Infobrief Datenschutz
Ausgabe 06 | 2013

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

richtiges Kommunizieren will gelernt sein. In dieser Ausgabe erfahren Sie deshalb, worauf Sie achten sollten, wenn Sie E-Mails an zahlreiche Empfänger senden möchten. Viele Personen erreichen Sie auch über eines der sozialen Netzwerke. Was Sie lieber nicht bei Facebook & Co. veröffentlichen sollten, verrät Ihnen der zweite Beitrag.

Auch beim Umgang mit mobilen Endgeräten gibt es wichtige Verhaltensregeln. Sie erhalten diesmal zentrale Sicherheitshinweise, wie Sie den Diebstahl Ihrer Geräte und damit der darauf gespeicherten Daten verhindern können. Speichern können Sie Ihre Daten auch im Internet. Doch vor Diebstahl sind die Daten auch hier nicht geschützt, wenn Sie nicht an die Verschlüsselung denken. Nutzen Sie den Wissenstest auf der letzten Seite, um Ihr Verhalten beim Speichern im Internet zu prüfen.

Passen Sie gut auf sich und Ihre Daten auf,

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

"cc" und "bcc" bei Mails - ein gewaltiger Unterschied!

Mails sind gerade dann praktisch, wenn ein identischer Text viele Adressaten auf einmal erreichen soll. Doch Vorsicht: Wissen Sie, wann Sie mit "cc" arbeiten dürfen und wann der Datenschutz das "bcc" notwendig macht? Sie sind sich da völlig sicher? Lesen Sie lieber erst einmal weiter!

Ein Praktikant darf Fragebögen per Mail verschicken

Ein BWL-Student war sehr froh darüber, dass er bei einer angesehenen Personalberatung ein Praktikum machen durfte. Man erlaubte ihm sogar, per Mail einen Fragebogen an die Kunden der Personalberatung zu versenden, um so Informationen für seine Hausarbeit einzuholen.

Leider hatte er keine Ahnung, wie man das richtig macht

Das ging dann allerdings gründlich schief. Er kopierte nämlich die komplette Adressenliste einfach in das "An"-Feld hinein. Die Folge: Für alle Adressaten war offen sichtbar, wer denn sonst noch zu den Kunden des Unternehmens zählte. Das Praktikum war natürlich sofort beendet. Was mit dem Betreuer des Praktikanten geschah, ist nicht bekannt.

"An" plus "bcc" hätten weitergeholfen

Richtig wäre es gewesen, wenn der Praktikant die Mail im "An"-Feld an sich selbst gerichtet und die Adressenliste dann in das "bcc"-Feld eingefügt hätte. Denn was im "bcc"-Feld steht, ist zwar für den Absender der Mail sichtbar, aber nicht für die Adressaten, an die sich die Mail richtet.

"An" plus "cc" - das liegt meist daneben!

Nichts geholfen hätte es übrigens, wenn der Praktikant statt des "bcc"-Feldes das "cc"-Feld benutzt und die Adressenliste dort eingefügt hätte. Denn alles, was in diesem Feld steht, ist genauso wie alles, was im "An"-Feld steht, für alle Adressaten der Mail sichtbar!

Vorsicht: Nicht immer sollen alle Empfänger einer E-Mail voneinander wissen. (Bild: Thinkstock)

Machen Sie doch mal einen Test!

Falls Sie glauben, dass das heute doch jeder weiß, fragen Sie einmal einige Kolleginnen oder Kollegen, gerne auch jüngere! Sie werden sich über das Ergebnis sehr wahrscheinlich wundern. Denn dass jemand dieselbe Mail an viele Adressaten verschicken will, ohne dass die Adressaten voneinander wissen, kommt eher selten vor, und deshalb wissen viele nicht, was dabei zu beachten ist.

Unternehmensleitung ist verantwortlich

Dass es ein Datenschutzverstoß ist, wenn eine komplette Kundenliste frei zugänglich per Mail verschickt wird, dürfte klar sein. Und selbstverständlich kann das entsprechende Maßnahmen der Datenschutzaufsicht nach sich ziehen, zum Beispiel die Verhängung eines Bußgeldes gegen die Unternehmensleitung. Denn sie ist verantwortlich, wenn es im Unternehmen zu Datenschutzverstößen kommt.

Was bedeuten eigentlich die beiden Abkürzungen?

Sie interessiert, was die Abkürzungen "cc" und "bcc" eigentlich bedeuten? Sie wurden aus der Bürowelt der Zeit übernommen, in der es noch gar keine Mails gab. "cc" heißt "carbon copy" und meint eine Kopie, die für jeden sichtbar ist. "bcc" bedeutet dagegen "blind carbon copy", also "Blindkopie" im Sinn von "für die anderen Adressaten nicht sichtbare Kopie".

Rüpeleien in sozialen Netzwerken

Manche Menschen scheinen in Facebook & Co. alle Grenzen zu vergessen. Da fallen dann Begriffe, die man im direkten persönlichen Gespräch kaum jemals zu hören bekommt. Wenn das schließlich Konsequenzen hat, ist das Entsetzen oft groß. Deshalb gilt gerade hier: Erst denken, dann schreiben! Lesen Sie, was zu beachten ist und wie Sie sich als Opfer im Ernstfall wehren können.

Die Realität ist manchmal erschreckend

"Du bist ein Klugscheißer, der wohl schlechten Sex gehabt hat. Wahrscheinlich hat dir zudem noch jemand ins Gehirn gesch ...".

Können Sie sich vorstellen, dass jemand einem Kollegen oder einer Kollegin solche Unverschämtheiten direkt ins Gesicht sagt? Wohl kaum. Und doch handelt es sich hier um Original-Formulierungen aus einem Facebook-Eintrag, die einen Vorgesetzten beschreiben sollten. Der Arbeitgeber hat mit der - natürlich fristlosen - Kündigung des Schreiberlings reagiert, weil er sich eine solche Schilderung schon im Interesse des Betriebsfriedens nicht gefallen lassen wollte.

Aber auch wenn man einmal von solchen Extremfällen absieht: Was man sonst so in Facebook & Co. ganz alltäglich über Kollegen, Nachbarn usw. zu lesen bekommt, ist oft noch drastisch genug. Unwillkürlich fragt man sich, woher solche Verhaltensweisen kommen.

Der Wohnzimmereffekt - eine tückische Sache!

Ein wesentlicher Grund dürfte eine Art Wohnzimmereffekt sein. Man meint, in einem solchen Netzwerk letztlich "unter sich" zu sein. Denn schließlich spricht man ja nur seine "Freunde" an.

Zu oft wird dabei leider vergessen, dass Einträge etwa bei Facebook völlig offen für jeden sind, solange man die entsprechenden Voreinstellungen dieses Systems nicht geändert hat. Und zu wenige denken daran, dass auch eine Eintragung, die tatsächlich nur für die "Freunde" sichtbar ist, letztlich eben doch eine Art öffentliche Bekanntmachung darstellt, wenn man beispielsweise 110 "Freunde" hat (so in einem Fall, der real von den Gerichten entschieden wurde!).

Im ersten Zorn geschrieben, ...

Zudem verleiten soziale Netzwerke dazu, etwas sofort im ersten Zorn zu schreiben, womöglich noch direkt am Arbeitsplatz, wenn es dort gerade Ärger gab. Das stets verfügbare Smartphone macht es besonders leicht. Und dann schreibt keineswegs nur der Azubi, der gerade wegen eines Fehlers gerüffelt wurde, schnell einmal Sätze wie "Die Bereichsleiterin ist eine frustrierte Zicke."

Wer sich in sozialen Netzwerken über seine Kollegen oder seinen Arbeitgeber äußert, sollte darauf achten, was er von sich gibt (Bild: Thinkstock)

... und andere hängen sich an!

Im kleinen Kreis gesagt, gehört sich ein solcher Satz zwar nicht, er ist aber normalerweise auch keine Katastrophe. Anders sieht es aus, wenn er in einem sozialen Netzwerk steht und von Dutzenden von Personen (oder sogar von jedem, der es möchte) gelesen werden kann. Dann hat er eine Art Multiplikationseffekt. Denn oft sehen sich andere dazu animiert, solche Äußerungen zu kommentieren, ihnen zuzustimmen oder sie durch weitaus üblere Formulierungen sogar noch zu toppen. Der Weg zu einem regelrechten Mobbing ist dann nicht mehr weit.

Was ein Opfer bedenken sollte

Was kann man tun, wenn man selbst das Opfer solcher Äußerungen ist? Natürlich ist es möglich, den Betreffenden, etwa einen Arbeitskollegen, direkt darauf anzusprechen. Das aber will genau überlegt sein. Denn leider hat diese Reaktion manchmal einen unerwarteten Effekt: Der eine oder andere meint, auf die im Netz schon vorhandenen Äußerungen noch eins draufsetzen zu müssen, weil er das Verhalten des Opfers so interpretiert, dass er die erhoffte Demütigung tatsächlich erreicht hat.

Holen Sie sich Unterstützung!

Deshalb ist zu empfehlen, bei einem solchen Gespräch immer jemanden dabei zu haben, der einen unterstützt, und ein solches Gespräch auch nur zu führen, wenn man sich ihm gewachsen fühlt. Wenn die Angelegenheit mit dem Arbeitsverhältnis zu tun hat, hilft oft der Betriebsrat weiter. Ansonsten sollte man sich nicht scheuen, Vorgesetzte mit der Sache zu befassen und sie um Unterstützung zu bitten. Eine Abmahnung ist rechtlich ebenso möglich wie eine Kündigung ohne Abmahnung, jedenfalls dann, wenn die Äußerungen in einem sozialen Netzwerk entsprechend drastisch sind.

Im Extremfall sind rechtliche Schritte nötig

Falls die Äußerungen nichts mit dem Arbeitsverhältnis zu tun haben, bleibt oft nur der Weg zum Rechtsanwalt. Er kann mehr erreichen, als viele glauben. Äußerungen, die das Persönlichkeitsrecht verletzen, vor allem Beleidigungen, führen zu Unterlassungsansprüchen. Solche Ansprüche lassen sich durchaus rasch durchsetzen, etwa im Wege einer einstweiligen Verfügung, die bei Gericht beantragt wird. Im Extremfall kommt auch ein strafrechtliches Vorgehen in Betracht. Bei dem groben Zitat am Anfang dieses Beitrags wäre es sicher möglich gewesen.

Soziale Netzwerke - an sich eine gute Sache!

Bei allen Problemen, die hier geschildert wurden, sollte man freilich nicht vergessen: Soziale Netzwerke sind eine gute Möglichkeit, Kontakte zu halten und sich auszutauschen! Und Rüpeleien sind auch dort die Ausnahme. Damit das so bleibt, sollte man darauf bestehen, dass bestimmte Regeln eingehalten werden - und das natürlich auch selbst tun.

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

Das kann mir nicht passieren?!

Ein Notebook prall gefüllt mit vertraulichen Daten verschwindet. Zu allem Überfluss sind die Daten unverschlüsselt. Für das betroffene Unternehmen ist dies eine Katastrophe. Sind Sie vor solch einem Diebstahl gefeit?

Es passiert immer wieder

Ende April 2013 teilte die Stadt Schneverdingen in Niedersachsen mit, dass ein Notebook mit Daten von Bürgern gestohlen wurde; Bankverbindungen mit Namen und Adressen sind betroffen. Die Daten waren zum Zweck der Softwareanalyse auf dem Notebook eines mit der Analyse beauftragten Berliner Unternehmens gespeichert.

Gestohlen wurde das Notebook bei einem Einbruch beim Dienstleister. Auch wenn das Notebook und die Anwendung mit einem Passwort geschützt waren, warnt die Stadtverwaltung vor einem möglichen Missbrauch der Daten. Dieser Notebook-Diebstahl ist leider keine Seltenheit.

Mobile Geräte, leichte Beute

Notebooks sind ein beliebtes Diebesgut, wie zum Beispiel der aktuelle Bericht eines Sicherheitsanbieters unterstreicht: Ob ein einzelnes Firmen-Notebook, das aus einer Mitarbeiterwohnung gestohlen wurde, die zehn Laptops einer Musikproduktionsfirma, die aus einem Fahrzeug entwendet wurden, oder mehrere Notebooks von Technologieunternehmen, die sich der Hausmeister des Bürogebäudes auf kriminellem Weg beschafft hat - das Sicherheitsunternehmen berichtet von 28.000 Fällen, bei denen der Diebstahl aufgeklärt werden konnte. Die Gesamtzahl der Notebook-Diebstähle liegt noch viel höher.

Notebooks sind ein beliebtes Ziel von Dieben. Dabei können leicht Kundendaten oder Geschäftsgeheimnisse in die falschen Hände geraten.
(Bild: Thinkstock)

Geräte aufgespürt, Daten trotzdem in Gefahr

Ohne spezielle Sicherheitssoftware, die im Verlustfall oder bei Diebstahl eine Ortung des Geräts erlaubt, verschwinden die meisten Notebooks auf Nimmerwiedersehen. Die wenigen Geräte, die wiedergefunden werden, tauchen zum Teil in Leihhäusern, Second-Hand-Shops und bei nichts ahnenden Händlern und Käufern wieder auf.

Doch selbst wenn sie bei den Dieben gefunden werden, sind nur die Geräte in Sicherheit. Was mit den Daten geschehen ist oder noch geschehen kann, ist unklar.

Kopien der Daten im Umlauf

Ungeschützte Daten lassen sich beliebig kopieren und verteilen. Nicht umsonst wies der betroffene Dienstleister der Stadt Schneverdingen darauf hin, dass auch bei einer möglichen Festnahme des oder der Einbrecher, sofern dies überhaupt geschehen werde, die Gefahr nicht gebannt sei. Der Grund: Die Bankdaten können nicht nur von dem Einbrecher missbraucht werden, sondern natürlich auch von anderen, wenn die Daten bereits in Umlauf gelangt sind.

Notebook im Blick, Daten verschlüsselt

Wenn Sie ein Notebook oder ein anderes mobiles Gerät wie einen Tablet-PC oder ein Smartphone nutzen, sollten Sie an das hohe Diebstahlrisiko denken. Schließlich ist das Gerät nicht nur für Sie leicht zu transportieren, sondern auch für Langfinger. Es reicht allerdings nicht, zum Beispiel das Notebook in einen Schrank zu schließen oder das Smartphone nie unbeobachtet auf dem Tisch liegen zu lassen.

Diebe suchen und finden Wege, mobile Geräte zu stehlen, wie die erwähnten Beispiele zeigen. Im Extremfall hat der Dieb sogar Zugang zu Ihrem Büro, zu Ihrer Wohnung oder zum Schrank. Deshalb darf die Verschlüsselung vertraulicher Daten nie fehlen. Denken Sie immer daran: Sind ungeschützte Daten erst einmal kopiert, hilft auch das Aufspüren des gestohlenen mobilen Geräts wenig für den Datenschutz!

So machen Sie Notebook-Dieben das Leben schwer

1. Lassen Sie Notebook, Tablet-PC und Smartphone nie unbeobachtet liegen.

2. Selbst Ihr Gang zum Waschraum oder zum Kaffeeautomaten kann einem Dieb genug Zeit geben, um das mobile Gerät zu stehlen.

3. Verstecken Sie das mobile Gerät nicht nur, sondern schließen Sie es weg.

4. Lassen Sie den Schlüssel zum Aufbewahrungsort nicht auf dem Tisch liegen oder einfach stecken.

5. Achten Sie auch unterwegs auf Ihre mobilen Geräte, nicht nur im Gedränge, sondern bei jeder Gelegenheit.

6. Nutzen Sie ein starkes Gerätepasswort und aktivieren Sie die Funktion, die Ihr Gerät bei kurzer Inaktivität in einen gesperrten Zustand versetzt.

7. Verlassen Sie sich weder auf die Kette am Notebook noch auf das Gerätepasswort allein, sondern verschlüsseln Sie alle vertraulichen Daten.

8. Geht doch einmal ein Notebook, Tablet-PC oder Smartphone verloren, dann zögern Sie nicht, sondern melden Sie sofort den Verlust oder Diebstahl der Stelle, von der Sie das Gerät im Betrieb erhalten haben.

Nur 21 Prozent der im Auftrag von Kaspersky Lab europaweit befragten IT-Leiter konnten bestätigen, dass im Normalfall zwischen dem Verlust und der entsprechenden Meldung durch die Mitarbeiter eine Zeitspanne von nur einer Stunde liegt. In zwölf Prozent aller Fälle vergeht mehr als ein Tag.

So lange haben die Diebe dann Zeit, die vertraulichen Daten von den Geräten zu kopieren und beliebig zu verteilen. Lassen Sie es dazu nicht kommen!

Das Internet ist kein Aktenschrank!

Rund sechs Millionen Deutsche speichern Office-Dokumente im Internet. Cloud-Speicherdienste wie Dropbox, SkyDrive und Google Drive werden wie ein Tresor mit vertraulichen Daten gefüllt. Das könnte schnell ins Auge gehen.

Einfacher Zugriff, auch für andere?

Ob private Fotos, persönliche Briefe, geschäftliche Präsentationen oder digitale Rechnungen - alles wandert ins Internet, um es dort kostenlos oder kostengünstig zu speichern.

Die Cloud-Speicher zum Beispiel von Dropbox, Google oder Microsoft bieten mehrere Gigabyte Speicherkapazität und können sowohl über den Browser als auch über bestimmte mobile Apps erreicht werden. So kann der Nutzer an jedem Ort mit Internetzugang über sein Smartphone ganz bequem auf seine persönlichen Daten zugreifen. Es fragt sich nur, ob er auch der einzige ist, der hier zugreifen kann.

Forscher kritisieren Sicherheitslücken

Bereits vor mehreren Monaten haben Sicherheitsexperten der Fraunhofer-Gesellschaft auf kritische Schwachstellen bei der Sicherheit verschiedener Cloud-Speicher hingewiesen. Gerade die Verschlüsselung ist lückenhaft.

Verschiedene Anbieter haben reagiert und bieten zum Teil neue Sicherheitsfunktionen, häufig aber erst in der professionellen und kostenpflichtigen Version. Doch selbst Unternehmen greifen lieber zu den kostenlosen Varianten und verzichten so auf die notwendige Datensicherheit.

Richtlinien werden missachtet

Der Sicherheitsanbieter Symantec berichtete davon, dass in verschiedenen Unternehmen einzelne Beschäftigte sogar Firmendaten in Cloud-Speicher ablegen, die eigentlich nur für den Privatgebrauch gedacht sind, was den betrieblichen Sicherheitsvorgaben in keinster Weise entspricht.

Dabei sollte eigentlich jedem Internetnutzer klar sein, dass das Internet ohne zusätzliche Sicherheitsmaßnahmen eben kein sicherer Datentresor sein kann. Einfache Passwörter zum Schutz der Cloud-Speicher kann mittlerweile jeder halbwegs begabte Hacker knacken, dank Internet von jedem Punkt der digitalen Welt aus.

Ohne Verschlüsselung geht nichts

So praktisch ein kostenloser Speicherplatz im Internet auch sein mag und so hilfreich der automatische Datenabgleich zwischen Smartphone und Desktop-Computer über den Cloud-Speicher auch ist: Zuerst muss die Datensicherheit stimmen. Schließlich geht es nicht um Daten, die im Internet veröffentlicht werden sollen, sondern um Daten, die eigentlich nur gespeichert werden sollen. Damit die Speicherung im Internet sicher ist, sollte die Verschlüsselung zu jedem Zeitpunkt gewährleistet sein.

Vor dem Hochladen immer verschlüsseln

Es reicht nicht, wenn die Anmeldung beim Cloud-Speicher über eine verschlüsselte Webseite erfolgt, die sich am "https" in der Adresszeile im Webbrowser erkennen lässt.

Neben der Übertragung von Benutzername und Passwort muss jede Datenübertragung zum und vom Cloud-Speicher verschlüsselt sein, also auch das Hochladen und Herunterladen der Dateien.

Damit nicht genug; es gilt auch, Ihre vertraulichen Daten innerhalb von Dropbox & Co. zu schützen. Niemandem außer Ihnen darf es möglich sein, ohne Ihre Zustimmung auf Ihre Daten in der Cloud zuzugreifen, auch nicht den Mitarbeitern des Cloud-Betreibers. Deshalb sollten Sie Ihre Dateien immer vor dem Hochladen verschlüsseln.

TrueCrypt, Cloudfogger & Co.

Möglichkeiten zur Verschlüsselung Ihrer Cloud-Dateien gibt es viele, angefangen bei klassischen Verschlüsselungsprogrammen wie TrueCrypt (www.truecrypt.org) bis hin zu Speziallösungen für Cloud-Speicher wie Cloudfogger (www.cloudfogger.com) oder BoxCryptor (www.boxcryptor.com).

Entscheidend ist, dass Sie die Dateien wirklich verschlüsseln und das Internet nicht mit einem sicheren Aktenschrank verwechseln.

Sind Ihre Dateien im Internet sicher? Testen Sie Ihr Wissen!

Stellen Sie sich vor, Sie wollen eine Angebotspräsentation auf jedem Ihrer Geräte verwenden können, ohne sie immer kopieren zu müssen. Dazu speichern Sie sie in einem Cloud-Dienst. Worauf achten Sie?

a) Ich wähle ein starkes Zugangspasswort für den Cloud-Speicher und gebe mein Passwort im Browser nur ein, wenn die Verbindung verschlüsselt ist (an "https" in der Adresszeile erkennbar).
b) Ich verschlüssele die Präsentation und merke mir meinen digitalen Schlüssel. Erst dann lade ich die Präsentationsdatei in die Cloud.

Lösung: Die Antworten a) und b) in Kombination sind richtig. Ein starkes Passwort und eine verschlüsselte Passwortübertragung sind wichtig, sie sorgen aber nicht für die Sicherheit der Dateien innerhalb des Cloud-Speichers. Eine zusätzliche Verschlüsselung ist ein Muss.

Frage: Sie nutzen einen Cloud-Speicher, dessen Betreiber verspricht, alle Dateien der Kunden zu verschlüsseln. Reicht Ihnen das?

a) Natürlich, denn Verschlüsselung muss sein, und der Anbieter kann dies am besten.
b) Die Verschlüsselung soll die Daten letztlich auch vor dem Cloud-Anbieter schützen. Also sollte meine eigene Verschlüsselung nicht fehlen.

Lösung: Die Antwort b) ist richtig. Wenn nur der Cloud-Anbieter für die Verschlüsselung sorgen will, wissen Sie weder, ob dies tatsächlich passiert, noch haben Sie einen Schutz vor möglichen Datendieben unter den Beschäftigten des Betreibers.