Infobrief Datenschutz
Ausgabe 02 | 2013

agentia wirtschaftsdienst

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

nicht nur das Leben ist voller Überraschungen, auch der Datenschutz ist es. In dieser Ausgabe erfahren Sie zum Beispiel, dass auch Ihr heimisches Büro ein Thema für den betrieblichen Datenschutz sein kann. Wann das der Fall ist und was Sie dann zu beachten haben, lesen Sie im ersten Beitrag.

Eine weitere Überraschung wartet im zweiten Beitrag und womöglich in Ihrem E-Mail-Posteingang auf Sie: Hinter dem Hilferuf eines Freundes kann in Wirklichkeit ein Angriff stecken, ein Versuch, Ihnen Geld und Ihre Bankdaten zu entlocken. Wenn Sie bisher glaubten, es sei am besten, immer die aktuellsten Geräte und Programme zu verwenden, werden Sie erstaunt sein: Für das mobile Banking nehmen Sie lieber Ihr altes Handy. Der dritte Beitrag sagt Ihnen, warum. Und wenn Sie denken, mit einem schwarzen Balken könnten Sie Text in einem digitalen Dokument verbergen, werden Sie erneut verwundert sein.

Viele neue Einsichten wünschen Ihnen Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

Home Office - und der Datenschutz?

Die Arbeit zu Hause soll Wege und Zeit sparen und insgesamt das Leben erleichtern. Das Letzte, was Mitarbeiter und Unternehmen dabei brauchen können, sind Datenschutzprobleme. Lesen Sie, wie sich mit wenigen, relativ einfachen Maßnahmen Schwachstellen vermeiden lassen!

Sie überlegen sich, ein oder zwei Tage pro Woche im Home Office zu arbeiten? Aber Sie haben gehört, da gebe es einigen Papierkram, und ganz so einfach soll es doch nicht sein? Zu Ihrer Beruhigung: Was geregelt und eingerichtet werden muss, ist X-fach erprobt! Am Datenschutz wird es jedenfalls nicht scheitern.

Die Verantwortung des Unternehmens besteht nach wie vor

Der Ausgangspunkt ist klar: Auch wenn ein Mitarbeiter personenbezogene Daten daheim verarbeitet, bleibt das Unternehmen für die Daten verantwortlich. Das wird besonders deutlich, wenn es zu einer "Datenschutzpanne" kommt. Dann halten sich die Betroffenen natürlich an das Unternehmen. Deshalb ist es auch Sache des Unternehmens, für den Datenschutz im Home Office zu sorgen.

Ihre Wohnung bleibt aber Ihre Wohnung

Andererseits ist das Home Office kein Betriebsraum, sondern befindet sich in einer Privatwohnung. Das schränkt den direkten Zugriff durch das Unternehmen ein. Vertragliche Vereinbarungen zwischen Unternehmen und Mitarbeiter müssen das ausgleichen.

Schriftliche Regelungen sind ein Muss

Seien Sie deshalb nicht überrascht, wenn das Unternehmen darauf besteht, mit Ihnen eine schriftliche Vereinbarung zu treffen. Das hat für Sie den Vorteil, dass auch Ihre Pflichten klar geregelt sind. Es gilt das, was in der Vereinbarung steht, nicht mehr und nicht weniger.

Was heißt "Kontrolle vor Ort"?

Lassen Sie sich nicht davon schrecken, wenn die Vereinbarung festlegt, dass eine Kontrolle durch den Datenschutzbeauftragten, die Datenschutzaufsichtsbehörden und Mitarbeiter der EDV-Abteilung vor Ort in Ihrer Wohnung zulässig sein soll. Dabei geht es nur darum, bei auftretenden Problemen - wenn nötig - Dinge an Ort und Stelle zu klären. In der Praxis kommt das bei gut eingerichteten Systemen nur selten vor. Und keine Sorge: Wenn Sie im Urlaub sind, darf niemand ohne Ihre Mitwirkung Ihre Wohnung betreten.

Home Office und Datenschutz sind meist gut miteinander zu vereinbaren (Bild: Thinkstock)

Manche Daten "gehen nicht"

Manche Daten (etwa bestimmte Gesundheitsdaten) sind so heikel, dass sie in einem Home Office nicht verarbeitet werden dürfen. Seien Sie also darauf vorbereitet, dass dieses Argument möglicherweise eine Rolle spielt und zu Einschränkungen führen kann.

Technische Sicherungen sind hilfreich

Ideal wäre es, wenn Sie für das Home Office ein eigenes, abschließbares Zimmer hätten. Sollte das nicht möglich sein, ist noch mehr als sonst auf die Zugriffssicherung an der technischen Ausstattung zu achten. Möglicherweise wird man Ihnen sagen, dass die gewohnte Kombination aus Benutzername und Passwort nicht ausreicht, sondern dass gegenüber der Situation "in der Arbeit" zusätzliche Maßnahmen erforderlich sind. Meistens wird es auch nötig sein, bestimmte Schnittstellen (etwa USB-Anschlüsse) stillzulegen. Wenn etwas unklar ist, fragen Sie nach, gern bei Ihrem Datenschutzbeauftragten!

"Hilf mir bitte gleich" - obwohl ich es gar nicht bin!

Eine Freundin oder ein Freund bittet Sie aus dem Urlaub per E-Mail um Hilfe. Was tun Sie? Klar: Sie kümmern sich sofort darum! Ungünstig nur, wenn sich das Ganze danach als Fake herausstellt, also nichts davon stimmt und Sie beide betrogen worden sind! Informieren Sie sich daher rechtzeitig über eine besonders niederträchtige Masche von Betrügern.

Schreck beim Mail-Check

Sie lesen beim Heimfahren in der S-Bahn schnell Ihre privaten E-Mails, die den Tag über so eingegangen sind. Eine Mail Ihrer Freundin Karin öffnen Sie als Erstes.

Aus den Zeilen spricht Panik. Sie berichtet davon, dass sie in London im Hotel festsitzt, die Tasche mit Ausweis und Kreditkarten ist gestohlen, und Geld hätte sie natürlich auch keines mehr. Sie sollen doch bitte gleich antworten, damit sie Ihnen schreiben kann, wie Sie ihr etwas Geld borgen können.

Ihnen schwirrt der Kopf

Was nun? Ist sie wirklich in Not? Sie sind unsicher und meinen sich zu erinnern, dass sie doch erst nächsten Monat in den Urlaub fahren wollte. Aber andererseits: Vielleicht täuschen Sie sich da, und zudem: Karin war für Sie ja auch da, als damals ...

Also lieber doch gleich antworten? Nein, das sollten Sie auf gar keinen Fall tun!

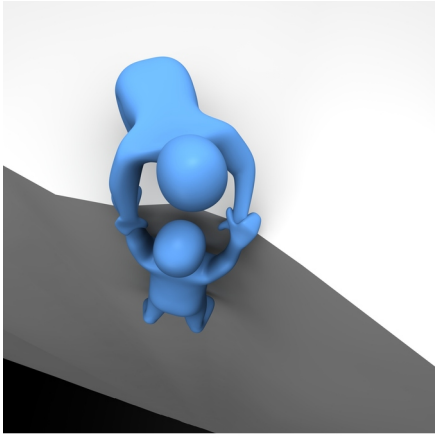
Denken Sie erst nach, ob die E-Mail-Adresse stimmen kann!

Denken Sie erst einmal noch etwas über die Mailadresse nach, die paar Minuten müssen drin sein! Vielleicht stimmt ja alles. Vielleicht ist es aber auch so, dass ein besonders dreister Betrüger am Werk ist. Aber wie kann das sein? Die Mail-Adresse stimmt doch?

Schon bei dem Punkt sollten Sie kritisch sein. Freilich, es ist der Name, den Sie kennen, vielleicht enthält die Mail-Adresse sogar den Vornamen und den Nachnamen. Aber sind Sie sich sicher, dass Ihre Freundin gerade bei diesem Provider überhaupt eine E-Mail-Adresse hat?

Prüfen Sie die Adresse, wenn möglich

Ein kurzer Gegencheck mit der Adresse, die Sie aus früheren Zeiten gespeichert haben, weckt möglicherweise bereits Ihr Misstrauen, wenn Sie Abweichungen feststellen.



Nicht jede E-Mail von Hilfe suchenden Freunden muss echt sein. Schauen Sie lieber ganz genau hin, bevor Sie zu Hilfe eilen.
(Bild: Thinkstock)

Vorsicht: Auch hinter einer echten Adresse kann der Falsche stecken!

Aber selbst wenn hier alles zu passen scheint, gönnen Sie Ihrem Argwohn noch etwas Raum! Denn vielleicht könnte die E-Mail-Adresse ja von einem Betrüger geknackt und geentert worden sein, um sie jetzt für einen fingierten Notruf zu missbrauchen.

Sicher, von solchen Dingen haben Sie gehört. Aber gibt es das wirklich? Und ist es denkbar, dass ausgerechnet Ihre Freundin und Sie davon betroffen werden? Spätestens wenn Sie gleich auf die Mail antworten und dann umgehend Geld schicken, werden Sie die Antwort auf diese Fragen vielleicht rascher kennen, als Ihnen lieb ist! Also übereilen Sie nichts!

Haben Sie vielleicht eine Telefonnummer für einen Rückruf zur Hand?

Die nächste Überlegung sollte sein, ob Sie irgendwo eine Telefonnummer Ihrer Freundin haben, und sei es nur die Büronummer. Falls ja, rufen Sie doch einfach einmal an! Vielleicht erwischen Sie Ihre Freundin dort, und es lässt sich leicht klären, was los ist.

Sagen Sie nicht voreilig, dass ihr das Handy ja wahrscheinlich auch gestohlen worden ist. Wenigstens Mails kann sie ja nachweislich noch schreiben.

Schauen Sie die E-Mail einmal genau an!

Auch einen Anruf können Sie nicht machen, weil Sie die Nummer gerade nicht finden? Dann schauen Sie sich die Mail Ihrer Freundin bitte nochmal genauer an.

Ist die E-Mail so geschrieben, wie die Freundin sonst auch schreibt? Gibt sie eine Telefonnummer an, die ihr wohl nicht gehört, unter der sie aber angeblich zu erreichen ist? Etwa die Nummer der Rezeption eines Hotels oder die angebliche Telefonnummer einer Bank?

Vielleicht hilft das Internet?

Dann wäre es als Nächstes eine gute Idee, diese Telefonnummer einmal zu googeln. Es wäre nicht das erste Mal, dass Sie folgende Überraschung erleben: Die Telefonnummer wurde schon öfter verwendet, um Notlagen vorzugaukeln, und hat mit Ihrer Freundin überhaupt nichts zu tun!

Das Phänomen heißt "Stranded Friend Scam"!

Soviel Niedertracht gibt es wirklich? Leider ja! Schon im Jahr 2005 hat die TU Berlin eine Warnung zum Thema "Stranded Friend Scam" ins Netz gestellt, die seither immer wieder aktualisiert wird. Sie finden sie unter *http://hoax-info.tubit.tu-berlin.de/scam/stranded.shtml*.

Freund sein: Ja. Blöd sein: Nein!

Sollen Sie also künftig nur noch ans Böse glauben? Im Gegenteil! Aber prüfen Sie erst nach, ob die Mail wirklich stimmen kann, und wenn ja, dann helfen Sie bitte auch. Aber mit Verstand und nicht überhastet!

Impressum

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

tel.: 030 2196 4390
fax: 030 2196 4393

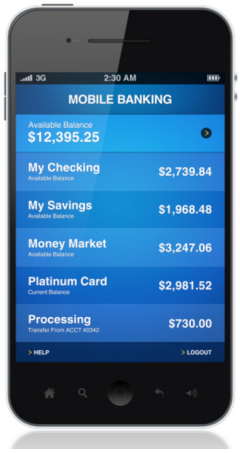
udo.wenzel@agentia.de
thorsten.ritter@agentia.de

Mobile Banking: Besser mit dem alten Handy?

Wenn Sie Ihre Bankgeschäfte im Internet erledigen, kommt immer häufiger das Mobiltelefon zum Einsatz. Lassen Sie die mobilen TANs aber besser nicht auf Ihr neues Smartphone senden, wenn Sie noch keinen professionellen Virenschutz verwenden!

Online-Banking ist beliebt

Über 28 Millionen Deutsche erledigen ihre Bankgeschäfte im Internet. Damit nutzen derzeit über 45 Prozent aller Bundesbürger im Alter von 16 bis 74 Jahren Online-Banking, wie aktuelle Daten der europäischen Statistikbehörde Eurostat zeigen. Jeder vierte Bundesbürger hat allerdings Sicherheitsbedenken, wenn Bankdaten durch das Internet fließen, und dafür gibt es gute Gründe.



Online- und Mobile Banking wollen gut abgesichert sein (Bild: Thinkstock)

Online-Banking ist aber auch riskant

Datendiebe verschicken gefälschte Bank-Mails, locken auf angebliche Bank-Webseiten und versuchen, die Zugangsdaten von Bankkunden und damit deren Geld zu stehlen. Deshalb wurden in den letzten Jahren immer neue Sicherheitsverfahren im Online-Banking eingeführt. Dazu gehören auch die mTANs, also die mobilen Transaktionsnummern. Statt wie früher die Transaktionsnummern zur Bestätigung einer Zahlung von einer Liste zu nehmen, bekommen Sie als Bankkunde heute die TAN auf Ihr Handy oder Smartphone geschickt.

Je aktueller, desto sicherer?

Generell kann man davon ausgehen, dass moderne Geräte und Betriebssysteme sicherer sind, denn bei ihnen wurden viele Sicherheitsmängel der Vergangenheit behoben. Doch tatsächlich sind moderne Smartphones nicht automatisch sicherer als alte Handys, wenn es ums Banking geht. Das Gegenteil ist oftmals eher der Fall.

Auch mobile TANs werden gestohlen

Viele Sicherheitsexperten halten die Attacken auf mobile Endgeräte für das größte Datenrisiko im Jahr 2013. Immer mehr mobile Schadprogramme kursieren im Internet. Dazu gehören auch Trojaner, die speziell die Aufgabe haben, mobile TANs einzusammeln, die Banken per SMS an den Mobiltelefon-Nutzer senden. Die mTANs werden dann sofort und heimlich an den Datendieb weitergeleitet, der die Zeit der Gültigkeit der mTAN ausnutzt und kriminelle Transaktionen mit dem Bankkonto des Opfers ausführt.

Neue Smartphones im Fokus

Die meisten Angriffe auf Mobiltelefone gelten modernen Geräten wie Android-Smartphones, iPhones und Windows Phones. So warnte in den letzten Monaten das Berliner Landeskriminalamt speziell vor einem Trojaner, der mTANs oder SMS-TANs auf Android-Smartphones abfangen und an Datendiebe weiterleiten konnte. Zuvor wurden die Opfer angeblich von ihrer Bank darum gebeten, ein Sicherheits-Update bei ihrem Android-Smartphone einzuspielen. In Wirklichkeit kam so der Banking-Trojaner an Bord.

Alte Handys, geringere Gefahren?

Die wichtigste Maßnahme zum Schutz gegen solche Banking-Trojaner ist und bleibt ein professioneller, aktueller Antivirenschutz, den es inzwischen für fast jedes Smartphone gibt.

Aber auch eine andere Maßnahme ist sinnvoll: Nutzen Sie lieber Ihr altes Handy zum Empfang der SMS-TANs. Alte Handys haben Betriebssysteme mit weniger Funktionen, für die es kaum Schadprogramme gibt. Android-Trojaner zum Beispiel können auf einem alten Handy mit einem alten Betriebssystem nichts anstellen. Allerdings gibt es kaum aktuelle Sicherheitssoftware für solche Handys.

So wird mobiles Banking sicherer

Deshalb ist ein Mix an Sicherheitsmaßnahmen erforderlich. Die folgenden Tipps helfen Ihnen, das Online-Banking in Verbindung mit Smartphone und Handy sicherer zu machen und Ihre Bankdaten auch im mobilen Internet besser zu schützen:

1. Verwenden Sie immer eine aktuelle und professionelle Antivirensoftware.

2. Nutzen Sie zum Banking immer nur die Bank-Webseite, die nach Eingabe der Ihnen bekannten Webadresse erscheint. Suchen Sie die Website der Bank nicht über Suchmaschinen, deren Treffer manipuliert sein könnten. Das gilt auch für mobile Browser.

3. Klicken Sie auf keine Links in E-Mails, die angeblich von Ihrer Bank kommen, ob am PC oder auf dem Smartphone.

4. Informieren Sie sich regelmäßig in den Medien, welche Angriffe stattfinden. Nutzen Sie lieber Ihr altes Handy, wenn zum Beispiel Android-Smartphones attackiert werden.

5. Speichern Sie keine Banking-Zugangsdaten oder andere Passwörter auf Ihrem Mobiltelefon.

6. Machen Sie Gebrauch von den aktuellen Sicherheitsverfahren Ihrer Bank, aber erst, wenn Sie mit dem Umgang wirklich vertraut sind.

7. Wenn Sie das komplette Online-Banking auf dem Smartphone machen wollen: Nutzen Sie Ihr Smartphone nicht für den Empfang der mTANs, sondern verwenden Sie dann zwei verschiedene Mobiltelefone und Mobilnummern. Andernfalls könnten Trojaner auf Ihrem Smartphone mit nur einer Infektion die mTANs und die mobile Banking-Software missbrauchen.

8. Verschlüsseln Sie sämtliche Banking-Dateien (z.B. Bankauszüge im PDF-Format), die Sie herunterladen. Noch besser ist es, gar keine Banking-Dateien auf Mobiltelefonen zu speichern. Denn mobile Geräte gehen leicht verloren.

Hier sollten Sie schwarzsehen!

Wenn bestimmte Passagen in Dokumenten für andere nicht sichtbar sein sollen, greift man oftmals zur Schwärzung der betreffenden Stellen. Das ist auch in elektronischen Dokumenten zuverlässig möglich - wenn man weiß, wie es geht.

Kein gutes Versteck!

In so manchem geschäftlichen Dokument verbergen sich mehr vertrauliche Daten, als man glaubt. So kann ein scheinbar allgemeines Projektdokument auch konkrete Hinweise zur Umsetzung bei einem Kunden enthalten, mit den kompletten Kontaktdaten des Kunden für den Fall einer Rückfrage.

Bevor das Dokument im weiten Feld der Projektteilnehmer verteilt wird, müssen vertrauliche Daten gezielt entfernt werden. Bei Ausdrucken greift man dazu oftmals zur Schwärzung der vertraulichen Passagen.

Digitale Ausdrucke nicht vergessen

Schon das Schwärzen bei Papierdokumenten will gelernt sein, damit Dritte die zu schützenden Textstellen nicht doch lesen können. Bei digitalen Ausdrucken, wie zum Beispiel bei den beliebten PDF-Dokumenten, wird es für die meisten Anwender noch schwieriger und fehleranfälliger. Statt die betreffenden Passagen aus der Ausgangsdatei zu löschen, werden Versuche mit schwarzen Balken gestartet, in Anlehnung an die Schwärzung bei Papierausdrucken.

Zwischen den Zeilen lesen

Wenn Sie ein Word-Dokument mit vertraulichen Stellen als PDF-Dokument verteilen wollen und eine Löschung der Passagen nicht in Betracht kommt, dann dürfen Sie nicht über die schwarzen Balken stolpern. Werden einfache schwarze Balken als Bildchen über die zu schützenden Stellen gelegt und das PDF-Dokument daraus erstellt, kann der Empfänger womöglich den Text unter den schwarzen Balken lesen!

Selbst im Anti-Terror-Kampf falsch geschwärzt

Der Fehler mit den schwarzen Balken passiert selbst Anti-Terror-Experten, die streng vertrauliche Teile eines Einsatzplans falsch geschwärzt hatten. Die einfachen schwarzen Balken überdecken die Daten nur. Ein Kopieren des Textabschnitts mit Copy & Paste rings um den Balken bringt die geheimen Daten schnell wieder zum Vorschein.

Löschen, ersetzen, anonymisieren

Sollen in einem Dokument vor dem Ausdruck oder vor der Übertragung in eine PDF-Datei spezielle Stellen geschützt werden, geht dies am besten durch ein gezieltes Löschen, durch das Ersetzen der Passagen durch nichtssagende Zeichen oder durch das Anonymisieren der personenbezogenen Daten im Text. Alternativ kann auch Spezialsoftware helfen.

Automatisch schwarz

Sogenannte Redaction-Software kann Dateien so bearbeiten, dass die vertraulichen Stellen automatisch durch schwarze Stellen ersetzt, nicht aber einfach nur überlagert werden. Dabei gibt man einer solchen Software vor, welche Art von Daten sie vor Erstellung der PDF-Datei schwärzen soll. Die Software sucht die entsprechenden Schlagwörter und Datenarten im Text und sorgt für eine digitale Schwärzung. Solch ein Verfahren ist bequem, klappt aber nicht immer hundertprozentig. Deshalb muss man das Ergebnisdokument immer gegenprüfen.

Sollen vertrauliche Daten vertraulich bleiben, darf man nicht einfach nur zum schwarzen Balken greifen (Bild: Thinkstock)

Vorsicht: Änderungsmodus und Metadaten

Aber selbst wenn Sie die vertraulichen Stellen löschen und dann erst die Dateien an die anderen Projektpartner verteilen: Denken Sie an die Funktion, Änderungen in Office-Dokumenten sichtbar und rückgängig zu machen. Vergessen Sie auch nicht die Dateieigenschaften (Metadaten), die so manche vertrauliche Informationen enthalten können und sich nicht so einfach schwärzen lassen.

Nutzen Sie deshalb vor Verteilung einer Datei immer den Dokumenten-Inspektor in Ihrem Office-Programm, mit dem sich Änderungsmarkierungen und Metadaten löschen lassen.

Schwärzen Sie richtig? Machen Sie den Test!

Frage: Ein Kollege sagt Ihnen, dass man vertrauliche Stellen in Word-Dateien dadurch verbergen kann, dass man die Schriftfarbe für diese Passagen auf Weiß stellt. Was sagen Sie dazu?

a) Tolle Idee, denn wer kann schon weiße Schrift auf weißem Hintergrund lesen.
b) Das klappt aber nur, wenn der Hintergrund in dem Word-Dokument nicht farbig ist.
c) Das ist unsicher und falsch. Denn mit einer einfachen Markierung des Textes in der PDF-Datei kann man die Stellen wieder lesen.

Lösung: Die Antwort c) ist richtig. Solange die Zeichen in der Datei ungeschützt enthalten sind, kann man sie auch finden und sichtbar machen. Weiße Schrift ist also keine Geheimtinte.

Frage: Wenn man vertrauliche Stellen in Word-Dateien durch nichtssagenden Text ersetzt, ist dies die beste Schwärzung. Stimmt das?

a) Nicht unbedingt, denn unter Umständen kann man die Änderungen in der Datei sichtbar und rückgängig machen.
b) Ja, denn damit vermeidet man die Verwendung eines schwarzen Balkens, die bekanntlich bei Dateien unsicher ist.

Lösung: Die Antwort a) ist richtig. Die Ersetzung von vertraulichen Zeichen ist zwar eine gute Möglichkeit, aber nur, wenn man die Änderungsmarkierungen zuverlässig entfernt. Dazu nimmt man den sogenannten Dokumenten-Inspektor (siehe Word-Hilfe).