Newsletter Datenschutz
Ausgabe 06 | 2015

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

Fehler gehören zum Alltag. Trotzdem sollte man wissen, was richtig und was falsch ist. Darf jemand zum Beispiel Ihren Personalausweis als Pfand verlangen, oder ist das verboten? Wenn im Krankenhaus ein Kunstfehler passiert: Kann man dann die Privatanschrift des betreffenden Klinikarztes verlangen, um mögliche Ansprüche gegen ihn geltend machen zu können?

Die neue Ausgabe Ihrer Datenschutz-Zeitung beantwortet nicht nur diese Fragen, sondern sie hilft Ihnen auch, Fehler zu vermeiden - bei der Datenübertragung zwischen PC und Smartphone genauso wie bei der Sicherung Ihrer Daten. Machen Sie auch den Wissenstest auf der letzten Seite und suchen Sie nach den Fehlern in den Antworten.

Wir wünschen Ihnen wieder viele wertvolle Einsichten in den Datenschutz!
Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

Der Personalausweis als Pfand?

Immer wieder gibt es Situationen, in denen es zumindest auf den ersten Blick sinnvoll erscheint, den Personalausweis als eine Art Pfand zu hinterlegen. Was sagt das Gesetz dazu? Und was ist unter Sicherheitsaspekten zu bedenken?

An der Tankstelle und beim Fahrradvermieter

Die Fälle sind ganz unterschiedlicher Art:

- Sie haben an der Tankstelle für 80 Euro getankt und stellen fest, dass Sie nur noch 20 Euro Bargeld dabei haben. Zum Unglück kommt noch Pech hinzu: Ihre EC-Karte funktioniert auch nicht. Sie überlegen, der Kassenfrau Ihren Personalausweis als Pfand anzubieten.
- Sie wollen ein Fahrrad mieten. Der Vermieter möchte eine Sicherheit dafür, dass das teure Rad auch wieder zurückkommt. Er schlägt vor, dass Sie Ihren Personalausweis hinterlegen.

Der Chip im Personalausweis

Beide Male stellt sich die Frage, ob es in Ordnung geht, wenn der Personalausweis als Pfand hinterlegt wird. Das ist unter Sicherheitsaspekten heikel. Der "neue" Personalausweis, der seit 2010 ausgegeben wird, ist nämlich mit einem Chip versehen. Er enthält Daten über den Ausweisinhaber, die sich im Extremfall missbrauchen lassen, z.B. mit der Funktion "elektronischer Identitätsnachweis". Sie ist standardmäßig aktiviert, sofern der Ausweisinhaber sie nicht bei der Ausweisbehörde ausschalten lässt.

Restriktive Regelung im Gesetz

Aus diesem Grund verbietet es das Personalausweisgesetz, dass die Hinterlegung des Personalausweises vom Ausweisinhaber "verlangt" werden darf (siehe § 1 Absatz 1 Satz 3 Personalausweisgesetz). Freiwillig darf der Ausweisinhaber seinen Personalausweis dagegen hinterlegen - sofern wirklich eine echte Freiwilligkeit gegeben ist! Auf dieser Basis sind die beiden Beispielfälle schnell gelöst:

Vor allem der Chip mit den Inhaberdaten ist ein Risiko, hinterlässt man den Ausweis als Pfand (Bild: BMI)

Einzugsermächtigung statt Ausweis als Pfand

Natürlich können Sie an der Tankstelle von sich aus vorschlagen, Ihren Ausweis zu hinterlegen. Vielleicht reicht es aber doch auch, wenn die Kassenfrau Ihre Daten notiert und sich von Ihnen eine Einzugsermächtigung unterschreiben lässt (so das in der Praxis weithin übliche Verfahren).

Notieren der Daten statt Ausweis als Pfand

Ähnlich ist es beim Fahrradvermieter. Normalerweise genügt es ihm, wenn er Ihre Daten notiert und sich den Ausweis zur Überprüfung der Daten vorlegen lässt. Denn wenn Sie wirklich ein Halunke wären, würden Sie den Ausweis einfach bei ihm liegen lassen, dann mit dem Fahrrad verschwinden und sich mit der falschen Behauptung, den Ausweis verloren zu haben, bei der zuständigen Behörde einen neuen Ausweis besorgen.

Dass Sie den Ausweis hinterlegt haben, würde dem Vermieter dann auch nichts bringen.

Vorsicht schadet auch hier nicht

Ist das nicht alles übertriebene Vorsicht? Wohl kaum, denn der "Personalausweis mit Chip" könnte im Extremfall durchaus missbraucht werden. Dieses Risiko sollten Sie nicht eingehen, wenn kein nachvollziehbarer Grund dafür besteht.

Hat ein Patient Anspruch auf Name und Privatanschrift eines Krankenhausarztes?

Sie lassen sich im Krankenhaus operieren. Leider ist das Ergebnis aus Ihrer Sicht ein Desaster. Sie möchten Schadensersatz. Dazu wollen Sie nicht nur das Krankenhaus verklagen, sondern auch den Arzt, der Sie operiert hat. Können Sie vom Krankenhaus seinen Namen und seine Privatanschrift verlangen? Ein Urteil des Bundesgerichtshofs vom 20.1.2015 (Aktenzeichen VI ZR 137/15) hat diese Fragen geklärt.

Parallele Klagen gegen Krankenhaus und Krankenhausarzt

Dass jemand sowohl das Krankenhaus als auch den dort angestellten Arzt verklagen will, der ihn operiert hat, mag zunächst überraschen. Ein solches Vorgehen kann jedoch sinnvoll sein, insbesondere deshalb, weil für die Haftung des Krankenhauses einerseits und für die Haftung des Arztes andererseits unterschiedliche rechtliche Voraussetzungen gegeben sein können.

Will man gegen den Arzt vorgehen, braucht man zunächst einmal seinen Namen. Häufig wird er dem Patienten bekannt sein, manchmal (insbesondere bei Operationen in Notfallsituationen) jedoch auch nicht.

Zweifelsfrei: Anspruch auf den Namen des Arztes

Dass ein Patient einen Anspruch darauf hat, den Namen des Arztes zu erfahren, der ihn operiert hat, steht für den Bundesgerichtshof völlig außer Frage. Er begründet dies unter anderem damit, dass der Patient einen Anspruch auf Einblick in die Behandlungsunterlagen hat. In den Behandlungsunterlagen müssen alle wesentlichen Aspekte der Behandlung dokumentiert sein. Und zu den wesentlichen Aspekten gehört auch der Name des Operateurs.

Das Problem der "ladungsfähigen Anschrift"

Doch wie sieht es mit der Privatanschrift des Arztes aus? Auf die Idee, vom Krankenhaus auch die Privatanschrift des Arztes zu verlangen, kann ein Patient vor folgendem Hintergrund kommen:

- Wer jemanden verklagen will, braucht dazu eine "ladungsfähige Anschrift".
- Darunter ist eine Anschrift zu verstehen, unter der die Klage auf Veranlassung des Gerichts amtlich zugestellt werden kann. Nur dann liegt eine wirksame Klageerhebung vor.

Die Privatanschrift eines Krankenhausarztes ist in der Regel tabu (Bild: Hollygraphic/iStock/Thinkstock)

- Falls ein Arzt verklagt werden soll, der in einem Krankenhaus tätig ist, stellt sich deshalb die Frage, ob (nur) die Privatanschrift des Arztes als eine solche "ladungsfähige Anschrift" anzusehen ist.
- Wäre das tatsächlich der Fall, müsste der Patient diese Privatanschrift kennen, damit die Klage zugestellt werden kann.

Anschrift der Arbeitsstelle als ladungsfähige Anschrift

So stellt sich die Situation nach Auffassung des Bundesgerichtshofs jedoch gerade nicht dar. Vielmehr gilt Folgendes:

- Als ladungsfähige Anschrift genügt in der Regel die Anschrift der Arbeitsstelle des Arztes.
- Gerade bei Arzthaftungsprozessen ist es vielfach üblich, dass eine Zustellung an Krankenhausärzte unter der Anschrift der Klinik erfolgt.
- Schwierigkeiten bei dieser Verfahrensweise sind in der Praxis nicht bekannt geworden.

Zweckbindung der Privatanschrift gemäß Bundesdatenschutzgesetz

Abgesehen davon ist eine Klinik nach Auffassung des Gerichts durch das Bundesdatenschutzgesetz daran gehindert, die Privatanschrift des Arztes an Außenstehende herauszugeben.

Dafür gibt es mehrere Gründe:

- Die Privatanschrift besteht aus personenbezogenen Daten, die durch § 32 BDSG (Daten für Zwecke des Beschäftigungsverhältnisses) besonders geschützt sind.
- Die Privatanschrift hat die Klinik nur für die Zwecke des Beschäftigungsverhältnisses erhoben.
- Das schließt eine Herausgabe der Privatanschrift an Außenstehende aus, wenn sie für andere Zwecke als für das Beschäftigungsverhältnis genutzt werden soll.
- Die Nutzung zur Zustellung einer Klage ist ein solcher anderer Zweck. Es würde deshalb gegen den Grundsatz der Zweckbindung verstoßen, wenn die Klinik als Arbeitgeber die Privatanschrift hierfür herausgeben würde.

Ungelöster Sonderfall: Arzt inzwischen anderweitig tätig

Leider sagt das Gericht nichts dazu, wie zu verfahren ist, wenn der behandelnde Arzt inzwischen nicht mehr im Krankenhaus tätig ist. Dann scheidet eine Zustellung an ihn unter der Anschrift des Krankenhauses nämlich aus. Das Schweigen des Gerichts zu dieser Frage hat seinen Grund darin, dass sie für den konkreten Fall keine Rolle spielte.

Wie ein solcher Fall entschieden würde, muss als offen angesehen werden. Zwar gibt es ältere Rechtsprechung, die das Krankenhaus in einem solchen Fall als verpflichtet ansah, die letzte ihm bekannte Privatanschrift des Arztes herauszugeben. Damals gab es allerdings die Vorschrift des § 32 BDSG noch nicht. Deshalb erscheint es durchaus denkbar, dass der Patient in einem solchen Fall nach heutiger Rechtslage mit leeren Händen dastünde.

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

Wenn das Smartphone den PC ansteckt

Ein Windows-Trojaner kann einem Android-Tablet nichts anhaben, so jedenfalls glaubte man bisher. Inzwischen gibt es Schadsoftware, die Gerätegrenzen überwinden kann. Die Verbindung von Geräten wird dadurch noch gefährlicher.

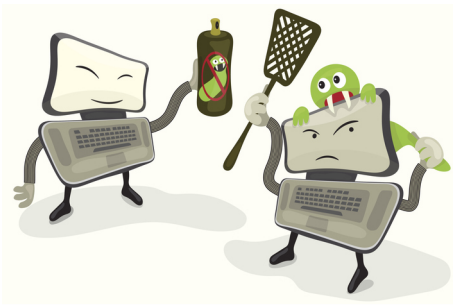
Was Malware mit dem Betriebssystem zu tun hat

Viele Nutzer von Apple-Geräten sind glücklich darüber, dass es für ihre Macbooks, iPhones und iPads kaum Schadprogramme gibt. Im Gegensatz dazu ist die Zahl der Viren, Würmer und Trojaner für Windows-Rechner geradezu riesig. Da könnte man sich doch fragen, warum eigentlich ein Windows-Trojaner kein Risiko für Apple-Geräte darstellen soll. Die Antwort liegt schlicht und ergreifend in den unterschiedlichen Betriebssystemen.

Schadprogramme nutzen gezielt Schwachstellen eines Betriebssystems und missbrauchen bestimmte Funktionen des jeweiligen Betriebssystems. Man kann sogar sagen, Schadprogramme laufen auf einem Betriebssystem, genau wie es legitime Programme tun. Ein Windows-Virus kann also mit einem Apple-Betriebssystem nicht zusammenarbeiten.

Malware musste bisher Grenzen beachten

Wenn ein Windows-Virus per E-Mail oder Internet-Download auf einen Apple-Rechner gelangen sollte, könnte er also keinen Schaden anrichten. Er könnte nicht aktiv werden. Denkbar jedoch wäre es, dass der Apple-Nutzer ungewollt den Windows-Virus in einer Textdatei an einen Windows-Anwender weiterleitet. Dort angekommen, könnte das Schadprogramm dann seinen kriminellen Zielen folgen.



Der ewige Kampf geht in die nächste Runde: Viren, Würmer & Co. sind mittlerweile in der Lage, Betriebssystemgrenzen zu überwinden. Antiviren-Software muss daher heutzutage entsprechend flexibel und umfassend sein. (Bild: belekekin/iStock/Thinkstock)

Die Schadfunktion von Malware ist also begrenzt. Diese Grenzen haben natürlich die Datendiebe schon lange gestört. Deshalb haben sich die Internetkriminellen etwas einfallen lassen.

Verbindung zwischen Geräten schafft gefährliche Brücken

Stellen Sie sich vor, Sie wollen Daten zwischen Ihrem Windows-PC und Ihrem Android-Smartphone austauschen, zum Beispiel Kontakte, Termine und Dokumente synchronisieren. Dazu nutzen Sie ein USB-Kabel oder vielleicht eine Bluetooth-Verbindung. Ganz gleich, wie Sie die Geräte verbinden: Es könnte eine Windows-Schadsoftware auf das Android-Smartphone gelangen oder umgekehrt ein Android-Trojaner auf den Windows-Rechner.

Nun werden Sie vielleicht sagen: Na und, es sind doch unterschiedliche Betriebssysteme. Es besteht also keine Gefahr. Doch leider besteht inzwischen sogar ein großes Risiko: Die Geräte könnten sich gegenseitig infizieren.

Kein Halt mehr an Betriebssystem-Grenzen

Sicherheitsforscher haben neuartige Malware-Typen entdeckt, die für mehrere Betriebssysteme gefährlich werden können. Damit reagieren die Datendiebe auf die Entwicklung, dass der typische Nutzer täglich zwei oder drei verschiedene Rechner nutzt, zum Beispiel den PC, das Tablet und das Smartphone als Mini-Computer.

Es gibt nun leider Schadprogramme, die zum Beispiel Android-Smartphones befallen und bei dem nächsten Kontakt mit einem Windows-Rechner auch diesen infizieren. Wie aber ist das möglich? Und was bedeutet das für Sie als Nutzer?

Windows-Viren können Android-Trojaner enthalten

Vorstellen können Sie sich die neuartige Malware wie ein Schadprogramm aus mehreren Schichten. Die erste Schicht gibt zum Beispiel vor, eine Anwendung (App) für Android-Smartphones zu sein. Wird die App installiert, kopiert die Malware gleich einen Ableger in das Austauschverzeichnis des Smartphones.

Dieser Ableger ist die zweite Schicht des Angriffs. Dort wartet nun die Schadsoftware auf Geräte, die mit dem Smartphone Daten austauschen wollen. Ist der Ableger eine Windows-Schadsoftware und wird ein Windows-Rechner mit dem Smartphone verknüpft, infiziert das Android-Smartphone den Windows-Computer. Dabei war die Windows-Malware gekapselt innerhalb des Android-Schadprogramms.

Doch auch die Umkehrung ist möglich: Windows-Malware kann einen Android-Virus enthalten, der Computer kann dann das Smartphone anstecken. Auch dabei wird ein Ableger in das Austauschverzeichnis kopiert.

Wer Daten von einem Gerät auf ein anderes kopiert oder Daten synchronisiert, muss damit rechnen, dass sich Schadsoftware auch Betriebssystem-übergreifend verbreitet (Bild: robuart/iStock/Thinkstock)

Viren-Scanner müssen mehrgleisig fahren

Entscheidend ist, dass Antivren-Programme zum Beispiel auf Windows-Computern auch nach Android-Schadsoftware suchen, denn darin könnte eine Schadfunktion enthalten sein, die auch dem Windows-System gefährlich wird.

Sie als Nutzer sollten daran denken, dass Schadprogramme nun auch die Grenzen von Geräten und Betriebssystemen überspringen können. Verbinden Sie zum Beispiel ein Android-Tablet und einen Windows-PC, kann es zu einer Computerviren-Infektion kommen. Nicht nur wir als Nutzer und unsere Geräte werden immer flexibler, auch die Schadprogramme und die Datendiebe werden es. Flexibilität bedeutet immer auch den Bedarf an flexibler Sicherheit.

So wird Ihre Datensicherung vollständig

Ein regelmäßiges Backup bringt wenig, wenn es lückenhaft ist. Fehlen wichtige Daten im Backup, kann die Datensicherung den Datenverlust nicht verhindern. Achten Sie deshalb auf umfassende Backups.

Flexible IT, verstreute Daten

So mancher PC-Nutzer erinnert sich noch an die Zeit, in der auf den Schreibtischen nur ein Bildschirm und eine Tastatur standen. Den Kasten mit Festplatten und CD-/DVD-Laufwerk unter dem Schreibtisch oder auf der Tischplatte gab es noch nicht. Die Daten befanden sich komplett auf einem zentralen Großrechner. Diese Zeit ist einerseits vorbei. Sie könnte aber andererseits wiederkommen, denn Cloud Computing in Reinform funktioniert letztlich ganz ähnlich.

Gegenwärtig jedoch befinden wir uns in der Zeit, in der die Daten auch lokal gespeichert werden können, auf den PCs, Notebooks, Tablets und Smartphones, um nur einige Typen von aktuellen Endgeräten zu nennen. Das macht die IT-Nutzung flexibler, man kann die lokal gespeicherten Daten auch ohne zentralen Serverzugang bearbeiten, zum Beispiel unterwegs im Zug, auch wenn es keine Internetverbindung zum Server oder zur Cloud gibt. Diese Flexibilität aber führt zu einer Verstreuung der Daten.

Backups haben oftmals "Löcher"

Verstreute Daten haben einige negative Konsequenzen: An verschiedenen Speicherorten liegen die gleichen Dateien mit unterschiedlichen Versionsständen. Bearbeitungen von Dateien finden womöglich an der falschen Version statt. Zudem besteht das hohe Risiko, dass nicht jede Version einer Datei auch dem Schutzbedarf entsprechend geschützt wird. Es kann durchaus sein, dass eine Datei auf dem PC verschlüsselt wird, auf dem Smartphone aber nicht. Wenn Dateien gelöscht werden sollen, ist es möglich, dass nicht alle Kopien der Dateien bei der Löschung berücksichtigt werden. Aber auch das Umgekehrte ist häufig der Fall: Bei der Sicherung der Daten werden Speicherorte übersehen. Handelt es sich um keine Datenkopien, sondern um verschiedene Dateien, ist das Backup unvollständig.

Viele Datensicherungen haben Mängel

Und das sind nicht die einzigen Probleme: Nicht nur die Zahl der regelmäßig genutzten Geräte steigt laufend an. Auch die Menge der zu sichernden Daten wächst und wächst. Wenn nun die Datensicherung zu selten erfolgt, wenn sie nicht der hohen Dynamik der Datenverarbeitung entspricht, befinden sich im Backup nicht die aktuellen Dateiversionen. Ein Datenverlust führt dann zumindest dazu, dass man zeitlich zurückgeworfen wird, dass also die Arbeit der letzten Stunden oder gar des gesamten Tages verloren ist.

Herausforderungen Mobilität und Cloud

Betrachtet man die Art der Lücken in Backups, so fehlen besonders oft die Daten, die auf den mobilen Endgeräten generiert und gespeichert wurden. Smartphones, Tablets und Notebooks werden immer noch bei der Datensicherung vergessen. Ähnlich verhält es sich mit der Cloud. Auch die Daten in einer Cloud müssen gesichert werden. Nur eine Übersicht über alle Verfahren der Datenverarbeitung, über alle genutzten Endgeräte und alle Speicherorte kann dabei helfen, die Lücken in den Backups zu schließen.

Denken Sie deshalb daran:

1) Wer zu selten Daten sichert, riskiert die Ergebnisse von Tagen und Wochen.

2) Daten, die unterwegs erfasst werden, können auch unterwegs verloren gehen, wenn es kein Backup gibt.

3) Auch Daten in der Cloud müssen gesichert werden, auch sie können verloren gehen.

4) Nur vollständige Backups schützen umfassend vor einem Datenverlust.

Ist Ihre Datensicherung komplett? Testen Sie sich!

Frage: Für das Backup bei Smartphones reichen die zusätzlichen Speicherkarten im mobilen Endgerät. Stimmt das?

a) Ja, denn dadurch sind die Daten an zwei Stellen gespeichert: im internen Speicher des Smartphones und zusätzlich auf der Speicherkarte.
b) Nein, denn wenn das Smartphone verloren geht, ist auch die Speicherkarte verloren.

Lösung: Die Antwort b) ist richtig. Das Backup muss getrennt von dem primären Speicherort erfolgen, also nicht etwa auf dem gleichen Gerät.

Frage: Regelmäßige Backups sind das A und O. Wichtig ist, dass die Datensicherung häufig genug erfolgt. Stimmt das?

a) Ja, die Häufigkeit der Backups ist sehr wichtig.
b) Ja, das stimmt. Zusätzlich müssen Backups aber auch vollständig sein.

Lösung: Die Antwort b) ist wieder richtig. Bei der Datensicherung entscheidet nicht nur die Frequenz, also die Häufigkeit der Backups, sondern auch die Vollständigkeit, also die Berücksichtigung aller relevanten Verfahren, Geräte und Speicherorte.

Frage: Wer seine Daten an möglichst vielen Stellen verteilt, erleichtert die Datensicherung, denn so gibt es viele Datenkopien. Stimmt das?

a) Nein, verstreute Daten erschweren die Datensicherung und sind eine Entwicklung, die es zu vermeiden gilt.
b) Ja, viele Datenkopien erhöhen die Wahrscheinlichkeit, dass es zu keinem vollständigen Datenverlust kommt. Eine Kopie bleibt in der Regel immer erhalten.

Lösung: Die Antwort a) ist richtig. Datensicherung bedeutet nicht, möglichst viele Kopien der Daten an beliebigen Stellen zu speichern. Datensicherung bedeutet vielmehr einen genau definierten Prozess, bei dem Kopien der zu sichernden Daten an kontrollierter, sicherer Stelle vorgehalten werden.