge erledigen können. Was man dabei alles falsch machen kann, zeigen die Portale vieler Energieversorger.

Jeder deutsche Bürger, der ein Haus oder eine Wohnung besitzt, hat Verträge mit dem örtlichen Stromanbieter, dem Wasserwerk, der Müllabfuhr und einem Energieversorger. Einige dieser Verträge kann man auch als Mieter abschließen. Die meisten dieser Vertragspartner bieten ein Onlineportal an, mit dem Kunden zum Beispiel ihre Stammdaten pflegen, Zählerstände eingeben und Rechnungen abrufen können. Den Zugang zu diesen Portalen können sie sich bei Bedarf selbst freischalten (siehe Abbildung).

Oft ist den Kunden nicht bewusst, dass ihre Daten online verfügbar sind. So kann es sein, dass ihnen ein Schreiben ins Haus flattert, das erklärt, dass ihre Kundendaten im Portal hinterlegt sind und darauf warten, aktiviert zu werden. Aber unabhängig davon, ob Kunden das dann tun oder lassen – ihre Daten stehen im Internet. Natürlich nicht frei zugänglich. Zur Freischaltung der personenbezogenen Daten in einem Onlineportal muss ein Kunde sich authentifizieren. Das heißt, er muss dem System Informationen liefern, die ihn als rechtmäßigen Besitzer eines Kundenkontos identifizieren.

Aus Sicherheitsgründen muss eine solche Authentifizierung so programmiert sein, dass ein Dritter keinen Zugriff auf das Konto erlangen kann. Doch was steht auf dem Spiel, wenn ein Unbefugter das Onlinekonto eines Kunden freischalten kann? Und wie schwierig ist so ein unerlaubter Zugriff in der Praxis?

Um diesen Fragen auf den Grund zu gehen, haben der Verfasser dieses Artikels und die beteiligten Sicherheitsforscher sowohl die Art als auch die Qualität der Schutzmechanismen von 240 deutschen Energieversorgern untersucht. Diese Schutzmechanismen stellen die einzige Verteidigungslinie zwischen Cyberangriffen und vielen Millionen Datensätzen deutscher Bürger dar. Deutschland hat schon jetzt eines der schärfsten Datenschutzgesetze, ab Mai 2018 gilt überdies die europäische Datenschutz-Grundverordnung. In diesem Kontext erscheint es zumindest verwunderlich, dass Unternehmen personenbezogene Daten ihrer Kunden ohne expliziten Auftrag online stellen.

Unnötige Risiken für heikle Daten

Selbst wenn man annimmt, dass die Verfahren zur Freischaltung der Kundendaten aus Sicherheitssicht dem Stand der Technik entsprechen, erhöht sich dennoch das Risiko, dass die Daten in falsche Hände geraten. Denn sie stehen im Netz. Im Fachjargon spricht man davon, dass die Angriffsoberfläche auf die Daten steigt.

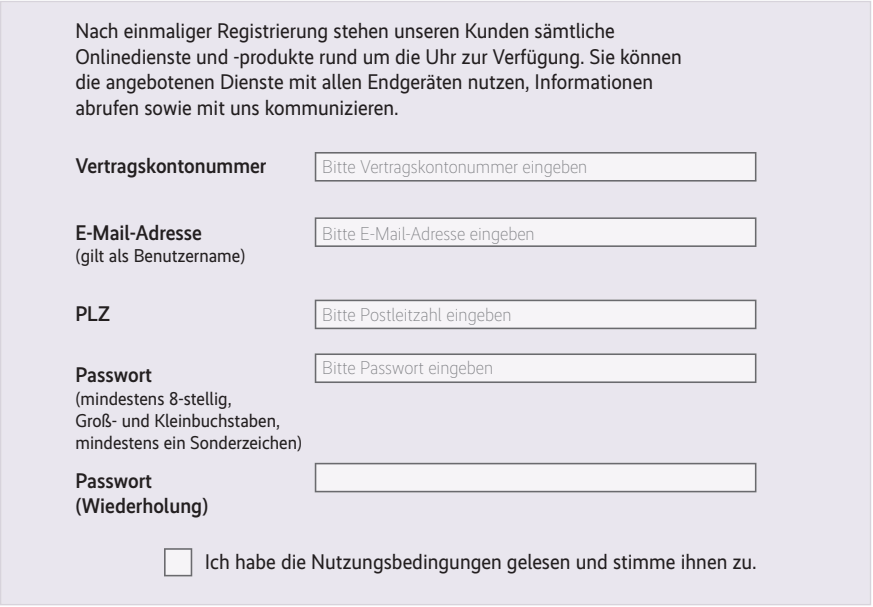
Insbesondere ist fraglich, wie viele Kunden die Funktionen dieser Portale überhaupt verwenden wollen. Für jeden, der das nicht beabsichtigt, besteht ein täglich wachsendes und völlig unnötiges Risiko, dass Dritte sich unbefugt Zugriff auf seine Daten verschaffen. Der Kasten „Daten, die in Kundenportalen hinterlegt sind“ liefert eine Übersicht, was typischerweise in Onlineportalen gespeichert ist.

Diese Daten reichen einem Angreifer bereits für einen Identitätsdiebstahl. Durch sogenanntes Social Engineering könnte sich ein Dieb bei anderen Stellen (beispielsweise Krankenkasse, Bank, Ar-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

beitgeber und Behörden) für die bestohlene Person ausgeben, in ihrem Namen Aufträge und Geschäfte tätigen oder sonstige Anweisungen geben. Selbstverständlich kann man die meisten Daten auch online ändern. Denn das ist ja der Zweck dieser Portale. Dadurch ergeben sich unter anderem weitere Risiken:
– Abmelden des Kunden (zum Beispiel durch fingierten Umzug), was unter Umständen dazu führen kann, dass die Leistung (Strom, Gas, Wasser, Müllabfuhr) eingestellt wird;
– Eingabe zu hoher Zählerstände, was bei bestehendem Bankeinzug kurzfristig zu unerwarteten finanziellen Engpässen beim Kunden führen kann;
– Eingabe zu niedriger Zählerstände am Ende einer Abrechnungsperiode, was bei gleichzeitiger Änderung der Bankverbindung zu unberechtigten Geldtransfers auf Konten des Angreifers führen kann.

Diese Daten sind im Interesse der Kunden nach Vorgabe des Datenschutzgesetzes zwingend zu schützen. Das bedeutet insbesondere, dass die Absicherung „auf dem Stand der Technik“ zu erfolgen hat. Dafür müssen die Informationen zur Authentifizierung so aufgebaut sein, dass man sie nicht durch simples Ausprobieren ermitteln oder durch geschicktes Analysieren ableiten kann.



Über ein Textformular – hier ein fiktives Beispiel – können Kunden ein eigenes Konto erstellen oder freischalten. Die Authentifizierungsmerkmale sind jedoch häufig zu einfach zu erraten.

Schutz nach „Stand der Technik“

Technisch bedeutet dies, dass die Entropie der abgefragten Informationen hoch sein muss. Das heißt, dass es genügend viele verschiedene mögliche Werte geben muss, um simples Ausprobieren zeitlich und somit wirtschaftlich unrentabel zu machen. Das lässt sich zum Beispiel durch eine sehr lange Zeichenkette erreichen oder durch Kombinieren von mindestens zwei kürzeren Zeichenketten.

In den untersuchten Portalen werden folgende Merkmale für das Freischalten der Konten verwendet: Kundennummer, Zählernummer, Vertragsnummer, Geburtsdatum, Postleitzahl – wobei die letzten beiden nur selten eingesetzt wurden. In allen Portalen sind mindestens zwei dieser Merkmale für die Freischaltung erforderlich. Schauen wir uns deren Entropie genauer an. Kunden- und Vertragsnummern haben den größten möglichen Werteraum. Die beteiligten Forscher haben bei den Recherchen bis zu 12-stellige Kunden- und Vertragsnummern gesehen. Die Zählernummern waren allerdings kürzer. Ein Geburtsdatum besteht aus acht Ziffern und Postleitzahlen sind in Deutschland fünfstellig.

Mathematisch kann man argumentieren, dass die Entropie einer 12-stelligen Vertragsnummer einen Raum von 10^{12} Möglichkeiten aufspannt, also eine Billion (1 000 000 000 000). Kombiniert man dies mit einem zweiten Merkmal, multiplizieren sich die beiden Zahlenräume. Somit käme man bereits in Kombination mit der (kurzen) Postleitzahl auf 100 Billiarden Möglichkeiten. Das wäre im Verhältnis zum Wert der Daten eines einzelnen Kunden ein sehr guter Schutz gegen Brute-Force-Angriffe, also simples automatisiertes Ausprobieren aller Möglichkeiten.

In der Realität ist die Entropie der verwendeten Merkmale allerdings deutlich kleiner. Man kann bei Kundennummern, Vertragsnummern und Zählernummern davon ausgehen, dass diese fortlaufend vergeben werden. Denn es ist für Unternehmen sinnlos, bei der Vergabe von Kundennummern und Verträgen nach dem Zufallsprinzip zu arbeiten. (Sollte ein Leser ein Unternehmen kennen, das dies tut, sind die Autoren für einen Hinweis dankbar.) Auch bei der Seriennummer eines Zählers ist eine Zufallszahl in der Praxis wenig sinnvoll. Daher kann man hier weitere Gedankenspiele anstellen, zum Beispiel, ob in einem Neubaugebiet viele Zähler unmittelbar fortlaufend nummeriert sind, weil sie zusammen gekauft wurden.

Zufall ist nicht gleich Zufall

Die Entropie eines Geburtsdatums liegt auch deutlich unter den 10^8 theoretischen Möglichkeiten. Geht man davon aus, dass Kunden ein Alter zwischen 18 und 80 Jahren haben und das Jahr im Schnitt 365,25 Tage hat, ergeben sich höchstens 23 000 sinnvolle Werte. Diese könnte man vermutlich weiter einschränken, wenn man statistisch untersucht, welches Mindest- und welches Höchstalter die meisten Kunden von Energieversorgern haben.

Dagegen ist die Entropie einer Postleitzahl mit Abstand am kleinsten. Man kann davon ausgehen, dass die meisten Kunden Postleitzahlen im Einzugsgebiet

iX-TRACT

- Nahezu alle öffentlichen Versorgungsunternehmen bieten Onlineportale für ihre Kunden an. Häufig sind darin deren persönliche Daten enthalten und stehen somit im Netz – auch ohne Freischaltung durch den Kunden.
- Da die Zugangsdaten zu den Benutzerkonten zum Teil auf fortlaufend nummerierten Merkmalen wie Vertrags- oder Kundennummern beruhen, besitzen sie zu wenig Entropie und sind zu erraten oder abzuleiten.
- Sicherheitsfeatures wie Captchas oder Verschlüsselung setzen die untersuchten Portale häufig nicht ein oder sie nutzen veraltete oder unsichere Verfahren.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

Daten, die in Kundenportalen hinterlegt sind

- Name und Vorname
- Anschrift
- E-Mail-Adresse
- Telefonnummer, Mobilnummer, Faxnummer
- Geburtsdatum
- Bankverbindung: IBAN (bei manchen Portalen teilweise geschwärzt), BIC, Institut, Mandat
- Verträge als PDF-Download aus den letzten (bis zu zehn) Jahren
- Rechnungen* als PDF-Download aus den letzten (bis zu zehn) Jahren
- Zählerstände mit Vertragsnummer, Zählernummer und Adresse
- Verbrauchshistorie über einen Zeitraum von mehreren Jahren

Bei einem Anbieter konnte mittels legitimer Zugangsdaten eine Freischaltung für einen Vertrag erwirkt werden, der schon über ein Jahr zuvor gekündigt worden war. Das wirft weitere Fragen zu den Praktiken solcher Datenbereitstellung auf.

* Die Rechnungen enthalten wiederum Namen, Adressdaten und (vollständige) Bankverbindungen.

der Stadt haben, in der der Betreiber des Portals ansässig ist. Selbst eine Stadt wie Berlin hat nur 191 verschiedene Postleitzahlen. Und deutschlandweit gibt es laut Wikipedia (Stand Mai 2013) nur 8208 sogenannte Hauszustellungspostleitzahlen.

Wenn nun Kunden-, Vertrags- und Zählernummern fortlaufend vergeben werden, kann ein Angreifer, der im Besitz einer gültigen Nummer ist, davon ausgehen, dass er andere gültige Nummern erhält, wenn er von seiner aus aufwärts- oder abwärtszählt. Somit kann er mindestens ein existierendes Merkmal für die Freischaltung ganz einfach ermitteln. Sollte der Angreifer nicht im Besitz eines gültigen Merkmals sein, kann er versuchen, von Informationslecks bei Fehlermeldungen zu profitieren. Da Menschen dazu neigen, sich nicht mehr an ihre Zugangsdaten zu erinnern, gibt es typischerweise Funktionen wie „Passwort vergessen“. Diese schicken Anwendern in der Regel eine E-Mail zur Wiederherstellung des Passworts, wenn zuvor eine andere Information des Benutzerkontos (zum Beispiel die Kundennummer) angegeben wird.

Bei vielen dieser Mechanismen verrät jedoch die Fehlermeldung, ob die eingegebene Information im System existiert, also beispielsweise ein Hinweis wie „Für diese Kundennummer gibt es keinen Eintrag im System“. In solchen Fälle kann ein Angreifer wieder durch simples Ausprobieren gültige Merkmale ermitteln. Gelangt er auf die eine oder andere Weise an ein Merkmal, wird die Sicherheit des Freischaltungsverfahrens auf die Entropie des anderen Merkmals reduziert. Ist dieses andere Merkmal die Postleitzahl, sind nur wenige Versuche nötig, um eine Freischaltung zu erwirken.

Diese praktischen Überlegungen zeigen sehr deutlich, dass eine rein mathematische Betrachtung der Entropie von Freischaltungsmerkmalen grundlegend falsch ist. Bei den heutigen Bandbreiten deutscher Internetprovider muss man davon ausgehen, dass selbst Bürger mit einem normalen Internetanschluss in der Lage sind, circa 20 000 automatisierte Anfragen pro Sekunde abzuschicken. Die tatsächliche Zahl der möglichen Anfragen beziehungsweise Freischaltungsversuche hängt im Wesentlichen von der CPU des Servers des Onlineportals ab.

Weitere Sicherheitsmaßnahmen vonnöten

Statistisch betrachtet ist hier noch zu erwähnen, dass man im Schnitt nur die Hälfte der möglichen Werte eines Werteraums ausprobieren muss, bis man Erfolg hat. Klar ist jedenfalls, dass Kombinationen von vorhersagbaren Merkmalen und Merkmalen mit kleinem Werteraum in wenigen Sekunden oder Minuten ermittelt werden können.

Zum Schutz gegen automatisiertes Ausprobieren von Authentifizierungsversuchen (Brute Force) verwenden manche Betreiber sogenannte Captchas. Captcha bedeutet Completely Automated Public Turing Test to tell Computers and Humans Apart – etwa „vollautomatischer öffentlicher Turing-Test zur Unterscheidung von Computern und Menschen“ (Wikipedia). Durch den Captcha muss der Anwender zusätzlich zu den Merkmalen noch Aufgaben lösen, die ein Computerprogramm nach aktuellem Stand nicht lösen kann. Das soll verhindern, dass Daten in schneller Folge automatisiert abgeschickt werden.

Neben der Verwendung eines sicheren Verfahrens zur Authentifizierung ist natürlich auch der Transport der Daten abzusichern. Denn das Bundesdatenschutzgesetz sieht unter anderem vor, dass die Übermittlung personenbezogener Daten verschlüsselt erfolgen muss. Technisch geschieht dies bei Onlineplattformen über das HTTPS-Protokoll, das alle übermittelten Daten mittels Transport Layer Security (TLS) schützt. Sollte ein Kunde eine Portalanwendung aber aus Versehen – oder durch einen manipulierten Link – mit dem unverschlüsselten HTTP-Protokoll aufrufen, darf die Anwendung dies nicht erlauben.

Hilfsweise muss sie zumindest die Verbindung sofort auf HTTPS umstellen, bevor Eingaben verarbeitet oder Daten angezeigt werden. Man könnte zwar argumentieren, Anwender seien selbst schuld, wenn sie kritische Dienste mit HTTP ansprechen und die Daten dadurch im Klartext übertragen werden. Aber es gibt immer noch Benutzer, die technisch wenig versiert sind und den Unterschied nicht erkennen. Insbesondere, wenn sie auf einen (manipulierten) Link klicken.

Das Datenschutzgesetz sieht ohnehin vor, dass die Sicherheitskonzepte dem Stand der Technik entsprechen. Und dieses Prinzip ist bei Verschlüsselung besonders wichtig, da regelmäßig neue Schwächen bei bis dato sicheren Verfahren entdeckt werden. Wenn ein Browser eine verschlüsselte Verbindung mit einem Server aufbauen will, bietet er dem Server dazu verschiedene Verfahren an. Der Server sollte dann das sicherste auswählen, das er unterstützt. Oftmals ist jedoch die vom Server bevorzugte Variante nicht die sicherste. Server sollten allerdings keine Verfahren akzeptieren, in denen Schwachstellen existieren beziehungsweise die als kryptografisch gebrochen

Fehler bei der Verschlüsselung

Von den untersuchten 240 Portalen

- ließen sich 15 komplett unverschlüsselt über HTTP ansprechen;
- bot eines Schlüssellängen von 40 und 56 Bit an, was komplett unsicher ist;
- boten 24 das als gebrochen eingestufte Verfahren RC4 an;
- boten 22 das als gebrochen eingestufte Verfahren SSL.v3 an;
- boten 98 das als unsicher eingestufte Verfahren 3DES an und
- unterstützten 15 nicht die neueste Version des TLS-Verfahrens (V1.2 zum Zeitpunkt der Analyse).

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

gelten. Die Autoren haben daher auch die von den Energieversorgern eingesetzten Verschlüsselungsverfahren überprüft und festgestellt, dass etliche veraltet oder unsicher sind (siehe Kasten „Fehler bei der Verschlüsselung“).

Erkenntnisse aus der Sicherheitsanalyse

Um eine Sicherheitsanalyse von Authentifizierungsmechanismen durchzuführen, ist es ausreichend, den logischen Aufbau der Anwendungen und die Flags beim SSL/TLS-Handshake der Server manuell zu analysieren. Will man eine Fehlermeldung provozieren, genügt schon eine einzige offensichtlich falsche Eingabe, beispielsweise eine Vertragsnummer, die nur aus Nullen besteht. Für die Analyse der 240 Onlineportale wurden also keinerlei Hacker-Tools oder Brute-Force-Methoden verwendet. Art und Länge der Freischaltungsmerkmale sind auch für Laien aus den Eingabemasken zu erkennen.

Vier Betreiber von Onlineportalen verwendeten zur Authentifizierung die Vertragsnummer zusammen mit der Postleitzahl der Kunden. Diese Kombination hat nur eine sehr geringe Entropie, da sich die Vertragsnummer durch Hoch- beziehungsweise Herunterzählen ermitteln lässt und die Postleitzahlenräume der zugehörigen Städte sehr klein sind. Da dies ein großes Risiko für die betroffenen Kunden darstellt, wurden die vier Betreiber umgehend benachrichtigt. Ihre Reaktionen und die der zuständigen Landesdatenschutzbeauftragten fielen allerdings dürftig aus, wie der Kasten „Reaktionen der Portalbetreiber und Landesdatenschutzbeauftragten“ zeigt.

Von 240 Portalen hatten 109 zudem Informationslecks bei Fehlermeldungen. Dadurch kann ein Angreifer Rückschlüsse auf eines der beiden zur Authentifizierung erforderlichen Merkmale ziehen. Das reduziert die Sicherheit des Freischaltungsverfahrens erheblich.

Auch bei den Captchas gab es Mängel. Zum einen muss ein Captcha technisch richtig in die Anwendung eingebunden werden. Es gab zwei Fälle, bei denen nach Absenden der Daten eine Fehlermeldung erschien, dass die Kundennummer nicht existiere, obwohl der zugehörige Captcha gar nicht ausgefüllt war. In so einem Fall ist ein Captcha sinnlos. Denn er soll ja verhindern, dass ein automatisiertes Skript prüfen kann, ob die Eingaben erfolgreich waren oder nicht. Außerdem besteht die primäre Aufgabe von Captchas nicht darin, Angriffe zu erkennen, sondern Computer von Menschen zu unterscheiden. Das blockiert (heutige) Programme und hindert sie somit daran, viele Anfragen in rascher Folge zu senden. Aber es blockiert keine Angriffe durch Menschen. Zumindest nicht, wenn die Entropie der möglichen Kombinationen wie oben beschrieben sehr klein ist. Beispielsweise braucht ein neugieriger Kunde ohne jegliches Hacker-Wissen bei den Betreibern, die mit Postleitzahlen arbeiten, trotz Captcha statistisch weniger als 30 Minuten, um an Daten eines anderen Kunden zu gelangen.

Bei den 240 untersuchten Portalen wurden insgesamt nur 39 Captchas gefunden, von denen aber zwei wie beschrieben falsch implementiert waren. Das legt nahe, dass 85 % der Portale nicht gegen automatisierte Angriffe geschützt sind. Ist – wie in den meisten Fällen – mindestens ein Authentifizierungsmerkmal einfach abzuleiten, sind Brute-Force-Angriffe sehr effektiv. Die gängigsten Fehler bei der Verschlüsselung der Datenübertragung sind im Kasten „Fehler bei der Verschlüsselung“ zusammengefasst. Aus der Fülle an veralteten Verfahren lässt sich schlussfolgern, dass die Konfiguration der zu verwendenden Verschlüsselungsprotokolle teilweise schon einige Jahre alt ist und nicht regelmäßig auf den neuesten Stand gebracht wird. Solche Praxis spiegelt nicht den von Bundesdatenschutzgesetz und europäischer Datenschutz-Grundverordnung geforderten Stand der Technik wider. Entsprechend ist die Datenübertragung bei einigen Portalbetreibern als unsicher zu betrachten. Insbesondere dort, wo man das Portal komplett unverschlüsselt aufrufen kann.

Fazit

Die Energieversorger sind ein Beispiel dafür, wie Firmen auf keinen Fall mit ihren Kundendaten umgehen sollten. Im Mai 2018 tritt die Datenschutz-Grundverordnung der EU in Kraft (EU-DSGVO). Die Strafen bei einem Verstoß können leicht mehrere Millionen Euro betragen. Betreiber von Onlinekundenportalen sind daher gut beraten, die Sicherheit der Daten ihrer Kunden mittels durchdachter, korrekt implementierter und vor allem aktueller Schutzmechanismen zu gewährleisten. Insgesamt stellt sich die Frage, ob personenbezogene Daten überhaupt ohne expliziten Wunsch eines Kunden online gestellt und damit einem (unnötig) hohen Risiko ausgesetzt werden sollten. Offen bleibt auch die Frage, ob von Kunden nicht genutzte Onlinekonten von Datendieben bereits kompromittiert wurden. (ur@ix.de)

Andreas Wiegenstein

ist Mitgründer und CEO des Sicherheitsanalyse- und -beratungsunternehmens SERPENTEQ. An der Untersuchung der Portale wirkten seine Kollegen Xu Jia und Sven Neuz sowie Prof. Dr.-Ing. Sebastian Schinzel von der FH Münster mit.

Reaktionen von Portalbetreibern und Landesdatenschutzbeauftragten

Die Kontaktaufnahme zu Betreiber Nummer eins fand über das Bundesamt für Sicherheit in der Informationstechnik (BSI) statt. Dieser Betreiber versicherte glaubhaft, dass er das Problem sehr ernst nehme und an einer Lösung arbeite. So weit, so vorbildlich.

In einem Folgegespräch in Bonn erklärte das BSI, dass es für diese Art von Sicherheitsproblemen eigentlich nicht zuständig sei und weitere Sicherheitsmängel an die jeweiligen Verbände (von Energieversorgern) oder Landesdatenschutzbeauftragten gemeldet werden sollten.

Betreiber Nummer zwei ignorierte das Anschreiben. Auch die zuständige Landesdatenschutzbeauftragte ließ eine diesbezügliche Kontaktaufnahme zunächst unbeantwortet. Nach einem Monat kam die Meldung, der Landesdatenschutzbeauftragten, dass man prüfe, ob Mitarbeiter „hier aufsichtsbehördlich tätig werden müssen“.

Betreiber Nummer drei schrieb einige Tage nach der Kontaktaufnahme: „Bitte streichen Sie mich aus Ihrer Mailingliste. Herzlichen Dank.“ Auch hier wurde das Advisory an die zuständige Landesdatenschutzbeauftragte (nicht identisch mit der vorigen) geschickt. Außer einem Einzeiler zum Erhalt der Nachricht gab es trotz Nachfrage keine Information vom Betreiber, ob man an einer Lösung arbeite.

Betreiber Nummer vier ignorierte das Anschreiben dem Anschein nach zunächst. Auch der zuständige Landesdatenschutzbeauftragte (wiederum jemand anders) ließ eine Kontaktaufnahme unbeantwortet. 12 Tage nach dem ersten Kontaktieren meldete sich Betreiber Nummer vier doch noch und bekundete Interesse an weiteren Details.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover