

Datenschutz Now!

10

Die Mitarbeiterzeitung rund um den Datenschutz



Liebe Leserin, lieber Leser,

beliebte private Geräte wie iPhone, iPad und Netbook eignen sich auch für den betrieblichen Einsatz. Doch die Vermischung von beruflicher und privater Nutzung kann gefährlich werden für die gespeicherten Daten. Wie ist es bei Ihnen? Trennen Sie die Nutzung von privaten und dienstlichen Geräten? Oder bringen Sie Ihre Daten unbewusst in Gefahr?

Wenn personenbezogene Firmendaten durch Ihr Verhalten verloren gehen, muss Ihr Arbeitgeber womöglich die Öffentlichkeit informieren. Das schädigt das Image der Firma und gefährdet vielleicht sogar Ihren Arbeitsplatz. Informieren Sie sich deshalb in dieser Ausgabe, wie sich der gute Ruf Ihres Arbeitgebers schützen lässt. Erfahren Sie zudem, auf welche Daten Ihr IT-Administrator wirklich zugreifen kann und was Ihnen passieren könnte, wenn jemand Ihren privaten WLAN-Zugang missbraucht.

Für Rückfragen stehe ich Ihnen gerne zur Verfügung! Ihr **Gilbert Staffler, Datenschutzbeauftragter**

Keine gute Mischung: Private Geräte und dienstliche Daten

Wenn Sie dienstliche E-Mails mit Ihrem privaten Smartphone abrufen, um auch nach Feierabend für die Firma erreichbar zu sein, tun Sie Ihrem Arbeitgeber nicht unbedingt einen Gefallen. Fragen Sie immer zuerst, ob Sie Firmendaten auf Ihren privaten Geräten vorhalten dürfen oder nicht.

Hoher Einsatz, hohes Risiko

Es ist wieder einmal spät geworden. Damit der Vorgang am nächsten Morgen wirklich fertig ist, sendet sich Herr Huber die Kundendaten auf sein privates E-Mail-Konto. Nach dem Abendessen wird er sie daheim mit seinem privaten Notebook bearbeiten. Was wie ein besonderer Einsatz für den Arbeitgeber klingt, kann schnell ins Auge gehen.

Arbeit im Home Office muss geregelt sein

Herr Hubers Arbeitgeber weiß nämlich nichts von der Arbeit nach Feierabend, auch nicht von der Übertragung der Kundendaten auf das private Notebook. Ohne eine Betriebsvereinbarung und ohne Erlaubnis des Vorgesetzten kann Herr Huber Ärger mit seinem Chef bekommen. Das ist keine Undankbarkeit, sondern es geht um den Schutz personenbezogener Daten.

Sicherheit privater Geräte ist unklar

Ein wesentliches Problem bei der Nutzung dienstlicher Daten mit Privatgeräten ist die

fehlende Kontrolle der Datensicherheit. Ob das private Smartphone, der private E-Mail-Dienst und das private Notebook den Sicherheitsanforderungen der Firma entsprechen oder nicht, kann Ihr Arbeitgeber nicht prüfen. Zudem ist unklar, wer alles auf Ihre Geräte zugreifen kann. Nutzen Sie zum Beispiel auch privat eine starke Verschlüsselung und komplexe Passwörter? Wer aus Ihrer Familie verwendet Ihre Geräte?



Eine geschäftliche E-Mail mal schnell auf dem privaten Gerät bearbeiten? Vorsicht!

Bitte keine eigenmächtigen Aktionen!

Wenn Sie einmal in die Situation kommen, nach Feierabend noch Firmendaten bearbeiten zu müssen, klären Sie zuerst die Voraussetzungen mit Ihrem Vorgesetzten. Können Sie ein Firmen-Notebook ausleihen,

dessen Sicherheit die Administration gewährleistet? Gibt es ein Pool-Smartphone, das Sie zur Verfügung gestellt bekommen können? Ganz gleich, wie die technischen Möglichkeiten in der Firma aussehen, machen Sie nichts eigenmächtig, was vertrauliche Daten in Gefahr bringen könnte.

Kein Geben und Nehmen!

Auch der umgekehrte Fall, die Privatnutzung von dienstlichen Geräten, ist ohne Zustimmung Ihres Arbeitgebers kein Kavaliersdelikt. Denn dabei werden Firmendaten in Gefahr gebracht. Denken Sie nur daran, was passieren kann, wenn Sie zum Beispiel Ihre Lieblingsmusik als MP3-Datei auf das Firmen-Laptop laden wollen und in Wirklichkeit ein Schadprogramm installieren, das Kundendaten ausspioniert.

Privates und Dienstliches nicht mischen

Aber auch aus Eigeninteresse sollten Sie weder dienstliche Daten auf Ihren Geräten nutzen noch Firmengeräte für eigene Zwecke einspannen. Denn dabei kommt es zu einer Mischung von privaten Daten mit Firmendaten. Greift etwa der Administrator nichts ahnend darauf zu, könnten intime Details aus Ihrem Privatleben offengelegt werden!

Ob Ihre Vorstellung von erlaubter und verbotener Gerätenutzung stimmt, erfahren Sie im Quiz auf Seite 4!

Informationspflichten bei Datenschutzpannen

Sie verlieren in der U-Bahn einen USB-Stick mit Daten von 20 Kunden. Sie denken sich: Außer Name, Anschrift, Telefonnummer und Bankkonto der Kunden ist nichts drauf. Das wird ja dann nicht gleich ein Drama sein? Von wegen: Der Vorfall ist ein Thema für den Vorstand!

Der USB-Stick fällt aus der Tasche, ...

Meist denkt man nur an böse Hacker, wenn das Thema "Personenbezogene Daten in falschen Händen" zur Sprache kommt. Den eigenen Leichtsinn verdrängt man lieber. Also wird der USB-Stick einfach in die Hosentasche gesteckt. Verschlüsselt sind die Daten auf dem Stick natürlich nicht.

... der Laptop bleibt im Taxi liegen

Und mit dem Laptop, der kürzlich hinten im Taxi liegen geblieben ist, ging es gerade noch einmal gut: Der nächste Fahrgast war ein ehrlicher Mensch, hat das Gerät dem Taxifahrer in die Hand gedrückt, und der hat es in der Taxizentrale abgegeben. Verschlüsselung der Festplatte? Natürlich Fehlangelegenheit, denn dann kommt man ja auch selbst nicht mehr so leicht an die Daten!

Beide sind nicht mehr zu finden

Aber was ist, wenn der USB-Stick und der Laptop verschwunden bleiben und wegen der fehlenden Verschlüsselung sich jeder, der sie findet, die Daten ohne Mühe anschauen kann?

Das Gesetz sieht Informationspflichten vor

Spätestens dann stößt man auf eine Regelung, die erst im Jahr 2009 eingeführt wurde. Ihre etwas sperrige Überschrift lautet "Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten". Zu finden ist sie in § 42a des Bundesdatenschutzgesetzes.

Dort ist festgelegt, dass in bestimmten Situationen die betroffenen Personen und außerdem auch noch die zuständigen Datenschutzaufsichtsbehörden benachrichtigt werden müssen, wenn Daten in die Hände von Außenstehenden geraten sind. Und die Voraussetzungen dafür sind schneller gegeben, als viele glauben!

Davon sind auch Daten über Bankkonten betroffen

Viele denken, das könne nur ganz besonders brisante Daten, etwa medizinische Diagnose-daten, betreffen. Solche Daten sind von der



Verlorene Geräte wie USB-Sticks, die z.B. Kundendaten enthalten, können viel Unheil anrichten

Vorschrift selbstverständlich erfasst. Dasselbe gilt für Daten, die etwas über die Gewerkschaftszugehörigkeit, die Religion oder die ethnische Herkunft aussagen.

Also nichts, was für die Praxis besonders relevant ist? Von wegen: Es genügt auch, wenn es um Daten zu Bank- oder Kreditkartenkonten geht. Solche Daten sind in fast jedem Datensatz enthalten, der Kunden betrifft.

Wehe, wenn sie in unrechte Hände geraten

Weiterhin setzt die Regelung voraus, dass Außenstehende unrechtmäßig Kenntnis von den Daten erlangt haben. Verschwindet ein USB-Stick oder ein Laptop, dann ist das meistens zu befürchten - jedenfalls dann, wenn die Daten nicht verschlüsselt sind. In diesem Fall unterstellt die Datenschutzaufsicht in der Regel, dass Außenstehende an die Daten gekommen sind.

Die Vorschrift wird also recht weit ausgelegt. Ihrem Wortlaut nach würde sie voraussetzen, dass Außenstehende Daten tatsächlich zur Kenntnis genommen haben. Da man oft nicht weiß, ob es dazu gekommen ist, lässt man es aber zum Schutz der Betroffenen genügen, wenn Außenstehende Daten zur Kenntnis nehmen konnten.

Mit Missbrauch ist zu rechnen

Als weitere Voraussetzung muss den Umständen nach davon auszugehen sein, dass für die betroffenen Personen schwerwiegende Beeinträchtigungen drohen.

Dafür reicht es schon aus, dass etwa Bankdaten benutzt werden können, um Überweisungen zu fälschen. Nur selten lässt sich die Datenschutzaufsicht auf die Argumentation ein, dass mit einer schwerwiegenden Beeinträchtigung der Betroffenen nicht zu rechnen ist. Vor allem wenn unklar ist, welche Personen genau betroffen sind, wird sie das auf keinen Fall tun.

Die Zahl der Betroffenen spielt keine Rolle

Um die Daten von wie vielen Personen es geht, ob also etwa zehn oder 1.000 Kunden betroffen sind, ist ohne Belang. In jedem Fall müssen alle Betroffenen über den Vorfall informiert werden, und auch die zuständige Datenschutzbehörde ist zu unterrichten.

Im Extremfall ist eine öffentliche Bekanntmachung notwendig

Lässt sich nicht feststellen, welche Personen betroffen sind (etwa weil Sie nicht genau wissen, von welchen Kunden Sie Daten auf den Geräten hatten), verlangt das Gesetz sogar "die Information der Öffentlichkeit durch Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen."

Das Ganze ist ein Thema für den Vorstand

Solche Vorgänge sind keine Routine. Es liegt deshalb auf der Hand, dass sich außer der IT-Sicherheit auch der Vorstand damit befassen wird. Schließlich muss man damit rechnen, dass die Medien aufmerksam werden. Und dann steht rasch das Ansehen des ganzen Unternehmens auf dem Spiel.

Sie sollten sich informieren

Sie meinen, dann wäre es doch besser, sich einmal mit dem Thema Verschlüsselung bei Laptops, mobilen Festplatten, USB-Sticks usw. zu befassen? Ihr Datenschutzbeauftragter kann Ihnen dazu gerne Informationen geben.

Impressum

Redaktion:

Gilbert Staffler
Datenschutzbeauftragter

Anschrift:

EHS-Datentechnik
Uhlendahlweg 24
45279 Essen
Telefon: 0201-530091
E-Mail: info@ehs-datentechnik.de

Der Administrator: Was darf er wirklich?

Die Systemadministratoren haben sehr weitreichende Berechtigungen, um im Netzwerk alles regeln zu können. Geregelt ist aber auch, dass sie nicht auf alle Daten zugreifen dürfen, auf die sie Zugriffsmöglichkeiten haben.

Private E-Mails sind tabu

"Und wie war Dein Urlaub auf Teneriffa?", beginnt ein Gespräch unter Kollegen. "Warum fragst Du? Als Administrator hast Du doch bestimmt schon meine E-Mails gelesen, die ich dazu verschickt habe." Diese Antwort betrübt den Administrator. "Glaubst Du wirklich, das würde ich tun? Das darf ich nicht, und das mache ich nicht."

Umfassende Zugriffsmöglichkeiten

Was der Administrator aber nicht sagt, ist, dass er dies nicht könnte. Tatsächlich hat ein Administrator sehr umfassende Möglichkeiten, auf die Daten im Netzwerk zuzugreifen. Diese Rechte muss er auch haben, um seinen Aufgaben nachgehen zu können.

Allerdings sind bestimmte Bereiche auch für Administratoren Sperrgebiet. Das gilt insbesondere dort, wo eine Privatnutzung erlaubt ist, also zum Beispiel bei privaten E-Mails oder bei der erlaubten privaten Nutzung des dienstlichen Internetanschlusses.



Ein Administrator benötigt viele Rechte; er darf sie aber nur unter bestimmten Umständen einsetzen

Keine gläsernen Mitarbeiter

Es gibt noch andere kritische Bereiche, in die der Administrator Einblick nehmen könnte, dies aber entsprechend den dienstlichen und gesetzlichen Vorgaben nicht macht. Fast jede Software und nahezu jedes Gerät generiert Protokolle über die Nutzung. Würde der Administrator diese Protokolle gezielt auswerten, wären Informationen über einzelne Mitarbeiter zu finden, zum Beispiel wann sie welche Anwendung genutzt haben, welche Internetseite mit dem Webbrowser aufgerufen wurde und wann der Computer vor Feierabend abgeschaltet wurde.

Doch solche Auswertungen dürfen nicht einfach vorgenommen werden, darauf achten Ihr Datenschutzbeauftragter und natürlich auch der Administrator selbst.

Auch Administratoren werden überprüft

Administratoren haben eine Vertrauensstellung im Unternehmen, aber auch sie werden kontrolliert, wenn es um den Schutz personenbezogener Daten geht. So können die Administrationsaufgaben auf mehrere Schultern verteilt werden, um eine gegenseitige Prüfung nach dem Vier-Augen-Prinzip zu ermöglichen. Zusätzlich werden alle sicherheitsrelevanten Aktivitäten der Administratoren protokolliert und unter anderem von Ihrem Datenschutzbeauftragten überprüft.

Passwörter werden nur verschlüsselt im System abgelegt

Zum Schutz der Benutzerzugänge vor unerlaubten Zugriffen werden zudem die Passwörter der Mitarbeiterinnen und Mitarbeiter nur verschlüsselt in den Systemen abgelegt. Das verhindert, dass ein Dritter das Benutzerkonto und damit die Identität übernimmt. Auch Administratoren dürfen die Benutzerpasswörter nicht kennen und werden nicht danach fragen. Wenn Sie Ihr Passwort vergessen, kann Ihnen auch der Administrator nicht damit aushelfen, sondern er setzt Ihr Benutzerkonto zurück, damit Sie sich ein neues Passwort vergeben können.

Administrationsrechte spärlich vergeben

Eine weitere Maßnahme zur Kontrolle der Administrationstätigkeiten besteht darin, möglichst wenigen Personen Administratorrechte zu erteilen. Auch Sie selbst als Anwender sollten sparsam mit Administrationsrechten umgehen.

Falls Sie für Ihren Arbeitsplatzrechner, Ihr Firmen-Notebook und/oder Ihr Firmen-Smartphone über einen Zugang als lokaler Administrator verfügen, sollten Sie ihn immer nur dann verwenden, wenn Sie erlaubte Änderungen an Ihren Endgeräten vornehmen. Das macht allerdings in der Regel Ihr Administrator, oder er sagt Ihnen konkret, was Sie als lokaler Administrator machen sollen.

Administratoren sind wichtige Partner für Datenschutz und Datensicherheit - und keine Spione im eigenen Netzwerk. Beachten Sie dazu einige goldene Regeln für die Zusammenarbeit mit Ihrer Systemadministration:

1. Systemadministratoren haben weitreichende Berechtigungen, um die Sicherheit und die Funktionstüchtigkeit im Netzwerk zu gewährleisten.
2. Systemadministratoren dürfen und werden nicht auf Ihre privaten Daten zugreifen, wenn Sie diese mit Erlaubnis im Netzwerk oder auf Endgeräten vorhalten.
3. Wenn Sie Fragen zur Systemadministration haben, sprechen Sie die Administratoren an. Bei Fragen zum Schutz Ihrer Daten wenden Sie sich an Ihren Datenschutzbeauftragten.
4. Geben Sie keine Passwörter weiter, auch nicht an die Administratoren.
5. Verschlüsseln Sie die Daten entsprechend den internen Vorgaben. Das ist kein Misstrauen gegen die Administratoren, sondern ein Schutz gegen Unbefugte.
6. Beschränken Sie Ihre eigenen Administrationsrechte. Nutzen Sie Endgeräte immer nur dann als lokaler Administrator, wenn es unbedingt erforderlich ist. Insbesondere sollten Sie kein Internet nutzen, wenn Sie als lokaler Administrator angemeldet sind.

Auch an daheim denken

Für Ihren privaten Computer oder den Rechner im Home Office gilt das Gleiche: Nutzen Sie auch hier den Zugang als lokaler Administrator nicht dauerhaft. Das gilt insbesondere dann, wenn Sie den Rechner für das Internet nutzen.

Administrationsrechte sind begehrt

Während die Arbeit eines Administrators fordernd und verantwortungsvoll ist, sind die Administratorrechte sehr begehrt. Diese Rechte zu erlangen, ist das erste Ziel eines Hackers und einer Schadssoftware. Unbefugte Dritte nämlich werden diese Rechte ausnutzen und missbrauchen. Ihr Administrator hingegen setzt seine Berechtigungen zum Schutz der Systeme und Ihrer Daten ein.

Missbrauch eines WLAN

Sie betreiben zuhause ein WLAN. Dass Böswillige dort von außen eindringen könnten, halten Sie kaum für möglich. Schließlich mussten Sie damals bei der Installation einen langen Authentifizierungsschlüssel eingeben. Nach Ihrem Urlaub liegt in Ihrem Briefkasten das Schreiben eines Rechtsanwalts. Er beschuldigt Sie, dass Ihr WLAN benutzt wurde, um Urheberrechte zu verletzen. Er fordert sogar Schadensersatz. Das gibt es nicht? Lesen Sie lieber erst einmal weiter!

"Sommer unseres Lebens" - im Fall, den der Bundesgerichtshof am 12.5.2010 entschieden hat, ging es um einen harmlosen Schlager, der diesen Titel trägt. Das Musikstück war über ein WLAN auf einer Tauschplattform im Internet zum Download angeboten worden. Das Ganze natürlich hinter dem Rücken des Künstlers und ohne dass dafür irgendetwas an ihn gezahlt worden wäre.

Fachfirmen spüren illegale Downloads auf

Verständlich, dass er sich das nicht gefallen lassen wollte. Weil es ihm ständig so ging, hatte er ein Fachunternehmen damit beauftragt, solche illegalen Download-Vorgänge im Internet mit einer speziellen Software aufzuspüren. Die Software kann natürlich keine Namen von Computerbesitzern ermitteln. Sie kann aber die IP-Adresse feststellen, unter der ein PC mit dem Internet verbunden ist.

Rechtsanwälte ermitteln den Namen des WLAN-Betreibers

Der Rest war dann anwaltliche Routine: Es wird Strafanzeige wegen Verletzung des Urheberrechts erstattet. Polizei und Staatsanwaltschaft ermitteln über den jeweiligen Internet-Provider (etwa die Telekom), wem die IP-Adresse zum Zeitpunkt des Downloads zugeordnet war. Der Anwalt beantragt Akteneinsicht und kommt so an den Namen dessen, der beim Provider als Nutzer angemeldet ist.

Ihr WLAN geht Sie etwas an!

Wer ein WLAN betreibt, kann nicht so tun, als ginge es ihn gar nichts an, wenn ein anderer dieses WLAN für illegale Aktivitäten missbraucht. Schließlich hat nur er die Möglichkeit, ausreichende Absicherungen gegen Missbrauch vorzusehen.

Sie müssen es "verkehrsüblich" absichern

Der Bundesgerichtshof vertritt die Auffassung, wer ein WLAN betreibt, müsse "verkehrsübliche Sicherungsmaßnahmen" gegen Missbrauch treffen. Dazu zählt vor allem eine aus-

reichende Verschlüsselung, die unbefugte Zugriffe von außen verhindert.

Tun Sie dies nicht, müssen Sie haften

Fehlt sie, müssen Sie als Betreiber des WLAN auch für den Missbrauch durch Außenstehende geradestehen. Die Folge: Sie müssen dann beispielsweise Schadensersatz für die Verletzung von Urheberrechten zahlen, obwohl Sie selbst gar nichts getan haben und im Extremfall - so wie hier - sogar im Urlaub waren, als der illegale Download stattfand. Wann aber ist eine Verschlüsselung ausreichend?

Einfache WPA-Verschlüsselung reicht nicht

Das Gericht legt sich nicht für alle Fälle fest, weil natürlich stets der Einzelfall betrachtet werden muss. Zwei Dinge sind der Entscheidung aber recht klar zu entnehmen:

1. Falls ein WLAN noch mit einer WPA-Verschlüsselung arbeitet, reicht das nicht aus.
2. Längere Schlüssel (etwa solche mit 32 Stellen) sind wesentlich sicherer als die früher üblichen Schlüssel mit 16 Stellen.

Forschen Sie lieber einmal nach!

Muss man Technikfreak sein, um die Anforderungen des Gerichts erfüllen zu können? Nein! Im Allgemeinen können Sie in den Unterlagen zu Ihrem Router leicht erkennen, ob er noch "WPA" verwendet oder ob Sie dort eine andere Abkürzung finden. Mehr müssen Sie zunächst nicht wissen. In jedem Fall gilt: Schauen Sie lieber nach, wie es mit der Verschlüsselung Ihres WLAN aussieht. Und wenn Sie sich selbst nicht auskennen, ziehen Sie den Fachmann hinzu, der Ihnen das Netz installiert hat.

Test: Vermischen Sie private und dienstliche Daten?

Frage: Für Ihr neues Projekt bekommen Sie ein Firmen-Notebook gestellt. Daheim zeigen Sie stolz das tolle Modell mit der hohen Bildschirmauflösung. Ihr Sohn bittet Sie, damit das neue Musikvideo seiner Lieblingsband ansehen zu dürfen. Würden Sie ja sagen?

- a) Ausnahmsweise, denn Musikvideos sind ungefährlich, und im Unternehmen wird es keiner merken.
- b) Wenn das Notebook zur rein dienstlichen Nutzung überlassen wurde, darf auch kein Musikvideo damit abgespielt werden.
- c) Nein, denn auch Musikvideos können mit Schadprogrammen präpariert sein, die die Firmendaten auf dem Notebook gefährden können.

Lösung: Antwort b) und c) sind richtig. Datendiebe nutzen zurzeit besonders gerne den Aufruf eines Musikvideos, um Malware zu installieren. Zudem darf die Einschränkung auf eine dienstliche Nutzung auch nicht für die eigenen Kinder missachtet werden.

Frage: Ihr neues Smartphone unterstützt zehn E-Mail-Konten gleichzeitig. Da wäre es doch eine Verschwendung, nicht alle E-Mails abzurufen, sowohl die privaten als auch die dienstlichen. Ist das aus Ihrer Sicht in Ordnung?

- a) Solange die dienstlichen E-Mails und die privaten E-Mails in verschiedenen Ordnern auf dem Smartphone gespeichert werden, besteht kein Risiko.
- b) Mein Chef macht das so, glaube ich. Warum sollte ich nicht auch mein Smartphone richtig nutzen?
- c) Ohne Zustimmung meines Arbeitgebers darf ich keine dienstlichen E-Mails auf mein privates Smartphone laden.

Lösung: Richtig ist nur Antwort c). Voraussetzung sind immer die Zustimmung des Arbeitgebers und die Absicherung des Geräts, damit keine Daten in Gefahr geraten können. Verschiedene E-Mail-Ordner für Dienstliches und Privates stellen keine Sicherheit dar.