

# Newsletter Datenschutz

## Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

Datenschutz ist keine Geheimniskrämerei, sondern hat sehr viel mit Transparenz zu tun. So ist es wichtig zu wissen, wo Daten gespeichert werden, auch dann, wenn die Daten in den Weiten des Internets verteilt sind. Diese Ausgabe informiert Sie über die Standortfrage bei der Nutzung von Online-Diensten ebenso wie über das neue Bundesmeldegesetz, das ebenfalls für mehr Transparenz sorgen soll.

Ein weiterer Beitrag zeigt, dass es mit der Transparenz aber nicht zu weit gehen darf, so etwa beim Einsatz von Videoüberwachung und Webcams. Nicht zuletzt kann das Gegenteil von Transparenz, die Verschlüsselung, zu einer Gefahr werden. Lesen Sie am besten jetzt gleich, wie Online-Erpresser versuchen, Ihre Daten zu verschlüsseln und Lösegeld für die Befreiung der Daten zu verlangen.

Wir wünschen Ihnen wieder viele wertvolle Einsichten in den Datenschutz!

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

## Online-Erpressung: So reagieren Sie richtig

**Schadsoftware aus dem Internet verschlüsselt wichtige Daten der Opfer und verlangt Lösegeld für die Entschlüsselung. Sowohl Unternehmen als auch Privatnutzer sind in Gefahr. Was tun, um dem zu begegnen?**

### Erpresser kommen über das Internet

2016 wird das Jahr der Online-Erpressung, da ist sich der IT-Sicherheitsanbieter Trend Micro sicher. Bereits seit zehn Jahren versuchen Internetkriminelle, ihren Opfern Angst einzujagen und Geld zu erpressen. Früher behaupteten die Erpresser, sie hätten die Nutzer bei einer illegalen Tat erwischt, zum Beispiel bei der Nutzung einer Raubkopie. Nur gegen Zahlung eines Geldbetrags würden sie der Polizei gegenüber schweigen. Die Erpressermasche hat sich inzwischen geändert und bedroht nun das Herzstück jeder IT, die Daten.

Die Erpressung beginnt mit einer Schadsoftware, die über E-Mail, Browser oder mobile App auf das Gerät des Opfers kommt. Dort verschlüsselt das Schadprogramm alle Daten des Nutzers. Nur gegen Zahlung des Lösegelds werden die Daten wieder freigegeben, also entschlüsselt, so die Drohung.

Leider sind viele Opfer so hilflos, dass sie tatsächlich bezahlen, oft aber ohne dass die versprochene Entschlüsselung stattfindet. Bezahlt man mit Kreditkarte, missbrauchen die

Täter womöglich auch diese Daten, zusätzlich zu den unbrauchbaren eigenen Daten.

### Der Schaden ist enorm

Wie erfolgreich die Online-Erpresser sind, zeigen aktuelle Beispiele: Die Schadsoftware CryptoWall konnten IT-Sicherheitsforscher in über 406.000 Fällen nachweisen. Die Erpresser erbeuteten dabei 325 Millionen US-Dollar als Lösegeld. Leider ist das kein Einzelfall. Der Schaden für die betroffenen Unternehmen und Nutzer geht aber noch weiter, als es die Höhe des Lösegelds vermuten lässt. Da die An-

greifer die Daten häufig gar nicht mehr entschlüsseln, fehlen sie dauerhaft.

Häufig gibt es keine Datensicherung bei den Betroffenen, oder die Datensicherung war ebenso schlecht geschützt wie die Daten selbst, und beides wurde verschlüsselt. Je nach Daten und Art des Unternehmens kann ein solcher Datenverlust die Existenz bedrohen oder aber den Ruf so stark schädigen, dass Kundenzahl und Umsatz drastisch zurückgehen. Bei Privatnutzern ist der Schaden finanziell gesehen zwar meist geringer. Aber wenn sich wichtige Daten wie die einzigen Fotos, die von einem geliebten Menschen noch vorhanden sind, nicht mehr öffnen lassen, ist der Verlust ebenfalls groß.

### Nicht erpressen lassen, sondern Daten besser schützen

Deutsche Sicherheitsbehörden wie das Bundeskriminalamt raten dazu, den Online-Erpressern kein Lösegeld zu zahlen. Der beste Schutz gegen Online-Erpresser ist eine gute Absicherung der IT: mit aktueller und professioneller Antiviren-Software und einer Begrenzung der Berechtigungen auf den Computern, die mit dem Internet verbunden sind. Entscheidend ist vor allem die regelmäßige, vollständige und geschützte Sicherung der Daten, um Online-Erpressung den Schrecken zu nehmen. Hat man ein Backup, braucht man keine Entschlüsselung - die oft sowieso nie kommen würde.



Online-Erpresser setzen derzeit verstärkt auf Daten-Verschlüsselung (Bild: Eyematrix/iStock/Thinkstock)

## Endlich: Spielregeln für Webcams

Wer Lust hat, sich einmal vom Sessel aus bequem in ganz Deutschland umzusehen, kann im Internet auf rund 2.000 Webcams zugreifen. An welche Spielregeln müssen sich die Betreiber der Webcams halten? Ein viel beachtetes Urteil des Verwaltungsgerichts Schwerin schafft in wichtigen Punkten Klarheit.

### Webcams im Überfluss

"Webcam Galore" heißt die wohl beliebteste Überblicksseite für Webcam-Fans im Internet. Das englische Wort "Galore" bedeutet dabei "zuhauf, im Überfluss". Dem Versprechen, das damit verbunden ist, macht die Seite alle Ehre: Allein für Deutschland weist sie nahezu 2.000 Webcams nach.

Viele dieser Kameras sind aus der Sicht des Datenschutzes völlig problemlos, so etwa Webcams mit dem Blick auf Sehenswürdigkeiten wie den Dresdner Zwinger. Aber es gibt auch ganz andere Kameras. Sie zeigen belebte öffentliche Plätze, Strände mit Badegästen oder auch Baustellen mit Bauarbeitern. Wer sich an solchen Örtlichkeiten aufhält, rechnet meist nicht damit, dass es eine Webcam gibt. Und schon gar nicht vermutet er, dass er im Internet zu sehen sein könnte.

### Stein des Anstoßes: Blick auf Strand und Fahrradweg

Damit ist das Problem umschrieben, mit dem sich das Verwaltungsgericht Schwerin zu befassen hatte. Gelegenheit dazu bot ihm eine Webcam, die der Eigentümer einer Ferienanlage installiert hatte. Die Kamera erfasste unter anderem den öffentlichen Fahrradweg neben dem Gelände, einen Teil der Strandpromenade und sogar einen Teil des Strands. Böses führte der Eigentümer eigentlich nicht im Schilde. Er wollte - so seine Argumentation - lediglich die Umgebung seiner Ferienwohnungen zeigen und so Interesse daran wecken.

### Die Aufsichtsbehörde greift hart durch

Die zuständige Datenschutzaufsicht sah das jedoch höchst kritisch. Nachdem gütliches Zureden nicht half, ordnete sie an, die Kameras dauerhaft außer Betrieb zu nehmen. Um dem Ganzen zusätzlichen Nachdruck zu verleihen, verfügte die Behörde außerdem, dass diese Anordnung sofort zu vollziehen ist. Aus ihrer Sicht verletzte die Webcam nämlich in erheblicher Weise das Persönlichkeitsrecht der Passanten und Badegäste, die von ihr erfasst wurden.



*Ist nicht auszuschließen, dass eine Webcam fürs Internet so filmt, dass Personen zu identifizieren sind, ist sie unzulässig (Bild: Eugene Gitlits/iStock/Thinkstock)*

### Der Streitpunkt: Identifizierung möglich oder nicht?

Der Unternehmer, der die Webcam betrieb, um für seine Ferienwohnungen Werbung zu machen, hatte sich auf der sicheren Seite geglaubt. Dabei argumentierte er wie folgt:

- Ihm gehe es lediglich um Panorama-Aufnahmen, die die Landschaft und das aktuelle Wetter zeigen sollten.
- Personen würden nur zufällig erfasst.
- Das sei aber belanglos. Die Bilder seien nämlich in sehr niedriger Auflösung gehalten.
- Die Kamera verfüge außerdem über keine Zoom-Funktion, und Gesichter seien auf den Bildern auf keinen Fall erkennbar.

Datenschutzaufsicht und Verwaltungsgericht sahen das freilich ganz anders. Darauf, ob das Gesicht zu erkennen ist, kommt es nach ihrer Auffassung letztlich nicht an. Selbstverständlich sei eine Person ohne Weiteres zu identifizieren, wenn man ihr Gesicht auf den Aufnahmen erkennen könne. Doch auch andere Kriterien könnten dazu führen, dass

Aufnahmen als personenbezogen anzusehen sind und damit dem Datenschutz unterliegen.

So könne eine Person etwa an ihrer Körperhaltung zu erkennen sein, aber auch an ihrer Kleidung oder an mitgeführten Gegenständen. Auch der Zeitpunkt und der Ort einer Aufnahme könnten Rückschlüsse darauf erlauben, welche Person man vor sich habe.

### Überwachung mittels Internet unzulässig

Die Interessen von Personen, die auf den Aufnahmen von Webcams zu erkennen sind, werden - so das Gericht - in erheblicher Weise beeinträchtigt. Damit werde nämlich zum Beispiel dokumentiert, wann sich ein Betroffener dort aufgehalten hat und ob er in Begleitung war oder nicht. Die entsprechenden Aufzeichnungen könnten noch im Nachhinein im Internet abgerufen und ausgewertet werden. Es sei auch möglich, sie zu speichern. Von alledem würden die Betroffenen nichts erfahren. Insgesamt gesehen sei deshalb der Betrieb einer Webcam unzulässig, wenn auf den Aufnahmen Personen zu identifizieren sind.

### Durchaus möglich: rein interne Kameras

Daraus ergibt sich im Umkehrschluss übrigens recht klar, dass Webcams, mit denen zum Beispiel Baustellen intern überwacht werden, rechtlich möglich sind.

Wichtig ist allerdings, dass Arbeitnehmer und Baustellenbesucher über die Kamera informiert werden und dass ein Abruf nur intern (etwa durch die Baustellenleitung) möglich ist, nicht dagegen für die Öffentlichkeit im Internet. Außerdem gilt es zu klären, ob und wie lange eine Speicherung nötig ist. Und dass der Betriebsrat auch noch ein Wort mitzureden hat, bevor eine solche Kamera installiert wird, ist selbstverständlich.

### Impressum

agentia wirtschaftsdienst  
dipl.-inform. udo wenzel  
budapester straße 31  
10787 berlin

tel.: 030 2196 4390  
fax: 030 2196 4393

udo.wenzel@agentia.de  
thorsten.ritter@agentia.de

## Meldepflicht beim Anmieten einer "Projektwohnung"

Manchmal ist es der vernünftigste Weg, wenn ein Projekt in einer anderen Stadt länger dauert: Man mietet sich dort (möglicherweise sogar auf Kosten des Arbeitgebers) vorübergehend eine kleine Wohnung. Was ist dabei zu beachten? Welche Neuregelungen hat das Bundesmeldegesetz gebracht, das seit dem 1. November 2015 in ganz Deutschland gilt?

### Wichtiges Projekt in Hamburg, also dieses Mal weit weg

Stellen Sie sich vor, dass zwei Arbeitnehmer im selben Unternehmen tätig sind. Stellen Sie sich weiter vor, dass dieses Unternehmen seinen Sitz irgendwo am Oberrhein hat, nur wenige Kilometer von Frankreich entfernt. Der eine Arbeitnehmer wohnt in Deutschland, der andere auch nicht viel weiter weg, aber in Frankreich, knapp hinter der Grenze. Das macht im Alltag heute kaum noch einen Unterschied.

Das Unternehmen bittet beide Arbeitnehmer, für voraussichtlich fünf Monate bei einem wichtigen Projekt mitzuarbeiten. Der Auftraggeber des Projekts hat seinen Sitz in Hamburg. Deshalb ist es nötig, dass beide Arbeitnehmer sich dort immer wieder einmal für längere Zeit aufhalten. Deshalb mietet das Unternehmen eine kleine Wohnung in Hamburg an und überlässt sie den beiden zur gemeinsamen Benutzung.

### Bemerkenswertes Telefonat mit der Meldebehörde

In den Medien war immer wieder zu lesen und zu hören, dass das neue Bundesmeldegesetz seit dem 1. November 2015 neue Spielregeln mit sich bringt. Deshalb fragt das Unternehmen bei der Meldebehörde in Hamburg an, was es in dieser Hinsicht beachten muss. Die Auskunft bietet für die Beteiligten manche Überraschung:

### Meldepflicht: Grundsatz und Ausnahmen

Rasch ist klar, dass prinzipiell für jeden, der eine Wohnung bezieht, eine Meldepflicht besteht. Sie muss innerhalb von zwei Wochen nach dem Einzug erfüllt werden. Formulare stellt auf Wunsch die Meldebehörde.

Allerdings gibt es von dieser prinzipiellen Meldepflicht Ausnahmen, falls jemand nur vorübergehend eine zusätzliche Wohnung bezieht. Also gilt: Für die gerade einmal fünf

Monate wird man ja wohl kaum eine Anmeldung verlangen? Das scheint naheliegend.

### Scheinbar merkwürdige Fragen der Behörde

Umso größer ist die Überraschung, als das Meldeamt anfängt, zusätzliche Fragen zu stellen. Zunächst möchte es wissen, ob die beiden Arbeitnehmer außer der vorübergehenden Wohnung in Hamburg noch woanders eine dauerhafte Wohnung haben. Das trifft bei beiden zu. Ist wenigstens damit jetzt alles erledigt?

Weit gefehlt! Nun möchte das Meldeamt wissen, wo diese dauerhafte Wohnung jeweils liegt, ob in Deutschland oder im Ausland. Die wahrheitsgemäße Antwort: Der eine hat seine dauerhafte Wohnung in Deutschland, der andere in Frankreich.

Daraufhin bedauert der freundliche Mensch vom Meldeamt und sagt: Der Arbeitnehmer, der in Frankreich wohnt, muss sich für die fünf Monate in Hamburg anmelden, der andere, der in Deutschland wohnt, dagegen nicht!

### Auch heute noch: Unterschied zwischen Inland und Ausland

Auf die ungläubige Nachfrage, ob das ernst gemeint sei, versichert der Behördenmitarbeiter, er wolle keinesfalls jemanden auf den Arm nehmen. Die gesetzliche Regelung (er erwähnt § 27 Absatz 2 Bundesmeldegesetz) sei aber nun einmal wie folgt:

Wer im Inland (also in Deutschland) schon für eine Wohnung gemeldet ist, muss sich für eine neue zusätzliche Wohnung nur dann anmelden, wenn er diese zusätzliche Wohnung länger als sechs Monate beibehalten will. Wer dagegen im Ausland (hier also in Frankreich) für eine Wohnung gemeldet ist, der muss sich für eine neue zusätzliche Wohnung schon dann anmelden, wenn er sie länger als drei Monate beibehalten will.

Da das Projekt fünf Monate dauern soll, muss sich somit der Arbeitnehmer mit dem Wohnsitz in Frankreich für die Wohnung am Projektort Hamburg anmelden, der Arbeitnehmer mit dem Wohnsitz in Deutschland dagegen nicht. Auf die Staatsangehörigkeit komme es dabei - so betont die Behörde - nicht an, nur auf den schon vorhandenen Wohnsitz im Inland oder im Ausland.

### "Compliance" ist hier sinnvoll

Ist es zu riskieren, diese im Ergebnis etwas merkwürdige Unterscheidung zu ignorieren und die gesetzlich vorgeschriebene Meldung beim Einwohnermeldeamt zu "vergessen"? Hier ist Vorsicht geboten. Immerhin könnte bei einem Verstoß gegen die Meldepflicht ein Bußgeld verhängt werden. Das wirft dann weder auf den Arbeitnehmer noch auf sein Unternehmen ein gutes Licht. Besser sollte man sich damit anfreunden, dass man nicht immer alles sofort verstehen muss, was der Gesetzgeber regelt.

### Wohnungsgeberbestätigung hier durch den Arbeitgeber

Damit die Anmeldung funktioniert, muss der Arbeitgeber in unserem Beispiel eine "Wohnungsgeberbestätigung" ausstellen. Sie wurde mit dem Bundesmeldegesetz neu eingeführt und ist dort in § 19 geregelt. Ausstellen muss sie derjenige, der einem anderen eine Wohnung überlässt. Im Alltag ist das meistens der Vermieter. Wenn aber - so wie hier der Arbeitgeber - jemand zwischengeschaltet ist, trifft diese Pflicht ihn. Formulare dafür gibt es auf der Homepage jeder Meldebehörde.



Gerade bei Projektarbeit kann es sein, dass für eine vorübergehende Wohnung eine Anmeldung bei der zuständigen Meldebehörde nötig ist  
(Bild: Viola08/Stock/Thinkstock)

## Cloud Computing: Wo liegen die Daten?

Bei vielen Produkten achtet man auf ihre Herkunft, um ein Gefühl für die Qualität zu haben. Das darf bei der Nutzung von IT-Diensten aus dem Internet nicht anders sein, allein schon aus Gründen des Datenschutzes.

### Wo sind die Daten?

Stellen Sie sich vor, Sie wollen wissen, ob die Daten eines wichtigen Kundenprojekts sicher gespeichert werden. Um das zu klären, müssen Sie zuerst in Erfahrung bringen, wo Ihr Unternehmen denn die Daten vorhält: Liegen sie auf einem bestimmten Speichermedium im Tresor, im Rechenzentrum, das Ihr Unternehmen nutzt, oder nur auf Ihrem lokalen Arbeitsplatz-PC? Sie merken schon: Der Standort der Datenspeicherung und Datenverarbeitung hat durchaus einen Einfluss auf den Grad der Sicherheit.

Wenn die Daten in einer Cloud gespeichert sind, also irgendwo im Internet, spielt der Standort ebenfalls eine Rolle, nur dass Sie nicht ohne Weiteres wissen, wo der Standort ist.

Das ist ein Problem, nicht nur für die Prüfung, wie sicher die wichtigen Daten sind. Es gibt rechtliche Vorgaben dazu, an welche Standorte personenbezogene Daten übertragen werden dürfen. Besondere Bedingungen herrschen, wenn die Daten das Gebiet der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR) verlassen. Doch woher weiß man eigentlich, wohin die Daten wandern, wenn man sie in einer Cloud speichert?

### Der Standort entscheidet über Sicherheit der Daten

Es ist zum Glück nicht unmöglich, Informationen über den Standort von Daten zu erhalten, wenn sie sich in einer Cloud befinden. Die Standortfrage sollte allerdings bereits vor der Nutzung einer Cloud gestellt werden, also zum Beispiel dann, wenn Sie Vorschläge für IT-Dienste aus dem Internet machen wollen, die Sie für Ihre betrieblichen Aufgaben benötigen. Aber auch dann, wenn Sie einmal privat Daten in eine Cloud übertragen wollen, sollten Sie an die Frage nach dem Standort der Cloud denken. Denn er kann die Sicherheit der Daten beeinflussen.

### Die Ortung der Daten

Die Klärung der Standortfrage beginnen Sie am besten mit dem Fragen selbst, also mit

einer Rücksprache bei dem Cloud-Anbieter oder einer Recherche in den Informationen des Anbieters. Kommt hierbei heraus, dass die Daten außerhalb der Europäischen Union gespeichert werden, sollten Sie sich den Rat der oder des Datenschutzbeauftragten, also von mir, einholen. Eine Datenübermittlung in Drittstaaten bedarf immer der genauen Überprüfung.

### Selbsterklärungen reichen nicht

Selbst wenn der Cloud-Anbieter sagt oder schreibt, alle Daten würden in Deutschland oder in der EU vorgehalten, ist diese Selbstbestätigung nicht ausreichend.

Wichtig wäre es, dass ein unabhängiger Dritter eine Bestätigung gibt, dass also zum Beispiel

ein anerkanntes Zertifikat bescheinigt, dass es sich um einen Cloud-Dienst aus Deutschland oder der Europäischen Union handelt. Zusätzlich gibt es technische Kontrollmöglichkeiten (Prüfung der Protokollierung, spezielle Abfragen und Berichte), die natürlich niemand von einem Cloud-Nutzer erwartet.

### Hinterfragen Sie immer den Standort

Grundlegend ist aber, dass Sie als Nutzer oder vielleicht auch als Entscheider, wenn es um die Wahl von Cloud-Diensten geht, immer im Auge behalten, dass es auch bei Diensten aus dem Internet darum geht, wo die Daten gespeichert und verarbeitet werden.

### Suchen Sie ggf. Expertenrat

Wenn Sie sich unsicher darüber sind, sprechen Sie mit mir oder der IT-Administration. Die Standortfrage muss gestellt und beantwortet werden. Denn es geht um den Schutz personenbezogener und anderer vertraulicher Daten. Und dieser Schutz ist nicht überall gleichermaßen gut und umfassend.

## Kennen Sie die Herkunft der von Ihnen genutzten Cloud? Machen Sie den Test!

**Frage: Cloud-Dienste, die man bei einem deutschen Anbieter bestellt, sind deutsche Cloud-Dienste. Stimmt das?**

- a) Ja, denn der Anbieter ist doch die verantwortliche Stelle in Deutschland.
- b) Nein, viele Anbieter vermitteln nur Dienste, die oftmals aus den USA stammen.

**Lösung:** Die Antwort b) ist richtig. Zum einen ist der Auftraggeber die verantwortliche Stelle für den Datenschutz. Zum anderen sind viele Auftragnehmer bei Cloud Computing nur Reseller. Die angebotene Cloud selbst kann überall sein, auch wenn der Händler in Deutschland sitzt.

**Frage: Wenn der Cloud-Anbieter sagt, die Cloud werde in Deutschland betrieben, reicht das. Ist das tatsächlich so?**

- a) Ja, damit hat man die Bescheinigung über den Standort der Cloud.
- b) Nein, zusätzlich zur Information des Anbieters muss es möglich sein, den Standort zu überprüfen. Immerhin hat man ja Kontrollpflicht als Auftraggeber.

**Lösung:** Die Antwort b) ist wieder richtig. Tatsächlich wird von einem Cloud-Anbieter gefordert, dass er den Standort der Cloud und damit der Datenspeicherung oder Datenverarbeitung transparent darlegt. Doch von dem Auftraggeber, also dem Cloud-Nutzer, wird erwartet, dass er die Datenschutzmaßnahmen des Anbieters kontrolliert. Zumindest sollte er sich die Aussage zum Cloud-Standort Deutschland oder EU durch einen unabhängigen Dritten bestätigen lassen. Hilfreich können hier anerkannte Zertifikate sein. Bescheinigen die Zertifikate die Einhaltung der in Deutschland gültigen Datenschutzvorgaben, ist damit auch die Frage nach dem Standort letztlich geklärt.